



config コマンド : r ~ z

- [config radius acct](#) (11 ページ)
- [config radius acct ipsec authentication](#) (15 ページ)
- [config radius acct ipsec disable](#) (16 ページ)
- [config radius acct ipsec enable](#) (17 ページ)
- [config radius acct ipsec encryption](#) (18 ページ)
- [config radius acct ipsec ike](#) (19 ページ)
- [config radius acct mac-delimiter](#) (20 ページ)
- [config radius acct network](#) (21 ページ)
- [config radius acct realm](#) (22 ページ)
- [config radius acct retransmit-timeout](#) (23 ページ)
- [config radius auth](#) (24 ページ)
- [config radius auth callStationIdType](#) (27 ページ)
- [config radius auth framed-mtu](#) (30 ページ)
- [config radius auth IPsec authentication](#) (31 ページ)
- [config radius auth ipsec disable](#) (32 ページ)
- [config radius auth ipsec encryption](#) (33 ページ)
- [config radius auth ipsec ike](#) (34 ページ)
- [config radius auth keywrap](#) (36 ページ)
- [config radius auth mac-delimiter](#) (37 ページ)
- [config radius auth management](#) (38 ページ)
- [config radius auth mgmt-retransmit-timeout](#) (39 ページ)
- [config radius auth network](#) (40 ページ)
- [config radius auth realm](#) (41 ページ)
- [config radius auth retransmit-timeout](#) (42 ページ)
- [config radius auth rfc3576](#) (43 ページ)
- [config radius auth retransmit-timeout](#) (44 ページ)
- [config radius aggressive-failover disabled](#) (45 ページ)
- [config radius backward compatibility](#) (46 ページ)
- [config radius callStationIdCase](#) (47 ページ)

- `config radius callStationIdType` (48 ページ)
- `config radius dns` (51 ページ)
- `config radius fallback-test` (53 ページ)
- `config radius ext-source-ports` (55 ページ)
- `config radius acct retransmit-timeout` (56 ページ)
- `config radius auth mgmt-retransmit-timeout` (57 ページ)
- `config radius auth retransmit-timeout` (58 ページ)
- `config radius auth retransmit-timeout` (59 ページ)
- `config redundancy interface address peer-service-port` (60 ページ)
- `config redundancy mobilitymac` (61 ページ)
- `config redundancy mode` (62 ページ)
- `config redundancy peer-route` (63 ページ)
- `config redundancy timer keep-alive-timer` (64 ページ)
- `config redundancy timer peer-search-timer` (65 ページ)
- `config redundancy unit` (66 ページ)
- `config remote-lan` (67 ページ)
- `config remote-lan aaa-override` (68 ページ)
- `config remote-lan acl` (69 ページ)
- `config remote-lan apgroup` (70 ページ)
- `config remote-lan create` (71 ページ)
- `config remote-lan custom-web` (72 ページ)
- `config remote-lan delete` (75 ページ)
- `config remote-lan dhcp_server` (76 ページ)
- `config remote-lan exclusionlist` (77 ページ)
- `config remote-lan host-mode` (78 ページ)
- `config remote-lan interface` (79 ページ)
- `config remote-lan ldap` (80 ページ)
- `config remote-lan mac-filtering` (81 ページ)
- `config remote-lan mab` (82 ページ)
- `config remote-lan max-associated-clients` (83 ページ)
- `config remote-lan pre-auth` (84 ページ)
- `config remote-lan radius_server` (85 ページ)
- `config remote-lan security` (87 ページ)
- `config remote-lan session-timeout` (88 ページ)
- `config remote-lan violation-mode` (89 ページ)
- `config remote-lan webauth-exclude` (90 ページ)
- `config rf-profile band-select` (91 ページ)
- `config rf-profile channel` (93 ページ)
- `config rf-profile client-trap-threshold` (94 ページ)
- `config rf-profile create` (95 ページ)
- `config rf-profile fra client-aware` (96 ページ)

- [config rf-profile data-rates](#) (97 ページ)
- [config rf-profile delete](#) (99 ページ)
- [config rf-profile description](#) (100 ページ)
- [config rf-profile fra client-aware](#) (101 ページ)
- [config rf-profile load-balancing](#) (102 ページ)
- [config rf-profile max-clients](#) (104 ページ)
- [config rf-profile multicast data-rate](#) (105 ページ)
- [config rf-profile out-of-box](#) (106 ページ)
- [config rf-profile rx-sop threshold](#) (107 ページ)
- [config rf-profile trap-threshold](#) (108 ページ)
- [config rf-profile tx-power-control-thresh-v1](#) (109 ページ)
- [config rf-profile tx-power-control-thresh-v2](#) (110 ページ)
- [config rf-profile tx-power-max](#) (111 ページ)
- [config rf-profile tx-power-min](#) (112 ページ)
- [config rogue ap timeout](#) (113 ページ)
- [config rogue adhoc](#) (114 ページ)
- [config rogue ap classify](#) (118 ページ)
- [config rogue ap friendly](#) (121 ページ)
- [config rogue ap rldp](#) (123 ページ)
- [config rogue ap ssid](#) (125 ページ)
- [config rogue ap timeout](#) (127 ページ)
- [config rogue auto-contain level](#) (128 ページ)
- [config rogue ap valid-client](#) (130 ページ)
- [config rogue client](#) (132 ページ)
- [config rogue containment](#) (134 ページ)
- [config rogue detection](#) (135 ページ)
- [config rogue detection client-threshold](#) (136 ページ)
- [config rogue detection min-rssi](#) (137 ページ)
- [config rogue detection monitor-ap](#) (138 ページ)
- [config rogue detection report-interval](#) (140 ページ)
- [config rogue detection security-level](#) (141 ページ)
- [config rogue detection transient-rogue-interval](#) (142 ページ)
- [config rogue rule](#) (143 ページ)
- [config rogue rule condition ap](#) (148 ページ)
- [config remote-lan session-timeout](#) (150 ページ)
- [config rfid auto-timeout](#) (151 ページ)
- [config rfid status](#) (152 ページ)
- [config rfid timeout](#) (153 ページ)
- [config rogue ap timeout](#) (154 ページ)
- [config route add](#) (155 ページ)
- [config route delete](#) (156 ページ)

- [config serial baudrate](#) (157 ページ)
- [config serial timeout](#) (158 ページ)
- [config service timestamps](#) (159 ページ)
- [config sessions maxsessions](#) (160 ページ)
- [config sessions timeout](#) (161 ページ)
- [config slot](#) (162 ページ)
- [config switchconfig boot-break](#) (164 ページ)
- [config switchconfig fips-prerequisite](#) (165 ページ)
- [config switchconfig ucapl](#) (166 ページ)
- [config switchconfig wlance](#) (167 ページ)
- [config switchconfig strong-pwd](#) (168 ページ)
- [config switchconfig flowcontrol](#) (171 ページ)
- [config switchconfig mode](#) (172 ページ)
- [config switchconfig secret-obfuscation](#) (173 ページ)
- [config sysname](#) (174 ページ)
- [config snmp community accessmode](#) (175 ページ)
- [config snmp community create](#) (176 ページ)
- [config snmp community delete](#) (177 ページ)
- [config snmp community ipaddr](#) (178 ページ)
- [config snmp community mode](#) (179 ページ)
- [config snmp engineID](#) (180 ページ)
- [config snmp syscontact](#) (181 ページ)
- [config snmp syslocation](#) (182 ページ)
- [config snmp trapreceiver create](#) (183 ページ)
- [config snmp trapreceiver delete](#) (184 ページ)
- [config snmp trapreceiver mode](#) (185 ページ)
- [config snmp v3user create](#) (186 ページ)
- [config snmp v3user delete](#) (188 ページ)
- [config snmp version](#) (189 ページ)
- [config tacacs acct](#) (190 ページ)
- [config tacacs auth](#) (192 ページ)
- [config tacacs auth mgmt-server-timeout](#) (194 ページ)
- [config tacacs dns](#) (195 ページ)
- [config tacacs fallback-test interval](#) (197 ページ)
- [config time manual](#) (198 ページ)
- [config time ntp](#) (199 ページ)
- [config time ntp version](#) (202 ページ)
- [config time timezone](#) (203 ページ)
- [config time timezone location](#) (204 ページ)
- [config trapflags 802.11-Security](#) (208 ページ)
- [config trapflags aaa](#) (209 ページ)

- [config trapflags adjchannel-rogueap \(210 ページ\)](#)
- [config trapflags ap \(211 ページ\)](#)
- [config trapflags authentication \(212 ページ\)](#)
- [config trapflags client \(213 ページ\)](#)
- [config trapflags client max-warning-threshold \(215 ページ\)](#)
- [config trapflags configsave \(217 ページ\)](#)
- [config trapflags IPsec \(218 ページ\)](#)
- [config trapflags linkmode \(220 ページ\)](#)
- [config trapflags mesh \(221 ページ\)](#)
- [config trapflags multiusers \(222 ページ\)](#)
- [config trapflags rfid \(223 ページ\)](#)
- [config trapflags rogueap \(225 ページ\)](#)
- [config trapflags rrm-params \(226 ページ\)](#)
- [config trapflags rrm-profile \(227 ページ\)](#)
- [config trapflags stpmode \(228 ページ\)](#)
- [config trapflags strong-pwdcheck \(229 ページ\)](#)
- [config trapflags wps \(230 ページ\)](#)
- [config tunnel eogre heart-beat \(231 ページ\)](#)
- [config tunnel eogre gateway \(232 ページ\)](#)
- [config tunnel eogre domain \(233 ページ\)](#)
- [config tunnel eogre domain primary \(234 ページ\)](#)
- [config tunnel profile \(235 ページ\)](#)
- [config tunnel profile_rule \(236 ページ\)](#)
- [config tunnel profile_rule-delete \(237 ページ\)](#)
- [config tunnel profile eogre-DHCP82 \(238 ページ\)](#)
- [config tunnel profile eogre-gateway-radius-proxy \(239 ページ\)](#)
- [config tunnel profile eogre-gateway-radius-proxy-accounting \(240 ページ\)](#)
- [config tunnel profile eogre-DHCP82 \(241 ページ\)](#)
- [config tunnel profile eogre-DHCP82-circuit-id \(242 ページ\)](#)
- [config tunnel profile eogre-DHCP82-delimiter \(243 ページ\)](#)
- [config tunnel profile eogre-DHCP82-format \(244 ページ\)](#)
- [config tunnel profile eogre-DHCP82-remote-id \(245 ページ\)](#)
- [config watchlist add \(246 ページ\)](#)
- [config watchlist delete \(247 ページ\)](#)
- [config watchlist disable \(248 ページ\)](#)
- [config watchlist enable \(249 ページ\)](#)
- [config wgb vlan \(250 ページ\)](#)
- [config wlan \(251 ページ\)](#)
- [config wlan 7920-support \(253 ページ\)](#)
- [config wlan 802.11e \(254 ページ\)](#)
- [config wlan aaa-override \(255 ページ\)](#)

- [config wlan acl \(257 ページ\)](#)
- [config wlan apgroup \(258 ページ\)](#)
- [config wlan apgroup atf 802.11 \(267 ページ\)](#)
- [config wlan apgroup atf 802.11 policy \(268 ページ\)](#)
- [config wlan apgroup.opendns-profile \(269 ページ\)](#)
- [config wlan apgroup qinq \(270 ページ\)](#)
- [config wlan assisted-roaming \(272 ページ\)](#)
- [config wlan atf \(273 ページ\)](#)
- [config wlan avc \(274 ページ\)](#)
- [config wlan band-select allow \(275 ページ\)](#)
- [config wlan broadcast-ssid \(276 ページ\)](#)
- [config wlan call-snoop \(277 ページ\)](#)
- [config wlan chd \(278 ページ\)](#)
- [config wlan ccx aironet-ie \(279 ページ\)](#)
- [config wlan channel-scan defer-priority \(280 ページ\)](#)
- [config wlan channel-scan defer-time \(281 ページ\)](#)
- [config wlan custom-web \(282 ページ\)](#)
- [config wlan dhcp_server \(284 ページ\)](#)
- [config wlan diag-channel \(285 ページ\)](#)
- [config wlan dtim \(286 ページ\)](#)
- [config wlan exclusionlist \(287 ページ\)](#)
- [config wlan fabric \(288 ページ\)](#)
- [config wlan fabric acl \(289 ページ\)](#)
- [config wlan fabric avc-policy \(290 ページ\)](#)
- [config wlan fabric encap vxlan \(291 ページ\)](#)
- [config wlan fabric switch-ip \(292 ページ\)](#)
- [config wlan fabric tag \(293 ページ\)](#)
- [config wlan fabric vnid \(294 ページ\)](#)
- [config wlan fabric avc-policy \(295 ページ\)](#)
- [config wlan flexconnect ap-auth \(296 ページ\)](#)
- [config wlan flexconnect central-assoc \(297 ページ\)](#)
- [config wlan flexconnect learn-ipaddr \(298 ページ\)](#)
- [config wlan flexconnect local-switching \(299 ページ\)](#)
- [config wlan flexconnect vlan-central-switching \(301 ページ\)](#)
- [config wlan flow \(302 ページ\)](#)
- [config wlan hotspot \(303 ページ\)](#)
- [config wlan hotspot dot11u \(304 ページ\)](#)
- [config wlan hotspot dot11u 3gpp-info \(305 ページ\)](#)
- [config wlan hotspot dot11u auth-type \(306 ページ\)](#)
- [config wlan hotspot dot11u disable \(307 ページ\)](#)
- [config wlan hotspot dot11u domain \(308 ページ\)](#)

- [config wlan hotspot dot11u enable](#) (309 ページ)
- [config wlan hotspot dot11u hessid](#) (310 ページ)
- [config wlan hotspot dot11u ipaddr-type](#) (311 ページ)
- [config wlan hotspot dot11u nai-realm](#) (312 ページ)
- [config wlan hotspot dot11u network-type](#) (315 ページ)
- [config wlan hotspot dot11u roam-oi](#) (316 ページ)
- [config wlan hotspot hs2](#) (317 ページ)
- [config wlan hotspot hs2 domain-id](#) (320 ページ)
- [config wlan hotspot hs2 osu legacy-ssid](#) (321 ページ)
- [config wlan hotspot hs2 osu sp create](#) (322 ページ)
- [config wlan hotspot hs2 osu sp delete](#) (323 ページ)
- [config wlan hotspot hs2 osu sp icon-file add](#) (324 ページ)
- [config wlan hotspot hs2 osu sp icon-file delete](#) (325 ページ)
- [config wlan hotspot hs2 osu sp method add](#) (326 ページ)
- [config wlan hotspot hs2 osu sp method delete](#) (327 ページ)
- [config wlan hotspot hs2 osu sp nai add](#) (328 ページ)
- [config wlan hotspot hs2 osu sp nai delete](#) (329 ページ)
- [config wlan hotspot hs2 osu sp uri add](#) (330 ページ)
- [config wlan hotspot hs2 osu sp uri delete](#) (331 ページ)
- [config wlan hotspot hs2 wan-metrics downlink](#) (332 ページ)
- [config wlan hotspot hs2 wan-metrics link-status](#) (333 ページ)
- [config wlan hotspot hs2 wan-metrics lmd](#) (334 ページ)
- [config wlan hotspot hs2 wan-metrics uplink](#) (335 ページ)
- [config wlan hotspot msap](#) (336 ページ)
- [config wlan interface](#) (337 ページ)
- [config wlan ipv6 acl](#) (338 ページ)
- [config wlan kts-cac](#) (339 ページ)
- [config wlan layer2 acl](#) (340 ページ)
- [config wlan ldap](#) (341 ページ)
- [config wlan learn-ipaddr-cswlan](#) (342 ページ)
- [config wlan load-balance](#) (343 ページ)
- [config wlan lobby-admin-access](#) (344 ページ)
- [config wlan mac-filtering](#) (345 ページ)
- [config wlan max-associated-clients](#) (346 ページ)
- [config wlan max-radio-clients](#) (347 ページ)
- [config wlan mdns](#) (348 ページ)
- [config wlan media-stream](#) (349 ページ)
- [config wlan mfp](#) (350 ページ)
- [config wlan mobility anchor](#) (351 ページ)
- [config wlan mobility foreign-map](#) (352 ページ)
- [config wlan multicast buffer](#) (353 ページ)

- [config wlan multicast interface \(354 ページ\)](#)
- [config wlan mu-mimo \(355 ページ\)](#)
- [config wlan nac \(356 ページ\)](#)
- [config wlan override-rate-limit \(357 ページ\)](#)
- [config wlan opendns-mode \(359 ページ\)](#)
- [config wlan opendns-profile \(360 ページ\)](#)
- [config wlan passive-client \(361 ページ\)](#)
- [config wlan peer-blocking \(362 ページ\)](#)
- [config wlan pmipv6 default-realm \(363 ページ\)](#)
- [config wlan pmipv6 mobility-type \(364 ページ\)](#)
- [config wlan pmipv6 profile_name \(365 ページ\)](#)
- [config wlan policy \(366 ページ\)](#)
- [config wlan profile \(367 ページ\)](#)
- [config wlan profiling \(368 ページ\)](#)
- [config wlan qos \(370 ページ\)](#)
- [config wlan radio \(371 ページ\)](#)
- [config wlan radius_server acct \(372 ページ\)](#)
- [config wlan radius_server acct interim-update \(374 ページ\)](#)
- [config wlan radius_server auth \(375 ページ\)](#)
- [config wlan radius_server overwrite-interface \(376 ページ\)](#)
- [config wlan radius_server realm \(377 ページ\)](#)
- [config wlan roamed-voice-client re-anchor \(378 ページ\)](#)
- [config wlan security 802.1X \(379 ページ\)](#)
- [config wlan security ckip \(381 ページ\)](#)
- [config wlan security cond-web-redir \(383 ページ\)](#)
- [config wlan security eap-params \(384 ページ\)](#)
- [config wlan security eap-passthru \(386 ページ\)](#)
- [config wlan security ft \(387 ページ\)](#)
- [config wlan security ft over-the-ds \(388 ページ\)](#)
- [config wlan security IPsec disable \(389 ページ\)](#)
- [config wlan security IPsec enable \(390 ページ\)](#)
- [config wlan security IPsec authentication \(391 ページ\)](#)
- [config wlan security IPsec encryption \(392 ページ\)](#)
- [config wlan security IPsec config \(393 ページ\)](#)
- [config wlan security IPsec ike authentication \(394 ページ\)](#)
- [config wlan security IPsec ike dh-group \(395 ページ\)](#)
- [config wlan security IPsec ike lifetime \(396 ページ\)](#)
- [config wlan security IPsec ike phase1 \(397 ページ\)](#)
- [config wlan security IPsec ike contivity \(398 ページ\)](#)
- [config wlan security wpa akm ft \(399 ページ\)](#)
- [config wlan security ft \(400 ページ\)](#)

- [config wlan security passthru](#) (401 ページ)
- [config wlan security pmf](#) (402 ページ)
- [config wlan security sgt](#) (404 ページ)
- [config wlan security splash-page-web-redir](#) (405 ページ)
- [config wlan security static-wep-key authentication](#) (406 ページ)
- [config wlan security static-wep-key disable](#) (407 ページ)
- [config wlan security static-wep-key enable](#) (408 ページ)
- [config wlan security static-wep-key encryption](#) (409 ページ)
- [config wlan security tkip](#) (410 ページ)
- [config wlan usertimeout](#) (411 ページ)
- [config wlan security web-auth](#) (412 ページ)
- [config wlan security web-auth captive-bypass](#) (414 ページ)
- [config wlan security web-auth qrscan-des-key](#) (415 ページ)
- [config wlan security web-passthrough acl](#) (416 ページ)
- [config wlan security web-passthrough disable](#) (417 ページ)
- [config wlan security web-passthrough email-input](#) (418 ページ)
- [config wlan security web-passthrough enable](#) (419 ページ)
- [config wlan security web-passthrough qr-scan](#) (420 ページ)
- [config wlan security wpa akm 802.1x](#) (421 ページ)
- [config wlan security wpa akm cckm](#) (422 ページ)
- [config wlan security wpa akm ft](#) (423 ページ)
- [config wlan security wpa akm pmf](#) (424 ページ)
- [config wlan security wpa akm psk](#) (425 ページ)
- [config wlan security wpa disable](#) (426 ページ)
- [config wlan security wpa enable](#) (427 ページ)
- [config wlan security wpa ciphers](#) (428 ページ)
- [config wlan security wpa gtk-random](#) (429 ページ)
- [config wlan security wpa osen disable](#) (430 ページ)
- [config wlan security wpa osen enable](#) (431 ページ)
- [config wlan security wpa wpa1 disable](#) (432 ページ)
- [config wlan security wpa wpa1 enable](#) (433 ページ)
- [config wlan security wpa wpa2 disable](#) (434 ページ)
- [config wlan security wpa wpa2 enable](#) (435 ページ)
- [config wlan security wpa wpa2 cache](#) (436 ページ)
- [config wlan security wpa wpa2 cache sticky](#) (437 ページ)
- [config wlan security wpa wpa2 ciphers](#) (438 ページ)
- [config wlan session-timeout](#) (439 ページ)
- [config wlan sip-cac disassoc-client](#) (441 ページ)
- [config wlan sip-cac send-486busy](#) (442 ページ)
- [config wlan ssid](#) (443 ページ)
- [config wlan static-ip tunneling](#) (444 ページ)

- config wlan uapsd compliant client enable (445 ページ)
- config wlan uapsd compliant-client disable (446 ページ)
- config wlan url-acl (447 ページ)
- config wlan user-idle-threshold (448 ページ)
- config wlan usertimeout (449 ページ)
- config wlan webauth-exclude (450 ページ)
- config wlan wgb broadcast-tagging (451 ページ)
- config wlan wifidirect (452 ページ)
- config wlan wmm (453 ページ)
- config wps ap-authentication (454 ページ)
- config wps auto-immune (455 ページ)
- config wps cids-sensor (456 ページ)
- config wps client-exclusion (458 ページ)
- config wps mfp (460 ページ)
- config wps shun-list re-sync (461 ページ)
- config wps signature (462 ページ)
- config wps signature frequency (464 ページ)
- config wps signature interval (465 ページ)
- config wps signature mac-frequency (466 ページ)
- config wps signature quiet-time (467 ページ)
- config wps signature reset (468 ページ)

config radius acct

Cisco ワイヤレス LAN コントローラ の RADIUS アカウンティング サーバの設定を行うには、**config radius acct** コマンドを使用します。

```
config radius acct { {add index IP addr port {ascii | hex} secret} | delete index | disable
index | enable index | ipsec {authentication {hmac-md5 index | hmac-sha1 index} |
disable index | enable index | encryption {256-aes | 3des | aes | des} index | ike
{auth-mode {pre-shared-key index type shared_secret_key | certificate index} | dh-group {
2048bit-group-14 | group-1 | group-2 | group-5} index | lifetime seconds index | phase1
{aggressive | main} index } } | {mac-delimiter {colon | hyphen | none |
single-hyphen} } | {network index {disable | enable} } | {region {group | none |
provincial} } | retransmit-timeout index seconds | realm {add | delete} index realm-string }
```

構文の説明

| | |
|----------------|---|
| add | RADIUS アカウンティング サーバ (IPv4 または IPv6) を追加します。 |
| <i>index</i> | RADIUS サーバインデックス (1 ~ 17)。 |
| <i>ip-addr</i> | RADIUS サーバの IP アドレス (IPv4 または IPv6)。 |
| <i>port</i> | RADIUS サーバのインターフェイス プロトコルの UDP ポート番号。 |
| ascii | RADIUS サーバの共有キーのタイプ (ascii) を指定します。 |
| hex | RADIUS サーバの共有キーのタイプ (hex) を指定します。 |
| <i>secret</i> | RADIUS サーバのシークレット。 |
| enable | RADIUS アカウンティング サーバを有効にします。 |
| disable | RADIUS アカウンティング サーバを無効にします。 |
| delete | RADIUS アカウンティング サーバを削除します。 |
| ipsec | <p>アカウンティングサーバに対する IPSec サポートを有効または無効にします。</p> <p>(注) IPSec は IPv6 ではサポートされません。</p> |

| | |
|-------------------------|---|
| authentication | IPSec 認証を設定します。 |
| hmac-md5 | IPSec HMAC-MD5 認証を有効にします。 |
| hmac-sha1 | IPSec HMAC-SHA1 認証を有効にします。 |
| disable | アカウントティングサーバに対する IPSec サポートを無効にします。 |
| enable | アカウントティングサーバに対する IPSec サポートを有効にします。 |
| encryption | IPSec 暗号化を設定します。 |
| 256-aes | IPSec AES 暗号化を有効にします。 |
| 3des | IPSec 3DES 暗号化を有効にします。 |
| aes | IPSec AES-128 暗号化を有効にします。 |
| des | IPSec DES 暗号化を有効にします。 |
| ike | インターネット キー エクスチェンジ (IKE) を設定します。 |
| auth-mode | IKE 認証方式を設定します。 |
| pre-shared-key | 認証の事前共有キー。 |
| certificate | 認証に使用される証明書。 |
| dh-group | IKE Diffie-Hellman グループを設定します。 |
| 2048bit-group-14 | DH グループ 14 (2048 ビット) を設定します。 |
| group-1 | DH グループ 1 (768 ビット) を設定します。 |
| group-2 | DH グループ 2 (1024 ビット) を設定します。 |
| group-5 | DH グループ 5 (1536 ビット) を設定します。 |
| lifetime seconds | IKE ライフタイム (秒単位) を設定します。指定できる範囲は 1800 ~ 57600 秒です。デフォルトは 28800 秒です。 |
| phase1 | IKE phase1 モードを設定します。 |
| aggressive | IKE アグレッシブ モードを有効にします。 |
| main | IKE メイン モードを有効にします。 |

| | |
|---------------------------|--|
| mac-delimiter | コール元ステーション ID とコール先ステーション ID の MAC デリミタを設定します。 |
| colon | デリミタをコロンに設定します (xx:xx:xx:xx:xx:xx など)。 |
| hyphen | デリミタをハイフンに設定します (xx-xx-xx-xx-xx-xx など)。 |
| none | デリミタを無効にします (xxxxxxxxxx など)。 |
| single-hyphen | デリミタを単一ハイフンに設定します (xxxxxxxx-xxxxxxxx など)。 |
| network | ネットワーク ユーザのデフォルト RADIUS サーバを設定します。 |
| group | RADIUS サーバタイプを group に指定します。 |
| none | RADIUS サーバタイプを none に指定します。 |
| provincial | RADIUS サーバタイプを provincial に指定します。 |
| retransmit-timeout | サーバのデフォルト再送信タイムアウトを変更します。 |
| <i>seconds</i> | 再送信の間隔 (秒単位)。 |
| realm | RADIUS アカウンティング レルムを指定します。 |
| add | RADIUS アカウンティング レルムを追加します。 |
| delete | RADIUS アカウンティング レルムを削除します。 |

コマンド デフォルト RADIUS サーバの追加時、ポート番号は 1813 にデフォルト設定され、状態が **enabled** になります。

使用上のガイドライン IPSec は IPv6 ではサポートされません。

| コマンド履歴 | リリース | 変更内容 |
|--------|------|-----------------------------------|
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

| リリース | 変更内容 |
|------|---|
| 8.0 | このコマンドは、IPv4 と IPv6 の両方のアドレス形式をサポートします。 |

次に、ポート *1813* で *admin* のログインパスワードを使用して、*10.10.10.10* にある優先順位 1 の RADIUS アカウンティング サーバを設定する例を示します。

```
(Cisco Controller) > config radius acct add 1 10.10.10.10 1813 ascii admin
```

次に、ポート *1813* で *admin* のログインパスワードを使用して、*2001:9:6:40::623* にある優先順位 1 の RADIUS アカウンティング サーバを設定する例を示します。

```
(Cisco Controller) > config radius acct add 1 2001:9:6:40::623 1813 ascii admin
```

config radius acct ipsec authentication

Cisco ワイヤレス LAN コントローラで IPsec 認証を設定するには、**config radius acct ipsec authentication** コマンドを使用します。

config radius acct ipsec authentication { **hmac-md5** | **hmac-sha1** } *index*

| | | |
|------------|------------------|-----------------------------------|
| 構文の説明 | hmac-md5 | IPsec HMAC-MD5 認証をイネーブルにします。 |
| | hmac-sha1 | IPsec HMAC-SHA1 認証をイネーブルにします。 |
| | <i>index</i> | RADIUS サーバインデックス。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、RADIUS アカウンティング サーバインデックス 1 で IPsec hmac-md5 認証サービスを設定する例を示します。

```
(Cisco Controller) > config radius acct ipsec authentication hmac-md5 1
```

関連コマンド **show radius acct statistics**

config radius acct ipsec disable

Cisco ワイヤレス LAN コントローラのアカウンティングサーバに対する IPSec サポートを無効にするには、**config radius acct ipsec disable** コマンドを使用します。

config radius acct ipsec disable *index*

| | | |
|------------|--------------|---|
| 構文の説明 | <i>index</i> | RADIUS サーバ インデックス。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース 7.6 | 変更内容 このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、RADIUS アカウンティング サーバ インデックス 1 に対する IPSec サポートを無効にする例を示します。

```
(Cisco Controller) > config radius acct ipsec disable 1
```

関連コマンド **show radius acct statistics**

config radius acct ipsec enable

Cisco ワイヤレス LAN コントローラのアカウンティングサーバに対する IPSec サポートを有効にするには、**config radius acct ipsec enable** コマンドを使用します。

config radius acct ipsec enable *index*

| | | |
|------------|--------------|-----------------------------------|
| 構文の説明 | <i>index</i> | RADIUS サーバインデックス。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

例

次に、RADIUS アカウンティングサーバインデックス 1 に対する IPSec サポートを有効にする例を示します。

```
(Cisco Controller) > config radius acct ipsec enable 1
```

関連コマンド **show radius acct statistics**

config radius acct ipsec encryption

Cisco ワイヤレス LAN コントローラのアカウンティング サーバに IPsec 暗号化を設定するには、**config radius acct ipsec encryption** コマンドを使用します。

config radius acct ipsec encryption {**3des** | **aes** | **des**} *index*

| | | |
|------------|----------------|-----------------------------------|
| 構文の説明 | 256-aes | IPsec AES-256 暗号化を有効にします。 |
| | 3des | IPsec 3DES 暗号化をイネーブルにします。 |
| | aes | IPsec AES 暗号化を有効にします。 |
| | des | IPsec DES 暗号化をイネーブルにします。 |
| | <i>index</i> | RADIUS サーバのインデックス値 (1 ~ 17)。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、RADIUS サーバのインデックス値 3 の IPsec 3DES 暗号化を設定する例を示します。

```
(Cisco Controller) > config radius acct ipsec encryption 3des 3
```

config radius acct ipsec ike

Cisco WLC でインターネット キー交換 (IKE) を設定するには、**config radius acct ipsec ike** コマンドを使用します。

config radius acct ipsec ike dh-group {group-1 | group-2 | group-5 | group-14} | lifetime seconds | phase1 {aggressive | main} } index

| | | |
|-----------|-------------------|-----------------------------------|
| 構文の説明 | dh-group | Dixie-Hellman (DH) グループを指定します。 |
| | group-1 | DH グループ 1 (768 ビット) を設定します。 |
| | group-2 | DH グループ 2 (1024 ビット) を設定します。 |
| | group-5 | DH グループ 5 (1024 ビット) を設定します。 |
| | group-14 | DH グループ 14 (2048 ビット) を設定します。 |
| | lifetime | IKE ライフタイムを設定します。 |
| | <i>seconds</i> | IKE の有効期間 (秒単位)。 |
| | phase1 | IKE phase1 ノードを設定します。 |
| | aggressive | アグレッシブ モードをイネーブルにします。 |
| | main | メイン モードをイネーブルにします。 |
| | <i>index</i> | RADIUS サーバインデックス。 |
| コマンドデフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、RADIUS サーバインデックス 1 の IKE の有効期間を 23 秒に設定する例を示します。

```
(Cisco Controller) > config radius acct ipsec ike lifetime 23 1
```

関連コマンド **show radius acct statistics**

config radius acct mac-delimiter

RADIUS アカウンティング サーバに送信される MAC アドレスで使用されるデリミタを指定するには、**config radius acct mac-delimiter** コマンドを使用します。

config radius acct mac-delimiter { **colon** | **hyphen** | **single-hyphen** | **none** }

| 構文の説明 | オプション | 説明 |
|-------|----------------------|---|
| | colon | デリミタをコロンに設定します (xx:xx:xx:xx:xx:xx など)。 |
| | hyphen | デリミタをハイフンに設定します (xx-xx-xx-xx-xx-xx など)。 |
| | single-hyphen | デリミタを単一ハイフンに設定します (xxxxxx-xxxxxx など)。 |
| | none | デリミタを無効にします (xxxxxxxxxxxx など)。 |

コマンド デフォルト デフォルトのデリミタは、ハイフンです。

| コマンド履歴 | リリース | 変更内容 |
|--------|------|-----------------------------------|
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、ネットワーク ユーザの RADIUS アカウンティング サーバに送信される MAC アドレスで使用されるデリミタ ハイフンを設定する例を示します。

```
(Cisco Controller) > config radius acct mac-delimiter hyphen
```

関連コマンド **show radius acct statistics**

config radius acct network

ネットワーク ユーザのデフォルト RADIUS サーバを設定するには、**config radius acct network** コマンドを使用します。

config radius acct network *index* {**enable** | **disable**}

| | | |
|-----------|----------------|---|
| 構文の説明 | <i>index</i> | RADIUS サーバ インデックス。 |
| | enable | サーバをネットワーク ユーザのデフォルト RADIUS サーバとして有効にします。 |
| | disable | サーバをネットワーク ユーザのデフォルト RADIUS サーバとして無効にします。 |
| コマンドデフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、RADIUS サーバ インデックス 1 でネットワーク ユーザのデフォルト RADIUS アカウンティング サーバを設定する例を示します。

```
(Cisco Controller) > config radius acct network 1 enable
```

関連コマンド **show radius acct statistics**

config radius acct realm

RADIUS アカウンティング サーバでレルムを設定するには、**config radius acct realm** コマンドを使用します。

```
config radius acct realm {add | delete} radius_index realm_string
```

| | | |
|------------|----------------------|--------------------------------------|
| 構文の説明 | <i>radius_server</i> | RADIUS サーバインデックス。範囲は 1 ~ 17 です。 |
| | add | RADIUS アカウンティング サーバにレルムを追加します。 |
| | delete | RADIUS アカウンティング サーバからレルムを削除します。 |
| | <i>realm_string</i> | RADIUS アカウンティング レルムに関連付けられた一意の文字列です。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 8.0 | このコマンドが導入されました。 |

次に、RADIUS アカウンティング サーバにレルムを追加する例を示します。

```
(Cisco Controller) > config radius acct realm add 3 test
```

config radius acct retransmit-timeout

Cisco ワイヤレス LAN コントローラ の RADIUS アカウンティング サーバのデフォルト送信タイムアウトを変更するには、**config radius acct retransmit-timeout** コマンドを使用します。

config radius acct retransmit-timeout *index timeout*

| | | |
|------------|----------------|-----------------------------------|
| 構文の説明 | <i>index</i> | RADIUS サーバ インデックス。 |
| | <i>timeout</i> | 秒単位での再送信間隔 (2 ~ 30) 。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、再送信間隔の再送信タイムアウト値を 5 秒に設定する例を示します。

```
(Cisco Controller) > config radius acct retransmit-timeout 5
```

関連コマンド **show radius acct statistics**

config radius auth

Cisco ワイヤレス LAN コントローラ の RADIUS 認証サーバの設定を行うには、**config radius auth** コマンドを使用します。

```

config radius auth {add index IP addr portascii/hexsecret} | | delete index | disable index |
enable index | framed-mtu mtu | { ipsec {authentication {hmac-md5 index | hmac-sha1
index} | disable index | enable index | encryption {256-aes | 3des | aes | des} index
| ike {auth-mode {pre-shared-key index ascii/hex shared_secret | certificate index} | dh-group
{ 2048bit-group-14 | group-1 | group-2 | group-5} index | lifetime seconds index |
phase1 {aggressive | main} index } } | { { keywrap{add ascii/hex kek mack index} |
delete index | disable | enable} } | { mac-delimiter {colon | hyphen | none |
single-hyphen} } | { management index {enable | disable} } | { mgmt-retransmit-timeout
index Retransmit Timeout } | { network index {enable | disable} } | { realm {add | delete}
radius-index realm-string } } | { region {group | none | provincial} } |
{ retransmit-timeout index Retransmit Timeout } | { rfc3576 {enable | disable} index }

```

構文の説明

| | |
|--------------------------|---|
| enable | RADIUS 認証サーバを有効にします。 |
| disable | RADIUS 認証サーバを無効にします。 |
| delete | RADIUS 認証サーバを削除します。 |
| <i>index</i> | RADIUS サーバインデックス。コントローラは、1 で検索を開始します。サーバインデックスの範囲は 1 ~ 17 です。 |
| add | RADIUS 認証サーバを追加します。「デフォルト」の項を参照してください。 |
| <i>ip-addr</i> | RADIUS サーバの IP アドレス (IPv4 または IPv6) です。 |
| <i>port</i> | RADIUS サーバのインターフェイスプロトコルの UDP ポート番号。 |
| <i>ascii/hex</i> | RADIUS サーバの秘密キーのタイプ (ascii または hex) を指定します。 |
| <i>secret</i> | RADIUS サーバのシークレット。 |
| callStationIdType | RADIUS 認証メッセージで送信されるコール先ステーション ID 情報を設定します。 |
| framed-mtu | すべての RADIUS サーバの Framed-MTU を設定します。Framed-MTU の範囲は 64 ~ 1300 バイトです。 |

| | |
|--------------------------------|---|
| ipsec | 認証サーバの IPsec サポートを有効または無効にします。 (注) IPsec は IPv6 ではサポートされません。 |
| keywrap | RADIUS キーラップを設定します。 |
| <i>ascii/hex</i> | キーラップ キーの入力形式を指定します。 |
| <i>kek</i> | 16 バイトのキー暗号化キーを入力します。 |
| <i>mack</i> | 20 バイトのメッセージオーセンティケータコード キーを入力します。 |
| mac-delimiter | コール元ステーション ID とコール先ステーション ID の MAC デリミタを設定します。 |
| management | 管理ユーザの RADIUS サーバを設定します。 |
| mgmt-retransmit-timeout | サーバのデフォルト管理ログイン再送信タイムアウトを変更します。 |
| network | ネットワーク ユーザのデフォルト RADIUS サーバを設定します。 |
| realm | RADIUS 認証レルムを設定します。 |
| region | RADIUS リージョンプロパティを設定します。 |
| retransmit-timeout | サーバのデフォルトネットワーク ログイン再送信タイムアウトを変更します。 |
| rfc3576 | 認証サーバに対する RFC-3576 サポートを有効または無効にします。 |

コマンド デフォルト RADIUS サーバの追加時、ポート番号は 1812 にデフォルト設定され、状態が **enabled** になります。

使用上のガイドライン IPsec は IPv6 ではサポートされません。

| コマンド履歴 | リリース | 変更内容 |
|--------|------|---|
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |
| | 8.0 | このコマンドは、IPv4 と IPv6 の両方のアドレス形式をサポートします。 |

次に、ポート *1812* で *admin* のログインパスワードを使用して、*10.10.10.10* にある優先順位 *3* の RADIUS 認証サーバを設定する例を示します。

```
(Cisco Controller) > config radius auth add 3 10.10.10.10 1812 ascii admin
```

次に、ポート *1812* で *admin* のログインパスワードを使用して、*2001:9:6:40::623* にある優先順位 *3* の RADIUS 認証サーバを設定する例を示します。

```
(Cisco Controller) > config radius auth add 3 2001:9:6:40::623 1812 ascii admin
```

config radius auth callStationIdType

RADIUS 認証サーバを設定するには、**config radius auth callStationIdType** コマンドを使用します。

```
config radius auth callStationIdType { ap-ethmac-only | ap-ethmac-ssid | ap-group-name |
ap-label-address | ap-label-address-ssid | ap-location | ap-mac-ssid-ap-group |
ap-macaddr-only | ap-macaddr-ssid | ap-name | ap-name-ssid | flex-group-name | ipaddr
| macaddr | vlan-id }
```

構文の説明

| | |
|------------------------|--|
| ipaddr | IP アドレスを使用する呼出端末 ID タイプを設定します (レイヤ 3 のみ)。 |
| macaddr | システムの MAC アドレスを使用する呼出端末 ID タイプを設定します (レイヤ 2 およびレイヤ 3)。 |
| ap-macaddr-only | アクセス ポイントの MAC アドレスを使用する呼出端末 ID タイプを設定します (レイヤ 2 およびレイヤ 3)。 |
| ap-macaddr-ssid | <i>AP MAC address:SSID</i> の形式でアクセス ポイントの MAC アドレスを使用する呼出端末 ID タイプを設定します (レイヤ 2 およびレイヤ 3)。 |
| ap-ethmac-only | アクセス ポイントのイーサネット MAC アドレスを使用する着信端末 ID タイプを設定します。 |
| ap-ethmac-ssid | <i>AP Ethernet MAC address:SSID</i> の形式でアクセス ポイントのイーサネット MAC アドレスを使用する着信端末 ID タイプを設定します。 |
| ap-group-name | AP グループ名を使用する呼出端末 ID タイプを設定します。AP が AP グループの一部でない場合、「default-group」が AP グループ名として使用されます。 |
| flex-group-name | FlexConnect グループ名を使用する呼出端末 ID タイプを設定します。FlexConnect AP が FlexConnect グループの一部でない場合、システム MAC アドレスが呼出端末 ID として使用されます。 |
| ap-name | アクセス ポイントの名前を使用する呼出端末 ID タイプを設定します。 |

| | |
|------------------------------|--|
| ap-name-ssid | AP name:SSID の形式でアクセス ポイントの名前を使用する呼出端末 ID タイプを設定します。 |
| ap-location | アクセス ポイントのロケーションを使用する呼出端末 ID タイプを設定します。 |
| ap-mac-ssid-ap-group | 着信端末 ID タイプを、<AP MAC address>:<SSID>:<AP Group> 形式に設定します。 |
| vlan-id | システムの VLAN-ID を使用する呼出端末 ID タイプを設定します。 |
| ap-label-address | 呼出端末 ID タイプを、アカウントिंगメッセージの AP ラベルに印刷されている APMAC アドレスに設定します。 |
| ap-label-address-ssid | 呼出端末 ID タイプを、AP MAC address:SSID 形式に設定します。 |

コマンド デフォルト システムの MAC アドレス。

使用上のガイドライン コントローラは、すべての認証パケットおよびアカウントングパケットで RADIUS サーバに着信端末 ID 属性を送信します。着信端末 ID 属性を使用すると、属性値に基づいて、異なるグループにユーザを分類できます。コマンドは着信端末に対してのみ適用可能であり、発信端末には適用できません。

SSID のみを Calling-Station-ID として送信することはできません。SSID は、アクセス ポイント MAC アドレスまたはアクセス ポイント名のいずれかのみ組み合わせることができます。

| コマンド履歴 | リリース | 変更内容 |
|--------|------|--|
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |
| | 7.6 | アクセス ポイントのイーサネット MAC アドレスをサポートするために ap-ethmac-only キーワードと ap-ethmac-ssid キーワードが追加されました。 ap-label-address および ap-label-address-ssid キーワードが追加されました。 |
| | 8.0 | このコマンドは、IPv4 と IPv6 の両方のアドレス形式をサポートします。 |
| | 8.3 | ap-mac-ssid-ap-group キーワードが追加されました。 |

次に、IP アドレスを使用する呼出端末 ID タイプを設定する例を示します。

```
(Cisco Controller) > config radius auth callStationIdType ipAddr
```

次に、システムの MAC アドレスを使用する呼出端末 ID タイプを設定する例を示します。

```
(Cisco Controller) > config radius auth callStationIdType macAddr
```

次に、アクセス ポイントの MAC アドレスを使用する呼出端末 ID タイプを設定する例を示します。

```
(Cisco Controller) > config radius auth callStationIdType ap-macAddr
```

config radius auth framed-mtu

すべての RADIUS サーバの Framed-MTU 値を設定するには、**config radius auth framed-mtu** コマンドを使用します。

config radius auth framed-mtu *mtu*

| | | |
|------------|------------|-----------------------------------|
| 構文の説明 | <i>mtu</i> | Framed-MTU 値の範囲は 64 ～ 1300 バイトです。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドが導入されました。 |

次に、RADIUS 認証サーバの Framed-MTU 値を設定する例を示します。

```
(Cisco Controller) > config radius auth framed-mtu 500
```

config radius auth IPsec authentication

Cisco ワイヤレス LAN コントローラの認証サーバに対する IPsec サポートを設定するには、**config radius auth IPsec authentication** コマンドを使用します。

config radius auth IPsec authentication { **hmac-md5** | **hmac-sha1** } *index*

| | | |
|-------|------------------|-------------------------------|
| 構文の説明 | hmac-md5 | IPsec HMAC-MD5 認証をイネーブルにします。 |
| | hmac-shal | IPsec HMAC-SHA1 認証をイネーブルにします。 |
| | <i>index</i> | RADIUS サーバ インデックス。 |

コマンド デフォルト なし

| コマンド履歴 | リリース | 変更内容 |
|--------|------|-----------------------------------|
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、RADIUS 認証サーバ インデックス 1 に対する IPsec hmac-md5 サポートを設定する例を示します。

```
(Cisco Controller) > config radius auth IPsec authentication hmac-md5 1
```

関連コマンド **show radius acct statistics**

config radius auth ipsec disable

Cisco ワイヤレス LAN コントローラの認証サーバに対する IPSec サポートを無効するには、**config radius auth IPsec disable** コマンドを使用します。

config radius auth ipsec {enable | disable} index

| | | |
|------------|----------------|-----------------------------------|
| 構文の説明 | enable | 認証サーバの IPSec サポートを有効にします。 |
| | disable | 認証サーバの IPSec サポートを無効にします。 |
| | <i>index</i> | RADIUS サーバ インデックス。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、RADIUS 認証サーバ インデックス 1 に対する IPSec サポートを有効にする例を示します。

```
(Cisco Controller) > config radius auth ipsec enable 1
```

次に、RADIUS 認証サーバ インデックス 1 に対する IPSec サポートを無効にする例を示します。

```
(Cisco Controller) > config radius auth ipsec disable 1
```

関連コマンド **show radius acct statistics**

config radius auth ipsec encryption

Cisco ワイヤレス LAN コントローラの認証サーバに対する IPsec 暗号化サポートを設定するには、**config radius auth ipsec encryption** コマンドを使用します。

config radius auth IPsec encryption {**256-aes** | **3des** | **aes** | **des**} *index*

| | | |
|-----------|----------------|-----------------------------------|
| 構文の説明 | 256-aes | IPsec 256 AES 暗号化を有効にします。 |
| | 3des | IPsec 3DES 暗号化を有効にします。 |
| | aes | IPsec AES 暗号化を有効にします。 |
| | des | IPsec DES 暗号化を有効にします。 |
| | <i>index</i> | RADIUS サーバ インデックス。 |
| コマンドデフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |
| | 8.0 | 256-aes キーワードが追加されました。 |

次に、IPsec 3des 暗号化の RADIUS 認証サーバ インデックス 3 を設定する例を示します。

```
(Cisco Controller) > config radius auth ipsec encryption 3des 3
```

関連コマンド **show radius acct statistics**

config radius auth ipsec ike

Cisco ワイヤレス LAN コントローラのインターネットキー交換 (IKE) を設定するには、**config radius auth IPsec ike** コマンドを使用します。

```
config radius auth ipsec ike {auth-mode {pre-shared-keyindex {ascii | hex shared-secret} |
certificate index} dh-group {2048bit-group-14 | group-1 | group-2 | group-5} | lifetime
seconds | phase1 {aggressive | main}} index
```

構文の説明

| | |
|-------------------------|--|
| auth-mode | IKE 認証方式を設定します。 |
| pre-shared-key | IKE 認証方式の事前共有キーを設定します。 |
| <i>index</i> | RADIUS サーバのインデックス (1 ~ 17)。 |
| ascii | ASCII 形式の RADIUS IPsec IKE 秘密キーを設定します。 |
| hex | 16 進数形式の RADIUS IPsec IKE 秘密キーを設定します。 |
| <i>shared-secret</i> | 共有 RADIUS IPsec 秘密キーを設定します。 |
| certificate | IKE 認証の証明書を設定します。 |
| dh-group | IKE Diffie-Hellman グループを設定します。 |
| 2048bit-group-14 | DH グループ 14 (2048 ビット) を設定します。 |
| group-1 | DH グループ 1 (768 ビット) を設定します。 |
| group-2 | DH グループ 2 (1024 ビット) を設定します。 |
| group-5 | DH グループ 2 (1024 ビット) を設定します。 |
| lifetime | IKE ライフタイムを設定します。 |
| <i>seconds</i> | IKE の有効期間 (秒単位)。有効な範囲は 1800 ~ 57600 秒です。 |
| phase1 | IKE phase1 モードを設定します。 |
| aggressive | アグレッシブ モードをイネーブルにします。 |
| main | メイン モードをイネーブルにします。 |
| <i>index</i> | RADIUS サーバインデックス。 |

コマンドデフォルト デフォルトでは、事前共有キーが IPSec セッションで使用され、IKE の有効期間は 28800 秒です。

| コマンド履歴 | リリース | 変更内容 |
|--------|------|-----------------------------------|
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、RADIUS 認証インデックス 1 の IKE の有効期間を 23 秒に設定する例を示します。

```
(Cisco Controller) > config radius auth ipsec ike lifetime 23 1
```

関連コマンド **show radius acct statistics**

config radius auth keywrap

Advanced Encryption Standard (AES) キー ラップを有効化および設定して、コントローラと RADIUS サーバの共有キーのセキュリティを強化するには、**config radius auth keywrap** コマンドを使用します。

config radius auth keywrap {**enable** | **disable** | **add** {**ascii** | **hex**} *kek mack* | **delete**} *index*

構文の説明

| | |
|----------------|---|
| enable | AES キー ラップを有効にします。 |
| disable | AES キー ラップを無効にします。 |
| add | AES キー ラップの属性を設定します。 |
| ascii | キー ラップを ASCII 形式で設定します。 |
| hex | キー ラップを 16 進数表記で設定します。 |
| <i>kek</i> | 16 バイトの Key Encryption Key (KEK)。 |
| <i>mack</i> | 20 バイトの Message Authentication Code Key (MACK)。 |
| delete | AES キー ラップの属性を削除します。 |
| <i>index</i> | AES キー ラップを設定する RADIUS 認証サーバのインデックス。 |

コマンド デフォルト

なし

コマンド履歴

| リリース | 変更内容 |
|------|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、RADIUS 認証サーバの AES キー ラップを有効にする例を示します。

```
(Cisco Controller) > config radius auth keywrap enable
```

関連コマンド

show radius auth statistics

config radius auth mac-delimiter

RADIUS 認証サーバに送信される MAC アドレスで使用されるデリミタを指定するには、**config radius auth mac-delimiter** コマンドを使用します。

config radius auth mac-delimiter { **colon** | **hyphen** | **single-hyphen** | **none** }

| 構文の説明 | オプション | 説明 |
|-------|----------------------|---|
| | colon | デリミタをコロンに設定します (xx:xx:xx:xx:xx:xx など)。 |
| | hyphen | デリミタをハイフンに設定します (xx-xx-xx-xx-xx-xx など)。 |
| | single-hyphen | デリミタを単一ハイフンに設定します (xxxxxx-xxxxxx など)。 |
| | none | デリミタを無効にします (xxxxxxxxxxxx など)。 |

コマンドデフォルト デフォルトのデリミタは、ハイフンです。

| コマンド履歴 | リリース | 変更内容 |
|--------|------|-----------------------------------|
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、RADIUS 認証サーバに使用するデリミタ ハイフンを指定する例を示します。

```
(Cisco Controller) > config radius auth mac-delimiter hyphen
```

関連コマンド **show radius auth statistics**

config radius auth management

管理ユーザのデフォルト RADIUS サーバを設定するには、**config radius auth management** コマンドを使用します。

config radius auth management *index* {**enable** | **disable**}

| | | |
|------------|----------------|--------------------------------------|
| 構文の説明 | <i>index</i> | RADIUS サーバ インデックス。 |
| | enable | サーバを管理ユーザのデフォルト RADIUS サーバとして有効にします。 |
| | disable | サーバを管理ユーザのデフォルト RADIUS サーバとして無効にします。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、管理ユーザの RADIUS サーバを設定する例を示します。

```
(Cisco Controller) > config radius auth management 1 enable
```

関連コマンド

show radius acct statistics
config radius acct network
config radius auth mgmt-retransmit-timeout

config radius auth mgmt-retransmit-timeout

管理ユーザのデフォルト RADIUS サーバの再送信タイムアウトを設定するには、**config radius auth mgmt-retransmit-timeout** コマンドを使用します。

config radius auth mgmt-retransmit-timeout *index retransmit-timeout*

| | | |
|------------|---------------------------|-----------------------------------|
| 構文の説明 | <i>index</i> | RADIUS サーバ インデックス。 |
| | <i>retransmit-timeout</i> | タイムアウト値。範囲は 1 ~ 30 秒です。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、管理ユーザのデフォルト RADIUS サーバの再送信タイムアウトを設定する例を示します。

```
(Cisco Controller) > config radius auth mgmt-retransmit-timeout 1 10
```

関連コマンド **config radius auth management**

config radius auth network

ネットワーク ユーザのデフォルト RADIUS サーバを設定するには、**config radius auth network** コマンドを使用します。

config radius auth network *index* { **enable** | **disable** }

| | | |
|------------|----------------|---|
| 構文の説明 | <i>index</i> | RADIUS サーバ インデックス。 |
| | enable | サーバをネットワーク ユーザのデフォルト RADIUS サーバとして有効にします。 |
| | disable | サーバをネットワーク ユーザのデフォルト RADIUS サーバとして無効にします。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、ネットワーク ユーザのデフォルト RADIUS サーバを設定する例を示します。

```
(Cisco Controller) > config radius auth network 1 enable
```

関連コマンド

show radius acct statistics
config radius acct network

config radius auth realm

RADIUS 認証サーバでレルムを設定するには、**config radius auth realm** コマンドを使用します。

```
config radius auth realm {add | delete} radius_index realm_string
```

| | | |
|-----------|----------------------|---------------------------------|
| 構文の説明 | <i>radius_server</i> | RADIUS サーバインデックス。範囲は 1 ~ 17 です。 |
| | add | RADIUS 認証サーバにレルムを追加します。 |
| | delete | RADIUS 認証サーバからレルムを削除します。 |
| | <i>realm_string</i> | RADIUS 認証レルムに関連付けられた一意の文字列です。 |
| コマンドデフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 8.0 | このコマンドが導入されました。 |

次に、RADIUS 認証サーバにレルムを追加する例を示します。

```
(Cisco Controller) > config radius auth realm add 3 test
```

config radius auth retransmit-timeout

Cisco ワイヤレス LAN コントローラの RADIUS 認証サーバのデフォルト送信タイムアウトを変更するには、**config radius auth retransmit-timeout** コマンドを使用します。

config radius auth retransmit-timeout *index timeout*

| | | |
|------------|----------------|-----------------------------------|
| 構文の説明 | <i>index</i> | RADIUS サーバ インデックス。 |
| | <i>timeout</i> | 秒単位での再送信間隔 (2 ~ 30) 。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、RADIUS 認証サーバの再送信タイムアウトを 5 秒に設定する例を示します。

```
(Cisco Controller) > config radius auth retransmit-timeout 5
```

関連コマンド **show radius auth statistics**

config radius auth rfc3576

Cisco WLC の認証サーバに RADIUS RFC-3576 サポートを設定するには、**config radius auth rfc3576** コマンドを使用します。

config radius auth rfc3576 {enable | disable} *index*

| | | |
|------------|----------------|-----------------------------------|
| 構文の説明 | enable | 認証サーバの RFC-3576 サポートを有効にします。 |
| | disable | 認証サーバの RFC-3576 サポートを無効にします。 |
| | <i>index</i> | RADIUS サーバ インデックス。 |
| コマンド デフォルト | 無効 | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン RFC 3576 は RADIUS プロトコルに対する拡張で、ユーザセッションの動的な変更を可能にします。RFC 3576 では、ユーザの切断およびユーザセッションに適用される許可の変更がサポートされています。Disconnect メッセージはユーザセッションをただちに終了させ、CoA メッセージはデータ フィルタなどのセッション認証属性を変更します。

次に、RADIUS 認証サーバに対する RADIUS RFC-3576 サポートを有効にする例を示します。

```
(Cisco Controller) > config radius auth rfc3576 enable 2
```

関連コマンド

show radius auth statistics
show radius summary
show radius rfc3576

config radius auth retransmit-timeout

RADIUS アカウンティング サーバの再送信タイムアウト値を設定するには、**config radius auth server-timeout** コマンドを使用します。

config radius auth retransmit-timeout *index timeout*

| | | |
|------------|----------------------|-----------------------------------|
| 構文の説明 | <i>index</i> | RADIUS サーバ インデックス。 |
| | <i>timeout</i> | タイムアウト値。範囲は 2 ~ 30 秒です。 |
| コマンド デフォルト | デフォルトのタイムアウトは 2 秒です。 | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、RADIUS 認証サーバ インデックス 10 のサーバタイムアウト値を 2 秒に設定する例を示します。

```
(Cisco Controller) > config radius auth retransmit-timeout 2 10
```

関連コマンド

- show radius auth statistics**
- show radius summary**

config radius aggressive-failover disabled

連続して3つのクライアントに応答しなかった RADIUS サーバをダウン（応答なし）としてマークするようにコントローラを設定するには、**config radius aggressive-failover disabled** コマンドを使用します。

config radius aggressive-failover disabled

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

| リリース | 変更内容 |
|------|---------------------------------|
| 7.6 | このコマンドは、リリース7.6以前のリリースで導入されました。 |

次に、RADIUS サーバをダウンとしてマークするようにコントローラを設定する例を示します。

```
(Cisco Controller) > config radius aggressive-failover disabled
```

関連コマンド

show radius summary

config radius backward compatibility

Cisco ワイヤレス LAN コントローラの RADIUS 下位互換性を設定するには、**config radius backward compatibility** コマンドを使用します。

config radius backward compatibility {enable | disable}

| | | |
|------------|----------------|-----------------------------------|
| 構文の説明 | enable | RADIUS ベンダー ID の下位互換性を有効にします。 |
| | disable | RADIUS ベンダー ID の下位互換性を無効にします。 |
| コマンド デフォルト | イネーブル | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、RADIUS 下位互換性の設定を有効にする例を示します。

```
(Cisco Controller) > config radius backward compatibility disable
```

関連コマンド **show radius summary**

config radius callStationIdCase

Cisco WLC の RADIUS メッセージとして送信される callStationIdCase 情報を設定するには、**config radius callStationIdCase** コマンドを使用します。

config radius callStationIdCase {legacy | lower | upper}

| | | |
|-----------|---------------|--|
| 構文の説明 | legacy | レイヤ 2 認証用の呼出端末 ID を大文字で RADIUS に設定します。 |
| | lower | すべての呼出端末 ID を小文字で RADIUS に設定します。 |
| | upper | すべての呼出端末 ID を大文字で RADIUS に設定します。 |
| コマンドデフォルト | イネーブル | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、呼出端末 ID を小文字で送信する例を示します。

```
(Cisco Controller) > config radius callStationIdCase lower
```

関連コマンド **show radius summary**

config radius callStationIdType

Cisco ワイヤレス LAN コントローラの RADIUS アカウンティング メッセージとして送信される着信端末 ID タイプ情報を設定するには、**config radius callStationIdType** コマンドを使用します。

```
config radius callStationIdType { ap-ethmac-only | ap-ethmac-ssid | ap-group-name |
ap-label-address | ap-label-address-ssid | ap-location | ap-mac-ssid-ap-group |
ap-macaddr-only | ap-macaddr-ssid | ap-name | ap-name-ssid | flex-group-name | ipaddr
| macaddr | vlan-id }
```

構文の説明

| | |
|------------------------|--|
| ipaddr | IP アドレスを使用する呼出端末 ID タイプを設定します (レイヤ 3 のみ)。 |
| macaddr | システムの MAC アドレスを使用する呼出端末 ID タイプを設定します (レイヤ 2 およびレイヤ 3)。 |
| ap-macaddr-only | アクセス ポイントの MAC アドレスを使用する呼出端末 ID タイプを設定します (レイヤ 2 およびレイヤ 3)。 |
| ap-macaddr-ssid | <i>AP MAC address:SSID</i> の形式でアクセス ポイントの MAC アドレスを使用する呼出端末 ID タイプを設定します (レイヤ 2 およびレイヤ 3)。 |
| ap-ethmac-only | アクセス ポイントのイーサネット MAC アドレスを使用する着信端末 ID タイプを設定します。 |
| ap-ethmac-ssid | <i>AP Ethernet MAC address:SSID</i> の形式でアクセス ポイントのイーサネット MAC アドレスを使用する着信端末 ID タイプを設定します。 |
| ap-group-name | AP グループ名を使用する呼出端末 ID タイプを設定します。AP が AP グループの一部でない場合、「default-group」が AP グループ名として使用されます。 |
| flex-group-name | FlexConnect グループ名を使用する呼出端末 ID タイプを設定します。FlexConnect AP が FlexConnect グループの一部でない場合、システム MAC アドレスが呼出端末 ID として使用されます。 |

| | |
|------------------------------|---|
| ap-name | アクセス ポイントの名前を使用する呼出端末 ID タイプを設定します。 |
| ap-name-ssid | <i>AP name:SSID</i> の形式でアクセス ポイントの名前を使用する呼出端末 ID タイプを設定します。 |
| ap-location | アクセス ポイントのロケーションを使用する呼出端末 ID タイプを設定します。 |
| ap-mac-ssid-ap-group | 着信端末 ID タイプを、<AP MAC address>:<SSID>:<AP Group> 形式に設定します。 |
| vlan-id | システムの VLAN-ID を使用する呼出端末 ID タイプを設定します。 |
| ap-label-address | 呼出端末 ID タイプを、アカウントメッセージの AP ラベルに印刷されている AP MAC アドレスに設定します。 |
| ap-label-address-ssid | 呼出端末 ID タイプを、AP MAC address:SSID 形式に設定します。 |

コマンド デフォルト サーバの IP アドレス。

使用上のガイドライン コントローラは、すべての認証パケットおよびアカウントメッセージパケットで RADIUS サーバに着信端末 ID 属性を送信します。着信端末 ID 属性を使用すると、属性値に基づいて、異なるグループにユーザを分類できます。コマンドは着信端末に対してのみ適用可能であり、発信端末には適用できません。

SSID のみを Calling-Station-ID として送信することはできません。SSID は、アクセス ポイント MAC アドレスまたはアクセス ポイント名のいずれかにのみ組み合わせることができます。

コマンド履歴

| リリース | 変更内容 |
|------|--|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |
| 7.6 | アクセス ポイントのイーサネット MAC アドレスをサポートするために ap-ethmac-only キーワードと ap-ethmac-ssid キーワードが追加されました。 ap-label-address および ap-label-address-ssid キーワードが追加されました。 |
| 8.0 | このコマンドは、IPv4 と IPv6 の両方のアドレス形式をサポートします。 |

| リリース | 変更内容 |
|------|--|
| 8.3 | ap-mac-ssid-ap-group キーワードが追加されました。 |

次に、IP アドレスを使用する呼出端末 ID タイプを設定する例を示します。

```
(Cisco Controller) > config radius callStationIdType ipaddr
```

次に、システムの MAC アドレスを使用する呼出端末 ID タイプを設定する例を示します。

```
(Cisco Controller) > config radius callStationIdType macaddr
```

次に、アクセスポイントの MAC アドレスを使用する呼出端末 ID タイプを設定する例を示します。

```
(Cisco Controller) > config radius callStationIdType ap-macaddr-only
```

config radius dns

DNS サーバから RADIUS IP 情報を取得するには、**config radius dns** コマンドを使用します。

```
config radius dns {global port {ascii | hex} secret | queryurl timeout | serverip ip_address
| disable | enable}
```

構文の説明

| | |
|-------------------|--|
| global | グローバルポートと、DNS サーバから RADIUS IP 情報を取得する秘密キーを設定します。 |
| <i>port</i> | 認証用のポート番号。有効な範囲は 1 ~ 65535 です。すべての DNS サーバは同じ認証ポートを使用する必要があります。 |
| <i>ascii</i> | ASCII に設定する必要がある共有秘密キーの形式。 |
| <i>hex</i> | 16 進数に設定する必要がある共有秘密キーの形式。 |
| <i>secret</i> | RADIUS サーバのログイン秘密キー。 |
| query | RADIUS サーバの完全修飾ドメイン名 (FQDN) と、DNS タイムアウトを設定します。 |
| <i>url</i> | RADIUS サーバの FQDN。FQDN は最大 63 文字の英数字 (大文字と小文字を区別) で指定できます。 |
| <i>timeout</i> | Cisco WLC がリクエストのタイムアウトを設定して再送信するまでの最大待機日数。指定できる範囲は 1 ~ 180 です。 |
| serverip | DNS サーバの IP アドレスを設定します。 |
| <i>ip_address</i> | DNS サーバの IP アドレス。 |
| disable | RADIUS DNS 機能を無効にします。デフォルトでは、この機能はディセーブルになっています。 |
| enable | Cisco WLC が DNS サーバから RADIUS IP 情報を取得できるようにします。 DNS クエリを有効にすると、スタティック設定よりも優先されます。つまり、DNS リストはスタティック AAA リストよりも優先されます。 |

コマンドデフォルト

グローバルポートと、RADIUS IP 情報を取得する秘密キーを設定できません。

コマンド履歴

| リリース | 変更内容 |
|------|-----------------|
| 7.5 | このコマンドが導入されました。 |

使用上のガイドライン

アカウントティングポートは認証ポートから取得されます。すべてのDNSサーバは同じ秘密キーを使用する必要があります。

次に、Cisco WLC で RADIUS DNS 機能を有効にする例を示します。

```
(Cisco Controller) > config radius dns enable
```

config radius fallback-test

RADIUS サーバのフォールバック動作を設定するには、**config radius fallback-test** コマンドを入力します。

```
config radius fallback-test mode {off | passive | active} | username username } | {interval interval}
```

| 構文の説明 | mode | モードを指定します。 |
|-----------|-----------------------|---|
| | off | RADIUS サーバのフォールバックを無効にします。 |
| | passive | 関係のないプローブメッセージを送信することなく、コントローラが使用可能なバックアップサーバから（サーバインデックスがより小さい）優先サーバに切り替えられます。コントローラは、しばらくの間非アクティブなすべてのサーバを無視し、あとで RADIUS メッセージの送信が必要になったときに再試行します。 |
| | active | RADIUS プローブメッセージを送信し、非アクティブだったサーバがオンライン状態に戻っているかどうかを事前に確認した上で、コントローラが使用可能なバックアップサーバから（サーバインデックスがより小さい）優先サーバに切り替えられます。コントローラは、すべてのアクティブな RADIUS 要求に対して、非アクティブなすべてのサーバを無視します。 |
| | username | ユーザ名を指定します。 |
| | <i>username</i> | [Username]。ユーザ名には、最大 16 文字の英数字を使用できます。 |
| | interval | プローブの間隔値を指定します。 |
| | <i>interval</i> | プローブの間隔。範囲は 180 ~ 3600 です。 |
| コマンドデフォルト | デフォルトのプローブ間隔は 300 です。 | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、RADIUS アカウンティング サーバのフォールバック動作を無効にする例を示します。

```
(Cisco Controller) > config radius fallback-test mode off
```

次に、関係のないプローブメッセージを送信することなく、コントローラが使用可能なバックアップサーバから優先サーバに切り替えられるように設定する例を示します。

```
(Cisco Controller) > config radius fallback-test mode passive
```

次に、RADIUS プローブメッセージを送信して、コントローラが使用可能なバックアップサーバから優先サーバに切り替えられるように設定する例を示します。

```
(Cisco Controller) > config radius fallback-test mode active
```

関連コマンド

config advanced probe filter

config advanced probe limit

show advanced probe

show radius acct statistics

config radius ext-source-ports

RADIUS サーバで拡張送信元ポートのサポートを設定するには、**config radius ext-source-ports** コマンドを使用します。

```
config radius ext-source-ports { enable | disable }
```

| | |
|------------|---|
| 構文の説明 | enable Radius 送信元ポートサポートを有効にします。 disable Radius 送信元ポートサポートを無効にします。 |
| コマンド デフォルト | なし |
| コマンド モード | Config |
| コマンド履歴 | リリース 変更内容 8.1 このコマンドが導入されました。 |

次に、RADIUS サーバで拡張送信元ポートを有効にする例を示します。

```
config radius ext-source-ports enable
```

config radius acct retransmit-timeout

Cisco ワイヤレス LAN コントローラ の RADIUS アカウンティング サーバのデフォルト送信タイムアウトを変更するには、**config radius acct retransmit-timeout** コマンドを使用します。

config radius acct retransmit-timeout *index timeout*

| | | |
|------------|----------------|-----------------------------------|
| 構文の説明 | <i>index</i> | RADIUS サーバ インデックス。 |
| | <i>timeout</i> | 秒単位での再送信間隔 (2 ~ 30) 。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、再送信間隔の再送信タイムアウト値を 5 秒に設定する例を示します。

```
(Cisco Controller) > config radius acct retransmit-timeout 5
```

関連コマンド **show radius acct statistics**

config radius auth mgmt-retransmit-timeout

管理ユーザのデフォルト RADIUS サーバの再送信タイムアウトを設定するには、**config radius auth mgmt-retransmit-timeout** コマンドを使用します。

config radius auth mgmt-retransmit-timeout *index retransmit-timeout*

| | | |
|------------|---------------------------|-----------------------------------|
| 構文の説明 | <i>index</i> | RADIUS サーバ インデックス。 |
| | <i>retransmit-timeout</i> | タイムアウト値。範囲は 1 ~ 30 秒です。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、管理ユーザのデフォルト RADIUS サーバの再送信タイムアウトを設定する例を示します。

```
(Cisco Controller) > config radius auth mgmt-retransmit-timeout 1 10
```

関連コマンド **config radius auth management**

config radius auth retransmit-timeout

Cisco ワイヤレス LAN コントローラの RADIUS 認証サーバのデフォルト送信タイムアウトを変更するには、**config radius auth retransmit-timeout** コマンドを使用します。

config radius auth retransmit-timeout *index timeout*

| | | |
|------------|----------------|-----------------------------------|
| 構文の説明 | <i>index</i> | RADIUS サーバ インデックス。 |
| | <i>timeout</i> | 秒単位での再送信間隔 (2 ~ 30) 。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、RADIUS 認証サーバの再送信タイムアウトを 5 秒に設定する例を示します。

```
(Cisco Controller) > config radius auth retransmit-timeout 5
```

関連コマンド **show radius auth statistics**

config radius auth retransmit-timeout

RADIUS アカウンティング サーバの再送信タイムアウト値を設定するには、**config radius auth server-timeout** コマンドを使用します。

config radius auth retransmit-timeout *index timeout*

構文の説明

| | |
|----------------|-------------------------|
| <i>index</i> | RADIUS サーバ インデックス。 |
| <i>timeout</i> | タイムアウト値。範囲は 2 ~ 30 秒です。 |

コマンド デフォルト

デフォルトのタイムアウトは 2 秒です。

コマンド履歴

| リリース | 変更内容 |
|------|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、RADIUS 認証サーバ インデックス 10 のサーバタイムアウト値を 2 秒に設定する例を示します。

```
(Cisco Controller) > config radius auth retransmit-timeout 2 10
```

関連コマンド

show radius auth statistics

show radius summary

config redundancy interface address peer-service-port

ピアコントローラまたはスタンバイコントローラのサービスポートのIPアドレスとネットマスクを設定するには、**config redundancy interface address peer-service-port** コマンドを使用します。

config redundancy interface address peer-service-port *ip_address netmask*

構文の説明

ip_address ピア サービス ポートの IP アドレス。

netmask ピア サービス ポートの ネットマスク。

コマンド デフォルト

なし

コマンド履歴

リリース

変更内容

7.6

このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

アクティブコントローラからのみこのコマンドを設定できます。HA 機能の場合、サービスポート設定はコントローラごとに行います。モードを HA から非 HA に変更すると（逆も同様）、これらの設定は失われます。

次に、ピアコントローラまたはスタンバイコントローラのサービスポート IP およびネットマスクを設定する例を示します。

```
(Cisco Controller) >config redundancy interface address peer-service-port 11.22.44.55
```

config redundancy mobilitymac

HA モビリティの MAC アドレスを識別子として使用するようには、**config redundancy mobilitymac** コマンドを使用します。

config redundancy mobilitymac mac_address

構文の説明

mac_address アクティブコントローラとスタンバイコントローラのペアの識別子である MAC アドレス。

コマンドデフォルト

なし

コマンド履歴

| リリース | 変更内容 |
|------|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン

リリース 8.0.110.0 からそれ以降リリースにアップグレードすると、コマンドの設定は削除されます。アップグレード後に手動でモビリティ MAC アドレスを再設定する必要があります。

次に、HA モビリティの MAC アドレスを設定する例を示します。

```
(Cisco Controller) >config redundancy mobilitymac ff:ff:ff:ff:ff:ff
```

config redundancy mode

冗長性またはハイ アベイラビリティ (HA) を有効または無効にするには、**config redundancy mode** コマンドを使用します。

config redundancy mode {sso | }

構文の説明

sso ステートフルスイッチオーバー (SSO) またはホットスタンバイ冗長モードを有効にします。

冗長モードを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース

変更内容

7.6

このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

冗長性を設定する前に、ローカルとピアの冗長管理 IP アドレスを設定する必要があります。

次に、冗長性を有効にする例を示します。

```
(Cisco Controller) >config redundancy mode sso
```

config redundancy peer-route

ピアまたはスタンバイ コントローラのルートを設定するには、**config redundancy peer-route** コマンドを使用します。

config redundancy peer-route { **add** | **delete** } *network_ip_address netmask gateway*

構文の説明

| | |
|---------------------------|----------------------------------|
| add | ネットワーク ルートを追加します。 |
| delete | スタンバイ コントローラ固有のネットワーク ルートを削除します。 |
| <i>network_ip_address</i> | ネットワーク IP アドレス。 |
| <i>netmask</i> | ネットワークのサブネット マスク。 |
| <i>gateway</i> | ルート ネットワークのゲートウェイの IP アドレス。 |

コマンドデフォルト

なし

コマンド履歴

| リリース | 変更内容 |
|------|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン

アクティブ コントローラからのみこのコマンドを設定できます。HA 機能の場合、サービスポート設定はコントローラごとに行います。モードを HA から非 HA に変更すると（逆も同様）、これらの設定は失われます。

次に、ピアまたはスタンバイ コントローラのルートを設定する例を示します。

```
(Cisco Controller) >config redundancy peer-route add 10.1.1.0 255.255.255.0 10.1.1.1
```

config redundancy timer keep-alive-timer

キープアライブ タイムアウト値を設定するには、**config redundancy timer keep-alive-timer** コマンドを使用します。

config redundancy timer keep-alive-timer *milliseconds*

構文の説明

milliseconds ミリ秒単位のキープアライブ タイムアウト値。範囲は 100 ~ 400 ミリ秒です。

コマンド デフォルト

デフォルトのキープアライブ タイムアウト値は 100 ミリ秒です。

コマンド履歴

| リリース | 変更内容 |
|------|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、キープアライブ タイムアウト値を設定する例を示します。

```
(Cisco Controller) >config redundancy timer keep-alive-timer 200
```


config redundancy timer peer-search-timer

ピアの検索タイマーを設定するには、`config redundancy timer peer-search-timer` コマンドを使用します。

`config redundancy timer peer-search-timer seconds`

構文の説明

seconds 秒単位のピアの検索タイマーの値。範囲は60~180秒です。

コマンド デフォルト

ピアの検索タイマーのデフォルト値は120秒です。

コマンド履歴

リリース

変更内容

7.6

このコマンドは、リリース7.6以前のリリースで導入されました。

使用上のガイドライン

このコマンドは、起動ロールネゴシエーションのタイムアウト値（秒単位）を設定するために使用できます。

次に、冗長ピアの検索タイマーを設定する例を示します。

```
(Cisco Controller) >config redundancy timer peer-search-timer 100
```

config redundancy unit

Cisco WLC をプライマリまたはセカンダリ WLC として設定するには、**config redundancy unit** コマンドを使用します。

config redundancy unit {primary | secondary}

構文の説明

primary Cisco WLC をプライマリ WLC として設定します。

secondary Cisco WLC をセカンダリ WLC として設定します。

コマンド デフォルト

プライマリ WLC がデフォルトの状態です。

コマンド履歴

リリース

変更内容

7.6

このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

セカンダリ WLC として設定された Cisco WLC は、有効な AP ライセンスのない HA の Stakable Unit (SKU) になります。

次に、Cisco WLC をプライマリ WLC として設定する例を示します。

```
(Cisco Controller) >config redundancy unit primary
```

config remote-lan

リモート LAN を設定するには、**config remote-lan** コマンドを使用します。

config remote-lan {**enable** | **disable**} {*remote-lan-id* | **all**}

| | | |
|-----------|----------------------|-----------------------------------|
| 構文の説明 | enable | リモート LAN をイネーブルにします。 |
| | disable | リモート LAN をディセーブルにします。 |
| | <i>remote-lan-id</i> | リモート LAN の識別子。有効な値は、1 ~ 512 です。 |
| | all | すべての無線 LAN を設定します。 |
| コマンドデフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、ID 2 のリモート LAN をイネーブルにする例を示します。

```
(Cisco Controller) >config remote-lan enable 2
```

config remote-lan aaa-override

リモート LAN で AAA を介したユーザ ポリシー オーバーライドを設定するには、**config remote-lan aaa-override** コマンドを使用します。

config remote-lan aaa-override {**enable** | **disable**} *remote-lan-id*

| | | |
|------------|----------------------|---|
| 構文の説明 | enable | リモート LAN で AAA を介したユーザ ポリシー オーバーライドをイネーブルにします。 |
| | disable | リモート LAN で AAA を介したユーザ ポリシー オーバーライドをディセーブルにします。 |
| | <i>remote-lan-id</i> | リモート LAN の識別子。有効な値は、1 ~ 512 です。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、リモート LAN ID が 2 のリモート LAN で、AAA を介したユーザ ポリシー オーバーライドをイネーブルにする例を示します。

```
(Cisco Controller) >config remote-lan aaa-override enable 2
```

config remote-lan acl

リモート LAN のアクセス コントロール リスト (ACL) を指定するには、**config remote-lan acl** コマンドを使用します。

config remote-lan acl *remote-lan-id* *acl_name*

| | | |
|------------|----------------------|--|
| 構文の説明 | <i>remote-lan-id</i> | リモート LAN の識別子。有効な値は、1 ~ 512 です。 |
| | <i>acl_name</i> | ACL 名です。 (注) 使用可能な ACL を確認するには、 show acl summary コマンドを使用します。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、ID が 2 のリモート LAN に、ACL1 を指定する例を示します。

```
(Cisco Controller) >config remote-lan acl 2 ACL1
```

config remote-lan apgroup

リモート LAN IEEE 802.1X にアクセス ポイント (AP) グループを追加するには、**config remote-lan apgroup** コマンドを使用します。

config remote-lan apgroup add *apgroup-name* *description*

構文の説明

add 新しい AP グループを作成します。

apgroup-name 設定する AP グループの名前。

description (任意) AP グループの説明。

コマンド デフォルト

なし

コマンド モード

コントローラの設定

コマンド履歴

リリー 変更内容
ス

8.4 このコマンドが導入されました。

使用上のガイドライン

例

次に、リモート LAN IEEE 802.1X に AP グループを追加する例を示します。

```
(Cisco Controller) > config remote-lan apgroup add testap
```

config remote-lan create

新しいリモート LAN 接続を設定するには、**config remote-lan create** コマンドを使用します。

config remote-lan create *remote-lan-id name*

| | | |
|------------|----------------------|-----------------------------------|
| 構文の説明 | <i>remote-lan-id</i> | リモート LAN の識別子。有効な値は、1 ～ 512 です。 |
| | <i>name</i> | リモート LAN の名前。有効な値は最大 32 文字の英数字です。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、LAN ID を 3 として、新しいリモート LAN、MyRemoteLAN を設定する例を示します。

```
(Cisco Controller) >config remote-lan create 3 MyRemoteLAN
```

config remote-lan custom-web

リモート LAN 用の Web 認証を設定するには、**config remote-lan custom-web** コマンドを使用します。

```
config remote-lan custom-web {ext-webauth-url URL} | global {enable | disable} | login-page
page-name | loginfailure-page {page-name | none} | logout-page {page-name | none} |
webauth-type {internal | customized | external}} remote-lan-id
```

| 構文の説明 | | |
|------------------------|--|------------------------------------|
| ext-webauth-url | | 外部 Web 認証の URL を設定します。 |
| <i>URL</i> | | ログイン ページ用の Web 認証 URL。 |
| global | | リモート LAN のグローバル ステータスを設定します。 |
| enable | | リモート LAN のグローバル ステータスをイネーブルにします。 |
| disable | | リモート LAN のグローバル ステータスをディセーブルにします。 |
| login-page | | ログイン ページを設定します。 |
| <i>page-name</i> | | ログイン ページの名前。 |
| none | | ログイン ページを設定しません。 |
| logout-page | | ログアウト ページを設定します。 |
| none | | ログアウト ページを設定しません。 |
| webauth-type | | リモート LAN の Web 認証タイプを設定します。 |
| internal | | デフォルト ログイン ページを表示します。 |
| customized | | ダウンロードされたログイン ページを表示します。 |
| external | | 外部サーバにあるログイン ページを表示します。 |
| <i>name</i> | | リモート LAN の名前。有効な値は最大 32 文字の英数字です。 |
| <i>remote-lan-id</i> | | リモート LAN の識別子。有効な値の範囲は 1 ~ 512 です。 |

| | |
|-----------|----|
| コマンドデフォルト | なし |
|-----------|----|

| | | |
|--------|------|-----------------------------------|
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン **config remote-lan custom-web** コマンドを使用するときは、次のガイドラインに従ってください。

- 外部 Web 認証 URL を設定する場合は、次のようにしてください。
 - Web 認証または Web パススルー セキュリティがイネーブル状態であることを確認します。Web 認証を有効にするには、**config remote-lan security web-auth enable** コマンドを使用します。Web パススルーを有効にするには、**config remote-lan security web-passthrough enable** コマンドを使用します。
 - リモート LAN のグローバル ステータスがディセーブル状態になっていることを確認します。リモート LAN のグローバル ステータスをイネーブルにするには、**config remote-lan custom-web global disable** コマンドを使用します。
 - リモート LAN がディセーブル状態になっていることを確認します。リモート LAN を無効にするには、**config remote-lan disable** コマンドを使用します。
- リモート LAN 用の Web 認証タイプを設定する場合は、次のようにしてください。
 - カスタマイズされたログイン ページを設定する場合は、ログイン ページが設定されていることを確認します。ログイン ページを設定するには、**config remote-lan custom-web login-page** コマンドを使用します。
 - 外部ログイン ページを設定する場合は、外部 Web 認証が動作するように、事前認証 ACL を設定したことを確認します。

次に、ID 3 のリモート LAN に対して、外部 Web 認証 URL を設定する例を示します。

```
(Cisco Controller) >config remote-lan custom-web ext-webauth-url
http://www.AuthorizationURL.com/ 3
```

次に、ID 3 のリモート LAN のグローバル ステータスをイネーブルにする例を示します。

```
(Cisco Controller) >config remote-lan custom-web global enable 3
```

次に、ID 3 のリモート LAN に対して、ログイン ページを設定する例を示します。

```
(Cisco Controller) >config remote-lan custom-web login-page custompage1 3
```

次に、ID 3 のリモート LAN に対して、デフォルト ログイン ページで Web 認証タイプを設定する例を示します。

```
(Cisco Controller) >config remote-lan custom-web webauth-type internal 3
```

config remote-lan delete

リモート LAN 接続を削除するには、**config remote-lan delete** コマンドを使用します。

config remote-lan delete *remote-lan-id*

| | | |
|------------|----------------------|-----------------------------------|
| 構文の説明 | <i>remote-lan-id</i> | リモート LAN の識別子。有効な値は、1 ~ 512 です。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、ID 3 のリモート LAN を削除する例を示します。

```
(Cisco Controller) >config remote-lan delete 3
```

config remote-lan dhcp_server

リモート LAN の Dynamic Host Configuration Protocol (DHCP) サーバを設定するには、**config remote-lan dhcp_server** コマンドを使用します。

config remote-lan dhcp_server remote-lan-id ip_address

| | | |
|-------|----------------------|---------------------------------|
| 構文の説明 | <i>remote-lan-id</i> | リモート LAN の識別子。有効な値は、1 ~ 512 です。 |
| | <i>ip_addr</i> | オーバーライド DHCP サーバの IPv4 アドレス。 |

コマンド デフォルト 0.0.0.0 がインターフェイスのデフォルト値として設定されます。

| コマンド履歴 | リリース | 変更内容 |
|--------|------|-----------------------------------|
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |
| | 8.0 | このコマンドは、IPv4 アドレス形式のみをサポートします。 |

次に、ID 3 のリモート LAN に対して、DHCP サーバを設定する例を示します。

```
(Cisco Controller) >config remote-lan dhcp_server 3 209.165.200.225
```

関連コマンド **show remote-lan**

config remote-lan exclusionlist

リモート LAN の除外リスト タイムアウトを設定するには、**config remote-lan exclusionlist** コマンドを使用します。

config remote-lan exclusionlist remote-lan-id {seconds | disabled | enabled}

| | | |
|-----------|----------------------|---|
| 構文の説明 | <i>remote-lan-id</i> | リモート LAN の識別子。有効な値は、1 ～ 512 です。 |
| | <i>seconds</i> | 除外リスト タイムアウト (秒)。値 0 には、管理者のオーバーライドが必要です。 |
| | disabled | 除外リストをディセーブルにします。 |
| | enabled | 除外リストをイネーブルにします。 |
| コマンドデフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、ID 3 のリモート LAN で、除外リスト タイムアウトを 20 秒に設定する例を示します。

```
(Cisco Controller) >config remote-lan exclusionlist 3 20
```

config remote-lan host-mode

リモート LAN IEEE 802.1X のホスト モードを設定するには、**config remote-lan host-mode** コマンドを使用します。

config remote-lan host-mode { **singlehost** | **multihost** } *remote-lan-id*

| | |
|------------|--|
| 構文の説明 | <p>singlehost リモート LAN シングルホストモードを設定します。</p> <p>multihost リモート LAN マルチホストモードを設定します。</p> <p><i>remote-lan-id</i> WLAN 識別子。範囲は 1 ~ 512 です。</p> |
| コマンド デフォルト | なし |
| コマンド モード | コントローラの設定 |
| コマンド履歴 | <p>リリー 変更内容</p> <p>ス</p> <p>8.4 このコマンドが導入されました。</p> |

例

次に、リモート LAN IEEE 802.1X のホスト モードをシングルとして設定する例を示します。

```
(Cisco Controller) > config remote-lan host-mode singlehost 1
```

config remote-lan interface

リモート LAN のインターフェイスを設定するには、**config remote-lan interface** コマンドを使用します。

config remote-lan interface *remote-lan-id interface_name*

| | | |
|-----------|-----------------------|---|
| 構文の説明 | <i>remote-lan-id</i> | リモート LAN の識別子。有効な値は、1 ~ 512 です。 |
| | <i>interface_name</i> | インターフェイス名。 (注) インターフェイス名は大文字にしないでください。 |
| コマンドデフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、ID 3 のリモート LAN に対して、インターフェイス `myinterface` を設定する例を示します。

```
(Cisco Controller) >config remote-lan interface 3 myinterface
```

config remote-lan ldap

リモート LAN の LDAP サーバを設定するには、**config remote-lan ldap** コマンドを使用します。

config remote-lan ldap {**add** | **delete**} リモート *lan id* インデックス

| | | |
|-------|----------------------|------------------------------------|
| 構文の説明 | add | 設定済みの LDAP サーバ（最大 3 台）へのリンクを追加します。 |
| | delete | 設定されている LDAP サーバへのリンクを削除します。 |
| | <i>remote-lan-id</i> | リモート LAN の識別子。有効な値は、1 ~ 512 です。 |
| | <i>index</i> | LDAP サーバ インデックス。 |

コマンド デフォルト なし

コマンド履歴

| リリース | 変更内容 |
|------|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、ID 3 のリモート LAN に対して、インデックス番号 10 の LDAP サーバを追加する例を示します。

```
(Cisco Controller) >config remote-lan ldap add 3 10
```


config remote-lan mac-filtering

リモート LAN で MAC フィルタリングを設定するには、**config remote-lan mac-filtering** コマンドを使用します。

config remote-lan mac-filtering {enable | disable} *remote-lan-id*

構文の説明

| | |
|----------------------|------------------------------------|
| enable | リモート LAN で MAC フィルタリングをイネーブルにします。 |
| disable | リモート LAN で MAC フィルタリングをディセーブルにします。 |
| <i>remote-lan-id</i> | リモート LAN の識別子。有効な値は、1 ~ 512 です。 |

コマンドデフォルト

リモート LAN で MAC フィルタリングがイネーブルになります。

コマンド履歴

| リリース | 変更内容 |
|------|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、ID 3 のリモート LAN で MAC フィルタリングをディセーブルにする例を示します。

```
(Cisco Controller) >config remote-lan mac-filtering disable 3
```

config remote-lan mab

AP ポート LAN クライアントのために MAC 認証バイパス (MAB) 認証のサポートを設定するには、**config remote-lan mab** コマンドを使用します。

config remote-lan mab {enable | disable} *remote-lan-id*

| | | |
|------------|----------------------|-----------------------------|
| 構文の説明 | enable | MAB 認証のサポートを有効にします。 |
| | disable | MAB 認証のサポートを無効にします。 |
| | remote-lan-id | WLAN 識別子。有効な範囲は 1 ~ 512 です。 |
| コマンド デフォルト | なし | |
| コマンド モード | コントローラの設定 | |
| コマンド履歴 | リリー | 変更内容 |
| | 8.4 | このコマンドが導入されました。 |

例

次に、AP ポート LAN クライアントのために MAB 認証のサポートを有効にする例を示します。

```
(Cisco Controller) >config remote-lan mab enable 8
```

config remote-lan max-associated-clients

リモート LAN のクライアント接続の最大数を設定するには、**config remote-lan max-associated-clients** コマンドを使用します。

config remote-lan max-associated-clients *remote-lan-id* *max-clients*

| | | |
|-----------|----------------------|-----------------------------------|
| 構文の説明 | <i>remote-lan-id</i> | リモート LAN の識別子。有効な値は、1 ~ 512 です。 |
| | <i>max-clients</i> | リモート LAN のクライアント接続の最大数を設定します。 |
| コマンドデフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、ID 3 のリモート LAN に対して、10 のクライアント接続を設定する例を示します。

```
(Cisco Controller) >config remote-lan max-associated-clients 3 10
```

config remote-lan pre-auth

RLAN IEEE 802.1X の事前認証 VLAN を設定するには、**config remote-lan pre-auth** コマンドを使用します。

config remote-lan pre-auth { **enable** | **disable** } *remote-lan-id* **vlan** *vlan-id*

構文の説明

| | |
|----------------------|-------------------------------------|
| enable | RLAN 事前認証をイネーブルにします。 |
| disable | RLAN 事前認証を無効になります。 |
| <i>remote-lan-id</i> | WLAN 識別子。範囲は 1 ~ 512 です。 |
| vlan | RLAN IEEE 802.1X の事前認証 VLAN を設定します。 |
| <i>vlan-id</i> | リモート LAN の事前認証 VLAN の識別子。 |

コマンド デフォルト

なし

コマンド モード

(コントローラの設定)

コマンド履歴

| リリース | 変更内容 |
|------|-----------------|
| 8.4 | このコマンドが導入されました。 |

例

次に、リモート LAN IEEE 802.1 の事前認証 VLAN を有効にする例を示します。

```
(Cisco Controller) > config remote-lan pre-auth enable 1 vlan vlan1
```

config remote-lan radius_server

リモート LAN で RADIUS サーバを設定するには、**config remote-lan radius_server** コマンドを使用します。

```
config remote-lan radius_server {acct {{add | delete} server-index | {enable | disable} |
interim-update {interval | enable | disable}} | auth {{add | delete} server-index | {enable
| disable }} | overwrite-interface {enable | disable}} remote-lan-id
```

| 構文の説明 | | |
|-----------------------|--|--|
| acct | | RADIUS アカウンティング サーバを設定します。 |
| add | | 設定されている RADIUS サーバへのリンクを追加します。 |
| delete | | 設定されている RADIUS サーバへのリンクを削除します。 |
| <i>remote-lan-id</i> | | リモート LAN の識別子。有効な値は、1 ~ 512 です。 |
| <i>server-index</i> | | RADIUS サーバインデックス。 |
| enable | | このリモート LAN の RADIUS アカウンティングをイネーブルにします。 |
| disable | | このリモート LAN の RADIUS アカウンティングをディセーブルにします。 |
| interim-update | | このリモート LAN の RADIUS アカウンティングをイネーブルにします。 |
| <i>interval</i> | | 中間アカウンティングの間隔。範囲は 180 ~ 3600 秒です。 |
| enable | | 中間アカウンティングアップデートをイネーブルにします。 |
| disable | | 中間アカウンティングアップデートをディセーブルにします。 |
| auth | | RADIUS 認証サーバを設定します。 |
| enable | | このリモート LAN に対して RADIUS 認証をイネーブルにします。 |
| disable | | このリモート LAN に対して RADIUS 認証をディセーブルにします。 |

| | |
|----------------------------|--|
| overwrite-interface | リモート LAN の RADIUS 動的インターフェイスを設定します。 |
| enable | リモート LAN の RADIUS 動的インターフェイスをイネーブルにします。 |
| disable | リモート LAN の RADIUS 動的インターフェイスをディセーブルにします。 |

コマンド デフォルト 暫定アップデート間隔は 600 秒です。

コマンド履歴

| リリース | 変更内容 |
|------|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、ID 3 のリモート LAN の RADIUS アカウンティングをイネーブルにする例を示します。

```
(Cisco Controller) >config remote-lan radius_server acct enable 3
```

config remote-lan security

リモート LAN のセキュリティ ポリシーを設定するには、**config remote-lan security** コマンドを使用します。

```
config remote-lan security {{web-auth {enable | disable | acl | server-precedence}
remote-lan-id | {web-passthrough {enable | disable | acl | email-input} remote-lan-id}}
```

| 構文の説明 | web-auth | Web 認証を指定します。 |
|-----------|--------------------------|---------------------------------------|
| | enable | Web 認証の設定をイネーブルにします。 |
| | disable | Web 認証の設定をディセーブルにします。 |
| | acl | アクセスコントロールリストを設定します。 |
| | server-precedence | Web 認証ユーザに対する認証サーバの優先順位を設定します。 |
| | <i>remote-lan-id</i> | リモート LAN の識別子。有効な値は、1 ~ 512 です。 |
| | email-input | 電子メールアドレスを使用して Web キャプティブ ポータルを設定します。 |
| | web-passthrough | 認証不要の Web キャプティブ ポータルを設定します。 |
| コマンドデフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |
| | 8.4 | 802.1X キーワードが追加されました。 |

次に、リモート LANID1 のセキュリティ Web 認証ポリシーを設定する例を示します。

```
(Cisco Controller) >config remote-lan security web-auth enable 1
```

config remote-lan session-timeout

クライアントセッションのタイムアウトを設定するには、**config remote-lan session-timeout** コマンドを使用します。

config remote-lan session-timeout *remote-lan-id* *seconds*

| | | |
|------------|----------------------|---|
| 構文の説明 | <i>remote-lan-id</i> | リモート LAN の識別子。有効な値は、1 ~ 512 です。 |
| | <i>seconds</i> | タイムアウトまたはセッション時間（秒）。値 0 は、タイムアウトなしに相当します。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、ID 1 のリモート LAN で、クライアントセッションタイムアウトを 6000 秒に設定する例を示します。

```
(Cisco Controller) >config remote-lan session-timeout 1 6000
```


config remote-lan violation-mode

リモート LAN IEEE 802.1X の違反モードを設定するには、**config remote-lan violation-mode** コマンドを使用します。

config remote-lan violation-mode { **protect** | **replace** | **shutdown** } *remote-lan-id*

| | | |
|-----------|----------------------|-----------------------------|
| 構文の説明 | protect | リモート LAN の保護モードを設定します。 |
| | replace | リモート LAN の置換モードを設定します。 |
| | shutdown | リモート LAN のシャットダウンモードを設定します。 |
| | <i>remote-lan-id</i> | WLAN 識別子。範囲は 1 ~ 512 です。 |
| コマンドデフォルト | なし | |
| コマンドモード | コントローラの設定 | |
| コマンド履歴 | リリース | 変更内容 |
| | 8.4 | このコマンドが導入されました。 |

使用上のガイドライン

例

次に、リモート LAN IEEE 802.1X の違反モードを保護モードとして設定する例を示します。

```
(Cisco Controller) > config remote-lan violation-mode protect 1
```

config remote-lan webauth-exclude

リモート LAN の Web 認証の除外を設定するには、**config remote-lan webauth-exclude** コマンドを使用します。

config remote-lan webauth-exclude *remote-lan-id* {**enable** | **disable**}

| | | |
|------------|----------------------|-----------------------------------|
| 構文の説明 | <i>remote-lan-id</i> | リモート LAN の識別子。有効な値は、1 ~ 512 です。 |
| | enable | リモート LAN の Web 認証の除外をイネーブルにします。 |
| | disable | リモート LAN の Web 認証の除外をディセーブルにします。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、ID 1 のリモート LAN で、Web 認証除外をイネーブルにする例を示します。

```
(Cisco Controller) >config remote-lan webauth-exclude 1 enable
```

config rf-profile band-select

RF プロファイルの帯域選択パラメータを設定するには、**config rf-profile band-select** コマンドを使用します。

```
config rf-profile band-select { client-rssi rssi | cycle-count cycles | cycle-threshold value | expire
{ dual-band value | suppression value } | probe-response { enable | disable } } profile_name
```

| 構文の説明 | |
|------------------------|---|
| client-rssi | RF プロファイルに対して、クライアントの Received Signal Strength Indicator (RSSI) のしきい値を設定します。 |
| <i>rssi</i> | プローブに応答するクライアントの RSSI の最小値。範囲は -20 ~ -90 dBm です。 |
| cycle-count | RF プロファイルのプローブサイクルカウントを設定します。サイクル回数は、新しいクライアントの抑制サイクルの回数を設定します。 |
| <i>cycles</i> | サイクルカウントの値。値の範囲は 1 ~ 10 です。 |
| cycle-threshold | 新しいスキャン RF プロファイルの帯域選択サイクル時間のしきい値を設定します。この設定は、クライアントからの新しいプローブ要求が新しいスキャンサイクルで送信される間の時間しきい値を決定します。 |
| <i>value</i> | RF プロファイルのサイクルのしきい値。範囲は 1 ~ 1000 ミリ秒です。 |
| expire | 帯域選択に対するクライアントの有効期限を設定します。 |
| dual-band | 既知のデュアルバンドクライアントを除去する有効期限を設定します。この時間が経過すると、クライアントは新規とみなされて、プローブ応答抑制の対象となります。 |
| <i>value</i> | デュアルバンドの値。範囲は 10 ~ 300 秒です。 |
| suppression | 既知の 802.11b/g クライアントを除去する有効期限を設定します。この時間が経過すると、クライアントは新規とみなされて、プローブ応答抑制の対象となります。 |
| <i>value</i> | 抑制の値。範囲は 10 ~ 200 秒です。 |
| probe-response | RF プロファイルのプローブ応答を設定します。 |
| enable | RF プロファイルに対して、2.4 GHz 帯域で動作しているクライアントのプローブ応答抑制をイネーブルにします。 |
| disable | RF プロファイルに対して、2.4 GHz 帯域で動作しているクライアントのプローブ応答抑制をディセーブルにします。 |

profile name RF プロファイルの名前。プロファイル名は最大 32 文字の英数字で、大文字と小文字を区別します。

コマンド デフォルト クライアント RSSI のデフォルト値は -80 dBm です。
 デフォルトのサイクル回数は 2 です。
 デフォルトのサイクル閾値は 200 ミリ秒です。
 デュアルバンドの有効期限のデフォルト値は 60 秒です。
 抑制の有効期限のデフォルト値は 20 秒です。

| コマンド履歴 | リリース | 変更内容 |
|--------|------|-----------------------------------|
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン WLAN で帯域選択を有効にすると、アクセスポイントによって 2.4 GHz でのクライアントプロローブが抑制され、デュアルバンドクライアントが 5 GHz スペクトルに移動されます。帯域選択アルゴリズムによるデュアルバンドクライアントの誘導は、同じアクセスポイントの 2.4 GHz 無線から 5 GHz 無線へに限られます。このアルゴリズムが機能するのは、アクセスポイントで 2.4 GHz と 5 GHz の両方の無線が稼働している場合のみです。帯域選択は、Cisco Aironet 1040、1140、1250、および 3500 シリーズのアクセスポイントでのみ使用できます。

次に、クライアント RSSI を設定する例を示します。

```
(Cisco Controller) >config rf-profile band-select client-rssi -70
```

config rf-profile channel

RF プロファイルの DCA を設定するには、**config rf-profile channel** コマンドを使用します。

```
config rf-profile channel {add chan profile name | delete chan profile name | foreign {enable | disable} profile name | chan-width {20 | 40 | 80} profile name}
```

構文の説明

| | |
|---------------------------------------|---|
| add | RF プロファイルの DCA チャンネル リストにチャンネルを追加します。 |
| delete | RF プロファイルの DCA チャンネル リストからチャンネルを削除します。 |
| foreign | RF プロファイルの DCA 外部 AP の寄与を設定します。 |
| chan-width | RF プロファイルの DCA チャンネル幅を設定します。 |
| <i>chan</i> | チャンネル番号を指定します。 |
| <i>profile name</i> | RF プロファイルの名前を指定します。プロファイル名は最大 32 文字の英数字で、大文字と小文字を区別します。 |
| enable | 外部 AP 干渉を有効にします。 |
| disable | 外部 AP 干渉を無効にします。 |
| { 20 40 80 } | RF プロファイルの DCA チャンネル幅を指定します。 |

コマンド デフォルト

なし

コマンド履歴

| リリース | 変更内容 |
|------|-----------------|
| 8.0 | このコマンドが導入されました。 |

次に、RF プロファイルの DCA チャンネル リストにチャンネルを追加する例を示します。

```
(Cisco Controller) >config rf-profile channel add 40 admin1
```

次に、RF プロファイルの DCA チャンネル幅を設定する例を示します。

```
(Cisco Controller) >config rf-profile channel chan-width 40 admin1
```

config rf-profile client-trap-threshold

アクセスポイントに関連付けられるクライアント数のしきい値を設定するには（このしきい値を超えると、SNMP トラップがコントローラに送信される）、**config rf-profile client-trap-threshold** コマンドを使用します。

config rf-profile client-trap-threshold *threshold profile_name*

| 構文の説明 | <p><i>threshold</i> アクセスポイントに関連付けられるクライアント数のしきい値。このしきい値を超えると、SNMP トラップがコントローラに送信されます。範囲は 0 ~ 200 です。トラップは、しきい値がゼロに設定されている場合はディセーブルです。</p> | | | | |
|------------|---|------|------|-----|-----------------------------------|
| | <p><i>profile_name</i> RF プロファイルの名前。プロファイル名は最大 32 文字の英数字で、大文字と小文字を区別します。</p> | | | | |
| コマンド デフォルト | なし | | | | |
| コマンド履歴 | <table border="1"> <thead> <tr> <th data-bbox="373 871 535 924">リリース</th> <th data-bbox="535 871 1497 924">変更内容</th> </tr> </thead> <tbody> <tr> <td data-bbox="373 924 535 978">7.6</td> <td data-bbox="535 924 1497 978">このコマンドは、リリース 7.6 以前のリリースで導入されました。</td> </tr> </tbody> </table> | リリース | 変更内容 | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |
| リリース | 変更内容 | | | | |
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 | | | | |

次に、アクセスポイントに関連付けられているクライアント数のしきい値を設定する例を示します。

```
(Cisco Controller) >config rf-profile client-trap-threshold 150
```

config rf-profile create

RF プロファイルを作成するには、**config rf-profile create** コマンドを使用します。

```
config rf-profile create {802.11a | 802.11b/g} profile-name
```

| | | |
|-----------|---------------------|-----------------------------------|
| 構文の説明 | 802.11a | 2.4GHz帯域のRFプロファイルを設定します。 |
| | 802.11b/g | 5GHz帯域のRFプロファイルを設定します。 |
| | <i>profile-name</i> | RFプロファイルの名前。 |
| コマンドデフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、新しいRFプロファイルを作成する例を示します。

```
(Cisco Controller) >config rf-profile create 802.11a RFtestgroup1
```

config rf-profile fra client-aware

RF プロファイルのクライアント認識 FRA 機能を設定するには、**config rf-profile fra client-aware** コマンドを使用します。

```
config rf-profile fra client-aware { client-reset percent rf-profile-name | client-select percent rf-profile-name | disable rf-profile-name | enable rf-profile-name }
```

| 構文の説明 | client-reset 無線をモニタ モードに戻すための RF プロファイルの AP 使用率のしきい値を設定します。 | | | | |
|------------|---|------|------|-----|-----------------|
| | <i>percent</i> 0 ~ 100 までの使用率の値。デフォルト値は 5% です。 | | | | |
| | <i>rf-profile-name</i> RF プロファイルの名前。 | | | | |
| | client-select 無線を 5GHz に切り替えるための RF プロファイル使用率のしきい値を設定します。 | | | | |
| | <i>percent</i> 0 ~ 100 までの使用率の値。デフォルト値は 50% です。 | | | | |
| | disable RF プロファイルのクライアント認識 FRA 機能を無効にします。 | | | | |
| | enable RF プロファイルのクライアント認識 FRA 機能を有効にします。 | | | | |
| コマンド デフォルト | client-select および client-reset のデフォルトのパーセント値は、それぞれ 50% および 5% です。 | | | | |
| コマンド履歴 | <table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>8.5</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table> | リリース | 変更内容 | 8.5 | このコマンドが導入されました。 |
| リリース | 変更内容 | | | | |
| 8.5 | このコマンドが導入されました。 | | | | |

次に、冗長デュアルバンド無線を 5 GHz クライアントサーバの役割からモニタ モードに戻すための RF プロファイル使用率のしきい値を設定する例を示します。

```
(Cisco Controller) >config rf-profile fra client-aware client-reset 15 profile1
```

次に、冗長デュアルバンド無線をモニタ モードから 5 GHz クライアントサーバの役割に切り替えるための RF プロファイル使用率のしきい値を設定する例を示します。

```
(Cisco Controller) >config rf-profile fra client-aware client-select 20 profile1
```

次に、RF プロファイルのクライアント認識 FRA 機能を無効にする例を示します。

```
(Cisco Controller) >config rf-profile fra client-aware disable profile1
```

次に、RF プロファイルのクライアント認識 FRA 機能を有効にする例を示します。

```
(Cisco Controller) >config rf-profile fra client-aware enable profile1
```


config rf-profile data-rates

RF プロファイルのデータ レートを設定するには、**config rf-profile data-rates** コマンドを使用します。

```
config rf-profile data-rates {802.11a | 802.11b} {disabled | mandatory | supported} data-rate
profile-name
```

| 構文の説明 | | |
|-------|---------------------|---|
| | 802.11a | RF プロファイルの無線ポリシーとして 802.11a を指定します。 |
| | 802.11b | RF プロファイルの無線ポリシーとして 802.11b を指定します。 |
| | disabled | レートをディセーブルにします。 |
| | mandatory | レートを必須に設定します。 |
| | supported | レートをサポートに設定します。 |
| | <i>data-rate</i> | 802.11 動作レート (1*、2*、5.5*、6、9、11*、12、18、24、36、48、および 54)。* は、802.11b のみのレートであることを示します。 |
| | <i>profile-name</i> | RF プロファイルの名前。 |

コマンド デフォルト RF プロファイルのデフォルトのデータ レートは、コントローラ システムのデフォルトであるグローバルデータ レート設定から取得されます。たとえば、RF プロファイルの無線ポリシーが 802.11a にマッピングされると、グローバル 802.11a データ レートは、作成時に RF プロファイルにコピーされます。

このコマンドで設定したデータ レートは、クライアントと Cisco ワイヤレス LAN コントローラとの間でネゴシエートされます。データ レートが **mandatory** に設定されている場合、クライアントはネットワークを使用するためにこのデータ レートをサポートする必要があります。Cisco ワイヤレス LAN コントローラでデータ レートが **supported** に設定されている場合、アソシエートされているその他のクライアントのうち、このレートをサポートするクライアントも、このレートを使用して Cisco Lightweight アクセスポイントと通信できます。アソシエートするために、クライアントが **supported** とマークされているすべてのレートを使用できる必要はありません。

| コマンド履歴 | リリース | 変更内容 |
|--------|------|-----------------------------------|
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、12 Mbps の必須レートで RF プロファイルの 802.11b 伝送を設定する例を示します。

```
(Cisco Controller) >config rf-profile 802.11b data-rates mandatory 12 RFGroupl
```

config rf-profile delete

RF プロファイルを削除するには、**config rf-profile delete** コマンドを使用します。

config rf-profile delete *profile-name*

| | | |
|------------|---------------------|-----------------------------------|
| 構文の説明 | <i>profile-name</i> | RF プロファイルの名前。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、RF プロファイルを削除する例を示します。

```
(Cisco Controller) >config rf-profile delete RFGroup1
```

config rf-profile description

RF プロファイルの説明を入力するには、**config rf-profile description** コマンドを使用します。

config rf-profile description *description profile-name*

| | | |
|------------|---------------------|-----------------------------------|
| 構文の説明 | <i>description</i> | RF プロファイルの説明。 |
| | <i>profile-name</i> | RF プロファイルの名前。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、RF プロファイルに説明を追加する例を示します。

```
(Cisco Controller) >config rf-profile description This is a demo description RFGroup1
```

config rf-profile fra client-aware

RF プロファイルのクライアント認識 FRA 機能を設定するには、**config rf-profile fra client-aware** コマンドを使用します。

```
config rf-profile fra client-aware { client-reset percent rf-profile-name | client-select percent rf-profile-name | disable rf-profile-name | enable rf-profile-name }
```

| | |
|------------|--|
| 構文の説明 | client-reset 無線をモニタ モードに戻すための RF プロファイルの AP 使用率のしきい値を設定します。 |
| | <i>percent</i> 0 ~ 100 までの使用率の値。デフォルト値は 5% です。 |
| | <i>rf-profile-name</i> RF プロファイルの名前。 |
| | client-select 無線を 5GHz に切り替えるための RF プロファイル使用率のしきい値を設定します。 |
| | <i>percent</i> 0 ~ 100 までの使用率の値。デフォルト値は 50% です。 |
| | disable RF プロファイルのクライアント認識 FRA 機能を無効にします。 |
| | enable RF プロファイルのクライアント認識 FRA 機能を有効にします。 |
| コマンド デフォルト | client-select および client-reset のデフォルトのパーセント値は、それぞれ 50% および 5% です。 |
| コマンド履歴 | リリース 変更内容 |
| | 8.5 このコマンドが導入されました。 |

次に、冗長デュアルバンド無線を 5GHz クライアントサーバの役割からモニタ モードに戻すための RF プロファイル使用率のしきい値を設定する例を示します。

```
(Cisco Controller) >config rf-profile fra client-aware client-reset 15 profile1
```

次に、冗長デュアルバンド無線をモニタ モードから 5GHz クライアントサーバの役割に切り替えるための RF プロファイル使用率のしきい値を設定する例を示します。

```
(Cisco Controller) >config rf-profile fra client-aware client-select 20 profile1
```

次に、RF プロファイルのクライアント認識 FRA 機能を無効にする例を示します。

```
(Cisco Controller) >config rf-profile fra client-aware disable profile1
```

次に、RF プロファイルのクライアント認識 FRA 機能を有効にする例を示します。

```
(Cisco Controller) >config rf-profile fra client-aware enable profile1
```

config rf-profile load-balancing

RF プロファイルのロード バランシングを設定するには、**config rf-profile load-balancing** コマンドを使用します。

config rf-profile load-balancing { **window** *clients* | **denial** *value* } *profile_name*

構文の説明

| | |
|---------------------|---|
| window | RF プロファイルのロード バランシング用のクライアント・ウィンドウを設定します。 |
| <i>clients</i> | <p>アクセス ポイントとのクライアント アソシエーションを制限するクライアント ウィンドウ サイズ。指定できる範囲は 0 ~ 20 です。デフォルト値は 5 です。</p> <p>このウィンドウ サイズは、アクセス ポイントの負荷が高すぎてそれ以上はクライアント アソシエーションを受け付けることができないかどうかを判断するアルゴリズムで使用されます。</p> <p>ロード バランシング ウィンドウ + 最も負荷が低いアクセス ポイント上のクライアント アソシエーション数 = ロード バランシングしきい値</p> <p>クライアント アソシエーションの数がこの閾値を超えるアクセス ポイントはビジー状態であるとみなされ、クライアントがアソシエートできるのは、クライアント数が閾値を下回るアクセスポイントだけとなります。このウィンドウでは、スティッキ クライアントをアソシエート解除することもできます。</p> |
| denial | RF プロファイルのロード バランシング用にクライアントの拒否数を設定します。 |
| <i>value</i> | <p>ロード バランシング中のアソシエーション拒否の最大数。値の範囲は 1 ~ 10 です。デフォルト値は 3 です。</p> <p>クライアントをワイヤレス ネットワークに関連付けようとする場合、クライアントは、アクセス ポイントにアソシエーション要求を送信します。アクセス ポイントが過負荷になり、ロード バランシングがコントローラ上でイネーブルな場合、アクセス ポイントはアソシエーション要求に対して拒否を送信します。他のアクセス ポイントがクライアントの範囲に含まれていない場合、クライアントは同じアクセス ポイントへの関連付けを再試行します。拒否の最大数に到達した後、クライアントが関連付けられます。AP に関連付けられる前のクライアントからアクセス ポイントへのアソシエーション試行は、アソシエーションのシーケンスと呼ばれます。デフォルトは 3 です。</p> |
| <i>profile_name</i> | RF プロファイルの名前。プロファイル名は最大 32 文字の英数字で、大文字と小文字を区別します。 |

コマンド デフォルト なし

コマンド履歴

| リリース | 変更内容 |
|------|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、RF プロファイルのクライアント ウィンドウ サイズを設定する例を示します。

```
(Cisco Controller) >config rf-profile load-balancing window 15
```

config rf-profile max-clients

RF プロファイルのアクセスポイントごとのクライアント接続の最大数を設定するには、**config rf-profile max-clients** コマンドを使用します。

config rf-profile max-clients *clients*

構文の説明

clients RF プロファイルのアクセスポイントあたりのクライアント接続の最大数。指定できる範囲は 1 ~ 200 です。

コマンド デフォルト

なし

コマンド履歴

| リリース | 変更内容 |
|------|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン

クライアントの高密度領域にあるアクセスポイント、または高帯域幅のビデオまたはミッションクリティカルな音声アプリケーションを提供しているアクセスポイント上でクライアントの最大数を設定するには、このコマンドを使用します。

次に、クライアントの最大数を 50 に設定する例を示します。

```
(Cisco Controller) >config rf-profile max-clients 50
```


config rf-profile multicast data-rate

RF プロファイルの最小マルチキャストデータ レートを設定するには、**config rf-profile multicast data-rate** コマンドを使用します。

config rf-profile multicast data-rate *value profile_name*

構文の説明

| | |
|---------------------|---|
| <i>value</i> | RF プロファイルの最小マルチキャストデータ レート。オプションは 6、9、12、18、24、36、48、54 です。アクセス ポイントで動的なデータ レートを調整する場合は 0 を入力します。 |
| <i>profile_name</i> | RF プロファイルの名前。プロファイル名は最大 32 文字の英数字で、大文字と小文字を区別します。 |

コマンドデフォルト

RF プロファイルの最小マルチキャストデータ レートは 0 です。

コマンド履歴

| リリース | 変更内容 |
|------|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、RF プロファイルのマルチキャストデータ レートを設定する例を示します。

```
(Cisco Controller) >config rf-profile multicast data-rate 24
```

config rf-profile out-of-box

新しく設置したアクセスポイントから構成されるアウトオブボックス AP グループを作成するには、**config rf-profile out-of-box** コマンドを使用します。

config rf-profile out-of-box {enable | disable}

構文の説明

enable アウトオブボックス AP グループの作成をイネーブルにします。このコマンドをイネーブルにすると、次の動作が発生します。

- デフォルト AP グループに含まれ、新しくインストールしたアクセスポイントは、アウトオブボックス AP グループの一部となります。その無線はオフに切り替えられ、新しいアクセスポイントによって生じる RF の不安定が解消されます。
- グループ名を持たないすべてのアクセスポイントは、アウトオブボックス AP グループの一部になります。
- 特別な RF プロファイルは 802.11 帯域ごとに作成されます。これらの RF プロファイルには、既存のすべての RF パラメータのデフォルト設定、および追加の新しい設定があります。

disable アウトオブボックス AP グループをディセーブルにします。この機能をディセーブルにすると、アウトオブボックス AP グループへの新しい AP サブスクリプションだけが停止します。アウトオブザボックス AP グループへサブスクライブされたすべての AP が、この AP グループに残ります。ネットワーク コンバージェンス時に、デフォルト グループまたはカスタム AP グループに AP を移動できます。

コマンド デフォルト なし

コマンド履歴

| リリース | 変更内容 |
|------|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン

アウトオブザボックス AP がコントローラに最初に関連付けられるとき、その AP は特別な AP グループにリダイレクトされ、この AP グループに適用可能な RF プロファイルは、AP の無線管理状態の設定を制御します。ネットワーク コンバージェンス時に、デフォルト グループまたはカスタム グループに AP を移動できます。

次に、アウトオブボックス AP グループの作成をイネーブルにする例を示します。

```
(Cisco Controller) >config rf-profile out-of-box enable
```

config rf-profile rx-sop threshold

802.11 帯域ごとに高、中、低の Rx SOP しきい値を設定するには、**config rf-profile rx-sop threshold** コマンドを入力します。

config rf-profile rx-sop threshold { **high** | **medium** | **low** | **auto** } *profile_name*

| 構文の説明 | |
|---------------------|---|
| high | RF プロファイルの高 Rx SOP しきい値を設定します。 |
| medium | RF プロファイルの中 Rx SOP しきい値を設定します。 |
| low | RF プロファイルの低 Rx SOP しきい値を設定します。 |
| auto | RF プロファイルの自動 Rx SOP しきい値を設定します。 auto を選択すると、アクセス ポイントが最適な Rx SOP しきい値を決定します。 |
| <i>profile_name</i> | Rx SOP しきい値を設定する RF プロファイル。 |

コマンドデフォルト デフォルトの Rx SOP しきい値オプションは **auto** です。

| コマンド履歴 | リリース | 変更内容 |
|--------|------|-----------------|
| | 8.0 | このコマンドが導入されました。 |

次に、RF プロファイルの高 Rx SOP しきい値を設定する例を示します。

```
(Cisco Controller) > config 802.11 rx-sop threshold high T1a
```

config rf-profile trap-threshold

RF プロファイルのトラップしきい値を設定するには、**config rf-profile trap-threshold** コマンドを使用します。

```
config rf-profile trap-threshold { clients clients profile name | interference percent profile name | noise dBm profile name | utilization percent profile name }
```

| | | |
|-----------|---------------------|---|
| 構文の説明 | clients | RF プロファイルのクライアントのトラップしきい値を設定します。 |
| | <i>clients</i> | トラップ用のアクセスポイントの無線のクライアント数は1～200です。デフォルトは12クライアントです。 |
| | <i>profile name</i> | RF プロファイルの名前を指定します。プロファイル名は最大32文字の英数字で、大文字と小文字を区別します。 |
| | interference | RF プロファイルの干渉のトラップしきい値を設定します。 |
| | <i>percent</i> | トラップ用の干渉しきい値の割合は0～100%です。デフォルトは10%です。 |
| | noise | RF プロファイルのノイズのトラップしきい値を設定します。 |
| | <i>dBm</i> | トラップ用のノイズしきい値のレベルは-127～0 dBmです。デフォルトは-17 dBmです。 |
| | utilization | RF プロファイルの使用率のトラップしきい値を設定します。 |
| | <i>percent</i> | アクセスポイントしきい値で使用されるトラップ用の帯域幅の割合は0～100%です。デフォルトは80%です。 |
| コマンドデフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 8.0 | このコマンドが導入されました。 |

次に、RF プロファイルのクライアントのトラップしきい値を設定する例を示します。

```
(Cisco Controller) >config rf-profile trap-threshold clients 50 admin1
```

config rf-profile tx-power-control-thresh-v1

RF プロファイルに Transmit Power Control バージョン 1 (TPCv1) を設定するには、**config rf-profile tx-power-control-thresh-v1** コマンドを使用します。

config rf-profile tx-power-control-thresh-v1 *tpc-threshold profile_name*

| | | |
|-----------|----------------------|-----------------------------------|
| 構文の説明 | <i>tpc-threshold</i> | TPC しきい値。 |
| | <i>profile-name</i> | RF プロファイルの名前。 |
| コマンドデフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、RF プロファイルの TPCv1 を設定する例を示します。

```
(Cisco Controller) >config rf-profile tx-power-control-thresh-v1 RFGroup1
```

config rf-profile tx-power-control-thresh-v2

RF プロファイルに Transmit Power Control バージョン 2 (TPCv2) を設定するには、**config rf-profile tx-power-control-thresh-v2** コマンドを使用します。

config rf-profile tx-power-control-thresh-v2 *tpc-threshold profile-name*

| | | |
|------------|----------------------|-----------------------------------|
| 構文の説明 | <i>tpc-threshold</i> | TPC しきい値。 |
| | <i>profile-name</i> | RF プロファイルの名前。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、RF プロファイルの TPCv2 を設定する例を示します。

```
(Cisco Controller) >config rf-profile tx-power-control-thresh-v2 RFGroup1
```

config rf-profile tx-power-max

RF プロファイルに最大自動 RF を設定するには、**config rf-profile tx-power-max** コマンドを使用します。

config rf-profile tx-power-max profile-name

| | | |
|-----------|---------------------|-----------------------------------|
| 構文の説明 | <i>tx-power-max</i> | 最大自動 RF TX 電力。 |
| | <i>profile-name</i> | RF プロファイルの名前。 |
| コマンドデフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、RF プロファイルの **tx-power-max** を設定する例を示します。

```
(Cisco Controller) >config rf-profile tx-power-max RFGroup1
```

config rf-profile tx-power-min

RF プロファイルに最小自動 RF を設定するには、**config rf-profile tx-power-min** コマンドを使用します。

config rf-profile tx-power-min *tx-power-min profile-name*

| | | |
|-----------|---------------------|-----------------------------------|
| 構文の説明 | <i>tx-power-min</i> | 最小自動 RF TX 電力。 |
| | <i>profile-name</i> | RF プロファイルの名前。 |
| コマンドデフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、RF プロファイルの **tx-power-min** を設定する例を示します。

```
(Cisco Controller) >config rf-profile tx-power-min RFGroup1
```


config rogue ap timeout

不正なアクセスポイントおよびクライアントのエントリが期限切れとなり、リストから削除されるまでの秒数を指定するには、**config rogue ap timeout** コマンドを使用します。

config rogue ap timeout *seconds*

| | | |
|-----------|---|---|
| 構文の説明 | <i>seconds</i> | 240 ～ 3600 秒までの値。デフォルト値は 1200 秒です。 |
| コマンドデフォルト | 不正なアクセスポイントおよびクライアントのエントリが期限切れとなるまでのデフォルトの秒数は、1200 秒です。 | |
| コマンド履歴 | リリース 7.6 | 変更内容 このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、不正アクセスポイントとクライアントリストのエントリの有効期限を 2400 秒に設定する例を示します。

```
(Cisco Controller) > config rogue ap timeout 2400
```

関連コマンド

config rogue ap classify
config rogue ap friendly
config rogue ap rldp
config rogue ap ssid
config rogue rule
config trapflags rogueap
show rogue ap clients
show rogue ap detailed
show rogue ap summary
show rogue ap friendly summary
show rogue ap malicious summary
show rogue ap unclassified summary
show rogue ignore-list
show rogue rule detailed
show rogue rule summary

config rogue adhoc

独立型基本サービスセット（IBSS またはアドホック）の不正なアクセスポイントのステータスをグローバルまたは個別に設定するには、**config rogue adhoc** コマンドを使用します。

```
config rogue adhoc {enable | disable | external rogue_MAC | alert {rogue_MAC | all} |
auto-contain [monitor_ap] | contain rogue_MAC 1234_aps | }
```

```
config rogue adhoc {delete {all | mac-address mac-address} | classify {friendly state {external
| internal} mac-address | malicious state {alert | contain} mac-address | unclassified state
{alert | contain} mac-address}}
```

| 構文の説明 | | |
|---------------------|--|---|
| enable | | アドホックの不正の検出とレポートをグローバルに有効にします。 |
| disable | | アドホックの不正の検出とレポートをグローバルに無効にします。 |
| external | | ネットワークの外側にあり、WLAN のセキュリティに脅威を与えない不正アクセスポイントの外部状態を設定します。コントローラはこの不正なアクセスポイントの存在を認識しています。 |
| <i>rogue_MAC</i> | | アドホックの不正なアクセスポイントの MAC アドレス。 |
| alert | | アドホックの不正を検出すると SMNP トラップを生成し、システム管理者に即座にアラートを発信し必要な措置を促します。 |
| all | | すべてのアドホックの不正なアクセスポイントに関するアラートを有効にします。 |
| auto-contain | | コントローラによって検出されたすべての有線アドホックの不正が含まれます。 |
| <i>monitor_ap</i> | | (任意) アドホックの不正なアクセスポイントの IP アドレス。 |
| contain | | 加害デバイスを阻止し、その信号が正規クライアントを阻止しないようにします。 |
| <i>1234_aps</i> | | アドホックの不正なアクセスポイントをアクティブに阻止するために割り当てられた、シスコのアクセスポイントの最大数 (1~4)。 |

| | |
|---------------------------|---|
| delete | アドホックの不正なアクセス ポイントを削除します。 |
| all | すべてのアドホックの不正なアクセス ポイントを削除します。 |
| mac-address | 指定したMACアドレスがあるアドホックの不正なアクセス ポイントを削除します。 |
| <i>mac-address</i> | アドホックの不正なアクセス ポイントのMAC アドレス。 |
| classify | アドホックの不正なアクセス ポイントの分類を設定します。 |
| friendly state | アドホックの不正なアクセス ポイントを危険性のないアクセスポイントとして分類します。 |
| internal | ネットワークの内側にあり、WLAN のセキュリティに脅威を与えない不正アクセス ポイントのアラート状態を設定します。コントローラはこの不正なアクセス ポイントを信頼します。 |
| malicious state | アドホックの不正なアクセス ポイントを悪意のあるアクセス ポイントとして分類します。 |
| alert | ネイバー リストにない、またはユーザが設定した危険性のないMACのリストに記載されていない不正アクセス ポイントのアラート状態を設定します。コントローラからシステム管理者に、さらなる処理を行うよう即時に警告が転送されます。 |
| contain | 不正アクセス ポイントを contain の状態に設定します。コントローラによって危険性のあるデバイスが阻止され、そのデバイスの信号が、認証されたクライアントに干渉しないようになります。 |
| unclassified state | アドホックの不正なアクセス ポイントを未分類のアクセス ポイントとして分類します。 |

コマンド デフォルト

このコマンドのデフォルトは**enabled**であり、**alert**に設定されます。自動阻止のデフォルトは、**disabled**です。

| コマンド履歴 | リリース | 変更内容 |
|--------|------|---------------------------------|
| | 7.6 | このコマンドは、リリース7.6以前のリリースで導入されました。 |

使用上のガイドライン

コントローラは、すべての近隣のアクセスポイントを継続的に監視し、不正なアクセスポイントおよびクライアントに関する情報を自動的に検出して収集します。コントローラが不正なアクセスポイントを検出すると、不正ロケーション検出プロトコル (RLDP) を使用して不正なアクセスポイントが有線ネットワークに接続されているかどうかを確認します。



- (注) RLDPは、シスコの Atonomous 不正アクセスポイントではサポートされていません。これらのアクセスポイントは、RLDPクライアントによって送信されたDHCP検出要求をドロップします。また不正なアクセスポイントチャンネルが動的周波数選択 (DFS) を必要とする場合、RLDPはサポートされません。

`containment` コマンドのいずれかを入力すると、次の警告が表示されます。

```
Using this feature may have legal consequences. Do you want to continue? (y/n) :
```

産業科学医療 (ISM) 帯域の 2.4 GHz- および 5 GHz の周波数は公開されており、ライセンスを受けずに使用できます。したがって、相手側のネットワーク上のデバイスを阻止すると、法的責任を問われる場合があります。

不正なアクセスポイントを阻止せずにそのアクセスポイントを監視するには、`monitor_ap` 引数を使用して `auto-contain` コマンドを入力します。コントローラで検出されたすべてのアドホックの不正な有線アクセスポイントを自動的に阻止するには、オプションの `monitor_ap` を使用せずに `auto-contain` コマンドを入力します。

次に、アドホックの不正の検出とレポートを有効にする例を示します。

```
(Cisco Controller) > config rogue adhoc enable
```

次に、すべてのアドホックの不正なアクセスポイントに対するアラートを有効にする例を示します。

```
(Cisco Controller) > config rogue adhoc alert all
```

次に、アドホックの不正なアクセスポイントを危険性なしとして分類し、外部状態を設定する例を示します。

```
(Cisco Controller) > config rogue adhoc classify friendly state internal 11:11:11:11:11:11
```

関連コマンド

`config rogue auto-contain level`
`show rogue ignore-list`

show rogue rule detailed
show rogue rule summary

config rogue ap classify

不正なアクセスポイントのステータスを分類するには、**config rogue ap classify** コマンドを使用します。

```
config rogue ap classify {friendly state {internal | external} ap_mac}
```

```
config rogue ap classify {malicious | unclassified} state {alert | contain} ap_mac
```

| 構文の説明 | | |
|-------|---------------------|---|
| | friendly | 不正なアクセスポイントを危険性なしとして分類します。 |
| | state | 分類への応答を指定します。 |
| | internal | この不正なアクセスポイントを信頼するようにコントローラを設定します。 |
| | external | このアクセスポイントの存在を認めるようにコントローラを設定します。 |
| | <i>ap_mac</i> | 不正なアクセスポイントの MAC アドレス。 |
| | malicious | 不正なアクセスポイントを潜在的悪意として分類します。 |
| | unclassified | 不正なアクセスポイントを不明として分類します。 |
| | alert | システム管理者に即座にアラートを発信し、必要な措置を促すようにコントローラを設定します。 |
| | contain | 危険性のあるデバイスを阻止して、そのデバイスの信号が認証されたクライアントに干渉しないようにコントローラを設定します。 |

コマンド デフォルト これらのコマンドは、デフォルトでは無効になっています。したがって、すべての不明なアクセスポイントは、デフォルトでは**unclassified**として分類されます。

| コマンド履歴 | リリース | 変更内容 |
|--------|------|---------------------------------|
| | 7.6 | このコマンドは、リリース7.6以前のリリースで導入されました。 |

使用上のガイドライン 現在の状態が **Contain** の場合、不正なアクセスポイントは **Unclassified** クラスに移動できません。

いずれかの containment コマンドを入力すると、「Using this feature may have legal consequences. Do you want to continue?」というメッセージが表示されます。産業科学医療（ISM）帯域の 2.4 GHz- および 5 GHz の周波数は一般に開放されており、ライセンスを受けずに使用できます。
★セグメント分割★ Do you want to continue?」というメッセージが表示されます。産業科学医療（ISM）帯域の 2.4 GHz- および 5 GHz の周波数は公開されており、ライセンスを受けずに使用できます。したがって、相手側のネットワーク上のデバイスを阻止すると、法的責任を問われる場合があります。

次に、不正なアクセスポイントを危険性なしとして分類し、信頼できるようにする例を示します。

```
(Cisco Controller) > config rogue ap classify friendly state internal 11:11:11:11:11:11
```

次に、不正なアクセスポイントを悪意として分類し、アラートを送信する例を示します。

```
(Cisco Controller) > config rogue ap classify malicious state alert 11:11:11:11:11:11
```

次に、不正なアクセスポイントを未分類として分類し、阻止する例を示します。

```
(Cisco Controller) > config rogue ap classify unclassified state contain 11:11:11:11:11:11
```

関連コマンド

- config rogue adhoc**
- config rogue ap friendly**
- config rogue ap rldp**
- config rogue ap ssid**
- config rogue ap timeout**
- config rogue ap valid-client**
- config rogue client**
- config trapflags rogueap**
- show rogue ap clients**
- show rogue ap detailed**
- show rogue ap summary**
- show rogue ap friendly summary**
- show rogue ap malicious summary**
- show rogue ap unclassified summary**
- show rogue client detailed**
- show rogue client summary**
- show rogue ignore-list**

show rogue rule detailed

show rogue rule summary

config rogue ap friendly

新しい危険性のないアクセス ポイント エントリを危険性のない MAC アドレスのリストに追加したり、リストから既存の危険性のないアクセス ポイント エントリを削除したりするには、**config rogue ap friendly** コマンドを入力します。

config rogue ap friendly {**add** | **delete**} *ap_mac*

| | | |
|------------|---------------|--|
| 構文の説明 | add | 危険性のない MAC アドレス リストからこの不正なアクセス ポイントを追加します。 |
| | delete | 危険性のない MAC アドレス リストからこの不正なアクセス ポイントを削除します。 |
| | <i>ap_mac</i> | 追加または削除する不正なアクセス ポイントの MAC アドレス。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、MAC アドレスが 11:11:11:11:11:11 の新しい危険性のないアクセス ポイントを危険性のない MAC アドレス リストに追加する例を示します。

```
(Cisco Controller) > config rogue ap friendly add 11:11:11:11:11:11
```

関連コマンド

config rogue adhoc
config rogue ap classify
config rogue ap rldp
config rogue ap ssid
config rogue ap timeout
config rogue ap valid-client
config rogue client
config trapflags rogueap
show rogue ap clients
show rogue ap detailed
show rogue ap summary
show rogue ap friendly summary

show rogue ap malicious summary
show rogue ap unclassified summary
show rogue client detailed
show rogue client summary
show rogue ignore-list
show rogue rule detailed
show rogue rule summary

config rogue ap rldp

Rogue Location Discovery Protocol (RLDP) を有効化、無効化、または開始するには、**config rogue ap rldp** コマンドを使用します。

config rogue ap rldp enable { **alarm-only** | **auto-contain** } [*monitor_ap_only*]

config rogue ap rldp initiate *rogue_mac_address*

config rogue ap rldp disable

構文の説明

| | |
|--------------------------|--|
| alarm-only | オプションの引数 <i>monitor_ap_only</i> を使用せずに入力すると、すべてのアクセス ポイントで RLDP が有効になります。 |
| auto-contain | オプションの引数 <i>monitor_ap_only</i> を使用せずに入力すると、すべての不正なアクセス ポイントが自動的に阻止されます。 |
| <i>monitor_ap_only</i> | (任意) 指定した監視アクセス ポイントだけで RLDP を有効にするか (alarm-only キーワードを使用した場合)、または自動阻止を有効にします (auto-contain キーワードを使用した場合)。 |
| initiate | 特定の不正なアクセス ポイントで RLDP を開始します。 |
| <i>rogue_mac_address</i> | 特定の不正なアクセス ポイントの MAC アドレス。 |
| disable | すべてのアクセス ポイントで RLDP を無効にします。 |

コマンドデフォルト

なし

コマンド履歴

| リリース | 変更内容 |
|------|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン

いずれかの containment コマンドを入力すると、「Using this feature may have legal consequences. Do you want to continue?」というメッセージが表示されます。産業科学医療 (ISM) 帯域の 2.4 GHz- および 5 GHz の周波数は一般に開放されており、ライセンスを受けずに使用できます。
 ★セグメント分割★ Do you want to continue?」というメッセージが表示されます。産業科学医療 (ISM) 帯域の 2.4 GHz- および 5 GHz の周波数は公開されており、ライセンスを受けずに使用

できます。したがって、相手側のネットワーク上のデバイスを阻止すると、法的責任を問われる場合があります。

次に、すべてのアクセス ポイントで RLDP を有効にする例を示します。

```
(Cisco Controller) > config rogue ap rldp enable alarm-only
```

次に、監視モードアクセス ポイント ap_1 で RLDP を有効にする例を示します。

```
(Cisco Controller) > config rogue ap rldp enable alarm-only ap_1
```

次に、MAC アドレスが 123.456.789.000 の不正なアクセス ポイントで RLDP を開始する例を示します。

```
(Cisco Controller) > config rogue ap rldp initiate 123.456.789.000
```

次に、すべてのアクセス ポイントで RLDP を無効にする例を示します。

```
(Cisco Controller) > config rogue ap rldp disable
```

関連コマンド

- config rogue adhoc**
- config rogue ap classify**
- config rogue ap friendly**
- config rogue ap ssid**
- config rogue ap timeout**
- config rogue ap valid-client**
- config rogue client**
- config trapflags rogueap**
- show rogue ap clients**
- show rogue ap detailed**
- show rogue ap summary**
- show rogue ap friendly summary**
- show rogue ap malicious summary**
- show rogue ap unclassified summary**
- show rogue client detailed**
- show rogue client summary**
- show rogue ignore-list**
- show rogue rule detailed**
- show rogue rule summary**

config rogue ap ssid

アラームだけを生成するか、またはネットワークの Service Set Identifier (SSID) をアドバタイズしている不正なアクセスポイントを阻止するには、**config rogue ap ssid** コマンドを使用します。

config rogue ap ssid {alarm | auto-contain}

| | | |
|-----------|---------------------|--|
| 構文の説明 | alarm | 不正なアクセスポイントがネットワークの SSID をアドバタイズしていることを検出すると、アラームだけを生成します。 |
| | auto-contain | ネットワークの SSID をアドバタイズしている不正なアクセスポイントを自動的に阻止します。 |
| コマンドデフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン いずれかの containment コマンドを入力すると、「Using this feature may have legal consequences. Do you want to continue?」というメッセージが表示されます。産業科学医療 (ISM) 帯域の 2.4 GHz- および 5 GHz の周波数は一般に開放されており、ライセンスを受けずに使用できます。
★セグメント分割★ Do you want to continue?」というメッセージが表示されます。産業科学医療 (ISM) 帯域の 2.4 GHz- および 5 GHz の周波数は公開されており、ライセンスを受けずに使用できます。したがって、相手側のネットワーク上のデバイスを阻止すると、法的責任を問われる場合があります。

次に、ネットワークの SSID をアドバタイズしている不正なアクセスポイントを自動的に阻止する例を示します。

```
(Cisco Controller) > config rogue ap ssid auto-contain
```

関連コマンド

config rogue adhoc
config rogue ap classify
config rogue ap friendly
config rogue ap rldp
config rogue ap timeout
config rogue ap valid-client

config rogue client
config trapflags rogueap
show rogue ap clients
show rogue ap detailed
show rogue ap summary
show rogue ap friendly summary
show rogue ap malicious summary
show rogue ap unclassified summary
show rogue client detailed
show rogue client summary
show rogue ignore-list
show rogue rule detailed
show rogue rule summary

config rogue ap timeout

不正なアクセスポイントおよびクライアントのエントリが期限切れとなり、リストから削除されるまでの秒数を指定するには、**config rogue ap timeout** コマンドを使用します。

config rogue ap timeout *seconds*

| | | |
|-----------|---|---|
| 構文の説明 | <i>seconds</i> | 240 ～ 3600 秒までの値。デフォルト値は 1200 秒です。 |
| コマンドデフォルト | 不正なアクセスポイントおよびクライアントのエントリが期限切れとなるまでのデフォルトの秒数は、1200 秒です。 | |
| コマンド履歴 | リリース 7.6 | 変更内容 このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、不正アクセスポイントとクライアントリストのエントリの有効期限を 2400 秒に設定する例を示します。

```
(Cisco Controller) > config rogue ap timeout 2400
```

関連コマンド

config rogue ap classify
config rogue ap friendly
config rogue ap rldp
config rogue ap ssid
config rogue rule
config trapflags rogueap
show rogue ap clients
show rogue ap detailed
show rogue ap summary
show rogue ap friendly summary
show rogue ap malicious summary
show rogue ap unclassified summary
show rogue ignore-list
show rogue rule detailed
show rogue rule summary

config rogue auto-contain level

不正の自動阻止レベルを設定するには、**config rogue auto-contain level** コマンドを使用します。

config rogue auto-contain level level [monitor_ap_only]

構文の説明

| | |
|------------------------|--|
| <i>level</i> | 1～4の範囲の不正の自動阻止レベル。0の値を入力すると、Cisco WLC が自動阻止に使用する AP の数を自動的に選択できるようになります。コントローラは、有効な阻止のために必要な AP の数を RSSI に基づいて選択します。 |
| monitor_ap_only | (任意) 監視 AP モードのみを使用して自動阻止を設定します。 |

コマンド デフォルト

デフォルトの自動阻止レベルは 1 です。

コマンド履歴

| リリース | 変更内容 |
|------|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン

コントローラは、すべての近隣のアクセスポイントを継続的に監視し、不正なアクセスポイントおよびクライアントに関する情報を自動的に検出して収集します。コントローラは、不正なアクセスポイントを検出すると、設定済み自動阻止ポリシーを使用して自動阻止を開始します。自動阻止を開始するポリシーは、ワイヤ上の不正 (RLDP または Rogue Detector AP によって検出)、管理対象 SSID を使用した不正、不正な AP の有効なクライアント、およびアドホック不正です。

このテーブルは、各阻止レベルに関連付けられている RSSI 値を示します。

表 1: 各阻止レベルに関連付けられている RSSI

| 自動阻止レベル | RSSI |
|---------|---------------|
| 1 | 0 ~ -55 dBm |
| 2 | -75 ~ -55 dBm |
| 3 | -85 ~ -75 dBm |
| 4 | -85 dBm 未満 |



- (注) RLDP は、シスコの Atonomous 不正アクセスポイントではサポートされていません。これらのアクセスポイントは、RLDP クライアントによって送信された DHCP 検出要求をドロップします。また不正なアクセスポイントチャンネルが動的周波数選択 (DFS) を必要とする場合、RLDP はサポートされません。

`containment` コマンドのいずれかを入力すると、次の警告が表示されます。

```
Using this feature may have legal consequences. Do you want to continue? (y/n) :
```

産業科学医療 (ISM) 帯域の 2.4 GHz および 5 GHz の周波数は一般に公開されており、ライセンスを受けずに使用できます。したがって、相手側のネットワーク上のデバイスを阻止すると、法的責任を問われる場合があります。

次に、自動阻止のレベルを 3 に設定する例を示します。

```
(Cisco Controller) > config rogue auto-contain level 3
```

関連コマンド

```
config rogue adhoc  
show rogue adhoc summary  
show rogue client summary  
show rogue ignore-list  
show rogue rule summary
```

config rogue ap valid-client

アラームだけを生成する、または信頼できるクライアントが関連付けられている不正なアクセス ポイントを自動的に阻止するには、**config rogue ap valid-client** コマンドを使用します。

config rogue ap valid-client { **alarm** | **auto-contain** }

| | | |
|------------|---------------------|--|
| 構文の説明 | alarm | 不正なアクセス ポイントが有効なクライアントに関連付けられていることが検出されると、アラームだけが生成されます。 |
| | auto-contain | 信頼できるクライアントに関連付けられている不正なアクセス ポイントを自動的に阻止します。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン いくつかの containment コマンドを入力すると、「Using this feature may have legal consequences. Do you want to continue?」というメッセージが表示されます。産業科学医療 (ISM) 帯域の 2.4 GHz- および 5 GHz の周波数は一般に開放されており、ライセンスを受けずに使用できます。
★セグメント分割★ Do you want to continue?」というメッセージが表示されます。産業科学医療 (ISM) 帯域の 2.4 GHz- および 5 GHz の周波数は公開されており、ライセンスを受けずに使用できます。したがって、相手側のネットワーク上のデバイスを阻止すると、法的責任を問われる場合があります。

次に、有効なクライアントに関連付けられている不正なアクセス ポイントを自動的に阻止する例を示します。

```
(Cisco Controllor) > config rogue ap valid-client auto-contain
```

関連コマンド

config rogue ap classify
config rogue ap friendly
config rogue ap rldp
config rogue ap timeout
config rogue ap ssid
config rogue rule
config trapflags rogueap

show rogue ap clients
show rogue ap detailed
show rogue ap summary
show rogue ap friendly summary
show rogue ap malicious summary
show rogue ap unclassified summary
show rogue ignore-list
show rogue rule detailed
show rogue rule summary

config rogue client

不正なクライアントを設定するには、**config rogue client** コマンドを使用します。

```
config rogue client {aaa {enable | disable} | alert ap_mac | contain client_mac | delete
{state {alert | any | contained | contained-pending} | all | mac-address client_mac} |
mse{enable | disable} } }
```

構文の説明

| | |
|--------------------------|---|
| aaa | 不正なクライアントが有効なクライアントかどうかを検証するように AAA サーバまたはローカル データベースを設定します。デフォルトではディセーブルになっています。 |
| enable | AAA サーバまたはローカルデータベースを有効にして、不正なクライアント MAC アドレスが有効かどうかを確認します。 |
| disable | AAA サーバまたはローカルデータベースを無効にして、不正なクライアント MAC アドレスが有効かどうかを確認しないようにします。 |
| alert | システム管理者に即座にアラートを発信し、必要な措置を促すようにコントローラを設定します。 |
| <i>ap_mac</i> | アクセス ポイントの MAC アドレス。 |
| contain | 危険性のあるデバイスを阻止して、そのデバイスの信号が認証されたクライアントに干渉しないようにコントローラを設定します。 |
| <i>client_mac</i> | 不正なクライアントの MAC アドレス。 |
| delete | 不正なクライアントを削除します。 |
| state | 不正なクライアントをその状態に応じて削除します。 |
| alert | アラート状態の不正クライアントを削除します。 |
| any | 任意の状態の不正クライアントを削除します。 |
| contained | 阻止状態になっているすべての不正クライアントを削除します。 |
| contained-pending | 阻止保留中の状態のすべての不正クライアントを削除します。 |

| | |
|--------------------|--|
| all | すべての不正クライアントを削除します。 |
| mac-address | 設定済みMACアドレスを持つ不正クライアントを削除します。 |
| mse | 不正クライアントが有効なクライアントかどうかをMSEを使用して検証します。デフォルトではディセーブルになっています。 |

コマンドデフォルト なし

| コマンド履歴 | リリース | 変更内容 |
|--------|------|---------------------------------|
| | 7.6 | このコマンドは、リリース7.6以前のリリースで導入されました。 |

使用上のガイドライン MSE と AAA に対して同時に不正クライアントを検証することはできません。

次に、AAA サーバまたはローカルデータベースがMACアドレスを確認できるようにする例を示します。

```
(Cisco Controller) > config rogue client aaa enable
```

次に、AAA サーバまたはローカルデータベースがMACアドレスを確認できないようにする例を示します。

```
(Cisco Controller) > config rogue client aaa disable
```

関連コマンド

config rogue rule
config trapflags rogueap
show rogue ap clients
show rogue ap detailed
show rogue client summary
show rogue ignore-list
show rogue rule detailed
show rogue rule summary

config rogue containment

不正な阻止を設定するには、**config rogue containment** コマンドを使用します。

config rogue containment {flexconnect | auto-rate} {enable | disable}

構文の説明

flexconnect スタンドアロン FlexConnect AP の不正な阻止を設定します。

auto-rate 不正な阻止の自動レート選択を設定します。

enable 不正な阻止を有効にします。

disable 不正な阻止を無効にします。

コマンド デフォルト

なし

コマンド履歴

リリース 変更内容
ス

7.5 このコマンドが導入されました。

使用上のガイドライン

次のテーブルに、不正な阻止の自動レート選択の詳細を示します。

表 2: 不正な阻止の自動レート選択

| RSSI (dBm) | 802.11b/g Tx レート (Mbps) | 802.11a Tx レート (Mbps) |
|------------|-------------------------|-----------------------|
| -74 | 1 | 6 |
| -70 | 2 | 12 |
| -55 | 5.5 | 12 |
| < -40 | 5.5 | 18 |

次に、不正な阻止の自動レート選択を有効にする例を示します。

```
(Cisco Controller) > config rogue containment auto-rate enable
```

config rogue detection

不正の検出を有効または無効にするには、**config rogue detection** コマンドを使用します。



(注) AP 自体が **all** キーワードで設定されている場合、**all access points** の場合は **all** というキーワードを持つ AP に優先します。

config rogue detection {enable | disable} {cisco_ap | all}

構文の説明

| | |
|-----------------|------------------------------|
| enable | このアクセス ポイントにおける不正の検出を有効にします。 |
| disable | このアクセス ポイントにおける不正の検出を無効にします。 |
| <i>cisco_ap</i> | シスコ アクセス ポイント。 |
| all | すべてのアクセス ポイントを指定します。 |

コマンドデフォルト

デフォルトの不正の検出値が有効になります。

コマンド履歴

| リリース | 変更内容 |
|------|---------------------------------|
| 7.6 | このコマンドは、リリース7.6以前のリリースで導入されました。 |

使用上のガイドライン

OfficeExtend アクセス ポイントを除き、コントローラに接続されたすべてのアクセス ポイントに対し、不正の検出がデフォルトで有効にされます。OfficeExtend アクセス ポイントは室内環境に導入され、多くの場合、大量の不正なデバイスを検出します。

次に、アクセス ポイント Cisco_AP の不正の検出を有効にする例を示します。

```
(Cisco Controller) > config rogue detection enable Cisco_AP
```

関連コマンド

config rogue rule
config trapflags rogueap
show rogue client detailed
show rogue client summary
show rogue ignore-list
show rogue rule detailed
show rogue rule summary

config rogue detection client-threshold

アクセス ポイントの不正なクライアントしきい値を設定するには、**config rogue detection client-threshold** コマンドを使用します。

config rogue detection client-threshold *value*

構文の説明

value アクセス ポイントでの不正なクライアント数のしきい値。この値を超えると Cisco Wireless LAN Controller (WLC) からトラップが送信されます。有効な範囲は 1 ~ 256 です。この機能を無効にするには 0 を入力します。

コマンド デフォルト

デフォルトの不正クライアントのしきい値は 12 です。

コマンド履歴

リリース 変更内容
ス

7.5 このコマンドが導入されました。

次に、不正クライアントのしきい値を設定する例を示します。

```
(Cisco Controller) >config rogue detection client-threshold 200
```


config rogue detection min-rssi

AP が不正を検出し、コントローラで不正なエントリを作成できる受信信号強度インジケータ (RSSI) の最小値を設定するには、**config rogue detection min-rssi** コマンドを使用します。

config rogue detection min-rssi *rss-in-dBm*

| | | |
|-------|-------------------|--|
| 構文の説明 | <i>rss-in-dBm</i> | RSSI の最小値。有効な範囲は -70 ~ -128 dBm で、デフォルト値は -128 dBm です。 |
|-------|-------------------|--|

コマンド デフォルト AP の不正を検出するデフォルトの RSSI 値は、-128 dBm です。

| コマンド履歴 | リリース | 変更内容 |
|--------|------|-----------------------------------|
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン この機能は、すべての AP モードに適用できます。

RSSI 値が非常に低い不正が多数あると、不正の分析に有用な情報を得られないことがあります。したがって、AP が不正を検出する最小 RSSI 値を指定することで、このオプションを使用して不正をフィルタリングすることができます。

次に、RSSI の最小値を設定する例を示します。

```
(Cisco Controller) > config rogue detection min-rssi -80
```

関連コマンド

```
config rogue detection
show rogue ap clients
config rogue rule
config trapflags rogueap
show rogue client detailed
show rogue client summary
show rogue ignore-list
show rogue rule detailed
show rogue rule summary
```

config rogue detection monitor-ap

すべての監視モードの Cisco AP に対する不正レポートの間隔を設定するには、**config rogue detection monitor-ap** コマンドを使用します。

config rogue detection monitor-ap {**report-interval** | **transient-rogue-interval**} *time-in-seconds*

構文の説明

| | |
|---------------------------------|---|
| report-interval | 不正レポートが送信される間隔を指定します。 |
| transient-rogue-interval | 最初に不正に対するスキャンを実行した後に、定期的にスキャンを行う間隔を指定します。 |
| <i>time-in-seconds</i> | 秒単位の時間。有効な範囲は次のとおりです。 <ul style="list-style-type: none"> • 10 ~ 300 : report-interval • 120 ~ 1800 : transient-rogue-interval |

コマンド履歴

| リリース | 変更内容 |
|------|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン

この機能は、モニタ モードの AP のみに適用されます。

一時的な間隔値を使用して、AP が不正をスキャンする間隔を制御できます。AP では、それぞれの一時的間隔値に基づいて、不正のフィルタリングも実行できます。

この機能には次の利点があります。

- AP からコントローラへの不正 AP レポートが短くなる。
- 一時的不正エントリをコントローラで回避できる。
- 一時的不正への不要なメモリ割り当てを回避できる。

次に、不正レポートの間隔を 60 秒に設定する例を示します。

```
(Cisco Controller) > config rogue detection monitor-ap report-interval 60
```

次に、一時的不正の間隔を 300 秒に設定する例を示します。

```
(Cisco Controller) > config rogue detection monitor-ap transient-rogue-interval 300
```

関連コマンド

config rogue detection
config rogue detection min-rssi

config rogue rule
config trapflags rogueap
show rogue ap clients
show rogue client detailed
show rogue client summary
show rogue ignore-list
show rogue rule detailed
show rogue rule summary

config rogue detection report-interval

不正検出レポート間隔を設定するには、**config rogue detection report-interval** コマンドを使用します。

config rogue detection report-interval *time*

構文の説明

time アクセスポイントからコントローラに不正検出レポートを送信する間隔（秒単位）です。範囲は 10 ~ 300 です。

コマンド デフォルト

デフォルトの不正検出レポート間隔は 10 秒です。

コマンド履歴

| リリース | 変更内容 |
|------|-----------------|
| 7.5 | このコマンドが導入されました。 |

使用上のガイドライン

この機能は、監視モードのアクセスポイントのみに適用されます。

次に、不正検出レポート間隔を設定する例を示します。

```
(Cisco Controller) >config rogue detection report-interval 60
```

config rogue detection security-level

不正検出セキュリティ レベルを設定するには、**config rogue detection security-level** コマンドを使用します。

config rogue detection security-level { **critical** | **custom** | **high** | **low** }

構文の説明

critical 不正検出セキュリティ レベルを「重大」に設定します。

custom 不正検出セキュリティ レベルを「カスタム」に設定し、不正なポリシーパラメータを設定できるようになります。

high 不正検出セキュリティ レベルを「高」に設定します。このセキュリティレベルは、中規模またはあまり重大でない展開のための基本的な不正検出と自動阻止を設定します。このセキュリティレベルではRogue Location Discovery Protocol (RLDP) は無効です。

low 不正検出セキュリティ レベルを「低」に設定します。このセキュリティレベルは、小規模の展開のための基本的な不正検出を設定します。このセキュリティレベルでは自動阻止はサポートされていません。

コマンドデフォルト

デフォルトの不正検出セキュリティ レベルは「カスタム」です。

コマンド履歴

リリース 変更内容

7.5 このコマンドが導入されました。

次に、不正検出セキュリティ レベルを「高」に設定する例を示します。

```
(Cisco Controller) > config rogue detection security-level high
```

config rogue detection transient-rogue-interval

不正検出の一時的間隔を設定するには、**config rogue detection transient-rogue-interval** コマンドを使用します。

config rogue detection transient-rogue-interval *time*

構文の説明

time 最初に不正がスキャンされた後、アクセス ポイントが継続的に不正をスキャンする必要がある間隔（秒単位）です。有効な範囲は 120 ~ 1800 です。

コマンド デフォルト

各セキュリティ レベルのデフォルトの不正検出の一時的間隔は次のとおりです。

- 低 : 120 秒
- 高 : 300 秒
- 重大 : 600 秒

コマンド履歴

リリー 変更内容
ス

7.5 このコマンドが導入されました。

使用上のガイドライン

この機能は、監視モードのアクセス ポイントのみに適用されます。

連続的に不正がスキャンされると、更新情報が定期的に Cisco Wireless LAN Controller (WLC) へ送信されます。アクセス ポイントは、非常に短い時間だけアクティブな一時的不正をフィルタリングし、その後は活動を停止します。

次に、不正検出の一時的間隔を設定する例を示します。

```
(Cisco Controller) > config rogue detection transient-rogue-interval 200
```

config rogue rule

不正分類ルールを追加および設定するには、**config rogue rule** コマンドを使用します。

```
config rogue rule {add ap priority priority classify {custom severity-score classification-name |
friendly | malicious} notify {all | global | none | local} state {alert | contain | delete |
internal | external} rule_name | classify {custom severity-score classification-name | friendly
| malicious} rule_name | condition ap {set | delete} condition_type condition_value rule_name
| {enable | delete | disable} {all | rule_name} | match {all | any} | priority priority |
notify {all | global | none | local} rule_name | state {alert | contain | internal |
external} rule_name}
```

構文の説明

| | |
|----------------------------|--|
| add ap priority | 指定した基準および優先順位に一致するルールを追加します。 |
| <i>priority</i> | このルールのルールリスト内での優先順位。 |
| classify | ルールの分類を指定します。 |
| custom | カスタムとしてのルールに一致するデバイスを分類します。 |
| <i>severity-score</i> | ルールのカスタム分類の重大度スコア。範囲は 1 ~ 100 です。 |
| <i>classification-name</i> | カスタム分類の名前。名前は最大 32 文字の英数字で、大文字と小文字を区別します。 |
| friendly | ルールを危険性のないルールとして分類します。 |
| malicious | ルールを悪意のあるルールとして分類します。 |
| notify | ルールの照合における通知のタイプを設定します。 |
| all | コントローラ、および Cisco Prime Infrastructure などのトラップレシーバに通知します。 |
| global | Cisco Prime Infrastructure などのトラップレシーバだけに通知します。 |
| local | コントローラだけに通知します。 |
| none | コントローラ、および Cisco Prime Infrastructure などのトラップレシーバのどちらにも通知しません。 |

| | |
|---------------------|---|
| state | ルールの照合後の不正なアクセス ポイントの状態を設定します。 |
| alert | ネイバー リストにない、またはユーザが設定した危険性のないMACのリストに記載されていない不正アクセス ポイントのアラート状態を設定します。コントローラからシステム管理者に、さらなる処理を行うよう即時に警告が転送されます。 |
| contain | 不正アクセス ポイントを contain の状態に設定します。コントローラによって危険性のあるデバイスが阻止され、そのデバイスの信号が、認証されたクライアントに干渉しないようになります。 |
| delete | 不正アクセス ポイントを delete の状態に設定します。 |
| external | ネットワークの外側にあり、WLAN のセキュリティに脅威を与えない不正アクセス ポイントの外部状態を設定します。コントローラはこの不正なアクセス ポイントの存在を認識しています。 |
| internal | ネットワークの内側にあり、WLAN のセキュリティに脅威を与えない不正アクセス ポイントのアラート状態を設定します。コントローラはこの不正なアクセス ポイントを信頼します。 |
| <i>rule_name</i> | コマンドを適用するルールまたは新しいルールの名前。 |
| condition ap | 不正なアクセス ポイントが満たす必要のあるルールに条件を指定します。 |
| set | 不正なアクセス ポイントが満たす必要のあるルールに条件を追加します。 |
| delete | 不正なアクセス ポイントが満たす必要のあるルールの条件を削除します。 |

| | |
|------------------------|---|
| <i>condition_type</i> | <p>設定する条件のタイプ。条件タイプは以下のとおりです。</p> <ul style="list-style-type: none"> • client-count : 最小数のクライアントが不正なアクセスポイントにアソシエートされていることが条件となります。有効な範囲は 1 ~ 10 です。 • duration : 不正なアクセスポイントが最短期間で検出されることが条件となります。有効な範囲は 0 ~ 3600 秒です。 • managed-ssid : 不正なアクセスポイントの SSID がコントローラで認識される必要があります。 • no-encryption : 不正なアクセスポイントのアドバタイズされた WLAN で暗号化が無効になっている必要があります。 • rssi : 不正なアクセスポイントには、最小の RSSI 値が必要です。範囲は、-95 ~ -50 dBm です。 • ssid : 不正なアクセスポイントには、特定の SSID が必要です。 • substring-ssid : 不正なアクセスポイントにユーザ設定 SSID のサブストリングが存在する必要があります。 |
| <i>condition_value</i> | <p>条件の値。この値は、condition_type によって異なります。たとえば、条件タイプが ssid の場合、条件値は SSID 名か all です。</p> |
| enable | <p>すべてのルールまたは特定のルール 1 つを有効にします。</p> |
| delete | <p>すべてのルールまたは特定のルール 1 つを削除します。</p> |
| disable | <p>すべてのルールまたは特定のルール 1 つを削除します。</p> |

| | |
|-----------------|--|
| match | 検出された不正なアクセス ポイントがルールに一致していると見なされ、そのルールの分類タイプが適用されるためには、ルールで定義されているすべての条件を満たす必要があるか、一部の条件を満たす必要があるかを指定します。 |
| all | 定義されているすべてのルールを指定します。 |
| any | 特定の条件を満たしているルールを指定します。 |
| priority | 特定のルールの優先順位を変更し、それに応じて、リスト内のその他のルールの優先順位を調整します。 |

コマンド デフォルト 不正ルールが設定されていません。

| コマンド履歴 | リリース | 変更内容 |
|--------|------|-----------------------------------|
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン 変更内容を有効にするには、ルールを有効にする必要があります。最大 64 のルールを設定できます。

不正なルールの RSSI 基準に応じた不正な AP の再分類は、RSSI が設定された RSSI 値から ± 2 dBm を超えて変更された場合のみ発生します。手動および自動による分類は、カスタムの不正なルールよりも優先されます。クラス タイプが未分類に変更され、状態が `alert` に変更されると、ルールは手動で変更された不正に適用されます。アドホックの不正は分類され、保留状態にはなりません。最大 50 個の分類タイプを設定できます。

次に、優先順位が 1、分類が `friendly` である、`rule_1` という名前のルールを作成する例を示します。

```
(Cisco Controller) > config rogue rule add ap priority 1 classify friendly rule_1
```

次に、`rule_1` を有効にする例を示します。

```
(Cisco Controller) > config rogue rule enable rule_1
```

次に、最後のコマンドの優先順位を変更する例を示します。

```
(Cisco Controller) > config rogue rule priority 2 rule_1
```

次に、最後のコマンドの分類を変更する例を示します。

```
(Cisco Controller) > config rogue rule classify malicious rule_1
```

次に、最後のコマンドを無効にする例を示します。

```
(Cisco Controller) > config rogue rule disable rule_1
```

次に、rule-5 のユーザが設定した SSID リストから SSID_2 を削除する例を示します。

```
(Cisco Controller) > config rogue rule condition ap delete ssid ssid_2 rule-5
```

次に、カスタムの不正なルールを作成する例を示します。

```
(Cisco Controller) > config rogue rule classify custom 1 VeryMalicious rule6
```

config rogue rule condition ap

不正アクセス ポイントの不正ルールの条件を設定するには、**config rogue rule condition ap** コマンドを使用します。

```
config rogue rule condition ap {set {client-count count | duration time | managed-ssid |
no-encryption | rssi rssi | ssid ssid | substring-ssid substring-ssid} | delete {all | client-count
| duration | managed-ssid | no-encryption | rssi | ssid | substring-ssid} rule_name
```

構文の説明

| | |
|-----------------------|--|
| set | 不正なアクセス ポイントが満たす必要のあるルールに条件を設定します。 |
| client-count | 不正アクセス ポイントに最小数のクライアントをアソシエートできるようにします。 |
| <i>count</i> | 不正アクセス ポイントにアソシエートする最小数のクライアント。範囲は 1 ~ 10 です。たとえば、不正なアクセス ポイントにアソシエートされたクライアントの数が設定値以上の場合、アクセス ポイントは Malicious に分類されます。 |
| duration | 不正アクセス ポイントを最小期間で検出できるようにします。 |
| <i>time</i> | 不正アクセス ポイントを検出する最小期間 (秒単位)。範囲は 0 ~ 3600 です。 |
| managed-ssid | 不正アクセス ポイントの SSID がコントローラで認識されるようにします。 |
| no-encryption | 不正アクセス ポイントのアドバタイズされた WLAN で暗号化を無効にできるようにします。不正なアクセス ポイントの暗号化が無効になっている場合、より多くのクライアントがそのアクセス ポイントに対してアソシエートを試行します。 |
| rssi | 不正なアクセス ポイントが最小の受信信号強度インジケータ (RSSI) 値を持てるようにします。 |
| <i>rssi</i> | アクセス ポイントに必要な最小 RSSI 値 (dBm)。範囲は、-95 ~ -50 です。たとえば、不正なアクセス ポイントが設定値より大きい RSSI を持つ場合、そのアクセス ポイントは Malicious に分類されます。 |
| ssid | 不正なアクセス ポイントが特定の SSID を持てるようにします。 |
| <i>ssid</i> | 不正アクセス ポイントの SSID。 |
| substring-ssid | 不正アクセス ポイントがユーザ設定の SSID のサブストリングを持てるようにします。 |
| <i>substring-ssid</i> | ユーザ設定 SSID のサブストリング。たとえば、ABCDE という SSID がある場合、ABCD または ABC としてサブストリングを指定できます。パターンが一致する複数の SSID を分類することができます。 |

| | |
|------------------|---------------------------------|
| delete | 不正なアクセス ポイントが満たす必要のあるルールを削除します。 |
| all | すべての不正ルールの条件を削除します。 |
| <i>rule_name</i> | コマンドが適用される不正ルール。 |

コマンド デフォルト

RSSI のデフォルト値は 0 dBm です。
 デフォルトの間隔値は 0 秒です。
 クライアント数のデフォルト値は 0 です。

コマンド履歴

| リリース | 変更内容 |
|------|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン

不正ルールあたり最大 25 の SSID を設定することができます。不正ルールあたり最大 25 の SSID サブストリングを設定することができます。

次に、RSSI 不正ルールの条件を設定する例を示します。

```
(Cisco Controller) > config rogue rule condition ap set rssi -50
```

config remote-lan session-timeout

クライアントセッションのタイムアウトを設定するには、**config remote-lan session-timeout** コマンドを使用します。

config remote-lan session-timeout *remote-lan-id* *seconds*

| | | |
|------------|----------------------|---|
| 構文の説明 | <i>remote-lan-id</i> | リモート LAN の識別子。有効な値は、1 ~ 512 です。 |
| | <i>seconds</i> | タイムアウトまたはセッション時間（秒）。値 0 は、タイムアウトなしに相当します。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、ID 1 のリモート LAN で、クライアントセッションタイムアウトを 6000 秒に設定する例を示します。

```
(Cisco Controller) >config remote-lan session-timeout 1 6000
```

config rfid auto-timeout

無線周波数 ID (RFID) タグの自動タイムアウトを設定するには、**config rfid auto-timeout** コマンドを使用します。

config rfid auto-timeout { **enable** | **disable** }

| | | |
|-----------|----------------|-----------------------------------|
| 構文の説明 | enable | 自動タイムアウトをイネーブルにします。 |
| | disable | 自動タイムアウトをディセーブルにします。 |
| コマンドデフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、RFID タグの自動タイムアウトをイネーブルにする例を示します。

```
(Cisco Controller) > config rfid auto-timeout enable
```

関連コマンド

- show rfid summary**
- config rfid status**
- config rfid timeout**

config rfid status

無線周波数 ID (RFID) タグのデータ追跡を設定するには、**config rfid status** コマンドを使用します。

config rfid status {enable | disable}

| | | |
|------------|----------------|-----------------------------------|
| 構文の説明 | enable | RFID タグ追跡をイネーブルにします。 |
| | disable | RFID タグ追跡をイネーブルにします。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、RFID タグ追跡を設定する例を示します。

```
(Cisco Controller) > config rfid status enable
```

関連コマンド

show rfid summary
config rfid auto-timeout
config rfid timeout

config rfid timeout

スタティック無線周波数 ID (RFID) タグのデータ タイムアウトを設定するには、**config rfid timeout** コマンドを使用します。

config rfid timeout *seconds*

| | | |
|------------|----------------|-----------------------------------|
| 構文の説明 | <i>seconds</i> | 秒単位でのタイムアウト (60 ~ 7,200)。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース ス | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、スタティック RFID タグのデータ タイムアウトを 60 秒に設定する例を示します。

```
(Cisco Controller) > config rfid timeout 60
```

関連コマンド

- show rfid summary**
- config rfid statistics**

config rogue ap timeout

不正なアクセスポイントおよびクライアントのエントリが期限切れとなり、リストから削除されるまでの秒数を指定するには、**config rogue ap timeout** コマンドを使用します。

config rogue ap timeout seconds

| | | |
|------------|---|------------------------------------|
| 構文の説明 | <i>seconds</i> | 240 ~ 3600 秒までの値。デフォルト値は 1200 秒です。 |
| コマンド デフォルト | 不正なアクセスポイントおよびクライアントのエントリが期限切れとなるまでのデフォルトの秒数は、1200 秒です。 | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、不正アクセスポイントとクライアントリストのエントリの有効期限を 2400 秒に設定する例を示します。

```
(Cisco Controller) > config rogue ap timeout 2400
```

関連コマンド

config rogue ap classify
config rogue ap friendly
config rogue ap rldp
config rogue ap ssid
config rogue rule
config trapflags rogueap
show rogue ap clients
show rogue ap detailed
show rogue ap summary
show rogue ap friendly summary
show rogue ap malicious summary
show rogue ap unclassified summary
show rogue ignore-list
show rogue rule detailed
show rogue rule summary

config route add

サービスポートから専用ワークステーションの IP アドレス範囲へのネットワーク ルートを設定するには、**config route add** コマンドを使用します。

config route add *ip_address netmask gateway*

| | | |
|------------|---|---|
| 構文の説明 | <i>ip_address</i> | ネットワーク IP アドレス。 |
| | <i>netmask</i> | ネットワークのサブネット マスク。 |
| | <i>gateway</i> | ルートネットワークのゲートウェイの IP アドレス。 |
| コマンド デフォルト | なし | |
| 使用上のガイドライン | リリース 7.6 の時点で、 <i>IP_address</i> は IPv4 アドレスのみをサポートします。 | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 このコマンドは、IPv4 アドレス形式のみをサポートします。 |

次に、専用ワークステーションの IP アドレス 10.1.1.0、サブネット マスク 255.255.255.0、およびゲートウェイ 10.1.1.1 へのネットワーク ルートを設定する例を示します。

```
(Cisco Controller) > config route add 10.1.1.0 255.255.255.0 10.1.1.1
```

config route delete

サービスポートからネットワークルートを削除するには、**config route delete** コマンドを使用します。

config route delete *ip_address*

| | | |
|------------|---|-----------------------------------|
| 構文の説明 | <i>ip_address</i> | ネットワーク IP アドレス。 |
| コマンド デフォルト | なし | |
| 使用上のガイドライン | リリース 7.6 の時点で、 <i>IP_address</i> は IPv4 アドレスのみをサポートします。 | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |
| | 8.0 | このコマンドは、IPv6 アドレス形式のみをサポートします。 |

次に、ネットワーク IP アドレス 10.1.1.0 からルートを削除する例を示します。

```
(Cisco Controller) > config route delete 10.1.1.0
```

config serial baudrate

シリアルポートのボーレートを設定するには、**config serial baudrate** コマンドを使用します。

config serial baudrate {1200 | 2400 | 4800 | 9600 | 19200 | 38400 | 57600}

| 構文の説明 | | |
|-------|-------|------------------------------|
| | 1200 | サポートされている接続速度を 1200 に指定します。 |
| | 2400 | サポートされている接続速度を 2400 に指定します。 |
| | 4800 | サポートされている接続速度を 4800 に指定します。 |
| | 9600 | サポートされている接続速度を 9600 に指定します。 |
| | 19200 | サポートされている接続速度を 19200 に指定します。 |
| | 38400 | サポートされている接続速度を 38400 に指定します。 |
| | 57600 | サポートされている接続速度を 57600 に指定します。 |

コマンドデフォルト デフォルトのシリアルポートのボーレートは 9600 です。

| コマンド履歴 | リリース | 変更内容 |
|--------|------|-----------------------------------|
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、9600 のデフォルトの接続速度でシリアルボーレートを設定する例を示します。

```
(Cisco Controller) > config serial baudrate 9600
```

config serial timeout

シリアルポートセッションのタイムアウトを設定するには、**config serial timeout** コマンドを使用します。

config serial timeout *minutes*

| | | |
|------------|---|--|
| 構文の説明 | <i>minutes</i> | 分単位でのタイムアウト (0 ~ 160 分)。値 0 は、タイムアウトなしを示します。 |
| コマンド デフォルト | 0 (タイムアウトなし) | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |
| 使用上のガイドライン | このコマンドを使用して、Cisco ワイヤレス LAN コントローラ前面のシリアル接続のタイムアウトを 0 ~ 160 分の範囲で設定します (0 はタイムアウトなし)。 | |

次に、シリアルポートセッションのタイムアウトを 10 分に設定する例を示します。

```
(Cisco Controller) > config serial timeout 10
```

config service timestamps

メッセージログのタイムスタンプを有効または無効にするには、**config service timestamps** コマンドを使用します。

config service timestamps {**debug** | **log**} {**datetime** | **disable**}

| 構文の説明 | | |
|-------|-----------------|---------------------------------|
| | debug | デバッグメッセージのタイムスタンプを設定します。 |
| | log | ログメッセージのタイムスタンプを設定します。 |
| | datetime | 標準日付を使用して、タイムスタンプメッセージログを指定します。 |
| | disable | メッセージログにタイムスタンプが設定されないように指定します。 |

コマンドデフォルト デフォルトでは、メッセージログのタイムスタンプは無効です。

コマンド履歴

リリース 変更内容
ス

7.6 このコマンドは、リリース7.6以前のリリースで導入されました。

次に、標準日付を使用して、タイムスタンプメッセージログを設定する例を示します。

```
(Cisco Controller) > config service timestamps log datetime
```

次に、メッセージログにタイムスタンプが設定されないようにする例を示します。

```
(Cisco Controller) > config service timestamps debug disable
```

関連コマンド

show logging

config sessions maxsessions

Cisco Wireless LAN Controller で許可する Telnet CLI セッション数を設定するには、**config sessions maxsessions** コマンドを使用します。

config sessions maxsessions session_num

| | |
|------------|--|
| 構文の説明 | <i>session_num</i> 0 ~ 5 のセッション数。 |
| コマンド デフォルト | Cisco WLC で許可される Telnet CLI セッションのデフォルト数は 5 です。 |
| コマンド履歴 | リリース 変更内容 7.6 このコマンドは、リリース 7.6 以前のリリースで導入されました。 |
| 使用上のガイドライン | 最大 5 セッションが許可されます。0 に設定するとすべての Telnet CLI セッションが禁止されます。 次に、許可される CLI セッションの数を 2 に設定する例を示します。 (Cisco Controller) > config sessions maxsessions 2 |
| 関連コマンド | show sessions |

config sessions timeout

Telnet CLI セッションの無活動タイムアウトを設定するには、**config sessions timeout** コマンドを使用します。

config sessions timeout *timeout*

| | | |
|-------|----------------|---|
| 構文の説明 | <i>timeout</i> | 分単位の Telnet セッションのタイムアウト (0 ~ 160 分)。値 0 は、タイムアウトなしを示します。 |
|-------|----------------|---|

| | |
|------------|--|
| コマンド デフォルト | Telnet CSI セッションのデフォルトの無活動タイムアウトは 5 分です。 |
|------------|--|

| | |
|--------|---------------------------------------|
| コマンド履歴 | リリース 変更内容 ス |
| | 7.6 このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、Telnet セッションの無活動タイムアウトを 20 分に設定する例を示します。

```
(Cisco Controller) > config sessions timeout 20
```

| | |
|--------|----------------------|
| 関連コマンド | show sessions |
|--------|----------------------|

config slot

さまざまなスロットパラメータを設定するには、**config slot** コマンドを使用します。

```
config slot slot_id {enable | disable | channel ap | chan_width | txpower ap | antenna  
extAntGain antenna_gain | rts} cisco_ap
```

構文の説明

| | |
|---------------------|---|
| <i>slot_id</i> | チャンネルが割り当てられたスロットのダウンリンク無線。リリース 7.5 以降のリリースでは、スロット 1 で 802.11a、スロット 2 で 802.11ac を設定できます。 |
| enable | スロットを有効にします。 |
| disable | スロットを無効にします。 |
| channel | スロットにチャンネルを設定します。 |
| ap | 1 個の 802.11a Cisco アクセス ポイントを設定します。 |
| chan_width | スロットのチャンネル幅を設定します。 |
| txpower | スロットの Tx 電力を設定します。 |
| antenna | 802.11a アンテナを設定します。 |
| extAntGain | 802.11a 外部アンテナ ゲインを設定します。 |
| <i>antenna_gain</i> | 0.5 dBi 単位の外部アンテナゲイン値（例：2.5 dBi = 5）。 |
| rts | アクセスポイントに対して RTS/CTS を設定します。 |
| <i>cisco_ap</i> | チャンネルが設定されている Cisco アクセスポイントの名前。 |

コマンド デフォルト

なし

コマンド履歴

| リリース | 変更内容 |
|------|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、アクセスポイント abc のスロット 3 を有効にする例を示します。

```
(Cisco Controller) >config slot 3 enable abc
```

次に、アクセスポイント abc の RTS を設定する例を示します。

```
(Cisco Controller) >config slot 2 rts abc
```

config switchconfig boot-break

システムの起動時に Esc キーを押して、ブートプロンプトに割り込む操作をイネーブルまたはディセーブルにするには、**config switchconfig boot-break** コマンドを使用します。

config switchconfig boot-break {enable | disable}

構文の説明

| | |
|----------------|--|
| enable | システムの起動時に Esc キーを押して、ブートプロンプトに割り込む操作をイネーブルにします。 |
| disable | システムの起動時に Esc キーを押して、ブートプロンプトに割り込むことをディセーブルにします。 |

コマンド デフォルト

デフォルトでは、システムの起動時に Esc キーを押して、ブートプロンプトに割り込む操作は無効です。

使用上のガイドライン

ブートにプロンプトへの割り込みをイネーブルまたはディセーブルにする前に、連邦情報処理標準 (FIPS) モードの前提条件である機能をイネーブルにする必要があります。

次に、システムの起動時に Esc キーを押して、ブートプロンプトに割り込む操作をイネーブルにする例を示します。

```
(Cisco Controller) > config switchconfig boot-break enable
```

関連コマンド

show switchconfig
config switchconfig flowcontrol
config switchconfig mode
config switchconfig secret-obfuscation
config switchconfig fips-prerequisite
config switchconfig strong-pwd

config switchconfig fips-prerequisite

連邦情報処理標準（FIPS）モードの前提条件である機能をイネーブルまたはディセーブルにするには、**config switchconfig fips-prerequisite** コマンドを使用します。

config switchconfig fips-prerequisite {**enable** | **disable**}

| | | |
|-------|----------------|--------------------------------|
| 構文の説明 | enable | FIPS モードの前提条件である機能をイネーブルにします。 |
| | disable | FIPS モードの前提条件である機能をディセーブルにします。 |

コマンドデフォルト デフォルトでは、FIPS モードの前提条件である機能は無効です。

使用上のガイドライン FIPS の前提条件である機能をイネーブルまたはディセーブルにするには、FIPS 承認のシークレットを設定する必要があります。

次に、FIPS モードの前提条件である機能をイネーブルにする例を示します。

```
(Cisco Controller) > config switchconfig fips-prerequisite enable
```

関連コマンド

- show switchconfig**
- config switchconfig flowcontrol**
- config switchconfig mode**
- config switchconfig secret-obfuscation**
- config switchconfig boot-break**
- config switchconfig strong-pwd**

config switchconfig ucapl

コントローラの米国の国防総省 (DoD) の統一機能承認製品リスト (APL) 認証を設定するには、**config switchconfig wlanca** コマンドを使用します。

config switchconfig ucapl {enable | disable}

| | | |
|------------|----------------|------------------------|
| 構文の説明 | enable | コントローラで UCAPL を有効にします。 |
| | disable | コントローラで UCAPL を無効にします。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 8.0 | このコマンドが導入されました。 |

次に、コントローラで UCAPL をイネーブルにする例を示します。

```
(Cisco Controller) > config switchconfig ucapl enable
```

config switchconfig wlancc

コントローラで WLAN コモンクライテリア (CC) を設定するには、**config switchconfig wlancc** コマンドを使用します。

config switchconfig wlancc { **enable** | **disable** }

| | | |
|-----------|----------------|--------------------------|
| 構文の説明 | enable | コントローラの WLAN CC を有効にします。 |
| | disable | コントローラの WLAN CC を無効にします。 |
| コマンドデフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 8.0 | このコマンドが導入されました。 |

次に、コントローラで WLAN CC を有効にする例を示します。

```
(Cisco Controller) > config switchconfig wlancc enable
```

config switchconfig strong-pwd

新しく作成されたパスワードの強度に対するコントローラのチェックをイネーブルまたはディセーブルにするには、**config switchconfig strong-pwd** コマンドを使用します。

```
config switchconfig strong-pwd { case-check | consecutive-check | default-check | username-check
| position-check | case-digit-check | minimum { upper-case | lower-case | digits |
special-chars } no_of_characters | min-length | password_length | lockout { mgmtuser |
snmpv3user | time | attempts } | lifetime { mgmtuser | snmpv3user } lifetime | all-checks }
{ enable | disable }
```

構文の説明

| | |
|--------------------------|---|
| case-check | 小文字、大文字、数字、または特種文字から少なくとも3つが組み合わされているかをチェックします。 |
| consecutive-check | 同じ文字が3回使用されていないかをチェックします。 |
| default-check | デフォルト値またはそれらのバリエーションが使用されていないかをチェックします。 |
| username-check | ユーザ名が指定されているかどうかをチェックします。 |
| position-check | 古いパスワードからの変更が4文字あるかどうかをチェックします。 |
| case-digit-check | パスワードに大文字、小文字、数字、特殊文字の4つすべての組み合わせが含まれているかどうかをチェックします。 |
| minimum | パスワードに大文字と小文字、数字、特殊文字の最小数が含まれているかどうかをチェックします。 |
| upper-case | パスワードに大文字の最小数が含まれているかどうかをチェックします。 |
| lower-case | パスワードに小文字の最小数が含まれているかどうかをチェックします。 |
| digits | パスワードに数字の最小数が含まれているかどうかをチェックします。 |
| special-chars | パスワードに特殊文字の最小数が含まれているかどうかをチェックします。 |
| min-length | パスワードの最小文字数を設定します。 |

| | |
|------------------------|--|
| <i>password_length</i> | パスワードの最小文字数。値の範囲は 3 ~ 24 文字です (大文字と小文字を区別します)。 |
| lockout | 管理ユーザまたは Simple Network Management Protocol version 3 (SNMPv3) ユーザのロックアウト機能を設定します。 |
| mgmtuser | 連続試行失敗回数が管理ユーザのロックアウト試行回数を超えると、管理ユーザをロックします。 |
| snmpv3user | 連続試行失敗回数が SNMPv3 ユーザのロックアウト試行回数を超えると、SNMPv3 ユーザをロックします。 |
| time | 管理ユーザまたは SNMPv3 ユーザがロックされているときの、ロックアウト試行後の継続時間を設定します。 |
| attempts | 不正パスワードの連続入力回数を設定します。この回数を超えると管理ユーザまたは SNMPv3 ユーザがロックされます。 |
| lifetime | パスワードのエージングが原因で、管理ユーザまたは SNMPv3 ユーザによるパスワードの変更が必要になるまでの日数を設定します。 |
| mgmtuser | パスワードのエージングが原因で、管理ユーザによるパスワードの変更が必要になるまでの日数を設定します。 |
| snmpv3user | パスワードのエージングが原因で、SNMPv3 ユーザによるパスワードの変更が必要になるまでの日数を設定します。 |
| <i>lifetime</i> | パスワードのエージングが原因で、管理ユーザまたは SNMPv3 ユーザによるパスワードの変更が必要になるまでの日数。 <i>lifetime</i> |
| all-checks | すべてのケースをチェックします。 |
| enable | アクセスポイントおよび Cisco WLC の強力なパスワードチェックを有効にします。 |
| disable | アクセスポイントおよび Cisco WLC の強力なパスワードチェックを無効にします。 |

コマンドデフォルト なし

コマンド履歴

| リリース | 変更内容 |
|------|------|
|------|------|

| | |
|-----|---------------------------------|
| 7.6 | このコマンドは、リリース7.6以前のリリースで導入されました。 |
|-----|---------------------------------|

次に、強力なパスワードチェック機能をイネーブルにする例を示します。

```
(Cisco Controller) > config switchconfig strong-pwd case-check enable
```

関連コマンド

show switchconfig

config switchconfig flowcontrol

config switchconfig mode

config switchconfig secret-obfuscation

config switchconfig fips-prerequisite

config switchconfig boot-break

config switchconfig flowcontrol

802.3x のフロー制御を有効または無効にするには、**config switchconfig flowcontrol** コマンドを使用します。

config switchconfig flowcontrol {enable | disable}

構文の説明

enable

802.3x フロー制御をイネーブルにします。

disable

802.3x フロー制御をディセーブルにします。

コマンド デフォルト

デフォルトでは、802.3X のフロー制御は無効にされています。

次に、Cisco ワイヤレス LAN コントローラ パラメータで 802.3x フロー制御をイネーブルにする例を示します。

```
(Cisco Controller) > config switchconfig flowcontrol enable
```

関連コマンド

show switchconfig

config switchconfig mode

レイヤ 2 またはレイヤ 3 の Lightweight Access Port Protocol (LWAPP) トランスポート モードを設定するには、**config switchconfig mode** コマンドを使用します。

config switchconfig mode {L2 | L3}

| 構文の説明 | L2 | L3 |
|-------|-----------------------------|-----------------------------|
| | トランスポート モードとしてレイヤ 2 を指定します。 | トランスポート モードとしてレイヤ 3 を指定します。 |

コマンド デフォルト デフォルトのトランスポート モードは L3 です。

コマンド履歴

リリース 変更内容
ス

7.6 このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、LWAPP トランスポート モードをレイヤ 3 に設定する例を示します。

```
(Cisco Controller) > config switchconfig mode L3
```

関連コマンド

show switchconfig

config switchconfig secret-obfuscation

機密事項の難読化を有効または無効にするには、**config switchconfig secret-obfuscation** コマンドを使用します。

config switchconfig secret-obfuscation { **enable** | **disable** }

構文の説明

enable

機密事項の難読化をイネーブルにします。

disable

機密事項の難読化をディセーブルにします。

コマンドデフォルト

機密事項およびユーザパスワードは、エクスポートされた XML 設定ファイルでは難読化されません。

コマンド履歴

リリース 変更内容
ス

7.6 このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

設定ファイルの機密の内容を安全に保護するには、機密事項の難読化を無効にしないでください。設定ファイルのセキュリティをさらに強化するには、設定ファイルの暗号化を有効にします。

次に、機密事項の難読化をイネーブルにする例を示します。

```
(Cisco Controller) > config switchconfig secret-obfuscation enable
```

関連コマンド

show switchconfig

config sysname

Cisco Wireless LAN Controller のシステム名を設定するには、**config sysname** コマンドを使用します。

config sysname *name*

| | | |
|-------|-------------|---------------------------------|
| 構文の説明 | <i>name</i> | システム名。名前には、最大 31 文字の英数字を使用できます。 |
|-------|-------------|---------------------------------|

| | |
|------------|----|
| コマンド デフォルト | なし |
|------------|----|

| | |
|--------|-----------|
| コマンド履歴 | リリース 変更内容 |
|--------|-----------|

| | |
|-----|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |
|-----|-----------------------------------|

次に、Ent_01 という名前のシステムを設定する例を示します。

```
(Cisco Controller) > config sysname Ent_01
```

| | |
|--------|---------------------|
| 関連コマンド | show sysinfo |
|--------|---------------------|

config snmp community accessmode

SNMP コミュニティのアクセスモード（読み取り専用または読み取りと書き込み）を変更するには、**config snmp community accessmode** コマンドを使用します。

config snmp community accessmode {ro | rw} name

構文の説明

| | |
|-------------|---------------------|
| ro | 読み取り専用モードを指定します。 |
| rw | 読み取り/書き込みモードを指定します。 |
| name | SNMP コミュニティ名。 |

コマンドデフォルト

デフォルトでは、次の設定を持つ2つのコミュニティが設定されています。

| SNMP Community Name | Client IP Address | Client IP Mask | Access Mode | Status |
|---------------------|-------------------|----------------|-------------|--------|
| public | 0.0.0.0 | 0.0.0.0 | Read Only | Enable |
| private | 0.0.0.0 | 0.0.0.0 | Read/Write | Enable |

コマンド履歴

リリース 変更内容
ス

7.6 このコマンドは、リリース7.6以前のリリースで導入されました。

次に、SNMP コミュニティに読み取り/書き込みアクセスモードを設定する例を示します。

```
(Cisco Controller) > config snmp community accessmode rw private
```

関連コマンド

show snmp community
config snmp community mode
config snmp community create
config snmp community delete
config snmp community ipaddr

config snmp community create

新規 SNMP コミュニティを作成するには、**config snmp community create** コマンドを使用します。

config snmp community create *name*

| | | |
|-------|-------------|-------------------------|
| 構文の説明 | <i>name</i> | 最大 16 文字の SNMP コミュニティ名。 |
|-------|-------------|-------------------------|

| | |
|-----------|----|
| コマンドデフォルト | なし |
|-----------|----|

| | |
|--------|--|
| コマンド履歴 | リリース 変更内容 7.6 このコマンドは、リリース 7.6 以前のリリースで導入されました。 |
|--------|--|

使用上のガイドライン 次のコマンドを使用して、デフォルト設定の新規コミュニティを作成します。
次に、**test** という名前の新しい SNMP コミュニティを作成する例を示します。

```
(Cisco Controller) > config snmp community create test
```

| | |
|--------|--|
| 関連コマンド | show snmp community config snmp community mode config snmp community accessmode config snmp community delete config snmp community ipaddr |
|--------|--|

config snmp community delete

SNMP コミュニティを削除するには、**config snmp community delete** コマンドを使用します。

config snmp community delete *name*

| | | |
|-----------|-------------|---------------------------------|
| 構文の説明 | <i>name</i> | SNMP コミュニティ名。 |
| コマンドデフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース7.6以前のリリースで導入されました。 |

次に、**test** という名前の SNMP コミュニティを削除する例を示します。

```
(Cisco Controller) > config snmp community delete test
```

関連コマンド

show snmp community
config snmp community mode
config snmp community accessmode
config snmp community create
config snmp community ipaddr

config snmp community ipaddr

SNMP コミュニティの IPv4 または IPv6 アドレスを設定するには、**config snmp community ipaddr** コマンドを使用します。

config snmp community ipaddr *IP addr IPv4 mask/IPv6 Prefix length* *name*

| | | |
|------------|-------------------------------------|---|
| 構文の説明 | <i>ip-addr</i> | SNMP コミュニティの IPv4 または IPv6 アドレス。 |
| | <i>IPv4 mask/IPv6 Prefix length</i> | SNMP コミュニティ IP マスク (IPv4 マスクまたは IPv6 プレフィックス長)。IPv6 プレフィックス長は、0 ~ 128 です。 |
| | <i>name</i> | SNMP コミュニティ名。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |
| | 8.0 | このコマンドは、IPv4 と IPv6 の両方のアドレス形式をサポートします。 |

使用上のガイドライン

- このコマンドは、IPv4 と IPv6 の両方のアドレスに適用されます。
- このコマンドは、デフォルトの SNMP コミュニティ (パブリック、プライベート) には適用されません。

次に、IPv4 アドレス 10.10.10.10、IPv4 マスク 255.255.255.0、および SNMP コミュニティ名 comaccess の SNMP コミュニティを設定する例を示します。

```
(Cisco Controller) > config snmp community ipaddr 10.10.10.10 255.255.255.0 comaccess
```

次に、IPv6 アドレス 2001:9:2:16::1、IPv6 プレフィックス長 60、および SNMP コミュニティ名 comaccess の SNMP コミュニティを設定する例を示します。

```
(Cisco Controller) > config snmp community ipaddr 2001:9:2:16::1 64 comaccess
```

config snmp community mode

SNMP コミュニティを有効または無効にするには、**config snmp community mode** コマンドを使用します。

config snmp community mode {enable | disable} *name*

| | | |
|-------|----------------|--------------------|
| 構文の説明 | enable | コミュニティをイネーブルにします。 |
| | disable | コミュニティをディセーブルにします。 |
| | <i>name</i> | SNMP コミュニティ名。 |

コマンドデフォルト なし

| | | |
|--------|------|---------------------------------|
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース7.6以前のリリースで導入されました。 |

次に、public という名前の SNMP コミュニティを有効にする例を示します。

```
(Cisco Controller) > config snmp community mode enable public
```

関連コマンド

- show snmp community**
- config snmp community delete**
- config snmp community accessmode**
- config snmp community create**
- config snmp community ipaddr**

config snmp engineID

SNMP エンジン ID を設定するには、**config snmp engineID** コマンドを使用します。

config snmp engineID {*engine_id* | **default**}

| | | |
|------------|------------------|---|
| 構文の説明 | <i>engine_id</i> | 16 進数文字のエンジン ID (最小で 10 文字、最大で 24 文字を使用できます)。 |
| | default | デフォルトのエンジン ID をリストアします。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン SNMP エンジン ID は、管理用にデバイスを識別するために使用する一意の文字列です。デフォルトの文字列はシスコの番号とデバイスの最初のインターフェイスの MAC アドレスを使用して自動的に生成されるため、デバイスのエンジン ID を指定する必要があります。

エンジン ID を変更する場合、変更を有効にするにリブートする必要があります。

注意 SNMP エンジン ID の値を変更すると、コマンドラインに入力されたユーザのパスワードが MD5 (Message Digest アルゴリズム 5) または SHA (セキュア ハッシュ アルゴリズム) セキュリティ ダイジェストに変換されます。このダイジェストはパスワードとローカル エンジン ID の両方に基づいています。コマンドラインのパスワードは削除されます。このため、エンジン ID のローカル値を変更した場合は、SNMP ユーザのセキュリティ ダイジェストが無効となり、ユーザを再設定しなければなりません。

次に、値 ffffffff を使用して SNMP エンジン ID を設定する例を示します。

```
(Cisco Controller) > config snmp engineID ffffffff
```

関連コマンド **show snmpengineID**

config snmp syscontact

SNMP システム接点名を設定するには、**config snmp syscontact** コマンドを使用します。

config snmp syscontact *contact*

| | | |
|------------|----------------|---------------------------------------|
| 構文の説明 | <i>contact</i> | SNMP システム接点名。有効な値は、最大255文字の出力可能な文字です。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース7.6以前のリリースで導入されました。 |

次に、SNMP システム接点を Cisco WLAN Solution_administrator という名前に設定する例を示します。

```
(Cisco Controller) > config snmp syscontact Cisco WLAN Solution_administrator
```

config snmp syslocation

SNMP システムのロケーション名を設定するには、**config snmp syslocation** コマンドを使用します。

config snmp syslocation *location*

| | | |
|-------|-----------------|--|
| 構文の説明 | <i>location</i> | SNMP システムのロケーション名。有効な値は、最大 255 文字の出力可能な文字です。 |
|-------|-----------------|--|

| | |
|------------|----|
| コマンド デフォルト | なし |
|------------|----|

| | |
|--------|----------------|
| コマンド履歴 | リリース 変更内容 ス |
|--------|----------------|

| | |
|-----|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |
|-----|-----------------------------------|

次に、SNMP システム ロケーション名を **Building_2a** に設定する例を示します。

```
(Cisco Controller) > config snmp syslocation Building_2a
```

config snmp trapreceiver create

サーバで SNMP トラップを受信するように設定するには、**config snmp trapreceiver create** コマンドを使用します。

config snmp trapreceiver create *name IP addr*

| | | |
|-------|----------------|---|
| 構文の説明 | <i>name</i> | SNMP コミュニティ名。名前には、最大で 31 文字まで使用できます。 |
| | <i>ip-addr</i> | SNMP トラップを送信する場所の IPv4 または IPv6 アドレスを設定します。 |

コマンドデフォルト なし

コマンド履歴

リリース 変更内容

7.6 このコマンドは、リリース 7.6 以前のリリースで導入されました。

8.0 このコマンドは、IPv4 と IPv6 の両方のアドレス形式をサポートします。

使用上のガイドライン このコマンドを実行して新しいサーバを追加するには、IPv4 または IPv6 アドレスが有効になっている必要があります。

次に、名前が `test` で IP アドレスが `10.1.1.1` の SNMP トラップ レシーバを持つ、新しい SNMP トラップ レシーバを追加する例を示します。

```
(Cisco Controller) > config snmp trapreceiver create test 10.1.1.1
```

次に、名前が `test` で IP アドレスが `2001:10:1:1::1` の SNMP トラップ レシーバを持つ、新しい SNMP トラップ レシーバを追加する例を示します。

```
(Cisco Controller) > config snmp trapreceiver create test 2001:10:1:1::1
```

config snmp trapreceiver delete

トラップレシーバリストからサーバを削除するには、**config snmp trapreceiver delete** コマンドを使用します。

config snmp trapreceiver delete *name*

| | | |
|-------|-------------|----------------------------------|
| 構文の説明 | <i>name</i> | SNMP コミュニティ名。名前は最大 16 文字で指定できます。 |
|-------|-------------|----------------------------------|

| | |
|------------|----|
| コマンド デフォルト | なし |
|------------|----|

| | |
|--------|-----------|
| コマンド履歴 | リリース 変更内容 |
|--------|-----------|

| | |
|-----|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |
|-----|-----------------------------------|

次に、**test** という名前のサーバを SNMP トラップレシーバリストから削除する例を示します。

```
(Cisco Controller) > config snmp trapreceiver delete test
```

| | |
|--------|-----------------------|
| 関連コマンド | show snmp trap |
|--------|-----------------------|

config snmp trapreceiver mode

選択したサーバへのトラップの送信を有効または無効にするには、**config snmp trapreceiver mode** コマンドを使用します。

config snmp trapreceiver mode {enable | disable} *name*

| | | |
|-------|----------------|----------------------------|
| 構文の説明 | enable | SNMP トラップをイネーブルにします。 |
| | disable | SNMP トラップ レシーバをディセーブルにします。 |
| | <i>name</i> | SNMP コミュニティ名。 |

コマンド デフォルト なし

コマンド履歴

リリース 変更内容
ス

7.6 このコマンドは、リリース 7.6 以前のリリースで導入されました。

使用上のガイドライン

このコマンドを使用して、Cisco ワイヤレス LAN コントローラから選択したサーバへのトラップの送信をイネーブルまたはディセーブルにできます。

次に、SNMP トラップ レシーバが、server1 という名前のサーバにトラップを送信しないようにする例を示します。

```
(Cisco Controller) > config snmp trapreceiver mode disable server1
```

関連コマンド

show snmp trap

config snmp v3user create

バージョン 3 の SNMP ユーザを作成するには、**config snmp v3user create** コマンドを使用します。

```
config snmp v3user create username {ro | rw} {none | hmacmd5 | hmacsha} {none | des | aescfb128} [auth_key] [encrypt_key]
```

| 構文の説明 | | |
|-------|--------------------|---|
| | <i>username</i> | バージョン 3 の SNMP ユーザ名。 |
| | ro | 読み取り専用ユーザ権限を指定します。 |
| | rw | 読み取り/書き込みユーザ権限を指定します。 |
| | none | 認証が必要ない場合に指定します。 |
| | hmacmd5 | 認証に Hashed Message Authentication コーディングのメッセージダイジェスト 5 (HMAC-MD5) を指定します。 |
| | hmacsha | 認証に Hashed Message Authentication コーディングのセキュア ハッシュ アルゴリズム (HMAC-SHA) を指定します。 |
| | none | 暗号化が必要ない場合に指定します。 |
| | des | Cipher Block Chaining-Digital Encryption Standard (CBC-DES) 暗号化を使用するように指定します。 |
| | aescfb128 | Cipher Feedback Mode-Advanced Encryption Standard-128 (CFB-AES-128) 暗号化を使用するように指定します。 |
| | <i>auth_key</i> | (任意) HMAC-MD5 または HMAC-SHA 認証プロトコルの認証キー。 |
| | <i>encrypt_key</i> | (任意) CBC-DES または CFB-AES-128 暗号プロトコルの暗号キー。 |

コマンド デフォルト SNMP v3 username AccessMode Authentication Encryption

```
-----
default          Read/Write      HMAC-SHA       CFB-AES
```

コマンド履歴

| リリース | 変更内容 |
|------|------|
|------|------|

| | |
|-----|---------------------------------|
| 7.6 | このコマンドは、リリース7.6以前のリリースで導入されました。 |
|-----|---------------------------------|

次に、読み取り専用権限を設定し、暗号化または認証を設定せずに、test という名前の SNMP ユーザ名を追加する例を示します。

```
(Cisco Controller) > config snmp v3user create test ro none none
```

関連コマンド**show snmpv3user**

config snmp v3user delete

バージョン 3 の SNMP ユーザを削除するには、**config snmp v3user delete** コマンドを使用します。

config snmp v3user delete *username*

構文の説明

username 削除するユーザ名。

コマンド デフォルト

なし

コマンド履歴

リリース 変更内容
ス

7.6 このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、**test** という名前の SNMP ユーザを削除する例を示します。

```
(Cisco Controller) > config snmp v3user delete test
```

関連コマンド

show snmp v3user

config snmp version

選択した SNMP バージョンを有効または無効にするには、**config snmp version** コマンドを使用します。

config snmp version {v1 | v2 | v3} {enable | disable}

| 構文の説明 | | |
|-------|---------|------------------------------|
| | v1 | 有効または無効にする SNMP バージョンを指定します。 |
| | v2 | 有効または無効にする SNMP バージョンを指定します。 |
| | v3 | 有効または無効にする SNMP バージョンを指定します。 |
| | enable | 指定されたバージョンをイネーブルにします。 |
| | disable | 指定されたバージョンをディセーブルにします。 |

コマンドデフォルト デフォルトでは、すべての SNMP バージョンはイネーブルになっています。

コマンド履歴

| リリース | 変更内容 |
|------|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、SNMP バージョン 1 をイネーブルにする例を示します。

```
(Cisco Controller) > config snmp version v1 enable
```

関連コマンド **show snmpversion**

config tacacs acct

TACACS+ アカウンティング サーバを設定するには、**config tacacs acct** コマンドを使用します。

config tacacs acct {**add** 1-3 *IP addr port ascii/hex secret* | **delete** 1-3 | **disable** 1-3 | **enable** 1-3 | **server-timeout** 1-3 *seconds*}

| 構文の説明 | | |
|------------|-----------------------|--|
| | add | 新しい TACACS+ アカウンティング サーバを追加します。 |
| | 1 ~ 3 | TACACS+ アカウンティング サーバインデックスを 1 から 3 に指定します。 |
| | <i>ip-addr</i> | TACACS+ アカウンティング サーバの IPv4 または IPv6 アドレスを指定します。 |
| | <i>port</i> | TACACS+ サーバの TCP ポートを指定します。 |
| | <i>ascii/hex</i> | 使用する TACACS+ サーバの秘密キーのタイプを指定します (ASCII または HEX)。 |
| | <i>secret</i> | 秘密キーを ASCII 文字または 16 進数文字で指定します。 |
| | delete | TACACS+ サーバを削除します。 |
| | disable | TACACS+ サーバを無効にします。 |
| | enable | TACACS+ サーバを有効にします。 |
| | server-timeout | TACACS+ サーバのデフォルト サーバ タイムアウトを変更します。 |
| | <i>seconds</i> | TACACS+ サーバがタイムアウトするまでの秒数を指定します。サーバ タイムアウトの範囲は 5 ~ 30 秒です。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |
| | 8.0 | このコマンドは、IPv4 と IPv6 の両方のアドレス形式をサポートします。 |

次に、IPv4 アドレス 10.0.0.0、ポート番号 49、および ASCII の秘密キー 12345678 の新しい TACACS+ アカウンティング サーバインデックス 1 を追加する例を示します。

```
(Cisco Controller) > config tacacs acct add 1 10.0.0.0 10 ascii 12345678
```

次に、IPv6 アドレス 2001:9:6:40::623、ポート番号 49、および ASCII の秘密キー 12345678 の新しい TACACS+ アカウンティング サーバインデックス 1 を追加する例を示します。

```
(Cisco Controller) > config tacacs acct add 1 2001:9:6:40::623 10 ascii 12345678
```

次に、TACACS+ アカウンティング サーバのサーバタイムアウトを5秒間に設定する例を示します。

```
(Cisco Controller) > config tacacs acct server-timeout 1 5
```

config tacacs auth

TACACS+ 認証サーバを設定するには、**config tacacs auth** コマンドを使用します。

```
config tacacs auth { add 1-3 IP addr port ascii/hex secret | delete 1-3 | disable 1-3 | enable
1-3 | mgmt-server-timeout 1-3 seconds | server-timeout 1-3seconds }
```

| 構文の説明 | | |
|---|------|---|
| add | | 新しい TACACS+ アカウンティング サーバを追加します。 |
| <i>1 ~ 3</i> | | 1 から 3 までの TACACS+ アカウンティング サーバインデックス。 |
| <i>ip-addr</i> | | TACACS+ アカウンティング サーバの IP アドレス。 |
| <i>port</i> | | TACACS+ アカウンティング サーバに使用するコントローラ ポート。 |
| <i>ascii/hex</i> | | 使用する秘密キーのタイプ (ASCII または HEX)。 |
| <i>secret</i> | | ASCII または HEX の文字による秘密キー。 |
| delete | | TACACS+ サーバを削除します。 |
| disable | | TACACS+ サーバを無効にします。 |
| enable | | TACACS+ サーバを有効にします。 |
| mgmt-server-timeout <i>1-3 seconds</i> | | サーバのデフォルトの管理ログインサーバタイムアウトを変更します。サーバがタイムアウトするまでの秒数は 1 ~ 30 秒です。 |
| server-timeout <i>1-3 seconds</i> | | サーバのデフォルトのネットワーク ログインサーバタイムアウトを変更します。サーバがタイムアウトするまでの秒数は 5 ~ 30 秒です。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |
| | 8.0 | このコマンドは、IPv4 と IPv6 の両方のアドレス形式をサポートします。 |

次に、IPv4 アドレス 10.0.0.3、ポート番号 49、および ASCII の秘密キー 12345678 の新しい TACACS+ 認証サーバ インデックス 1 を追加する例を示します。

```
(Cisco Controller) > config tacacs auth add 1 10.0.0.3 49 ascii 12345678
```

次に、IPv6 アドレス 2001:9:6:40::623、ポート番号 49、および ASCII の秘密キー 12345678 の新しい TACACS+ 認証サーバ インデックス 1 を追加する例を示します。

```
(Cisco Controller) > config tacacs auth add 1 2001:9:6:40::623 49 ascii 12345678
```

次に、TACACS+ 認証サーバのサーバ タイムアウトを設定する例を示します。

```
(Cisco Controller) > config tacacs auth server-timeout 1 5
```

config tacacs auth mgmt-server-timeout

管理ユーザのデフォルト TACACS+ 認証サーバのタイムアウトを設定するには、**config tacacs auth mgmt-server-timeout** コマンドを使用します。

config tacacs auth mgmt-server-timeout *index timeout*

| | | |
|------------|----------------|-----------------------------------|
| 構文の説明 | <i>index</i> | TACACS+ 認証サーバインデックス。 |
| | <i>timeout</i> | タイムアウト値。指定できる範囲は 1 ~ 30 秒です。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、管理ユーザのデフォルト TACACS+ 認証サーバのタイムアウトを設定する例を示します。

```
(Cisco Controller) > config tacacs auth mgmt-server-timeout 1 10
```

関連コマンド **config tacacs auth**

config tacacs dns

DNS サーバから TACACS IP 情報を取得するには、**config radius dns** コマンドを使用します。

```
config radius dns {global port {ascii | hex} secret | query url timeout | serverip ip_address
| disable | enable}
```

構文の説明

| | |
|-------------------|---|
| global | グローバル ポートおよび DNS サーバから TACACS IP 情報を取得する秘密キーを設定します。 |
| port | 認証用のポート番号。有効な範囲は 1 ~ 65535 です。すべての DNS サーバは同じ認証ポートを使用する必要があります。 |
| ascii | ASCII に設定する必要がある共有秘密キーの形式。 |
| hex | 16 進数に設定する必要がある共有秘密キーの形式。 |
| secret | TACACS サーバのログイン秘密。 |
| query | TACACS サーバと DNS タイムアウトの完全修飾ドメイン名 (FQDN) を設定します。 |
| url | TACACS サーバの FQDN。FQDN は最大 63 文字の英数字 (大文字と小文字を区別) で指定できます。 |
| timeout | Cisco Wireless LAN Controller (WLC) がリクエストのタイムアウトを設定して再送信するまでの最大待機日数。指定できる範囲は 1 ~ 180 です。 |
| serverip | DNS サーバの IP アドレスを設定します。 |
| ip_address | DNS サーバの IP アドレス。 |
| disable | TACACS DNS 機能を無効にします。デフォルトではディセーブルになっています。 |
| enable | Cisco WLC が DNS サーバから TACACS IP 情報を取得できるようにします。 |

コマンド デフォルト

DNS サーバから TACACS IP 情報を取得することはできません。

コマンド履歴

| リリース | 変更内容 |
|------|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン

アカウントリングポートは認証ポートから取得されます。すべての DNS サーバは同じ秘密キーを使用する必要があります。DNS クエリを有効にすると、スタティック設定は上書きされます。DNS リストはスタティック AAA リストよりも優先されます。

次に、Cisco WLC で TACACS DNS 機能を有効にする例を示します。

```
(Cisco Controller) > config tacacs dns enable
```

config tacacs fallback-test interval

TACACS+プローブ間隔を設定するには、**config tacacs fallback-test interval** コマンドを使用します。

config tacacs fallback-test interval { *seconds* }

| | | |
|-----------|----------------|--|
| 構文の説明 | <i>seconds</i> | TACACS+プローブ間隔（秒単位）。無効は0で、範囲は180～3600秒です。 |
| コマンドデフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 8.2 | このコマンドは本リリースで追加されました。 |

次に、TACACS+プローブ間隔を設定する例を示します。

```
(Cisco Controller) > config tacacs fallback-test interval 200
```

config time manual

システムの時刻を設定するには、**config time manual** コマンドを使用します。

config time manual *MM |DD | YY HH:MM:SS*

構文の説明

MM/DD/YY

日付。

*HH:MM:SS*時刻。

コマンドデフォルト

なし

コマンド履歴

リリース 変更内容
ス

7.6 このコマンドは、リリース7.6以前のリリースで導入されました。

次に、システムの日付を 04/04/2010 に設定し、システムの時刻を 15:29:00 に設定する例を示します。

```
(Cisco Controller) > config time manual 04/04/2010 15:29:00
```

関連コマンド**show time**

config time ntp

ネットワーク タイム プロトコル (NTP) を設定するには、**config time ntp** コマンドを使用します。

```
config time ntp {auth {enable server-index key-index | disable server-index} | interval interval
| key-auth {add key-index md5 {ascii | hex} key} | delete key-index} | pollinterval maxpoll
minpollserver-index | server index IP Address}
```

構文の説明

| | |
|--------------------------|---|
| auth | NTP 認証を設定します。 |
| enable | NTP 認証をイネーブルにします。 |
| <i>server-index</i> | NTP サーバインデックス。 |
| <i>key-index</i> | 1 ~ 4294967295 のキーインデックス。 |
| disable | NTP 認証をディセーブルにします。 |
| interval | NTP バージョン 3 のポーリング間隔を設定します。 |
| <i>interval</i> | NTP ポーリング間隔 (秒)。有効範囲は 3600 ~ 604800 秒です。 |
| key-auth | NTP 認証キーを設定します。 |
| add | NTP 認証キーを追加します。 |
| md5 | 認証プロトコルを指定します。 |
| ascii | ASCII キータイプを指定します。 |
| hex | 16 進数キータイプを指定します。 |
| <i>key</i> | 最大 16 文字の ASCII キー形式または最大 32 桁の 16 進キー形式を指定します。 |
| delete | NTP サーバを削除します。 |
| pollinterval | ネットワーク タイム プロトコルバージョン 4 のポーリング間隔を設定します。 |
| <i>maxpoll minpoll</i> | 最大および最小の NTP ポーリング間隔を (2 の累乗) 秒で入力します。 |
| <i>server-index</i> | NTP サーバインデックス番号を入力します。 |
| server | NTP サーバを設定します。 |

| | | |
|------------|-------------------|--|
| | <i>IP Address</i> | NTP サーバの IP アドレス。エントリを削除するには 0.0.0.0 または :: を使用します。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |
| | 8.0 | このコマンドは、IPv4 と IPv6 の両方のアドレス形式をサポートします。 |
| | 8.6 | このコマンドは、本リリースで強化されました。追加された新しいキーワードは、 <code>pollinterval</code> 、 <code>maxpoll</code> 、 <code>minpoll</code> です。 |
| | 8.6 | NTP サーバ削除オプションは、 <code>config time ntp delete server-index</code> で使用できます。 |
| 使用上のガイドライン | | <ul style="list-style-type: none"> • コントローラに NTP サーバを追加するには、<code>config time ntp server index IP Address</code> コマンドを使用します。 • コントローラ上で設定されている NTP サーバを表示するには、<code>show time</code> コマンドを使用します。 |

次に、NTP のポーリング間隔を 7000 秒に設定する例を示します。

```
(Cisco Controller) > config time ntp interval 7000
```

次に、サーバインデックスが 4 で、キーインデックスが 1 である NTP 認証をイネーブルにする例を示します。

```
(Cisco Controller) > config time ntp auth enable 4 1
```

次に、キー形式が 16 進数文字で、キーインデックスが 1 である、値が ff の NTP 認証キーを追加する例を示します。

```
(Cisco Controller) > config time ntp key-auth add 1 md5 hex ff
```

次に、キー形式が ASCII 文字で、キーインデックスが 1 である、値が ff の NTP 認証キーを追加する例を示します。

```
(Cisco Controller) > config time ntp key-auth add 1 md5 ascii ciscokey
```

次に、NTP サーバを追加し、コントローラに設定されているサーバを表示する例を示します。

```
(Cisco Controller) > config time ntp server 1 10.92.125.52
(Cisco Controller) > config time ntp server 2 2001:9:6:40::623
```



```
(Cisco Controller) > show time
Time..... Fri May 23 12:04:18 2014

Timezone delta..... 0:0
Timezone location..... (GMT +5:30) Colombo, New Delhi, Chennai,
  Kolkata

NTP Servers
NTP Polling Interval..... 3600

Index NTP Key Index  NTP Server NTP      Msg Auth Status
-----
1          1      10.92.125.52  AUTH SUCCESS
2          1      2001:9:6:40::623  AUTH SUCCESS
```

次に、NTP サーバを削除する例を示します。

```
(Cisco Controller) > config time ntp delete 1
```

config time ntp version

Cisco WLC のネットワーク タイム プロトコル (NTP) バージョンを設定するには、**config time ntp version** コマンドを使用します。



(注) NTP プロトコルバージョンの変更中に、既存のサーバおよび Cisco WLC のキーは削除されま
す。

config time ntp version *version-number*

構文の説明

version-number

Cisco WLC を実行する NTP バージョン 3 また
は 4 を入力します。

コマンド デフォルト

なし

コマンド履歴

リリース

変更内容

8.6

このコマンドが導入されました。

次に、Cisco WLC で NTP バージョン 4 を設定する方法を示します。

```
(Cisco Controller) > config time ntp version 4
```

config time timezone

システムのタイムゾーンを設定するには、**config time timezone** コマンドを使用します。

config time timezone {**enable** | **disable**} *delta_hours delta_mins*

| | | |
|-------|--------------------|---|
| 構文の説明 | enable | 夏時間をイネーブルにします。 |
| | disable | 夏時間をディセーブルにします。 |
| | <i>delta_hours</i> | Universal Coordinated Time (UCT) からのローカル時間の差。 |
| | <i>delta_mins</i> | UCT からのローカル分の差。 |

コマンドデフォルト なし

コマンド履歴

リリース 変更内容
ス

7.6 このコマンドは、リリース7.6以前のリリースで導入されました。

次に、夏時間をイネーブルにする例を示します。

```
(Cisco Controller) > config time timezone enable 2 0
```

関連コマンド

show time

config time timezone location

適切な時期が来たら自動的に夏時間が設定されるようにタイムゾーンの場所を設定するには、**config time timezone location** コマンドを使用します。

config time timezone location *location_index*

構文の説明

location_index

必要な時間帯を表す番号。時間帯は次のとおりです。

- (GMT-12:00) 日付変更線、西側
- (GMT-11:00) サモア
- (GMT-10:00) ハワイ
- (GMT-9:00) アラスカ
- (GMT-8:00) 太平洋標準時 (米国およびカナダ)
- (GMT-7:00) 山岳部標準時 (米国およびカナダ)
- (GMT-6:00) 中央標準時 (米国およびカナダ)
- (GMT-5:00) 東部標準時 (米国およびカナダ)
- (GMT-4:00) 大西洋標準時 (カナダ)
- (GMT-3:00) ブエノスアイレス (アルゼンチン)
- (GMT-2:00) 中部大西洋
- (GMT-1:00) アゾレス諸島
- (GMT) ロンドン、リスボン、ダブリン、エディンバラ (デフォルト値)
- (GMT+1:00) アムステルダム、ベルリン、ローマ、ウィーン
- (GMT+2:00) エルサレム
- (GMT+3:00) バグダッド
- (GMT+4:00) マスカット、アブダビ
- (GMT+4:30) カブール
- (GMT+5:00) カラチ、イスラマバード、タシュケント
- (GMT+5:30) コロンボ、コルカタ、ムンバイ、ニューデリー
- (GMT+5:45) カトマンズ
- (GMT+6:00) アルマトイ、ノボシビルス

ク

- (GMT+6:30) ラングーン
- (GMT+7:00) サイゴン、ハノイ、バンコク、ジャカルタ
- (GMT+8:00) 香港、北京、重慶
- (GMT+9:00) 東京、大阪、札幌
- (GMT+9:30) ダーウィン
- (GMT+10:00) シドニー、メルボルン、キャンベラ
- (GMT+11:00) マガダン、ソロモン諸島、ニューカレドニア
- (GMT+12:00) カムチャツカ、マーシャル諸島、フィジー
- (GMT+12:00) オークランド (ニュージーランド)

コマンドデフォルト

なし

コマンド履歴

リリース 変更内容
ス

7.6 このコマンドは、リリース7.6以前のリリースで導入されました。

次に、夏時間が場所インデックス10に自動的に設定されるようにタイムゾーンの場所を設定する例を示します。

```
(Cisco Controller) > config time timezone location 10
```

関連コマンド

show time

config trapflags 802.11-Security

802.11 セキュリティ関連トラップの送信を有効または無効にするには、**config trapflags 802.11-Security** コマンドを使用します。

config trapflags 802.11-Security wepDecryptError {enable | disable}

| 構文の説明 | enable | 802.11 セキュリティ関連トラップの送信をイネーブルにします。 |
|-------|---------|------------------------------------|
| | disable | 802.11 セキュリティ関連トラップの送信をディセーブルにします。 |

コマンド デフォルト デフォルトでは、802.11 セキュリティ関連トラップの送信はイネーブルです。

コマンド履歴 リリース 変更内容
ス

7.6 このコマンドは、リリース7.6以前のリリースで導入されました。

次に、802.11 セキュリティ関連トラップをディセーブルにする例を示します。

```
(Cisco Controller) > config trapflags 802.11-Security wepDecryptError disable
```

関連コマンド show trapflags

config trapflags aaa

AAA サーバ関連トラップの送信をイネーブルまたはディセーブルにするには、**config trapflags aaa** コマンドを使用します。

```
config trapflags aaa {auth | servers} {enable | disable}
```

構文の説明

| | |
|----------------|---|
| auth | 管理ユーザ、ネットユーザ、またはMACフィルタにAAA認証エラーが発生した場合に、トラップの送信をイネーブルにします。 |
| servers | RADIUS サーバが応答していない場合に、トラップの送信をイネーブルにします。 |
| enable | AAA サーバ関連トラップの送信をイネーブルにします。 |
| disable | AAA サーバ関連トラップの送信をディセーブルにします。 |

コマンド デフォルト

デフォルトでは、AAA サーバ関連トラップの送信はイネーブルです。

コマンド履歴

| リリース | 変更内容 |
|------|---------------------------------|
| 7.6 | このコマンドは、リリース7.6以前のリリースで導入されました。 |

次に、AAA サーバ関連トラップの送信をイネーブルにする例を示します。

```
(Cisco Controller) > config trapflags aaa auth enable
```

関連コマンド

show watchlist

config trapflags adjchannel-rogueap

隣接チャンネルで不正なアクセスポイントが検出された場合に、トラップ通知を設定するには、**config trapflags adjchannel-rogueap** コマンドを使用します。

config trapflags adjchannel-rogueap {enable | disable}

構文の説明

enable 隣接チャンネルで不正なアクセスポイントが検出された場合に、トラップ通知をイネーブルにします。

disable 隣接チャンネルで不正なアクセスポイントが検出された場合に、トラップ通知をディセーブルにします。

コマンド デフォルト

なし

コマンド履歴

リリース 変更内容
ス

7.6 このコマンドは、リリース7.6以前のリリースで導入されました。

次に、隣接チャンネルで不正なアクセスポイントが検出された場合に、トラップ通知をイネーブルにする例を示します。

```
(Cisco Controller) > config trapflags adjchannel-rogueap enable
```

関連コマンド

config trapflags 802.11-Security
config trapflags aaa
config trapflags ap
config trapflags authentication
config trapflags client
config trapflags configsave
config trapflags IPsec
config trapflags linkmode
config trapflags multiusers
config trapflags mesh
config trapflags strong-pwdcheck
config trapflags rfid
config trapflags rogueap
show trapflags

config trapflags ap

Cisco Lightweight アクセス ポイント関連トラップの送信をイネーブルまたはディセーブルにするには、**config trapflags ap** コマンドを使用します。

config trapflags ap {register | interfaceUp} {enable | disable}

構文の説明

| | |
|--------------------|---|
| register | Cisco Lightweight アクセス ポイントが Cisco スイッチに登録する場合に、トラップの送信をイネーブルにします。 |
| interfaceUp | Cisco Lightweight アクセス ポイント インターフェイス (A または B) が表示された場合に、トラップの送信をイネーブルにします。 |
| enable | アクセス ポイント関連トラップの送信をイネーブルにします。 |
| disable | アクセス ポイント関連トラップの送信をディセーブルにします。 |

コマンド デフォルト

デフォルトでは、Cisco Lightweight アクセス ポイント関連トラップの送信はイネーブルです。

コマンド履歴

リリース 変更内容
ス

7.6 このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、トラップで、アクセス ポイント関連トラップの送信が行われなくにする例を示します。

```
(Cisco Controller) > config trapflags ap register disable
```

関連コマンド

show trapflags

config trapflags authentication

無効な SNMP アクセス権を持つトラップ送信をイネーブまたはディセーブするには、**config trapflags authentication** コマンドを使用します。

config trapflags authentication {enable | disable}

| | | |
|-------|----------------|-------------------------------------|
| 構文の説明 | enable | 無効な SNMP アクセス権を持つトラップの送信をイネーブにします。 |
| | disable | 無効な SNMP アクセス権を持つトラップの送信をディセーブにします。 |

コマンド デフォルト デフォルトでは、無効な SNMP アクセス権を持つトラップの送信はイネーブです。

コマンド履歴 リリース 変更内容
ス

7.6 このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、無効な SNMP アクセス権で、トラップの送信を行えないようにする例を示します。

```
(Cisco Controller) > config trapflags authentication disable
```

関連コマンド **show trapflags**

config trapflags client

クライアント関連DOT11トラップの送信をイネーブルまたはディセーブルにするには、**config trapflags client** コマンドを使用します。

config trapflags client {**802.11-associate** **802.11-disassociate** | **802.11-deauthenticate** | **802.11-authfail** | **802.11-assocfail** | **authentication** | **excluded**} {**enable** | **disable**}

| 構文の説明 | | |
|-------|------------------------------|--|
| | 802.11-associate | クライアントへの Dot11 アソシエーショントラップの送信をイネーブルにします。 |
| | 802.11-disassociate | クライアントへの Dot11 ディスアソシエーショントラップの送信をイネーブルにします。 |
| | 802.11-deauthenticate | クライアントへの Dot11 認証解除トラップの送信をイネーブルにします。 |
| | 802.11-authfail | クライアントへの Dot11 認証エラートラップの送信をイネーブルにします。 |
| | 802.11-assocfail | クライアントへの Dot11 アソシエーションエラートラップの送信をイネーブルにします。 |
| | authentication | クライアントへの認証成功トラップの送信をイネーブルにします。 |
| | excluded | 除外したトラップのクライアントへの送信をイネーブルにします。 |
| | enable | クライアント関連DOT11トラップの送信をイネーブルにします。 |
| | disable | クライアント関連 DOT11 トラップの送信をディセーブルにします。 |

コマンドデフォルト デフォルトでは、クライアント関連 DOT11 トラップの送信はディセーブルです。

コマンド履歴

リリー 変更内容
ス

7.6 このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、クライアントへの Dot11 アソシエーション解除トラップの送信をイネーブルにする例を示します。

```
(Cisco Controller) > config trapflags client 802.11-disassociate enable
```

関連コマンド

show trapflags

config trapflags client max-warning-threshold

コントローラに関連付けるクライアントの数のしきい値を設定し、その後、SNMPトラップとsyslogメッセージがコントローラに送信されるようにするには、**config trapflags client max-warning-threshold** コマンドを使用します。

config trapflags client max-warning-threshold {**threshold** | **enable** | **disable**}

構文の説明

threshold コントローラに関連付けるクライアントの数のしきい値パーセントを設定し、その後、SNMPトラップとsyslogメッセージがコントローラに送信されます。範囲は80～100です。

2つの警告の間の最小間隔は10分間です。この間隔を設定することはできません。

enable トラップとsyslogメッセージの生成をイネーブルにします。

disable トラップとsyslogメッセージの生成をディセーブルにします。

コマンドデフォルト

コントローラに関連付けられているクライアント数のデフォルトのしきい値は90%です。

コマンド履歴

リリース 変更内容
ス

7.6 このコマンドは、リリース7.6以前のリリースで導入されました。

使用上のガイドライン

このテーブルは、異なるコントローラのクライアントの最大数を示します。

表 3:異なるコントローラでサポートされているクライアントの最大数

| コントローラ | サポートされているクライアントの最大数 |
|---------------------------------------|---------------------|
| Cisco 5500 シリーズ コントローラ | 7000 |
| Cisco 2500 シリーズ コントローラ | 500 |
| Cisco ワイヤレス サービス モジュール 2 | 15000 |
| Cisco Flex 7500 シリーズ コントローラ | 64000 |
| Cisco 8500 シリーズ コントローラ | 64000 |
| Cisco Virtual Wireless LAN Controller | 30000 |

次に、コントローラに関連付けられているクライアント数のしきい値を設定する例を示します。

```
(Cisco Controller) > config trapflags client max-warning-threshold 80
```

関連コマンド**show trapflags****config trapflags client**

config trapflags configsave

設定保存トラップの送信をイネーブルまたはディセーブルにするには、**config trapflags configsave** コマンドを使用します。

config trapflags configsave {enable | disable}

| | | |
|-------|----------------|-------------------------|
| 構文の説明 | enable | 設定保存トラップの送信をイネーブルにします。 |
| | disable | 設定保存トラップの送信をディセーブルにします。 |

コマンドデフォルト デフォルトでは、設定保存トラップの送信はイネーブルです。

| | | |
|--------|------|---------------------------------|
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース7.6以前のリリースで導入されました。 |

次に、設定保存トラップの送信をイネーブルにする例を示します。

```
(Cisco Controller) > config trapflags configsave enable
```

関連コマンド **show trapflags**

config trapflags IPsec

IPSec トラップの送信を有効または無効にするには、**config trapflags IPsec** コマンドを使用します。

```
config trapflags IPsec { esp-auth | esp-reply | invalidSPI | ike-neg | suite-neg |
invalid-cookie } { enable | disable }
```

| 構文の説明 | | |
|-------|-----------------------|--|
| | esp-auth | ESP 認証エラーが発生したときに、IPSec トラップを送信できるようにします。 |
| | esp-reply | ESP 再送エラーが発生したときに、IPSec トラップの送信をイネーブルにします。 |
| | invalidSPI | ESP で無効な SPI が検出されたときに、IPSec トラップの送信をイネーブルにします。 |
| | ike-neg | IKE ネゴシエーション エラーが発生したときに、IPSec トラップの送信をイネーブルにします。 |
| | suite-neg | スイートネゴシエーションエラーが発生したときに、IPSec トラップの送信をイネーブルにします。 |
| | invalid-cookie | Isakamp で無効なクッキーが検出されたときに、IPSec トラップの送信をイネーブルにします。 |
| | enable | IPSec トラップの送信をイネーブルにします。 |
| | disable | IPSec トラップの送信をディセーブルにします。 |

コマンド デフォルト デフォルトでは、IPSec トラップの送信はイネーブルです。

| コマンド履歴 | リリース | 変更内容 |
|--------|------|-----------------------------------|
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、ESP 認証エラーが発生したときに、IPSec トラップの送信をイネーブルにする例を示します。

```
(Cisco Controller) > config trapflags IPsec esp-auth enable
```

関連コマンド

show trapflags

config trapflags linkmode

Cisco ワイヤレス LAN コントローラのレベルリンクのアップ/ダウントラップフラグをイネーブルまたはディセーブルにするには、**config trapflags linkmode** コマンドを使用します。

config trapflags linkmode {enable | disable}

構文の説明

enable

これにより、Cisco ワイヤレス LAN コントローラのレベルリンクのアップ/ダウントラップフラグをイネーブルにします。

disable

これにより、Cisco ワイヤレス LAN コントローラのレベルリンクのアップ/ダウントラップフラグをディセーブルにします。

コマンドデフォルト

デフォルトでは、Cisco WLC のレベルリンクのアップ/ダウントラップフラグはイネーブルです。

コマンド履歴

リリース 変更内容
ス

7.6 このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、Cisco ワイヤレス LAN コントローラのレベルリンクのアップ/ダウントラップをイネーブルにする例を示します。

```
(Cisco Controller) > config trapflags linkmode disable
```

関連コマンド

show trapflags

config trapflags mesh

メッシュアクセスポイントが検出された場合に、トラップ通知を設定するには、**config trapflags mesh** コマンドを使用します。

config trapflags mesh {enable | disable}

構文の説明

enable メッシュアクセスポイントが検出された場合に、トラップ通知をイネーブルにします。

disable メッシュアクセスポイントが検出された場合に、トラップ通知をディセーブルにします。

コマンドデフォルト

なし

コマンド履歴

リリース 変更内容

7.6 このコマンドは、リリース7.6以前のリリースで導入されました。

次に、メッシュアクセスポイントが検出された場合に、トラップ通知をイネーブルにする例を示します。

```
(Cisco Controller) > config trapflags mesh enable
```

関連コマンド

config trapflags 802.11-Security
config trapflags aaa
config trapflags ap
config trapflags adjchannel-rogueap
config trapflags authentication
config trapflags client
config trapflags configsave
config trapflags IPsec
config trapflags linkmode
config trapflags multiusers
config trapflags strong-pwdcheck
config trapflags rfid
config trapflags rogueap
show trapflags

config trapflags multiusers

複数ログインがアクティブな場合にトラップ送信をイネーブルまたはディセーブルにするには、**config trapflags multiusers** コマンドを使用します。

config trapflags multiusers {enable | disable}

| | | |
|-------|----------------|-------------------------------------|
| 構文の説明 | enable | 複数ログインがアクティブな場合に、トラップ送信をイネーブルにします。 |
| | disable | 複数ログインがアクティブな場合に、トラップ送信をディセーブルにします。 |

コマンド デフォルト デフォルトでは、複数ログインがアクティブな場合、トラップ送信はイネーブルです。

コマンド履歴 リリース 変更内容
ス

7.6 このコマンドは、リリース7.6以前のリリースで導入されました。

次に、複数ログインがアクティブな場合に、トラップ送信をディセーブルにする例を示します。

```
(Cisco Controller) > config trapflags multiusers disable
```

関連コマンド **show trapflags**

config trapflags rfid

電波による個体識別 (RFID) タグの最大数のしきい値を設定し、その後、SNMP トラップと syslog メッセージをコントローラに送信するには、**config trapflags rfid** コマンドを使用します。

config trapflags rfid {**threshold** | **enable** | **disable**}

構文の説明

| | |
|------------------|--|
| threshold | RFID タグの最大数のしきい値パーセントを設定し、その後、SNMP トラップと syslog メッセージがコントローラに送信されるようにします。範囲は 80 ~ 100 です。 トラップと syslog メッセージが 10 分ごとに生成されます。この間隔は設定できません。 |
| enable | トラップと syslog メッセージの生成をイネーブルにします。 |
| disable | トラップと syslog メッセージの生成をディセーブルにします。 |

コマンドデフォルト

RFID タグの最大数のデフォルトのしきい値は、90% です。

コマンド履歴

| | |
|------|-----------------------------------|
| リリース | 変更内容 |
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン

次の表に、異なるコントローラでサポートされる RFID タグの最大数を示します。

表 4: 異なるコントローラでサポートされる RFID タグの最大数

| コントローラ | サポートされているクライアントの最大数 |
|---------------------------------------|---------------------|
| Cisco 5500 シリーズ コントローラ | 5000 |
| Cisco 2500 シリーズ コントローラ | 500 |
| Cisco ワイヤレス サービス モジュール 2 | 10000 |
| Cisco Flex 7500 シリーズ コントローラ | 50000 |
| Cisco 8500 シリーズ コントローラ | 50000 |
| Cisco Virtual Wireless LAN Controller | 3000 |

次に、RFID タグの最大数のしきい値を設定する例を示します。

```
(Cisco Controller) > config trapflags rfid 80
```

関連コマンド

config trapflags 802.11-Security
config trapflags aaa
config trapflags ap
config trapflags adjchannel-rogueap
config trapflags authentication
config trapflags client
config trapflags configsave
config trapflags IPsec
config trapflags linkmode
config trapflags multiusers
config trapflags mesh
config trapflags strong-pwdcheck
config trapflags rogueap
config trapflags mesh
show trapflags

config trapflags rogueap

不正なアクセス ポイント検出トラップの送信をイネーブルまたはディセーブルにするには、**config trapflags rogueap** コマンドを使用します。

config trapflags rogueap {enable | disable}

| | | |
|-------|----------------|-----------------------------------|
| 構文の説明 | enable | 不正なアクセス ポイント検出トラップの送信をイネーブルにします。 |
| | disable | 不正なアクセス ポイント検出トラップの送信をディセーブルにします。 |

コマンドデフォルト デフォルトでは、不正なアクセス ポイント検出トラップの送信はイネーブルです。

コマンド履歴

リリース 変更内容
ス

7.6 このコマンドは、リリース7.6以前のリリースで導入されました。

次に、不正なアクセス ポイント検出トラップの送信をディセーブルにする例を示します。

```
(Cisco Controller) > config trapflags rogueap disable
```

関連コマンド

config rogue ap classify
config rogue ap friendly
config rogue ap rldp
config rogue ap ssid
config rogue ap timeout
config rogue ap valid-client
show rogue ap clients
show rogue ap detailed
show rogue ap summary
show rogue ap friendly summary
show rogue ap malicious summary
show rogue ap unclassified summary
show trapflags

config trapflags rrm-params

無線リソース管理 (RRM) パラメータ トラップの送信をイネーブルまたはディセーブルにするには、**config trapflags rrm-params** コマンドを使用します。

config trapflags rrm-params {tx-power | channel | antenna} {enable | disable}

構文の説明

| | |
|-----------------|---|
| tx-power | RF マネージャが Cisco Lightweight アクセス ポイント インターフェイスの tx パワー レベルを自動的に変更する場合に、トラップの送信をイネーブルにします。 |
| channel | RF マネージャが Cisco Lightweight アクセス ポイント インターフェイスのチャンネルを自動的に変更する場合に、トラップの送信をイネーブルにします。 |
| antenna | RF マネージャが Cisco Lightweight アクセス ポイント インターフェイスのアンテナを自動的に変更する場合に、トラップの送信をイネーブルにします。 |
| enable | RRM パラメータ関連トラップの送信をイネーブルにします。 |
| disable | RRM パラメータ関連トラップの送信をディセーブルにします。 |

コマンド デフォルト

デフォルトでは、RRM パラメータ トラップの送信はイネーブルです。

コマンド履歴

リリース 変更内容
ス

7.6 このコマンドは、リリース 7.6 以前のリリースで導入されました。

次に、RRM パラメータ関連トラップの送信をイネーブルにする例を示します。

```
(Cisco Controller) > config trapflags rrm-params tx-power enable
```

関連コマンド

show trapflags

config trapflags rrm-profile

無線リソース管理（RRM）プロファイル関連トラップの送信をイネーブルまたはディセーブルにするには、**config trapflags rrm-profile** コマンドを使用します。

config trapflags rrm-profile {load | noise | interference | coverage} {enable | disable}

| 構文の説明 | | |
|-------|---------------------|--|
| | load | RF マネージャによって管理されるロードプロファイルが失敗した場合に、トラップの送信をイネーブルにします。 |
| | noise | RF マネージャによって管理されるノイズプロファイルが失敗した場合に、トラップの送信をイネーブルにします。 |
| | interference | RF マネージャによって管理されるインターフェイスプロファイルが失敗した場合に、トラップの送信をイネーブルにします。 |
| | coverage | RF マネージャによって管理されるカバレッジプロファイルが失敗した場合に、トラップの送信をイネーブルにします。 |
| | enable | RRM プロファイル関連トラップの送信をイネーブルにします。 |
| | disable | RRM プロファイル関連トラップの送信をディセーブルにします。 |

コマンド デフォルト デフォルトでは、RRM プロファイル関連トラップの送信はイネーブルです。

コマンド履歴

| リリース | 変更内容 |
|------|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、RRM プロファイル関連トラップの送信をディセーブルにする例を示します。

```
(Cisco Controller) > config trapflags rrm-profile load disable
```

関連コマンド **show trapflags**

config trapflags stpmode

スパニングツリートラップの送信をイネーブルまたはディセーブルにするには、**config trapflags stpmode** コマンドを使用します。

config trapflags stpmode {enable | disable}

| 構文の説明 | enable | disable |
|-------|----------------------------|-----------------------------|
| | スパニングツリートラップの送信をイネーブルにします。 | スパニングツリートラップの送信をディセーブルにします。 |

コマンド デフォルト デフォルトでは、スパニングツリートラップの送信はイネーブルです。

コマンド履歴 リリース 変更内容
ス

7.6 このコマンドは、リリース7.6以前のリリースで導入されました。

次に、スパニングツリートラップの送信をディセーブルにする例を示します。

```
(Cisco Controller) > config trapflags stpmode disable
```

関連コマンド show trapflags

config trapflags strong-pwdcheck

強力なパスワードのチェック用のトラップ通知を設定するには、**config trapflags strong-pwdcheck** コマンドを使用します。

config trapflags strong-pwdcheck {enable | disable}

構文の説明

enable 強力なパスワードのチェック用のトラップ通知をイネーブルにします。

disable 強力なパスワードのチェック用のトラップ通知をディセーブルにします。

コマンドデフォルト

なし

コマンド履歴

リリース 変更内容
ス

7.6 このコマンドは、リリース7.6以前のリリースで導入されました。

次に、強力なパスワードチェック用のトラップ通知をイネーブルにする例を示します。

```
(Cisco Controller) > config trapflags strong-pwdcheck enable
```

関連コマンド

config trapflags 802.11-Security
config trapflags aaa
config trapflags ap
config trapflags adjchannel-rogueap
config trapflags authentication
config trapflags client
config trapflags configsave
config trapflags IPsec
config trapflags linkmode
config trapflags multiusers
config trapflags mesh
config trapflags rfid
config trapflags rogueap
show trapflags

config trapflags wps

Wireless Protection System (WPS) トラップの送信をイネーブルまたはディセーブルにするには、**config trapflags wps** コマンドを使用します。

config trapflags wps { **enable** | **disable** }

| 構文の説明 | enable | disable |
|-------|------------------------|-------------------------|
| | WPS トラップの送信をイネーブルにします。 | WPS トラップの送信をディセーブルにします。 |

コマンド デフォルト デフォルトでは、WPS トラップの送信はイネーブルです。

| コマンド履歴 | リリース | 変更内容 |
|--------|------|---------------------------------|
| | 7.6 | このコマンドは、リリース7.6以前のリリースで導入されました。 |

次に、WPS トラップの送信をディセーブルにする例を示します。

```
(Cisco Controller) > config trapflags wps disable
```

関連コマンド **show trapflags**

config tunnel eogre heart-beat

キーブアライブ ping 間隔を設定するには、**config tunnel eogre** コマンドを使用します。

```
config tunnel eogre heart-beat {interval | max-skip-count} number-value
```

構文の説明

interval *number-value* エコー要求メッセージ間の間隔（秒単位）。

max-skip-count *number-value* メンバーが機能していないと見なすまでの最大再試行回数。

コマンドデフォルト

ハートビート *interval* のデフォルト値は 60 秒です。範囲は 10 ~ 600 秒です。

ハートビート *max-skip-count* のデフォルト値は 3 回の再試行です。範囲は、3 ~ 10 回の再試行です。

コマンド履歴

リリー 変更内容
ス

8.1 このコマンドが導入されました。

次に、ハートビート間隔の値を 45 秒に設定する例を示します。

```
config tunnel eogre heart-beat interval 45
```

config tunnel eogre gateway

GRE ゲートウェイの IPv4 アドレス経由でイーサネットを設定するには、**config tunnel eogre gateway** コマンドを使用します。

```
config tunnel eogre gateway {{{add | modify}} gateway-name {ipv4-address | ipv6-address}
gateway-ip-address} | {delete gateway-name}}
```

| 構文の説明 | | |
|---------------------------|--|-------------------------------|
| add | | 新しいゲートウェイを追加します。 |
| delete | | ゲートウェイを削除します。 |
| modify | | 既存のゲートウェイを変更します。 |
| ipv4-address | | ゲートウェイの IPv4 アドレスを入力します。 |
| ipv6-address | | ゲートウェイの IPv6 アドレスを入力します。 |
| <i>gateway-ip-address</i> | | ゲートウェイの IPv4 または IPv6 アドレスです。 |
| <i>gateway-name</i> | | トンネル ゲートウェイ名。 |

コマンド デフォルト なし

| コマンド履歴 | リリース | 変更内容 |
|--------|------|--|
| | 8.1 | このコマンドが導入されました。 |
| | 8.3 | トンネルゲートウェイの IPv6 アドレス形式のオプションが追加されました。 |

- IPv4 アドレスの例

```
config tunnel eogre gateway add hurricane ipv4 192.168.10.1
```

- IPv6 アドレスの例

```
config tunnel eogre gateway add hurricane ipv6 2001:DB8::1
```


config tunnel eogre domain

トンネル ゲートウェイ ドメイン構成を実行するには、**config tunnel eogre domain** コマンドを使用します。

```
config tunnel eogre domain {{create | delete}domain-name} {{add | remove}domain-name gateway-name
```

| | | |
|-------|---------------------|-----------------------|
| 構文の説明 | create | 新しいゲートウェイドメイン名を作成します。 |
| | delete | ゲートウェイドメインを削除します。 |
| | add | ゲートウェイ名をドメインに追加します |
| | remove | ドメインからゲートウェイ名を削除します |
| | <i>domain-name</i> | ドメイン名 |
| | <i>gateway-name</i> | ゲートウェイ名 |

コマンドデフォルト なし

コマンド履歴 リリー 変更内容
ス

8.1 このコマンドが導入されました。

次に、新しいドメイン名を作成する例を示します。

```
config tunnel eogre domain create web.com data
```

config tunnel eogre domain primary

プライマリまたはセカンダリ ゲートウェイ名をドメインに追加するには、**config tunnel eogre domain primary** コマンドを使用します。

config tunnel eogre domain primary *domain-name gateway-name*

構文の説明

domain-name ドメイン名を入力します

gateway-name ドメインに追加するゲートウェイ名を入力します

使用上のガイドライン

ドメインでは、プライマリ ゲートウェイはデフォルトでアクティブになります。プライマリ ゲートウェイが動作していない場合、セカンダリゲートウェイがアクティブなゲートウェイになります。クライアントは、セカンダリゲートウェイと再度関連付ける必要があります。フェールオーバーの最中や後でも、Cisco WLC はプライマリ ゲートウェイへの ping を続けます。プライマリゲートウェイが再び動作可能になると、プライマリゲートウェイがアクティブなゲートウェイになります。その後、クライアントがプライマリゲートウェイにフォールバックします。同じオプションは、ローカルスイッチドモードの FlexConnect からの TGW でも利用できます。EoGRE トンネルには、DTLS 暗号化 CAPWAP IPv4 または IPv6 を指定できます。この機能は、このリリースでサポートされているすべての Wave 1 AP および Wave 2 AP でサポートされています。

コマンド履歴

リリース 変更内容
ス

8.5 このコマンドが導入されました。

config tunnel profile

プロファイルを作成、コピーまたは削除するには、**config tunnel profile** コマンドを使用します。

```
config tunnel profile {copy | create | delete} profile-name
```

| | |
|-----------|--------------------------------|
| 構文の説明 | copy 既存のプロファイルのコピーします。 |
| | create 新しいプロファイルを作成します。 |
| | delete 既存のプロファイルを削除します。 |
| コマンドデフォルト | なし |
| コマンド履歴 | リリース 変更内容 ス |
| | 8.1 このコマンドが導入されました。 |

次に、新しいプロファイルを作成する例を示します。

```
config tunnel profile create floorone
```

config tunnel profile_rule

プロファイルにルールを追加したりルールを変更するには、**config tunnel profile** コマンドを使用します。

```
config tunnel profile rule {add | modify} profile-name realm-filter realm-string eogre vlan vlan-id
gateway-domain-name
```

| | |
|-----------|---|
| 構文の説明 | <p>add 新規ルールを追加します。</p> <p>modify 既存のルールを変更します。</p> |
| コマンドデフォルト | なし |
| コマンド履歴 | <p>リリース 変更内容</p> <p>8.1 このコマンドが導入されました。</p> |

次に、プロファイルにルールを追加する例を示します。

```
config tunnel profile add table realm filter 5 eogre vlan 3 web.com
```

config tunnel profile_rule-delete

プロファイルからルールを削除するには、**config tunnel profile** コマンドを使用します。

```
config tunnel profile ruledelete profile-name realm-filter realm-string
```

| | |
|------------|---------------------------------------|
| 構文の説明 | delete プロファイルから既存のルールを削除します。 |
| コマンド デフォルト | なし |
| コマンド履歴 | リリース 変更内容 ス 8.1 このコマンドが導入されました。 |

次に、プロファイルからルールを削除する例を示します。

```
config tunnel profile delete table realm filter 5
```

config tunnel profile eogre-DHCP82

DHCP オプション 82 パラメータを有効または無効にするには、**config tunnel profile** コマンドを使用します。

```
config tunnel profile eogre profile-name DHCP-Opt-82 {enable | disable}
```

構文の説明

enable システムの DHCP オプション 82 パラメータを有効にします。

disable システムの DHCP オプション 82 パラメータを無効にします。

コマンド デフォルト

なし

コマンド履歴

リリー 変更内容
ス

8.1 このコマンドが導入されました。

次に、DHCP オプション 82 パラメータを有効にする例を示します。

```
config tunnel profile eogre test dhcp-opt-82 enable
```

config tunnel profile eogre-gateway-radius-proxy

ゲートウェイ Radius プロキシを有効または無効にするには、`config tunnel profile` コマンドを使用します。

```
config tunnel profile eogre profile-name gateway-radius-proxy {enable | disable}
```

構文の説明

enable Radius プロキシとしてゲートウェイを有効にします。

disable Radius のプロキシとしてゲートウェイを無効にします。

コマンドデフォルト

なし

コマンド履歴

リリース 変更内容
ス

8.1 このコマンドが導入されました。

次に、ゲートウェイ プロキシを有効にする例を示します。

```
config tunnel profile eogre test gateway-radius-proxy enable
```

config tunnel profile eogre-gateway-radius-proxy-accounting

アカウントリング Radius プロキシとしてゲートウェイを有効または無効にするには、`config tunnel profile` コマンドを使用します。

```
config tunnel profile eogre profile-name gateway-radius-proxy accounting {enable | disable}
```

構文の説明

enable アカウントリング Radius プロキシとしてゲートウェイを有効にします。

disable アカウントリング Radius プロキシとしてゲートウェイを無効にします。

コマンドデフォルト

なし

コマンド履歴

リリー 変更内容
ス

8.1 このコマンドが導入されました。

次に、アカウントリング Radius プロキシとしてゲートウェイを無効にする例を示します。

```
config tunnel profile eogre test gateway-radius-proxy accounting disable
```


config tunnel profile eogre-DHCP82

DHCP オプション 82 パラメータを有効または無効にするには、**config tunnel profile** コマンドを使用します。

```
config tunnel profile eogre profile-name DHCP-Opt-82 {enable | disable}
```

構文の説明

enable システムの DHCP オプション 82 パラメータを有効にします。

disable システムの DHCP オプション 82 パラメータを無効にします。

コマンドデフォルト

なし

コマンド履歴

リリース 変更内容
ス

8.1 このコマンドが導入されました。

次に、DHCP オプション 82 パラメータを有効にする例を示します。

```
config tunnel profile eogre test dhcp-opt-82 enable
```

config tunnel profile eogre-DHCP82-circuit-id

DHCP オプション 82 パラメータで回路 ID フィールドの形式を設定するには、**config tunnel profile** コマンドを使用します。

```
config tunnel profile eogre profile-name DHCP-Opt-82 circuit-id parameter-id
```

構文の説明

circuit-id DHCPオプション 82 の回路 ID フィールドの形式を設定します

parameter-id サポートされているパラメータのリスト。

- ap-mac
- ap-ethmac
- ap-name
- ap-group-name
- flex-group-name
- ap-location
- vlan-id
- SSID-name
- SSID-TYPE
- Client-mac

コマンド デフォルト なし

コマンド履歴

リリース 変更内容
ス

8.1 このコマンドが導入されました。

次に、DHCP オプション 82 パラメータで回路 ID の形式を設定する例を示します。

```
config tunnel profile eogre test dhcp-opt-82 circuit-id access1bldg
```

config tunnel profile eogre-DHCP82-delimiter

DHCP オプション 82 パラメータのデリミタ（区切り文字）を設定するには、**config tunnel profile** コマンドを使用します。

config tunnel profile eogre *profile-name* DHCP-Opt-82 delimiter *delimiter character*

| 構文の説明 | delimiter システムの DHCP オプション 82 パラメータの区切り文字を設定します。 | | | | |
|-----------|---|------|------|-----|-----------------|
| | <i>delimiter character</i> 区切り文字は DHCP オプション 82 パラメータを区切るために使用されます。 | | | | |
| コマンドデフォルト | なし | | | | |
| コマンド履歴 | <table><thead><tr><th>リリース</th><th>変更内容</th></tr></thead><tbody><tr><td>8.1</td><td>このコマンドが導入されました。</td></tr></tbody></table> | リリース | 変更内容 | 8.1 | このコマンドが導入されました。 |
| リリース | 変更内容 | | | | |
| 8.1 | このコマンドが導入されました。 | | | | |

次に、DHCP オプション 82 パラメータを区切り文字で分割する例を示します。

```
config tunnel profile eogre test dhcp-opt-82 delimiter -
```

config tunnel profile eogre-DHCP82-format

DHCP オプション 82 で必要な形式を設定するには、`config tunnel profile` コマンドを使用します。

```
config tunnel profile eogre profile-name dhcp-opt-82 format { binary | ascii }
```

| | |
|-----------|---|
| 構文の説明 | binary DHCPオプション82の形式をバイナリに設定します |
| | ascii DHCPオプション82の形式をAsciiに設定します |
| コマンドデフォルト | なし |
| コマンド履歴 | リリー 変更内容 ス |
| | 8.1 このコマンドが導入されました。 |

次に、DHCPオプション82パラメータに「バイナリ」形式を設定する例を示します。

```
config tunnel profile eogre test dhcp-opt-82 format binary
```

config tunnel profile eogre-DHCP82-remote-id

DHCP オプション 82 パラメータでリモート ID フィールドの形式を設定するには、**config tunnel profile** コマンドを使用します。

config tunnel profile eogre *profile-name* **DHCP-Opt-82** **remote-id** *parameter-id*

構文の説明

remote-id DHCP オプション 82 のリモート ID フィールドの形式を設定します

parameter-id サポートされているパラメータのリスト。

- ap-mac
- ap-ethmac
- ap-name
- ap-group-name
- flex-group-name
- ap-location
- vlan-id
- SSID-name
- SSID-TYPE
- Client-mac

コマンドデフォルト

なし

コマンド履歴

リリース 変更内容

8.1 このコマンドが導入されました。

次に、DHCP オプション 82 パラメータでリモート ID の形式を設定する例を示します。

```
config tunnel profile eogre test dhcp-opt-82 remote-id access1flr
```

config watchlist add

無線 LAN の監視リストエントリを追加するには、**config watchlist add** コマンドを使用します。

```
config watchlist add { mac MAC | username username }
```

| | | |
|------------|---------------------------------|-----------------------------------|
| 構文の説明 | mac <i>MAC</i> | 無線 LAN の MAC アドレスを指定します。 |
| | username <i>username</i> | 監視するユーザの名前を指定します。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、MAC アドレス a5:6b:ac:10:01:6b で監視リストエントリを追加する例を示します。

```
(Cisco Controller) >config watchlist add mac a5:6b:ac:10:01:6b
```

config watchlist delete

無線 LAN の監視リスト エントリを削除するには、**config watchlist delete** コマンドを使用します。

```
config watchlist delete { mac MAC | username username }
```

| | | |
|-----------|---------------------------------|-----------------------------------|
| 構文の説明 | mac <i>MAC</i> | リストから削除する無線 LAN の MAC アドレスを指定します。 |
| | username <i>username</i> | リストから削除するユーザの名前を指定します。 |
| コマンドデフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、MAC アドレス a5:6b:ac:10:01:6b で監視リスト エントリを削除する例を示します。

```
(Cisco Controller) >config watchlist delete mac a5:6b:ac:10:01:6b
```

config watchlist disable

クライアントの監視リストを無効にするには、**config watchlist disable** コマンドを使用します。

config watchlist disable

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

| リリース | 変更内容 |
|------|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、クライアントの監視リストをディセーブルにする例を示します。

```
(Cisco Controller) >config watchlist disable
```


config watchlist enable

無線 LAN の監視リスト エントリを有効にするには、**config watchlist enable** コマンドを使用します。

config watchlist enable

構文の説明

このコマンドには引数またはキーワードはありません。

コマンド デフォルト

なし

コマンド履歴

| リリース | 変更内容 |
|------|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、監視リスト エントリをイネーブルにする例を示します。

```
(Cisco Controller) >config watchlist enable
```

config wgb vlan

VLAN ワークグループブリッジ (WGB) クライアントのサポートを設定するには、**config wgb vlan** コマンドを使用します。

config wgb vlan {enable | disable}

| | | |
|-----------|----------------|--|
| 構文の説明 | enable | WGB の背後にある有線クライアントをデータ管理ゾーン (DMZ) のアンカーコントローラに接続できるようにします。 |
| | disable | WGB の背後にある有線クライアントを DMZ のアンカーコントローラへの接続から無効にします。 |
| コマンドデフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、VLAN WGB クライアントのサポートを有効にする例を示します。

```
(Cisco Controller) >config wgb vlan enable
```

config wlan

無線 LAN を作成、削除、イネーブル、またはディセーブルにするには、**config wlan** コマンドを使用します。

config wlan { **enable** | **disable** | **create** | **delete** } *wlan_id* [*name* | **foreignAp** *name ssid* | **all**]

| 構文の説明 | | |
|------------------|------|-----------------------------------|
| enable | | ワイヤレス LAN をイネーブルにします。 |
| disable | | ワイヤレス LAN をディセーブルにします。 |
| create | | 無線 LAN を作成します。 |
| delete | | 無線 LAN を削除します。 |
| <i>wlan_id</i> | | 1 ~ 512 の無線 LAN 識別子。 |
| <i>name</i> | | (任意) 最大 32 文字の英数字の WLAN プロファイル名。 |
| foreignAp | | (任意) サードパーティのアクセス ポイント設定を指定します。 |
| <i>ssid</i> | | 最大 32 文字の英数字の SSID (ネットワーク名)。 |
| all | | (任意) すべての無線 LAN を指定します。 |
| コマンドデフォルト | | なし |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン **config wlan create** コマンドを使用して新しい WLAN を作成すると、無効モードで作成されません。設定が終了するまでは、無効のままにしてください。

SSID を指定しない場合は、プロファイル名パラメータがプロファイル名と SSID の両方に使用されます。

管理インターフェイスおよび AP マネージャインターフェイスが同じポートにマップされており、いずれも同じ VLAN のメンバである場合は、WLAN を無効にしてから、ポートマッピングをいずれかのインターフェイスに変更する必要があります。管理インターフェイスと AP マネージャインターフェイスが別々の VLAN に割り当てられている場合は、WLAN を無効にする必要はありません。

アクセスポイントグループに割り当てられている WLAN を削除しようとする、エラーメッセージが表示されます。そのまま続行すると、アクセスポイントグループとアクセスポイントの無線から WLAN が削除されます。

次に、無線 LAN 識別子 16 をイネーブルにする例を示します。

```
(Cisco Controller) >config wlan enable 16
```

config wlan 7920-support

電話に対するサポートを設定するには、**config wlan 7920-support** コマンドを使用します。

```
config wlan 7920-support {client-cac-limit | ap-cac-limit} {enable | disable} wlan_id
```

| 構文の説明 | | |
|-------|-------------------------|---|
| | ap-cac-limit | クライアント制御のコールアドミッション制御 (CAC) を必要とする (シスコのベンダー固有情報要素 (IE) が要求される) 電話をサポートします。 |
| | client-cac-limit | アクセスポイント制御の CAC を必要とする (IEEE 802.11e Draft 6 QBSS-load が要求される) 電話をサポートします。 |
| | enable | 電話サポートをイネーブルにします。 |
| | disable | 電話サポートをディセーブルにします。 |
| | <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |

コマンドデフォルト なし

| コマンド履歴 | リリース | 変更内容 |
|--------|------|-----------------------------------|
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン 1 つの WLAN で、WMM モードとクライアントにより制御された CAC モードの両方を有効にすることはできません。

次に、無線 LAN ID 8 で、クライアント制御される CAC を必要とする電話サポートをイネーブルにする例を示します。

```
(Cisco Controller) >config wlan 7920-support ap-cac-limit enable 8
```

config wlan 802.11e

無線 LAN で 802.11e サポートを設定するには、**config wlan 802.11e** コマンドを使用します。

config wlan 802.11e { **allow** | **disable** | **require** } *wlan_id*

| | | |
|------------|----------------|-----------------------------------|
| 構文の説明 | allow | 無線 LAN で 802.11e 対応クライアントを許可します。 |
| | disable | 無線 LAN で 802.11e サポートをディセーブルにします。 |
| | require | 無線 LAN で 802.11e 対応クライアントを要求します。 |
| | <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン 802.11e は LAN アプリケーションに Quality of Service (QoS) サポートを提供します。これは、Voice over Wireless IP (VoWIP) など遅延に影響されやすいアプリケーションにとって重要なサポートです。

802.11e は 802.11 メディア アクセス コントロール レイヤ (MAC レイヤ) の拡張版であり、調整済時分割多元接続 (TDMA) が設定され、音声やビデオなど遅延に影響されやすいアプリケーション向けのエラー修正メカニズムが追加されています。802.11e 仕様は特にマルチメディア機能が組み込まれたネットワークでの使用に適しており、シームレスな相互運用性を実現します。

次に、LAN ID 1 の無線 LAN で 802.11e を許可する例を示します。

```
(Cisco Controller) >config wlan 802.11e allow 1
```

config wlan aaa-override

無線 LAN で AAA を介したユーザ ポリシー オーバーライドを設定するには、**config wlan aaa-override** コマンドを使用します。

```
config wlan aaa-override {enable | disable} {wlan_id | foreignAp}
```

| 構文の説明 | enable | disable | wlan_id | foreignAp |
|-------|-------------------------|--------------------------|----------------------|--------------------------|
| | ポリシー オーバーライドをイネーブルにします。 | ポリシー オーバーライドをディセーブルにします。 | 1 ~ 512 の無線 LAN 識別子。 | サードパーティのアクセス ポイントを指定します。 |

コマンドデフォルト AAA はディセーブルです。

| コマンド履歴 | リリース | 変更内容 |
|--------|------|-----------------------------------|
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン AAA オーバーライドが有効になっていて、クライアントで AAA と Cisco Wireless LAN Controller の無線 LAN 認証パラメータが競合している場合、クライアント認証は AAA サーバによって行われます。この認証の一環として、オペレーティングシステムはクライアントをデフォルトの Cisco Wireless LAN VLAN から、AAA サーバによって返されたコントローラのインターフェイス構成（MAC フィルタリング、802.1X、および Wi-Fi Protected Access（WPA）動作に対してだけ設定されている場合）で事前定義された VLAN に移動します。すべてのケースで、コントローラのインターフェイス構成で事前定義されている限り、オペレーティングシステムは QoS、DSCP、802.1p 優先順位タグ値および AAA サーバで指定された ACLs を使用します（この AAA オーバーライドによる VLAN スイッチングは、ID ネットワーキングとも呼ばれます）。

企業の無線 LAN が VLAN 2 に割り当てられている管理インターフェイスを使用し、AAA オーバーライドが VLAN 100 へのリダイレクトを返す場合、VLAN 100 が割り当てられている物理ポートに関係なく、オペレーティングシステムはすべてのクライアント送信を VLAN 100 にリダイレクトします。

AAA Override をディセーブルにすると、コントローラの認証パラメータ設定がすべてのクライアント認証においてデフォルトで使用され、コントローラ無線 LAN にクライアント固有の認証パラメータがない場合は、AAA サーバのみによって認証が実行されます。

AAA オーバーライド値は、RADIUS サーバから取り込まれる場合があります。

次に、WLAN ID 1 で AAA を介したユーザ ポリシー オーバーライドを設定する例を示します。

```
(Cisco Controller) >config wlan aaa-override enable 1
```


config wlan acl

無線 LAN のアクセス コントロール リスト (ACL) を設定するには、**config wlan acl** コマンドを使用します。

config wlan acl [*acl_name* | **none**]

| | | |
|------------|-----------------|-----------------------------------|
| 構文の説明 | <i>wlan_id</i> | 無線 LAN 識別子 (1~512)。 |
| | <i>acl_name</i> | (任意) ACL 名です。 |
| | none | (任意) 指定された無線 LAN の ACL 設定をクリアします。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、WLAN ID 1 と **office_1** という名前の ACL で WLAN アクセス コントロール リストを設定する例を示します。

```
(Cisco Controller) >config wlan acl 1 office_1
```

config wlan apgroup

アクセス ポイント グループの VLAN 機能を管理するには、**config wlan apgroup** コマンドを使用します。

```
config wlan apgroup {add apgroup_name [description] | delete apgroup_name | description
apgroup_name description | interface-mapping {add | delete} apgroup_name wlan_id
interface_name | nac-snmp {enable | disable} apgroup_name wlan_id | nasid NAS-ID
apgroup_name | profile-mapping {add | delete} apgroup_name profile_name | wlan-radio-policy
apgroup_name wlan-id {802.11a-only | 802.11bg | 802.11g-only | all} | hotspot {venue {type
apgroup_name group_codetype_code | name apgroup_name language_code venue_name} |
operating-class {add | delete} apgroup_name operating_class_value}
```

構文の説明

| | |
|--------------------------|--|
| add | 新しいアクセス ポイント グループ (AP グループ) を作成します。 |
| <i>apgroup_name</i> | アクセス ポイント グループ名。 |
| <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| delete | AP グループから無線 LAN を除外します。 |
| description | AP グループについて説明します。 |
| <i>description</i> | AP グループの説明。 |
| interface-mapping | (任意) AP グループから無線 LAN を割り当てるか削除します。 |
| <i>interface_name</i> | (任意) AP グループをマップするインターフェイス。 |
| nac-snmp | 特定の AP グループの NAC SNMP 機能を設定します。アクセス ポイント グループでの Network Admission Control (NAC) アウトオブバンドサポートをイネーブルまたはディセーブルにします。 |
| enable | AP グループ上で NAC アウトオブバンドのサポートをイネーブルにします。 |
| disable | AP グループ上で NAC アウトオブバンドのサポートをディセーブルにします。 |

| | |
|--------------------------|---|
| <i>NAS-ID</i> | AP グループのネットワーク アクセス サーバ ID (NAS-ID)。NAS-ID は、認証要求を使用してコントローラによって (RADIUS クライアントとして) RADIUS サーバに送られます。これはユーザをさまざまなグループに分類するために使用されます。最大 32 文字の英数字を入力できます。リリース 7.4 以降では、NAS-ID をインターフェイス、WLAN、またはアクセスポイントグループに設定できます。優先順位は AP グループの NAS-ID > WLAN の NAS-ID > インターフェイスの NAS-ID の順です。 |
| none | コントローラのシステム名を NAS-ID として設定します。 |
| profile-mapping | AP グループの RF プロファイルマッピングを設定します。 |
| <i>profile_name</i> | 指定した AP グループの RF プロファイル名。 |
| wlan-radio-policy | AP グループに WLAN 無線ポリシーを設定します。 |
| 802.11a-only | AP グループに WLAN 無線ポリシーを設定します。 |
| 802.11bg | AP グループに WLAN 無線ポリシーを設定します。 |
| 802.11g-only | AP グループに WLAN 無線ポリシーを設定します。 |
| all | AP グループに WLAN 無線ポリシーを設定します。 |
| hotspot | AP グループのホットスポットを設定します。 |
| venue | AP グループの場所情報を設定します。 |
| type | AP グループの場所のタイプを設定します。 |

group_code

AP グループの場所グループの情報。
次のオプションを使用できます。

- 0 : 指定なし
 - 1 : 集会施設
 - 2 : ビジネス
 - 3 : 教育
 - 4 : 工場および産業
 - 5 : 機関
 - 6 : 商業施設
 - 7 : 居住施設
 - 8 : 倉庫
 - 9 : 公共施設、その他
 - 10 : 乗り物
 - 11 : アウトドア
-

type_code

AP グループの場所タイプの情報。

場所グループ 1（集会施設）には、次のオプションが使用できます。

- 0 : 指定されていない集会施設
- 1 : アリーナ
- 2 : スタジアム
- 3 : 旅客ターミナル
- 4 : 円形劇場
- 5 : 遊園地
- 6 : 礼拝場所
- 7 : 会議室
- 8 : 図書館
- 9 : 博物館
- 10 : レストラン
- 11 : シアター
- 12 : バー
- 13 : カフェ
- 14 : 動物園または水族館
- 15 : 緊急時の調整センター

場所グループ 2（ビジネス）には、次のオプションが使用できます。

- 0 : 指定されていないビジネス
- 1 : 医師または歯科医のオフィス
- 2 : 銀行
- 3 : 消防局
- 4 : 警察署
- 6 : 郵便局
- 7 : 専門家のオフィス
- 8 : 研究開発施設
- 9 : 弁護士のオフィス

場所グループ 3（教育施設）には、次のオプションが使用できます。

- 0 : 指定されていない教育施設
- 1 : 小学校
- 2 : 中学校
- 3 : 大学または専門学校

場所グループ 4（工場および産業）には、次のオプションが使用できます。

- 0 : 指定されていない工場および産業
- 1 : 工場

場所グループ 5（機関）には、次のオプションが使用できます。

- 0 : 指定されていない機関
- 1 : 病院
- 2 : 長期介護施設
- 3 : アルコールおよび麻薬のリハビリテーションセンター
- 4 : グループ ホーム
- 5 : 刑務所や拘置所

場所グループ 6（商業施設）には、次のオプションが使用できます。

- 0 : 指定されていない商業施設
- 1 : 小売店
- 2 : 食料品市場
- 3 : 自動車サービス ステーション
- 4 : ショッピング モール
- 5 : ガソリン スタンド

場所グループ7（居住施設）には、次のオプションが使用できます。

- 0 : 指定されていない居住施設
- 1 : 個人の住宅
- 2 : ホテルまたはモーテル
- 3 : 寮
- 4 : 寄宿舍

場所グループ8（倉庫）には、次のオプションが使用できます。

- 0 : 指定されていない倉庫

場所グループ9（公共施設、その他）には、次のオプションが使用できます。

- 0 : 指定されていない公共施設およびその他

場所グループ10（乗り物）には、次のオプションが使用できます。

- 0 : 指定されていない乗り物
 - 1 : 自動車またはトラック
 - 2 : 航空機
 - 3 : バス
 - 4 : フェリー
 - 5 : 船舶またはボート
 - 6 : 鉄道
 - 7 : バイク
-

場所グループ 11（アウトドア）には、次のオプションが使用できます。

- 0 : 指定されていないアウトドア
- 1 : ミニメッシュ ネットワーク
- 2 : 都市公園
- 3 : 休憩所
- 4 : 交通制御施設
- 5 : バス停
- 6 : キオスク

| | |
|------------------------------|---|
| name | AP グループの場所の名前を設定します。 |
| <i>language_code</i> | 場所で使用される言語を定義するの ISO-639 符号化文字列。この文字列は3文字の言語コードです。たとえば、英語の場合はENGと入力します。 |
| <i>venue_name</i> | この AP グループ会場の名前。この名前は、基本サービス セット（BSS）に関連付けられ、SSID で場所に関する十分な情報が得られないときに使用されます。場所の名前は最大 252 文字の英数字で、大文字と小文字を区別します。 |
| add | AP グループの運用クラスを追加します。 |
| delete | AP グループの運用クラスを削除します。 |
| <i>operating_class_value</i> | AP グループの運用クラス。使用可能な運用クラスは、81、83、84、112、113、115、116、117、118、119、120、121、122、123、124、125、126、127 です。 |

コマンドデフォルト AP グループの VLAN は無効です。

コマンド履歴

| リリース | 変更内容 |
|------|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン

1 つ以上のアクセス ポイントで使用しているアクセス ポイント グループを削除しようとする時、エラー メッセージが表示されます。コントローラ ソフトウェア リリース 6.0 で AP を削除するには、まず、このグループのすべての AP を別のグループに移動します。以前のリリースのように、アクセス ポイントが **default-group** アクセス ポイント グループに移動されること

はありません。AP を表示するには、**show wlan apgroups** コマンドを入力します。AP を移動するには、**config ap group-name groupname cisco_ap** コマンドを入力します。

AP グループ、WLAN、またはインターフェイスのコントローラに設定されている NAS-ID が認証に使用されます。NAS-ID はコントローラに伝播されません。

次に、アクセス ポイント グループ 4 で、NAC アウトオブバンド サポートをイネーブルにする例を示します。

```
(Cisco Controller) >config wlan apgroup nac enable apgroup 4
```

config wlan apgroup atf 802.11

config wlan apgroup atf 802.11 コマンドを使用して、AP グループ レベルでの Cisco Airtime Fairness を設定します。

```
config wlan apgroups atf 802.11{a | b} {mode {disable | monitor | enforce-policy}
ap-group-name} | {optimization {enable | disable}}
```

構文の説明

| | |
|-----------------------|----------------------------|
| a | 802.11a ネットワーク設定を指定します。 |
| b | 802.11b/g ネットワーク設定を指定します。 |
| mode | Cisco ATF の強制のきめ細かさを設定します。 |
| disable | Cisco ATF を無効にします。 |
| monitor | Cisco ATF をモニタ モードで設定します。 |
| enforce-policy | Cisco ATF を強制モードで設定します。 |
| <i>ap-group-name</i> | 指定する必要がある AP グループ名 |
| optimization | 通信時間の最適化を設定します。 |
| enable | 通信時間の最適化を有効にします。 |
| disable | 通信時間の最適化を無効にします。 |

コマンド履歴

リリース 変更内容

8.1 このコマンドが追加されました。

802.11a ネットワークで Cisco ATF を強制モードで設定するには、AP グループ *my-ap-group* に、次のコマンドを入力します。

```
(Cisco Controller) >config wlan apgroup atf 802.11a mode enforce-policy my-ap-group
```

config wlan apgroup atf 802.11 policy

WLAN で Cisco ATF ポリシーの AP レベルのオーバーライドを設定するには、次のコマンドを使用します。

```
config wlan apgroup atf 802.11 {a | b} policy ap-group-name wlan-id policy-name override {enable | disable}
```

| 構文の説明 | | |
|-------|----------------------|--|
| | a | 802.11a ネットワーク設定を指定します。 |
| | b | 802.11b ネットワーク設定を指定します。 |
| | policy | Cisco ATF ポリシーを指定します。 |
| | <i>ap-group-name</i> | 指定する必要がある AP グループ名 |
| | <i>wlan-id</i> | 指定する必要がある WLAN ID またはリモート LAN ID。 |
| | <i>policy-name</i> | 指定する必要がある Cisco ATF ポリシー名。 |
| | override | AP グループの WLAN の ATF ポリシー オーバーライドを設定します。 |
| | enable | AP グループの WLAN の ATF ポリシー オーバーライドを有効にします。 |
| | disable | AP グループの WLAN の ATF ポリシー オーバーライドを無効にします。 |

| コマンド履歴 | リリース | 変更内容 |
|--------|------|-----------------|
| | 8.1 | このコマンドが追加されました。 |

config wlan apgroup.opendns-profile

オープンドメインネームシステム (DNS) のプロファイルをアクセスポイント (AP) グループの無線 LAN (WLAN) に設定するには、**config wlan apgroup.opendns-profile** コマンドを使用します。

config wlan apgroup.opendns-profile *wlan-id site-name profile-name enable*

構文の説明

| | |
|---------------------|--|
| <i>wlan-id</i> | WLAN 識別子。 |
| <i>site-name</i> | 設定する AP グループの名前。 |
| <i>profile-name</i> | このプロファイルを追跡するために使用される OpenDNS プロファイル名。 |
| enable | OpenDNS のアイデンティティを有効にします。 |
| disable | OpenDNS のアイデンティティを無効にします。 |

コマンドデフォルト

AP グループの WLAN に OpenDNS プロファイルは作成されません。

コマンドモード

(コントローラの設定) >

コマンド履歴

| リリース | 変更内容 |
|------|-----------------|
| 8.4 | このコマンドが導入されました。 |

使用上のガイドライン

なし

例

次に、AP グループの WLAN に openDNS プロファイルを設定する例を示します。

```
(Cisco Controller) > config wlan apgroup.opendns-profile wlan1 sitel user1
```

config wlan apgroup qinq

AP グループのトラフィックの 802.1Q-in-Q VLAN タギングを設定するには、**config wlan apgroup qinq** コマンドを使用します。

```
config wlan apgroup qinq {tagging {client-traffic | dhcp-v4 | eap-sim-aka} apgroup_name {enable | disable}|service-vlanapgroup_name vlan_id}
```

| 構文の説明 | パラメータ | 説明 |
|-------|-----------------------|--|
| | tagging | トラフィックの 802.1Q-in-Q VLAN タギングを設定します。 |
| | client-traffic | AP グループのクライアントトラフィックの 802.1Q-in-Q タギングを設定します。 |
| | dhcp-v4 | AP グループの DHCPv4 トラフィックの 802.1Q-in-Q タギングを設定します。 |
| | eap-sim-aka | AP グループの Extensible Authentication Protocol for Authentication and Key Agreement (EAP-AKA) 、および EAP for Global System for Mobile Communications Subscriber Identity Module (EAP-SIM) トラフィックの 802.1Q-in-Q タギングを設定します。 |
| | enable | トラフィックの 802.1Q-in-Q タギングを有効にします。 |
| | disable | トラフィックの 802.1Q-in-Q タギングを無効にします。 |
| | service-vlan | AP グループのサービス VLAN を設定します。 |
| | <i>apgroup_name</i> | アクセス ポイントグループの名前。 |
| | <i>vlan_id</i> | VLAN 識別番号。 |

コマンド デフォルト デフォルトでは、AP グループのクライアントおよび DHCPv4 トラフィックの 802.1Q-in-Q タギングは無効です。

| コマンド履歴 | リリース | 変更内容 |
|--------|------|-----------------|
| | 8.0 | このコマンドが導入されました。 |

使用上のガイドライン



(注) DHCPv4 トラフィックの 802.1Q-in-Q タギングを有効にする前に、クライアントトラフィックの 802.1Q-in-Q タギングを有効にする必要があります。

クライアントトラフィックの 802.1Q-in-Q タギングを有効にすると、EAP-AKA および EAP-SIM トラフィックの 802.1Q-in-Q タギングも有効になります。

次に、AP グループのクライアントトラフィックの 802.1Q-in-Q タギングを有効にする例を示します。

```
(Cisco Controller) >config wlan apgroup qinq tagging client-traffic APg1 enable
```

次に、AP グループのサービス VLAN を設定する例を示します。

```
(Cisco Controller) >config wlan apgroup qinq service-vlan APg1 10
```

config wlan assisted-roaming

WLAN で経路ローミングを設定するには、**config wlan assisted-roaming** コマンドを使用します。

```
config wlan assisted-roaming {neighbor-list | dual-list | prediction} {enable | disable}
wlan_id
```

構文の説明

| | |
|----------------------|---|
| neighbor-list | WLAN の 802.11k ネイバー リストを設定します。 |
| dual-list | WLAN のデュアルバンド 802.11k ネイバー リストを設定します。デフォルトは、クライアントが現在関連付けられている帯域です。 |
| prediction | WLAN の経路ローミング最適化の予測を設定します。 |
| enable | WLAN の設定をイネーブルにします。 |
| disable | WLAN の設定をディセーブルにします。 |
| wlan_id | 1 ~ 512 の無線 LAN 識別子。 |

コマンド デフォルト

すべての WLAN で 802.11k ネイバー リストが有効です。

デフォルトでは、ネイバー リスト機能が WLAN に対してイネーブルな場合に、デュアルバンド リストはイネーブルになります。

コマンド履歴

| リリース | 変更内容 |
|------|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン

経路ローミングの予測のリストをイネーブルにすると、警告が表示されます。また、WLAN でロードバランシングがすでにイネーブルになっている場合、ロードバランシングはその WLAN でディセーブルになります。

次に、WLAN の 802.11k ネイバー リストをイネーブルにする例を示します。

```
(Cisco Controller) >config wlan assisted-roaming neighbor-list enable 1
```


config wlan atf

config wlan atf コマンドを使用して、Cisco ATF ポリシーに WLAN をマッピングします。

config wlan atf *wlan-id* **policy** *policy-id*

構文の説明

wlan-id Cisco ATF ポリシーをマッピングする必要がある、指定すべき WLAN ID。

policy Cisco ATF ポリシーを指定します。

policy-id 指定する必要がある Cisco ATF ポリシー ID。

コマンド履歴

| リリース | 変更内容 |
|------|------|
|------|------|

| | |
|-----|-----------------|
| 8.1 | このコマンドが追加されました。 |
|-----|-----------------|

config wlan avc

WLAN に Application Visibility and Control (AVC) を設定するには、**config wlan avc** コマンドを使用します。

```
config wlan avc wlan_id {profile profile_name | visibility} {enable | disable}
```

| 構文の説明 | |
|---------------------|--|
| <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| profile | WLAN から AVC プロファイルをアソシエーションまたは削除します。 |
| <i>profile_name</i> | AVC プロファイルの名前。プロファイル名は最大 32 文字の英数字で、大文字と小文字を区別します。 |
| visibility | WLAN にアプリケーションの表示を設定します。 |
| enable | WLAN でアプリケーションの表示をイネーブルにします。Network Based Application Recognition (NBAR) ディープ パケット インスペクション テクノロジーに基づいて、アプリケーションの分類を確認できます。 クライアント AVC 統計情報を表示するには、 show avc statistics client コマンドを使用します。 |
| disable | WLAN でアプリケーションの表示をディセーブルにします。 |

コマンド デフォルト なし

| コマンド履歴 | リリース | 変更内容 |
|--------|------|-----------------------------------|
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン 1 つの WLAN には AVC プロファイルを 1 つだけ設定できます。また各 AVC プロファイルに最大 32 のルールを設定できます。各ルールはアプリケーションに対してマーキングまたは廃棄アクションを指定し、WLAN ごとに最大 32 のアプリケーションのアクションを設定できます。コントローラ 1 台に最大 16 の AVC プロファイルを設定し、AVC プロファイル 1 つを複数の WLAN に関連付けることができます。

次に、WLAN に AVC プロファイルを関連付ける例を示します。

```
(Cisco Controller) >config wlan avc 5 profile profile1 enable
```

config wlan band-select allow

WLAN で帯域選択を設定するには、**config wlan band-select allow** コマンドを使用します。

```
config wlan band-select allow {enable | disable} wlan_id
```

構文の説明

enable WLAN で帯域選択をイネーブルにします。

disable WLAN で帯域選択をディセーブルにします。

wlan_id 1 ~ 512 の無線 LAN 識別子。

コマンドデフォルト

なし

コマンド履歴

| リリース | 変更内容 |
|------|------|
|------|------|

| | |
|-----|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |
|-----|-----------------------------------|

使用上のガイドライン

WLAN で帯域選択を有効にすると、アクセスポイントによって 2.4 GHz でのクライアントプロローブが抑制され、デュアルバンドクライアントが 5 GHz スペクトルに移動されます。帯域選択アルゴリズムによるデュアルバンドクライアントの誘導は、同じアクセスポイントの 2.4 GHz 無線から 5 GHz 無線へに限られます。このアルゴリズムが機能するのは、アクセスポイントで 2.4 GHz と 5 GHz の両方の無線が稼働している場合のみです。帯域選択は、Cisco Aironet 1040、1140、1250、および 3500 シリーズのアクセスポイントでのみ使用できます。

次に、WLAN で帯域選択をイネーブルにする例を示します。

```
(Cisco Controller) >config wlan band-select allow enable 6
```

config wlan broadcast-ssid

無線 LAN でサービス セット識別子 (SSID) ブロードキャストを設定するには、**config wlan broadcast-ssid** コマンドを使用します。

```
config wlan broadcast-ssid {enable | disable} wlan_id
```

| | | |
|------------|--------------------------|------------------------------------|
| 構文の説明 | enable | 無線 LAN で SSID ブロードキャストをイネーブルにします。 |
| | disable | 無線 LAN で SSID ブロードキャストをディセーブルにします。 |
| | <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| コマンド デフォルト | SSID のブロードキャストはディセーブルです。 | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、無線 LAN ID 1 の SSID ブロードキャストを設定する例を示します。

```
(Cisco Controller) >config wlan broadcast-ssid enable 1
```

config wlan call-snoop

特定の WLAN に対して Voice-over-IP (VoIP) スヌーピングをイネーブルまたはディセーブルにするには、**config wlan call-snoop** コマンドを使用します。

config wlan call-snoop {enable | disable} wlan_id

| | | |
|-------|----------------|-----------------------------------|
| 構文の説明 | enable | 無線 LAN 上の VoIP スヌーピングをイネーブルにします。 |
| | disable | 無線 LAN 上の VoIP スヌーピングをディセーブルにします。 |
| | <i>wlan_id</i> | 1 ～ 512 の無線 LAN 識別子。 |

コマンドデフォルト なし

| コマンド履歴 | リリース | 変更内容 |
|--------|------|-----------------------------------|
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン WLAN は Platinum QoS とし、この CLI を起動中にディセーブルにする必要があります。

次の例では、VoIP スヌーピングを WLAN 3 でイネーブルにする方法を示します。

```
(Cisco Controller) >config wlan call-snoop 3 enable
```

config wlan chd

無線 LAN に対してカバレッジ ホール検出 (CHD) を有効または無効にするには、**config wlan chd** コマンドを使用します。

config wlan chd *wlan_id* {**enable** | **disable**}

| | | |
|------------|----------------|------------------------------------|
| 構文の説明 | <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| | enable | 無線 LAN で SSID ブロードキャストをイネーブルにします。 |
| | disable | 無線 LAN で SSID ブロードキャストをディセーブルにします。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次の例では、CHD を WLAN 3 でイネーブルにする方法を示します。

```
(Cisco Controller) >config wlan chd 3 enable
```

config wlan ccx aironet-ie

WLAN に対する Aironet 情報要素 (IE) を有効または無効にするには、**config wlan ccx aironet-ie** コマンドを使用します。

config wlan ccx aironet-ie {enable | disable}

| | | |
|-----------|----------------|-----------------------------------|
| 構文の説明 | enable | Aironet 情報要素をイネーブルにします。 |
| | disable | Aironet 情報要素をディセーブルにします。 |
| コマンドデフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、WLAN に対する Aironet 情報要素をイネーブルにする例を示します。

```
(Cisco Controller) >config wlan ccx aironet-ie enable
```

config wlan channel-scan defer-priority

オフ チャネル スキャンを延期できるパケットの優先順位マーキングに対して、延期するようにコントローラを設定するには、**config wlan channel-scan defer-priority** コマンドを使用します。

config wlan channel-scan defer-priority *priority* [**enable** | **disable**] *wlan_id*

| | | |
|------------|-----------------|--|
| 構文の説明 | <i>priority</i> | ユーザ プライオリティ値 (0~7)。 |
| | enable | (任意) 特定の優先順位のパケットでオフチャネル スキャンの延期をイネーブルにします。 |
| | disable | (任意) 特定の優先順位のパケットでオフチャネル スキャンの延期をディセーブルにします。 |
| | <i>wlan_id</i> | 無線 LAN 識別子 (1~512)。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン priority 値は、クライアントおよび WLAN では 6 に設定する必要があります。

次に、ユーザ プライオリティ値 6 および WLAN ID 30 のオフ チャネル スキャンを延期できる優先順位マーキングのコントローラによる延期をイネーブルにする例を示します。

```
(Cisco Controller) >config wlan channel-scan defer-priority 6 enable 30
```


config wlan channel-scan defer-time

ミリ秒単位でチャンネルスキャンの遅延時間を割り当てるには、**config wlan channel-scan defer-time** コマンドを使用します。

config wlan channel-scan defer-time msec wlan_id

| | | |
|------------|-----------------------------------|-----------------------------------|
| 構文の説明 | <i>msecs</i> | ミリ秒単位の遅延時間 (0~60000 ミリ秒)。 |
| | <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| コマンドデフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |
| 使用上のガイドライン | ミリ秒単位の時間値は、WLAN 機器の要件を満たす必要があります。 | |

次に、WLAN ID 50 に対して、40 ミリ秒のスキャン遅延時間を割り当てる例を示します。

```
(Cisco Controller) >config wlan channel-scan defer-time 40 50
```

config wlan custom-web

WLAN の Web 認証ページを設定するには、**config wlan custom-web** コマンドを使用します。

```
config wlan custom-web { {ext-webauth-url ext-webauth-url wlan_id } | {global {enable |
disable}} | {ms-open {enable | disable | url}} | {login-page page-name } |
{loginfailure-page {page-name | none}} | {logout-page {page-name | none}} | {sleep-client
{enable | disable} wlan_id timeout duration} | {webauth-type {internal | customized |
external} wlan_id}}
```

構文の説明

| | |
|--------------------------|-------------------------------------|
| ext-webauth-url | 外部 Web 認証の URL を設定します。 |
| <i>ext-webauth-url</i> | 外部 Web 認証の URL。 |
| <i>wlan_id</i> | WLAN 識別子。デフォルトの範囲は 1 ~ 512 です。 |
| global | WLAN のグローバル ステータスを設定します。 |
| enable | WLAN のグローバル ステータスをイネーブルにします。 |
| disable | WLAN のグローバル ステータスをディセーブルにします。 |
| ms-open | WLAN で ms オープン機能を設定します。 |
| enable | WLAN で ms オープン機能をイネーブルにします。 |
| disable | WLAN で ms オープン機能をディセーブルにします。 |
| url | ms オープン URL を設定します。 |
| login-page | 外部 Web 認証 URL へのログイン ページの名前を設定します。 |
| <i>page-name</i> | 外部 Web 認証 URL へのログイン ページ名。 |
| loginfailure-page | 外部 Web 認証 URL へのログイン失敗ページの名前を設定します。 |
| none | 外部 Web 認証 URL へのログイン失敗ページを設定しません。 |
| logout-page | 外部 Web 認証 URL のログアウト ページの名前を設定します。 |
| sleep-client | WLAN でスリープ クライアント機能を設定します。 |
| timeout | WLAN でスリープ クライアントのタイムアウトを設定します。 |

| | |
|---------------------|---|
| <i>duration</i> | スリープ状態にあるクライアントが強制的に再認証されるまでの、アイドルタイムアウト後の最大時間数（時間単位）。範囲は1～720時間です。デフォルト値は12です。スリープクライアント機能が有効になると、スリープと再起動時間の間、クライアントは同じモビリティグループ内で1つの Cisco WLC から別の Cisco WLC に移動した場合、ログイン資格情報を入力する必要はありません。 |
| webauth-type | WLAN 用の Web 認証のタイプを設定します。 |
| internal | デフォルト ログイン ページを表示します。 |
| customized | カスタマイズされたログイン ページを表示します。 |
| external | 外部 Web サーバにあるログイン ページを表示します。 |

コマンド デフォルト なし

コマンド履歴

| リリース | 変更内容 |
|------|------------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |
| 8.2 | このコマンドが変更され、ms オープン パラメータが追加されました。 |

次に、WLAN で Web 認証タイプを設定する例を示します。

```
Cisco Controller config wlan custom-web webauth-type external
```

config wlan dhcp_server

無線 LAN の内部 DHCP サーバを設定するには、**config wlan dhcp_server** コマンドを使用します。

config wlan dhcp_server {*wlan_id* | **foreignAp**} *ip_address* [**required**]

| | | |
|------------|-------------------|-------------------------------------|
| 構文の説明 | <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| | foreignAp | サードパーティのアクセス ポイントを指定します。 |
| | <i>ip_address</i> | 内部 DHCP サーバの IP アドレス（このパラメータは必須です）。 |
| | required | （任意）DHCP アドレス割り当てが必要かどうかを指定します。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン DHCP の設定には、DHCP サーバのオーバーライドではなく、特定のインターフェイスに割り当てられたプライマリの DHCP アドレスを使用する方式が優先されます。オーバーライドを有効にする場合は、**show wlan** コマンドを使用して、DHCP サーバが WLAN に割り当てられていることを確認できます。

次に、無線 LAN ID 16 の内部 DHCP サーバの IP アドレス 10.10.2.1 を設定する例を示します。

```
(Cisco Controller) >config wlan dhcp_server 16 10.10.2.1
```

config wlan diag-channel

特定の WLAN で診断チャネルのトラブルシューティングを有効にするには、**config wlan diag-channel** コマンドを使用します。

config wlan diag-channel [**enable** | **disable**] *wlan_id*

| | | |
|-----------|----------------|-----------------------------------|
| 構文の説明 | enable | (任意) 無線 LAN の診断チャネルをイネーブルにします。 |
| | disable | (任意) 無線 LAN の診断チャネルをディセーブルにします。 |
| | <i>wlan_id</i> | 無線 LAN 識別子 (1～512)。 |
| コマンドデフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、WLAN ID 1 の無線 LAN の診断チャネルをイネーブルにする例を示します。

```
(Cisco Controller) >config wlan diag-channel enable 1
```

config wlan dtim

802.11 無線ネットワークの Delivery Traffic Indicator Message (DTIM) を設定するには、**config wlan dtim** コマンドを使用します。

config wlan dtim {802.11a | 802.11b} dtim wlan_id

| 構文の説明 | パラメータ | 説明 |
|-------|----------------|--------------------------------|
| | 802.11a | 802.11a 無線ネットワークの DTIM を設定します。 |
| | 802.11b | 802.11b 無線ネットワークの DTIM を設定します。 |
| | <i>dtim</i> | DTIM の値 (1 ~ 255)。 |
| | <i>wlan_id</i> | 設定する WLAN の番号。 |

コマンド デフォルト デフォルトは DTIM 1 です。

| コマンド履歴 | リリース | 変更内容 |
|--------|------|-----------------------------------|
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、DTIM 値 128 および WLAN ID 1 で、802.11a 無線ネットワークの DTIM を設定する例を示します。

```
(Cisco Controller) >config wlan dtim 802.11a 128 1
```

config wlan exclusionlist

無線 LAN の除外リストを設定するには、**config wlan exclusionlist** コマンドを使用します。

```
config wlan exclusionlist {wlan_id [enabled | disabled | time] | foreignAp [enabled | disabled | time] }
```

構文の説明

| | |
|------------------|--|
| <i>wlan_id</i> | 無線 LAN 識別子 (1～512)。 |
| enabled | (任意) 特定の無線 LAN または外部アクセスポイントの除外リストをイネーブルにします。 |
| disabled | (任意) 特定の無線 LAN または外部アクセスポイントの除外リストをディセーブルにします。 |
| <i>time</i> | (任意) 除外リスト タイムアウト (秒)。値 0 は無期限を示します。 |
| foreignAp | サードパーティのアクセス ポイントを指定します。 |

コマンド デフォルト

なし

コマンド履歴

| リリース | 変更内容 |
|------|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン

このコマンドは **config wlan blacklist** コマンドの代わりに使用します。

次に、WLAN ID 1 の除外リストをイネーブルにする例を示します。

```
(Cisco Controller) >config wlan exclusionlist 1 enabled
```

config wlan fabric

WLAN でファブリックを有効または無効にするには、**config wlan fabric** コマンドを使用します。

config wlan fabric { **enable** | **disable** } *wlan-id*

構文の説明

enable WLAN でファブリックをイネーブルにします。

disable WLAN でファブリックをディセーブルにします。

wlan-id WLAN 識別子。

コマンド デフォルト

コマンド モード

コマンド履歴

リリース 変更内容
ス

8.5 このコマンドが導入されました。

使用上のガイドライン

非ファブリック AP はファブリック WLAN では設定されません。

例

次に、WLAN でファブリックをイネーブルにする例を示します。

```
config wlan fabric enable wlan1
```


config wlan fabric acl

ファブリック WLAN のアクセス コントロール リスト (ACL) を設定するには、**config wlan fabric acl** コマンドを使用します。

```
config wlan fabric acl flex-acl-name wlan-id
```

構文の説明

flex acl ACL 名です。
名

wlan-id WLAN 識別
子。

コマンド デフォルト

コマンド モード

コマンド履歴

リリー 変更内容
ス

8.5 このコマンドが導入されました。

使用上のガイドライン

使用する ACL は、Flex ACL テーブルから取得されます。

例

次に、ファブリック WLAN の ACL 名を設定する例を示します。

```
config wlan fabric acl flexACL wlan1
```

config wlan fabric avc-policy

ファブリック WLAN の Application Visibility and Control (AVC) プロファイル名を設定するには、**config wlan fabric avc-policy** コマンドを使用します。

config wlan fabric avc-policy *flex-avc-policy-name* *wlan-id*

| | |
|-------|--|
| 構文の説明 | <i>flex-avc-policy-name</i> AVC ポリシーの名前。 |
| | <i>wlan-id</i> WLAN 識別子。 |

コマンドデフォルト

コマンドモード

| | |
|--------|---------------------|
| コマンド履歴 | リリース 変更内容 |
| | 8.5 このコマンドが導入されました。 |

使用上のガイドライン

例

次に、ファブリック WLAN の ACL プロファイル名を設定する例を示します。

```
config wlan fabric acl AVCpolicy wlan1
```

config wlan fabric encap vxlan

WLAN に仮想拡張 LAN (VXLAN) ネットワーク識別子 (VNID) をマッピングするには、**config wlan fabric encap vxlan** コマンドを使用します。

config wlan fabric encap vxlan*wlan-id*

構文の説明

wlan-id WLAN 識別子。

コマンド デフォルト

コマンド モード

コマンド履歴

リリー 変更内容
ス

8.5 このコマンドが導入されました。

使用上のガイドライン

例

次に、WLAN に VNID をマッピングする例を示します。

```
config wlan fabric encap vxlan wlan1
```

config wlan fabric switch-ip

AP VXLAN トンネルに使用されるファブリック スイッチの IP アドレスを設定するには、**config wlan fabric switch-ip** コマンドを使用します。

config wlan fabric switch-ip *ip-address* *wlan-id*

構文の説明

ip-address スイッチの IP アドレス。

wlan-id WLAN 識別子。

コマンドデフォルト

コマンドモード

コマンド履歴

リリー 変更内容
ス

8.5 このコマンドが導入されました。

使用上のガイドライン

このコマンドはファブリック設定ではオプションであり、主にゲスト AP トンネルに使用されます。ファブリックが有効になっている場合、デフォルトでは AP が接続されているスイッチの IP アドレスが検索されます。IP を 0.0.0.0 に設定すると設定が無効になり、デフォルト設定に戻すことができます。

例

次に、AP VXLAN トンネルに使用されるファブリック スイッチの IP アドレスを設定する例を示します。

```
config wlan fabric switch-ip 10.1.1.1 wlan1
```

config wlan fabric tag

WLAN でセキュリティグループタグ (SGT) を設定するには、**config wlan fabric tag** コマンドを使用します。

```
config wlan fabric tag sgt wlan-id
```

構文の説明

sgt セキュリティグループタグ。

wlan-id WLAN 識別子。

コマンドデフォルト

コマンドモード

コマンド履歴

リリース 変更内容
ス

8.5 このコマンドが導入されました。

使用上のガイドライン

WLAN で SGT を無効にするには、*sgt*変数に 0 を使用します。

SGT は、RADIUS サーバからの認証時に取得すると理想的です。ゲスト向けにこの値を設定できます。デフォルト値は 0 です

例

次に、WLAN に SGT を設定する例を示します。

```
config wlan fabric tag sgt1 wlan1
```

次に、WLAN から SGT を無効にする例を示します。

```
config wlan fabric tag 0 wlan1
```

config wlan fabric vnid

ファブリック WLAN に仮想拡張 LAN (VXLAN) ネットワーク識別子 (VNID) を設定するには、**config wlan fabric vnid** コマンドを使用します。

config wlan fabric vnid *vnid wlan-id*

構文の説明

vnid VXLAN ネットワーク ID。

wlan-id WLAN 識別子。

コマンドデフォルト

コマンドモード

コマンド履歴

リリー 変更内容
ス

16.5 このコマンドが導入されました。

使用上のガイドライン

WLAN から VXLAN のマッピングを削除するには、*vnid*変数に 0 を使用します。

WLAN でのインターフェイスまたは VLAN マッピングは、スイッチで行われます。

例

次に、ファブリック WLAN で VNID を設定する例を示します。

```
config wlan fabric vnid1 wlan1
```

次に、ファブリック WLAN から VNID マッピングを削除する例を示します。

```
config wlan fabric 0 wlan1
```

config wlan fabric avc-policy

ファブリック WLAN の Application Visibility and Control (AVC) プロファイル名を設定するには、**config wlan fabric avc-policy** コマンドを使用します。

```
config wlan fabric avc-policy flex-avc-policy-name wlan-id
```

構文の説明

flex-avc-policy-name AVC ポリシーの名前。

wlan-id WLAN 識別子。

コマンドデフォルト

コマンドモード

コマンド履歴

リリー 変更内容
ス

8.5 このコマンドが導入されました。

使用上のガイドライン

例

次に、ファブリック WLAN の ACL プロファイル名を設定する例を示します。

```
config wlan fabric acl AVCpolicy wlan1
```

config wlan flexconnect ap-auth

ローカルでスイッチされる WLAN で、FlexConnect に関連付けられるクライアントのローカル認証を設定するには、**config wlan flexconnect ap-auth** コマンドを使用します。

config wlan flexconnect ap-auth *wlan_id* { **enable** | **disable** }

| | | |
|-------|----------------|--|
| 構文の説明 | ap-auth | ローカルでスイッチされる WLAN で、FlexConnect に関連付けられたクライアントのローカル認証を設定します。 |
| | <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| | enable | WLAN の AP 認証をイネーブルにします。 |
| | disable | WLAN の AP 認証をディセーブルにします。 |

コマンド デフォルト なし

| コマンド履歴 | リリース | 変更内容 |
|--------|------|-----------------------------------|
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン FlexConnect に関連付けられたクライアントのローカル認証を設定する WLAN で、ローカルスイッチングをイネーブルにする必要があります。

次に、指定した WLAN で FlexConnect に関連付けられているクライアントの認証をイネーブルにする例を示します。

```
(Cisco Controller) >config wlan flexconnect ap-auth 6 enable
```


config wlan flexconnect central-assoc

Cisco WLC でクライアントの再アソシエーションとセキュリティキーのキャッシュを設定するには、**config wlan flexconnect central-assoc** コマンドを使用します。

config wlan flexconnect central-assoc *wlan-id* {**enable** | **disable**}

| 構文の説明 | <i>wlan-id</i> | WLAN の ID |
|-------|----------------|--|
| | enable | Cisco WLC のクライアントの再アソシエーションとセキュリティキーのキャッシュを有効にします。 |
| | disable | Cisco WLC のクライアントの再アソシエーションとセキュリティキーのキャッシュを無効にします。 |

コマンドデフォルト Cisco WLC のクライアント再アソシエーションとセキュリティキー キャッシュは、無効の状態です。

| コマンド履歴 | リリース | 変更内容 |
|--------|------|-----------------|
| | 8.0 | このコマンドが導入されました。 |

使用上のガイドライン この設定の使用例は、高速ローミングを使用した大規模な展開です。

ローカル認証での中央アソシエーションの設定は、WLAN でサポートされません。PMIPv6 トンネルが設定されると、PMIPv6 クライアントからのすべてのデータトラフィックは、Cisco AP から Generic Routing Encapsulation (GRE) トンネルのローカルモビリティアンカー (LM) に転送されます。Cisco AP と Cisco WLC の間の接続が失われた場合、既存の PMIPv6 クライアントのデータトラフィックは、Cisco AP とクライアントの間の接続が失われるまで引き続き送受信されます。AP がスタンドアロンモードの場合、PMIPv6 対応 WLAN では新規クライアントアソシエーションが受け入れられません。

次に、ID が 2 の WLAN で Cisco WLC のクライアントの再アソシエーションとセキュリティキーのキャッシングを有効にする例を示します。

```
(Cisco Controller) >config wlan flexconnect central-assoc 2 enable
```

config wlan flexconnect learn-ipaddr

Cisco WLAN コントローラに対してクライアント IP アドレスの学習を有効または無効にするには、**config wlan flexconnect learn-ipaddr** コマンドを使用します。

config wlan flexconnect learn-ipaddr *wlan_id* {**enable** | **disable**}

構文の説明

| | |
|----------------|---|
| <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| enable | 無線 LAN でクライアント IPv4 アドレスの学習をイネーブルにします。 |
| disable | 無線 LAN でクライアント IPv4 アドレスの学習をディセーブルにします。 |

コマンド デフォルト

config wlan flexconnect local-switching コマンドが無効である場合は、無効になります。**config wlan flexconnect local-switching** コマンドが有効である場合は、有効になります。

コマンド履歴

| リリース | 変更内容 |
|------|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |
| 8.0 | このコマンドは、IPv4 アドレス形式のみをサポートします。 |

使用上のガイドライン

クライアントに Layer 2 暗号化が設定されている場合、コントローラはクライアント IP アドレスを学習できず、定期的にクライアントをドロップします。クライアント IP アドレスの学習を待たずにクライアントの接続を維持するには、このオプションを無効にします。



(注) このコマンドは IPv4 でのみ有効です。



(注) IP アドレスの学習を無効にする機能は、FlexConnect 中央スイッチングではサポートされていません。

次に、WLAN 6 に対してクライアント IP アドレスの学習をディセーブルにする例を示します。

```
(Cisco Controller) >config wlan flexconnect learn-ipaddr disable 6
```

関連コマンド

show wlan

config wlan flexconnect local-switching

FlexConnect WLAN で、ローカルスイッチング、集中管理 DHCP、NAT-PAT、またはオーバーライド DNS オプションを設定するには、**config wlan flexconnect local switching** コマンドを使用します。

```
config wlan flexconnect local-switching wlan_id {enable | disable} { {central-dhcp {enable | disable} nat-pat {enable | disable} } | {override option dns { enable | disable} } }
```

構文の説明

| | |
|---------------------|---|
| <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| enable | FlexConnect WLAN でローカルスイッチングをイネーブルにします。 |
| disable | FlexConnect WLAN でローカルスイッチングをディセーブルにします。 |
| central-dhcp | ローカルスイッチング FlexConnect WLAN で、DHCP パケットの中央スイッチングを設定します。この機能をイネーブルにすると、AP から受信した DHCP パケットは、コントローラに中央でスイッチされ、AP および SSID に基づいて対応する VLAN に転送されます。 |
| enable | FlexConnect WLAN の集中管理 DHCP をイネーブルにします。 |
| disable | FlexConnect WLAN の集中管理 DHCP をディセーブルにします。 |
| nat-pat | ローカルスイッチング FlexConnect WLAN で、ネットワーク アドレス変換 (NAT) とポートアドレス変換 (PAT) を設定します。 |
| enable | FlexConnect WLAN の NAT-PAT をイネーブルにします。 |
| disable | FlexConnect WLAN の NAT-PAT をディセーブルにします。 |
| override | FlexConnect WLAN で DHCP オーバーライドオプションを指定します。 |

| | |
|-------------------|---|
| option dns | FlexConnect WLAN でオーバーライド DNS オプションを指定します。このオプションをオーバーライドすると、クライアントは、コントローラではなく、AP から DNS サーバの IP アドレスを取得します。 |
| enable | FlexConnect WLAN でオーバーライド DNS オプションをイネーブルにします。 |
| disable | FlexConnect WLAN でオーバーライド DNS オプションをディセーブルにします。 |

コマンド デフォルト この機能はディセーブルです。

コマンド履歴

| リリース | 変更内容 |
|------|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |
| 8.0 | このコマンドは、IPv4 アドレス形式のみをサポートします。 |

使用上のガイドライン **config wlan flexconnect local-switching** コマンドを有効にすると、**config wlan flexconnect learn-ipaddr** コマンドもデフォルトで有効にされます。



(注) このコマンドは IPv4 でのみ有効です。



(注) IP アドレスの学習を無効にする機能は、FlexConnect 中央スイッチングではサポートされていません。

次に、ローカルスイッチングで WLAN 6 をイネーブルにし、集中管理 DHCP および NAT-PAT をイネーブルにする例を示します。

```
(Cisco Controller) >config wlan flexconnect local-switching 6 enable central-dhcp enable nat-pat enable
```

次に、WLAN 6 で、オーバーライド DNS オプションをイネーブルにする例を示します。

```
(Cisco Controller) >config wlan flexconnect local-switching 6 override option dns enable
```

config wlan flexconnect vlan-central-switching

ローカルでスイッチされる WLAN で、中央スイッチングを設定するには、**config wlan flexconnect vlan-central-switching** コマンドを使用します。

config wlan flexconnect vlan-central-switching *wlan_id* { **enable** | **disable** }

| | | |
|-----------|----------------|--|
| 構文の説明 | <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| | enable | ローカルでスイッチされるワイヤレス LAN で、中央スイッチングをイネーブルにします。 |
| | disable | ローカルでスイッチされるワイヤレス LAN で、中央スイッチングをディセーブルにします。 |
| コマンドデフォルト | 中央スイッチングは無効です。 | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン VLAN の中央スイッチングをイネーブルにするには、Flexconnect のローカルスイッチングをイネーブルにする必要があります。WLAN 中央スイッチングをイネーブルにすると、WLAN がローカル IEEE 802.1Q リンク上で設定されている場合、アクセスポイントはトラフィックをローカルにブリッジします。アクセスポイントに VLAN が設定されていない場合、AP は、トンネルを使用してコントローラーにトラフィックを戻し、コントローラーは対応する VLAN にトラフィックをブリッジします。

WLAN 中央スイッチングは、以下をサポートしていません。

- FlexConnect ローカル認証。
- ローカルスイッチングクライアントのレイヤ 3 ローミング。

次に、WLAN 6 で中央スイッチングをイネーブルにする例を示します。

```
(Cisco Controller) >config wlan flexconnect vlan-central-switching 6 enable
```

config wlan flow

WLAN に NetFlow モニタを関連付けるには、**config wlan flow** コマンドを使用します。

```
config wlan flow wlan_id monitor monitor_name {enable | disable}
```

| | | |
|------------|---------------------|--|
| 構文の説明 | wlan_id | 1 ~ 512 の無線 LAN 識別子（両端の値を含む）。 |
| | monitor | NetFlow モニタを設定します。 |
| | monitor_name | NetFlow モニタの名前。モニタ名は最大 32 文字の英数字で、大文字と小文字を区別します。モニタ名にスペースを含めることはできません。 |
| | enable | WLAN と NetFlow モニタを関連付けます。 |
| | disable | WLAN から NetFlow モニタの関連付けを解除します。 |
| コマンド デフォルト | | なし |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン **config flow** コマンドを使用して、新しい NetFlow モニタを作成できます。

次に、WLAN と NetFlow モニタを関連付ける例を示します。

```
(Cisco Controller) >config wlan flow 5 monitor monitor1 enable
```

config wlan hotspot

WLAN のホットスポットを設定するには、**config wlan hotspot** コマンドを使用します。

config wlan hotspot {**clear-all** *wlan_id* | **dot11u** | **hs2** | **msap**}

構文の説明

clear-all WLAN のホットスポット設定をクリアします。

wlan_id 1 ~ 512 の無線 LAN 識別子。

dot11u WLAN の 802.11u ホットスポットを設定します。

hs2 WLAN の HotSpot2 を設定します。

msap WLAN の Mobility Services Advertisement Protocol (MSAP) を設定します。

コマンドデフォルト

なし

コマンド履歴

| リリース | 変更内容 |
|------|------|
|------|------|

| | |
|-----|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |
|-----|-----------------------------------|

使用上のガイドライン

最大 32 ホットスポット WLAN を設定できます。

次に、WLAN に HotSpot2 を設定する例を示します。

```
(Cisco Controller) >config wlan hotspot hs2 enable 2
```

config wlan hotspot dot11u

WLAN の 802.11u ホットスポットを設定するには、**config wlan hotspot dot11u** コマンドを使用します。

config wlan hotspot dot11u {**3gpp-info** | **auth-type** | **enable** | **disable** | **domain** | **hessid** | **ipaddr-type** | **nai-realm** | **network-type** | **roam-oi**}

| 構文の説明 | 3gpp-info | 3GPP セルラー ネットワーク情報を設定します。 |
|------------|--------------|---|
| | auth-type | ネットワーク認証タイプを設定します。 |
| | disable | ホットスポットのプロファイルで、802.11u をディセーブルにします。 |
| | domain | ドメインを設定します。 |
| | enable | ホットスポットのプロファイルで、802.11u をイネーブルにします。IEEE 802.11u は、モバイルまたはローミングパートナーのホットスポットで、802.1X デバイスの自動 WLAN オフロードをイネーブルにします。 |
| | hessid | Homogenous Extended Service Set Identifier (HESSID) を設定します。HESSID は、ネットワークを一意に識別する 6 オクテットの MAC アドレスです。 |
| | ipaddr-type | IPv4 アドレスの可用性タイプを設定します。 |
| | nai-realm | 802.11u 対応 WLAN のレルムを設定します。 |
| | network-type | 802.11u ネットワーク タイプおよびインターネット アクセスを設定します。 |
| | roam-oi | ローミング コンソーシアムの組織識別子 (OI) のリストを設定します。 |
| コマンド デフォルト | | なし。 |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |
| | 8.0 | このコマンドは、IPv4 アドレス形式のみをサポートします。 |

次に、ホットスポット プロファイルで 802.11u をイネーブルにする例を示します。

```
(Cisco Controller) >config wlan hotspot dot11u enable 6
```


config wlan hotspot dot11u 3gpp-info

802.11u ホットスポット WLAN で 3GPP セルラー ネットワーク情報を設定するには、**config wlan hotspot dot11u 3gpp-info** コマンドを使用します。

config wlan hotspot dot11u 3gpp-info {**add** | **delete**} *index country_code network_code wlan_id*

構文の説明

| | |
|---------------------|---|
| add | モバイルセルラー ネットワーク情報を追加します。 |
| delete | モバイルセルラー ネットワーク情報を削除します。 |
| <i>index</i> | セルラー インデックス。指定できる範囲は 1 ~ 32 です。 |
| <i>country_code</i> | 2 進化 10 進数 (BCD) 形式のモバイル国番号 (MCC)。国番号は最大 3 文字です。たとえば、米国の MCC は 310 です。 |
| <i>network_code</i> | BCD形式のモバイルネットワークコード (MNC)。モバイル国番号 (MCC) と組み合わせて、MNC は携帯電話の運営事業者または通信事業者を一意に識別するために使用されます。ネットワーク コードは最大 3 文字です。たとえば、T-Mobile の MNC は 026 です。 |
| <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |

コマンドデフォルト

なし

コマンド履歴

| リリース | 変更内容 |
|------|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン

サポートされているモバイル ネットワーク コードの数は、WLAN あたり 32 です。

次に、WLAN の 3GPP セルラー ネットワーク情報を設定する例を示します。

```
(Cisco Controller) >config wlan hotspot dot11u 3gpp-info add
```

config wlan hotspot dot11u auth-type

802.11u ホットスポット WLAN のネットワーク認証タイプを設定するには、**config wlan hotspot dot11u auth-type** コマンドを使用します。

config wlan hotspot dot11u auth-type network-auth wlan_id

構文の説明

network-auth WLAN で設定するネットワーク認証。使用できる値は、次のとおりです。

- 0 : 条件に同意。
- 1 : オンライン登録。
- 2 : HTTP/HTTPS リダイレクション。
- 3 : DNS リダイレクション。
- 4 : 適用されない

wlan_id 1 ~ 512 の無線 LAN 識別子。

コマンド デフォルト

なし

コマンド履歴

| リリース | 変更内容 |
|------|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン

DNS リダイレクション オプションは、リリース 7.3 ではサポートされていません。

次に 802.11u ホットスポット WLAN のネットワーク認証タイプとして、HTTP/HTTPS リダイレクションを設定する例を示します。

```
(Cisco Controller) >config wlan hotspot dot11u auth-type 2 1
```

config wlan hotspot dot11u disable

WLAN の 802.11u ホットスポットをディセーブルにするには、**config wlan hotspot dot11u disable** コマンドを使用します。

config wlan hotspot dot11u disable *wlan_id*

構文の説明

wlan_id 1～512 の無線 LAN 識別子。

コマンド デフォルト

なし

コマンド履歴

| リリース | 変更内容 |
|------|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、WLAN の 802.11u ホットスポットをディセーブルにする例を示します。

```
(Cisco Controller) >config wlan hotspot dot11u disable 6
```

config wlan hotspot dot11u domain

802.11 アクセス ネットワークで動作しているドメインを設定するには、**config wlan hotspot dot11u domain** コマンドを使用します。

config wlan hotspot dot11u domain { **add** *wlan_id domain-index domain_name* | **delete** *wlan_id domain-index* | **modify** *wlan_id domain-index domain_name* }

| | | |
|------------|---------------------|---|
| 構文の説明 | add | ドメインを追加します。 |
| | <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| | <i>domain-index</i> | 1~32 のドメイン インデックス。 |
| | <i>domain_name</i> | ドメイン名。ドメイン名は最大255文字の英数字で、大文字と小文字を区別します。 |
| | delete | ドメインを削除します。 |
| | modify | ドメインを変更します。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、802.11 アクセス ネットワークでドメインを追加する例を示します。

```
(Cisco Controller) >config wlan hotspot dot11u domain add 6 30 domain1
```

config wlan hotspot dot11u enable

WLAN の 802.11u ホットスポットをイネーブルにするには、**config wlan hotspot dot11u enable** コマンドを使用します。

config wlan hotspot dot11u enable *wlan_id*

構文の説明

wlan_id 1～512 の無線 LAN 識別子。

コマンド デフォルト

なし

コマンド履歴

| リリース | 変更内容 |
|------|------|
|------|------|

| | |
|-----|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |
|-----|-----------------------------------|

次に、WLAN の 802.11u ホットスポットをイネーブルにする例を示します。

```
(Cisco Controller) >config wlan hotspot dot11u enable 6
```

config wlan hotspot dot11u hessid

802.11u ホットスポット WLAN で Homogenous Extended Service Set Identifier (HESSID) を設定するには、**config wlan hotspot dot11u hessid** コマンドを使用します。

config wlan hotspot dot11u hessid *hessid wlan_id*

| 構文の説明 | <p><i>hessid</i> HESSID として設定できる MAC アドレス。HESSID は、ネットワークを一意に識別する 6 オクテットの MAC アドレスです。たとえば、WLAN の Basic Service Set Identification (BSSID) は、HESSID として使用できます。</p> | | | | |
|------------|---|------|------|-----|-----------------------------------|
| | <p><i>wlan_id</i> 1 ~ 512 の無線 LAN 識別子。</p> | | | | |
| コマンド デフォルト | なし | | | | |
| コマンド履歴 | <table border="1"> <thead> <tr> <th data-bbox="370 808 609 850">リリース</th> <th data-bbox="609 808 1497 850">変更内容</th> </tr> </thead> <tbody> <tr> <td data-bbox="370 850 609 905">7.6</td> <td data-bbox="609 850 1497 905">このコマンドは、リリース 7.6 以前のリリースで導入されました。</td> </tr> </tbody> </table> | リリース | 変更内容 | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |
| リリース | 変更内容 | | | | |
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 | | | | |

次に 802.11u ホットスポット WLAN の HESSID を設定する例を示します。

```
(Cisco Controller) >config wlan hotspot dot11u hessid 00:21:1b:ea:36:60 6
```

config wlan hotspot dot11u ipaddr-type

802.11u ホットスポット WLAN で利用できる IP アドレスのタイプを設定するには、**config wlan hotspot dot11u ipaddr-type** コマンドを使用します。

```
config wlan hotspot dot11u ipaddr-type IPv4Type {0 - 7} IPv6Type {0 - 2} wlan_id
```

構文の説明

IPv4Type IPv4 タイプのアドレス。次のいずれかの値を入力します。

- 0 : IPv4 アドレスは使用できません。
- 1 : パブリック IPv4 アドレスが使用できます。
- 2 : ポート制限付き IPv4 アドレスが使用できます。
- 3 : シングル NAT 対応プライベート IPv4 アドレスが使用できます。
- 4 : ダブル NAT 対応プライベート IPv4 アドレスが使用できます。
- 5 : ポート制限付き IPv4 アドレスおよびシングル NAT 対応 IPv4 アドレスが使用できます。
- 6 : ポート制限付き IPv4 アドレスおよびダブル NAT 対応 IPv4 アドレスが使用できます。
- 7 : IPv4 アドレスが使用できるかどうか不明です。

IPv6Type IPv6 タイプのアドレス。次のいずれかの値を入力します。

- 0 : IPv6 アドレスは使用できません。
- 1 : IPv6 アドレスは使用できます。
- 2 : IPv6 アドレスが使用できるかどうか不明です。

wlan_id 1 ~ 512 の無線 LAN 識別子。

コマンドデフォルト

IPv4 タイプのアドレスのデフォルト値は 1 です。

コマンド履歴

| リリース | 変更内容 |
|------|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |
| 8.0 | このコマンドは、IPv4 アドレス形式のみをサポートします。 |

次に 802.11u ホットスポット WLAN の IP アドレスの可用性タイプを設定する例を示します。

```
(Cisco Controller) >config wlan hotspot dot11u ipaddr-type 6 2 6
```

関連コマンド

show wlan

config wlan hotspot dot11u nai-realm

WLAN の 802.11u ホットスポットのレルムを設定するには、**config wlan hotspot dot11u nai-realm** コマンドを使用します。

```
config wlan hotspot dot11u nai-realm {add | delete | modify} {auth-method wlan_id realm-index eap-index auth-index auth-method auth-parameter | eap-method wlan_id realm-index eap-index eap-method | realm-name wlan_id realm-index realm}
```

構文の説明

| | |
|-----------------------|--|
| add | レルムを追加します。 |
| delete | レルムを削除します。 |
| modify | レルムを変更します。 |
| auth-method | 使用する認証方式を指定します。 |
| <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| <i>realm-index</i> | レルム インデックス。指定できる範囲は 1 ~ 32 です。 |
| <i>eap-index</i> | EAP インデックス。指定できる範囲は 1 ~ 4 です。 |
| <i>auth-index</i> | 認証インデックス値。値の範囲は 1 ~ 10 です。 |
| <i>auth-method</i> | 使用する認証方式。指定できる範囲は 1 ~ 4 です。次のオプションを使用できます。 <ul style="list-style-type: none"> • 1 : 非 EAP 内部認証方式 • 2 : 内部認証タイプ • 3—クレデンシヤル タイプ • 4 : トンネル EAP 方式のクレデンシヤル タイプ |
| <i>auth-parameter</i> | 使用する認証パラメータ。この値は、使用する認証方式によって異なります。詳細については、次の表を参照してください。 |
| eap-method | 使用される拡張認証プロトコル (EAP) 方式を指定します。 |

eap-method EAP 方式。有効な範囲は 0 ~ 7 です。次のオプションを使用できます。

- 0 : 適用されない
- 1 : Lightweight Extensible Authentication Protocol (LEAP)
- 2 : Protected EAP (PEAP)
- 3 : EAP-Transport Layer Security (EAP-TLS)
- 4 : EAP-FAST (セキュア トンネリングを介したフレキシブル認証)
- 5 : EAP for GSM Subscriber Identity Module (EAP-SIM)
- 6 : EAP-Tunneled Transport Layer Security (EAP-TTLS)
- 7 : EAP for UMTS Authentication and Key Agreement (EAP-AKA)

realm-name レルムの名前を指定します。

realm レルムの名前。レルム名は、RFC 4282 に準拠している必要があります。たとえば、Cisco のようになります。レルム名は最大 255 文字の英数字で、大文字と小文字を区別します。

コマンドデフォルト なし

コマンド履歴

| リリース | 変更内容 |
|------|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン 次の表は、認証パラメータがリストされています。

表 5: 認証パラメータ

| 非 EAP 内部方式 (1) | 内部 EAP 認証方式のタイプ (2) | クレデンシャルタイプ (3) /Tunneled EAP クレデンシャルタイプ (4) |
|---|---------------------|---|
| 0 : 予約済 | 1 : LEAP | 1 : SIM |
| 1 : Password Authentication Protocol (PAP) | 2 : PEAP | 2 : USIM |
| 2 : Challenge-Handshake Authentication Protocol (CHAP) | 3 : EAP-TLS | 3 : NFC セキュア エlement |
| 3 : Microsoft Challenge Handshake Authentication Protocol (MS-CHAP) | 4 : EAP-FAST | 4 : ハードウェア トークン |
| 4 : MSCHAPV2 | 5 : EAP-SIM | 5 : ソフト トークン |
| | 6 : EAP-TTLS | 6 : 証明書 |
| | 7 : EAP-AKA | 7 : ユーザ名/パスワード |
| | | 8 : Reserver |
| | | 9 : 匿名 |
| | | 10 : ベンダー固有 |

次に、WLAN 4 で Tunneled EAP Method Credential 認証方式を追加する例を示します。

```
(Cisco Controller) >config wlan hotspot dot11u nai-realm add auth-method 4 10 3 5 4 6
```

config wlan hotspot dot11u network-type

802.11u ホットスポット WLAN のネットワーク タイプとインターネットの可用性を設定するには、**config wlan hotspot dot11u network-type** コマンドを使用します。

config wlan hotspot dot11u network-type *wlan_id network-type internet-access*

| 構文の説明 | <p><i>wlan_id</i> 1 ~ 512 の無線 LAN 識別子。</p> <hr/> <p><i>network-type</i> ネットワーク タイプ。使用できるオプションは、次のとおりです。</p> <ul style="list-style-type: none"> • 0 : プライベート ネットワーク • 1 : ゲスト アクセスを使用したプライベート ネットワーク • 2 : 有料のパブリック ネットワーク • 3 : 無料のパブリック ネットワーク • 4 : 個人のデバイス ネットワーク • 5 : 緊急サービス専用ネットワーク • 14 : テストまたは実験用 • 15 : ワイルドカード <hr/> <p><i>internet-access</i> インターネット可用性のステータス。0 の値は、インターネットを使用できないこと、1 はインターネットを使用できることを示します。</p> | | | | |
|------------|--|------|------|-----|-----------------------------------|
| コマンド デフォルト | なし | | | | |
| コマンド履歴 | <table border="1"> <thead> <tr> <th data-bbox="430 1312 532 1339">リリース</th> <th data-bbox="651 1312 753 1339">変更内容</th> </tr> </thead> <tbody> <tr> <td data-bbox="430 1354 461 1381">7.6</td> <td data-bbox="651 1354 1422 1381">このコマンドは、リリース 7.6 以前のリリースで導入されました。</td> </tr> </tbody> </table> | リリース | 変更内容 | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |
| リリース | 変更内容 | | | | |
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 | | | | |

次に 802.11u ホットスポット WLAN でネットワーク タイプとインターネットの可用性を設定する例を示します。

```
(Cisco Controller) >config wlan hotspot dot11u network-type 2 1
```

config wlan hotspot dot11u roam-oi

802.11u ホットスポット WLAN でローミング コンソーシアムの組織識別子 (OI) のリストを設定するには、**config wlan hotspot dot11u roam-oi** コマンドを使用します。

config wlan hotspot dot11u roam-oi { **add** *wlan_id oi-index oi is-beacon* | **modify** *wlan_id oi-index oi is-beacon* | **delete** *wlan_id oi-index* }

| | | |
|------------|------------------|---|
| 構文の説明 | add | OI を追加します。 |
| | <i>wlan-id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| | <i>oi-index</i> | 1~32 の範囲のインデックス。 |
| | <i>oi</i> | 有効な 6 桁の 16 進数、長さを 6 バイトにする必要がある番号。たとえば、004096 または AABBDf とします。 |
| | <i>is-beacon</i> | ビーコンに OI を追加するために使用するビーコンフラグ。0 はディセーブル、1 がイネーブルであることを示します。フラグが設定された WLAN に対して、最大 3 つの OI を追加できます。 |
| | modify | OI を変更します。 |
| | delete | OI を削除します。 |
| コマンド デフォルト | | なし。 |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、ローミング コンソーシアムの OI リストを設定する例を示します。

```
(Cisco Controller) >config wlan hotspot dot11u roam-oi add 4 10 004096 1
```

config wlan hotspot hs2

HotSpot2 パラメータを設定するには、**config wlan hotspot hs2** コマンドを使用します。

```
config wlan hotspot hs2 { disable wlan_id | enable wlan_id | operator-name { add wlan_id index operator_name language-code | delete wlan_id index | modify wlan_id index operator_name language-code } | port-config { add wlan_id port_config_index ip-protocol port-number status | delete wlan_id port-config-index | modify wlan_id port-config-index ip-protocol port-number status } | wan-metrics wlan_id link-status symet-link downlink-speed uplink-speed }
```

構文の説明

| | |
|--------------------------|--|
| disable | HotSpot2 をディセーブルにします。 |
| <i>wlan-id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| enable | HotSpot2 をイネーブルにします。 |
| operator-name | 802.11 オペレータの名前を指定します。 |
| add | WLAN 設定に、オペレータ名、ポート設定、または WAN メトリック パラメータを追加します。 |
| <i>index</i> | オペレータのインデックス。指定できる範囲は 1 ~ 32 です。 |
| <i>operator-name</i> | オペレータの名前。 |
| <i>language-code</i> | 使用する言語。言語を定義する ISO-14962-1997 エンコード文字列。この文字列は 3 文字の言語コードです。言語の最初の 3 文字を英語で入力します (たとえば、英語の場合は eng)。 |
| delete | WLAN からオペレータ名、ポート設定、または WAN メトリック パラメータを削除します。 |
| modify | WLAN のオペレータ名、ポート設定、または WAN メトリック パラメータを変更します。 |
| port-config | ポート設定値を設定します。 |
| <i>port_config_index</i> | ポート設定インデックス。指定できる範囲は 1 ~ 32 です。デフォルト値は 1 です。 |

| | |
|--------------------|--|
| <i>ip-protocol</i> | <p>使用するプロトコル。このパラメータは、頻繁に使用される通信プロトコルとポートの接続状態に関する情報を提供します。次のオプションを使用できます。</p> <p>1 : ICMP</p> <p>6 : FTP/SSH/TLS/PPTP-VPN/VoIP</p> <p>17 : IKEv2 (IPSec-VPN/VoIP/ESP)</p> <p>50 : ESP (IPSec-VPN)</p> |
| <i>port-number</i> | <p>ポート番号。次のオプションを使用できます。</p> <p>0 : ICMP/ESP (IPSec-VPN)</p> <p>20 : FTP</p> <p>22 : SSH</p> <p>443 : TLS-VPN</p> <p>500 : IKEv2</p> <p>1723 : PPTP-VPN</p> <p>4500 : IKEv2</p> <p>5060 : VoIP</p> |
| <i>status</i> | <p>IP ポートのステータス。次のオプションを使用できます。</p> <p>0 : クローズ</p> <p>1 : オープン</p> <p>2 : 不明</p> |
| wan-metrics | <p>WAN メトリックを設定します。</p> |
| <i>link-status</i> | <p>リンク ステータス。次のオプションを使用できます。</p> <ul style="list-style-type: none"> • 0 : 不明 • 1 : リンク アップ • 2 : リンク ダウン • 3 : テスト状態のリンク |

| | |
|-----------------------|---|
| <i>symet-link</i> | 対称的なリンク ステータス。次のオプションを使用できます。 <ul style="list-style-type: none"> • 0 : リンク速度はアップリンクとダウンリンクで異なります (ADSL など)。 • 1 : リンク速度はアップリンクとダウンリンクで同じです (DS1 など)。 |
| <i>downlink-speed</i> | kbps 単位の WAN バックホール リンクのダウンリンク速度。最大値は 4,194,304 kbps です。 |
| <i>uplink-speed</i> | kbps 単位の WAN バックホール リンクのアップリンク速度。最大値は 4,194,304 kbps です。 |

コマンド デフォルト なし

コマンド履歴

| リリース | 変更内容 |
|------|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、WAN メトリック パラメータの設定例を示します。

```
(Cisco Controller) >config wlan hotspot hs2 wan-metrics add 345 1 0 3333
```

config wlan hotspot hs2 domain-id

ドメイン ID を設定するには、WLAN コンフィギュレーションモードで **config wlan hotspot hs2 domain-id** コマンドを使用します。

config wlan hotspot hs2 domain-id *wlan-id domain-id*

構文の説明

wlan-id WLAN ID 番号。1 ~ 512 の値を入力します。

domain-id ドメイン ID。0 ~ 65535 の範囲で値を入力します。

コマンド デフォルト

ドメイン ID が設定されていません。

コマンド モード

WLAN の設定

コマンド履歴

| リリース | 変更内容 |
|------|-----------------|
| リリース | このコマンドが導入されました。 |
| 8.2 | |

次に、ドメイン ID を設定する例を示します。

```
Cisco Controller > config wlan hotspot hs2 domain-id 12 2
```


config wlan hotspot hs2 osu legacy-ssid

オンライン サインアップ (OSU) サービス セット 識別子 (SSID) 名を設定するには、WLAN コンフィギュレーション モードで **config wlan hotspot hs2 osu legacy-ssid** コマンドを使用します。

config wlan hotspot hs2 osu legacy-ssid *wlan-id ssid-name*

構文の説明

wlan-id WLAN ID 番号。1 ~ 512 の値を入力します。

ssid-name SSID 名。

コマンド デフォルト

OSU SSID 名が設定されていません。

コマンド モード

WLAN の設定

コマンド履歴

リリース 変更内容

リリース このコマンドが導入されました。
8.2

次に、OSU SSID 名を設定する例を示します。

```
Cisco Controllor > config wlan hotspot hs2 osu legacy-ssid 12 cisco
```

config wlan hotspot hs2 osu sp create

オンラインサインアップ (OSU) サービスプロバイダ名を作成するには、WLAN コンフィギュレーションモードで **config wlan hotspot hs2 osu sp create** コマンドを使用します。

config wlan hotspot hs2 osu sp create *wlan-id osu-index lang-code* **ascii/hex** *friendly-name* [*description*]

| 構文の説明 | |
|----------------------|--|
| <i>wlan-id</i> | WLAN ID 番号。1 ~ 512 の値を入力します。 |
| <i>osu-index</i> | OSU インデックス。1 ~ 16 の範囲で値を入力します。 |
| <i>lang-code</i> | 言語コード。ISO-639 の 2 文字または 3 文字のコードを入力します (たとえば、英語の場合は <i>eng</i>) 。 |
| ascii/hex | テキスト形式を指定します (ASCII または 16 進数) 。 |
| <i>friendly-name</i> | サービスプロバイダ名。最大文字数は 252 文字です。 |
| <i>description</i> | (任意) サーバの説明。最大文字数は 252 文字です。 |

コマンド デフォルト OSU サービスプロバイダ名が設定されていません。

コマンド モード WLAN の設定

| コマンド履歴 | リリース | 変更内容 |
|--------|------|-----------------|
| | リリース | このコマンドが導入されました。 |
| | 8.2 | |

次に、OSU サービスプロバイダ名を設定する例を示します。

```
Cisco Controller > config wlan hotspot hs2 osu sp create 12 2 eng ascii cisco server-1
```

config wlan hotspot hs2 osu sp delete

オンラインサインアップ (OSU) サービス プロバイダーを削除するには、**config wlan hotspot hs2 osu sp delete** コマンドを使用します。

config wlan hotspot hs2 osu sp delete *wlan-id* *index* *lang-code*

構文の説明

wlan-id WLAN ID 番号。1 ～ 512 の値を入力します。

index OSU インデックス。1 ～ 16 の範囲で値を入力します。

lang-code 言語コード。ISO-639 の 2 文字または 3 文字のコードを入力します (たとえば、英語の場合は *eng*) 。

コマンド デフォルト

OSU サービス プロバイダーが設定されます。

コマンド モード

WLAN の設定

コマンド履歴

リリース 変更内容

リリース このコマンドが導入されました。
8.2

次に、OSU サービス プロバイダーを削除する例を示します。

```
Cisco Controller > config wlan hotspot hs2 osu sp delete 12 2 eng
```

config wlan hotspot hs2 osu sp icon-file add

特定の WLAN でオンラインサインアップ (OSU) アイコンファイルを設定するには、WLAN コンフィギュレーションモードで **config wlan hotspot hs2 osu sp icon-file add** コマンドを使用します。

config wlan hotspot hs2 osu sp icon-file add *wlan-id* *osu-index* *icon-filename*

構文の説明

| | |
|----------------------|--------------------------------|
| <i>wlan-id</i> | WLAN ID 番号。1 ~ 512 の値を入力します。 |
| <i>osu-index</i> | OSU インデックス。1 ~ 16 の範囲で値を入力します。 |
| <i>icon-filename</i> | アイコンのファイル名です。 |

コマンド デフォルト

OSU アイコン ファイルが設定されていません。

コマンド モード

WLAN の設定

コマンド履歴

| リリース | 変更内容 |
|------|------------------------|
| リリース | このコマンドが導入されました。 8.2 |

使用上のガイドライン

このコマンドを使用する前に、**config icon file-info** コマンドを使用してアイコン パラメータを設定します。

次に、WLAN で OSU アイコン ファイルを設定する例を示します。

```
Cisco Controller > config wlan hotspot hs2 osu sp icon-file add 12 2 test-icon
```

config wlan hotspot hs2 osu sp icon-file delete

WLAN からオンラインサインアップ (OSU) アイコンファイルを削除するには、WLAN コンフィギュレーションモードで **config wlan hotspot hs2 osu sp icon-file delete** コマンドを使用します。

config wlan hotspot hs2 osu sp icon-file delete *wlan-id* *osu-index* *icon-filename*

構文の説明

wlan-id WLAN ID 番号。1 ~ 512 の値を入力します。

osu-index OSU インデックス。1 ~ 16 の範囲で値を入力します。

icon-filename アイコンのファイル名です。

コマンド デフォルト

OSU アイコン ファイルが設定されます。

コマンド モード

WLAN の設定

コマンド履歴

| リリース | 変更内容 |
|------|------|
|------|------|

| | |
|------|------------------------|
| リリース | このコマンドが導入されました。 8.2 |
|------|------------------------|

次に、WLAN から OSU アイコン ファイルを削除する例を示します。

```
Cisco Controller > config wlan hotspot hs2 osu sp icon-file delete 12 2 test-icon
```

config wlan hotspot hs2 osu sp method add

オンラインサインアップ (OSU) 方法リストを設定するには、WLAN コンフィギュレーションモードで **config wlan hotspot hs2 osu sp method add** コマンドを使用します。

config wlan hotspot hs2 osu sp method add *wlan-id osu-index method-primary method-secondary*

| | | |
|------------|-------------------------|--|
| 構文の説明 | <i>wlan-id</i> | WLAN ID 番号。1 ~ 512 の値を入力します。 |
| | <i>osu-index</i> | OSU インデックス。1 ~ 16 の範囲で値を入力します。 |
| | <i>method-primary</i> | プライマリ OSU エンコード方法。有効な値は、 oma-dm または soap-xml です。 |
| | <i>method-secondary</i> | (オプション) セカンダリ OSU エンコード方法。有効な値は、 oma-dm または soap-xml です。 |
| コマンド デフォルト | OSU 方法リストが設定されていません。 | |
| コマンド モード | WLAN の設定 | |
| コマンド履歴 | リリース | 変更内容 |
| | リリース | このコマンドが導入されました。 8.2 |

次に、OSU 方法リストを設定する例を示します。

```
Cisco Controller > config wlan hotspot hs2 osu sp method add 12 2 oma-dm oma-dm
```

config wlan hotspot hs2 osu sp method delete

オンラインサインアップ (OSU) 方法リストを削除するには、WLAN コンフィギュレーションモードで **config wlan hotspot hs2 osu sp method delete** コマンドを使用します。

config wlan hotspot hs2 osu sp method delete *wlan-id osu-index method*

構文の説明

wlan-id WLAN ID 番号。1 ～ 512 の値を入力します。

osu-index OSU インデックス。1 ～ 16 の範囲で値を入力します。

method OSU エンコード方法。有効な値は、**oma dm**または**soap xml**です。

コマンドデフォルト

OSU 方法リストが設定されます。

コマンドモード

WLAN の設定

コマンド履歴

| リリース | 変更内容 |
|------|------|
|------|------|

| | |
|------|-----------------|
| リリース | このコマンドが導入されました。 |
| 8.2 | |

次に、OSU 方法リストを削除する例を示します。

```
Cisco Controller > config wlan hotspot hs2 osu sp method delete 12 2 oma-dm
```

config wlan hotspot hs2 osu sp nai add

オンラインサインアップ (OSU) ネットワーク アクセス識別子 (NAI) を作成するには、WLAN コンフィギュレーション モードで **config wlan hotspot hs2 osu sp nai add** コマンドを使用します。

config wlan hotspot hs2 osu sp nai add *wlan-id osu-index nai*

構文の説明

wlan-id WLAN ID 番号。1 ~ 512 の値を入力します。

osu-index OSU インデックス。1 ~ 16 の範囲で値を入力します。

nai OSU サーバの NAI。255 文字以内で名前を入力します。

コマンド デフォルト

OSU NAI が設定されていません。

コマンド モード

WLAN の設定

コマンド履歴

リリース 変更内容

リリース このコマンドが導入されました。
8.2

次に、OSU NAI を設定する例を示します。

```
Cisco Controller > config wlan hotspot hs2 osu sp nai add 12 2 nai-1
```


config wlan hotspot hs2 osu sp nai delete

オンライン サインアップ (OSU) ネットワーク アクセス識別子 (NAI) を削除するには、WLAN コンフィギュレーションモードで **config wlan hotspot hs2 osu sp nai delete** コマンドを使用します。

config wlan hotspot hs2 osu sp nai delete *wlan-id osu-index*

| 構文の説明 | <i>wlan-id</i> WLAN ID 番号。1 ~ 512 の値を入力します。 | | | | |
|------------|--|------|------|----------|-----------------|
| | <i>osu-index</i> OSU インデックス。1 ~ 16 の範囲で値を入力します。 | | | | |
| コマンド デフォルト | OSU NAI が設定されます。 | | | | |
| コマンド モード | WLAN の設定 | | | | |
| コマンド履歴 | <table><thead><tr><th>リリース</th><th>変更内容</th></tr></thead><tbody><tr><td>リリース 8.2</td><td>このコマンドが導入されました。</td></tr></tbody></table> | リリース | 変更内容 | リリース 8.2 | このコマンドが導入されました。 |
| リリース | 変更内容 | | | | |
| リリース 8.2 | このコマンドが導入されました。 | | | | |

次に、OSU NAI を削除する例を示します。

```
Cisco Controllor > config wlan hotspot hs2 osu sp nai delete 12 2
```

config wlan hotspot hs2 osu sp uri add

オンラインサインアップ (OSU) URI を作成するには、WLAN コンフィギュレーション モードで **config wlan hotspot hs2 osu sp uri add** コマンドを使用します。

config wlan hotspot hs2 osu sp uri add *wlan-id osu-index uri*

構文の説明

wlan-id WLAN ID 番号。1 ~ 512 の値を入力します。

osu-index OSU インデックス。1 ~ 16 の範囲で値を入力します。

uri OSU サーバ名。最大 255 文字の Uniform Resource Identifier (URI) を入力します。

コマンド デフォルト

OSU URI が設定されていません。

コマンド モード

WLAN の設定

コマンド履歴

リリース 変更内容

リリース このコマンドが導入されました。
8.2

次に、OSU NAI を作成する例を示します。

```
Cisco Controller > config wlan hotspot hs2 osu sp uri add 12 2 server
```

config wlan hotspot hs2 osu sp uri delete

オンラインサインアップ (OSU) URI を削除するには、**config wlan hotspot hs2 osu sp uri delete** コマンドを使用します。

config wlan hotspot hs2 osu sp uri delete *wlan-id* *osu-index*

構文の説明

wlan-id WLAN ID 番号。1～512 の値を入力します。

osu-index OSU インデックス。1～16 の範囲で値を入力します。

コマンド デフォルト

OSU URI が設定されています。

コマンド モード

WLAN の設定

コマンド履歴

| リリース | 変更内容 |
|------|------|
|------|------|

| | |
|------|------------------------|
| リリース | このコマンドが導入されました。 8.2 |
|------|------------------------|

次に、OSU URI を削除する例を示します。

```
Cisco Controller > config wlan hotspot hs2 osu sp uri delete 12 2
```

config wlan hotspot hs2 wan-metrics downlink

ダウンリンク WAN メトリックを設定するには、WLAN コンフィギュレーション モードで **config wlan hotspot hs2 wan-metrics downlink** コマンドを使用します。

config wlan hotspot hs2 wan-metrics downlink *wlan-id dlink-speed dlink-load*

構文の説明

wlan-id WLAN ID 番号。1 ~ 512 の値を入力します。

dlink-speed kbps 単位の WAN バックホールリンクの速度。範囲は 0 ~ 4,294,967,295 です。

dlink-load WAN バックホールリンクの負荷。範囲は 0 ~ 100 です。

コマンド デフォルト

ダウンリンク WAN メトリックが設定されていません。

コマンド モード

WLAN の設定

コマンド履歴

リリース 変更内容

リリース このコマンドが導入されました。
8.2

次に、ダウンリンク WAN メトリックの設定例を示します。

```
Cisco Controller > config wlan hotspot hs2 wan-metrics downlink 12 2468 10
```

config wlan hotspot hs2 wan-metrics link-status

WAN メトリックのリンク ステータスを設定するには、WLAN コンフィギュレーション モードで **config wlan hotspot hs2 wan-metrics link-status** コマンドを使用します。

config wlan hotspot hs2 wan-metrics link-status *wlan-id link-status*

構文の説明

wlan-id WLAN ID 番号。1 ～ 512 の値を入力します。

link-status リンク ステータス。有効な値は次のとおりです。

- 0 : 不明
- 1 : アップ
- 2 : ダウン
- 3 : テスト

コマンド デフォルト

リンク ステータスが設定されていません。

コマンド モード

WLAN の設定

コマンド履歴

| リリース | 変更内容 |
|------|-----------------|
| リリース | このコマンドが導入されました。 |
| 8.2 | |

次に、WAN メトリックのリンク ステータスの設定例を示します。

```
Cisco Controller > config wlan hotspot hs2 wan-metrics link-status 12 1
```

config wlan hotspot hs2 wan-metrics lmd

WAN メトリックの負荷測定期間を設定するには、WLAN コンフィギュレーション モードで **config wlan hotspot hs2 wan-metrics lmd** コマンドを使用します。

config wlan hotspot hs2 wan-metrics lmd *wlan-id lmd-value*

構文の説明

wlan-id WLAN ID 番号。1 ~ 512 の値を入力します。

lmd-value WAN の負荷測定期間。範囲は 0 ~ 65535 です。

コマンド デフォルト

WAN の負荷測定期間が設定されていません。

コマンド モード

WLAN の設定

コマンド履歴

リリース 変更内容

リリース このコマンドが導入されました。
8.2

次に、WAN メトリックの負荷測定期間の設定例を示します。

```
Cisco Controller > config wlan hotspot hs2 wan-metrics lmd 1 2456
```

config wlan hotspot hs2 wan-metrics uplink

アップリンク WAN メトリックを設定するには、WLAN コンフィギュレーション モードで **config wlan hotspot hs2 wan-metrics uplink** コマンドを使用します。

config wlan hotspot hs2 wan-metrics uplink *wlan-id ulink-speed ulink-load*

構文の説明

wlan-id WLAN ID 番号。1 ～ 512 の値を入力します。

ulink-speed kbps 単位の WAN バックホール リンク の速度。範囲は 0 ～ 4,294,967,295 です。

ulink-load WAN バックホール リンク の負荷。範囲は 0 ～ 100 です。

コマンド デフォルト

アップリンク WAN メトリックが設定されていません。

コマンド モード

WLAN の設定

コマンド履歴

リリース 変更内容

リリース このコマンドが導入されました。
8.2

次に、アップリンク WAN メトリックの設定例を示します。

```
Cisco Controller > config wlan hotspot hs2 wan-metrics uplink 12 2468 10
```

config wlan hotspot msap

WLAN の Mobility Service Advertisement Protocol (MSAP) のパラメータを設定するには、**config wlan hotspot msap** コマンドを使用します。

config wlan hotspot msap {enable | disable | server-id *server_id*} *wlan_id*

構文の説明

| | |
|------------------|------------------------------|
| enable | WLAN の MSAP をイネーブルにします。 |
| disable | WLAN の MSAP をディセーブルにします。 |
| server-id | MSAP サーバ ID を指定します。 |
| <i>server_id</i> | MSAP サーバ ID。値の範囲は 1 ~ 10 です。 |
| <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |

コマンド デフォルト

なし

コマンド履歴

| リリース | 変更内容 |
|------|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、WLAN で MSAP をイネーブルにする例を示します。

```
(Cisco Controller) >config wlan hotspot msap enable 4
```


config wlan interface

無線 LAN インターフェイスまたはインターフェイス グループを設定するには、**config wlan interface** コマンドを使用します。

config wlan interface {*wlan_id* | **foreignAp**} {*interface-name* | *interface-group-name*}

| | | |
|------------|-----------------------------|-----------------------------------|
| 構文の説明 | <i>wlan_id</i> | (任意) 無線 LAN 識別子 (1～512)。 |
| | foreignAp | サードパーティのアクセス ポイントを指定します。 |
| | <i>interface-name</i> | インターフェイス名。 |
| | <i>interface-group-name</i> | インターフェイス グループの名前。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、VLAN901 という名前のインターフェイスを設定する例を示します。

```
(Cisco Controller) >config wlan interface 16 VLAN901
```

config wlan ipv6 acl

無線 LAN の IPv6 アクセス コントロール リスト (ACL) を設定するには、**config wlan ipv6 acl** コマンドを使用します。

config wlan ipv6 acl *wlan_id* *acl_name*

| | | |
|------------|-----------------|-----------------------------------|
| 構文の説明 | <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| | <i>acl_name</i> | IPv6 ACL の名前。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、ローカル スイッチング用の IPv6 ACL を設定する例を示します。

```
(Cisco Controller) >config wlan ipv6 acl 22 acl_sample
```

config wlan kts-cac

WLAN のボタン電話システム ベースの CAC ポリシーを設定するには、**config wlan kts-cac** コマンドを使用します。

config wlan kts-cac {**enable** | **disable**} *wlan_id*

| | | |
|-----------|----------------|-----------------------------------|
| 構文の説明 | enable | KTS ベースの CAC ポリシーをイネーブルにします。 |
| | disable | KTS ベースの CAC ポリシーをディセーブルにします。 |
| | <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| コマンドデフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン WLAN の KTS ベースの CAC ポリシーをイネーブルにするには、次の手順を実行します。

- WLAN の QoS プロファイルを **Platinum** に設定するには、次のコマンドを入力します。
config wlan qos wlan-id platinum
- WLAN を無効にするには、次のコマンドを入力します。
config wlan disable wlan-id
- WLAN に対する FlexConnect ローカルスイッチングをディセーブルにするには、次のコマンドを入力します。
config wlan flexconnect local-switching wlan-id disable

次に、ID 4 の WLAN に対して、KTS ベースの CAC ポリシーをイネーブルにする例を示します。

```
(Cisco Controller) >config wlan kts-cac enable 4
```

config wlan layer2 acl

中央でスイッチングされる WLAN でレイヤ 2 アクセス コントロール リスト (ACL) を設定するには、**config wlan acl layer2** コマンドを使用します。

```
config wlan layer2 acl wlan_id {acl_name | none}
```

構文の説明

wlan_id 無線 LAN の ID。範囲は 1 ~ 512 です。

acl_name レイヤ 2 ACL 名。名前には 32 文字以内の英数字を使用できます。

none WLAN にマッピングされた任意のレイヤ 2 ACL をクリアします。

コマンド デフォルト

なし

コマンド履歴

リリー 変更内容
ス

7.5 このコマンドが導入されました。

使用上のガイドライン

レイヤ 2 ACL に対して最大 16 のルールを作成できます。

Cisco WLC には、最大で 64 の レイヤ 2 ACL を作成できます。

アクセス ポイントは最大 16 の WLAN をサポートするので、アクセス ポイントごとに最大 16 のレイヤ 2 ACL がサポートされます。

アクセス ポイントはレイヤ 2 およびレイヤ 3 の同じ ACL 名をサポートしないため、レイヤ 2 ACL 名が FlexConnect ACL 名と競合していないことを確認します。

次に、WLAN にレイヤ 2 ACL を適用する例を示します。

```
(Cisco Controller) >config wlan layer2 acl 1 acl_12_1
```

config wlan ldap

設定されている Lightweight Directory Access Protocol (LDAP) サーバへのリンクを追加または削除するには、**config wlan ldap** コマンドを入力します。

```
config wlan ldap {add wlan_id server_id | delete wlan_id {all | server_id}}
```

| | | |
|-------|------------------|------------------------------|
| 構文の説明 | add | 設定されている LDAP サーバへのリンクを追加します。 |
| | <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| | <i>server_id</i> | LDAP サーバ インデックス。 |
| | delete | 設定されている LDAP サーバへのリンクを削除します。 |
| | all | すべての LDAP サーバを指定します。 |

コマンド デフォルト なし

| | | |
|--------|------|-----------------------------------|
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン このコマンドを使用して、WLAN に LDAP サーバの優先順位を指定します。LDAP サーバの優先順位を指定するには、次のいずれかを設定し、有効にする必要があります。

- 802.1X 認証およびローカル EAP
- Web 認証および LDAP



(注) ローカル EAP はコントローラ ソフトウェア リリース 4.1 で導入されました。また、Web 認証での LDAP のサポートは、コントローラ ソフトウェア リリース 4.2 で導入されました。

次に、WLAN ID 100 およびサーバ ID 4 に設定されている LDAP サーバへのリンクを追加する例を示します。

```
(Cisco Controller) >config wlan ldap add 100 4
```

config wlan learn-ipaddr-cswlan

中央でスイッチングされる WLAN でクライアントの IP アドレス学習を設定するには、**config wlan learn-ipaddr-cswlan** コマンドを使用します。

config wlan learn-ipaddr-cswlan *wlan_id* {**enable** | **disable**}

構文の説明

wlan_id 1 ~ 512 の無線 LAN 識別子。

enable 中央でスイッチングされる WLAN でのクライアントの IPv4 アドレス学習を有効にします。

disable 中央でスイッチングされる WLAN でのクライアントの IPv4 アドレス学習を無効にします。

コマンド デフォルト

なし

コマンド履歴

| リリース | 変更内容 |
|------|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |
| 8.0 | このコマンドは、IPv4 アドレス形式のみをサポートします。 |

使用上のガイドライン

クライアントに Layer 2 暗号化が設定されている場合、Cisco WLC はクライアント IP アドレスを学習できず、定期的にクライアントをドロップします。Cisco WLC がクライアント IP アドレスを知らなくてもクライアント接続を維持できるように、このオプションを無効にしてください。

次に、中央でスイッチングされる WLAN でクライアント IP アドレスの学習をディセーブルにする例を示します。

```
(Cisco Controller) >config wlan learn-ipaddr-cswlan 2 enable
```

関連コマンド

show wlan

config wlan load-balance

グローバルロードバランシングの設定をオーバーライドし、特定のWLANでロードバランシングをイネーブルまたはディセーブルにするには、**config wlan load-balance** コマンドを使用します。

config wlan load-balance allow { **enable** | **disable** } *wlan_id*

| 構文の説明 | enable | 無線LANで帯域選択をイネーブルにします。 |
|-----------|--------------------------------|---------------------------------|
| | disable | 無線LANで帯域選択をディセーブルにします。 |
| | <i>wlan_id</i> | 1～512の無線LAN識別子。 |
| コマンドデフォルト | ロードバランシングはデフォルトではイネーブルになっています。 | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース7.6以前のリリースで導入されました。 |

次に、WLAN ID 3の無線LANで帯域選択をイネーブルにする例を示します。

```
(Cisco Controller) >config wlan load-balance allow enable 3
```

config wlan lobby-admin-access

特定の WLAN でロビーユーザに管理者アクセスを提供するには、**config wlan lobby-admin-access** コマンドを使用します。

config wlan lobby-admin-access {enable | disable} *wlan_id*

| | | |
|------------|------------------------|--------------------------|
| 構文の説明 | enable | 無線 LAN で帯域選択をイネーブルにします。 |
| | disable | 無線 LAN で帯域選択をディセーブルにします。 |
| | <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| コマンド デフォルト | ロビー管理者ユーザはデフォルトでは無効です。 | |
| コマンド履歴 | リリース | 変更内容 |
| | 8.4 | このコマンドが導入されました。 |

次に、WLAN でロビー管理者をイネーブルにする例を示します。

```
(Cisco Controller) >config wlan lobby-admin-access enable 2
```


config wlan mac-filtering

無線 LAN で MAC フィルタリングの状態を変更するには、**config wlan mac-filtering** コマンドを使用します。

config wlan mac-filtering {enable | disable} {wlan_id | foreignAp}

| | | |
|-----------|------------------|-----------------------------------|
| 構文の説明 | enable | 無線 LAN で MAC フィルタリングをイネーブルにします。 |
| | disable | 無線 LAN で MAC フィルタリングをディセーブルにします。 |
| | <i>wlan_id</i> | 1 ～ 512 の無線 LAN 識別子。 |
| | foreignAp | サードパーティのアクセス ポイントを指定します。 |
| コマンドデフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、WLAN ID 1 で MAC フィルタリングをイネーブルにする例を示します。

```
(Cisco Controller) >config wlan mac-filtering enable 1
```

config wlan max-associated-clients

無線 LAN、ゲスト LAN、またはリモート LAN のクライアント接続の最大数を設定するには、**config wlan max-associated-clients** コマンドを使用します。

config wlan max-associated-clients *max_clients* *wlan_id*

| | | |
|------------|--------------------|-----------------------------------|
| 構文の説明 | <i>max_clients</i> | 許可されるクライアント接続の最大数。 |
| | <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、WLAN ID 2 のクライアント接続の最大数を指定する例を示します。

```
(Cisco Controller) >config wlan max-associated-clients 25 2
```

config wlan max-radio-clients

アクセス ポイントごとの WLAN クライアントの最大数を設定するには、**config wlan max-radio-clients** コマンドを使用します。

config wlan max-radio-clients *max_radio_clients wlan_id*

| | | |
|-----------|--------------------------|---|
| 構文の説明 | <i>max_radio_clients</i> | 無線アクセス ポイントあたりに許可されるクライアント接続の最大数。有効値は 1 ~ 200 です。 |
| | <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| コマンドデフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、WLAN ID 2 で、無線アクセス ポイントあたりのクライアント接続の最大数を指定する例を示します。

```
(Cisco Controller) >config wlan max-radio-clients 25 2
```

config wlan mdns

WLAN のマルチキャスト DNS (mDNS) プロファイルを設定するには、**config wlan mdns** コマンドを使用します。

```
config wlan mdns {enable | disable | profile {profile-name | none}} {wlan_id | all}
```

構文の説明

| | |
|---------------------|--|
| enable | WLAN で mDNS スヌーピングをイネーブルにします。 |
| disable | WLAN で mDNS スヌーピングをディセーブルにします。 |
| profile | WLAN の mDNS プロファイルを設定します。 |
| <i>profile-name</i> | WLAN に関連付ける mDNS プロファイルの名前。 |
| none | WLAN から既存の mDNS プロファイルを削除します。WLAN に mDNS プロファイルを設定できません。 |
| <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| all | すべての WLAN の mDNS プロファイルを設定します。 |

コマンド デフォルト

デフォルトでは、WLAN で mDNS スヌーピングが有効になっています。

コマンド履歴

| リリース | 変更内容 |
|------|-----------------|
| 7.4 | このコマンドが導入されました。 |

使用上のガイドライン

このコマンドを使用する前に、WLAN をディセーブルにします。クライアントはプロファイルに関連付けられたサービスのみのサービスアドバタイズメントを受信します。コントローラはインターフェイスグループに関連付けられたプロファイルに最高の優先順位を与えます。次にインターフェイスプロファイル、WLAN プロファイルが続きます。各クライアントは、優先順位に従ってプロファイルにマップされます。

次に、WLAN の mDNS プロファイルを設定する例を示します。

```
(Cisco Controller) >config wlan mdns profile profile1 1
```

config wlan media-stream

無線 LAN メディア ストリームのマルチキャスト ダイレクトを設定するには、**config wlan media-stream** コマンドを使用します。

config wlan media-stream multicast-direct {*wlan_id* | **all**} {**enable** | **disable**}

| 構文の説明 | multicast-direct | 無線 LAN メディア ストリームのマルチキャスト ダイレクトを設定します。 |
|-------|------------------|--|
| | <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| | all | すべてのメディア ストリームで無線 LAN を設定します。 |
| | enable | ユニキャスト変換するグローバル マルチキャストを有効にします。 |
| | disable | ユニキャスト変換するグローバル マルチキャストを無効にします。 |

コマンド デフォルト なし

| コマンド履歴 | リリース | 変更内容 |
|--------|------|-----------------------------------|
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン メディア ストリーム マルチキャスト ダイレクトを使用するには、負荷ベースのコール アドミッション制御 (CAC) が実行されている必要があります。WLAN Quality of Service (QoS) を **gold** または **platinum** のいずれかに設定する必要があります。

次に、WLAN ID 2 によってグローバル マルチキャスト ダイレクト メディア ストリームを有効にする例を示します。

```
(Cisco Controller) >config wlan media-stream multicast-direct 2 enable
```

config wlan mfp

無線 LAN に管理フレーム保護 (MFP) オプションを設定するには、**config wlan mfp** コマンドを使用します。

```
config wlan mfp { client [enable | disable] wlan_id | infrastructure protection [enable | disable] wlan_id}
```

| | | |
|------------|----------------------------------|-------------------------------------|
| 構文の説明 | client | 無線 LAN にクライアント MFP を設定します。 |
| | enable | (任意) 機能をイネーブルにします。 |
| | disable | (任意) 機能をディセーブルにします。 |
| | <i>wlan_id</i> | 無線 LAN 識別子 (1~512)。 |
| | infrastructure protection | (任意) 無線 LAN にインフラストラクチャ MFP を設定します。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、WLAN ID 1 のクライアント管理フレームの保護を設定する例を示します。

```
(Cisco Controller) >config wlan mfp client enable 1
```

config wlan mobility anchor

無線 LAN で MAC フィルタリングの状態を変更するには、**config wlan mobility anchor** コマンドを使用します。

config wlan mobility anchor { **add** | **delete** } *wlan_id ip_addr priority priority-number*

| 構文の説明 | パラメータ | 説明 |
|-------|------------------------|--|
| | add | 無線 LAN で MAC フィルタリングをイネーブルにします。 |
| | delete | 無線 LAN で MAC フィルタリングをディセーブルにします。 |
| | <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| | <i>ip_addr</i> | 無線 LAN をアンカーするメンバスイッチの IPv4 アドレス。 |
| | priority | アンカーされたワイヤレス LAN の IP アドレスに優先順位を設定します。 |
| | <i>priority-number</i> | 範囲は 1 ~ 3 の間です。 |

コマンドデフォルト なし

| コマンド履歴 | リリース | 変更内容 |
|--------|------|---|
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |
| | 8.0 | このコマンドは、IPv4 アドレス形式のみをサポートします。 |
| | 8.1 | prioritypriority number パラメータが導入されました。 |

次に、WLAN ID 4 と IPv4 アドレス 192.168.0.14 で、モビリティ無線 LAN アンカー リストに優先順位を設定する例を示します。

```
(Cisco Controller) >config wlan mobility anchor add 4 192.168.0.14 priority 1
```

関連コマンド **show wlan**

config wlan mobility foreign-map

外部 Cisco WLC のインターフェイスまたはインターフェイス グループを設定するには、**config wlan mobility foreign-map** コマンドを使用します。

```
config wlan mobility foreign-map {add | delete} wlan_id foreign_mac_address {interface_name | interface_group_name}
```

| 構文の説明 | add | delete |
|-------|--|---|
| | 外部コントローラ マップにインターフェイスまたはインターフェイス グループを追加します。 | 外部コントローラ マップからインターフェイスまたはインターフェイス グループを削除します。 |
| | <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| | <i>foreign_mac_address</i> | WLAN の外部スイッチの MAC アドレス。 |
| | <i>interface_name</i> | 最大 32 文字の英数字のインターフェイス名。 |
| | <i>interface_group_name</i> | 最大 32 文字の英数字のインターフェイス グループ名。 |

コマンド デフォルト なし

コマンド履歴

| リリース | 変更内容 |
|------|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、WLAN ID 4 の Cisco WLC に対するインターフェイス グループと、WLAN 00:21:1b:ea:36:60 の外部スイッチの MAC アドレスを追加する例を示します。

```
(Cisco Controller) >config wlan mobility foreign-map add 4 00:21:1b:ea:36:60 mygroup1
```


config wlan multicast buffer

無線マルチキャストパケットバッファサイズを設定するには、**config wlan multicast buffer** コマンドを使用します。

config wlan multicast buffer {enable | disable} *buffer-size*

| | | |
|------------|-----------------------|---|
| 構文の説明 | enable | 無線 LAN のマルチキャストインターフェイス機能をイネーブルにします。 |
| | disable | 無線 LAN のマルチキャストインターフェイス機能をディセーブルにします。 |
| | <i>buffer-size</i> | 無線マルチキャストパケットバッファサイズ。範囲は 30 ~ 60 です。AP がマルチキャストに割り当てられるバッファ数を動的に調整することを指定するには、0 を入力します。 |
| | <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| コマンド デフォルト | デフォルトのバッファサイズは 30 です。 | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、無線マルチキャストバッファを設定する例を示します。

```
(Cisco Controller) >config wlan multicast buffer enable 45 222
```

config wlan multicast interface

無線 LAN にマルチキャスト インターフェイスを設定するには、**config wlan multicast interface** コマンドを使用します。

config wlan multicast interface *wlan_id* {**enable** | **disable**} *interface_name*

構文の説明

| | |
|-----------------------|---|
| <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| enable | 無線 LAN のマルチキャスト インターフェイス機能をイネーブルにします。 |
| delete | 無線 LAN のマルチキャスト インターフェイス機能をディセーブルにします。 |
| <i>interface_name</i> | インターフェイス名。 (注) インターフェイス名は、小文字でしか指定できません。 |

コマンド デフォルト

マルチキャストはディセーブルです。

コマンド履歴

| リリース | 変更内容 |
|------|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、WLANID4 およびインターフェイス名 `myinterface1` の無線 LAN のマルチキャスト インターフェイス機能をイネーブルにする例を示します。

```
(Cisco Controller) >config wlan multicast interface 4 enable myinterface1
```

config wlan mu-mimo

WLAN でマルチユーザ Multiple-Input Multiple-Output (MU-MIMO) を有効にするには、**config wlan mu-mimo** コマンドを入力します。

```
config wlan mu-mimo {enable | disable} wlan-id
```

構文の説明

enable *wlan-id* 指定された WLAN で MU-MIMO を有効にします

disable *wlan-id* 指定された WLAN で MU-MIMO を無効にします

コマンド履歴

リリース 変更内容
ス

8.1 このコマンドが導入されました。

config wlan nac

WLAN に対するネットワーク アドミッション コントロール (NAC) のアウトオブバンド サポートをイネーブルまたはディセーブルにするには、**config wlan nac** コマンドを使用します。

config wlan nac {snmp | radius} {enable | disable} wlan_id

| | | |
|------------|----------------|-----------------------------------|
| 構文の説明 | snmp | SNMP NAC サポートを設定します。 |
| | radius | RADIUS NAC サポートを設定します。 |
| | enable | WLAN で NAC をイネーブルにします。 |
| | disable | WLAN で NAC をディセーブルにします。 |
| | wlan_id | 1～512 の WLAN 識別子。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン RADIUS NAC 状態を有効にする前に、AAA オーバーライドを有効にする必要があります。RADIUS NAC 状態をイネーブルにする前に、FlexConnect ローカルスイッチングをディセーブルにする必要があります。

次に、WLAN 13 の SNMP NAC サポートを設定する例を示します。

```
(Cisco Controller) >config wlan nac snmp enable 13
```

次に、WLAN 34 の RADIUS NAC サポートを設定する例を示します。

```
(Cisco Controller) >config wlan nac radius enable 20
```

config wlan override-rate-limit

QoS プロファイルで定義されたユーザおよび Service Set Identifier (SSID) ごとに、アップストリームおよびダウンストリームの帯域幅制限をオーバーライドするには、**config wlan override-rate-limit** コマンドを使用します。

```
config wlan override-rate-limit wlan_id { average-data-rate | average-rttime-rate |
burst-data-rate | burst-rttime-rate } { per-ssid | per-client } { downstream | upstream
} rate
```

構文の説明

| | |
|----------------------------|---|
| <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| average-data-rate | ユーザまたは SSID ごとに TCP トラフィックの平均データレートを指定します。範囲は 0 ~ 51,200 Kbps です。 |
| average-rttime-rate | ユーザまたは SSID ごとに UDP トラフィックの平均リアルタイムデータレートを指定します。範囲は 0 ~ 51,200 Kbps です。 |
| burst-data-rate | ユーザまたは SSID ごとに TCP トラフィックのピークデータレートを指定します。範囲は 0 ~ 51,200 Kbps です。 |
| burst-rttime-rate | ユーザまたは SSID ごとに UDP トラフィックのピークリアルタイムデータレートを指定します。範囲は 0 ~ 51,200 Kbps です。 |
| per-ssid | 無線ごとの SSID のレート制限を設定します。すべてのクライアントの混合トラフィックはこの制限を超えないようになります。 |
| per-client | SSID に関連付けられた各クライアントのレート制限を設定します。 |
| downstream | ダウンストリーム トラフィックのレート制限を設定します。 |
| upstream | アップストリーム トラフィックのレート制限を設定します。 |
| <i>rate</i> | ユーザまたは SSID ごとの TCP または UDP トラフィックのデータレート。範囲は 0 ~ 51,200 Kbps です。値に 0 を指定すると、QoS プロファイルに対する帯域幅の制限は行われません。 |

コマンド デフォルト なし

| コマンド履歴 | リリース | 変更内容 |
|--------|------|-----------------------------------|
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン レート制限は、コントローラと AP によって適用されます。中央スイッチングのために、コントローラは、ダウンストリームに対するクライアントごとのレート制限の適用を処理し、AP はアップストリームトラフィックと、ダウンストリームトラフィックに対する SSID ごとのレート制限の適用を処理します。AP は、スタンドアロンモードになったときに、ダウンストリームに対するクライアントごとのレート制限の適用も処理します。

FlexConnect ローカルスイッチングモードおよびスタンドアロンモードで、クライアントごと、SSID ごとのレート制限は、ダウンストリームおよびアップストリームトラフィックに対して、AP によって実行されます。ただし、FlexConnect スタンドアロンモードの設定は AP に保存されないため、AP をリロードしたときに設定が失われ、レート制限は再起動後に適用されません。

ローミングクライアントが同じコントローラ上の AP 間でローミングする場合は、同じレート制限パラメータがクライアントに適用されます。ただし、クライアントがアンカーコントローラから外部コントローラへローミングする場合、クライアントごとのダウンストリームレート制限では、アンカーコントローラで設定されたパラメータが使用され、アップストリームレート制限では、外部コントローラのパラメータが使用されます。

次に、SSID ごとにアップストリームトラフィックに対して 2000 kbps Burst Real-time の実際のレートを設定する例を示します。

```
(Cisco Controller) >config wlan override-rate-limit 2 burst-realttime-rate per-ssid
upstream 2000
```

config wlan.opendns-mode

OpenDNS サーバアクセスに対して DNS を強制またはコピーまたは無視するように WLAN OpenDNS モードを設定するには、**config wlan.opendns-mode** コマンドを使用します。

```
config wlan.opendns-mode wlan-id { ignore | force | copy }
```

構文の説明

wlan-id 無線 LAN (WLAN) の ID。

ignore OpenDNS モードを無視します。

force OpenDNS モードを強制します。

copy OpenDNS モードをコピーします。

コマンドモード

(コントローラの設定) >

コマンド履歴

リリース 変更内容

8.4 このコマンドが導入されました。

例

次に、WLAN OpenDNS モードごとに OpenDNS サーバに DNS をコピーするように設定する方法を示します。

```
(Cisco Controller) > config wlan.opendns-mode wlan1 copy
```

config wlan.opendns-profile

OpenDNS サーバアクセスに対してドメインネームシステム (DNS) を強制またはコピーまたは無視するように WLAN OpenDNS プロファイルを設定するには、**config wlan.opendns-profile** コマンドを使用します。

```
config wlan.opendns profile wlan-id profile-name {enable | disable}
```

構文の説明

| | |
|---------------------|--|
| <i>wlan-id</i> | ワイヤレス LAN ネットワーク。 |
| <i>profile-name</i> | このプロファイルを追跡するために使用される OpenDNS プロファイル名。 |
| enable | OpenDNS のアイデンティティをマッピングします。 |
| disable | OpenDNS のアイデンティティを削除します。 |

コマンドモード

(コントローラの設定) >

コマンド履歴

| リリース | 変更内容 |
|------|-----------------|
| 8.4 | このコマンドが導入されました。 |

使用上のガイドライン

なし

例

次に、OpenDNS サーバに DNS を強制するように OpenDNS プロファイルの WLAN を設定する方法を示します。

```
(Cisco Controller) > config wlan.opendns-profile wlan1 user1 enable
```


config wlan passive-client

無線 LAN のパッシブクライアント機能を設定するには、**config wlan passive-client** コマンドを使用します。

config wlan passive-client {enable | disable} wlan_id

| | | |
|-------|----------------|--------------------------------|
| 構文の説明 | enable | WLAN のパッシブクライアント機能をイネーブルにします。 |
| | disable | WLAN のパッシブクライアント機能をディセーブルにします。 |
| | wlan_id | 1 ~ 512 の WLAN 識別子。 |

コマンドデフォルト なし

| | | |
|--------|------|-----------------------------------|
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン このコマンドを入力する前に、**config network multicast global** および **config network multicast mode** コマンドを使用して、グローバル マルチキャスト モードとマルチキャスト-マルチキャスト モードを有効にする必要があります。



(注) マルチキャストマルチキャスト モードのマルチキャストは、ユニキャスト モード以外のみで設定する必要があります。このリリースで、パッシブクライアント機能は、マルチキャストユニキャスト モードで動作しません。

次に、無線 LAN ID 2 のパッシブクライアントを設定する例を示します。

```
(Cisco Controller) >config wlan passive-client enable 2
```

config wlan peer-blocking

WLAN にピアツーピア ブロッキング機能を設定するには、**config wlan peer-blocking** コマンドを使用します。

```
config wlan peer-blocking {disable | drop | forward-upstream} wlan_id
```

| | | |
|------------|-------------------------|--|
| 構文の説明 | disable | ピアツーピア ブロッキングをディセーブルにして、可能な場合にはコントローラ内でトラフィックをローカルにブリッジします。 |
| | drop | コントローラでパケットを破棄するようにします。 |
| | forward-upstream | パケットがアップストリーム VLAN に転送されるようにします。これらのパケットに対して行われる動作は、コントローラよりも上流にあるデバイスにより決定されます。 |
| | <i>wlan_id</i> | 1 ~ 512 の WLAN 識別子。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、WLANID1 のピアツーピアブロッキングをディセーブルにする例を示します。

```
(Cisco Controller) >config wlan peer-blocking disable 1
```

config wlan pmipv6 default-realm

PMIPv6 WLAN のデフォルト レルムを設定するには、**config wlan pmipv6 default-realm** コマンドを使用します。

```
config wlan pmipv6 default-realm { default-realm-name | none } wlan_id
```

構文の説明

default-realm-name WLAN のデフォルトのレルム名。

none WLAN のレルム名をクリアします。

wlan_id 1 ~ 512 の無線 LAN 識別子。

コマンドデフォルト

なし。

コマンド履歴

| リリース | 変更内容 |
|------|------|
|------|------|

| | |
|-----|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |
|-----|-----------------------------------|

次に、PMIPv6 WLAN のデフォルト レルム名を設定する例を示します。

```
(Cisco Controller) >config wlan pmipv6 default-realm XYZ 6
```

config wlan pmipv6 mobility-type

WLAN のモビリティのタイプを設定するには、**config wlan pmipv6 mobility-type** コマンドを使用します。

```
config wlan pmipv6 mobility-type { none | pmipv6 } { wlan_id | all }
```

構文の説明

| | |
|----------------|---|
| none | 簡易 IP モビリティで WLAN を設定します。 |
| pmipv6 | PMIPv6 モビリティで WLAN を設定します。 |
| all | すべての WLAN に対して、指定したモビリティのタイプをイネーブルにします。 |
| wlan_id | 1 ~ 512 の WLAN 識別子。 |

コマンド デフォルト

なし

コマンド履歴

| リリース | 変更内容 |
|------|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン

モビリティのタイプを設定する場合は、WLAN をディセーブルにする必要があります。

次に、WLAN で PMIPv6 としてモビリティのタイプを設定する例を示します。

```
(Cisco Controller) >config wlan pmipv6 mobility-type pmipv6 16
```

config wlan pmipv6 profile_name

PMIPv6 WLAN のプロファイル名を設定するには、**config wlan pmipv6 profile_name** コマンドを使用します。

```
config wlan pmipv6 profile_name profile_name wlan_id
```

構文の説明

profile_name PMIPv6 WLAN のプロファイル名。

wlan_id 1 ~ 512 の無線 LAN 識別子。

コマンドデフォルト

なし

コマンド履歴

| リリース | 変更内容 |
|------|------|
|------|------|

| | |
|-----|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |
|-----|-----------------------------------|

使用上のガイドライン

このコマンドは PMIPv6 WLAN または SSID にプロファイル名をバインドします。モバイルノードをコントローラに関連付けるたびに、PMIPV6 モジュールのトリガーにプロファイル名および NAI が使用されます。PMIPV6 モジュールは、LMA IP、APN、NAI など、すべてのプロファイル固有のパラメータを抽出し、PBU を ASR5K に送信します。

次に、PMIPv6 WLAN で ABC01 という名前のプロファイルを作成する例を示します。

```
(Cisco Controller) >config wlan pmipv6 profile_name ABC01 16
```

config wlan policy

WLAN でポリシーを設定するには、**config wlan policy** コマンドを使用します。

config wlan policy {**add** | **delete**} *priority-index wlan-id*

構文の説明

| | |
|-----------------------|---|
| add | WLAN にポリシーを追加します。 |
| delete | WLAN から既存のポリシーを削除します。 |
| <i>priority-index</i> | WLAN で設定するポリシーの優先順位インデックス。ポリシーは、優先順位インデックスに従ってクライアントに適用されます。指定できる範囲は1～16です。 |
| <i>policy_name</i> | プロファイルのポリシーの名前。 |
| <i>wlan-id</i> | 1～512 の WLAN 識別子。 |

コマンド デフォルト

WLAN ポリシーはありません。

コマンド履歴

| | |
|----------|-----------------|
| リリー ス | 変更内容 |
| 7.5 | このコマンドが導入されました。 |

使用上のガイドライン

WLAN に対して最大 16 のポリシーを適用できます。

次に、WLAN にポリシーを設定する例を示します。

```
(Cisco Controller) >config wlan policy add 1 teacher_policy 1
```

config wlan profile

WLAN に関連付けられているプロファイルを編集するには、**config wlan profile** コマンドを使用します。

config wlan profile *wlan_id profile-name*

| | | |
|-----------|---------------------|-------------------|
| 構文の説明 | <i>wlan_id</i> | 1～512 の WLAN 識別子。 |
| | <i>profile-name</i> | WLAN プロファイルの名前。 |
| コマンドデフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 8.0 | このコマンドが導入されました。 |

次に、WLAN に関連付けられているプロファイルを編集する例を示します。

```
(Cisco Controller) > config wlan disable 1
(Cisco Controller) > config wlan profile 1 new_sample
(Cisco Controller) > show wlan summary
```

Number of WLANs..... 1

| WLAN ID | WLAN Profile Name / SSID | Status | Interface Name | PMIPv6 Mobility |
|---------|--------------------------|----------|----------------|-----------------|
| 1 | new_sample / new_samp | Disabled | management | none |

config wlan profiling

WLAN でクライアント プロファイリングを設定するには、**config wlan profiling** コマンドを使用します。

```
config wlan profiling {local | radius} {all | dhcp | http} {enable | disable} wlan_id
```

構文の説明

| | |
|----------------|---|
| local | WLAN のローカルモードでクライアント プロファイリングを設定します。 |
| radius | WLAN 上の RADIUS モードでクライアント プロファイリングを設定します。 |
| all | WLAN で DHCP および HTTP クライアント プロファイリングを設定します。 |
| dhcp | WLAN で、DHCP クライアント プロファイリングだけを設定します。 |
| http | WLAN で、HTTP クライアント プロファイリングを設定します。 |
| enable | <p>WLAN で、クライアント プロファイリングの特定のタイプをイネーブルにします。</p> <p>HTTP プロファイリングをイネーブルにすると、Cisco WLC は、プロファイリングのために、クライアントの HTTP 属性を収集します。</p> <p>DHCP プロファイリングをイネーブルにすると、Cisco WLC は、プロファイリングのために、クライアントの DHCP 属性を収集します。</p> |
| disable | WLAN で、クライアント プロファイリングの特定のタイプをディセーブルにします。 |
| wlan_id | 1 ~ 512 の無線 LAN 識別子。 |

使用上のガイドライン

WLAN のクライアント プロファイリングを設定する前に、WLAN をディセーブルにしたことを確認します。

コマンド デフォルト

クライアントのプロファイリングは無効です。

コマンド履歴

| リリース | 変更内容 |
|------|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン HTTP でポート 80 に接続されたクライアントだけをプロファイリングできます。IPv6 専用クライアントはプロファイリングされません。

セッションタイムアウトが WLAN に対して設定されている場合、クライアントは、設定されたタイムアウトがプロファイリングされる前に HTTP トラフィックを送信する必要があります。

この機能は、以下ではサポートされていません。

- FlexConnect スタンドアロンモード
- FlexConnect ローカル認証

次に、WLAN で DHCP プロファイリングと HTTP プロファイリングの両方をイネーブルにする例を示します。

```
(Cisco Controller) >config wlan profiling radius all enable 6
HTTP Profiling successfully enabled.
DHCP Profiling successfully enabled.
```

config wlan qos

無線 LAN の Quality Of Service (QoS) を変更するには、**config wlan qos** コマンドを使用します。

```
config wlan qos wlan_id {bronze | silver | gold | platinum}
config wlan qos foreignAp {bronze | silver | gold | platinum}
```

| | | |
|------------|-------------------------|-----------------------------------|
| 構文の説明 | <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| | bronze | Bronze QoS ポリシーを指定します。 |
| | silver | Silver QoS ポリシーを指定します。 |
| | gold | Gold QoS ポリシーを指定します。 |
| | platinum | Platinum QoS ポリシーを指定します。 |
| | foreignAp | サードパーティのアクセス ポイントを指定します。 |
| コマンド デフォルト | デフォルトの QoS ポリシーはシルバーです。 | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、無線 LAN 1 に最高レベルのサービスを設定する例を示します。

```
(Cisco Controller) >config wlan qos 1 gold
```

config wlan radio

無線 LAN にシスコの無線ポリシーを設定するには、**config wlan radio** コマンドを使用します。

config wlan radio *wlan_id* { **all** | **802.11a** | **802.11bg** | **802.11g** | **802.11ag** }

構文の説明

| | |
|-----------------|--|
| <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| all | すべての無線帯域で無線 LAN を設定します。 |
| 802.11a | 802.11a だけに無線 LAN を設定します。 |
| 802.11bg | 802.11b/g だけに無線 LAN を設定します (802.11g がディセーブルな場合は 802.11b だけに設定)。 |
| 802.11g | 802.11g だけに無線 LAN を設定します。 |

コマンドデフォルト

なし

コマンド履歴

| リリース | 変更内容 |
|------|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、すべての無線帯域に無線 LAN を設定する例を示します。

```
(Cisco Controller) >config wlan radio 1 all
```

config wlan radius_server acct

WLAN で RADIUS アカウンティング サーバを設定するには、**config wlan radius_server acct** コマンドを使用します。

```
config wlan radius_server acct {enable | disable} wlan_id | add wlan_id server_id | delete
wlan_id {all | server_id} | framed-ipv6 { address | both | prefix } wlan_id
```

| 構文の説明 | | |
|------------------|--|---|
| enable | | WLAN の RADIUS アカウンティングをイネーブルにします。 |
| disable | | WLAN の RADIUS アカウンティングをディセーブルにします。 |
| <i>wlan_id</i> | | 1 ~ 512 の無線 LAN 識別子。 |
| add | | 設定されている RADIUS アカウンティングサーバへのリンクを追加します。 |
| <i>server_id</i> | | RADIUS サーバインデックス。 |
| delete | | 設定されている RADIUS アカウンティングサーバへのリンクを削除します。 |
| address | | IPv6 アドレスにアカウンティングフレーム化された IPv6 属性を設定します。 |
| both | | IPv6 アドレスとプレフィックスにアカウンティングフレーム化された IPv6 属性を設定します。 |
| prefix | | IPv6 プレフィックスにアカウンティングフレーム化された IPv6 属性を設定します。 |

コマンド デフォルト なし

コマンド履歴

| リリース | 変更内容 |
|------|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、WLAN 2 の RADIUS アカウンティングをイネーブルにする例を示します。

```
(Cisco Controller) >config wlan radius_server acct enable 2
```

次に、設定された RADIUS アカウンティングサーバへのリンクを追加する例を示します。

```
(Cisco Controller) > config wlan radius_server acct add 2 5
```

config wlan radius_server acct interim-update

WLAN で RADIUS アカウンティング サーバの中間アップデートを設定するには、**config wlan radius_server acct interim-update** コマンドを使用します。

config wlan radius_server acct interim-update { **enable** | **disable** | *interval* } *wlan_id*

構文の説明

| | |
|-----------------------|--|
| interim-update | RADIUS アカウンティング サーバの中間アップデートを設定します。 |
| enable | WLAN の RADIUS アカウンティングサーバの中間アップデートをイネーブルにします。 |
| disable | WLAN の RADIUS アカウンティングサーバの中間アップデートをディセーブルにします。 |
| <i>interval</i> | ユーザが指定する中間アップデート間隔。有効な値の範囲は 60 ~ 3600 秒です。 |
| <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |

コマンド デフォルト

RADIUS アカウンティング サーバの中間アップデートは 600 秒に設定されます。

コマンド履歴

| リリース | 変更内容 |
|------|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、WLAN 2 の RADIUS アカウンティング サーバに 200 秒の中間アップデートを指定する例を示します。

```
(Cisco Controller) >config wlan radius_server acct interim-update 200 2
```

config wlan radius_server auth

WLAN で RADIUS 認証サーバを設定するには、**config wlan radius_server auth** コマンドを使用します。

```
config wlan radius_server auth {enable wlan_id | disable wlan_id} {add wlan_id server_id | delete wlan_id {all | server_id}}
```

| | | |
|-----------|------------------|------------------------------------|
| 構文の説明 | auth | RADIUS 認証を設定します |
| | enable | この WLAN に対して RADIUS 認証をイネーブルにします。 |
| | <i>wlan_id</i> | 1 ～ 512 の無線 LAN 識別子。 |
| | disable | この WLAN に対して RADIUS 認証をディセーブルにします。 |
| | add | 設定されている RADIUS サーバへのリンクを追加します。 |
| | <i>server_id</i> | RADIUS サーバインデックス。 |
| | delete | 設定されている RADIUS サーバへのリンクを削除します。 |
| | all | 設定されている RADIUS サーバへのすべてのリンクを削除します。 |
| コマンドデフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、WLAN ID 1 およびサーバ ID 1 の設定済み RADIUS 認証サーバにリンクを追加する例を示します。

```
(Cisco Controller) >config wlan radius_server auth add 1 1
```

config wlan radius_server overwrite-interface

無線 LAN の RADIUS 動的インターフェイスを設定するには、**config wlan radius_server overwrite-interface** コマンドを使用します。

config wlan radius_server overwrite-interface {enable | disable} *wlan_id*

| | | |
|------------|----------------|--|
| 構文の説明 | enable | この WLAN に対して RADIUS 動的インターフェイスをイネーブルにします。 |
| | disable | この WLAN に対して RADIUS 動的インターフェイスをディセーブルにします。 |
| | <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン コントローラは、ID として管理インターフェイスを使用します。RADIUS サーバが直接接続された動的インターフェイスにある場合、トラフィックは動的インターフェイスから送信されます。それ以外の場合は、管理 IP アドレスが使用されます。

この機能を有効にすると、コントローラは、その WLAN 上のすべての RADIUS 関連トラフィックの Identity および送信元として、WLAN の設定に指定されたインターフェイスを Identity として使用します。

次に、ID 1 の WLAN に対して RADIUS 動的インターフェイスをイネーブルにする例を示します。

```
(Cisco Controller) >config wlan radius_server overwrite-interface enable 1
```


config wlan radius_server realm

WLAN でレルムを設定するには、`config wlan radius_server realm` コマンドを使用します。

```
config wlan radius_serverrealm {enable | disable} wlan-id
```

| | | |
|-----------|----------------------|---------------------------------|
| 構文の説明 | <i>radius_server</i> | RADIUS サーバインデックス。範囲は 1 ~ 17 です。 |
| | enable | WLAN でレルムを有効にします。 |
| | disable | WLAN でレルムを無効にします。 |
| | <i>wlan-id</i> | WLAN ID。範囲は 1 ~ 512 です。 |
| コマンドデフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 8.0 | このコマンドが導入されました。 |

次に、WLAN でレルムをイネーブルにする例を示します。

```
(Cisco Controller) > config wlan 2 realm enable 50
```

config wlan roamed-voice-client re-anchor

ローミングされる音声クライアントのリアンカー ポリシーを設定するには、**config wlan roamed-voice-client re-anchor** コマンドを使用します。

config wlan roamed-voice-client re-anchor {enable | disable} *wlan_id*

| | | |
|------------|---------------------------------|---------------------------------------|
| 構文の説明 | enable | ローミングされるクライアントのリアンカー ポリシーをイネーブルにします。 |
| | disable | ローミングされるクライアントのリアンカー ポリシーをディセーブルにします。 |
| | <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| コマンド デフォルト | ローミングされるクライアントのリアンカー ポリシーは無効です。 | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、WLAN ID が 1 のローミングされる音声クライアントで、リアンカー ポリシーをイネーブルにする例を示します。

```
(Cisco Controller) >config wlan roamed-voice-client re-anchor enable 1
```

config wlan security 802.1X

無線 LAN のシスコ無線の 802.1X セキュリティの状態を変更するには、**config wlan security 802.1X** コマンドを使用します。

```
config wlan security 802.1X {enable {wlan_id | foreignAp} | disable {wlan_id | foreignAp}
| encryption {wlan_id | foreignAp} {0 | 40 | 104} | on-macfilter-failure {enable |
disable}}
```

| | | |
|-------|-----------------------------|---|
| 構文の説明 | enable | 802.1X 設定を有効にします。 |
| | <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| | foreignAp | サードパーティのアクセス ポイントを指定します。 |
| | disable | 802.1X 設定を無効にします。 |
| | encryption | 静的 WEP キーとインデックスを指定します。 |
| | 0 | WEP キーのサイズを 0 (暗号化なし) に指定します。デフォルト値は 104 です。 (注) 無線 LAN 内のすべてのキーは、同じサイズでなければなりません。 |
| | 40 | WEP キーのサイズを 40 ビットに指定します。デフォルト値は 104 です。 (注) 無線 LAN 内のすべてのキーは、同じサイズでなければなりません。 |
| | 104 | WEP キーのサイズを 104 ビットに指定します。デフォルト値は 104 です。 (注) 無線 LAN 内のすべてのキーは、同じサイズでなければなりません。 |
| | on-macfilter-failure | MAC フィルタの失敗に対する 802.1X を設定します。 |
| | enable | MAC フィルタの失敗に対する 802.1X 認証を有効にします。 |
| | disable | MAC フィルタの失敗に対する 802.1X 認証を無効にします。 |

コマンド デフォルト なし

| コマンド履歴 | リリース | 変更内容 |
|--------|------|-----------------------------------|
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン 無線 LAN のシスコ無線の 802.1X セキュリティの暗号化レベルを変更するには、次のキー サイズを使用します。

- 0 : 802.1X 暗号化なし。
- 40 : 40/64 ビット暗号化。
- 104 : 104/128 ビット暗号化（これは、デフォルトの暗号化設定です）。

次に、WLAN ID 16 で 802.1X セキュリティを設定する例を示します。

```
(Cisco Controller) >config wlan security 802.1X enable 16
```

config wlan security ckip

無線 LAN に Cisco Key Integrity Protocol (CKIP) セキュリティ オプションを設定するには、**config wlan security ckip** コマンドを使用します。

```
config wlan security ckip {enable | disable} wlan_id [akm psk set-key {hex | ascii} {40 | 104} key key_index wlan_id | mmh-mic {enable | disable} wlan_id | kp {enable | disable} wlan_id]
```

| | | |
|-----------|------------------------|--|
| 構文の説明 | enable | CKIP セキュリティを有効にします。 |
| | disable | CKIP セキュリティを無効にします。 |
| | <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| | akm psk set-key | (任意) CKIP 無線 LAN の暗号キー管理を設定します。 |
| | hex | 16 進数の暗号キーを指定します。 |
| | ascii | ASCII の暗号キーを指定します。 |
| | 40 | CKIP WLAN の静的暗号キーの長さを 40 ビットに設定します。40 ビットキーには、ASCII テキスト文字が 5 文字と 16 進数文字が 10 文字必要です。 |
| | 104 | CKIP WLAN の静的暗号キーの長さを 104 ビットに設定します。104 ビットキーには、ASCII テキスト文字が 13 文字と 16 進数文字が 26 文字必要です。 |
| | key | CKIP WLAN のキーの設定を指定します。 |
| | <i>key_index</i> | 設定済み PSK キー インデックス。 |
| コマンドデフォルト | mmh-mic | (任意) CKIP 無線 LAN のマルチモジュール ハッシュ メッセージ整合性チェック (MMH MIC) 検証を設定します。 |
| | kp | (任意) CKIP 無線 LAN のキー置換を設定します。 |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、WLAN 03 の PSK キー インデックス 2 に 104 ビット（16 進数文字 26 字）の CKIP WLAN 暗号キーを設定する例を示します。

```
(Cisco Controller) >config wlan security ckip akm psk set-key hex 104 key 2 03
```

config wlan security cond-web-redir

条件付き Web リダイレクトを有効または無効にするには、**config wlan security cond-web-redir** コマンドを使用します。

```
config wlan security cond-web-redir {enable | disable} wlan_id
```

| | | |
|------------|----------------|-----------------------------------|
| 構文の説明 | enable | 条件付き Web リダイレクトを有効にします。 |
| | disable | 条件付き Web リダイレクトを無効にします。 |
| | <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、WLAN ID 2 で条件付き Web リダイレクトを有効にする例を示します。

```
(Cisco Controller) >config wlan security cond-web-redir enable 2
```

config wlan security eap-params

WLAN でローカル EAP タイマーを設定するには、**config wlan security eap-params** コマンドを使用します。

```
config wlan security eap-params { {enable | disable} | eapol-key-timeout timeout | eap-key-retries
retries | identity-request-timeout timeout | identity-request-retries retries | request-timeout
timeout | request-retries retries } wlan_id
```

構文の説明

{ **enable** | **disable** }

SSID 固有の EAP タイムアウトまたは再試行を有効または無効にするように指定します。デフォルト値は [disabled] です。

eapol-key-timeout *timeout*

コントローラがローカル EAP を使用してワイヤレスクライアントに WLAN 経由で EAP キーの送信を試みる時間 (200 ~ 5000 ミリ秒) を指定します。有効な範囲は 200 ~ 5000 ミリ秒です。

デフォルト値は 1000 ミリ秒です。

eapol-key-retries *retries*

コントローラがローカル EAP を使用してワイヤレスクライアントに WLAN 経由で EAP キーの送信を試みる最大回数 (0 ~ 4 回) を指定します。

デフォルト値は 2 です。

identity-request-timeout *timeout*

コントローラがローカル EAP を使用して WLAN 内部のワイヤレスクライアントに EAP ID 要求の送信を試みる時間 (1 ~ 120 秒) を指定します。

デフォルト値は 30 秒です。

identity-request-retries *retries*

コントローラがローカル EAP を使用して WLAN 内部のワイヤレスクライアントに EAP ID 要求の再送信を試みる最大回数 (0 ~ 4 回) を指定します。

デフォルト値は 2 です。

request-timeout

コントローラがローカル EAP を使用して WLAN 内部のワイヤレスクライアントに EAP パラメータ要求の送信を試みる時間 (1 ~ 120 秒) を指定します。

デフォルト値は 30 秒です。

| | |
|---------------------------------------|--|
| request-retries <i>retries</i> | コントローラがローカル EAP を使用して WLAN 内部のワイヤレスクライアントに EAP パラメータ要求の再送信を試みる最大回数 (0 ~ 20 回) を指定します。 デフォルト値は 2 です。 |
| wlan-id | WLAN ID 番号。 |

コマンド デフォルト

デフォルトの EAPOL キー タイムアウトは 1000 ミリ秒です。

EAPOL キーの再試行回数のデフォルトは 2 です。

デフォルトの ID 要求タイムアウト値は 30 秒です。

デフォルトの ID 要求試行回数は 2 です。

デフォルトの要求タイムアウト値は 30 秒です。

デフォルトの要求試行回数は 2 です。

コマンド履歴

| リリース | 変更内容 |
|------|-----------------|
| 7.6 | このコマンドが導入されました。 |

次に、WLAN で SSID 固有の EAP パラメータを有効にする例を示します。

```
(Cisco Controller) > config wlan security eap-params enable 4
```

次に、WLAN で EAPOL キー タイムアウト パラメータを設定する例を示します。

```
(Cisco Controller) > config wlan security eap-params eapol-key-retries 4
```

次に、WLAN で EAPOL キーの再試行回数を設定する例を示します。

```
(Cisco Controller) > config wlan security eap-params eapol-key-retries 4
```

config wlan security eap-passthru

外部オーセンティケータに 802.1X フレーム パス スルーを設定するには、**config wlan security eap-passthru** コマンドを使用します。

config wlan security eap-passthru {enable | disable} wlan_id

| | | |
|------------|----------------|--|
| 構文の説明 | enable | 外部オーセンティケータへの 802.1X フレーム パス スルーを有効にします。 |
| | disable | 外部オーセンティケータへの 802.1X フレーム パス スルーを無効にします。 |
| | wlan_id | 1 ~ 512 の無線 LAN 識別子。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、WLAN ID 2 の外部オーセンティケータへの 802.1X フレーム パス スルーを有効にする例を示します。

```
(Cisco Controller) >config wlan security eap-passthru enable 2
```

config wlan security ft

802.11r 高速移行ローミング パラメータを設定するには、**config wlan security ft** コマンドを使用します。

```
config wlan security ft {adaptive | enable | disable | reassociation-timeout timeout-in-seconds}
wlan_id
```

| 構文の説明 | | |
|-------|------------------------------|---|
| | adaptive | 802.11r 高速移行ローミング アダプティブ サポートを設定します。これがデフォルトのオプションです。 |
| | enable | 802.11r 高速移行ローミング サポートを有効にします。 |
| | disable | 802.11r 高速移行ローミング サポートを無効にします。 |
| | reassociation-timeout | 再アソシエーション期限の間隔を設定します。 |
| | <i>timeout-in-seconds</i> | 再アソシエーションのタイムアウト値 (秒単位)。有効範囲は 1 ~ 100 秒です。 |
| | <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |

コマンド デフォルト なし

| コマンド履歴 | リリース | 変更内容 |
|--------|------|--|
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |
| | 8.3 | このコマンドが変更されました。 adaptive キーワードが追加されました。 |

使用上のガイドライン 先に進む前に、WLAN を無効にしたことを確認します。

次に、WLAN 2 で 802.11r 高速移行ローミング サポートを有効にする例を示します。

```
(Cisco Controller) >config wlan security ft enable 2
```

次に、WLAN 2 の 802.11r 高速移行ローミング サポートに対する再アソシエーションのタイムアウト値を 20 秒に設定する例を示します。

```
(Cisco Controller) >config wlan security ft reassociation-timeout 20 2
```

config wlan security ft over-the-ds

分散システム上の 802.11r 高速移行パラメータを設定するには、**config wlan security ft over-the-ds** コマンドを使用します。

config wlan security ft over-the-ds {enable | disable} wlan_id

| | | |
|------------|----------------|--|
| 構文の説明 | enable | 分散システム上の 802.11r 高速移行ローミングサポートを有効にします。 |
| | disable | 分散システム上の 802.11r 高速移行ローミングサポートを無効にします。 |
| | wlan_id | 1 ~ 512 の無線 LAN 識別子。 |
| コマンド デフォルト | イネーブル | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン 先に進む前に、WLAN を無効にしたことを確認します。

802.11r 高速移行が WLAN で有効であることを確認します。

次に、WLAN ID 2 の分散システム上の 802.11r 高速移行ローミングサポートを有効にする例を示します。

```
(Cisco Controller) >config wlan security ft over-the-ds enable 2
```

config wlan security IPsec disable

IPSec セキュリティを無効にするには、**config wlan security IPsec disable** コマンドを使用します。

config wlan security IPsec disable {*wlan_id* | **foreignAp**}

| | | |
|-----------|------------------|-----------------------------------|
| 構文の説明 | <i>wlan_id</i> | 1 ～ 512 の無線 LAN 識別子。 |
| | foreignAp | サードパーティのアクセス ポイントを指定します。 |
| コマンドデフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、WLAN ID 16 の IPSec を無効にする例を示します。

```
(Cisco Controller) >config wlan security IPsec disable 16
```

config wlan security IPsec enable

IPSec セキュリティを有効にするには、**config wlan security IPsec enable** コマンドを使用します。

config wlan security IPsec enable {*wlan_id* | **foreignAp**}

| | | |
|------------|------------------|-----------------------------------|
| 構文の説明 | <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| | foreignAp | サードパーティのアクセス ポイントを指定します。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、WLAN ID 16 の IPSec を有効にする例を示します。

```
(Cisco Controller) >config wlan security IPsec enable 16
```

config wlan security IPsec authentication

無線 LAN で使用する IPsec セキュリティ認証プロトコルを変更するには、**config wlan security IPsec authentication** コマンドを使用します。

config wlan security IPsec authentication { hmac-md5 | hmac-sha-1 } { wlan_id | foreignAp }

| | | |
|-------|-------------------|---------------------------------|
| 構文の説明 | hmac-md5 | IPsec HMAC-MD5 認証プロトコルを指定します。 |
| | hmac-sha-1 | IPsec HMAC-SHA-1 認証プロトコルを指定します。 |
| | <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| | foreignAp | サードパーティのアクセス ポイントを指定します。 |

コマンドデフォルト なし

| コマンド履歴 | リリース | 変更内容 |
|--------|------|-----------------------------------|
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、WLAN ID 1 の IPsec HMAC-SHA-1 セキュリティ認証パラメータを設定する例を示します。

```
(Cisco Controller) >config wlan security IPsec authentication hmac-sha-1 1
```

config wlan security IPsec encryption

無線 LAN で使用する IPsec セキュリティ暗号化プロトコルを変更するには、**config wlan security IPsec encryption** コマンドを使用します。

config wlan security IPsec encryption {**3des** | **aes** | **des**} {*wlan_id* | **foreignAp**}

| | | |
|-----------|------------------|-----------------------------------|
| 構文の説明 | 3des | IPsec 3DES 暗号化をイネーブルにします。 |
| | aes | IPsec AES 128 ビット暗号化を有効にします。 |
| | des | IPsec DES 暗号化をイネーブルにします。 |
| | <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| | foreignAp | サードパーティのアクセスポイントを指定します。 |
| コマンドデフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、IPsec AES 暗号化を設定する例を示します。

```
(Cisco Controller) >config wlan security IPsec encryption aes 1
```


config wlan security IPsec config

無線 LAN で使用する適切なインターネット キー交換 (IKE) CFG-Mode パラメータを設定するには、**config wlan security IPsec config** コマンドを使用します。

config wlan security IPsec config qotd *ip_address* { *wlan_id* | **foreignAp** }

| 構文の説明 | パラメータ | 説明 |
|-------|-------------------|--|
| | qotd | cfg-mode の quote-of-the day サーバ IP を設定します。 |
| | <i>ip_address</i> | cfg-mode の quote-of-the-day サーバ IP。 |
| | <i>wlan_id</i> | 1 ～ 512 の無線 LAN 識別子。 |
| | foreignAp | サードパーティのアクセス ポイントを指定します。 |

コマンドデフォルト なし

| コマンド履歴 | リリース | 変更内容 |
|--------|------|-----------------------------------|
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン IKE はセッションキー (暗号化および認証) の配布方式として、および VPN エンドポイントにデータの保護方法を提供する手法として使用されます。IKE はセキュリティアソシエーション (SA) のバンドルを各接続に割り当てて、接続を追跡します。

次に、WLAN 1 の CFG-mode の quote-of-the-day サーバ IP 44.55.66.77 を設定する例を示します。

```
(Cisco Controller) >config wlan security IPsec config qotd 44.55.66.77 1
```

config wlan security IPsec ike authentication

無線 LAN で使用する IPsec インターネット キー交換 (IKE) 認証プロトコルを変更するには、**config wlan security IPsec ike authentication** コマンドを使用します。

```
config wlan security IPsec ike authentication {certificates {wlan_id | foreignAp} |  
pre-share-key {wlan_id | foreignAp} key | xauth-psk {wlan_id | foreignAp} key}
```

| | | |
|-----------|----------------------|-----------------------------------|
| 構文の説明 | certificates | IKE 認証モードを有効にします。 |
| | <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| | foreignAp | サードパーティのアクセスポイントを指定します。 |
| | pre-share-key | 事前共有キーを持つ IKE Xauth を有効にします。 |
| | xauth-psk | IKE 事前共有キーを有効にします。 |
| | <i>key</i> | 事前共有および xauth-psk に必要なキー。 |
| コマンドデフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、IKE 認証モードを設定する例を示します。

```
(Cisco Controller) >config wlan security IPsec ike authentication certificates 16
```

config wlan security IPsec ike dh-group

無線 LAN で使用する IPsec インターネット キー交換 (IKE) Diffie-Hellman グループを変更するには、**config wlan security IPsec ike dh-group** コマンドを使用します。

config wlan security IPsec ike dh-group {*wlan_id* | **foreignAp**} {**group-1** | **group-2** | **group-5**}

| 構文の説明 | | |
|-------|------------------|------------------------------|
| | <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| | foreignAp | サードパーティのアクセス ポイントを指定します。 |
| | group-1 | DH グループ 1 (768 ビット) を指定します。 |
| | group-2 | DH グループ 2 (1024 ビット) を指定します。 |
| | group-5 | DH グループ 5 (1536 ビット) を指定します。 |

コマンド デフォルト なし

| コマンド履歴 | リリース | 変更内容 |
|--------|------|-----------------------------------|
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、グループ 1 の Diffie Hellman グループ パラメータを設定する例を示します。

```
(Cisco Controller) >config wlan security IPsec ike dh-group 1 group-1
```

config wlan security IPsec ike lifetime

無線 LAN で使用する IPsec インターネット キー交換 (IKE) ライフタイムを変更するには、**config wlan security IPsec ike lifetime** コマンドを使用します。

config wlan security IPsec ike lifetime {*wlan_id* | **foreignAp**} *seconds*

| | | |
|------------|------------------|-----------------------------------|
| 構文の説明 | <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| | foreignAp | サードパーティのアクセス ポイントを指定します。 |
| | <i>seconds</i> | 1800 ~ 345600 の IKE ライフタイム (秒)。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、無線 LAN で使用する IPsec IKE ライフタイムを設定する例を示します。

```
(Cisco Controller) >config wlan security IPsec ike lifetime 1 1900
```

config wlan security IPsec ike phase1

無線 LAN で使用する IPsec インターネットキー交換 (IKE) フェーズ 1 を変更するには、**config wlan security IPsec ike phase1** コマンドを使用します。

config wlan security IPsec ike phase1 { **aggressive** | **main** } { *wlan_id* | **foreignAp** }

| | | |
|------------|-------------------|-----------------------------------|
| 構文の説明 | aggressive | IKE アグレッシブ モードを有効にします。 |
| | main | IKE メイン モードを有効にします。 |
| | <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| | foreignAp | サードパーティのアクセス ポイントを指定します。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、IPsec IKE フェーズ 1 を変更する例を示します。

```
(Cisco Controller) >config wlan security IPsec ike phase1 aggressive 16
```

config wlan security IPsec ike contivity

無線 LAN で Nortel の Contivity VPN クライアント サポートを変更するには、**config wlan security IPsec ike contivity** コマンドを使用します。

config wlan security IPsec ike contivity {**enable** | **disable**} {*wlan_id* | **foreignAp**}

| | | |
|------------|------------------|--------------------------------------|
| 構文の説明 | enable | この WLAN に対する Contivity のサポートを有効にします。 |
| | disable | この WLAN に対する Contivity のサポートを無効にします。 |
| | <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| | foreignAp | サードパーティのアクセス ポイントを指定します。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、Contivity VPN クライアント サポートを変更する例を示します。

```
(Cisco Controller) >config wlan security IPsec ike contivity enable 14
```

config wlan security wpa akm ft

802.11r 高速移行 802.1X を使用して認証キー管理を設定するには、**config wlan security wpa akm ft** コマンドを使用します。

```
config wlan security wpa akm ft [over-the-air | over-the-ds | psk | [reassociation-timeout
seconds]] {enable | disable} wlan_id
```

| 構文の説明 | over-the-air | (任意) 802.11r 高速移行地上波ローミングサポートを設定します。 |
|-------|-----------------------|--|
| | over-the-ds | (任意) 802.11r 高速移行ローミング DS サポートを設定します。 |
| | psk | (任意) 802.11r 高速移行 PSK サポートを設定します。 |
| | reassociation-timeout | (任意) 再アソシエーションの期限間隔を設定します。 有効な範囲は 1 ~ 100 秒です。デフォルト値は 20 秒です。 |
| | seconds | 再アソシエーションの期限間隔 (秒単位)。 |
| | enable | 802.11r 高速移行 802.1X サポートを有効にします。 |
| | disable | 802.11r 高速移行 802.1X サポートを無効にします。 |
| | wlan_id | 1 ~ 512 の無線 LAN 識別子。 |

コマンドデフォルト なし

| コマンド履歴 | リリース | 変更内容 |
|--------|------|-----------------------------------|
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、802.11r 高速移行を使用して認証キー管理を設定する例を示します。

```
(Cisco Controller) >config wlan security wpa akm ft reassociation-timeout 25 1
```

config wlan security ft

802.11r 高速移行ローミング パラメータを設定するには、**config wlan security ft** コマンドを使用します。

```
config wlan security ft {adaptive | enable | disable | reassociation-timeout timeout-in-seconds}
wlan_id
```

| 構文の説明 | パラメータ | 説明 |
|-------|------------------------------|---|
| | adaptive | 802.11r 高速移行ローミング アダプティブ サポートを設定します。これがデフォルトのオプションです。 |
| | enable | 802.11r 高速移行ローミング サポートを有効にします。 |
| | disable | 802.11r 高速移行ローミング サポートを無効にします。 |
| | reassociation-timeout | 再アソシエーション期限の間隔を設定します。 |
| | <i>timeout-in-seconds</i> | 再アソシエーションのタイムアウト値（秒単位）。有効範囲は 1 ~ 100 秒です。 |
| | <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |

コマンド デフォルト なし

| コマンド履歴 | リリース | 変更内容 |
|--------|------|--|
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |
| | 8.3 | このコマンドが変更されました。 adaptive キーワードが追加されました。 |

使用上のガイドライン 先に進む前に、WLAN を無効にしたことを確認します。

次に、WLAN 2 で 802.11r 高速移行ローミング サポートを有効にする例を示します。

```
(Cisco Controller) >config wlan security ft enable 2
```

次に、WLAN 2 の 802.11r 高速移行ローミング サポートに対する再アソシエーションのタイムアウト値を 20 秒に設定する例を示します。

```
(Cisco Controller) >config wlan security ft reassociation-timeout 20 2
```


config wlan security passthru

無線 LAN で使用する IPSec パススルーを変更するには、**config wlan security passthru** コマンドを使用します。

```
config wlan security passthru {enable | disable} {wlan_id | foreignAp} [ip_address]
```

| | | |
|-----------|-------------------|--|
| 構文の説明 | enable | IPSec パススルーを有効にします。 |
| | disable | IPSec パススルーを無効にします。 |
| | <i>wlan_id</i> | 1 ～ 512 の無線 LAN 識別子。 |
| | foreignAp | サードパーティのアクセス ポイントを指定します。 |
| | <i>ip_address</i> | (任意) VPN トンネルを終端している IPSec ゲートウェイ (ルータ) の IP アドレスを入力します。 |
| コマンドデフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、無線 LAN で使用する IPSec パススルーを変更する例を示します。

```
(Cisco Controller) >config wlan security passthru enable 3 192.12.1.1
```

config wlan security pmf

WLAN の 802.11w 管理フレーム保護 (MFP) を設定するには、**config wlan security pmf** コマンドを使用します。

```
config wlan security pmf {disable | optional | required | association-comeback
association-comeback_timeout | saquery-retrytimeout saquery-retry_timeout} wlan_id
```

| | | |
|------------|-------------------------------------|---|
| 構文の説明 | disable | WLAN の 802.11w MFP 保護を無効にします。 |
| | optional | WLAN の 802.11w MFP 保護を有効にします。 |
| | required | クライアントが WLAN の 802.11w MFP 保護をネゴシエートすることを要求します。 |
| | association-comeback | 802.11w アソシエーション復帰時間を設定します。 |
| | <i>association-comeback_timeout</i> | アソシエーション復帰間隔 (秒単位)。アソシエーションがステータスコード 30 によって拒否された後に、アソシエートされているクライアントがアソシエーションを再試行するまでに待機する必要がある時間間隔。ステータスコード 30 のメッセージは、「Association request rejected temporarily; Try again later」です。 範囲は、1 ~ 20 秒です。 |
| | saquery-retrytimeout | 802.11w セキュリティアソシエーション (SA) クエリリトライタイムアウトを設定します。 |
| | <i>saquery-retry_timeout</i> | アソシエーションを再試行する前に、すでにアソシエートされているクライアントへのアソシエーション応答で特定される時間間隔。アソシエーションの復帰期間中、この時間間隔により、クライアントが実際のクライアントであり、不正なクライアントではないかどうかを確認されます。クライアントがこの時間内に応答しない場合は、クライアントアソシエーションがコントローラから削除されます。指定できる範囲は 100 ~ 500 ミリ秒です。 |
| | <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| コマンド デフォルト | | デフォルトの SA クエリリトライタイムアウトは 200 ミリ秒です。 デフォルトのアソシエーション復帰タイムアウトは 1 秒です。 |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン

802.11w では、ブロードキャストまたはマルチキャストの堅牢な管理フレームを保護するために使用される Integrity Group Temporal Key (IGTK) が導入されています。IGTK は、ソース STA からの MAC 管理プロトコルデータユニット (MMPDU) を保護するために使用するオーセンティケータステーション (コントローラ) によって割り当てられる、ランダムな値です。802.11w IGTK キーは、4 ウェイ ハンドシェイクを使用して取得され、レイヤ 2 で WPA または WPA2 セキュリティによって設定されている WLAN でのみ使用されます。

次に、WLAN の 802.11w MFP 保護を有効にする例を示します。

```
(Cisco Controller) > config wlan security pmf optional 1
```

次に、WLAN の SA クエリ リトライ タイムアウトを設定する例を示します。

```
(Cisco Controller) > config wlan security pmf saquery-retrytimeout 300 1
```

config wlan security sgt

WLAN でセキュリティグループタグ (SGT) を設定するには、**config wlan security sgt** コマンドを使用します。

```
config wlan security sgt {value | wlan-id} wlan_id
```

| | | |
|------------|----------------|-----------------|
| 構文の説明 | <i>value</i> | SGT 値 |
| | <i>wlan-id</i> | WLAN ID |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 8.4 | このコマンドが追加されました。 |

config wlan security splash-page-web-redir

スプラッシュ ページ Web リダイレクトを有効または無効にするには、**config wlan security splash-page-web-redir** コマンドを入力します。

config wlan security splash-page-web-redir {**enable** | **disable**} *wlan_id*

| | | |
|------------|-----------------------------|-----------------------------------|
| 構文の説明 | enable | スプラッシュ ページ Web リダイレクトを有効にします。 |
| | disable | スプラッシュ ページ Web リダイレクトを無効にします。 |
| | <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| コマンド デフォルト | スプラッシュ ページ Web リダイレクトは無効です。 | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、スプラッシュ ページ Web リダイレクトを有効にする例を示します。

```
(Cisco Controller) >config wlan security splash-page-web-redir enable 2
```

config wlan security static-wep-key authentication

無線 LAN で静的 Wired Equivalent Privacy (WEP) キー 802.11 認証を設定するには、**config wlan security static-wep-key authentication** コマンドを使用します。

config wlan security static-wep-key authentication {**shared-key** | **open**} *wlan_id*

| | | |
|------------|-------------------|-----------------------------------|
| 構文の説明 | shared-key | 共有キー認証を有効にします。 |
| | open | オープン システム認証を有効にします。 |
| | <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、WLAN ID 1 の静的 WEP 共有キー認証を有効にする例を示します。

```
(Cisco Controller) >config wlan security static-wep-key authentication shared-key 1
```

config wlan security static-wep-key disable

静的 Wired Equivalent Privacy (WEP) キーの使用を無効にするには、**config wlan security static-wep-key disable** コマンドを使用します。

config wlan security static-wep-key disable *wlan_id*

| | | |
|------------|----------------|-----------------------------------|
| 構文の説明 | <i>wlan_id</i> | 1 ～ 512 の無線 LAN 識別子。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、WLAN ID 1 の静的 WEP キーを無効にする例を示します。

```
(Cisco Controller) >config wlan security static-wep-key disable 1
```

config wlan security static-wep-key enable

静的 Wired Equivalent Privacy (WEP) キーの使用を有効にするには、**config wlan security static-wep-key enable** コマンドを使用します。

config wlan security static-wep-key enable *wlan_id*

| | | |
|------------|----------------|-----------------------------------|
| 構文の説明 | <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、WLAN ID 1 の静的 WEK キーを有効にする例を示します。

```
(Cisco Controller) >config wlan security static-wep-key enable 1
```


config wlan security static-wep-key encryption

静的 Wired Equivalent Privacy (WEP) キーとインデックスを設定するには、**config wlan security static-wep-key encryption** コマンドを使用します。

config wlan security static-wep-key encryption *wlan_id* {**40** | **104**} {**hex** | **ascii**} *key key-index*

| 構文の説明 | | |
|-------|------------------|------------------------------|
| | <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| | 40 | 暗号化レベルを 40 に指定します。 |
| | 104 | 暗号化レベルを 104 に指定します。 |
| | hex | キー入力に 16 進数文字を使用するように指定します。 |
| | ascii | キー入力に ASCII 文字を使用するように指定します。 |
| | <i>key</i> | ASCII の WEP キー。 |
| | <i>key-index</i> | キー インデックス (1 ~ 4) 。 |

コマンド デフォルト なし

| コマンド履歴 | リリース | 変更内容 |
|--------|------|-----------------------------------|
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン 各無線 LAN に 1 つの一意的な WEP キー インデックスを適用できます。WEP キー インデックスは 4 つしかないため、静的 WEP レイヤ 2 暗号化には 4 つの無線 LAN しか設定できません。

このコマンドを使用する前に、802.1X を無効にしてください。

次に、16 進数文字 0201702001 およびキー インデックス 2 を使用して WLAN ID 1 の静的 WEP キーを設定する例を示します。

```
(Cisco Controller) >config wlan security static-wep-key encryption 1 40 hex 0201702001
2
```

config wlan security tkip

Temporal Key Integrity Protocol (TKIP) Message Integrity Check (MIC) カウンターメジャー ホールドダウン タイマーを設定するには、**config wlan security tkip** コマンドを使用します。

config wlan security tkip hold-down time wlan_id

構文の説明

hold-down TKIP MIC カウンターメジャー ホールドダウン タイマーを設定します。

time TKIP MIC カウンターメジャー ホールドダウンの秒単位の時間。有効な範囲は 0 ~ 60 秒です。

wlan_id 1 ~ 512 の無線 LAN 識別子。

コマンド デフォルト

デフォルトの TKIP カウンターメジャーは 60 秒に設定されます。

コマンド履歴

| リリース | 変更内容 |
|------|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン

TKIP カウンターメジャー モードは、アクセス ポイントが 60 秒の期間内に 2 つの MIC エラーを受信した場合に発生することがあります。この状況が発生した場合、アクセス ポイントは、802.11 無線にアソシエートされているすべての TKIP クライアントの認証を解除し、カウンターメジャー ホールドオフ時間のクライアントを阻止します。

次に、TKIP MIC カウンターメジャー ホールドダウン タイマーを設定する例を示します。

```
(Cisco Controller) >config wlan security tkip
```

config wlan usertimeout

WLAN でアイドル状態のクライアントセッションのタイムアウトを設定するには、**config wlan usertimeout** コマンドを使用します。

config wlan usertimeout *timeout wlan_id*

構文の説明

timeout WLAN に対するアイドル状態のクライアントセッションのタイムアウト。クライアントにより送信されるトラフィックがしきい値を下回る場合、クライアントはタイムアウト時に削除されます。範囲は 15 ~ 100000 秒です。

wlan_id 1 ~ 512 の無線 LAN 識別子。

コマンドデフォルト

デフォルトのクライアントセッションアイドルタイムアウトは 300 秒です。

コマンド履歴

| リリース | 変更内容 |
|------|------|
|------|------|

| | |
|-----|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |
|-----|-----------------------------------|

使用上のガイドライン

ここで設定したタイムアウト値は、コマンド **config network usertimeout** を使用して定義するグローバルタイムアウトをオーバーライドします。

次に、WLAN でアイドル状態のクライアントセッションを設定する例を示します。

```
(Cisco Controller) >config wlan usertimeout 100 1
```

config wlan security web-auth

無線 LAN で使用する Web 認証のステータスを変更するには、**config wlan security web-auth** コマンドを使用します。

```
config wlan security web-auth {{acl | enable | disable} {wlan_id | foreignAp} [acl_name | none]} | {on-macfilter-failure wlan_id} | {server-precedence wlan_id | local | ldap | radius} | {flexacl wlan_id [ipv4_acl_name | none]} | {ipv6 acl wlan_id [ipv6_acl_name | none]} | {mac-auth-server {ip_address wlan_id}} | {timeout {value_in_seconds wlan_id}} | {web-portal-server {ip_address wlan_id}}
```

構文の説明

| | |
|-----------------------------|--|
| acl | アクセスコントロールリストを設定します。 |
| enable | Web 認証を有効にします。 |
| disable | Web 認証を無効にします。 |
| <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| foreignAp | サードパーティのアクセスポイントを指定します。 |
| <i>acl_name</i> | (任意) ACL 名 (最大 32 文字の英数字)。 |
| none | (任意) ACL 名を指定しません。 |
| on-macfilter-failure | MAC フィルタの失敗における Web 認証を有効にします。 |
| server-precedence | Web 認証ユーザに対する認証サーバの優先順位を設定します。 |
| local | サーバタイプを指定します。 |
| ldap | サーバタイプを指定します。 |
| radius | サーバタイプを指定します。 |
| flexacl | FlexConnect のアクセスコントロールリストを設定します。 |
| <i>ipv4_acl_name</i> | (任意) IPv4 ACL の名前。最大 32 文字の英数字を入力できます。 |
| <i>ipv6_acl_name</i> | (任意) IPv6 ACL の名前。最大 32 文字の英数字を入力できます。 |
| <i>ipv6</i> | IPv6 関連パラメータを設定します。 |

| | |
|--------------------------|--------------------------------------|
| mac-auth-server | WLAN の MAC 認証サーバを設定します。 |
| timeout | Web 認証タイムアウトを設定します。 |
| <i>value_in_seconds</i> | タイムアウト値 (秒) 。有効な範囲は 300 ~ 14400 秒です。 |
| web-portal-server | WLAN の CMCC Web ポータルのサーバを設定します。 |

コマンドデフォルト なし

| コマンド履歴 | リリース | 変更内容 |
|--------|------|-----------------------------------|
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、WLAN ID 1 および ACL03 という名前の ACL のセキュリティ ポリシーを設定する例を示します。

```
(Cisco Controller) >config wlan security web-auth acl 1 ACL03
```

config wlan security web-auth captive-bypass

ワイヤレス LAN のキャプティブ バイパスを設定するには、**config wlan security web-auth captive-bypass** コマンドを使用します。

config wlan security web-auth captive-bypass { **enable** | **disable** | **none** }

| 構文の説明 | enable | WLAN のキャプティブ バイパスを有効にします。 |
|-------|----------------|---|
| | disable | WLAN のキャプティブ バイパスを無効にします。 |
| | none | WLAN のキャプティブ バイパス設定をオフにします。グローバルなキャプティブ ネットワーク アシスタント バイパス設定が適用されます |
| | <i>wlan-id</i> | 1 ~ 16 の WLAN 識別子を入力します。 |

コマンド履歴

| リリース | 変更内容 |
|------|-----------------|
| 8.4 | このコマンドが追加されました。 |

次に、キャプティブ ネットワーク バイパスを有効にする例を示します。

```
(Cisco Controller) >config wlan security web-auth captive-bypass enable 1
```

config wlan security web-auth qrscan-des-key

WLAN 内で QR スキャン DES キーを設定するには、**config wlan security web-auth qrscan-des-key** コマンドを使用します。

config wlan security web-auth qrscan-des-key {*DES key string**wlan_id* }

| 構文の説明 | | |
|--------|------------------|--------------------------|
| | <i>DES</i> キー文字列 | 8 文字の DES キーを入力します。 |
| | <i>wlan-id</i> | 1 ~ 16 の WLAN 識別子を入力します。 |
| コマンド履歴 | リリース | 変更内容 |
| | 8.4 | このコマンドが導入されました。 |

次に、QR スキャン DES キーを設定する例を示します。

```
(Cisco Controller) >config wlan security web-auth qrscan-des-key 1
```

config wlan security web-passthrough acl

アクセスコントロールリスト (ACL) を無線 LAN 定義に追加するには、**config wlan security web-passthrough acl** コマンドを使用します。

```
config wlan security web-passthrough acl {wlan_id | foreignAp} {acl_name | none}
```

| | | |
|-----------|------------------|-----------------------------------|
| 構文の説明 | <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| | foreignAp | サードパーティのアクセス ポイントを指定します。 |
| | <i>acl_name</i> | ACL 名 (最大 32 文字の英数字)。 |
| | none | ACL がないことを指定します。 |
| コマンドデフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、ACL を無線 LAN 定義に追加する例を示します。

```
(Cisco Controller) >config wlan security web-passthrough acl 1 ACL03
```


config wlan security web-passthrough disable

無線 LAN で認証不要の Web キャプティブ ポータルを無効にするには、**config wlan security web-passthrough disable** コマンドを使用します。

config wlan security web-passthrough disable {*wlan_id* | **foreignAp**}

| | | |
|-----------|------------------|-----------------------------------|
| 構文の説明 | <i>wlan_id</i> | 1 ～ 512 の無線 LAN 識別子。 |
| | foreignAp | サードパーティのアクセス ポイントを指定します。 |
| コマンドデフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、無線 LAN ID 1 で認証不要の Web キャプティブ ポータルを無効にする例を示します。

```
(Cisco Controller) >config wlan security web-passthrough disable 1
```

config wlan security web-passthrough email-input

電子メールアドレスを使用して Web キャプティブ ポータルを設定するには、**config wlan security web-passthrough email-input** コマンドを使用します。

config wlan security web-passthrough email-input {enable | disable} {wlan_id | foreignAp}

| | | |
|------------|--------------------|--|
| 構文の説明 | email-input | 電子メールアドレスを使用して Web キャプティブ ポータルを設定します。 |
| | enable | 電子メールアドレスを使用して Web キャプティブ ポータルを有効にします。 |
| | disable | 電子メールアドレスを使用して Web キャプティブ ポータルを無効にします。 |
| | <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| | foreignAp | サードパーティのアクセス ポイントを指定します。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、電子メールアドレスを使用して Web キャプティブ ポータルを設定する例を示します。

```
(Cisco Controller) >config wlan security web-passthrough email-input enable 1
```

config wlan security web-passthrough enable

無線 LAN で認証不要の Web キャプティブ ポータルを有効にするには、**config wlan security web-passthrough enable** コマンドを使用します。

config wlan security web-passthrough enable {*wlan_id* | **foreignAp**}

| | | |
|------------|------------------|-----------------------------------|
| 構文の説明 | <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| | foreignAp | サードパーティのアクセス ポイントを指定します。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、無線 LAN ID 1 で認証不要の Web キャプティブ ポータルを有効にする例を示します。

```
(Cisco Controller) >config wlan security web-passthrough enable 1
```

config wlan security web-passthrough qr-scan

WLAN で QR スキャンを有効または無効にするには、**config wlan security web-passthrough qr-scan** コマンドを使用します。

config wlan security web-passthrough qr-scan {{localenable | disable} | enable | disable}

| | | |
|------------|----------------|--|
| 構文の説明 | local | クライアントの AP でローカルでサポートされる QR コード スキャンを設定します。 <ul style="list-style-type: none"> • enable—クライアントに対する QR コード スキャンのサポートを有効にします。 • disable—クライアントに対する QR コード スキャンのサポートを無効にします。 |
| | enable | クライアントに対する QR コード スキャンのサポートを有効にします。 |
| | disable | クライアントに対する QR コード スキャンのサポートを無効にします。 |
| | <i>wlan-id</i> | 1 ~ 16 の WLAN 識別子を入力します。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 8.4 | このコマンドが導入されました。 |

次に、WLAN ID 1 で QR スキャンをイネーブルにする例を示します。

```
(Cisco Controller) >config wlan security web-passthrough qr-scan enable 1
```

config wlan security wpa akm 802.1x

802.1X を使用して認証キー管理（AKM）を設定するには、**config wlan security wpa akm 802.1x** コマンドを使用します。

config wlan security wpa akm 802.1x {enable | disable} *wlan_id*

| | | |
|-----------|----------------|-----------------------------------|
| 構文の説明 | enable | 802.1X サポートを有効にします。 |
| | disable | 802.1X サポートを無効にします。 |
| | <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| コマンドデフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、802.1X を使用して認証を設定する例を示します。

```
(Cisco Controller) >config wlan security wpa akm 802.1x enable 1
```

config wlan security wpa akm cckm

Cisco Centralized Key Management (CCKM) を使用して認証キー管理を設定するには、**config wlan security wpa akm cckm** コマンドを使用します。

config wlan security wpa akm cckm { **enable** *wlan_id* | **disable** *wlan_id* | *timestamp-tolerance* }

| | | |
|------------|----------------------------|--|
| 構文の説明 | enable | CCKM サポートを有効にします。 |
| | disable | CCKM サポートを無効にします。 |
| | <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| | <i>timestamp-tolerance</i> | CCKM IE のタイムスタンプのトレランス。有効な範囲は 1000 ~ 5000 ミリ秒です。デフォルトは 1000 ミリ秒です。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、CCKM を使用して認証キー管理を設定する例を示します。

```
(Cisco Controller) >config wlan security wpa akm cckm 1500
```

config wlan security wpa akm ft

802.11r 高速移行 802.1X を使用して認証キー管理を設定するには、**config wlan security wpa akm ft** コマンドを使用します。

config wlan security wpa akm ft [**over-the-air** | **over-the-ds** | **psk** | [**reassociation-timeout seconds**]] {**enable** | **disable**} *wlan_id*

| | | |
|-----------|------------------------------|--|
| 構文の説明 | over-the-air | (任意) 802.11r 高速移行地上波ローミングサポートを設定します。 |
| | over-the-ds | (任意) 802.11r 高速移行ローミング DS サポートを設定します。 |
| | psk | (任意) 802.11r 高速移行 PSK サポートを設定します。 |
| | reassociation-timeout | (任意) 再アソシエーションの期限間隔を設定します。 有効な範囲は 1 ～ 100 秒です。デフォルト値は 20 秒です。 |
| | <i>seconds</i> | 再アソシエーションの期限間隔 (秒単位)。 |
| | enable | 802.11r 高速移行 802.1X サポートを有効にします。 |
| | disable | 802.11r 高速移行 802.1X サポートを無効にします。 |
| | <i>wlan_id</i> | 1 ～ 512 の無線 LAN 識別子。 |
| コマンドデフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、802.11r 高速移行を使用して認証キー管理を設定する例を示します。

```
(Cisco Controller) >config wlan security wpa akm ft reassociation-timeout 25 1
```

config wlan security wpa akm pmf

管理フレームの認証キー管理（AKM）を設定するには、**config wlan security wpa akm pmf** コマンドを使用します。

config wlan security wpa akm pmf {802.1x | psk} {enable | disable} wlan_id

構文の説明

802.1x 管理フレームの保護（PMF）の 802.1X 認証を設定します。

psk PMF の事前共有キー（PSK）を設定します。

enable PMF の 802.1X 認証または PSK を有効にします。

disable PMF の 802.1X 認証または PSK を無効にします。

wlan_id 1 ~ 512 の無線 LAN 識別子。

コマンド デフォルト

ディセーブル

コマンド履歴

| リリース | 変更内容 |
|------|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン

802.11w には、00-0F-AC:5 または 00-0F-AC:6 の 2 つの新しい AKM スイートがあります。WPA を有効にし、次に WLAN を無効にして WLAN 上で PMF を設定する必要があります。

次に、WLAN の PMF の 802.1X 認証を有効にする例を示します。

```
(Cisco Controller) >config wlan security wpa akm pmf 802.1x enable 1
```


config wlan security wpa akm psk

Wi-Fi Protected Access (WPA) 事前共有キー モードを設定するには、**config wlan security wpa akm psk** コマンドを使用します。

config wlan security wpa akm psk {**enable** | **disable** | **set-key** *key-format* *key*} *wlan_id*

| | | |
|-----------|-------------------|---------------------------------------|
| 構文の説明 | enable | WPA-PSK を有効にします。 |
| | disable | WPA-PSK を無効にします。 |
| | set-key | 事前共有キーを設定します。 |
| | <i>key-format</i> | キー形式を指定します。ASCII または 16 進数のいずれかになります。 |
| | <i>key</i> | WPA 事前共有キー。 |
| | <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| コマンドデフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、WPA 事前共有キー モードを設定する例を示します。

```
(Cisco Controller) >config wlan security wpa akm psk disable 1
```

config wlan security wpa disable

WPA1 を無効にするには、**config wlan security wpa disable** コマンドを使用します。

config wlan security wpa disable *wlan_id*

| | | |
|------------|----------------|-----------------------------------|
| 構文の説明 | <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、WPA を無効にする例を示します。

```
(Cisco Controller) >config wlan security wpa disable 1
```

config wlan security wpa enable

WPA1 を有効にするには、**config wlan security wpa enable** コマンドを使用します。

config wlan security wpa enable *wlan_id*

| | | |
|------------|----------------|-----------------------------------|
| 構文の説明 | <i>wlan_id</i> | 1 ～ 512 の無線 LAN 識別子。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、WLAN ID 1 で WPA を設定する例を示します。

```
(Cisco Controller) >config wlan security wpa enable 1
```

config wlan security wpa ciphers

Wi-Fi 保護認証 (WPA1) または Wi-Fi 保護認証 (WPA2) を設定するには、**config wlan security wpa ciphers** コマンドを使用します。

config wlan security wpa {wpa1 | wpa2} ciphers {aes | tkip} {enable | disable} wlan_id

構文の説明

| | |
|----------------|--------------------------|
| wpa1 | WPA1 サポートを設定します。 |
| wpa2 | WPA2 サポートを設定します。 |
| ciphers | WPA 暗号方式を設定します。 |
| aes | AES 暗号化のサポートを設定します。 |
| tkip | TKIP 暗号化のサポートを設定します。 |
| enable | WPA AES/TKIP モードを有効にします。 |
| disable | WPA AES/TKIP モードを無効にします。 |
| wlan_id | 1 ~ 512 の無線 LAN 識別子。 |

コマンド デフォルト

なし

コマンド履歴

| リリース | 変更内容 |
|------|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン

WPA バージョンを指定しない場合は、次のようになります。

- 有効化された暗号が AES の場合、WPA2/AES を設定しています。
- 有効化された暗号が AES+TKIP の場合、WPA/TKIP、WPA2/AES、または WPA/TKIP を設定しています。
- 有効化された暗号が TKIP の場合、WPA/TKIP または WPA2/TKIP を設定しています。

リリース 8.0 から、スタンドアロン暗号化方式として TKIP を設定できなくなりました。TKIP は、AES 暗号化方式でのみ使用できます。

次に、WPA を暗号化する例を示します。

```
(Cisco Controller) >config wlan security wpa wpa1 ciphers aes enable 1
```

config wlan security wpa gtk-random

WLAN のアクセス ポイントとクライアントとの間で Group Temporal Key (GTK) のランダム化を有効にするには、**config wlan security wpa gtk-random** コマンドを使用します。

```
config wlan security wpa gtk-random {enable | disable} wlan_id
```

構文の説明

enable アクセスポイントとクライアント間の GTK キーのランダム化を有効にします。

disable アクセスポイントとクライアント間の GTK キーのランダム化を無効にします。

wlan_id 1 ~ 512 の WLAN 識別子。

コマンドデフォルト

なし

コマンド履歴

| リリース | 変更内容 |
|------|------|
|------|------|

| | |
|-----|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |
|-----|-----------------------------------|

使用上のガイドライン

このコマンドを有効にすると、基本サービスセット (BSS) のクライアントに一意的 GTK キーが提供されます。クライアントは、マルチキャストトラフィックまたはブロードキャストトラフィックを受信しません。

次に、WLAN でアソシエートされている各クライアントの GTK のランダム化を有効にする例を示します。

```
(Cisco Controller) >config wlan security wpa gtk-random enable 3
```

config wlan security wpa osen disable

WLAN で OSU Server-Only Authenticated L2 Encryption Network (OSEN) を無効にするには、WLAN コンフィギュレーション モードで **config wlan security wpa osen enable** コマンドを使用します。

config wlan security wpa osen disable *wlan-id*

| 構文の説明 | <i>wlan-id</i> WLANID 番号。1 ~ 512 の値を入力します。 | | | | |
|------------|--|------|------|----------|-----------------|
| コマンド デフォルト | OSEN が有効になります。 | | | | |
| コマンド モード | WLAN の設定 | | | | |
| コマンド履歴 | <table border="1"> <thead> <tr> <th>リリース</th> <th>変更内容</th> </tr> </thead> <tbody> <tr> <td>リリース 8.2</td> <td>このコマンドが導入されました。</td> </tr> </tbody> </table> | リリース | 変更内容 | リリース 8.2 | このコマンドが導入されました。 |
| リリース | 変更内容 | | | | |
| リリース 8.2 | このコマンドが導入されました。 | | | | |

次に、WLAN で OSEN を無効にする例を示します。

```
Cisco Controller > config wlan security wpa osen disable 12
```

config wlan security wpa osen enable

WLAN で OSU Server-Only Authenticated L2 Encryption Network (OSEN) を有効にするには、WLAN コンフィギュレーションモードで **config wlan security wpa osen enable** コマンドを使用します。

config wlan security wpa osen enable *wlan-id*

構文の説明

wlan-id WLANID 番号。1～512 の値を入力します。

コマンド デフォルト

OSEN が有効ではありません

コマンド モード

WLAN の設定

コマンド履歴

| リリース | 変更内容 |
|------|------|
|------|------|

| | |
|------|------------------------|
| リリース | このコマンドが導入されました。 8.2 |
|------|------------------------|

次に、WLAN で OSEN を有効にする例を示します。

```
Cisco Controller > config wlan security wpa osen enable 12
```

config wlan security wpa wpa1 disable

WPA1 を無効にするには、**config wlan security wpa wpa1 disable** コマンドを使用します。

config wlan security wpa wpa1 disable *wlan_id*

| | | |
|------------|----------------|-----------------------------------|
| 構文の説明 | <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、WPA1 を無効にする例を示します。

```
(Cisco Controller) >config wlan security wpa wpa1 disable 1
```


config wlan security wpa wpa1 enable

WPA1 を有効にするには、**config wlan security wpa wpa1 enable** コマンドを使用します。

config wlan security wpa wpa1 enable *wlan_id*

| | | |
|------------|----------------|-----------------------------------|
| 構文の説明 | <i>wlan_id</i> | 1 ～ 512 の無線 LAN 識別子。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、WPA1 を有効にする例を示します。

```
(Cisco Controller) >config wlan security wpa wpa1 enable 1
```

config wlan security wpa wpa2 disable

WPA2 を無効にするには、**config wlan security wpa wpa2 disable** コマンドを使用します。

config wlan security wpa wpa2 disable *wlan_id*

| | | |
|------------|----------------|-----------------------------------|
| 構文の説明 | <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、WPA2 を無効にする例を示します。

```
(Cisco Controller) >config wlan security wpa wpa2 disable 1
```

config wlan security wpa wpa2 enable

WPA2 を有効にするには、**config wlan security wpa wpa2 enable** コマンドを使用します。

config wlan security wpa wpa2 enable *wlan_id*

構文の説明*wlan_id*1 ～ 512 の無線 LAN 識別子。

コマンド デフォルトなし

コマンド履歴

| リリース | 変更内容 |
|------|------|
|------|------|

| | |
|-----|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |
|-----|-----------------------------------|

次に、WPA2 を有効にする例を示します。

```
(Cisco Controller) >config wlan security wpa wpa2 enable 1
```

config wlan security wpa wpa2 cache

WLAN のキャッシュ方法を設定するには、**config wlan security wpa wpa2 cache** コマンドを使用します。

config wlan security wpa wpa2 cache sticky {enable | disable} wlan_id

構文の説明

sticky WLAN の Sticky Key Caching (SKC) ローミングサポートを設定します。

enable WLAN で SKC ローミングサポートを有効にします。

disable WLAN で SKC ローミングサポートを無効にします。

wlan_id 1 ~ 512 の無線 LAN 識別子。

コマンドデフォルト

なし

コマンド履歴

| リリース | 変更内容 |
|------|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン

PKC (Pro Active Key caching) とも呼ばれる SKC (Sticky Key caching) では、クライアントは Pairwise Master Key Security Association (PMKSA) に対して各 Pairwise Master Key (PMK) ID (PMKID) を保存します。クライアントがそれに対する PMKSA を保持する AP を見つけた場合、アソシエーション要求内で PMKID を AP に送信します。PMKSA が AP で稼働している場合は、AP は、高速ローミングをサポートします。SKC では、クライアントがアソシエートする新しい AP に関して完全な認証が実行され、すべての AP とアソシエートされる PMKSA をクライアントが維持しなければなりません。

次に、WLAN の SKC ローミングサポートを有効にする例を示します。

```
(Cisco Controller) >config wlan security wpa wpa2 cache sticky enable 1
```

config wlan security wpa wpa2 cache sticky

WLAN の Sticky PMKID Caching (SKC) を設定するには、`config wlan security wpa wpa2 cache sticky` コマンドを使用します。

`config wlan security wpa wpa2 cache sticky {enable | disable} wlan_id`

| | | |
|------------|-----------------------------|-----------------------------------|
| 構文の説明 | enable | WLAN でSKCを有効にします。 |
| | disable | WLAN でSKCを無効にします。 |
| | wlan_id | 1 ~ 512 の無線 LAN 識別子。 |
| コマンド デフォルト | Stkcky PMKID Caching は無効です。 | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン リリース 7.2 以降のリリースから、Sticky PMKID Caching (SKC) をサポートします。sticky PMKID キャッシュにより、クライアントは、アソシエートする AP ごとに異なる PMKID を受信し、保存します。AP も、クライアントに発行される PMKID のデータベースを維持します。PKC (Proactive Key Caching) と呼ばれる SKC では、クライアントは Pairwise Master Key Security Association (PMKSA) に対して各 Pairwise Master Key (PMK) ID (PMKID) を保存します。クライアントがそれに対する PMKSA を保持する AP を見つけた場合、アソシエーション要求内で PMKID を AP に送信します。PMKSA が AP で稼働している場合は、AP は、高速ローミングをサポートします。SKC では、クライアントがアソシエートする新しい AP に関して完全な認証が実行され、すべての AP とアソシエートされる PMKSA をクライアントが維持しなければなりません。SKC の場合、PMKSA はクライアントが保存する AP のキャッシュごとであり、新しい AP の BSSID に基づいて事前に計算されます。

- コントローラは最大 8 つの SKC しかサポートしていないため、大規模な展開に SKC を使用することはできません。
- SKC は、モビリティ グループのアクセス コントローラでは機能しません。
- SKC は、WPA2 が有効になっている WLAN でのみ動作します。
- SKC はローカル モードの AP でのみ動作します。

次に、WLAN 5 で Sticky PMKID Caching を有効にする例を示します。

```
(Cisco Controller) >config wlan security wpa wpa2 cache sticky enable 5
```

config wlan security wpa wpa2 ciphers

WPA2 暗号方式を設定し、WPA2 の Advanced Encryption Standard (AES) または Temporal Key Integrity Protocol (TKIP) データ暗号化を有効または無効にするには、**config wlan security wpa wpa2 ciphers** コマンドを使用します。

config wlan security wpa wpa2 ciphers {**aes** | **tkip**} {**enable** | **disable**} *wlan_id*

構文の説明

(Cisco Controller) > **aes** WPA2 に対する AES データ暗号化を設定します。

tkip WPA2 に対する TKIP データ暗号化を設定します。

enable WPA2 に対する AES または TKIP データ暗号化を有効にします。

disable WPA2 の AES または TKIP データ暗号化を無効にします。

wlan_id 1 ~ 512 の無線 LAN 識別子。

コマンド デフォルト

AES はデフォルトで有効です。

コマンド履歴

| リリース | 変更内容 |
|------|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、WPA2 に対する AES データ暗号化を有効にする例を示します。

```
(Cisco Controller) >config wlan security wpa wpa2 ciphers aes enable 1
```

config wlan session-timeout

無線 LAN クライアントのタイムアウトを変更するには、**config wlan session-timeout** コマンドを使用します。

config wlan session-timeout {*wlan_id* | **foreignAp**} *seconds*

構文の説明

| | |
|------------------|---|
| <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| foreignAp | サードパーティのアクセス ポイントを指定します。 |
| <i>seconds</i> | タイムアウトまたはセッション時間 (秒)。値 0 は、タイムアウトなしに相当します。 (注) セッション タイムアウトの範囲は、セキュリティ タイプによって異なります。 <ul style="list-style-type: none"> • オープン システム : 0 ~ 65535 (秒) • 802.1x : 300 ~ 86400 (秒) • Static WEP : 0 ~ 65535 (秒) • Cranite : 0 ~ 65535 (秒) • Fortress : 0 ~ 65535 (秒) • CKIP : 0 ~ 65535 (秒) • Open + Web Auth : 0 ~ 65535 (秒) • Web Pass-thru : 0 ~ 65535 (秒) • WPA-PSK : 0 ~ 65535 (秒) • disable : 再認証/セッション タイムアウト タイマーを無効にします。 |

コマンドデフォルト

なし

使用上のガイドライン

PMK キャッシュを作成する 802.1x クライアント セキュリティ タイプでは、セッション タイムアウトが無効になっている場合、設定できる最大セッションタイムアウトは 86400 秒です。PMK キャッシュが作成されない、オープン、WebAuth、PSK などのその他のクライアント セキュリティでは、セッション タイムアウトが無効になっている場合、セッション タイムアウト値は [infinite] と表示されます。

コマンド履歴

| リリース | 変更内容 |
|------|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、WLAN ID 1 に対してクライアントのタイムアウトを 6000 秒に設定する例を示します。

```
(Cisco Controller) >config wlan session-timeout 1 6000
```


config wlan sip-cac disassoc-client

セッション開始プロトコル (SIP) のコール アドミッション制御 (CAC) の障害時にクライアントのディスアソシエーションをイネーブルにするには、**config wlan sip-cac disassoc-client** コマンドを使用します。

config wlan sip-cac disassoc-client {enable | disable} wlan_id

| 構文の説明 | enable | SIP CAC 障害時のクライアントのディスアソシエーションをイネーブルにします。 |
|-------|---------|--|
| | disable | SIP CAC 障害時のクライアントのディスアソシエーションをディセーブルにします。 |
| | wlan_id | 1 ~ 512 の無線 LAN 識別子。 |

コマンド デフォルト SIP CAC のクライアントのディスアソシエーションがディセーブルです。

| コマンド履歴 | リリース | 変更内容 |
|--------|------|-----------------------------------|
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、WLAN ID が 1 である SIP CAC 障害時のクライアントのディスアソシエーションをイネーブルにする例を示します。

```
(Cisco Controller) >config wlan sip-cac disassoc-client enable 1
```

config wlan sip-cac send-486busy

SIP コール アドミッション制御 (CAC) の障害が発生した場合にセッション開始プロトコル (SIP) の 486 Busy メッセージを送信するように設定するには、**config wlan sip-cac send-486busy** コマンドを使用します。

```
config wlan sip-cac send-486busy {enable | disable} wlan_id
```

| | | |
|-------|----------------|--|
| 構文の説明 | enable | SIP CAC 障害時の SIP 486 Busy メッセージの送信をイネーブルにします。 |
| | disable | SIP CAC 障害時の SIP 486 Busy メッセージの送信をディセーブルにします。 |
| | <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |

コマンド デフォルト セッション開始プロトコルはデフォルトで有効です。

| コマンド履歴 | リリース | 変更内容 |
|--------|------|-----------------------------------|
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、WLAN ID が 1 である SIP CAC 障害時の SIP 486 Busy メッセージの送信をイネーブルにする方法を示します。

```
(Cisco Controller) >config wlan sip-cac send-busy486 enable 1
```

config wlan ssid

WLANに関連付けられている SSID を編集するには、**config wlan ssid** コマンドを使用します。

config wlan ssid *wlan_id ssid*

| | | |
|-----------|----------------|----------------------------------|
| 構文の説明 | <i>wlan_id</i> | 1~512 の WLAN 識別子。 |
| | <i>ssid</i> | WLANに関連付けられているサービスセット識別子 (SSID)。 |
| コマンドデフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 8.0 | このコマンドが導入されました。 |

次に、WLANに関連付けられている SSID を編集する例を示します。

```
(Cisco Controller) >config wlan disable 1
(Cisco Controller) >config wlan ssid 1 new_samp
(Cisco Controller) >show wlan summary
Number of WLANs..... 1

WLAN ID   WLAN Profile Name / SSID   Status   Interface Name   PMIPv6 Mobility
-----
1         sample / new_samp         Disabled management   none
```

config wlan static-ip tunneling

WLAN でスタティック IP クライアント トンネリングのサポートを設定するには、**config wlan static-ip tunneling** コマンドを使用します。

```
config wlan static-ip tunneling {enable | disable} wlan_id
```

| | | |
|------------|------------------|--|
| 構文の説明 | tunneling | WLAN でスタティック IP クライアント トンネリングのサポートを設定します。 |
| | enable | WLAN でスタティック IP クライアント トンネリングのサポートをイネーブルにします。 |
| | disable | WLAN でスタティック IP クライアント トンネリングのサポートをディセーブルにします。 |
| | <i>wlan_id</i> | 1 ~ 512 の無線 LAN 識別子。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、WLAN ID 3 のスタティック IP クライアント トンネリングのサポートをイネーブルにする例を示します。

```
(Cisco Controller) >config wlan static-ip tunneling enable 34
```

config wlan uapsd compliant client enable

WPA1 を有効にするには、**config wlan uapsd compliant-client enable** コマンドを使用します。



(注) これは Ascom WMM 非対応電話機向けに導入されたもので、Cisco 792x/9971 IPフォンには適用されません。

config wlan uapsd compliant-client enable *wlan-id*

構文の説明

wlan_id 1 ～ 512 の無線 LAN 識別子。

コマンド デフォルト

なし

| リリース | 変更内容 |
|------|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、WPA1 を有効にする例を示します。

```
(Cisco Controller) >config wlan uapsd compliant-client enable 1
```

| プロパティタイプ | プロパティ値 | プロパティの説明 |
|----------|--------|----------|
|----------|--------|----------|

config wlan uapsd compliant-client disable

WPA1 を無効にするには、**config wlan uapsd compliant-client disable** コマンドを使用します。



(注) これは Ascom WMM 非対応電話機向けに導入されたもので、Cisco 792x/9971 IPフォンには適用されません。

config wlan uapsd compliant-client disable *wlan-id*

構文の説明

wlan_id 1 ~ 512 の無線 LAN 識別子。

コマンド デフォルト

なし

| リリース | 変更内容 |
|------|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、WPA1 を有効にする例を示します。

```
(Cisco Controller) >config wlan uapsd compliant-client disable 1
```

config wlan url-acl

WLAN の URL ACL を設定するには、**config wlan url-acl** コマンドを使用します。

config wlan url-acl*WLAN-id acl-name*

| | | |
|-----------|-----------------|--------------------------|
| 構文の説明 | <i>WLAN-id</i> | WLAN 識別子。範囲は 1 ~ 512 です。 |
| | <i>acl-name</i> | ACL の名前 |
| コマンドデフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 8.3 | このコマンドが導入されました。 |

次に、WLAN の URL ACL を設定する例を示します。

```
(Cisco Controller) >config wlan url-acl 3 testacl
```

config wlan user-idle-threshold

WLAN クライアントセッションのアイドルタイムアウト中に、クライアントから送信されるしきい値のデータを設定するには、**config wlan user-idle-threshold** コマンドを使用します。

config wlan user-idle-threshold bytes wlan_id

構文の説明

bytes WLAN クライアントセッションのアイドルタイムアウト中にクライアントから送信されるしきい値のデータ。クライアントにより送信されるトラフィックが、定義されているしきい値を下回る場合、クライアントはタイムアウト時に削除されます。範囲は 0 ~ 10000000 バイトです。

wlan_id 1 ~ 512 の無線 LAN 識別子。

コマンド デフォルト

アイドルタイムアウト中に、クライアントによりしきい値データが送信されるデフォルトのタイムアウトは 0 バイトです。

コマンド履歴

| リリース | 変更内容 |
|------|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、WLAN クライアントセッションのアイドルタイムアウト中にクライアントから送信されるしきい値データを設定する例を示します。

```
(Cisco Controller) >config wlan user-idle-threshold 100 1
```


config wlan usertimeout

WLAN でアイドル状態のクライアントセッションのタイムアウトを設定するには、**config wlan usertimeout** コマンドを使用します。

config wlan usertimeout *timeout wlan_id*

構文の説明

timeout WLAN に対するアイドル状態のクライアントセッションのタイムアウト。クライアントにより送信されるトラフィックがしきい値を下回る場合、クライアントはタイムアウト時に削除されます。範囲は 15 ~ 100000 秒です。

wlan_id 1 ~ 512 の無線 LAN 識別子。

コマンドデフォルト

デフォルトのクライアントセッションアイドルタイムアウトは 300 秒です。

コマンド履歴

| リリース | 変更内容 |
|------|------|
|------|------|

| | |
|-----|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |
|-----|-----------------------------------|

使用上のガイドライン

ここで設定したタイムアウト値は、コマンド **config network usertimeout** を使用して定義するグローバルタイムアウトをオーバーライドします。

次に、WLAN でアイドル状態のクライアントセッションを設定する例を示します。

```
(Cisco Controller) >config wlan usertimeout 100 1
```

config wlan webauth-exclude

Web 認証ポリシーが期限切れになった時点でゲスト ユーザの IP アドレスを解放し、3 分間 IP アドレスを取得できないよう、そのゲストユーザを除外するには、**config wlan webauth-exclude** コマンドを使用します。

config wlan webauth-exclude *wlan_id* { **enable** | **disable** }

構文の説明

| | |
|----------------|-----------------------|
| <i>wlan_id</i> | 無線 LAN 識別子 (1~512)。 |
| enable | Web 認証の除外をイネーブルにします。 |
| disable | Web 認証の除外をディセーブルにします。 |

コマンド デフォルト

ディセーブル

コマンド履歴

| リリース | 変更内容 |
|------|-----------------------------------|
| 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン

このコマンドは、Web 認証が設定されているゲスト WLAN に使用できます。

コントローラに内部 DHCP スコープを設定するときに、このコマンドを適用できます。

デフォルトでは、ゲスト ユーザの Web 認証タイマーが期限切れになった時点で、ゲスト ユーザは、別のゲスト ユーザがその IP アドレスを取得する前にただちに同じ IP アドレスを再アソシエートすることができます。DHCP プールに多数のゲスト ユーザまたは制限付きの IP アドレスが存在する場合、一部のゲスト ユーザが IP アドレスを取得できない場合があります。

ゲスト WLAN でこの機能を有効にすると、Web 認証ポリシーが期限切れになった時点でゲスト ユーザの IP アドレスが解放され、そのゲスト ユーザは IP アドレスを取得できないよう、3 分間除外されます。その IP アドレスは、別のゲスト ユーザが使用できます。3 分経過すると、除外されていたゲスト ユーザは再アソシエートし、可能であれば IP アドレスを取得できるようになります。

次に、WLAN ID 5 の Web 認証除外をイネーブルにする例を示します。

```
(Cisco Controller) >config wlan webauth-exclude 5 enable
```

config wlan wgb broadcast-tagging

WLAN で WGB ブロードキャスト タギングを設定するには、**config wlan wgb broadcast-tagging** コマンドを使用します。

config wlan wgb broadcast-tagging {enable |disable} wlan-id

| | | |
|-------|----------------|---|
| 構文の説明 | enable | WLAN でダウンリンク ブロードキャスト パケットの VLAN タギングを有効にします。 |
| | disable | WLAN でダウンリンク ブロードキャスト パケットの VLAN タギングを無効にします。 |
| | <i>wlan-id</i> | 設定を適用する WLAN ID。 |

コマンド デフォルト WGB ブロードキャスト タギングはデフォルトで無効に設定されています。

| | | |
|--------|------|-----------------|
| コマンド履歴 | リリース | 変更内容 |
| | 8.3 | このコマンドが導入されました。 |

次に、WLAN ID 1 で WGB ブロードキャスト タギングをイネーブルにする例を示します。

```
(Cisco Controller) >config wlan wgb broadcast-tagging wlan 1
```

config wlan wifidirect

WLAN で Wi-Fi Direct クライアント ポリシーを設定するには、**config wlan wifidirect** コマンドを使用します。

config wlan wifidirect { **allow** | **disable** | **not-allow** | **xconnect-not-allow** } *wlan_id*

| | | |
|------------|---------------------------|---|
| 構文の説明 | allow | Wi-Fi Direct クライアントと WLAN のアソシエーションを許可します。 |
| | disable | クライアントの Wi-Fi Direct ステータスを無視し、それによって Wi-Fi Direct クライアントのアソシエーションを許可します。 |
| | not-allow | Wi-Fi Direct クライアントと WLAN のアソシエーションを禁止します。 |
| | xconnect-not-allow | AP による、Wi-Fi Direct オプションが有効になっているクライアントのアソシエーションの許可を有効にしますが、クライアント (Wi-Fi 標準に従って動作する場合は、ピアツーピア接続を差し控えます。 |
| | <i>wlan_id</i> | 無線 LAN 識別子 (1 ~ 16)。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、WLAN ID 1 で Wi-Fi Direct クライアント ポリシーを許可する例を示します。

```
(Cisco Controller) >config wlan wifidirect allow 1
```

config wlan wmm

無線 LAN に Wi-Fi マルチメディア (WMM) モードを設定するには、**config wlan wmm** コマンドを使用します。

config wlan wmm {**allow** | **disable** | **require**} *wlan_id*

| | | |
|-------|----------------|------------------------------------|
| 構文の説明 | allow | 無線 LAN で WMM を許可します。 |
| | disable | 無線 LAN で WMM をディセーブルにします。 |
| | require | 指定した無線 LAN でクライアントに WMM の使用を指定します。 |
| | <i>wlan_id</i> | 無線 LAN 識別子 (1～512)。 |

コマンドデフォルト なし

| コマンド履歴 | リリース | 変更内容 |
|--------|------|-----------------------------------|
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン コントローラがレイヤ2モードで、WMMが有効化されている場合にアクセスポイントをコントローラに結合できるようにするには、これらのアクセスポイントをトランクポート上に配置する必要があります。

次に、WMM を許可にするように無線 LAN ID 1 を設定する例を示します。

```
(Cisco Controller) >config wlan wmm allow 1
```

次に、クライアントによる WMM の使用を指定するように無線 LAN ID 1 を設定する例を示します。

```
(Cisco Controller) >config wlan wmm require 1
```

config wps ap-authentication

アクセスポイントのネイバー認証を設定するには、**config wps ap-authentication** コマンドを使用します。

config wps ap-authentication [**enable** | **disable** **threshold** *threshold_value*]

| 構文の説明 | enable | (任意) 無線LANでWMMを有効にします。 |
|-------|------------------------|------------------------------------|
| | disable | (任意) 無線LANでWMMを無効にします。 |
| | threshold | (任意) 無線LANのWMM対応クライアントであることを指定します。 |
| | <i>threshold_value</i> | しきい値 (1 ~ 255)。 |

コマンドデフォルト なし

| コマンド履歴 | リリース | 変更内容 |
|--------|------|---------------------------------|
| | 7.6 | このコマンドは、リリース7.6以前のリリースで導入されました。 |

次に、アクセスポイントネイバー認証を設定する例を示します。

```
(Cisco Controller) > config wps ap-authentication threshold 25
```

関連コマンド **show wps ap-authentication summary**

config wps auto-immune

サービス拒否 (DoS) 攻撃からの保護を有効または無効にするには、**config wps auto-immune** コマンドを使用します。

config wps auto-immune {enable | disable | stop}

| | | |
|-------|----------------|---------------------|
| 構文の説明 | enable | 自己免疫機能を有効にします。 |
| | disable | 自己免疫機能を無効にします。 |
| | stop | ダイナミック自己免疫機能を停止します。 |

コマンド デフォルト 無効

| コマンド履歴 | リリース | 変更内容 |
|--------|------|-----------------------------------|
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン 潜在的な攻撃者は特別に作成したパケットを使用し、正規のクライアントを攻撃者として処理するように侵入検知システム (IDS) を誘導する場合があります。それによって、コントローラはこの正規のクライアントの接続を解除し、DoS 攻撃が開始されます。自己免疫機能は、有効な場合にこのような攻撃を防ぐように設計されています。ただし、自己免疫機能を有効にすると、Cisco 792x フォンを使用した会話が断続的に中断されることがあります。792x フォンを使用しているときに頻繁に中断されるようであれば、この機能を無効にしてください。

次に、自己免疫モードを設定する例を示します。

```
(Cisco Controller) > config wps auto-immune enable
```

次に、自己免疫モードを停止する例を示します。

```
(Cisco Controller) > config wps auto-immune stop  
Dynamic Auto Immune by WIPS is stopped
```

関連コマンド **show wps summary**

config wps cids-sensor

Wireless Protection System (WPS) の侵入検知システム (IDS) センサーを設定するには、**config wps cids-sensor** コマンドを使用します。

```
config wps cids-sensor { [add index ip_address username password] | [delete index] | [enable
index] | [disable index] | [port index port] | [interval index query_interval] | [fingerprint
sha1 fingerprint] }
```

構文の説明

| | |
|-----------------------|-------------------------------------|
| add | (任意) 新しい IDS センサーを設定します。 |
| <i>index</i> | IDS センサーの内部インデックス。 |
| <i>ip_address</i> | IDS センサーの IP アドレス。 |
| <i>username</i> | IDS センサーのユーザ名。 |
| <i>password</i> | IDS センサーのパスワード。 |
| delete | (任意) IDS センサーを削除します。 |
| enable | (任意) IDS センサーを有効にします。 |
| disable | (任意) IDS センサーを無効にします。 |
| port | (任意) IDS センサーのポート番号を設定します。 |
| <i>port</i> | ポート番号。 |
| interval | (任意) IDS センサーのクエリ間隔を指定します。 |
| <i>query_interval</i> | クエリ間隔の設定。 |
| fingerprint | (任意) IDS センサーの TLS フィンガープリントを指定します。 |
| sha1 | (任意) TLS フィンガープリントを指定します。 |
| <i>fingerprint</i> | TLS フィンガープリント。 |

コマンド デフォルト

コマンドのデフォルトを次に示します。

| | |
|-------------|-----|
| ポート | 443 |
| クエリー インターバル | 60 |

config wps client-exclusion

クライアント除外ポリシーを設定するには、**config wps client-exclusion** コマンドを使用します。

```
config wps client-exclusion {802.11-assoc | 802.11-auth | 802.11x-auth | ip-theft | web-auth
| all} {enable | disable}
```

| 構文の説明 | | |
|-------|---------------------|--|
| | 802.11-assoc | コントローラが 802.11 アソシエーションに連続 5 回失敗すると、6 回目の試行を除外することを指定します。 |
| | 802.11-auth | コントローラが 802.11 認証に連続 5 回失敗すると、6 回目の試行を除外することを指定します。 |
| | 802.1x-auth | コントローラが 802.11X 認証に連続 5 回失敗すると、6 回目の試行を除外することを指定します。 |
| | ip-theft | IP アドレスがすでに別のデバイスに割り当てられている場合は、コントローラがクライアントを除外することを指定します。 |
| | web-auth | コントローラが Web 認証に連続 3 回失敗すると、4 回目の試行を除外することを指定します。 |
| | all | コントローラが上記のすべての理由でクライアントを除外することを指定します。 |
| | enable | クライアント除外ポリシーを有効にします。 |
| | disable | クライアント除外ポリシーを無効にします。 |

コマンド デフォルト すべてのポリシーが有効になります。

| コマンド履歴 | リリース | 変更内容 |
|--------|------|-----------------------------------|
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、802.11 アソシエーションに連続 5 回失敗した場合にクライアントを無効にする例を示します。

```
(Cisco Controller) > config wps client-exclusion 802.11-assoc disable
```

関連コマンド

show wps summary

config wps mfp

管理フレーム保護 (MFP) を設定するには、**config wps mfp** コマンドを使用します。

```
config wps mfp {infrastructure | ap-impersonation} {enable | disable}
```

| | | |
|------------|-------------------------|-----------------------------------|
| 構文の説明 | infrastructure | MFP インフラストラクチャを設定します。 |
| | ap-impersonation | MFP で AP 偽装検出を設定します。 |
| | enable | MFP 機能を有効にします。 |
| | disable | MFP 機能を無効にします。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

次に、インフラストラクチャ MFP を有効にする例を示します。

```
(Cisco Controller) > config wps mfp infrastructure enable
```

関連コマンド

show wps mfp

config wps shun-list re-sync

回避リストのコントローラをモビリティ グループ内の他のコントローラと同期させるには、**config wps shun-list re-sync** コマンドを使用します。

config wps shun-list re-sync

構文の説明

このコマンドには引数またはキーワードはありません。

コマンドデフォルト

なし

コマンド履歴

| リリース | 変更内容 |
|------|---------------------------------|
| 7.6 | このコマンドは、リリース7.6以前のリリースで導入されました。 |

次に、回避リストのコントローラを他のコントローラと同期するように設定する例を示します。

```
(Cisco Controller) > config wps shun-list re-sync
```

関連コマンド

show wps shun-list

config wps signature

侵入検知システム (IDS) シグニチャ処理を有効または無効にする、または、特定の IDS シグニチャを有効または無効にするには、**config wps signature** コマンドを使用します。

config wps signature {standard | custom} state *signature_id* {enable | disable}

| 構文の説明 | standard | 標準の IDS シグニチャを設定します。 |
|-------|---------------------|-------------------------------------|
| | custom | 標準の IDS シグニチャを設定します。 |
| | state | IDS シグニチャの状態を指定します。 |
| | <i>signature_id</i> | 有効または無効にするシグニチャの ID。 |
| | enable | IDS シグニチャ処理または特定の IDS シグニチャを有効にします。 |
| | disable | IDS シグニチャ処理または特定の IDS シグニチャを無効にします。 |

コマンド デフォルト IDS シグニチャ処理は、デフォルトで有効になります。

| コマンド履歴 | リリース | 変更内容 |
|--------|------|-----------------------------------|
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン IDS シグニチャ処理を無効にすると、個々のシグニチャに設定されている状態に関係なく、すべてのシグニチャが無効になります。

次に、すべての IDS シグニチャの処理が有効になるように、IDS シグニチャ処理を有効にする例を示します。

```
(Cisco Controller) >config wps signature enable
```

次に、標準の個別の IDS シグニチャを無効にする例を示します。

```
(Cisco Controller) > config wps signature standard state 15 disable
```

関連コマンド

config wps signature frequency
config wps signature interval
config wps signature mac-frequency
config wps signature quiet-time

config wps signature reset
show wps signature events
show wps signature summary
show wps summary

config wps signature frequency

個々のアクセスポイントレベルで特定されるべき、1間隔あたりの一致パケット数を指定するには、**config wps signature frequency** コマンドを入力します。この値に達すると攻撃が検出されたと判断されます。

config wps signature frequency signature_id frequency

| | | |
|-------|---------------------|--|
| 構文の説明 | <i>signature_id</i> | 設定するシグニチャの ID。 |
| | <i>frequency</i> | 各アクセスポイントレベルで、攻撃と見なされるまでに識別される必要のある間隔あたりの一致パケット数。範囲は間隔あたり 1 ~ 32,000 パケットです。 |

コマンド デフォルト *frequency* デフォルト値は、シグニチャごとに異なります。

| コマンド履歴 | リリース | 変更内容 |
|--------|------|-----------------------------------|
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン IDS シグニチャ処理を無効にすると、個々のシグニチャに設定されている状態に関係なく、すべてのシグニチャが無効になります。

次に、シグニチャ ID 4 に対して、各アクセスポイントで攻撃と見なされる、間隔あたりの一致パケット数を 1800 に設定する例を示します。

```
(Cisco Controller) > config wps signature frequency 4 1800
```

| | |
|--------|--|
| 関連コマンド | config wps signature frequency |
| | config wps signature interval |
| | config wps signature quiet-time |
| | config wps signature reset |
| | show wps signature events |
| | show wps signature summary |
| | show wps summary |

config wps signature interval

シグニチャ頻度が設定された間隔内でしきい値に達するまでの経過時間（秒数）を指定するには、**config wps signature interval** コマンドを入力します。

config wps signature interval *signature_id interval*

| | | |
|-------|---------------------|---|
| 構文の説明 | <i>signature_id</i> | 設定するシグニチャの ID。 |
| | <i>interval</i> | シグニチャの頻度しきい値に達するまでに経過する必要がある秒数。値の範囲は 1～3,600 秒です。 |

コマンドデフォルト *interval* のデフォルト値は、シグニチャごとに異なります。

| コマンド履歴 | リリース | 変更内容 |
|--------|------|-----------------------------------|
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン IDS シグニチャ処理を無効にすると、個々のシグニチャに設定されている状態に関係なく、すべてのシグニチャが無効になります。

次に、シグニチャ ID 1 に対して、シグニチャの頻度しきい値に達するまでに経過する秒数を 200 秒に設定する例を示します。

```
(Cisco Controller) > config wps signature interval 1 200
```

| | |
|--------|--|
| 関連コマンド | config wps signature frequency config wps signature config wps signature mac-frequency config wps signature quiet-time config wps signature reset show wps signature events show wps signature summary show wps summary |
|--------|--|

config wps signature mac-frequency

個々のアクセスポイントでクライアント別に特定されるべき、1 間隔あたりの一致パケット数を指定するには、**config wps signature mac-frequency** コマンドを入力します。この値に達すると攻撃が検出されたと判断されます。

config wps signature mac-frequency signature_id mac_frequency

| | | |
|-------|----------------------|---|
| 構文の説明 | <i>signature_id</i> | 設定するシグニチャの ID。 |
| | <i>mac_frequency</i> | 各クライアントおよびアクセスポイントで、攻撃と見なされる間隔あたりの一致パケット数。範囲は間隔あたり 1 ~ 32,000 パケットです。 |

コマンド デフォルト *mac_frequency* デフォルト値は、シグニチャごとに異なります。

| | | |
|--------|------|-----------------------------------|
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン IDS シグニチャ処理を無効にすると、個々のシグニチャに設定されている状態に関係なく、すべてのシグニチャが無効になります。

次に、シグニチャ ID 3 に対して、各クライアントで攻撃と見なされる、間隔あたりの一致パケット数を 50 に設定する例を示します。

```
(Cisco Controller) > config wps signature mac-frequency 3 50
```

| | |
|--------|--|
| 関連コマンド | config wps signature frequency |
| | config wps signature interval |
| | config wps signature |
| | config wps signature quiet-time |
| | config wps signature reset |
| | show wps signature events |
| | show wps signature summary |
| | show wps summary |

config wps signature quiet-time

各アクセスポイントで攻撃が検出されず、アラームが停止するまでの時間の長さを指定するには、**config wps signature quiet-time** コマンドを使用します。

config wps signature quiet-time *signature_id* *quiet_time*

| | | |
|-------|---------------------|--|
| 構文の説明 | <i>signature_id</i> | 設定するシグニチャの ID。 |
| | <i>quiet_time</i> | 各アクセスポイントレベルで攻撃が検出されず、アラームが停止するまでの時間の長さ。値の範囲は 60 ~ 32,000 秒です。 |

コマンドデフォルト *quiet_time* のデフォルト値は、シグニチャごとに異なります。

| コマンド履歴 | リリース | 変更内容 |
|--------|------|-----------------------------------|
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン IDS シグニチャ処理を無効にすると、個々のシグニチャに設定されている状態に関係なく、すべてのシグニチャが無効になります。

次に、シグニチャ ID 1 に対して、アクセスポイントごとに攻撃が検出されなかったとする経過秒数を 60 秒に設定する例を示します。

```
(Cisco Controller) > config wps signature quiet-time 1 60
```

| 関連コマンド |
|---|
| config wps signature |
| config wps signature frequency |
| config wps signature interval |
| config wps signature mac-frequency |
| config wps signature reset |
| show wps signature events |
| show wps signature summary |
| show wps summary |

config wps signature reset

特定の侵入検知システム (IDS) シグニチャまたはすべての IDS シグニチャをデフォルト値にリセットするには、**config wps signature reset** コマンドを使用します。

config wps signature reset {*signature_id* | **all**}

| | | |
|------------|---------------------|-----------------------------------|
| 構文の説明 | <i>signature_id</i> | リセットする特定の IDS シグニチャの ID。 |
| | all | すべての IDS シグニチャをリセットします。 |
| コマンド デフォルト | なし | |
| コマンド履歴 | リリース | 変更内容 |
| | 7.6 | このコマンドは、リリース 7.6 以前のリリースで導入されました。 |

使用上のガイドライン IDS シグニチャ処理を無効にすると、個々のシグニチャに設定されている状態に関係なく、すべてのシグニチャが無効になります。

次に、IDS シグニチャ 1 をデフォルト値にリセットする例を示します。

```
(Cisco Controller) > config wps signature reset 1
```

関連コマンド

config wps signature
config wps signature frequency
config wps signature interval
config wps signature mac-frequency
config wps signature quiet-time
show wps signature events
show wps signature summary
show wps summary