config コマンド：a ～ i

config aaa auth

管理ユーザに対する AAA 認証の検索順序を設定するには、**config aaa auth** コマンドを使用します。

config aaa auth mgmt [*aaa_server_type1* | *aaa_server_type2*]

構文の説明

mgmt	最大 3 つの AAA 認証サーバ タイプを指定して、コントローラの管理ユーザに対する AAA 認証の検索順序を設定します。サーバ タイプの入力順序により AAA 認証の検索順序が指定されます。
aaa_server_type	（任意）AAA 認証サーバのタイプ（**local**、**radius**、または **tacacs**）。**local** 設定ではローカル データベース、**radius** 設定では RADIUS サーバ、**tacacs** 設定では TACACS+ サーバが指定されます。

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。

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。

使用上のガイドライン

AAA サーバ タイプは、片方が **local** ならば 2 つ入力できます。**radius** と **tacacs** をいっしょに入力することはできません。

次に、local の認証サーバ タイプによってコントローラの管理ユーザに対する AAA 認証の検索順序を設定する例を示します。

```
(Cisco Controller) > config aaa auth radius local
```

関連コマンド

show aaa auth

config aaa auth mgmt

複数データベースが設定されている場合に認証の順序を設定するには、**config aaa auth mgmt** コマンドを使用します。

config aaa auth mgmt［**radius** | **tacacs**］

構文の説明

radius	（任意）RADIUS サーバに認証の順序を設定します。
tacacs	（任意）TACACS サーバに認証の順序を設定します。

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。

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、RADIUS サーバに認証の順序を設定する例を示します。

```
(Cisco Controller) > config aaa auth mgmt radius
```

次に、TACACS サーバに認証の順序を設定する例を示します。

```
(Cisco Controller) > config aaa auth mgmt tacacs
```

関連コマンド

show aaa auth order

config acl apply

アクセス コントロール リスト（ACL）をデータ パスに適用するには、**config acl apply** コマンドを使用します。

config acl apply *rule_name*

構文の説明

rule_name	最大 32 文字の英数字による ACL 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

Cisco 2100 シリーズ ワイヤレス LAN コントローラの場合、外部 Web サーバに対して無線 LAN で事前認証 ACL を設定する必要があります。この ACL は、Web ポリシーで無線 LAN 事前認証 ACL として設定する必要があります。ただし、Cisco 4400 シリーズ ワイヤレス LAN コントローラの場合は事前認証 ACL を設定する必要はありません。

次に、ACL をデータ パスに適用する例を示します。

```
(Cisco Controller) > config acl apply acl01
```

関連コマンド

show acl

config acl counter

パケットが、コントローラ上に設定されたアクセス コントロール リスト（ACL）のいずれかをヒットしたかどうかを確認するには、**config acl counter** コマンドを使用します。

config acl counter {**start** | **stop**}

構文の説明

start	コントローラで ACL カウンタを有効にします。
stop	コントローラで ACL カウンタを無効にします。

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
7.6	このコマンドは、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

ACL カウンタを使用できるコントローラは、4400 シリーズ、Cisco WiSM、Catalyst 3750G Integrated Wireless LAN Controller Switch だけです。

次に、コントローラで ACL カウンタを有効にする例を示します。

```
(Cisco Controller) > config acl counter start
```

関連コマンド

clear acl counters

show acl detailed

config acl create

新しいアクセス コントロール リスト（ACL）を作成するには、**config acl create** コマンドを使用します。

config acl create *rule_name*

構文の説明

rule_name	最大 32 文字の英数字による ACL 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

Cisco 2100 シリーズ ワイヤレス LAN コントローラの場合、外部 Web サーバに対して無線 LAN で事前認証 ACL を設定する必要があります。この ACL は、Web ポリシーで無線 LAN 事前認証 ACL として設定する必要があります。ただし、Cisco 4400 シリーズ ワイヤレス LAN コントローラの場合は事前認証 ACL を設定する必要はありません。

次に、新しい ACL を作成する例を示します。

```
(Cisco Controller) > config acl create acl01
```

関連コマンド

show acl

config acl cpu

CPU に到達するトラフィックを制限する新しいアクセス コントロール リスト（ACL）を作成するには、**config acl cpu** コマンドを使用します。

config acl cpu *rule_name* {**wired** | **wireless** | **both**}

構文の説明

rule_name	ACL 名を指定します。
wired	有線トラフィックで ACL を指定します。
wireless	無線トラフィックで ACL を指定します。
both	有線と無線両方のトラフィックで ACL 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

このコマンドにより、CPU に到達するパケットのタイプを制御できます。

次に、CPU で acl101 という ACL を作成し、有線トラフィックに適用する例を示します。

```
(Cisco Controller) > config acl cpu acl01 wired
```

関連コマンド

show acl cpu

config acl delete

アクセス コントロール リスト（ACL）を削除するには、**config acl delete** コマンドを使用します。

config acl delete *rule_name*

構文の説明

rule_name	最大 32 文字の英数字による ACL 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

Cisco 2100 シリーズ ワイヤレス LAN コントローラの場合、外部 Web サーバに対して無線 LAN で事前認証 ACL を設定する必要があります。この ACL は、Web ポリシーで無線 LAN 事前認証 ACL として設定する必要があります。ただし、Cisco 4400 シリーズ ワイヤレス LAN コントローラの場合は事前認証 ACL を設定する必要はありません。

次に、CPU で acl101 という ACL を削除する例を示します。

```
(Cisco Controller) > config acl delete acl01
```

関連コマンド

show acl

config acl layer2

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 acl layer2** コマンドを使用します。

config acl layer2 {**apply** *acl_name* | **create** *acl_name* | **delete** *acl_name* | **rule** {**action** *acl_name index* {**permit** | **deny**} | **add** *acl_name index* | **change index** *acl_name old_index new_index* | **delete** *acl_name index* | **etherType** *acl_name index etherType etherTypeMask* | **swap index** *acl_name index1 index2*}}

構文の説明

apply	レイヤ 2 ACL をデータ パスに適用します。
acl_name	レイヤ 2 ACL の名前。名前には 32 文字以内の英数字を使用できます。
create	レイヤ 2 ACL を作成します。
delete	レイヤ 2 ACL を削除します。
rule	レイヤ 2 ACL ルールを設定します。
action	レイヤ 2 ACL ルールのアクションを設定します。
index	レイヤ 2 ACL ルールのインデックス。
permit	ルールのアクションを許可します。
deny	ルールのアクションを拒否します。
add	レイヤ 2 ACL ルールを作成します。
change index	レイヤ 2 ACL ルールのインデックスを変更します。
old_index	レイヤ 2 ACL ルールの古いインデックス。
new_index	レイヤ 2 ACL ルールの新しいインデックス。
delete	レイヤ 2 ACL ルールを削除します。
etherType	レイヤ 2 ACLルールの EtherType を設定します。
etherType	レイヤ 2 ACLルールの EtherType。EtherType は、イーサネット フレームのペイロードにカプセル化されるプロトコルを示すために使用されます。範囲は 16 進値の 0x0 ～ 0xffff です。

etherTypeMask	EtherType のネットマスク。範囲は 16 進値の 0x0 ～ 0xffff です。
swap index	2 つのルールのインデックス値を交換します。
index1 index2	2 つのレイヤ 2 ACL ルールのインデックス値。

コマンド デフォルト

Cisco WLC はレイヤ 2 ACL を持っていません。

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。

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

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、レイヤ 2 ACL を適用する例を示します。

```
(Cisco Controller) >config acl layer2 apply acl_l2_1
```

config acl rule

ACL ルールを設定するには、**config acl rule** コマンドを使用します。

config acl rule {**action** *rule_name rule_index* {**permit** | **deny**} | **add** *rule_name rule_index* | **change index** *rule_name old_index new_index* | **delete** *rule_name rule_index* | **destination address** *rule_name rule_index ip_address netmask* | **destination port range** *rule_name rule_index start_port end_port* | **direction** *rule_name rule_index* {**in** | **out** | **any**} | **dscp** *rule_name rule_index dscp* | **protocol** *rule_name rule_index protocol* | **source address** *rule_name rule_index ip_address netmask* | **source port range** *rule_name rule_index start_port end_port* | **swap index** *rule_name index_1 index_2*}

構文の説明

action	アクセスを許可するか拒否するかを設定します。
rule_name	最大 32 文字の英数字による ACL 名。
rule_index	1 ～ 32 のルールのインデックス。
permit	ルールのアクションを許可します。
deny	ルールのアクションを拒否します。
add	新規ルールを追加します。
change	ルールのインデックスを変更します。
index	ルールのインデックスを指定します。
delete	ルールを削除します。
destination address	ルールの宛先 IP アドレスとネットマスクを設定します。
destination port range	ルールの宛先ポート範囲を設定します。
ip_address	ルールの IP アドレス。
netmask	ルールのネットマスク。
start_port	開始ポート番号（0 ～ 65535）。
end_port	終了ポート番号（0 ～ 65535）。
direction	ルールの方向（in、out、または any）を設定します。
in	ルールの方向を in に設定します。
out	ルールの方向を out に設定します。

any	ルールの方向を any に設定します。
dscp	ルールの DSCP を設定します。
dscp	0 ～ 63 の数値または **any**。
protocol	ルールの DSCP を設定します。
protocol	0 ～ 255 の数値または **any**。
source address	ルールの送信元 IP アドレスとネットマスクを設定します。
source port range	ルールの送信元ポート範囲を設定します。
swap	ルールの2つのインデックスを入れ替えます。

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

Cisco 2100 シリーズ ワイヤレス LAN コントローラの場合、外部 Web サーバに対して無線 LAN で事前認証 ACL を設定する必要があります。この ACL は、Web Policy で無線 LAN 事前認証 ACL として設定する必要があります。ただし、Cisco 4400 シリーズ ワイヤレス LAN コントローラの場合は事前認証 ACL を設定する必要はありません。

次に、アクセスを許可するよう ACL を設定する例を示します。

```
(Cisco Controller) > config acl rule action lab1 4 permit
```

関連コマンド

show acl

config acl url-acl

URL アクセス コントロール リストを設定するには、**config acl url-acl** コマンドを使用します。

config acl url-acl [**apply** | **create** | **delete** | **disable** | **enable** | **rule**]
config acl url-aclapply *acl-name*
config acl url-acl create *acl-name*
config acl url-acl delete *acl-name*
config acl url-acldisable
config acl url-aclenable
config acl url-aclrule [**action** | **add** | **delete** | **url**]
config acl url-aclrule action *acl-name index* {**permit** | **deny**}
config acl url-aclrule add *acl-name index*
config acl url-aclrule delete *acl-name index*
config acl url-aclrule url *acl-name index url-name*

構文の説明

apply *acl-name*	ACL 名（最大 32 文字の英数字）を入力します。
create	新しい URL ACL を作成します。
delete	URL ACL を削除します。
disable	URL ACL 機能を無効にします。
enable	URL ACL 機能を有効にします。
rule（**action**）（*acl-name*）（*index*）	URL ACL のルールによる処理（アクセスの許可または拒否）を設定します。URL ACL 名には最大 32 文字の英数字を使用でき、URL ACL ルール インデックスには 1 ー 100 を指定できます。
{**permit** | **deny**}	URL ルールを許可または拒否します。
add *acl-name index*	新しいルールおよびルール インデックスを追加します。
delete *acl-name index*	ルールおよびルール インデックスを削除します。
url *acl-name index url-name*	ルールの URL アドレスを設定します。URL アドレスを入力し、インデックス（1～100）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
8.3	このコマンドが導入されました。

次に、新しい URL ACL を作成する例を示します。

```
(Cisco Controller) >config acl url-acl create test
```

config acl url-acl external-server-ip

要求された URL がブロックされたときに表示するページにユーザをリダイレクトします。外部サーバの IP アドレスを設定するには、**config acl url-acl external-server-ip** コマンドを使用します。

config acl url-acl external-server-ip *ip-address*

構文の説明

external-server-ip	ACL 名を指定します。
ip-address	外部サーバの 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
8.4	このコマンドが導入されました。

次に、URL がブロックされたときにリダイレクトしてページを表示するために、外部サーバの IP アドレスを設定する例を示します。

```
(Cisco Controller) > config acl url-acl external-server-ip 192.0.2.1
```

config acl url-acl list-type

特定のACLのルールに関してトラフィックを許可または拒否するには、**config acl url-acl list-type** コマンドを使用します。

config acl url-acl list-type *acl_name*{**blacklist|||whitelist**}

構文の説明

list-type	URL ACL のリスト タイプを設定します。
blacklist	すべてのルールのアクションが「拒否」になります。
whitelist	すべてのルールのアクションが「許可」になります。

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、ACL に関してトラフィックを許可する例を示します。

```
(Cisco Controller) > config acl url-acl list-type testacl whitelist
```

config acl url-domain

アクセス コントロール リストの URL ドメインを追加または削除するには、**config acl url-domain** コマンドを使用します。

config acl url-domain {**add**|**delete**} *domain_name acl_name*

構文の説明

domain_name	アクセス コントロール リストの URL ドメイン名。
acl_name	アクセス コントロール リストの名前。

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	このコマンドが導入されました。

次に、アクセス コントロール リストの新しい URL ドメインを追加する例を示します。

```
(Cisco Controller) > config acl url-domain add cisco.com android
```

次に、アクセス コントロール リストから既存の URL ドメインを削除する例を示します。

```
(Cisco Controller) > config acl url-domain delete play.google.com android
```

config advanced 802.11 7920VSIEConfig

Cisco Unified Wireless IP Phone 7920 VISE パラメータを設定するには、**config advanced 802.11 7920VSIEConfig** コマンドを使用します。

config advanced 802.11 {**a** | **b**} **7920VSIEConfig** {**call-admission-limit** *limit* | **G711-CU-Quantum** *quantum*}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
call-admission-limit	7920s のコール アドミッション制限を設定します。
G711-CU-Quantum	単一の G.711-20ms コールで使用されるチャネル使用率の単位の現在の数を示すインフラストラクチャによって提供される値を設定します。
limit	コール アドミッション制限（0 ～ 255）。デフォルト値は 105 です。
quantum	G711 量子値。デフォルト値は 15 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。

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、7920 VISE パラメータのコール アドミッション制限を設定する例を示します。

```
(Cisco Controller) >config advanced 802.11 7920VSIEConfig call-admission-limit 4
```

config advanced 802.11 channel add

802.11 ネットワーク自動 RF チャネルのリストにチャネルを追加するには、**config advanced 802.11 channel add** コマンドを使用します。

config advanced 802.11 {**a** | **b**} **channel add** *channel_number*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
add	802.11 ネットワーク自動 RF チャネルのリストにチャネルを追加します。
channel_number	802.11 ネットワーク自動 RF チャネルのリストに追加するチャネル番号。

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。

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、802.11a ネットワーク自動 RF チャネルのリストにチャネルを追加する例を示します。

```
(Cisco Controller) >config advanced 802.11 channel add 132
```

config advanced 802.11 channel cleanair-event

すべての 802.11 Cisco Lightweight アクセス ポイントの CleanAir イベント駆動型無線リソース管理（RRM）パラメータを設定するには、**config advanced 802.11 channel cleanair-event** コマンドを使用します。

config advanced 802.11｛**a** ｜ **b**｝ **channel cleanair-event**｛**enable** ｜ **disable** ｜ **sensitivity**［**low** ｜ **medium** ｜ **high**］ ｜ **custom threshold** *threshold_value*｝

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
enable	CleanAirイベント駆動型RRMパラメータを有効にします。
disable	CleanAirイベント駆動型RRMパラメータを無効にします。
sensitivity	CleanAirイベント駆動型RRMの感度を設定します。
low	（任意）低感度を指定します。
medium	（任意）中感度を指定します。
high	（任意）高感度を指定します。
custom	カスタム感度を指定します。
threshold	EDRRM AQ しきい値を指定します。
threshold_value	カスタムしきい値の数。

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、CleanAir イベント駆動 RRM パラメータを有効にする例を示します。

```
(Cisco Controller) > config advanced 802.11 channel cleanair-event enable
```

次に、CleanAir イベント駆動型 RRM に高感度を設定する例を示します。

```
(Cisco Controller) > config advanced 802.11 channel cleanair-event sensitivity high
```

config advanced 802.11 channel dca anchor-time

チャネルの動的割り当て（DCA）アルゴリズムの開始時刻を指定するには、 **config advanced 802.11 channel dca anchor-time** コマンドを使用します。

config advanced 802.11 {**a** | **b**} **channel dca anchor-time** *value*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
value	0 ～ 23 の時刻。この値は、午前 12 時から午後 11 時までの時間を表します。

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。

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、DCA アルゴリズムが開始したときに遅延時間を設定する例を示します。

```
(Cisco Controller) > config advanced 802.11 channel dca anchor-time 17
```

関連コマンド

config advanced 802.11 channel dca interval

config advanced 802.11 channel dca sensitivity

config advanced 802.11 channel

config advanced 802.11 channel dca chan-width-11n

5 GHz 帯域のすべての 802.11n 無線に、チャネルの動的割り当て（DCA）チャネル幅を設定するには、**config advanced 802.11 channel dca chan-width-11n** コマンドを使用します。

config advanced 802.11{**a** | **b**} **channel dca chan-width-11n** {**20** | **40** | **80**}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
20	802.11n 無線のチャネル幅を 20 MHz に設定します。
40	802.11n 無線のチャネル幅を 40 MHz に設定します。
80	802.11ac 無線のチャネル幅を 80 MHz に設定します。

コマンド デフォルト

デフォルトのチャネル幅は 20 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。

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。

使用上のガイドライン

40 を選択する場合は、 **config advanced 802.11 channel** {**add** | **delete**} *channel_number* コマンドで少なくとも 2 つの隣接チャネルを設定する必要があります（プライマリ チャネルの 36 と拡張チャネルの 40 など）。1 つのチャネルしか設定しないと、そのチャネルは 40 MHz チャネル幅として使用されません。

グローバルに設定されている DCA チャネル幅設定を上書きするには、**config 802.11 chan_width** コマンドを使用して、特定のアクセス ポイントの無線を 20 または 40 MHz モードに静的に設定します。後でこのアクセスポイントの無線に対する静的な設定をグローバルに変更すると、それまでアクセス ポイントで使用されていたチャネル幅設定はグローバルな DCA 設定で上書きされます。

次に、802.11a ネットワーク自動チャネルのリストにチャネルを追加する例を示します。

```
(Cisco Controller) >config advanced 802.11a channel dca chan-width-11n 40
```

次に、802.11ac 無線のチャネル幅を 80 MHz に設定する例を示します。

```
(Cisco Controller) >config advanced 802.11a channel dca chan-width-11n 80
```

config advanced 802.11 channel dca interval

チャネルの動的割り当て（DCA）が実行される頻度を指定するには、 **config advanced 802.11 channel dca interval** コマンドを使用します。

config advanced 802.11 {**a** | **b**} **channel dca interval** *value*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
value	有効な値は0、1、2、3、4、6、8、12、または24時間です。0の場合は10分になります（600秒）。

コマンド デフォルト

DCA チャネルのデフォルトの間隔は 10（10 分）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。

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。

使用上のガイドライン

コントローラがOfficeExtendアクセスポイントしかサポートしていない場合は、最適なパフォーマンスを得るために、DCA 間隔を 6 時間に設定することをお勧めします。OfficeExtend アクセス ポイントとローカル アクセス ポイントを組み合わせて展開している場合は、10 分から 24 時間までの範囲を使用できます。

次に、DCA アルゴリズムが実行される頻度の例を示します。

```
(Cisco Controller) > config advanced 802.11 channel dca interval 8
```

関連コマンド

config advanced 802.11 dca anchor-time

config advanced 802.11 dca sensitivity

show advanced 802.11 channel

config advanced 802.11 channel dca min-metric

DCA の 5 GHz 最小 RSSI エネルギー メトリックを設定するには、**config advanced 802.11 channel dca min-metric** コマンドを使用します。

config advanced 802.11 {**a** | **b**} **channel dca** *RSSI_value*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
RSSI_value	DCA がチャネルの変更をトリガーするために必要な最小の受信信号強度インジケータ（RSSI）。範囲は、-100 ～ -60 dBm です。

コマンド デフォルト

DCA のデフォルトの最小 RSSI エネルギー メトリックは、–95 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。

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、DCA の 5 GHz 最小 RSSI エネルギー メトリックを設定する例を示します。

```
(Cisco Controller) > config advanced 802.11a channel dca min-metric –80
```

上記の例では、DCA がチャネルの変更をトリガーするために、RSSI で少なくとも -80 dBm の干渉エネルギーを RRM が検出する必要があります。

関連コマンド

config advanced 802.11 dca interval

config advanced 802.11 dca anchor-time

show advanced 802.11 channel

config advanced 802.11 channel dca sensitivity

チャネル変更の判定時の環境の変化（信号、負荷、ノイズ、干渉など）に対するチャネルの動的割り当て（DCA）アルゴリズムの感度を指定するには、**config advanced 802.11 channel dca sensitivity** コマンドを使用します。

config advanced 802.11 {**a** | **b**} **channel dcasensitivity** {**low** | **medium** | **high**}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
low	環境の変化に対する DCA アルゴリズムの感度は特に高くないことを指定します。詳細については、「使用上のガイドライン」を参照してください。
medium	環境の変化に対する DCA アルゴリズムの感度は中程度であることを指定します。詳細については、「使用上のガイドライン」を参照してください。
high	環境の変化に対する DCA アルゴリズムの感度が高いことを指定します。詳細については、「使用上のガイドライン」を参照してください。

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。

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。

使用上のガイドライン

DCA の感度のしきい値は、次の表で示すように、無線帯域によって異なります。

トラブルシューティングに役立つように、このコマンドの出力には失敗したコールすべてのエラー コードが示されます。次の表では、失敗したコールの考えられるエラー コードについて説明します。

表 *1 : DCA* の感度のしきい値

感度	2.4 GHz DCA 感度しきい値	5 GHz DCA 感度しきい値
High	5 dB	5 dB
Medium	15 dB	20 dB
Low	30 dB	35 dB

次に、DCA アルゴリズムの感度の値を low に設定する例を示します。

```
(Cisco Controller) > config advanced 802.11 channel dca sensitivity low
```

関連コマンド

config advanced 802.11 dca interval

config advanced 802.11 dca anchor-time

show advanced 802.11 channel

config advanced 802.11 channel foreign

802.11a対応のすべてのCisco Lightweightアクセス ポイントについて、無線リソース管理（RRM）によるチャネル選択時に外部 802.11a 干渉回避を考慮するか、無視するかを指定するには、**config advanced 802.11 channel foreign** コマンドを使用します。

config advanced 802.11｛**a** ｜ **b**｝ **channel foreign** ｛**enable** ｜ **disable**｝

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
enable	チャネル割り当てで、外部アクセス ポイント 802.11a 干渉回避を有効にします。
disable	チャネル割り当てで、外部アクセス ポイント 802.11a 干渉回避を無効にします。

コマンド デフォルト

チャネル割り当てでの外部アクセス ポイント 802.11a 干渉回避は、デフォルトでは有効になっています。

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。

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、802.11a 対応のすべての Cisco Lightweight アクセス ポイントについて、RRM によるチャネル選択時に外部 802.11a 干渉が考慮されるようにする例を示します。

```
(Cisco Controller) > config advanced 802.11a channel foreign enable
```

関連コマンド

show advanced 802.11a channel

config advanced 802.11b channel foreign

config advanced 802.11 channel load

802.11a 対応のすべての Cisco Lightweight アクセス ポイントについて、無線リソース管理（RRM）によるチャネル選択更新時にトラフィックの負荷を考慮するか、無視するかを指定するには、**config advanced 802.11 channel load** コマンドを使用します。

config advanced 802.11 {**a** | **b**} **channel load** {**enable** | **disable**}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
enable	チャネル割り当てで、Cisco Lightweight アクセス ポイント 802.11a 負荷回避を有効にします。
disable	チャネル割り当てで、Cisco Lightweight アクセス ポイント 802.11a 負荷回避を無効にします。

コマンド デフォルト

チャネル割り当てでの Cisco Lightweight アクセス ポイント 802.11a 負荷回避は、デフォルトでは無効になっています。

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。

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、802.11a 対応のすべての Cisco Lightweight アクセス ポイントについて、RRM によるチャネル選択時にトラフィックの負荷が考慮されるようにする例を示します。

```
(Cisco Controller) > config advanced 802.11 channel load enable
```

関連コマンド

show advanced 802.11a channel

config advanced 802.11b channel load

config advanced 802.11 channel noise

802.11a対応のすべてのCisco Lightweightアクセス ポイントについて、無線リソース管理（RRM）によるチャネル選択更新時に802.11a以外のノイズを考慮するか、無視するかを指定するには、**config advanced 802.11 channel noise** コマンドを使用します。

config advanced 802.11 {**a** | **b**} **channel noise** {**enable** | **disable**}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
enable	チャネル割り当てで802.11a以外のノイズ回避を有効にするか、無視します。
disable	チャネル割り当てで802.11a以外のノイズ回避を無効にします。

コマンド デフォルト

チャネル割り当てで 802.11a 以外のノイズ回避は、デフォルトでは無効になっています。

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。

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、802.11a 対応のすべての Cisco Lightweight アクセス ポイントについて、RRM によるチャネル選択時に 802.11a 以外のノイズが考慮されるようにする例を示します。

```
(Cisco Controller) > config advanced 802.11 channel noise enable
```

関連コマンド

show advanced 802.11a channel

config advanced 802.11b channel noise

config advanced 802.11 channel outdoor-ap-dca

非動的周波数選択（DFS）チャネルのチェックのコントローラによる回避を有効または無効にするには、**config advanced 802.11 channel outdoor-ap-dca** コマンドを使用します。

config advanced 802.11 {**a** | **b**} **channel outdoor-ap-dca** {**enable** | **disable**}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
enable	屋外アクセス ポイントの 802.11 ネットワーク DCA のリストのオプションを有効にします。
disable	屋外アクセス ポイントの 802.11 ネットワーク DCA のリストのオプションを無効にします。

コマンド デフォルト

屋外アクセス ポイントの 802.11 ネットワーク DCA のリストのオプションは、デフォルトでは無効になっています。

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。

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。

使用上のガイドライン

config advanced 802.11 {**a** | **b**} **channel outdoor-ap-dca** {**enable** | **disable**} コマンドは、1522 や 1524 などの屋外アクセス ポイントを持つ展開にのみ適用されます。

次に、屋外アクセス ポイントで 802.11a DCA のリスト オプションを有効にする例を示します。

```
(Cisco Controller) > config advanced 802.11a channel outdoor-ap-dca enable
```

関連コマンド

show advanced 802.11a channel

config advanced 802.11b channel noise

config advanced 802.11 channel pda-prop

永続デバイスの伝播を有効または無効にするには、**config advanced 802.11 channel pda-prop** コマンドを使用します。

config advanced 802.11{**a** | **b**} **channel pda-prop** {**enable** | **disable**}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
enable	屋外アクセス ポイントの 802.11 ネットワーク DCA のリストのオプションを有効にします。
disable	屋外アクセス ポイントの 802.11 ネットワーク DCA のリストのオプションを無効にします。

コマンド デフォルト

屋外アクセス ポイントの 802.11 ネットワーク DCA のリストのオプションは、デフォルトでは無効になっています。

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。

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、永続デバイスの伝播を有効または無効にする例を示します。

```
(Cisco Controller) > config advanced 802.11 channel pda-prop enable
```

config advanced 802.11 channel update

802.11a 対応のすべての Cisco Lightweight アクセス ポイントを対象に、無線リソース管理（RRM）によるチャネル選択更新が開始されるようにするには、**config advanced 802.11 channel update** コマンドを使用します。

config advanced 802.11 {**a** | **b**} **channel update**

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。

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。

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、すべての 802.11a ネットワーク アクセス ポイントのチャネル選択の更新を開始する例を示します。

```
(Cisco Controller) > config advanced 802.11a channel update
```

config advanced 802.11 coverage

カバレッジ ホール検出を有効または無効にするには、**config advanced 802.11 coverage** コマンドを使用します。

config advanced 802.11{**a** | **b**} **coverage** {**enable** | **disable**}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
enable	カバレッジ ホールの検出を有効にします。
disable	カバレッジ ホールの検出を無効にします。

コマンド デフォルト

カバレッジ ホール検出は、デフォルトでは無効になっています。

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。

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。

使用上のガイドライン

カバレッジホール検出を有効にすると、カバレッジが不完全な領域に位置する可能性のあるクライアントを持つアクセス ポイントがあるかどうかを、アクセス ポイントから受信したデータに基づいて Cisco WLC が自動的に判断します。

5 秒間で失敗したパケットの数と割合の両方が、**config advanced 802.11 coverage packet-count** コマンドおよび **config advanced 802.11 coverage fail-rate** コマンドで入力した値を超えると、そのクライアントは事前アラーム状態と判断されます。コントローラは、この情報を使用してカバレッジホールの真偽を判断し、ローミング ロジックが不完全なクライアントを除外します。90 秒間で失敗したクライアントの数と割合の両方が、**config advanced 802.11 coverage level global**コマンドおよび **config advanced 802.11 coverage exception global** コマンドで入力した値を満たすか超えると、カバレッジ ホールが検出されます。Cisco WLC は、カバレッジ ホールを修正可能か判断し、適切ならば、その特定のアクセス ポイントの伝送パワー レベルを上げてカバレッジ ホールを解消します。

次に、802.11a ネットワーク上でカバレッジホールの検出を有効にする例を示します。

```
(Cisco Controller) > config advanced 802.11a coverage enable
```

関連コマンド

config advanced 802.11 coverage exception global

config advanced 802.11 coverage fail-rate

config advanced 802.11 coverage level global

config advanced 802.11 coverage packet-count

config advanced 802.11 coverage rssi-threshold

config advanced 802.11 coverage exception global

アクセス ポイント上で、信号レベルが低くなっているにもかかわらず、別のアクセス ポイントにローミングできないクライアントの割合を指定するには、**config advanced 802.11 coverage exception global** コマンドを使用します。

config advanced 802.11 {**a** | **b**} **coverage exception global** *percent*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
percent	クライアントの割合。有効な値は 0 ～ 100 % です。

コマンド デフォルト

アクセス ポイントでのクライアントの割合は、デフォルトでは 25 % 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。

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。

使用上のガイドライン

5 秒間で失敗したパケットの数と割合の両方が、**config advanced 802.11 coverage packet-count** コマンドおよび **config advanced 802.11 coverage fail-rate** コマンドで入力した値を超えると、そのクライアントは事前アラーム状態と判断されます。コントローラは、この情報を使用してカバレッジホールの真偽を判断し、ローミング ロジックが不完全なクライアントを除外します。90 秒間で失敗したクライアントの数と割合の両方が、**config advanced 802.11 coverage level global** コマンドおよび **config advanced 802.11 coverage exception global** コマンドで入力した値を満たすか超えると、カバレッジ ホールが検出されます。コントローラは、カバレッジ ホールを修正可能か判断し、適切ならば、その特定のアクセス ポイントの伝送パワー レベルを上げてカバレッジ ホールを解消します。

次に、信号レベルが低くなっているすべての 802.11a アクセス ポイントにクライアントの割合を指定する例を示します。

```
(Cisco Controller) > config advanced 802.11 coverage exception global 50
```

関連コマンド

config advanced 802.11 coverage exception global

config advanced 802.11 coverage fail-rate

config advanced 802.11 coverage level global

config advanced 802.11 coverage packet-count

config advanced 802.11 coverage rssi-threshold

config advanced 802.11 coverage

config advanced 802.11 coverage fail-rate

アップリンクのデータ パケットまたは音声パケットの失敗率のしきい値を指定するには、**config advanced 802.11 coverage fail-rate** コマンドを使用します。

config advanced 802.11{**a** | **b**} **coverage** {**data** | **voice**} **fail-rate** *percent*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
data	データ パケットのしきい値を指定します。
voice	音声パケットのしきい値を指定します。
percent	失敗率のパーセント。有効な値は 1 ～ 100 % です。

コマンド デフォルト

アップリンク カバレッジ失敗率値のデフォルトの失敗率しきい値は、20 % 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

5 秒間で失敗したパケットの数と割合の両方が、**config advanced 802.11 coverage packet-count** コマンドおよび **config advanced 802.11 coverage fail-rate** コマンドで入力した値を超えると、そのクライアントは事前アラーム状態と判断されます。コントローラは、この情報を使用してカバレッジホールの真偽を判断し、ローミング ロジックが不完全なクライアントを除外します。90 秒間で失敗したクライアントの数と割合の両方が、**config advanced 802.11 coverage level global**コマンドおよび **config advanced 802.11 coverage exception global** コマンドで入力した値を満たすか超えると、カバレッジ ホールが検出されます。コントローラは、カバレッジ ホールを修正可能か判断し、適切ならば、その特定のアクセス ポイントの伝送パワー レベルを上げてカバレッジ ホールを解消します。

次に、データ パケットの最小アップリンク失敗率のしきい値を設定する例を示します。

```
(Cisco Controller) > config advanced 802.11 coverage fail-rate 80
```

関連コマンド

config advanced 802.11 coverage exception global

config advanced 802.11 coverage level global

config advanced 802.11 coverage packet-count

config advanced 802.11 coverage rssi-threshold

config advanced 802.11 coverage

config advanced 802.11 coverage level global

アクセス ポイント上でデータまたは音声受信信号強度インジケータ（RSSI）しきい値以下の RSSI 値を持つクライアントの最小数を指定するには、**config advanced 802.11 coverage level global** コマンドを使用します。

config advanced 802.11 {**a** | **b**} **coverage level global** *clients*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
clients	クライアントの最小数。有効な値は 1 ～ 75 です。

コマンド デフォルト

アクセス ポイント上のクライアントのデフォルトの最小数は 3 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。

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。

使用上のガイドライン

5 秒間で失敗したパケットの数と割合の両方が、**config advanced 802.11 coverage packet-count** コマンドおよび **config advanced 802.11 coverage fail-rate** コマンドで入力した値を超えると、そのクライアントは事前アラーム状態と判断されます。コントローラは、この情報を使用してカバレッジホールの真偽を判断し、ローミング ロジックが不完全なクライアントを除外します。90 秒間で失敗したクライアントの数と割合の両方が、**config advanced 802.11 coverage level global** コマンドおよび **config advanced 802.11 coverage exception global** コマンドで入力した値を満たすか超えると、カバレッジ ホールが検出されます。コントローラは、カバレッジ ホールを修正可能か判断し、適切ならば、その特定のアクセス ポイントの伝送パワー レベルを上げてカバレッジ ホールを解消します。

次に、RSSI しきい値以下の RSSI 値をすべての 802.11a アクセス ポイントでクライアントの最小数を指定する例を示します。

```
(Cisco Controller) > config advanced 802.11 coverage level global 60
```

関連コマンド

config advanced 802.11 coverage exception global

config advanced 802.11 coverage fail-rate

config advanced 802.11 coverage packet-count

config advanced 802.11 coverage rssi-threshold

config advanced 802.11 coverage

config advanced 802.11 coverage packet-count

アップリンクのデータ パケットまたは音声パケットの最小失敗数のしきい値を指定するには、**config advanced 802.11 coverage packet-count** コマンドを使用します。

config advanced 802.11{**a** | **b**} **coverage** {**data** | **voice**} **packet-count** *packets*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
data	データ パケットのしきい値を指定します。
voice	音声パケットのしきい値を指定します。
packets	パケットの最小数。有効な値は 1 ～ 255 パケットです。

コマンド デフォルト

アップリンク データまたは音声パケットのデフォルトの失敗カウントしきい値は 10 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。

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。

使用上のガイドライン

5 秒間で失敗したパケットの数と割合の両方が、**config advanced 802.11 coverage packet-count** コマンドおよび **config advanced 802.11 coverage fail-rate** コマンドで入力した値を超えると、そのクライアントは事前アラーム状態と判断されます。コントローラは、この情報を使用してカバレッジホールの真偽を判断し、ローミング ロジックが不完全なクライアントを除外します。90 秒間で失敗したクライアントの数と割合の両方が、**config advanced 802.11 coverage level global**コマンドおよび **config advanced 802.11 coverage exception global** コマンドで入力した値を満たすか超えると、カバレッジ ホールが検出されます。コントローラは、カバレッジ ホールを修正可能か判断し、適切ならば、その特定のアクセス ポイントの伝送パワー レベルを上げてカバレッジ ホールを解消します。

次に、アップリンク データ パケットに対して失敗数のしきい値を設定する例を示します。

```
(Cisco Controller) > config advanced 802.11 coverage packet-count 100
```

関連コマンド

config advanced 802.11 coverage exception global

config advanced 802.11 coverage fail-rate

config advanced 802.11 coverage level global

config advanced 802.11 coverage rssi-threshold

config advanced 802.11 coverage

config advanced 802.11 coverage rssi-threshold

アクセス ポイントで受信されるパケットの最小の受信信号強度インジケータ（RSSI）値を指定するには、**config advanced 802.11 coverage rssi-threshold** コマンドを使用します。

config advanced 802.11{**a** | **b**} **coverage** {**data** | **voice**} **rssi-threshold** *rssi*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
data	データ パケットのしきい値を指定します。
voice	音声パケットのしきい値を指定します。
rssi	有効な値は –60 ～ –90 dBm です。

コマンド デフォルト

- データ パケットのデフォルトの RSSI 値は -80 dBm です。
- 音声パケットのデフォルトの RSSI 値は -75 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。

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。

使用上のガイドライン

入力した *rssi* 値は、ネットワーク内のカバレッジホール（カバレッジが不完全な領域）を特定するために使用されます。入力した値よりも小さい RSSI 値を持つパケットが、アクセス ポイントのデータ キューまたは音声キューで受信されると、カバレッジ ホールの可能性が検出されます。

アクセス ポイントでは、5 秒ごとに RSSI が測定され、90 秒間隔でそれらがコントローラに報告されます。

5 秒間で失敗したパケットの数と割合の両方が、**config advanced 802.11 coverage packet-count** コマンドおよび **config advanced 802.11 coverage fail-rate** コマンドで入力した値を超えると、そのクライアントは事前アラーム状態と判断されます。コントローラは、この情報を使用してカバレッジホールの真偽を判断し、ローミング ロジックが不完全なクライアントを除外します。90 秒間で失敗したクライアントの数と割合の両方が、**config advanced 802.11 coverage level global** コマンドおよび **config advanced 802.11 coverage exception global** コマンドで入力した値を満たすか超えると、カバレッジ ホールが検出されます。コントローラは、カバレッジ ホール

を修正可能か判断し、適切ならば、その特定のアクセス ポイントの伝送パワー レベルを上げてカバレッジ ホールを解消します。

次に、802.11a アクセス ポイントが受信したデータ パケットに対して最小の受信信号強度インジケータを設定する例を示します。

```
(Cisco Controller) > config advanced 802.11a coverage rssi-threshold -60
```

関連コマンド

config advanced 802.11 coverage exception global

config advanced 802.11 coverage fail-rate

config advanced 802.11 coverage level global

config advanced 802.11 coverage packet-count

config advanced 802.11 coverage

config advanced 802.11 edca-parameters

802.11a ネットワーク上で、特定の拡張型分散チャネル アクセス（EDCA）プロファイルを有効にするには、**config advanced 802.11 edca-parameters** コマンドを使用します。

config advanced 802.11 {**a** | **b**} **edca-parameters** {**wmm-default** | **svp-voice** | **optimized-voice** | **optimized-video-voice** | **custom-voice** | **fastlane** | **custom-set** { *QoS Profile Name* } { **aifs** *AP-value (0-16) Client value (0-16)* | **ecwmax** *AP-Value (0-10) Client value (0-10)* | **ecwmin** *AP-Value (0-10) Client value (0-10)* | **txop** *AP-Value (0-255) Client value (0-255)* } }

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
wmm-default	Wi-Fi Multimedia（WMM）デフォルト パラメータを有効にします。音声サービスまたはビデオ サービスがネットワーク上に展開されていない場合に、このオプションを選択します。
svp-voice	Spectralink 音声優先パラメータを有効にします。通話の質を向上するため、ネットワークに Spectralink 電話技術を実装している場合に、このオプションを選択します。
optimized-voice	EDCA 音声最適化パラメータを有効にします。Spectralink 以外の音声サービスをネットワーク上で展開している場合に、このオプションを選択します。
optimized-video-voice	音声およびビデオ用に最適化された EDCA プロファイル パラメータを有効にします。ネットワーク上で音声サービスとビデオ サービスを両方とも展開する場合に、このオプションを選択します。 （注） ビデオ サービスを展開する場合は、アドミッション制御を無効にする必要があります。
custom-voice	802.11a のカスタム音声 EDCA パラメータをイネーブルにします。このオプションの EDCA パラメータは、このプロファイルが適用された場合、6.0 WMM EDCA パラメータとも一致します。

fastlane	互換性のあるデバイスでファストレーンを有効にします。
custom-set	EDCA パラメータのカスタマイズを有効にします。 • **aifs—Configures the Arbitration Inter-Frame Space.** **AP Value (0-16) Client value (0-16)** • **ecwmax—Configures the maximum Contention Window.** **AP Value(0-10) Client Value (0-10)** • **ecwmin—Configures the minimum Contention Window.** **AP Value(0-10) Client Value(0-10)** • **txop—Configures the Arbitration Transmission Opportunity Limit.** **AP Value(0-255) Client Value(0-255)** QoS プロファイル名：QoS プロファイル名を入力します。 • bronze • silver • Gold • platinum

コマンド デフォルト

デフォルトの EDCA パラメータは **wmm-default** 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。
8.2.110.0	このリリースで、edca-parameters コマンドに custom-set キーワードが追加されました。
8.3	このコマンドが変更され、**fastlane** キーワードが追加されました。

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。

例

次に、Spectralink 音声優先パラメータを有効にする例を示します。

```
(Cisco Controller) > config advanced 802.11 edca-parameters svp-voice
```

関連コマンド

config advanced 802.11b edca-parameters	802.11aネットワーク上で、特定の拡張型分散チャネル アクセス（EDCA）プロファイルを有効にします。
show 802.11a	802.11aネットワークの基本的な設定を表示します。

config advanced 802.11 factory

802.11a の詳細設定を工場出荷時のデフォルトにリセットするには、**config advanced 802.11 factory** コマンドを使用します。

config advanced 802.11{**a** | **b**} **factory**

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。

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。

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、すべての 802.11a の詳細設定を工場出荷時のデフォルトに戻す例を示します。

```
(Cisco Controller) > config advanced 802.11a factory
```

関連コマンド

show advanced 802.11a channel

config advanced 802.11 group-member

802.11 静的 RF グループのメンバを設定するには、**config advanced 802.11 group-member** コマンドを使用します。

config advanced 802.11{**a** | **b**} **group-member**{**add** | **remove**} *controller controller-ip-address*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
add	静的 RF グループにコントローラを追加します。
remove	静的RF グループからコントローラを除外します。
controller	追加するコントローラの名前。
controller-ip-address	追加するコントローラの 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。

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、802.11a 自動 RF グループにコントローラを追加する例を示します。

```
(Cisco Controller) > config advanced 802.11a group-member add cisco-controller
209.165.200.225
```

関連コマンド

show advanced 802.11a group

config advanced 802.11 group-mode

config advanced 802.11 group-mode

802.11a の自動 RF グループ選択モードをオンまたはオフに設定するには、**config advanced 802.11 group-mode** コマンドを使用します。

config advanced 802.11 {**a** | **b**} **group-mode** {**auto** | **leader** | **off** | **restart**}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
auto	802.11a RF グループ選択を自動更新モードに設定します。
leader	802.11a RF グループ選択をスタティック モードに設定し、グループ リーダーとしてこのコントローラを設定します。
off	802.11a RF グループ選択をオフに設定します。
restart	802.11a RF グループ選択を再起動します。

コマンド デフォルト

802.11a の自動 RF グループ選択モードは、デフォルトでは auto 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。

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、802.11a の自動 RF グループ選択モードをオンに設定する例を示します。

```
(Cisco Controller) > config advanced 802.11a group-mode auto
```

次に、802.11a の自動 RF グループ選択モードをオフに設定する例を示します。

```
(Cisco Controller) > config advanced 802.11a group-mode off
```

関連コマンド

show advanced 802.11a group

config advanced 802.11 group-member

config advanced 802.11 logging channel

チャネル変更ロギング モードをオンまたはオフに設定するには、**config advanced 802.11 logging channel** コマンドを使用します。

config advanced 802.11｛**a** ｜ **b**｝ **logging channel** ｛**on** ｜ **off**｝

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
logging channel	チャネル変更をロギングします。
on	802.11 チャネルのロギングを有効にします。
off	802.11 チャネルのロギングを無効にします。

コマンド デフォルト

デフォルトのチャネル変更ロギング モードはオフ（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。

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、802.11a ロギング チャネル選択モードをオンにする例を示します。

```
(Cisco Controller) > config advanced 802.11a logging channel on
```

関連コマンド

show advanced 802.11a logging

config advanced 802.11b logging channel

config advanced 802.11 logging coverage

カバレッジ プロファイル ロギング モードをオンまたはオフに設定するには、**config advanced 802.11 logging coverage** コマンドを使用します。

config advanced 802.11{**a** | **b**} **logging coverage** {**on** | **off**}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
on	802.11 のカバレッジ プロファイル違反ロギングを有効にします。
off	802.11 のカバレッジ プロファイル違反ロギングを無効にします。

コマンド デフォルト

デフォルトのカバレッジ プロファイル ロギング モードはオフ（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。

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、802.11a カバレッジ プロファイル違反ロギング選択モードをオンにする例を示します。

```
(Cisco Controller) > config advanced 802.11a logging coverage on
```

関連コマンド

show advanced 802.11a logging

config advanced 802.11b logging coverage

config advanced 802.11 logging foreign

外部干渉プロファイル ロギング モードをオンまたはオフに設定するには、**config advanced 802.11 logging foreign** コマンドを使用します。

config advanced 802.11｛**a** ｜ **b**｝ **logging foreign** ｛**on** ｜ **off**｝

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
on	802.11 外部干渉プロファイル違反ロギングを有効にします。
off	802.11 外部干渉プロファイル違反ロギングを無効にします。

コマンド デフォルト

デフォルトの外部干渉プロファイル ロギング モードはオフ（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。

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、802.11a外部干渉プロファイル違反ロギング選択モードをオンにする例を示します。

```
(Cisco Controller) > config advanced 802.11a logging foreign on
```

関連コマンド

show advanced 802.11a logging

config advanced 802.11b logging foreign

config advanced 802.11 logging load

802.11a 負荷プロファイル ロギング モードをオンまたはオフに設定するには、**config advanced 802.11 logging load** コマンドを使用します。

config advanced 802.11 {**a** | **b**} **logging load** {**on** | **off**}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
on	802.11 負荷プロファイル違反ロギングを有効にします。
off	802.11 負荷プロファイル違反ロギングを無効にします。

コマンド デフォルト

デフォルトの 802.11 a 負荷プロファイル ロギング モードはオフ (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。

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、802.11a 負荷プロファイル ロギング モードをオンにする例を示します。

```
(Cisco Controller) > config advanced 802.11 logging load on
```

関連コマンド

show advanced 802.11a logging

config advanced 802.11b logging load

config advanced 802.11 logging noise

802.11a ノイズ プロファイル ロギング モードをオンまたはオフに設定するには、**config advanced 802.11 logging noise** コマンドを使用します。

config advanced 802.11 {**a** | **b**} **logging noise** {**on** | **off**}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
on	802.11 ノイズ プロファイル違反ロギングを有効にします。
off	802.11 ノイズ プロファイル違反ロギングを無効にします。

コマンド デフォルト

デフォルトの 802.11 a ノイズ プロファイル ロギング モードはオフ (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。

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、802.11a ノイズ プロファイル ロギング モードをオンにする例を示します。

```
(Cisco Controller) > config advanced 802.11a logging noise on
```

関連コマンド

show advanced 802.11a logging

config advanced 802.11b logging noise

config advanced 802.11 logging performance

802.11aパフォーマンス プロファイル ロギング モードをオンまたはオフに設定するには、**config advanced 802.11 logging performance** コマンドを使用します。

config advanced 802.11｛**a** ｜ **b**｝ **logging performance** ｛**on** ｜ **off**｝

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
on	802.11 パフォーマンス プロファイル違反ロギングを有効にします。
off	802.11 パフォーマンス プロファイル違反ロギングを無効にします。

コマンド デフォルト

デフォルトの 802.11 a パフォーマンス プロファイル ロギング モードはオフ (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。

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、802.11a パフォーマンス プロファイル ロギング モードをオンにする例を示します。

```
(Cisco Controller) > config advanced 802.11a logging performance on
```

関連コマンド

show advanced 802.11a logging

config advanced 802.11b logging performance

config advanced 802.11 logging txpower

802.11a 伝送パワー変更ロギング モードをオンまたはオフに設定するには、**config advanced 802.11 logging txpower** コマンドを使用します。

config advanced 802.11｛**a** ｜ **b**｝ **logging txpower** ｛**on** ｜ **off**｝

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
on	802.11 伝送パワー変更のロギングを有効にします。
off	802.11 伝送パワー変更のロギングを無効にします。

コマンド デフォルト

デフォルトの 802.11 a 伝送パワー変更ロギング モードはオフ（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。

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、802.11a 伝送パワー変更モードをオンにする例を示します。

```
(Cisco Controller) > config advanced 802.11 logging txpower off
```

関連コマンド

show advanced 802.11 logging

config advanced 802.11b logging power

config advanced 802.11 monitor channel-list

802.11a ノイズ、干渉、および不正な監視チャネル リストを設定するには、**config advanced 802.11 monitor channel-list** コマンドを使用します。

config advanced 802.11{**a** | **b**} **monitor channel-list** {**all** | **country** | **dca**}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
all	すべてのチャネルを監視します。
country	設定されている国コードで使用するチャネルを監視します。
dca	自動チャネル割り当てで使用するチャネルを監視します。

コマンド デフォルト

802.11a ノイズ、干渉、および不正な監視チャネル リストは、デフォルトでは country に設定されています。

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。

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、設定されている国で使用するチャネルを監視する例を示します。

```
(Cisco Controller) > config advanced 802.11 monitor channel-list country
```

関連コマンド

show advanced 802.11a monitor coverage

config advanced 802.11 monitor load

負荷測定間隔を 60 ～ 3,600 秒に設定するには、**config advanced 802.11 monitor load** コマンドを使用します。

config advanced 802.11{**a** | **b**} **monitor load** *seconds*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
seconds	60 ～ 3,600 秒の負荷測定間隔。

コマンド デフォルト

デフォルトの負荷測定間隔は 60 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。

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、負荷測定間隔を 60 秒に設定する例を示します。

```
(Cisco Controller) > config advanced 802.11 monitor load 60
```

関連コマンド

show advanced 802.11a monitor

config advanced 802.11b monitor load

config advanced 802.11 monitor measurement

信号測定間隔を 60 ～ 3,600 秒に設定するには、**config advanced 802.11 monitor measurement** コマンドを使用します。

config advanced 802.11 {**a** | **b**} **monitor measurement** *seconds*

構文の説明

seconds	入力する必要がある信号測定間隔。有効な範囲は、60 ～ 3600 秒です。

コマンド デフォルト

デフォルトの信号測定間隔は 180 秒です。

コマンド履歴

リリース	変更内容
8.2	このコマンドが導入されました。

次に、信号測定間隔を 300 秒に設定する例を示します。

```
(Cisco Controller) > config advanced 802.11 monitor measurement 300
```

config advanced 802.11 monitor mode

802.11a アクセス ポイントの監視を有効または無効にするには、**config advanced 802.11 monitor mode** コマンドを使用します。

config advanced 802.11 {**a** | **b**} **monitor mode** {**enable** | **disable**}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
enable	802.11 アクセス ポイントの監視を有効にします。
disable	802.11 アクセス ポイントの監視を無効にします。

コマンド デフォルト

802.11 a アクセス ポイントの監視は、デフォルトでは有効になっています。

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。

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、802.11a アクセス ポイントの監視を有効にする例を示します。

```
(Cisco Controller) > config advanced 802.11a monitor mode enable
```

関連コマンド

show advanced 802.11a monitor

config advanced 802.11b monitor mode

config advanced 802.11 monitor ndp-type

802.11 アクセス ポイントの無線リソース管理（RRM）ネイバー ディスカバリ プロトコル（NDP）タイプを設定するには、**config advanced 802.11 monitor ndp-type** コマンドを使用します。

config advanced 802.11 {**a** | **b**} **monitor ndp-type** {**protected** | **transparent**}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
protected	Tx RRM によって保護された NDP を指定します。
transparent	Tx RRM の透過的な NDP 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。

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。

使用上のガイドライン

802.11 アクセス ポイントの RRM NDP タイプを設定する前に、**config 802.11 disable network** コマンドを入力して、ネットワークを無効にしたことを確認します。

次に、802.11a アクセス ポイント RRM NDP タイプを protected として有効にする例を示します。

```
(Cisco Controller) > config advanced 802.11 monitor ndp-type protected
```

関連コマンド

config advanced 802.11 monitor

config advanced 802.11 monitor mode

config advanced 802.11 disable

config advanced 802.11 monitor timeout-factor

802.11 ネイバー タイムアウト要因を設定するには、**config advanced 802.11 monitor timeout-factor** コマンドを使用します。

config advanced 802.11{**a** | **b**} **monitor timeout-factor** *factor-value-in-minutes*

構文の説明

factor-value-in-minutes	入力する必要のあるネイバー タイムアウト要因の値。有効な範囲は 5 ～ 60 分です。タイムアウト要因を 60 分に設定することをお勧めします。

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
8.1	このコマンドが追加されました。

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。

使用上のガイドライン

リリース 8.1 以降のリリースを使用している場合は、タイムアウト要因を 60 分に設定することをお勧めします。アクセス ポイント無線が 60 分以内に既存のネイバーからネイバー パケットを受信しない場合、Cisco WLC によってネイバー リストからそのネイバーが削除されます。

（注） ネイバー タイムアウト要因は、リリース 7.6 では 60 分にハードコードされていましたが、リリース 8.0.100.0 では 5 分に変更されました。

config advanced 802.11 optimized roaming

各 802.11 帯域の最適化されたローミングのパラメータを設定するには、**config advanced 802.11 optimized roaming** コマンドを使用します。

config advanced {**802.11a** | **802.11b**} **optimized-roaming** {**enable** | **disable** | **interval** *seconds* | **datarate** *mbps*}

構文の説明

802.11a	802.11a ネットワークの最適化されたローミングのパラメータを設定します。
802.11b	802.11b ネットワークの最適化されたローミングのパラメータを設定します。
enable	最適化されたローミングを有効にします。
disable	最適化されたローミングを無効にします。
interval	802.11a/b ネットワークのクライアント カバレッジのレポート間隔を設定します。
seconds	クライアント カバレッジのレポート間隔（秒単位）。範囲は 5 ～ 90 秒です。
datarate	802.11a/b ネットワークのしきい値データ レートを設定します。
mbps	802.11a/b ネットワークのしきい値データ レート（Mbps 単位）。 802.11a の場合、設定可能なデータ レートは 6、9、12、18、24、36、48、および 54 です。 802.11b の場合、設定可能なデータ レートは、1、2、5.5、11、6、9、12、18、24、36、48、および 54 です。 データ レートを 無効にしてクライアントの関連付けを解除するには 0 を設定します。

コマンド デフォルト

デフォルトでは、ローミングの最適化は無効になっています。クライアント カバレッジのレポート間隔のデフォルト値は 90 秒、しきい値データ レートのデフォルト値は 0（無効状態）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。

コマンド履歴

リリース	変更内容
8.8	このコマンドが導入されました。

使用上のガイドライン

ローミングの最適化のレポート間隔を設定する前に、802.11a/b ネットワークを無効にする必要があります。レポートの間隔に対して低い値を設定すると、カバレッジ レポートのメッセージでネットワークが過負荷になることがあります。

次に、802.11a ネットワークの最適化されたローミングを有効にする例を示します。

```
(Cisco Controller) > config advanced 802.11a optimized roaming enable
```

次に、802.11 a ネットワークのデータ レート間隔を設定する例を示します。

```
(Cisco Controller) > config advanced 802.11a optimized roaming datarate 9
```

config advanced 802.11 packet

最大パケット再試行回数、連続パケット障害しきい値、およびデフォルトタイムアウト値を設定するには、**config advanced 802.11 packet** コマンドを使用します。

config advanced 802.11 {**a** | **b**} < *QoS Profile Name* > { **max-client-count** <*threshold value (0-1000)*> | **max-packet-count** <*threshold value (0-1000)*> | **max-retry** <*maximum retry count*> | **timeout** <*time(in miliseconds)*> }

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
QoS Profile Name	• bronze • silver • Gold • platinum
max-client-count	クライアントの関連付けを解除するまでの連続パケット障害しきい値を設定します。 *threshold value*：クライアント数しきい値を 0 ー 1000 の範囲で入力します。
max-packet-count	障害パケットの再試行をやめるまでの連続パケット障害しきい値を設定します。 *threshold value*：パケット障害しきい値を 0 ー 1000 の範囲で入力します。
max-retry	障害パケットのパケット再試行回数を設定します。 *maximum retry count*：再試行の最大許容回数を入力します。
timeout	パケット エージングまたは廃棄タイムアウトしきい値を設定します。 *time*：パケットがタイムアウトするまでの最大時間を入力します。

コマンド デフォルト

config advanced 802.11 packet コマンドのパラメータのデフォルト値は次のとおりです。

キーワード	デフォルト値
max-client-count	500

キーワード	デフォルト値
max-packet-count	100
max-retry	3
timeout	35 ミリ秒

コマンド履歴

リリース	変更内容
8.2	このリリースで packet コマンドが追加されました。

```
(Cisco Controller) > config advanced 802.11a packet platinum max-packet-count 200
```

関連コマンド

show 802.11a	802.11a ネットワークの基本的な設定を表示します。

config advanced 802.11 profile clients

Cisco Lightweight アクセス ポイントのクライアント数のしきい値を 1 ～ 75 に設定するには、**config advanced 802.11 profile clients** コマンドを使用します。

config advanced 802.11 {**a** | **b**} **profile clients** {**global** | *cisco_ap*} *clients*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
global	すべての 802.11a 対応 Cisco Lightweight アクセス ポイントを設定します。
cisco_ap	Cisco Lightweight アクセス ポイント名。
clients	802.11a 対応 Cisco Lightweight アクセス ポイントのクライアント数のしきい値（1 ～ 75）。

コマンド デフォルト

Cisco Lightweight アクセス ポイントのクライアント数のしきい値は、デフォルトでは 12 に設定されています。

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。

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、すべての Cisco Lightweight アクセス ポイントのクライアント数のしきい値を 25 に設定する例を示します。

```
(Cisco Controller) >config advanced 802.11 profile clients global 25
Global client count profile set.
```

次に、AP1 のクライアント数のしきい値を 75 に設定する例を示します。

```
(Cisco Controller) >config advanced 802.11 profile clients AP1 75
Global client count profile set.
```

config advanced 802.11 profile customize

802.11a 対応 Cisco Lightweight アクセス ポイントのパフォーマンス プロファイルのカスタマイズをオンまたはオフにするには、**config advanced 802.11 profile customize** コマンドを使用します。

config advanced 802.11 {**a** | **b**} **profile customize** *cisco_ap* {**on** | **off**}

構文の説明

a	802.11a/n ネットワークを指定します。
b	802.11b/g/n ネットワークを指定します。
cisco_ap	Cisco Lightweight アクセス ポイント。
on	この Cisco Lightweight アクセス ポイントのパフォーマンス プロファイルをカスタマイズします。
off	この Cisco Lightweight アクセス ポイントに対してグローバルデフォルト パフォーマンス プロファイルを使用します。

コマンド デフォルト

パフォーマンス プロファイルのカスタマイズは、デフォルトではオフになっています。

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。

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、802.11a 対応 Cisco Lightweight アクセス ポイント AP1 のパフォーマンス プロファイルのカスタマイズをオンにする例を示します。

```
(Cisco Controller) >config advanced 802.11 profile customize AP1 on
```

config advanced 802.11 profile foreign

外部 802.11a トランスミッタ干渉しきい値を 0 ～ 100 % に設定するには、**config advanced 802.11 profile foreign** コマンドを使用します。

config advanced 802.11 {**a** | **b**} **profile foreign** {**global** | *cisco_ap*} *percent*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
global	すべての 802.11a 対応 Cisco Lightweight アクセス ポイントを設定します。
cisco_ap	Cisco Lightweight アクセス ポイント名。
percent	0 ～ 100 % の外部 802.11a 干渉しきい値。

コマンド デフォルト

デフォルトの外部 802.11a トランスミッタ干渉しきい値は 10 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。

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、すべての Cisco Lightweight アクセス ポイントの外部 802.11a トランスミッタ干渉しきい値を 50 % に設定する例を示します。

```
(Cisco Controller) >config advanced 802.11a profile foreign global 50
```

次に、AP1 の外部 802.11a トランスミッタ干渉しきい値を 0 % に設定する例を示します。

```
(Cisco Controller) >config advanced 802.11 profile foreign AP1 0
```

config advanced 802.11 profile noise

802.11a 外部ノイズしきい値を -127 ～ 0 dBm に設定するには、**config advanced 802.11 profile noise** コマンドを使用します。

config advanced 802.11｛**a** ｜ **b**｝ **profile noise** ｛**global** ｜ *cisco_ap*｝ *dBm*

構文の説明

a	802.11a/n ネットワークを指定します。
b	802.11b/g/n ネットワークを指定します。
global	すべての 802.11a 対応 Cisco Lightweight アクセス ポイントの特定のプロファイルを設定します。
cisco_ap	Cisco Lightweight アクセス ポイント名。
dBm	-127 ～ 0 dBm の 802.11a 外部ノイズしきい値。

コマンド デフォルト

デフォルトの外部ノイズしきい値は –70 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。

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、すべての Cisco Lightweight アクセス ポイントの 802.11a 外部ノイズしきい値を –127 dBm に設定する例を示します。

```
(Cisco Controller) >config advanced 802.11a profile noise global -127
```

次に、AP1 の 802.11a 外部ノイズしきい値を 0 dBm に設定する例を示します。

```
(Cisco Controller) >config advanced 802.11a profile noise AP1 0
```

config advanced 802.11 profile throughput

Cisco Lightweight アクセス ポイントのデータレート スループットしきい値を 1,000 ～ 10,000,000 バイト/秒に設定するには、**config advanced 802.11 profile throughput** コマンドを使用します。

config advanced 802.11 {**a** | **b**} **profile throughput** {**global** | *cisco_ap*} *value*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
global	すべての 802.11a 対応 Cisco Lightweight アクセス ポイントの特定のプロファイルを設定します。
cisco_ap	Cisco Lightweight アクセス ポイント名。
value	802.11a 対応 Cisco Lightweight アクセス ポイントのスループットしきい値（1,000 ～ 10,000,000 バイト/秒）。

コマンド デフォルト

Cisco Lightweight アクセス ポイントのデフォルトのデータレート スループットしきい値は 1,000,000 バイト/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。

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、すべての Cisco Lightweight アクセス ポイントのデータ レートしきい値を 1,000 バイト/秒に設定する例を示します。

```
(Cisco Controller) >config advanced 802.11 profile throughput global 1000
```

次に、AP1 のデータ レートしきい値を 10,000,000 バイト/秒に設定する例を示します。

```
(Cisco Controller) >config advanced 802.11 profile throughput AP1 10000000
```

config advanced 802.11 profile utilization

RF 利用率のしきい値を 0 ～ 100 % に設定するには、**config advanced 802.11 profile utilization** コマンドを使用します。オペレーティング システムがこのしきい値を超えた場合にトラップを生成します。

config advanced 802.11 {**a** | **b**} **profile utilization** {**global** | *cisco_ap*} *percent*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
global	グローバルの Cisco Lightweight アクセス ポイント固有のプロファイルを設定します。
cisco_ap	Cisco Lightweight アクセス ポイント名。
percent	0 ～ 100 % の 802.11a の RF 利用率のしきい値。

コマンド デフォルト

RF 利用率のデフォルトのしきい値は 80% 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。

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、すべての Cisco Lightweight アクセス ポイントの RF 利用率のしきい値を 0 % に設定する例を示します。

```
(Cisco Controller) >config advanced 802.11 profile utilization global 0
```

次に、AP1 の RF 利用率のしきい値を 100 % に設定する例を示します。

```
(Cisco Controller) >config advanced 802.11 profile utilization AP1 100
```

config advanced 802.11 receiver

詳細なレシーバ設定を行うには、**config advanced 802.11 receiver** コマンドを使用します。

config advanced 802.11{**a** | **b**} **receiver** {**default** | **rxstart jumpThreshold** *value*}

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
receiver	レシーバ設定を指定します。
default	デフォルトの詳細なレシーバ設定を指定します。
rxstart jumpThreshold	レシーバ起動信号を指定します。 （注） このオプションは、シスコ社内専用であるため、使用しないことをお勧めします。
value	ジャンプしきい値設定の値（0 ～ 127）。

コマンド デフォルト

なし

使用上のガイドライン

- 802.11 レシーバ設定を変更する前に、802.11 ネットワークを無効にする必要があります。
- **rxstart jumpThreshold** *value* オプションは、シスコ社内専用であるため、使用しないことをお勧めします。

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。

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、ネットワークが有効なとき次にレシーバパラメータを変更できないようにする例を示します。

```
(Cisco Controller) > config advanced 802.11 receiver default
```

config advanced 802.11 reporting measurement

レポート測定間隔を 60 ～ 3,600 秒に設定するには、**config advanced 802.11 reporting measurement** コマンドを使用します。

config advanced 802.11 {**a** | **b**} **reporting measurement** *seconds*

構文の説明

seconds	入力する必要があるレポート測定間隔。有効な範囲は、60 ～ 3600 秒です。

コマンド デフォルト

デフォルトのレポート測定間隔は 180 秒です。

コマンド履歴

リリース	変更内容
8.2	このコマンドが導入されました。

次に、信号測定間隔を 300 秒に設定する例を示します。

```
(Cisco Controller) > config advanced 802.11 reporting measurement 300
```

config advanced 802.11 tpc-version

無線の送信電力の制御（TPC）バージョンを設定するには、**config advanced 802.11 tpc-version** コマンドを使用します。

config advanced 802.11{**a** | **b**} **tpc-version** {**1** | **2**}

構文の説明

1	強力な信号カバレッジおよび安定性を提供する TPC バージョン 1 を指定します。
2	音声コールが広く使用されるシナリオ用の TPC バージョン 2 を指定します。干渉を最小にするために、送信電力が動的に調整されます。これは、高密度のネットワークに適しています。このモードでは、ローミングの遅延およびカバレッジ ホールのインシデントが多く発生する可能性があります。

コマンド デフォルト

無線のデフォルトの TPC のバージョンは 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。

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、802.11a 無線の 1 として TPC のバージョンを設定する例を示します。

```
(Cisco Controller) > config advanced 802.11a tpc-version 1
```

関連コマンド

config advanced 802.11 tpcv1-thresh

config advanced 802.11 tpcv1-thresh

無線の送信電力の制御（TPC）バージョン1のしきい値を設定するには、**config advanced 802.11 tpcv1-thresh** コマンドを使用します。

config advanced 802.11{**a** | **b**} **tpcv1-thresh** *threshold*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g/n ネットワークを指定します。
threshold	50 dBm ～ 80 dBm の範囲のしきい値。

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。

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、802.11a 無線の TPC バージョン 1 でしきい値を -60 dBm として設定する例を示します。

```
(Cisco Controller) > config advanced 802.11 tpcv1-thresh -60
```

関連コマンド

config advanced 802.11 tpc-thresh

config advanced 802.11 tpcv2-thresh

config advanced 802.11 tpcv2-intense

無線の送信電力の制御（TPC）バージョン 2 の算出の強度を設定するには、**config advanced 802.11 tpcv2-intense** コマンドを使用します。

config advanced 802.11{**a** | **b**} **tpcv2-intense** *intensity*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g/n ネットワークを指定します。
intensity	1～100 の算出の強度。

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。

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、802.11a 無線の TPC バージョン 2 で算出の強度を 50 として設定する例を示します。

```
(Cisco Controller) > config advanced 802.11 tpcv2-intense 50
```

関連コマンド

config advanced 802.11 tpc-thresh

config advanced 802.11 tpcv2-thresh

config advanced 802.11 tpcv2-per-chan

config advanced 802.11 tpcv2-per-chan

送信電力の制御バージョン 2 をチャネル単位で設定するには、**config advanced 802.11 tpcv2-per-chan** コマンドを使用します。

config advanced 802.11{**a** | **b**} **tpcv2-per-chan** {**enable** | **disable**}

構文の説明

enable	TPC バージョン 2 の設定をチャネル単位で有効にします。
disable	TPC バージョン 2 の設定をチャネル単位で無効にします。

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。

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、802.11a 無線の TPC バージョン 2 をチャネル単位で有効にする例を示します。

```
(Cisco Controller) > config advanced 802.11 tpcv2-per-chan enable
```

関連コマンド

config advanced 802.11 tpc-thresh

config advanced 802.11 tpcv2-thresh

config advanced 802.11 tpcv2-intense

config advanced 802.11 tpcv2-thresh

無線の送信電力の制御（TPC）バージョン2のしきい値を設定するには、**config advanced 802.11 tpcv2-thresh** コマンドを使用します。

config advanced 802.11{**a** | **b**} **tpcv2-thresh** *threshold*

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。
threshold	50 dBm ～ 80 dBm の範囲のしきい値。

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。

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、802.11a 無線の TPC バージョン 2 でしきい値を -60 dBm として設定する例を示します。

```
(Cisco Controller) > config advanced 802.11a tpcv2-thresh -60
```

関連コマンド

config advanced 802.11 tpc-thresh

config advanced 802.11 tpcv1-thresh

config advanced 802.11 tpcv2-per-chan

config advanced 802.11 txpower-update

すべての Cisco Lightweight アクセス ポイントで 802.11a 伝送パワーの更新を開始するには、**config advanced 802.11 txpower-update** コマンドを使用します。

config advanced 802.11{**a** | **b**} **txpower-update**

構文の説明

a	802.11a ネットワークを指定します。
b	802.11b/g ネットワークを指定します。

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。

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、802.11a アクセス ポイントで 802.11a 伝送パワーの更新を開始する例を示します。

```
(Cisco Controller) > config advanced 802.11 txpower-update
```

関連コマンド

config advance 802.11b txpower-update

config advanced eap

詳細な拡張認証プロトコル（EAP）設定を行うには、**config advanced eap** コマンドを使用します。

config advanced eap {**bcast-key-interval** *seconds* | **eapol-key-timeout** *timeout* | **eapol-key-retries** *retries* | **identity-request-timeout** *timeout* | **identity-request-retries** *retries* | **key-index** *index* | **max-login-ignore-identity-response** {**enable** | **disable**} **request-timeout** *timeout* | **request-retries** *retries*}

構文の説明

bcast-key-interval *seconds*	EAP ブロードキャスト キー更新間隔を秒単位で指定します。 範囲は 120 ～ 86400 秒です。
eapol-key-timeout *timeout*	EAP または WPA/WPA-2 PSK を使用してコントローラが無線クライアントに EAPOL（WPA）キー メッセージを再送信するまでに待機する時間（200 ～ 5000 ミリ秒）を指定します。 デフォルト値は 1000 ミリ秒です。
eapol-key-retries *retries*	コントローラが無線クライアントに EAPOL（WPA）キー メッセージを再送信する最大回数（0～4）を指定します。 デフォルト値は 2 です。
identity-request- timeout *timeout*	コントローラが無線クライアントに EAP ID 要求メッセージを再送信するまでに待機する時間（1 ～ 120 秒）を指定します。 デフォルト値は 30 秒です。
identity-request- retries	コントローラが無線クライアントに EAPOL（WPA）キー メッセージを再送信する最大回数（0～4）を指定します。 デフォルト値は 2 です。
key-index *index*	ダイナミック Wired Equivalent Privacy（WEP）で使用するキーインデックス（0 または 3）を指定します。

max-login-ignore- identity-response	有効になっている場合、このコマンドは、802.1x 認証を使用して同じユーザ名のコントローラに接続可能なデバイスの数に対して設定されている制限を無視します。ディセーブルにすると、このコマンドは、コントローラに同じユーザ名で接続できるデバイスの数を制限します。このオプションは、Web認証ユーザには適用されません。 同じユーザ名で接続できるデバイスの最大数を制限するには、**config netuser maxUserLogin** コマンドを使用します。
enable	最大EAP ID応答に到達する同じユーザ名を無視します。
disable	最大EAP ID応答に到達する同じユーザ名を確認します。
request-timeout	ID 要求または EAPOL（WPA）キー メッセージ以外の EAP メッセージについて、コントローラが無線クライアントにメッセージを再送信するまでに待機する時間（1 ～ 120 秒）を指定します。 デフォルト値は 30 秒です。
request-retries	（任意）ID 要求または EAPOL（WPA）キー メッセージ以外の EAP メッセージについて、コントローラが無線クライアントにメッセージを再送信する最大回数（0 ～ 20）を指定します。 デフォルト値は 2 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。

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、ダイナミック Wired Equivalent Privacy（WEP）に使用するキー インデックスを設定する例を示します。

```
(Cisco Controller) > config advanced eap key-index 0
```

関連コマンド

show advanced eap

config advanced fra service-priority

フレキシブル ラジオ アサインメント（FRA）サービスの優先順位を設定するには、**config advanced fra service-priority** コマンドを使用します。

config advanced fra service-priority［**client-aware** | **coverage** | **service-assurance**］

構文の説明

client-aware	FRA サービスの優先順位をクライアント認識に設定します。
coverage	FRA サービスの優先順位をカバレッジに設定します。
service-assurance	FRA サービスの優先順位をサービス保証に設定します。**service-assurance** は 8.5 リリースではサポートされていません。

コマンド デフォルト

なし

コマンド モード

グローバル コンフィギュレーション（config）

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

次に、FRA サービスの優先順位を client-aware に設定する例を示します。

```
(Cisco Controller) > config advanced fra service-priority client-aware
```

次に、FRA サービスの優先順位を coverage に設定する例を示します。

```
(Cisco Controller) > config advanced fra service-priority coverage
```

関連コマンド

config advanced fra client-aware client-select

config advanced fra client-aware client-reset

config advanced fra client-aware client-select

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使用率のしきい値を設定するには、**config advanced fra client-aware client-select** コマンドを使用します。

config advanced fra client-aware client-select パーセント

構文の説明

percent	0 ～ 100 までの使用率の値。 （注） **client-select** *percent* の値は **client-reset** *percent* の値よりも大きくする必要があります。そうしない場合は、次のメッセージが表示されます。 Input for Client Aware FRA Client Reset Utilization Threshold is out of range.

コマンド デフォルト

client-select のデフォルトの percent 値は 50 % です。

コマンド モード

グローバル コンフィギュレーション（config）

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

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使用率のしきい値を設定する例を示します。

```
(Cisco Controller) > config advanced fra client-aware client-select 20
```

関連コマンド

config advanced fra client-aware client-reset

config advanced fra client-aware client-reset

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使用率のしきい値を設定するには、**config advanced fra client-aware client-reset** コマンドを使用します。

config advanced fra client-aware client-reset パーセント

構文の説明

percent	0 ～ 100 までの使用率の値。 （注） **client-reset** *percent* の値が **client-select** *percent* の値よりも大きい場合は、次のメッセージが表示されます。 Input for Client Aware FRA Client Reset Utilization Threshold is out of range.

コマンド デフォルト

client-reset のデフォルトの percent 値は 5 % です。

コマンド モード

グローバル コンフィギュレーション（config）

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

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使用率のしきい値を設定する例を示します。

```
(Cisco Controller) > config advanced fra client-aware client-reset 15
```

関連コマンド

config advanced fra client-aware client-select

config advanced hyperlocation

Cisco HyperLocation モジュールを搭載するすべての AP で Cisco HyperLocation をグローバルに設定するには、**config advanced hyperlocation** コマンドを使用します。

config advanced hyperlocation{**enable** |**disable** |**ntp** *ipv4-addr* |**flag-unset** *ap-name*|**reset-threshold** *value*|**threshold** *value*|**trigger-threshold** *value*}

構文の説明

enable	Cisco HyperLocation モジュールを搭載するすべての Cisco AP で Cisco HyperLocation をグローバルに有効にします。
disable	Cisco HyperLocation モジュールを搭載するすべての Cisco AP で Cisco HyperLocation をグローバルに無効にします。
ntp *ipv4-addr*	Cisco HyperLocation 用に NTPサーバをセットアップします。この計算に関係するすべての AP が同期する必要がある NTP サーバの IPv4 アドレスを入力します。
flag-unset *ap-name*	他のすべての Cisco HyperLocation 設定レベルを受け入れるように、指定された AP を設定します。
reset-threshold *value*	この値未満の場合、Cisco WLC に送信中に RSSI が無視される PRL リセットしきい値を設定します。
reset-threshold *value*	この値未満の場合、Cisco WLC に送信中に RSSI が無視されるしきい値を設定します。
trigger-threshold *value*	PAK RSSI ロケーション トリガー間でのスキャン サイクル数を設定します。

コマンド デフォルト

無効

使用上のガイドライン

- 有効な状態になっている Cisco HyperLocation はパフォーマンスに影響を与え、Cisco HyperLocation モジュールを搭載していない AP の両方の無線が 3 秒ごとに約 10 ミリ秒間オフチャネルになります。
- 一般的な Cisco WLC インフラストラクチャで使用されるのと同じ NTP サーバを使用することをお勧めします。ロケーションを正確に計算するためには、複数の AP からのスキャンが同期されている必要があります。

コマンド履歴

リリース	変更内容
8.1	このコマンドが導入されました。

次に、すべての AP で Cisco HyperLocation を有効にする例を示します。

```
(Cisco Controller) >config advanced hyperlocation enable
```

config advanced hyperlocation apgroup

Cisco HyperLocation モジュールを搭載する AP が含まれる AP グループ用に Cisco HyperLocation を設定するには、**config advanced hyperlocation apgroup** コマンドを使用します。

config advanced hyperlocation apgroup *group-name* {**enable** |**disable**}

構文の説明

enable	Cisco HyperLocation モジュールを搭載する AP が含まれる AP グループ用に Cisco HyperLocation を有効にします。
disable	Cisco HyperLocation モジュールを搭載する AP が含まれる AP グループ用に Cisco HyperLocation を無効にします。

コマンド デフォルト

無効

使用上のガイドライン

有効な状態になっている Cisco HyperLocation はパフォーマンスに影響を与え、Cisco HyperLocation モジュールを搭載していない AP の両方の無線が 3 秒ごとに約 10 ミリ秒間オフチャネルになります。

コマンド履歴

リリース	変更内容
8.1	このコマンドが導入されました。

次に、AP グループ用に Cisco HyperLocation を有効にする例を示します。

```
(Cisco Controller) >config advanced hyperlocation apgroup myapgroup enable
```

config advanced hyperlocation ble-beacon

BLE ビーコン パラメータを設定するには、**config advanced hyperlocation ble-beacon** コマンドを使用します。

config advanced hyperlocation ble-beacon {**advertised-power** *rssi-value* |**interval** *value* |**ap-name** *ap-name*|{**advertised-power** *rssi-value* |**interval** *value* |**unset**}}

構文の説明

advertised-power *rssi-value*	すべての AP の BLE アドバタイズ送信電力を設定します。有効な範囲は -40 ～ -100 dBm です。
interval *value*	すべての AP の BLE ビーコン間隔を設定します。有効な範囲は 1 ～ 10 秒です。
ap-name *ap-name*	指定された AP の BLE ビーコンのパラメータを設定します。
unset	AP 固有の BLE 設定をクリアし、グローバル BLE 設定が適用されている場合はそれを設定します。

コマンド履歴

リリース	変更内容
8.1	このコマンドが導入されました。

次に、すべての AP の BLE ビーコン間隔を 8 秒に設定する例を示します。

```
(Cisco Controller) >config advanced hyperlocation ble-beacon interval 8
```

config advanced hyperlocation ble-beacon beacon-id

特定のビーコンの BLE ビーコン パラメータを設定するには、**config advanced hyperlocation ble-beacon beacon-id** コマンドを使用します。

config advanced hyperlocation ble-beacon beacon-id *id* {{**delete** |**enable** |**disable** }| **add** {**txpwr** *value*| **uuid** *value*}| **add ap-group** *group-name* {**enable** |**disable** | **major** *mjr-value* | **minor** *mnr-value* | **txpwr** *value*| **uuid** *value*}| **add ap-name** *ap-name*{**enable** |**disable** | **major** *mjr-value* | **minor** *mnr-value* | **txpwr** *value*| **uuid** *value*}}

構文の説明

beacon-id *id*	入力するビーコン ID の BLE パラメータを設定します。有効な範囲は 1 ～ 5 です。
delete	BLE ビーコンを削除します。
enable	BLE ビーコンを有効にします。
disable	BLE ビーコンを無効にします。
add	BLE ビーコンを追加します。
txpwr *value*	BLE減衰レベルを設定します。これはすべてのAP、APグループ、または特定のAPに設定するために選択できます。有効な範囲は-52 ～ 0 dBm です。
uuid *value*	ビーコンの汎用一意識別子（UUID）を設定します。これはすべての AP、AP グループ、または特定の AP に設定するために選択できます。xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx 形式で値を入力します。
ap-group *group-name*	指定された AP グループの BLE ビーコンのパラメータを設定します。
ap-name *ap-name*	指定された AP の BLE ビーコンのパラメータを設定します。
major *mjr-value*	BLE ビーコンのメジャー値を設定します。これは AP グループまたは特定の AP に設定するために選択できます。
minor *mnr-value*	BLE ビーコンのマイナー値を設定します。これは AP グループまたは特定の AP に設定するために選択できます。

コマンド履歴

リリース	変更内容
8.1	このコマンドが導入されました。

次に、ID 値が 3 の BLE ビーコンを有効にする例を示します。

```
(Cisco Controller) >config advanced hyperlocation ble-beacon beacon-id 3 enable
```

config advanced hotspot

高度なホットスポット設定を指定するには、**config advanced hotspot** コマンドを使用します。

config advanced hotspot {**anqp-4way** {**disable** | **enable** | **threshold** *value* } | **cmbk-delay** *value* | **garp** {**disable** | **enable** } | **gas-limit** {**disable** | **enable** }}

構文の説明

anqp-4way	Network Query Protocol（ANQP）4-way フラグメントのしきい値をイネーブル化、ディセーブル化、または設定します。
disable	ANQP 4-way メッセージをディセーブルにします。
enable	ANQP 4-way メッセージをイネーブルにします。
threshold	ANQP 4-way フラグメントのしきい値を設定します。
value	バイト単位の ANQP 4-way フラグメントのしきい値。範囲は 10 ～ 1500 です。デフォルト値は 1500 です
cmbk-delay	時間単位（TU）の ANQP の戻り遅延を設定します。
value	時間単位（TU）の ANQP の戻り遅延。1 TU は、1024 usec として 802.11 で定義されています。指定できる範囲は 1～ 30 秒です。
garp	ワイヤレス ネットワークへの Gratuitous ARP（GARP）転送をディセーブルまたはイネーブルにします。
disable	ワイヤレス ネットワークへの Gratuitous ARP（GARP）転送をディセーブルにします。
enable	ワイヤレス ネットワークへの Gratuitous ARP（GARP）転送をイネーブルにします。
gas-limit	指定した間隔で、アクセス ポイントによりスイッチに送信される Generic Advertisement Service（GAS）要求アクション フレームの数を制限します。
disable	アクセス ポイントの GAS 要求アクション フレームの制限をディセーブルにします。
enable	アクセス ポイントの GAS 要求アクション フレームの制限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 ANQP 4-way フラグメントのしきい値を設定する例を示します。

```
(Cisco Controller) >config advanced hotspot anqp-4way threshold 200
```

config advanced timers auth-timeout

認証タイムアウトを設定するには、**config advanced timers auth-timeout** コマンドを使用します。

config advanced timers auth-timeout *seconds*

構文の説明

seconds	10 ～600 秒の認証応答タイムアウト値。

コマンド デフォルト

デフォルトの認証タイムアウト値は 10 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。

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、認証タイムアウトを 20 秒に設定する例を示します。

```
(Cisco Controller) >config advanced timers auth-timeout 20
```

config advanced timers eap-timeout

拡張可能認証プロトコル（EAP）有効期限タイムアウトを設定するには、**config advanced timers eap-timeout** コマンドを使用します。

config advanced timers eap-timeout *seconds*

構文の説明

seconds	8 ～ 120 秒の EAP タイムアウト値。

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。

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、EAP 有効期限タイムアウトを 10 秒に設定する例を示します。

```
(Cisco Controller) >config advanced timers eap-timeout 10
```

config advanced timers eap-identity-request-delay

詳細な拡張可能認証プロトコル（EAP）アイデンティティ要求遅延を秒単位で設定するには、**config advanced timers eap-identity-request-delay** コマンドを使用します。

config advanced timers eap-identity-request-delay *seconds*

構文の説明

seconds	0 ～ 10 秒の詳細な EAP ID 要求遅延。

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。

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、詳細な EAP アイデンティティ要求遅延を 8 秒に設定する例を示します。

```
(Cisco Controller) >config advanced timers eap-identity-request-delay 8
```

config advanced timers

高度なシステム タイマーを設定するには、**config advanced timers** コマンドを使用します。

config advanced timers {**ap-coverage-report** *seconds* | **ap-discovery-timeout** *discovery-timeout* | **ap-fast-heartbeat** {**local** | **flexconnect** | **all**} {**enable** | **disable**} *fast_heartbeat_seconds* | **ap-heartbeat-timeout** *heartbeat_seconds* | **ap-primary-discovery-timeout** *primary_discovery_timeout* | **ap-primed-join-timeout** *primed_join_timeout* | **auth-timeout** *auth_timeout* | **pkt-fwd-watchdog** {**enable** | **disable**} {*watchdog_timer* | **default**} | **eap-identity-request-delay** *eap_identity_request_delay* | **eap-timeout** *eap_timeout*}

構文の説明

ap-coverage-report	すべての AP の RRM カバレッジ レポート間隔を設定します。
seconds	AP のカバレッジ レポート間隔を秒単位で設定します。範囲は 60 ~ 90 秒です。デフォルトは 90 秒です。
ap-discovery-timeout	Cisco Lightweight アクセス ポイントの検出タイムアウト値を設定します。
discovery-timeout	Cisco Lightweight アクセス ポイントの検出タイムアウト値（秒単位）。値の範囲は 1 ～ 10 です。
ap-fast-heartbeat	アクセス ポイントのコントローラ障害を検出するために要する時間を短縮する高速ハートビート タイマーを設定にします。
local	ローカル モードのアクセス ポイントの高速ハートビート間隔を設定します。
flexconnect	FlexConnect モードのアクセス ポイントの高速ハートビート間隔を設定します。
all	すべてのアクセス ポイントの高速ハートビート間隔を設定します。
enable	ファーストハートビート間隔を有効にします。
disable	ファーストハートビート間隔を無効にします。
fast_heartbeat_seconds	コントローラ障害を検出するために要する時間を短縮する小さい値のハートビート間隔（秒単位）。値の範囲は 1 ～ 10 です。
ap-heartbeat-timeout	Cisco Lightweight アクセス ポイントのハートビート タイムアウト値を設定します。

heartbeat_seconds	Cisco Lightweight アクセス ポイントのハートビート タイムアウト値（秒単位）。値の範囲は 1 ～ 30 です。この値は、高速ハートビート タイマーの 3 倍以上の値である必要があります。
ap-primary-discovery-timeout	アクセス ポイントのプライマリ ディスカバリ要求タイマーを設定します。
primary_discovery_timeout	アクセス ポイントのプライマリ検出要求時間（秒単位）。範囲は 30 ～ 3600 です。
ap-primed-join-timeout	アクセス ポイントのプライミングされた検出タイムアウト値を設定します。
primed_join_timeout	アクセス ポイントのプライミングされた検出タイムアウト値（秒単位）。範囲は 120 ～ 43200 です。
auth-timeout	認証タイムアウトを設定します。
auth_timeout	認証応答タイムアウト値（秒単位）。範囲は 10 ～ 600 です。
pkt-fwd-watchdog	ファストパスのデッドロックから保護するためのパケット転送ウォッチドッグ タイマーを設定します。
watchdog_timer	パケット転送ウォッチドッグ タイマー（秒単位）。範囲は 60 ～ 300 です。
default	ウォッチドッグ タイマーをデフォルト値の 240 秒に設定します。
eap-identity-request-delay	詳細な拡張可能認証プロトコル（EAP）アイデンティティ要求遅延を秒単位で設定します。
eap_identity_request_delay	詳細な EAP アイデンティティ要求遅延（秒単位）。範囲は 0 ～ 10 です。
eap-timeout	EAP 有効期限タイムアウトを設定します。
eap_timeout	EAP タイムアウト値（秒単位）。範囲は 8 ～ 120 です。

コマンド デフォルト

- デフォルトのアクセス ポイント検出タイムアウトは 10 秒です。
- デフォルトのアクセス ポイント ハートビート タイムアウトは 30 秒です。

- デフォルトのアクセス ポイント プライマリ検出要求タイマーは 120 秒です。
- デフォルトの認証タイムアウトは 10 秒です。
- デフォルトのパケット転送ウォッチドッグ タイマーは 240 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。
8.3	コマンドの機能が拡張されました。
8.6	このコマンドはリリース 8.6 で新しいキーワードによって機能が拡張されました。追加された新しいキーワードは **ap-coverage-report** です。

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。

使用上のガイドライン

Cisco Lightweight アクセス ポイントの検出タイムアウトとは、Cisco WLC が、接続されていない Cisco Lightweight アクセス ポイントの検出を試行する頻度です。

Cisco Lightweight アクセス ポイントのハートビート タイムアウトは、Cisco Lightweight アクセス ポイントが Cisco Wireless LAN Controller にハートビート キープアライブ信号を送信する頻度を制御します。

次に、タイムアウト値を 20 でアクセス ポイント検出タイムアウトを設定する例を示します。

```
(Cisco Controller) >config advanced timers ap-discovery-timeout 20
```

次に、FlexConnect モードのアクセス ポイントを対象に高速ハートビート間隔を有効にする例を示します。

```
(Cisco Controller) >config advanced timers ap-fast-heartbeat flexconnect enable 8
```

次に、認証タイムアウトを 20 秒に設定する例を示します。

```
(Cisco Controller) >config advanced timers auth-timeout 20
```

config advanced fastpath fastcache

ファストパスのファスト キャッシュ制御を設定するには、**config advanced fastpath fastcache** コマンドを使用します。

config advanced fastpath fastcache {**enable** | **disable**}

構文の説明

enable	ファストパスのファスト キャッシュ制御をイネーブルにします。
disable	ファストパスのファストキャッシュ制御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、ファストパスのファスト キャッシュ制御を有効にする例を示します。

```
(Cisco Controller) > config advanced fastpath fastcache enable
```

関連コマンド

config advanced fastpath pkt-capture

config advanced fastpath pkt-capture

ファストパスのパケット キャプチャを設定するには、**config advanced fastpath pkt-capture** コマンドを使用します。

config advanced fastpath pkt-capture {**enable** | **disable**}

構文の説明

enable	ファストパスのパケット キャプチャをイネーブルにします。
disable	ファストパスのパケットキャプチャ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、ファストパスのパケット キャプチャを有効にする例を示します。

```
(Cisco Controller) > config advanced fastpath pkt-capture enable
```

関連コマンド

config advanced fastpath fastcache

config advanced sip-preferred-call-no

音声優先制御を設定するには、**config advanced sip-preferred-call-no** コマンドを使用します。

config advanced sip-preferred-call-no *call_index* {*call_number* | **none**}

構文の説明

call_index	1 ～ 6 の間の有効な値を持つコール インデックス。
call_number	27 文字まで使用できる優先コール数。
none	指定されたインデックスにセットされている優先コールを削除します。

コマンド デフォルト

なし

使用上のガイドライン

音声優先制御を設定する前に、次の前提条件を実行する必要があります。

- **config wlan qos** *wlan-id* **platinum** コマンドを入力して、音声をプラチナ QoS レベルに設定します。
- **config 802.11** {**a** | **b**} **cac** {**voice** | **video**} **acm enable** コマンドを入力して、この無線に対するアドミッション コントロール（ACM）を有効にします。
- **config wlan call-snoop enable** *wlan-id* コマンドを入力して、特定の WLAN に対するコールスヌーピング機能を有効にします。

  優先コールの統計情報を表示するには、**show ap stats** {**802.11**{**a** | **b**} | **wlan**} *cisco_ap* コマンドを入力します。

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、インデックス 2 に、新しい優先コールを追加する例を示します。

```
(Cisco Controller) > config advanced sip-preferred-call-no 2 0123456789
```

関連コマンド

config wlan qos

config 802.11 cac video acm

config 802.11 cac voice acm

config wlan call-snoop

show ap stats

config advanced sip-snooping-ports

コール スヌーピング ポートを設定するには、**config advanced sip-snooping-ports** コマンドを使用します。

config advanced sip-snooping-ports *start_port end_port*

構文の説明

start_port	コール スヌーピング用の開始ポート。範囲は 0 ～ 65535 です。
end_port	コール スヌーピング用の終了ポート。範囲は 0 ～ 65535 です。

使用上のガイドライン

コール スヌーピング用に 1 つのポートしか必要ない場合は、開始ポートと終了ポートを同じ番号に設定します。

CIUS タブレットで使用されるポートは 5060 で、Facetime で使用されるポート範囲は 16384 ～ 16402 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、コール スヌーピング ポートを設定する例を示します。

```
(Cisco Controller) > config advanced sip-snooping-ports 4000 4500
```

関連コマンド

show cac voice stats

show cac voice summary

show cac video stats

show cac video summary

config 802.11 cac video sip

config 802.11 cac voice sip

show advanced sip-preferred-call-no

show advanced sip-snooping-ports

debug cac

config advanced backup-controller primary

プライマリ バックアップ コントローラを設定するには、**config advanced backup-controller primary** コマンドを使用します。

config advanced backup-controller primary *system name IP addr*

構文の説明

system name	プライマリ	セカンダリ バックアップ コントローラを設定します。
ip-addr	バックアップ コントローラの 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。
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

プライマリ バックアップ コントローラ エントリ（IPv6 または IPv4）を削除するには、コントローラの IP アドレスとして 0.0.0.0 と入力します。

次に、IPv4 プライマリ バックアップ コントローラを設定する例を示します。

```
(Cisco Controller) >config advanced backup-controller primary Controller_1 10.10.10.10
```

次に、IPv6 プライマリ バックアップ コントローラを設定する例を示します。

```
(Cisco Controller) >config advanced backup-controller primary systemname 2001:9:6:40::623
```

次に、IPv4 プライマリ バックアップ コントローラを削除する例を示します。

```
(Cisco Controller) >config advanced backup-controller primary Controller_1 10.10.10.10
```

次に、IPv6 プライマリ バックアップ コントローラを削除する例を示します。

```
(Cisco Controller) >config advanced backup-controller primary Controller_1 0.0.0.0
```

関連コマンド

show advanced back-up controller

config advanced backup-controller secondary

セカンダリ バックアップ コントローラを設定するには、**config advanced backup-controller secondary** コマンドを使用します。

config advanced backup-controller secondary *system name IP addr*

構文の説明

system name	プライマリ	セカンダリ バックアップ コントローラを設定します。
ip-addr	バックアップ コントローラの 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。
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。

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。

使用上のガイドライン

セカンダリ バックアップ コントローラ エントリ（IPv4 または IPv6）を削除するには、コントローラの IP アドレスとして 0.0.0.0 と入力します。

次に、IPv4 セカンダリ バックアップ コントローラを設定する例を示します。

```
(Cisco Controller) >config advanced backup-controller secondary Controller_2 10.10.10.10
```

次に、IPv6 セカンダリ バックアップ コントローラを設定する例を示します。

```
(Cisco Controller) >config advanced backup-controller secondary Controller_2
2001:9:6:40::623
```

次に、IPv4 セカンダリ バックアップ コントローラを削除する例を示します。

```
(Cisco Controller) >config advanced backup-controller secondary Controller_2 0.0.0.0
```

次に、IPv6 セカンダリ バックアップ コントローラを削除する例を示します。

```
(Cisco Controller) >config advanced backup-controller secondary Controller_2 0.0.0.0
```

関連コマンド

show advanced back-up controller

config advanced client-handoff

802.11 データ パケットの再試行が指定した回数に達した時点でクライアント ハンドオフが行われるように設定するには、**config advanced client-handoff** コマンドを使用します。

config advanced client-handoff *num_of_retries*

構文の説明

num_of_retries	クライアント ハンドオフが行われる前の再試行数の限度（0 ～ 255）。

コマンド デフォルト

802.11 データ パケットの再試行数の限度のデフォルト値は 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。

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。

使用上のガイドライン

このコマンドは 1000/1510 シリーズ アクセス ポイントでのみサポートされます。

次に、クライアント ハンドオフを再試行数の限度 100 に設定する例を示します。

```
(Cisco Controller) >config advanced client-handoff 100
```

config advanced dot11-padding

Over-the-Air フレーム パディングを有効または無効にするには、**config advanced dot11-padding** コマンドを使用します。

config advanced dot11-padding {**enable** | **disable**}

構文の説明

enable	Over-the-Air フレーム パディングを有効にします。
disable	Over-the-Air フレーム パディングを無効にします。

コマンド デフォルト

Over-the-Air フレーム パディングは、デフォルトでは無効になっています。

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。

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、Over-the-Air フレーム パディングを有効にする例を示します。

```
(Cisco Controller) > config advanced dot11-padding enable
```

関連コマンド

debug dot11

debug dot11 mgmt interface

debug dot11 mgmt msg

debug dot11 mgmt ssid

debug dot11 mgmt state-machine

debug dot11 mgmt station

show advanced dot11-padding

config advanced assoc-limit

アクセス ポイント無線がアソシエーション要求および認証要求をコントローラに送信するレートを設定するには、**config advanced assoc-limit** コマンドを使用します。

config advanced assoc-limit {**enable** [*number of associations per interval* | *interval*] | **disable**}

構文の説明

enable	アクセス ポイントごとのアソシエーション要求の設定を有効にします。
disable	アクセス ポイントごとのアソシエーション要求の設定を無効にします。
number of associations per interval	（任意）指定した間隔での 1 つのアクセス ポイント スロットあたりのアソシエーション要求数。範囲は 1 ～ 100 です。
interval	（任意）アソシエーション要求制限間隔。範囲は 100 ～ 10000 ミリ秒です。

コマンド デフォルト

このコマンドのデフォルト状態は無効です。

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。

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。

使用上のガイドライン

200 以上の無線クライアントが同時にコントローラにアソシエートしようとする際、**config advanced assoc-limit** コマンドを使用してアクセス ポイントからのアソシエーション要求を制限している場合は、クライアントが DHCP_REQD のステータスにとどまることはなくなります。

次に、20 の指定した間隔での 1 つのアクセス ポイント スロットあたりのアソシエーション要求数を 250 のアソシエーション要求制限間隔で設定する例を示します。

```
(Cisco Controller) >config advanced assoc-limit enable 20 250
```

config advanced max-1x-sessions

各アクセス ポイントに許可されている同時802.1Xセッションの最大数を設定するには、**config advanced max-1x-sessions** コマンドを使用します。

config advanced max-1x-sessions *no_of_sessions*

構文の説明

no_of_sessions	一度の AP あたりの 802.1x セッション開始の最大数。範囲は 0～255 で、0 は無制限を示します。

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。

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、同時 802.1X セッションの最大数を設定する例を示します。

```
(Cisco Controller) >config advanced max-1x-sessions 200
```

config advanced rate

スイッチ制御パス レート制限を設定するには、**config advanced rate** コマンドを使用します。

config advanced rate {**enable** | **disable**}

構文の説明

enable	スイッチ制御パス レート制限機能を有効にします。
disable	スイッチ制御パス レート制限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、スイッチ制御パス レート制限を有効にする例を示します。

```
(Cisco Controller) >config advanced rate enable
```

config advanced probe backoff

Cisco AP のプローブ キューのバックオフ パラメータを設定するには、**config advanced probe backoff** コマンドを使用します。

config advanced probe backoff {**enable** | **disable**}

構文の説明

enable	プローブ応答にデフォルトのバックオフ パラメータ値を使用する場合に選択します。
disable	プローブ応答に増加されたバックオフ パラメータを使用する場合に選択します。

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
7.5	このコマンドが導入されました。

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、プローブ応答に増加されたバックオフ パラメータを使用する例を示します。

```
(Cisco Controller) >config advanced probe backoff enable
```

config advanced probe filter

アクセスポイントからコントローラに転送されたプローブ要求のフィルタリングを設定するには、**config advanced probe filter** コマンドを入力します。

config advanced probe filter {**enable** | **disable**}

構文の説明

enable	プローブ要求のフィルタリングを有効にします。
disable	プローブ要求のフィルタリングを無効にします。

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。

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、アクセスポイントからコントローラに転送されたプローブ要求のフィルタリングを有効にする例を示します。

```
(Cisco Controller) >config advanced probe filter enable
```

config advanced probe limit

指定された間隔での、1 つのクライアントおよび 1 つのアクセス ポイントあたりの WLAN コントローラに送信されるプローブ数を制限するには、**config advanced probe limit** コマンドを入力します。

config advanced probe limit *num_probesinterval*

構文の説明

num_probes	指定された間隔での、1 つのアクセス ポイント無線および 1 つのクライアントあたりのプローブ要求数（1 ～ 100）。
interval	プローブ制限間隔（100 ～ 10,000 ミリ秒）。

コマンド デフォルト

プローブ要求のデフォルト数は 2 です。デフォルトの間隔は 500 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。

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、1 つのクライアントおよび 1 つのアクセス ポイントあたりのプローブ数を 5 に、プローブ間隔を 800 ミリ秒に設定する例を示します。

```
(Cisco Controller) >config advanced probe limit 5 800
```

config advanced timers

高度なシステム タイマーを設定するには、**config advanced timers** コマンドを使用します。

config advanced timers {**ap-coverage-report** *seconds* | **ap-discovery-timeout** *discovery-timeout* | **ap-fast-heartbeat** {**local** | **flexconnect** | **all**} {**enable** | **disable**} *fast_heartbeat_seconds* | **ap-heartbeat-timeout** *heartbeat_seconds* | **ap-primary-discovery-timeout** *primary_discovery_timeout* | **ap-primed-join-timeout** *primed_join_timeout* | **auth-timeout** *auth_timeout* | **pkt-fwd-watchdog** {**enable** | **disable**} {*watchdog_timer* | **default**} | **eap-identity-request-delay** *eap_identity_request_delay* | **eap-timeout** *eap_timeout*}

構文の説明

ap-coverage-report	すべての AP の RRM カバレッジ レポート間隔を設定します。
seconds	AP のカバレッジ レポート間隔を秒単位で設定します。範囲は 60 ~ 90 秒です。デフォルトは 90 秒です。
ap-discovery-timeout	Cisco Lightweight アクセス ポイントの検出タイムアウト値を設定します。
discovery-timeout	Cisco Lightweight アクセス ポイントの検出タイムアウト値（秒単位）。値の範囲は 1 ～ 10 です。
ap-fast-heartbeat	アクセス ポイントのコントローラ障害を検出するために要する時間を短縮する高速ハートビート タイマーを設定にします。
local	ローカル モードのアクセス ポイントの高速ハートビート間隔を設定します。
flexconnect	FlexConnect モードのアクセス ポイントの高速ハートビート間隔を設定します。
all	すべてのアクセス ポイントの高速ハートビート間隔を設定します。
enable	ファーストハートビート間隔を有効にします。
disable	ファーストハートビート間隔を無効にします。
fast_heartbeat_seconds	コントローラ障害を検出するために要する時間を短縮する小さい値のハートビート間隔（秒単位）。値の範囲は 1 ～ 10 です。
ap-heartbeat-timeout	Cisco Lightweight アクセス ポイントのハートビート タイムアウト値を設定します。

heartbeat_seconds	Cisco Lightweight アクセス ポイントのハートビート タイムアウト値（秒単位）。値の範囲は 1 ～ 30 です。この値は、高速ハートビート タイマーの 3 倍以上の値である必要があります。
ap-primary-discovery-timeout	アクセス ポイントのプライマリ ディスカバリ要求タイマーを設定します。
primary_discovery_timeout	アクセス ポイントのプライマリ検出要求時間（秒単位）。範囲は 30 ～ 3600 です。
ap-primed-join-timeout	アクセス ポイントのプライミングされた検出タイムアウト値を設定します。
primed_join_timeout	アクセス ポイントのプライミングされた検出タイムアウト値（秒単位）。範囲は 120 ～ 43200 です。
auth-timeout	認証タイムアウトを設定します。
auth_timeout	認証応答タイムアウト値（秒単位）。範囲は 10 ～ 600 です。
pkt-fwd-watchdog	ファストパスのデッドロックから保護するためのパケット転送ウォッチドッグ タイマーを設定します。
watchdog_timer	パケット転送ウォッチドッグ タイマー（秒単位）。範囲は 60 ～ 300 です。
default	ウォッチドッグ タイマーをデフォルト値の 240 秒に設定します。
eap-identity-request-delay	詳細な拡張可能認証プロトコル（EAP）アイデンティティ要求遅延を秒単位で設定します。
eap_identity_request_delay	詳細な EAP アイデンティティ要求遅延（秒単位）。範囲は 0 ～ 10 です。
eap-timeout	EAP 有効期限タイムアウトを設定します。
eap_timeout	EAP タイムアウト値（秒単位）。範囲は 8 ～ 120 です。

コマンド デフォルト

- デフォルトのアクセス ポイント検出タイムアウトは 10 秒です。
- デフォルトのアクセス ポイント ハートビート タイムアウトは 30 秒です。

- デフォルトのアクセス ポイント プライマリ検出要求タイマーは 120 秒です。
- デフォルトの認証タイムアウトは 10 秒です。
- デフォルトのパケット転送ウォッチドッグ タイマーは 240 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。
8.3	コマンドの機能が拡張されました。
8.6	このコマンドはリリース8.6で新しいキーワードによって機能が拡張されました。追加された新しいキーワードは **ap-coverage-report** です。

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。

使用上のガイドライン

Cisco Lightweight アクセス ポイントの検出タイムアウトとは、Cisco WLC が、接続されていない Cisco Lightweight アクセス ポイントの検出を試行する頻度です。

Cisco Lightweight アクセス ポイントのハートビート タイムアウトは、Cisco Lightweight アクセス ポイントが Cisco Wireless LAN Controller にハートビート キープアライブ信号を送信する頻度を制御します。

次に、タイムアウト値を 20 でアクセス ポイント検出タイムアウトを設定する例を示します。

```
(Cisco Controller) >config advanced timers ap-discovery-timeout 20
```

次に、FlexConnectモードのアクセス ポイントを対象に高速ハートビート間隔を有効にする例を示します。

```
(Cisco Controller) >config advanced timers ap-fast-heartbeat flexconnect enable 8
```

次に、認証タイムアウトを 20 秒に設定する例を示します。

```
(Cisco Controller) >config advanced timers auth-timeout 20
```

config ap 802.1Xuser

コントローラに現在関連付けられているアクセスポイント、および今後関連付けられるすべてのアクセスポイントについて、グローバル認証のユーザ名とパスワードを設定するには、**config ap 802.1Xuser** コマンドを使用します。

config ap 802.1Xuser add username *ap-username* **password** *ap-password* {**all** | *cisco_ap*}

構文の説明

add username	ユーザ名を追加することを指定します。
ap-username	Cisco AP でのユーザ名。
password	パスワードを追加することを指定します。
ap-password	パスワード。
cisco_ap	特定のアクセス 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

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

強度が高いパスワードを入力する必要があります。強度が高いパスワードの特徴は次のとおりです。

- 少なくとも 8 文字の長さである。
- 小文字と大文字、数字、および記号の組み合わせを含む。
- どの言語の単語でもない。

特定のアクセス ポイントの値を設定できます。

次に、すべてのアクセスポイントにグローバル認証ユーザ名およびパスワードを設定する例を示します。

```
(Cisco Controller) >config ap 802.1Xuser add username cisco123 password cisco2020 all
```

config ap 802.1Xuser delete

特定のアクセス ポイントがコントローラのグローバル認証設定を使用するように強制するには、**config ap 802.1Xuser delete** コマンドを使用します。

config ap 802.1Xuser delete *cisco_ap*

構文の説明

cisco_ap	アクセス ポイント。

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、コントローラのグローバル認証設定を使用するアクセス ポイント AP01 を削除する例を示します。

```
(Cisco Controller) >config ap 802.1Xuser delete AP01
```

config ap 802.1Xuser disable

すべてのアクセス ポイントまたは特定のアクセス ポイントの認証を無効にするには、**config ap 802.1Xuser disable** コマンドを使用します。

config ap 802.1Xuser disable {**all** | *cisco_ap* }

構文の説明

disable	認証を無効にします。
all	すべてのアクセス ポイントを指定します。
cisco_ap	アクセス ポイント。

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

特定のアクセス ポイントの 802.1X 認証は、グローバル 802.1X 認証が有効でない場合にだけ無効にできます。グローバル 802.1X 認証が有効な場合は、すべてのアクセス ポイントに対してだけ 802.1X を無効にできます。

次に、アクセス ポイント cisco_ap1 の認証を無効にする例を示します。

```
(Cisco Controller) >config ap 802.1Xuser disable
```

config advanced dot11-padding

Over-the-Air フレーム パディングを有効または無効にするには、**config advanced dot11-padding** コマンドを使用します。

config advanced dot11-padding {**enable** | **disable**}

構文の説明

enable	Over-the-Air フレーム パディングを有効にします。
disable	Over-the-Air フレーム パディングを無効にします。

コマンド デフォルト

Over-the-Air フレーム パディングは、デフォルトでは無効になっています。

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。

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、Over-the-Air フレーム パディングを有効にする例を示します。

```
(Cisco Controller) > config advanced dot11-padding enable
```

関連コマンド

debug dot11

debug dot11 mgmt interface

debug dot11 mgmt msg

debug dot11 mgmt ssid

debug dot11 mgmt state-machine

debug dot11 mgmt station

show advanced dot11-padding

config ap

Cisco Lightweight アクセス ポイントを設定する、またはサードパーティ（外部）アクセス ポイントを追加または削除するには、**config ap** コマンドを使用します。

config ap {{**enable** | **disable**} *cisco_ap* | {**add** | **delete**} *MAC port* {**enable** | **disable**} *IP_address*}

構文の説明

enable	Cisco Lightweight アクセス ポイントを有効にします。
disable	Cisco Lightweight アクセス ポイントを無効にします。
cisco_ap	Cisco Lightweight アクセス ポイントの名前。
add	外部アクセス ポイントを追加します。
delete	外部アクセス ポイントを削除します。
MAC	外部アクセス ポイントの MAC アドレス。
port	外部アクセス ポイントに到達できるポート番号。
IP_address	外部アクセス ポイントの 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。
8.0	このコマンドは、IPv4 と IPv6 の両方をサポートします。

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、Lightweight アクセス ポイント AP1 を無効にする例を示します。

```
(Cisco Controller) >config ap disable AP1
```

次に、MAC アドレスが 12:12:12:12:12:12、IP アドレスが 192.12.12.1 の外部アクセス ポイントをポート 2033 から追加する例を示します。

```
(Cisco Controller) >config ap add 12:12:12:12:12:12 2033 enable 192.12.12.1
```

config ap aid-audit

Cisco Lightweight アクセス ポイントの AID 監査メカニズムを設定するには、**config ap aid-audit** コマンドを使用します。

config ap aid-audit {**enable** | **disable**}

構文の説明

aid-audit	AID 監査メカニズムを設定します。
enable	AID 監査メカニズムを有効にします。
disable	AID 監査メカニズムを無効にします。

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
8.6	このコマンドが導入されました。

次に、AP で AID 監査を有効にする例を示します。

```
(Cisco Controller) >config ap aid-audit enable
```

config ap antenna band-mode

Cisco AP のアンテナのバンド モードをシングルまたはデュアルとして設定するには、**config ap antenna band-mode** コマンドを使用します。

config ap antenna band-mode {**single** | **dual**} *cisco-ap*

構文の説明

single	Cisco AP のシングル バンド アンテナ モードを設定します。
dual	Cisco AP のデュアル バンド アンテナ モードを設定します。
cisco-ap	Cisco AP 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	このコマンドが導入されました。
8.3 以降のリリース	**antenna-band-mode** パラメータが **antenna band-mode** に変更されました。

config ap atf 802.11

config ap atf 802.11 コマンドを使用することにより、AP レベルで Cisco Air Time Fairness を設定します。

config ap atf 802.11{**a** | **b**} {**mode** {**disable** | **monitor** | **enforce-policy**} *ap-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。
ap-name	指定する必要がある AP 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 AP（*my-ap*）の通信時間の最適化を有効にするには、次のコマンドを入力します。

```
(Cisco Controller) >config ap atf 802.11a optimization enable my-ap
```

config ap atf 802.11 client-access airtime-allocation

メッシュ AP で ATF 通信時間割り当てのオーバーライドを設定するには、**config ap atf 802.11 client-access airtime-allocation override** {**enable** | **disable**} コマンドを使用します。

config ap atf 802.11{**a** | **b**} **client-access airtime-allocation** *%-of-airtime-allocation-bw-5-to-90 mesh-ap-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/g ネットワーク設定を指定します。
%-of-airtime-allocation-bw-5-to-90	クライアント アクセスの通信時間割り当てのパーセンテージ。有効な範囲は5～90です。この通信時間割り当てのパーセンテージは、クライアントとアップリンクの両方のバックホール パーセンテージに影響します。
mesh-ap-name	メッシュ AP の名前。
override	メッシュ AP での ATF 通信時間割り当てのオーバーライドを可能にします。
enable	通信時間割り当てのオーバーライドを有効にします。
disable	通信時間割り当ての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
8.4	このコマンドが追加されました。

802.11a ネットワークで、メッシュ AP（*map1*）での ATF 通信時間割り当てのオーバーライドを設定するには、次のコマンドを入力します。

```
(Cisco Controller) >config ap atf 802.11a client-access airtime-allocation
10 override map1 enable
```

config ap 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、次のコマンドを入力します。

confit ap atf 802.11{**a** | **b**} **policy** *wlan-id policy-name ap-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。
wlan-id	指定する必要がある WLAN ID またはリモート LAN ID。
policy-name	指定する必要がある Cisco ATF ポリシー名。
ap-name	指定する必要がある AP 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 ap autoconvert

Cisco WLC と関連付けるときに、すべてのアクセス ポイントを FlexConnect モードまたは Monitor モードに自動的に変換するには、**config ap autoconvert** コマンドを使用します。

config ap autoconvert {**flexconnect** | **monitor** | **disable**}

構文の説明

flexconnect	FlexConnect モードへのすべてのアクセス ポイントが自動的に設定されます。
monitor	モニタ モードへのすべてのアクセス ポイントが自動的に設定されます。
disable	アクセス ポイントに対する autoconvert 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

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

ローカル モードのアクセス ポイントが Cisco 7500 シリーズ ワイヤレス コントローラに接続している場合、そのアクセス ポイントはクライアントにサービスを提供しません。アクセス ポイントの詳細はコントローラで使用できます。アクセス ポイントが Cisco 7500 シリーズ ワイヤレス コントローラに接続しているときに、クライアントにサービスを提供できる、またはモニタ関連のタスクを実行できるようにするには、アクセス ポイントのモードを FlexConnect モードまたは Monitor モードにします。

このコマンドは、Cisco 5520、8540、および 8510 シリーズ ワイヤレス コントローラ プラットフォームでの AP モードの変換にも使用できます。

次に、すべてのアクセス ポイントを FlexConnect モードに自動的に変換する例を示します。

```
(Cisco Controller) >config ap autoconvert flexconnect
```

次に、AP の自動変換オプションを無効にする例を示します。

```
(Cisco Controller) >config ap autoconvert disable
```

config ap bhrate

Cisco Bridge Backhaul Tx Rate を設定するには、**config ap bhrate** コマンドを使用します。

config ap bhrate {*rate* | **auto**} *cisco_ap*

構文の説明

rate	Cisco Bridge Backhaul Tx Rate（Kbps）。有効な値は、6000、12000、18000、24000、36000、48000、および 54000 です。
auto	自動データ レートを設定します。
cisco_ap	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

コマンドのデフォルトのステータスは auto に設定されています。

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。

使用上のガイドライン

以前のソフトウェア リリースでは、ブリッジデータ レートのデフォルト値は24000（24 Mbps）でした。コントローラ ソフトウェアのリリース 6.0 では、ブリッジ データ レートのデフォルト値は **auto** です。以前のコントローラ ソフトウェアのリリースでデフォルトのブリッジ データ レート値（24000）を設定した場合は、コントローラ ソフトウェア リリース 6.0 にアップグレードしたときにブリッジデータ レートが新しいデフォルト値（auto）で設定されます。ただし、以前のコントローラ ソフトウェアのリリースでデフォルト値以外の値（たとえば、18000）を設定した場合は、Cisco WLC リリース 6.0 にアップグレードしたときにその設定が保持されます。

ブリッジデータ レートが **auto** に設定されている場合、メッシュ バックホールは最大レートを選択します。次に大きいレートは、（すべてのレートではなく）その特定のレートが不適切な状況にあるため、使用できません。

次に、Cisco Bridge Backhaul Tx Rate を 54000 kbps に設定する例を示します。

```
(Cisco Controller) >config ap bhrate 54000 AP01
```

config ap bridgegroupname

Cisco Lightweight アクセス ポイントでブリッジ グループ名を設定または削除するには、**config ap bridgegroupname** コマンドを使用します。

config ap bridgegroupname {**set** *groupname* | **delete** | {**strict-matching** {**enable** | **disable**}}}*cisco_ap*

構文の説明

set	Cisco Lightweight アクセス ポイントのブリッジ グループ名を設定します。
groupname	ブリッジ グループ名
delete	Cisco Lightweight アクセス ポイントのブリッジ グループ名を削除します。
cisco_ap	Cisco Lightweight アクセス ポイントの名前。
strict-matching	MAP にデフォルト以外のブリッジ グループ名が設定されており、潜在的な親に異なるブリッジ グループ名が設定されている場合、可能な親のリストを制限します。
enable	Cisco Lightweight アクセス ポイントのグループ名を有効にします。
disable	Cisco Lightweight アクセス ポイントのグループ名を無効にします。

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	**strict-matching** パラメータが追加されました。

使用上のガイドライン

同じブリッジ グループ名を持つアクセス ポイントだけが相互に接続できます。AP ブリッジ グループ名を変更すると、ブリッジ AP が残る場合があります。

次に、Cisco アクセス ポイントのブリッジ グループ名 AP02 でブリッジ グループ名を削除する例を示します。

```
(Cisco Controller) >config ap bridgegroupname delete AP02
Changing the AP's bridgegroupname may strand the bridge AP. Please continue with caution.
Changing the AP's bridgegroupname will also cause the AP to reboot.
Are you sure you want to continue? (y/n)
```

config ap bridging

Cisco Lightweight アクセス ポイントでのイーサネット間ブリッジングを設定するには、**config ap bridging** コマンドを使用します。

config ap bridging {**enable** | **disable**} *cisco_ap*

構文の説明

enable	Cisco Lightweight アクセス ポイントでのイーサネット間ブリッジングを有効にします。
disable	イーサネット間ブリッジングを無効にします。
cisco_ap	Cisco Lightweight 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 ポイントでブリッジングを有効にする例を示します。

```
(Cisco Controller) >config ap bridging enable nyc04-44-1240
```

次に、アクセス ポイントでブリッジングを無効にする例を示します。

```
(Cisco Controller) >config ap bridging disable nyc04-44-1240
```

config ap cdp

Cisco Lightweight アクセス ポイントで Cisco Discovery Protocol（CDP）を設定するには、**config ap cdp** コマンドを使用します。

config ap cdp {**enable** | **disable** | **interface** {**ethernet** *interface_number* | **slot** *slot_id*}} {*cisco_ap* | **all**}

構文の説明

enable	アクセス ポイントで CDP を有効にします。
disable	アクセス ポイントで CDP を無効にします。
interface	特定のインターフェイスの CDP を設定します。
ethernet	イーサネットインターフェイスの CDP を設定します。
interface_number	0～3 のイーサネットインターフェイス番号。
slot	無線インターフェイスの CDP を設定します。
slot_id	0～3 のスロット番号。
cisco_ap	Cisco Lightweight アクセス ポイントの名前。
all	すべてのアクセス ポイントを指定します。

（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。

コマンド デフォルト

メッシュ AP の無線インターフェイスで有効になっていて、非メッシュ AP の無線インターフェイスで無効になっています。すべての AP のイーサネットインターフェイスで有効になっています。

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。

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。

使用上のガイドライン

config ap cdp disable all コマンドは、コントローラに join しているすべてのアクセス ポイントおよび今後 join するすべてのアクセス ポイントの CDP を無効にします。CDP は、コントローラまたはアクセス ポイントのリブート後も現在と将来のアクセス ポイントで無効のままになります。CDP を有効にするには、**config ap cdp enable all** コマンドを入力します。

（注） イーサネット/無線インターフェイス上の CDP は、CDP が有効になっている場合にだけ使用できます。コントローラに join しているすべてのアクセス ポイントで CDP を有効にした後、**config ap cdp** {**enable** | **disable**} *cisco_ap* コマンドを使用して個々のアクセス ポイントで CDP を無効にした後再び有効にできます。コントローラに join されたすべてのアクセス ポイントで CDP を無効にした後は、個々のアクセス ポイントで CDP を有効にし、無効にすることはできません。

次に、すべてのアクセス ポイントで CDP を有効にする例を示します。

```
(Cisco Controller) >config ap cdp enable all
```

次に ap02 アクセス ポイントで CDP を無効にする例を示します。

```
(Cisco Controller) >config ap cdp disable ap02
```

次に、すべてのアクセス ポイントでイーサネット インターフェイス番号 2 の CDP を有効にする例を示します。

```
(Cisco Controller) >config ap cdp ethernet 2 enable all
```

config ap cert-expiry-ignore

デバイス証明書日付検証チェックを設定するには、**config ap cert-expiry-ignore** コマンドを使用します。

config ap cert-expiry-ignore {**mic | ssc** {**enable** | **disable** }

構文の説明

cert-expiry-ignore	証明書失効無視チェック動作を設定します。
mic	MIC の証明書失効無視チェック動作を設定します。
ssc	SSC の証明書失効無視チェック動作を設定します。
enable	有効化すると、ライフタイムチェックが無視されます。
disable	無効にすると、ライフタイムチェックが実行されます。

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。
8.7	コマンドの機能が拡張され、Cisco WLC の証明書日付検証チェックが組み込まれました。

次に、MIC での証明書ライフタイム チェックを無視する例を示します。

```
(Cisco Controller) >config ap cert-expiry-ignore mic enable
```

config ap core-dump

Cisco Lightweight アクセス ポイントのメモリ コア ダンプを設定するには、**config ap core-dump** コマンドを使用します。

config ap core-dump {**disable** | **enable** *tftp_server_ipaddress filename* {**compress** | **uncompress**} {*cisco_ap* | **all**}

構文の説明

enable	Cisco Lightweight アクセス ポイントのメモリ コア ダンプ設定を有効にします。
disable	Cisco Lightweight アクセス ポイントのメモリ コア ダンプ設定を無効にします。
tftp_server_ipaddress	アクセス ポイントがコア ダンプ ファイルを送信する Trivial File Transfer Protocol（TFTP）サーバの IP アドレス。
filename	コア ファイルのラベルを付けるためにアクセス ポイントが使用する名前。
compress	コア ダンプ ファイルを圧縮します。
uncompress	コア ダンプ ファイルを圧縮解除します。
cisco_ap	Cisco Lightweight アクセス ポイントの名前。
all	すべてのアクセス ポイントを指定します。

（注） AP 自体が「all」という名前で設定されている場合、「all access points」の場合は「all」という名前の AP に優先します。

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 の両方をサポートします。

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。

使用上のガイドライン

アクセス ポイントはTFTPサーバに到達できる必要があります。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。

次に、コア ダンプ ファイルを設定して圧縮する例を示します。

```
(Cisco Controller) >config ap core-dump enable 209.165.200.225 log compress AP02
```

config ap crash-file clear-all

すべてのクラッシュおよび無線コア ダンプ ファイルを削除するには、**config ap crash-file clear-all** コマンドを使用します。

config ap crash-file clear-all

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。

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、すべてのクラッシュ ファイルを削除する例を示します。

```
(Cisco Controller) >config ap crash-file clear-all
```

config ap crash-file delete

単一のクラッシュまたは無線コア ダンプ ファイルを削除するには、**config ap crash-file delete** コマンドを使用します。

config ap crash-file delete *filename*

構文の説明

filename	削除するファイル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。

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、クラッシュ ファイル 1 を削除する例を示します。

```
(Cisco Controller) >config ap crash-file delete crash_file_1
```

config ap crash-file get-crash-file

Cisco Lightweight アクセス ポイントの最新のクラッシュ データを収集するには、**config ap crash-file get-crash-file** コマンドを使用します。

config ap crash-file get-crash-file *cisco_ap*

構文の説明

cisco_ap	Cisco Lightweight 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。

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。

使用上のガイドライン

transfer upload datatype コマンドを使用して、Cisco Wireless LAN Controller に収集されたデータを転送します。

次に、アクセス ポイント A3 の最新のクラッシュ データを収集する例を示します。

```
(Cisco Controller) >config ap crash-file get-crash-file AP3
```

config ap crash-file get-radio-core-dump

Cisco Lightweight アクセス ポイントの無線コア ダンプを取得するには、**config ap crash-file get-radio-core-dump** コマンドを使用します。

config ap crash-file get-radio-core-dump *slot_id cisco_ap*

構文の説明

slot_id	スロット ID（0 または 1）。
cisco_ap	Cisco Lightweight 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。

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、アクセス ポイント AP02 とスロット 0 の無線コア ダンプを収集する例を示します。

```
(Cisco Controller) >config ap crash-file get-radio-core-dump 0 AP02
```

config ap dhcp release-override

Cisco AP で DHCP リリース オーバーライドを設定するには、**config ap dhcp release-override** コマンドを使用します。

config ap dhcp release-override {**enable** | **disable**} {*cisco-ap-name* | **all**}

構文の説明

enable	DHCP リリース オーバーライドを有効にして、AP によって送信される DHCP リリースの数を 1 に設定します。AP の IP アドレスを不良としてマークする少数の DHCP サーバに関する回避策として使用されます。この設定は、信頼性の高いネットワークでのみ使用することをお勧めします。
disable	DHCP リリース オーバーライドを無効にして、AP によって送信される DHCP リリースの数を 3（デフォルト値）に設定します。これにより、いずれかのパケットが失われた場合でも、DHCP サーバはリリース メッセージを受信します。
cisco-ap-name	ユーザが入力する Cisco AP に適用される設定。
all	すべての Cisco AP に適用される設定。

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
8.2	このコマンドが導入されました。

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。

使用上のガイドライン

Windows Server 2008 R2 または 2012 を搭載した Cisco Lightweight AP を DHCP サーバとしてを使用している場合は、このコマンドを使用してください。

config ap dtls-cipher-suite

AP とコントローラの間の DTLS 接続用の新しい暗号スイートを有効にするには、**config ap dtls-cipher-suite** コマンドを使用します。

config ap dtls-cipher-suite {**RSA-AES256-SHA256** | **RSA-AES256-SHA** | **RSA-AES128-SHA**}

構文の説明

RSA-AES256-SHA256	RSA キー交換または認証を使用する暗号スイート（256 ビット AES と SHA 256 を使用）。
RSA-AES256-SHA	RSA キー交換または認証を使用する暗号スイート（256 ビット AES と SHA を使用）。
RSA-AES128-SHA	RSA キー交換または認証を使用する暗号スイート（128 ビット AES と SHA を使用）。

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、AP とコントローラの間の DTLS 接続に 256 ビット AES と SHA 256 を使用する RSA 暗号スイートを有効にする例を示します。

```
(Cisco Controller) > config ap dtls-cipher-suite RSA-AES256-SHA256
```

config ap dtls-version

暗号 DTLS バージョンを設定するには、**config ap dtls-version** コマンドを使用します。

config ap dtls-version {**dtls1.0 | dtls1.2 | dtls_all**}

構文の説明

dtls1.0	DTLS 1.0 バージョンを選択します。
dtls1.2	DTLS 1.2 バージョンを選択します。
dtls_all	後方互換性のためにすべての DTLS バージョンを選択します。

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
8.3.111.0	このコマンドが導入されました。

次に、暗号 DTLS バージョン 1.2 を設定する例を示します。

```
(Cisco Controller) > config ap dtls-version dtls1.2
```

config ap ethernet duplex

Lightweight アクセス ポイントのイーサネット ポート デュプレックスおよび速度を設定するには、**config ap ethernet duplex** コマンドを使用します。

config ap ethernet duplex［**auto** | **half** | **full**］ **speed**［**auto** | **10** | **100** | **1000**］｛ **all** | *cisco_ap* ｝

構文の説明

auto	（任意）イーサネット ポートの自動二重設定を指定します。
half	（任意）イーサネット ポートの半二重設定を指定します。
full	（任意）イーサネット ポートの全二重設定を指定します。
speed	イーサネットポート速度の設定を指定します。
auto	（任意）イーサネット ポート速度を自動に指定します。
10	（任意）イーサネット ポート速度を 10 Mbps に指定します。
100	（任意）イーサネット ポート速度を 100 Mbps に指定します。
1000	（任意）イーサネット ポート速度を 1000 Mbps に指定します。
all	接続されているすべてのアクセス ポイントにイーサネット ポートの設定を指定します。
cisco_ap	シスコ アクセス ポイント。

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、すべてのアクセス ポイントで 10 Mbps としてイーサネット ポートの半二重を設定する例を示します。

```
(Cisco Controller) >config ap ethernet duplex half speed 10 all
```

config ap ethernet tag

Control and Provisioning of Wireless Access Points（CAPWAP）パケットの VLAN タギングを設定するには、**config ap ethernet tag** コマンドを使用します。

config ap ethernet tag {**id** *vlan_id* | **disable**} {*cisco_ap* | **all**}

構文の説明

id	VLAN ID を指定します。
vlan_id	トランク VLAN の ID。
disable	VLAN タグ機能を無効にします。VLAN タグ機能を無効にすると、アクセス ポイントは CAPWAP パケットのタグ付けを解除します。
cisco_ap	Cisco AP の名前。
all	すべての Cisco アクセス ポイントに VLAN タギングを設定します。

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。

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。

使用上のガイドライン

VLAN タギングを設定すると、その設定はアクセス ポイントがリブートした後で有効になります。

メッシュ アクセス ポイントには VLAN タギングを設定できません。

アクセス ポイントが指定したトランク VLAN を使用してトラフィックをルーティングできないか、コントローラに到達できない場合は、タグなし設定にフォールバックします。アクセス ポイントがこのフォール バック設定を使用してコントローラに接続すると、コントローラは Cisco Prime Infrastructure などのトラップ サーバにトランク VLAN の障害を示すトラップを送信します。このシナリオでは、show コマンドの出力に「Failover to untagged」というメッセージが表示されます。

次に、トランク VLAN に VLAN タギングを設定する例を示します。

```
(Cisco Controller) >config ap ethernet tag 6 AP1
```

config ap autoconvert

Cisco WLC と関連付けるときに、すべてのアクセス ポイントを FlexConnect モードまたは Monitor モードに自動的に変換するには、**config ap autoconvert** コマンドを使用します。

config ap autoconvert {**flexconnect** | **monitor** | **disable**}

構文の説明

flexconnect	FlexConnect モードへのすべてのアクセス ポイントが自動的に設定されます。
monitor	モニタ モードへのすべてのアクセス ポイントが自動的に設定されます。
disable	アクセス ポイントに対する autoconvert 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

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

ローカル モードのアクセス ポイントが Cisco 7500 シリーズ ワイヤレス コントローラに接続している場合、そのアクセス ポイントはクライアントにサービスを提供しません。アクセス ポイントの詳細はコントローラで使用できます。アクセス ポイントが Cisco 7500 シリーズ ワイヤレス コントローラに接続しているときに、クライアントにサービスを提供できる、またはモニタ関連のタスクを実行できるようにするには、アクセス ポイントのモードを FlexConnect モードまたは Monitor モードにします。

このコマンドは、Cisco 5520、8540、および 8510 シリーズ ワイヤレス コントローラ プラットフォームでの AP モードの変換にも使用できます。

次に、すべてのアクセス ポイントを FlexConnect モードに自動的に変換する例を示します。

```
(Cisco Controller) >config ap autoconvert flexconnect
```

次に、AP の自動変換オプションを無効にする例を示します。

```
(Cisco Controller) >config ap autoconvert disable
```

config ap flexconnect bridge

Flex＋ブリッジアクセス ポイントでFlexConnectブリッジバックホールを設定するには、**config ap flexconnect bridge** コマンドを使用します。

config ap flexconnect bridge {**backhaul-wlan** | **resilient**} *cisco_ap* {**enable** | **disable**}

構文の説明

backhaul-wlan	FlexConnect AP でバックホール WLAN を有効にします。
resilient	Flex＋ブリッジ AP でスタンドアロン モードを有効にします。
cisco_ap	アクセス ポイントの名前。
enable	アクセス ポイントで選択されたモードを有効にします。
disable	アクセス ポイントで選択されたモードを無効にします。

コマンド デフォルト

Flex＋ブリッジ AP でデフォルトの高復元力モードが有効になっています。

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、AP で高復元力モードを有効にする例を示します。

```
(Cisco Controller) >config ap flexconnect bridge resilient AP2 enable
```

config ap flexconnect central-dhcp

WLAN の FlexConnect アクセス ポイントで中央 DHCP を有効にするには、**config ap flexconnect central-dhcp** コマンドを使用します。

config ap flexconnect central-dhcp *wlan_id cisco_ap* ［**add** | **delete**］｛**enable** | **disable**｝ **override dns**｛**enable** | **disable**｝ **nat-pat**｛**enable** | **disable**｝

構文の説明

wlan_id	1 ～ 512 の無線 LAN 識別子。
cisco_ap	Cisco Lightweight アクセス ポイントの名前。
add	（任意）新しい WLAN DHCP マッピングを追加します。
delete	（任意）WLAN DHCP マッピングを削除します。
enable	FlexConnect アクセス ポイントで中央 DHCP を有効にします。この機能を有効にすると、アクセス ポイントから受信した DHCP パケットは、コントローラに中央でスイッチされ、次に AP と SSID に基づいて対応する VLAN に転送されます。
disable	FlexConnect アクセス ポイントで中央 DHCP を無効にします。
override dns	コントローラによって割り当てられたインターフェイス上の DNS サーバ アドレスを上書きします。中央でスイッチされる WLAN で DNS を上書きすると、クライアントは、コントローラからではなく AP から DNS サーバの IP アドレスを取得します。
enable	FlexConnect アクセス ポイントのオーバーライド DNS 機能を有効にします。
disable	FlexConnect アクセス ポイントのオーバーライド DNS 機能を無効にします。
nat-pat	有効または無効に設定できるネットワーク アドレス変換（NAT）およびポート アドレス変換（PAT）。
enable	FlexConnect アクセス ポイントで NAT-PAT を有効にします。
disable	FlexConnect アクセス ポイントで NAT-PAT 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、中央 DHCP、オーバーライド DNS、および FlexConnect アクセス ポイントの NAT-PAT を有効にする例を示します。

```
(Cisco Controller) >config ap flexconnect central-dhcp 1 ap1250 enable override dns
enable nat-pat enable
```

config ap flexconnect local-split

FlexConnect アクセス ポイントのローカル スプリット トンネルを設定するには、 **config ap flexconnect local-split** コマンドを使用します。

config ap flexconnect local-split *wlan_id cisco_ap* {**enable** | **disable**} **acl** *acl_name*

構文の説明

wlan_id	1 ～ 512 の無線 LAN 識別子。
cisco_ap	FlexConnect アクセス ポイントの名前。
enable	FlexConnect アクセス ポイントでローカル スプリット トンネルを有効にします。
disable	FlexConnect アクセス ポイントでローカル スプリット トンネルを無効にします。
acl	FlexConnect のローカル スプリット アクセス コントロール リストを設定します。
acl_name	FlexConnect のアクセス コントロール リストの名前。

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。

使用上のガイドライン

このコマンドを使用すると、FlexConnect ACL を使用して、中央でスイッチされる WLAN にローカル スプリット トンネルを設定することができます。NAT/PAT はマルチキャスト IP トラフィックをサポートしないため、ローカル スプリット トンネルがサポートするのはユニキャスト レイヤ 4 IP トラフィックのみです。

次に、FlexConnect ACL を使用してローカル スプリット トンネルを設定する例を示します。

```
(Cisco Controller) >config ap flexconnect local-split 6 AP2 enable acl flex6
```

config ap flexconnect module-vlan

FlexConnect ローカル スイッチングにおける Cisco USC 8x18 デュアル モード モジュール用の VLAN タギングを設定するには、**config ap flexconnect module-vlan** コマンドを使用します。

config ap flexconnect module-vlan {{**enable** *ap-name* [**vlan** *vlan-id*]} | {{**disable** | **remove**} *ap-name*}}

構文の説明

enable *ap-name*	指定された Cisco AP の外部モジュールに対し、ネイティブ VLAN を使用して FlexConnect ローカル スイッチングを有効にします。
enable *ap-name* **vlan** *vlan-id*	指定された Cisco AP の外部モジュールに対し、非ネイティブ VLAN を使用して FlexConnect ローカル スイッチングを有効にします。
disable *ap-name*	指定された Cisco AP の外部モジュールに対して FlexConnect ローカル スイッチングを無効にします。
remove *ap-name*	AP 固有の外部モジュール VLAN 設定を削除します。

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
8.1	このコマンドが導入されました。

次に、Cisco AP の外部モジュールに対し、非ネイティブ VLAN を使用して FlexConnect ローカル スイッチングを有効にする例を示します。

```
(Cisco Controller) >config ap flexconnect module-vlan enable 3600i-ap vlan4
```

config ap flexconnect policy

FlexConnect アクセス ポイントのポリシー ACL を設定するには、**config ap flexconnect policy** コマンドを使用します。

config ap flexconnect policy {**add** | **delete**} *acl_name*

構文の説明

add	FlexConnect アクセス ポイントのポリシー ACL を追加します。
deletes	FlexConnect アクセス ポイントのポリシー ACL を削除します。
acl_name	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
7.5	このコマンドが導入されました。

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、FlexConnect アクセス ポイントのポリシー ACL を追加する例を示します。

```
(Cisco Controller) >config ap flexconnect policy add acl1
```

config ap flexconnect radius auth set

特定の FlexConnect アクセス ポイントのプライマリまたはセカンダリ RADIUS サーバを設定するには、**config ap flexconnect radius auth set** コマンドを使用します。

config ap flexconnect radius auth set {**primary** | **secondary**} *ip_address auth_port secret*

構文の説明

primary	特定の FlexConnect アクセス ポイントのプライマリ RADIUS サーバを指定します。
secondary	特定の FlexConnect アクセス ポイントのセカンダリ RADIUS サーバを指定します。
ip_address	RADIUS サーバの IP アドレス。
auth_port secret	ポート名
secret	RADIUS サーバのシークレット

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、特定のアクセス ポイントのプライマリ RADIUS サーバを設定する例を示します。

```
(Cisco Controller) >config ap flexconnect radius auth set primary 192.12.12.1
```

config ap flexconnect vlan

FlexConnect アクセスの VLAN タギングを有効または無効にするには、**config ap flexconnect vlan** コマンドを使用します。

config ap flexconnect vlan {**enable** | **disable**} *cisco_ap*

構文の説明

enable	アクセス ポイントの VLAN タギングを有効にします。
disable	アクセス ポイントの VLAN タギングを無効にします。
cisco_ap	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

ディセーブルローカル スイッチに対していったん有効化された WLAN は、Cisco WLC で割り当てられた VLAN を継承します。

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。

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、FlexConnect アクセスのアクセス ポイントの VLAN タギングを有効にする例を示します。

```
(Cisco Controller) >config ap flexconnect vlan enable AP02
```

config ap flexconnect vlan add

FlexConnect アクセス ポイントに VLAN を追加するには、**config ap flexconnect vlan add** コマンドを使用します。

config ap flexconnect vlan add *vlan-id acl in-acl out-acl cisco_ap*

構文の説明

vlan-id	VLAN 識別番号。
acl	最大 32 文字の英数字による ACL 名。
in-acl	最大 32 文字の英数字による着信 ACL 名。
out-acl	最大 32 文字の英数字による発信 ACL 名。
cisco_ap	Cisco Lightweight 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。

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、FlexConnect アクセス ポイントを設定する例を示します。

```
(Cisco Controller) >config ap flexconnect vlan add 21 acl inacl1 outacl1 ap1
```

config ap flexconnect vlan native

FlexConnect アクセス ポイントのネイティブ VLAN を設定するには、**config ap flexconnect vlan native** コマンドを使用します。

config ap flexconnect vlan native *vlan-id cisco_ap*

構文の説明

vlan-id	VLAN 識別番号。
cisco_ap	Cisco Lightweight 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。

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、FlexConnect アクセス ポイント モードにネイティブ VLAN を設定する例を示します。

```
(Cisco Controller) >config ap flexconnect vlan native 6 AP02
```

config ap flexconnect vlan wlan

FlexConnect アクセス ポイントに VLAN ID を割り当てるには、**config ap flexconnect vlan wlan** コマンドを使用します。

config ap flexconnect vlan wlan *wlan-id vlan-id cisco_ap*

構文の説明

wlan-id	WLAN 識別子。
vlan-id	VLAN 識別子（1 ～ 4094）。
cisco_ap	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

WLAN にアソシエートされている VLAN ID。

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。

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、FlexConnect アクセス ポイントに VLAN ID を割り当てる例を示します。

```
(Cisco Controller) >config ap flexconnect vlan wlan 192.12.12.1 6 AP02
```

config ap flexconnect web-auth

ローカルでスイッチされる WLAN に外部 Web 認証用 FlexConnect ACL を設定するには、**config ap flexconnect web-auth** コマンドを使用します。

config ap flexconnect web-auth wlan *wlan_id cisco_ap acl_name* { **enable** | **disable** }

構文の説明

wlan	FlexConnect ACL を設定する無線 LAN を指定します。
wlan_id	1 ～ 512 の無線 LAN 識別子。
cisco_ap	FlexConnect アクセス ポイントの名前。
acl_name	FlexConnect ACL の名前。
enable	ローカルでスイッチされる無線 LAN に対して FlexConnect ACL をイネーブルにします。
disable	ローカルでスイッチされる無線 LAN に対して FlexConnect ACL をディセーブルにします。

コマンド デフォルト

ローカルでスイッチされる WLAN の外部 Web 認証用 FlexConnect ACL を無効にします。

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。

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。

使用上のガイドライン

AP に固有の FlexConnect ACL のプライオリティは、最も高くなります。WLAN に固有の FlexConnect ACL のプライオリティは、最も低くなります。

次に、WLAN 6 に対して外部 Web 認証用 FlexConnect ACL を有効にする例を示します。

```
(Cisco Controller) >config ap flexconnect web-auth wlan 6 AP2 flexacl2 enable
```

config ap flexconnect web-policy acl

アクセス ポイントに対して Web ポリシー FlexConnect ACL を設定するには、 **config ap flexconnect web-policy acl** コマンドを使用します。

config ap flexconnect web-policy acl {**add** | **delete**} *acl_name*

構文の説明

add	アクセス ポイントに Web ポリシー FlexConnect ACL を追加します。
delete	アクセス ポイントの Web ポリシー FlexConnect ACL を削除します。
acl_name	Web ポリシー FlexConnect 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。

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、アクセス ポイントに Web ポリシー FlexConnect ACL を追加する例を示します。

```
(Cisco Controller) >config ap flexconnect web-policy acl add flexacl2
```

config ap flexconnect wlan

ローカルでスイッチされる WLAN の FlexConnect アクセス ポイントを設定するには、**config ap flexconnect wlan** コマンドを使用します。

config ap flexconnect wlan l2acl {**add** *wlan_id cisco_ap acl_name* | **delete** *wlan_id cisco_ap*}

構文の説明

add	FlexConnect アクセス ポイントにレイヤ 2 ACL を追加します。
wlan_id	1 ～ 512 の無線 LAN 識別子。
cisco_ap	Cisco Lightweight アクセス ポイントの名前。
acl_name	レイヤ 2 ACL の名前。名前には 32 文字以内の英数字を使用できます。
delete	FlexConnect アクセス ポイントからレイヤ 2 ACL 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
7.5	このコマンドが導入されました。

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。

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。
- AP は最大 16 の WLAN をサポートするので、AP ごとに最大 16 のレイヤ 2 ACL がサポートされます。
- AP 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、FlexConnect AP でレイヤ 2 ACL を設定する例を示します。

```
(Cisco Controller) >config ap flexconnect wlan add 1 AP1600_1 acl_l2_1
```

config ap group-name

Cisco Lightweight アクセス ポイントの内容がわかるグループ名を指定するには、**config ap group-name** コマンドを使用します。

config ap group-name *groupname cisco_ap*

構文の説明

groupname	アクセス ポイント グループの内容がわかる名前。
cisco_ap	Cisco Lightweight 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。

使用上のガイドライン

Cisco Lightweight アクセス ポイントを無効にしてから、このパラメータを変更する必要があります。

次に、アクセス ポイント AP01 の内容がわかる名前を設定する例を示します。

```
(Cisco Controller) >config ap group-name superusers AP01
```

config ap hotspot

アクセス ポイントにホットスポット パラメータを設定するには、**config ap hotspot** コマンドを使用します。

config ap hotspot venue {**type** *group_code type_code* | **name** {**add** *language_code venue_name* | **delete**}} *cisco_ap*

構文の説明

venue	特定の AP グループの場所の情報を設定します。
type	特定の AP グループの場所のタイプを設定します。
group_code	特定の 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：未指定 • 1：アセンブリ • 2：ビジネス • 3：教育 • 4：工場および産業 • 5：機関 • 6：商業 • 7：住居 • 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：未指定のアセンブリ
- 1：アリーナ
- 2：スタジアム
- 3：乗客ターミナル
- 4：円形劇場
- 5：アミューズメント パーク
- 6：礼拝所
- 7：会議場
- 8：図書館
- 9：博物館
- 10：レストラン
- 11：シアター
- 12：バー
- 13：喫茶店
- 14：動物園または水族館
- 15：緊急対応センター

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：未指定のビジネス
- 1：医師または歯科医師のオフィス
- 2：銀行
- 3：消防署
- 4：警察署
- 6：郵便局
- 7：専門家のオフィス
- 8：研究および開発施設
- 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：未指定の教育機関
- 1：小学校
- 2：中学校
- 3：大学

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：未指定の工場および産業
- 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：未指定の公共機関
- 1：病院
- 2：長期看護施設
- 3：アルコールおよび薬物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

type_code

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：未指定の商業施設
- 1：小売店
- 2：食料品店
- 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：未指定の居住施設
- 1：私邸
- 2：ホテルまたはモーテル
- 3：寄宿舎
- 4：宿泊施設

場所グループ 8（倉庫）のオプションは次のとおりです。

- 0：未指定の倉庫

場所グループ 9（公共施設、その他）のオプションは次のとおりです。

- 0：未指定の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：未指定の乗り物
- 1：自動車またはトラック
- 2：飛行機
- 3：バス
- 4：フェリー
- 5：船またはボート
- 6：電車
- 7：モーター 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：未指定のアウトドア
- 1：MINI-MESH ネットワーク

- 2：都市公園
- 3：休憩施設
- 4：交通管制施設
- 5：バス停留所
- 6：売店

name	このアクセス ポイントの場所の名前を設定します。
language_code	場所で使用される言語を定義する ISO-639 のコード化文字列。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。
venue_name	このアクセスポイントの場所の名前。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	このアクセス ポイントの HotSpot 場所名を追加します。
delete	このアクセス ポイントの HotSpot 場所名を削除します。
cisco_ap	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、場所のグループを教育施設として、場所のタイプを大学として設定する例を示します。

```
(Cisco Controller) >config ap hotspot venue type 3 3
```

config ap image predownload

指定したアクセス ポイントにイメージを設定するには、**config ap image predownload** コマンドを使用します。

config ap image predownload {**abort** | **primary** | **backup**} {*cisco_ap* | **all**}

構文の説明

abort	プレダウンロード イメージ・プロセスを中断します。
primary	コントローラのプライマリ・イメージから Cisco アクセス ポイントにイメージをプレダウンロードします。
cisco_ap	Cisco Lightweight アクセス ポイントの名前。
all (Cisco Controller) >	すべてのアクセス ポイントにイメージをプレダウンロードすることを指定します。

（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。

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、プライマリ イメージからアクセス ポイントにイメージをプレダウンロードする例を示します。

```
(Cisco Controller) >config ap image predownload primary all
```

config ap image swap

アクセス ポイントのプライマリ イメージとバックアップ イメージを切り替えるには、**config ap image swap** コマンドを使用します。

config ap image swap {*cisco_ap* | **all**}

構文の説明

cisco_ap	Cisco Lightweight アクセス ポイントの名前。
all	すべてのアクセス ポイントに起動イメージを交換することを指定します。

（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。

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。

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、アクセス ポイントのプライマリおよびセカンダリ イメージを切り替える例を示します。

```
(Cisco Controller) >config ap image swap all
```

config ap lag-mode support

次のコマンドを入力することにより、すべての Cisco Aironet 1850 シリーズ AP または特定の Cisco Aironet 1850 シリーズ AP のリンク集約を設定します。

config ap lag-mode support {**enable** | **disable**} [*ap-name*]

構文の説明

enable	すべての Cisco Aironet 1850 シリーズ AP のリンク集約を有効にします。
disable	すべての Cisco Aironet 1850 シリーズ AP のリンク集約を無効にします。
enable *ap-name*	指定した Cisco Aironet 1850 シリーズ AP のリンク集約を有効にします。
disable *ap-name*	指定した Cisco Aironet 1850 シリーズ AP のリンク集約を無効にします。

コマンド履歴

リリース	変更内容
8.1.110.0	このコマンドが導入されました。

config ap led-state

アクセス ポイントの LED ステートを設定にする場合、または LED の点滅を設定する場合には、**config ap led-state** コマンドを使用します。

config ap led-state {**enable** | **disable**} {*cisco_ap* | **all**}

config ap led-state flash {*seconds* | **indefinite** | **disable**} {*cisco_ap* | **dual-band**}

構文の説明

enable	アクセスポイントのLEDステートを有効にします。
disable	アクセスポイントのLEDステートを無効にします。
cisco_ap	Cisco Lightweight アクセス ポイントの名前。
flash	アクセス ポイントの LED の点滅を設定します。
seconds	LED が点滅している期間。指定できる範囲は 1 ～ 3600 秒です。
indefinite	アクセスポイントのLEDに無制限の点滅を設定します。
dual-band	すべてのデュアルバンドアクセスポイントの LED ステートを設定します。

使用上のガイドライン

（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。

デュアル バンド無線モジュールを持つアクセス ポイントの LED は、led state flash コマンドを実行する場合に青緑色に点滅します。

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。

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、アクセス ポイントの LED ステートを有効にする例を示します。

```
(Cisco Controller) >config ap led-state enable AP02
```

次に、デュアル バンド アクセス ポイントの LED の点滅を有効にする例を示します。

```
(Cisco Controller) >config ap led-state flash 20 dual-band
```

config ap link-encryption

5500 シリーズ コントローラのアクセス ポイントに対して Datagram Transport Layer Security（DTLS）データ暗号化を設定するには、 **config ap link-encryption** 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 ap link-encryption {**enable** | **disable**} {*cisco_ap* | **all**}

構文の説明

enable	アクセス ポイントの DTLS データ暗号化を有効にします。
disable	アクセス ポイントの DTLS データ暗号化を無効にします。
cisco_ap	Cisco Lightweight アクセス ポイントの名前。
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

DTLS データ暗号化は OfficeExtend アクセス ポイントに対しては自動的に有効になりますが、他のすべてのアクセス ポイントに対してはデフォルトで無効になります。

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

DTLS データ暗号化をサポートするのは Cisco 5500 シリーズのコントローラだけです。この機能は、他のコントローラ プラットフォームでは利用できません。データ暗号化が有効なアクセス ポイントが他のいずれかのコントローラに接続しようとすると、アクセス ポイントはコントローラに接続しますが、データ パケットは暗号化されない状態で送信されます。

DTLS データ暗号化をサポートするのは Cisco 1130、1140、1240、および 1250 シリーズのアクセス ポイントだけであり、データが暗号化されたアクセス ポイントは WPLUS ライセンスがコントローラにインストールされている場合にだけ 5500 シリーズのコントローラに接続できます。WPLUS ライセンスがインストールされていない場合、アクセス ポイントはコントローラに接続できません。

次に、アクセス ポイントのデータ暗号化を有効にする例を示します。

```
(Cisco Controller) >config ap link-encryption enable AP02
```

config ap link-latency

特定のアクセス ポイントまたは現在コントローラにアソシエートされているすべてのアクセス ポイントのリンク遅延を設定するには、**config ap link-latency** 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 ap link-latency {**enable** | **disable** | **reset**} {*cisco_ap* | **all**}

構文の説明

enable	アクセス ポイントのリンク遅延を有効にします。
disable	アクセス ポイントのリンク遅延を無効にします。
reset	すべてのアクセス ポイントのリンク遅延をリセットします。
cisco_ap	Cisco Lightweight アクセス ポイントの名前。
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

リンク遅延は、デフォルトでは無効になっています。

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。

使用上のガイドライン

このコマンドは、現在コントローラに接続されているアクセス ポイントだけに対してリンク遅延を有効または無効にします。将来 join されるアクセス ポイントには適用されません。

次に、すべてのアクセス ポイントのリンク遅延を有効にする例を示します。

```
(Cisco Controller) >config ap link-latency enable all
```

config ap location

Cisco Lightweight アクセス ポイントのロケーション説明を変更するには、**config ap location** コマンドを使用します。

config ap location *location cisco_ap*

構文の説明

location	アクセス ポイントのロケーション名（二重引用符で囲みます）。
cisco_ap	Cisco Lightweight 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。

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。

使用上のガイドライン

Cisco Lightweight アクセス ポイントを無効にしてから、このパラメータを変更する必要があります。

次に、アクセス ポイント AP1 のロケーション説明を設定する例を示します。

```
(Cisco Controller) >config ap location "Building 1" AP1
```

config ap logging syslog level

特定のアクセス ポイントまたはすべてのアクセス ポイントに対する syslog メッセージのフィルタリングの重大度レベルを設定するには、**config ap logging syslog level** コマンドを使用します。

config ap logging syslog level *severity_level* {*cisco_ap* | **all**}

構文の説明

severity_level	重大度レベルは次のとおりです。 • 緊急：重大度 0 • アラート：重大度 1 • 重要：重大度 2 • エラー：重大度 3 • 警告：重大度 4 • 通知：重大度 5 • 情報：重大度 6 • デバッグ：重大度 7
cisco_ap	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。

（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。

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。

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。

使用上のガイドライン

syslog レベルを設定する場合は、重大度がそのレベル以下のメッセージだけがアクセスポイントに送信されます。たとえば、syslog レベルを警告（重大度 4）に設定した場合は、重大度が 0 ～ 4 のメッセージだけがアクセス ポイントに送信されます。

次に、syslog メッセージのフィルタリングの重大度を 3 に設定する例を示します。

```
(Cisco Controller) >config ap logging syslog level 3
```

config ap logging syslog facility

特定のアクセス ポイントまたはすべてのアクセス ポイントに対する syslog メッセージのフィルタリングのファシリティ レベルを設定するには、**config ap logging syslog facility** コマンドを使用します。

config ap logging syslog facility *facility-level* {*cisco_ap* | **all**}

構文の説明

facility-level	ファシリティ レベルは次のいずれかです。 • auth = 認証システム。 • cron = cron/at ファシリティ。 • daemon = システム デーモン。 • kern = カーネル。 • local0 = ローカル使用。 • local1 = ローカル使用。 • local2 = ローカル使用。 • local3 = ローカル使用。 • local4 = ローカル使用。 • local5 = ローカル使用。 • local5 = ローカル使用。 • local6 = ローカル使用。 • local7 = ローカル使用。 • lpr = ライン プリンタ システム。 • mail = メール システム。 • news = USENET ニュース。 • sys10 = システム使用。 • sys11 = システム使用。 • sys12 = システム使用。 • sys13 = システム使用。 • sys14 = システム使用。 • sys9 = システム使用。 • syslog = Syslog 自体。 • user = ユーザ プロセス。 • uucp = UNIX 間コピー システム。
cisco_ap	特定のアクセスポイントに対して設定します。
all	すべてのアクセス ポイントに対して設定します。

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、すべてのアクセス ポイントに対する syslog メッセージのフィルタリングのフィルタリング レベルを auth に設定する例を示します。

```
(Cisco Controller) >config ap logging syslog facility auth all
```

config ap max-count

Cisco Wireless LAN Controller（WLC）でサポートされるアクセス ポイントの最大数を設定するには、**config ap max-count** コマンドを使用します。

config ap max-count *number*

構文の説明

number	Cisco WLC でサポートされるアクセス ポイントの数。

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

設定された値がライセンスのアクセス ポイント数を超えている場合、Cisco WLC ライセンスのアクセス ポイント数がこの数よりも優先されます。値が 0 の場合は、アクセス ポイントの最大数に制限がなくなります。高可用性が設定されている場合は、Cisco WLC でサポートされるアクセス ポイントの最大数を設定した後に、アクティブ Cisco WLC とスタンバイ Cisco WLC の両方を再起動する必要があります。

次に、Cisco WLC でサポートされるアクセス ポイントの数を設定する例を示します。

```
(Cisco Controller) >config ap max-count 100
```

config ap mgmtuser add

AP 管理用のユーザ名、パスワード、シークレット パスワードを設定するには、 **config ap mgmtuser add** コマンドを使用します。

config ap mgmtuser add username *AP_username* **password** *AP_password* **secret** *secret* {**all** | *cisco_ap*}

構文の説明

username	AP 管理用のユーザ名を設定します。
AP_username	管理ユーザ名。
password	AP 管理用のパスワードを設定します。
AP_password	AP 管理パスワード。
secret	特権 AP 管理用のシークレット パスワードを設定します。
secret	AP 管理シークレット パスワード。
all	特定のユーザ名がないすべてのAPに設定を適用します。
cisco_ap	シスコ アクセス ポイント。

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。

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。

使用上のガイドライン

パスワードについて、次の要件が実施されます。

- パスワードには、小文字、大文字、数字、特殊文字のうち、3 つ以上の文字クラスが含まれる必要があります。
- パスワード内で同じ文字を連続して 4 回以上繰り返すことはできません。
- パスワードには、管理ユーザ名やユーザ名を逆にしたものを使用しないでください。

- パスワードに使用しないほうがよい文字には、Cisco、oscic、admin、nimda のような語のほか、大文字の代わりに 1 や |、！を、o の代わりに 0 を、s の代わりに $ を使用して置き換えた文字などがあります。

  シークレット パスワードについて、次の要件が実施されます。

- シークレットパスワードには、小文字、大文字、数字、特殊文字のうち、3 つ以上の文字クラスが含まれる必要があります。

次に、AP 管理用のユーザ名、パスワード、シークレット パスワードを追加する例を示します。

```
(Cisco Controller) > config ap mgmtuser add username acd password Arc_1234 secret Mid_45
 all
```

config ap mgmtuser delete

特定のアクセス ポイントがコントローラのグローバル クレデンシャルを使用するように強制するには、**config ap mgmtuser delete** コマンドを使用します。

config ap mgmtuser delete *cisco_ap*

構文の説明

cisco_ap	アクセス ポイント。

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。

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、アクセス ポイントのクレデンシャルを削除する例を示します。

```
(Cisco Controller) > config ap mgmtuser delete cisco_ap1
```

config ap mode

個別の Cisco Lightweight アクセス ポイントの Cisco WLC 通信オプションを変更するには、**config ap mode** コマンドを使用します。

config ap mode {**bridge** | **flexconnect sensor submode** {**none** | **wips** | **pppoe-only** | **pppoe-wips**} | **local submode** {**none** | **wips**} | **reap** | **rogue** | **sniffer** | **se-connect** | **monitor submode** {**none** | **wips**} | **flex+bridge submode**{**none** | **wips** | **pppoe-only** | **pppoe-wips**} } *cisco_ap*

構文の説明

bridge	Lightweight アクセス ポイントからメッシュ アクセス ポイント（ブリッジモード）に変換します。
flexconnect	アクセス ポイントで FlexConnect モードを有効にします。
local	屋内メッシュ アクセス ポイント（MAP または RAP）から nonmesh Lightweight アクセス ポイント（ローカル モード）に変換します。
reap	アクセス ポイントでリモート エッジ アクセス ポイント モードを有効にします。
rogue	アクセス ポイントで有線の不正なアクセス ポイントの検出モードを有効にします。
sniffer	アクセス ポイントで無線スニファ モードを有効にします。
se-connect	アクセス ポイントで Flex + ブリッジ モードを有効にします。
flex+bridge	アクセス ポイントで Spectrum Expert モードを有効にします。
submode	（任意）アクセス ポイントで wIPS サブモードを設定します。
none	アクセス ポイントで wIPS を無効にします。
wips	アクセス ポイントで wIPS サブモードを有効にします。
pppoe-only	アクセス ポイントで PPPoE サブモードを有効にします。

pppoe-wips	アクセス ポイントで PPPoE-wIPS サブモードを有効にします。
sensor	Cisco AP のセンサー モードを有効にします。
cisco_ap	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

ローカル

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。
8.0	**flex+bridge** キーワードが追加されました。
8.3	このコマンドが変更されました。**sensor** キーワードが追加されました。

使用上のガイドライン

スニファ モードは、そのチャネル上のクライアントからすべてのパケットを取得し、Airopeek を実行するリモート マシンまたはその他のサポート対象パケット アナライザ ソフトウェアに転送します。これには、タイムスタンプ、信号強度、パケット サイズなどの情報が含まれます。

次に、ブリッジ モードでアクセス ポイント AP91 と通信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 ap mode bridge AP91
```

次に、ローカル モードでアクセス ポイント AP01 と通信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 ap mode local AP01
```

次に、リモート オフィス（REAP）モードでアクセス ポイント AP91 と通信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 ap mode flexconnect AP91
```

次に、有線の不正なアクセス ポイントの検出モードでアクセス ポイント AP91 と通信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 ap mode rogue AP91
```

次に、無線スニファ モードでアクセス ポイント AP02 と通信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 ap mode sniffer AP02
```

config ap module3g

Cisco Universal Small Cell（USC）8x18 デュアルモード モジュールを設定するには、**config ap module3g** コマンドを使用します。

config ap module3g {**enable** | **disable**} *ap-name*

構文の説明

enable	指定した Cisco AP で Cisco USC 8x18 デュアル モード モジュールを有効にします。
disable	指定した Cisco AP で Cisco USC 8x18 デュアル モード モジュールを無効にします。
ap-name	Cisco AP の名前。 （注） リリース 8.1 では、Cisco Aironet 3600I および 3700I AP のみがサポートされています。

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
8.1	このコマンドが導入されました。

使用上のガイドライン

2.4 GHz の Wi-Fi と 3G/4G モジュールを有効にすると、共存の警告が表示される場合があります。

次に、*my-ap* という Cisco AP で Cisco USC 8x18 デュアル モード モジュールを有効にする例を示します。

```
(Cisco Controller) >config ap module3g enable my-ap
```

config ap monitor-mode

Cisco Lightweight アクセス ポイント チャネルの最適化を設定するには、**config ap monitor-mode** コマンドを使用します。

config ap monitor-mode {**802.11b fast-channel** | **no-optimization** | **tracking-opt** | **wips-optimized**} *cisco_ap*

構文の説明

802.11b fast-channel	監視モードアクセスポイントに対して802.11bスキャン チャネルを設定します。
no-optimization	アクセスポイントに対してチャネルスキャンの最適化を行わないことを指定します。
tracking-opt	アクセス ポイントに対してトラッキングが最適化されたチャネルスキャンを有効にします。
wips-optimized	アクセス ポイントに対して wIPS が最適化されたチャネル スキャンを有効にします。
cisco_ap	Cisco Lightweight 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。

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、アクセス ポイント AP01 に Cisco wireless Intrusion Prevention System（wIPS）監視モードを設定する例を示します。

```
(Cisco Controller) > config ap monitor-mode wips-optimized AP01
```

config ap name

Cisco Lightweight アクセス ポイントの名前を変更するには、**config ap name** コマンドを使用します。

config ap name *new_name old_name*

構文の説明

new_name	Cisco Lightweight アクセス ポイントの新しい名前。
old_name	Cisco Lightweight アクセス ポイントの現在の名前。

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。

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、アクセス ポイントの名前を AP1 から AP2 に変更する例を示します。

```
(Cisco Controller) > config ap name AP1 AP2
```

config ap packet-dump

アクセス ポイントのパケット キャプチャ パラメータを設定するには、**config ap packet-dump** コマンドを使用します。

config ap packet-dump {**buffer-size** *Size _in_KB* | **capture-time** *Time_in_Min* | **ftp serverip** *IP_addr* **path** *path* **username** *username***password** *password* | **start** *MAC_address Cisco_AP* | **stop** | **truncate** *Length_in_Bytes*}
config ap packet-dump classifier {{**arp** | **broadcast** | **control** | **data** | **dot1x** | **iapp** | **ip** | **management** | **multicast** } {**enable** | **disable**} | **tcp** {**enable** | **disable** | **port** *TCP_Port* {**enable** | **disable**}} | **udp** {**enable** | **disable** | **port** *UDP_Port* {**enable** | **disable**}}}

構文の説明

buffer-size	アクセス ポイントにパケット キャプチャのバッファ サイズを設定します。
Size _in_KB	バッファのサイズ。指定できる範囲は 1024 ～ 4096 KB です。
capture-time	パケット キャプチャのタイマー値を設定します。
Time_in_Min	パケット キャプチャのタイマー値。範囲は 1 ～ 60 分です。
ftp	パケット キャプチャの FTP パラメータを設定します。
serverip	FTP サーバを設定します。
IP_addr	FTP サーバの IP アドレスです。
path *path*	FTP サーバのパスを設定します。
username *user_ID*	FTP サーバ用のユーザ名を設定します。
password *password*	FTP サーバ用のパスワードを設定します。
start	アクセス ポイントからパケット キャプチャを開始します。

MAC_address	パケット キャプチャのクライアントの MAC アドレス。
Cisco_AP	Cisco アクセス ポイントの名前。
stop	アクセス ポイントからパケット キャプチャを停止します。
truncate	パケット キャプチャ中にパケットを指定の長さに切り捨てます。
Length_in_Bytes	切り捨て後のパケットの長さ。範囲は 20 ～ 1500 です。
classifier	パケット キャプチャの分類子情報を設定します。キャプチャ対象とする必要のあるパケットのタイプを指定できます。
arp	ARP パケットをキャプチャします。
enable	ARP、ブロードキャスト、802.11 制御、802.11 データ、dot1x、Inter Access Point Protocol（IAPP）、IP、802.11 管理、またはマルチキャスト パケットのキャプチャを有効にします。
disable	ARP、ブロードキャスト、802.11 制御、802.11 データ、dot1x、IAPP、IP、802.11 管理、またはマルチキャスト パケットのキャプチャを無効にします。
broadcast	ブロードキャスト パケットをキャプチャします。
control	802.11 制御パケットをキャプチャします。
data	802.11 データ パケットをキャプチャします。

dot1x	dot1x パケットをキャプチャします。
iapp	IAPP パケットをキャプチャします。
ip	IP パケットをキャプチャします。
management	802.11 管理パケットをキャプチャします。
multicast	マルチキャスト パケットをキャプチャします。
tcp	TCP パケットをキャプチャします。
TCP_Port	TCP ポート番号。有効な範囲は 1 ～ 65535 です。
udp	TCP パケットをキャプチャします。
UDP_Port	UDP ポート番号。有効な範囲は 1 ～ 65535 です。
ftp	パケット キャプチャの FTP パラメータを設定します。
server_ip	FTP サーバの IP アドレス。

コマンド デフォルト

デフォルトのバッファ サイズは 2 MB です。デフォルトのキャプチャ時間は 10 分です。

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 と IPv6 の両方のアドレス形式をサポートします。
8.8	このコマンドは、Cisco Wave 2 AP ではサポートされていません。詳細については、CSCvj19314 を参照してください。

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。

使用上のガイドライン

コントローラ間ローミング中には、パケット キャプチャは機能しません。

コントローラでは、ビーコンやプローブの応答など、無線ファームウェアに作成され、アクセス ポイントから送信されたパケットをキャプチャしません。Tx パスで無線ドライバを通過するパケットだけがキャプチャされます。

config ap packet-dump start コマンドを使用して、アクセス ポイントからパケット キャプチャを開始します。パケット キャプチャを開始すると、コントローラは、クライアントがアソシエートされるアクセス ポイントに Control and Provisioning of Wireless Access Points（CAPWAP）メッセージを送信し、パケットをキャプチャします。パケット キャプチャを開始する前に、FTP サーバを設定し、クライアントがアクセス ポイントにアソシエートされている必要があります。クライアントがアクセス ポイントにアソシエートされていない場合、アクセス ポイントの名前を指定する必要があります。

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、アクセス ポイントからパケット キャプチャを開始する例を示します。

```
(Cisco Controller) >config ap packet-dump start 00:0d:28:f4:c0:45 AP1
```

次に、アクセス ポイントから 802.11 制御パケットをキャプチャする例を示します。

```
(Cisco Controller) >config ap packet-dump classifier control enable
```

config ap port

外部アクセス ポイントのポートを設定するには、**config ap port** コマンドを使用します。

config ap port *MAC port*

構文の説明

MAC	外部アクセス ポイントの MAC アドレス。
port	外部アクセス ポイントにアクセスするポート番号。

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。

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、外部アクセス ポイントの MAC アドレスのポートを設定する例を示します。

```
(Cisco Controller) > config ap port 12:12:12:12:12:12 20
```

config ap power injector

アクセス ポイントのパワー インジェクタ ステートを設定するには、**config ap power injector** コマンドを使用します。

config ap power injector {**enable** | **disable**} {*cisco_ap* | **all**} {**installed** | **override** | *switch_MAC*}

構文の説明

enable	アクセス ポイントのパワー インジェクタ ステートを有効にします。
disable	アクセス ポイントのパワー インジェクタ ステートを無効にします。
cisco_ap	Cisco Lightweight アクセス ポイントの名前。
all	コントローラに接続されたすべての Cisco Lightweight アクセス ポイントを指定します。
installed	パワーインジェクタが設置された現在のスイッチ ポートの MAC アドレスを検出します。
override	安全性チェックを上書きし、パワー インジェクタが常にインストールされていることを前提とします。
switch_MAC	パワー インジェクタが設置されたスイッチ ポートの MAC アドレス。

（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。

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。

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、すべてのアクセス ポイントのパワー インジェクタ ステートを有効にする例を示します。

```
(Cisco Controller) > config ap power injector enable all 12:12:12:12:12:12
```

config ap power pre-standard

アクセス ポイントに対してインライン パワー搭載のシスコの先行標準スイッチ ステートを有効または無効にするには、**config ap power pre-standard** コマンドを使用します。

config ap power pre-standard {**enable** | **disable**} *cisco_ap*

構文の説明

enable	アクセス ポイントに対してインライン パワー搭載のシスコの先行標準スイッチ ステートを有効にします。
disable	アクセス ポイントに対してインライン パワー搭載のシスコの先行標準スイッチ ステートを無効にします。
cisco_ap	Cisco Lightweight アクセス ポイントの名前。

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。

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、アクセス ポイント AP02 に対してインライン パワー搭載のシスコの先行標準スイッチ ステートを有効にする例を示します。

```
(Cisco Controller) > config ap power pre-standard enable AP02
```

config ap preferred-mode

優先モードを設定するには、**config ap preferred-mode** コマンドを使用します。

config appreferred-mode{**ipv4** | **ipv6**|**any**}{*AP_name* | *Ap-group_name* | *all* }

構文の説明

ipv4	IPv4 を優先モードに設定します。
ipv6	IPv6 を優先モードに設定します。
any	any を優先モードに設定します。
AP_name	AP に優先モードを設定します。
Ap-group_name	AP グループのメンバーに優先モードを設定します。
all	すべての AP に優先モードを設定します。

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
8.0	このコマンドが導入されました。IPv4 と IPv6 の両方がサポートされています。

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。

例

次に、Lightweight アクセス ポイント AP1 に対して IPv6 を優先モードに設定する例を示します。

```
(Cisco Controller) >config ap preferred-mode ipv6 AP1
```

config ap primary-base

Cisco Lightweight アクセス ポイントのプライマリ Cisco WLC を設定するには、**config ap primary-base** コマンドを使用します。

config ap primary-base *controller_name Cisco_AP* [*controller_ip_address*]

構文の説明

controller_name	Cisco WLC の名前。
Cisco_AP	Cisco Lightweight アクセス ポイント名。
controller_ip_address	（任意）アクセスポイントの接続先モビリティグループの外部にバックアップ コントローラが配置されている場合は、プライマリ、セカンダリ、またはターシャリ コントローラの IP アドレスを指定する必要があります。 （注） OfficeExtend アクセス ポイントの場合は、コントローラに対して名前と IP アドレスの両方を入力する必要があります。入力しないと、アクセス ポイントはコントローラに join できません。

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。
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。

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。

使用上のガイドライン

Cisco Lightweight アクセス ポイントは、すべてのネットワーク操作に関して、およびハードウェア リセットが発生した場合に、Cisco WLC と関連付けられます。

OfficeExtend アクセス ポイントは、コントローラを見つけるために一般的なブロードキャストまたは無線（OTAP）検出プロセスを使用しません。OfficeExtend アクセス ポイントは設定されたコントローラにだけ接続しようとするため、1 つまたは複数のコントローラを設定する必要があります。

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、Cisco AP のアクセス ポイントのプライマリ Cisco WLC IPv4 アドレスを設定する例を示します。

```
(Cisco Controller) > config ap primary-base SW_1 AP2 10.0.0.0
```

次に、Cisco AP のアクセス ポイントのプライマリ Cisco WLC IPv6 アドレスを設定する例を示します。

```
(Cisco Controller) > config ap primary-base SW_1 AP2 2001:DB8:0:1::1
```

関連コマンド

show ap config general

config ap priority

アクセスポイントに優先度を割り当ててコントローラの障害発生後に早い順ではなく優先度に従ってアクセス ポイントの再認証を行うには、**config ap priority** コマンドを使用します。

config ap priority {**1** | **2** | **3** | **4**} *cisco_ap*

構文の説明

1	低優先度を指定します。
2	中間の優先度を指定します。
3	高プライオリティを指定します。
4	最高（クリティカル）の優先度を指定します。
cisco_ap	Cisco Lightweight アクセス ポイント名。

コマンド デフォルト

1：低い優先度。

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

フェールオーバーの状況では、影響を受ける領域内のすべてのアクセスポイントを再認証するのに十分なポートがバックアップ コントローラに存在しない場合に、低い優先度のアクセスポイントよりも高い優先度のアクセスポイントが優先されます（これは低い優先度のアクセスポイントを置き換える場合であっても同様です）。

次に、アクセス ポイント AP02 に優先度を割り当ててコントローラの障害発生後に再認証優先度 3 を割り当てることによって、アクセス ポイントを再認証する例を示します。

```
(Cisco Controller) > config ap priority 3 AP02
```

config ap reporting-period

Cisco Lightweight アクセス ポイントをリセットするには、**config ap reporting-period** コマンドを使用します。

config ap reporting-period *period*

構文の説明

period	10 ～ 120 秒の期間。

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。

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、120 秒にアクセス ポイント レポート期間をリセットする例を示します。

```
> config ap reporting-period 120
```

config ap reset

Cisco Lightweight アクセス ポイントをリセットするには、**config ap reset** コマンドを使用します。

config ap reset *cisco_ap*

構文の説明

cisco_ap	Cisco Lightweight アクセス ポイント名。

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。

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、アクセス ポイントをリセットする例を示します。

```
(Cisco Controller) > config ap reset AP2
```

config ap retransmit interval

アクセス ポイントで制御パケットの再送信間隔を設定するには、**config ap retransmit interval** コマンドを使用します。

config ap retransmit interval *seconds* {**all** | *cisco_ap*}

構文の説明

seconds	2～5 秒の AP 制御パケットの再送信タイムアウト。
all	すべてのアクセス ポイントを指定します。
cisco_ap	Cisco Lightweight アクセス ポイント名。

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。

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、すべてのアクセス ポイントの再送信の間隔をグローバルに設定する例を示します。

```
(Cisco Controller) > config ap retransmit interval 4 all
```

config ap retransmit count

アクセス ポイントで制御パケットの再送信回数を設定するには、**config ap retransmit count** コマンドを使用します。

config ap retransmit count *count* {**all** | *cisco_ap*}

構文の説明

count	制御パケットが再送信される回数。範囲は 3 ～ 8 です。
all	すべてのアクセス ポイントを指定します。
cisco_ap	Cisco Lightweight アクセス ポイント名。

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。

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、特定のアクセス ポイントに対する再送信の再試行回数を設定する例を示します。

```
(Cisco Controller) > config ap retransmit count 6 cisco_ap
```

config ap role

メッシュ ネットワーク内のアクセス ポイントのロールを指定するには、**config ap role** コマンドを使用します。

config ap role {**rootAP** | **meshAP**} *cisco_ap*

構文の説明

rootAP	ルート アクセス ポイント（RAP）としてメッシュ アクセス ポイントを指定します。
meshAP	メッシュ アクセス ポイント（MAP）としてメッシュ アクセス ポイントを指定します。
cisco_ap	Cisco Lightweight アクセス ポイントの名前。

コマンド デフォルト

meshAPを使用して無効にすることができます。

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。

使用上のガイドライン

アクセス ポイントでコントローラに対して無線接続が存在する場合は **meshAP** キーワード、アクセス ポイントでコントローラに対して有線接続が存在する場合は **rootAP** キーワードを使用します。AP のロールを変更すると、AP が再起動します。

次に、ルート アクセス ポイントとしてメッシュ アクセス ポイント AP02 を指定する例を示します。

```
(Cisco Controller) > config ap role rootAP AP02
Changing the AP's role will cause the AP to reboot.
Are you sure you want to continue? (y/n)
```

config ap rst-button

アクセス ポイントの Reset ボタンを設定するには、**config ap rst-button** コマンドを使用します。

config ap rst-button {**enable** | **disable**} *cisco_ap*

構文の説明

enable	アクセス ポイントの Reset ボタンを有効にします。
disable	アクセス ポイントの Reset ボタンを無効にします。
cisco_ap	Cisco Lightweight 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 AP03 の Reset ボタンを設定する例を示します。

```
(Cisco Controller) > config ap rst-button enable AP03
```

config ap secondary-base

Cisco Lightweight アクセス ポイントのセカンダリ Cisco WLC を設定するには、 **config ap secondary-base** コマンドを使用します。

config ap secondary-base *Controller_name Cisco_AP*［*Controller_IP_address*］

構文の説明

controller_name	Cisco WLC の名前。
Cisco_AP	Cisco Lightweight アクセス ポイント名。
Controller_IP_address	（任意）。アクセス ポイントの接続先モビリティ グループの外部にバックアップ Cisco WLC が配置されている場合は、プライマリ、セカンダリ、またはターシャリ Cisco WLC の IP アドレスを指定する必要があります。 （注） OfficeExtend アクセス ポイントの場合は、Cisco WLC に対して名前と IP アドレスの両方を入力する必要があります。入力しないと、アクセス ポイントはこの Cisco WLC に join できません。

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。
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

Cisco Lightweight アクセス ポイントは、すべてのネットワーク操作に関して、およびハードウェア リセットが発生した場合に、Cisco WLC と関連付けられます。

OfficeExtend アクセス ポイントは、Cisco WLC を見つけるために一般的なブロードキャストまたは無線（OTAP）検出プロセスを使用しません。OfficeExtend アクセス ポイントは設定された Cisco WLC にだけ接続しようとするため、1 つまたは複数の Cisco WLC を設定する必要があります。

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、アクセス ポイントのセカンダリ Cisco WLC を設定する例を示します。

```
(Cisco Controller) > config ap secondary-base SW_1 AP2 10.0.0.0
```

次に、Cisco AP のアクセス ポイントのプライマリ Cisco WLC IPv6 アドレスを設定する例を示します。

```
(Cisco Controller) > config ap secondary-base SW_1 AP2 2001:DB8:0:1::1
```

関連コマンド

show ap config general

config ap slub-debug

アクセス ポイントでの slub デバッグを設定するには、**config ap slub-debug** コマンドを使用します。

（注）

config ap slub-debug {**sanity** | **red-zoning** | **poisoning** | **user-tracking** | **disable**} *cisco_ap* | **all**

構文の説明

sanity	健全性 slub デバッグ モードを設定します。
red-zoning	レッドゾーン化 slub デバッグ モードを設定します。
poisoning	ポイズニング slub デバッグ モードを設定します。
user-tracking	ユーザ トラッキング slub デバッグ モードを設定します。
disable	slub デバッグ モードを無効にします。
cisco_ap	Cisco Lightweight アクセス ポイント名。
all	すべての Cisco アクセス ポイントに適用されます。

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
8.2.160.0	このコマンドが導入されました。

使用上のガイドライン

有効/無効になる場合または slub デバッグ機能のモードを切り替える場合は、Cisco AP が再起動します。

次に、すべての Cisco AP で slub デバッグを無効にする例を示します。

```
(Cisco Controller) >config ap slub-debug disable all

Changing the AP's slub debug mode will cause the AP to reboot.
Are you sure you want to continue? (y/n) n
```

```
Slub debug mode not changed!
(Cisco Controller) >
```

config ap sniff

アクセス ポイントでスニフィングを有効または無効にするには、**config ap sniff** コマンドを使用します。

config ap sniff {**802.11a** | **802.11b**} {**enable** *channel server_ip* | **disable**} *cisco_ap*

構文の説明

802.11a	802.11a ネットワークを指定します。
802.11b	802.11b ネットワークを指定します。
enable	アクセス ポイントでスニフィングを有効にします。
channel	スニファ対象チャネル。
server_ip	Omnipeek、Airopeek、AirMagnet、または Wireshark を実行するリモート マシンの IP アドレス。
disable	アクセス ポイントでスニフィングを無効にします。
cisco_ap	スニファとして設定されたアクセスポイント。

コマンド デフォルト

チャネル 36。

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。

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。

使用上のガイドライン

アクセス ポイントでスニフィング機能が有効になっている場合、そのアクセス ポイントは指定されたチャネルで信号のスニフィングを開始します。すべてのパケットが取得され、Omnipeek、Airopeek、AirMagnet、または Wireshark ソフトウェアを実行しているリモート コンピュータに転送されます。これには、タイムスタンプ、信号強度、パケット サイズなどの情報が含まれます。

アクセス ポイントをスニファとして機能させるには、そのアクセス ポイントが送信したパケットを、上記いずれかのパケット アナライザを実行しているリモート コンピュータが受信できるように設定しておく必要があります。Airopeek のインストール後、次の .dll ファイルを Airopeek がインストールされている場所にコピーします。

- socket.dll ファイルを Plug-ins フォルダにコピーします（C:\Program Files\WildPackets\AiroPeek\Plugins など）
- socketres.dll ファイルを PluginRes フォルダにコピーします（C:\Program Files\WildPackets\AiroPeek\ 1033\PluginRes など）

次に、802.11a アクセス ポイントでのスニフィングをプライマリ Cisco WLC から有効にする例を示します。

```
(Cisco Controller) > config ap sniff 80211a enable 23 11.22.44.55 AP01
```

config ap ssh

アクセス ポイントで Secure Shell（SSH）接続を有効にするには、**config ap ssh** コマンドを使用します。

config ap ssh {**enable** | **disable** | **default**} *cisco_ap* | *all*

構文の説明

enable	アクセス ポイントで SSH 接続を有効にします。
disable	アクセス ポイントで SSH 接続を無効にします。
default	アクセス ポイントの特定の SSH 設定をグローバル SSH 設定で置き換えます。
cisco_ap	Cisco Lightweight アクセス ポイント名。
all	すべてのアクセス ポイント。

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。

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。

使用上のガイドライン

Cisco Lightweight アクセス ポイントは、すべてのネットワーク操作に関して、およびハードウェア リセットが発生した場合に、Cisco ワイヤレス LAN コントローラと関連付けられます。

次に、アクセス ポイント Cisco_ap2 で SSH 接続を有効にする例を示します。

```
> config ap ssh enable cisco_ap2
```

config ap static-ip

Cisco Lightweight アクセス ポイントの静的 IP アドレスを設定するには、**config ap static-ip** コマンドを使用します。

config ap static-ip {**enable** *Cisco_AP AP_IP_addr IP_netmask /prefix_length gateway* | **disable** *Cisco_AP* | **add** {**domain** {*Cisco_AP* | **all**} *domain_name* | **nameserver** {*Cisco_AP* | **all**} *nameserver-ip*} | **delete** {**domain** | **nameserver**} {*Cisco_AP* | **all**}}

構文の説明

enable	Cisco Lightweight アクセス ポイントの静的 IP アドレスを有効にします。
disable	Cisco Lightweight アクセス ポイントの静的 IP アドレスを無効にします。その場合、アクセス ポイントは DHCP を使用して IP アドレスを取得します。
Cisco_AP	Cisco Lightweight アクセス ポイント名。
AP_IP_addr	Cisco Lightweight アクセス ポイントの IP アドレス。
IP_netmask/prefix_length	Cisco Lightweight アクセス ポイントのネットワーク マスク。
gateway	Cisco Lightweight アクセス ポイント ゲートウェイの IP アドレス。
add	ドメインまたは DNS サーバを追加します。
domain	特定のアクセス ポイントまたはすべてのアクセスポイントが属するドメインを指定します。
all	すべてのアクセス ポイントを指定します。
domain_name	ドメイン名を指定します。
nameserver	特定のアクセス ポイントまたはすべてのアクセス ポイントが DNS 解決を使用してコントローラを検出できるよう DNS サーバを指定します。
nameserver-ip	DNS サーバの IP アドレス。
delete	ドメインまたは DNS サーバを削除します。

（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。

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。

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。

使用上のガイドライン

静的 IP アドレスがアクセス ポイントに設定されている場合は、DNS サーバとアクセス ポイントが属するドメインを指定しない限り、アクセス ポイントはドメイン ネーム システム（DNS）解決を使用してコントローラを検出できません。

IPv6 アドレス、プレフィックス長、および IPv6 ゲートウェイ アドレスの を入力すると、アクセス ポイント用に CAPWAP トンネルが再起動します。AP の IP アドレスを変更すると、AP の接続が解除されます。アクセス ポイントのコントローラへの再接続後、ドメインと IPv6 DNS サーバ情報を入力できます。

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、アクセス ポイントの静的 IP アドレスを設定する例を示します。

```
(Cisco Controller) >config ap static-ip enable AP2 209.165.200.225 255.255.255.0
209.165.200.254
```

次に、アクセス ポイントの静的 IPv6 アドレスを設定する例を示します。

```
(Cisco Controller) > config ap static-ip enable AP2 2001:DB8:0:1::1
```

関連コマンド

show ap config general

config ap stats-timer

Cisco Lightweight アクセス ポイントが Cisco ワイヤレス LAN コントローラに DOT11 統計情報を送信する時間（秒単位）を設定するには、**config ap stats-timer** コマンドを使用します。

config ap stats-timer *period cisco_ap*

構文の説明

period	0 ～ 65535 の時間（秒単位）。ゼロの値を指定すると、タイマーが無効になります。
cisco_ap	Cisco Lightweight アクセス ポイント名。

コマンド デフォルト

デフォルト値は 0（無効状態）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。

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。

使用上のガイドライン

値 0 は、Cisco Lightweight アクセス ポイントが DOT11 統計情報を送信しないことを意味します。このタイマーには 0 ～ 65,535 秒を指定できます。Cisco Lightweight アクセス ポイントを無効にしてから、この値を設定する必要があります。

次に、アクセス ポイント AP2 で、統計情報タイマーを 600 秒に設定する例を示します。

```
(Cisco Controller) > config ap stats-timer 600 AP2
```

config ap syslog host global

コントローラに結合されているアクセス ポイントすべてのグローバル syslog サーバを設定するには、**config ap syslog host global** コマンドを使用します。

config ap syslog host global *ip_address*

構文の説明

ip_address	syslog サーバの IPv4/IPv6 アドレス。

コマンド デフォルト

syslog サーバの IPv4 アドレスのデフォルト値は 255.255.255.255 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 と IPv6 の両方のアドレス形式をサポートします。

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。

使用上のガイドライン

デフォルトでは、すべてのアクセス ポイントのグローバル syslog サーバ IP アドレスは 255.255.255.255 です。コントローラ上の syslog サーバを設定する前に、アクセス ポイントがこのサーバが常駐するサブネットにアクセスできることを確認します。このサブネットにアクセスできない場合、アクセス ポイントは syslog メッセージを送信できません。

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 アドレスを使用してすべてのアクセス ポイントにグローバル syslog サーバを設定する例を示します。

```
(Cisco Controller) > config ap syslog host global 255.255.255.255
```

次に、IPv6 アドレスを使用してすべてのアクセス ポイントにグローバル syslog サーバを設定する例を示します。

```
(Cisco Controller) > config ap syslog host global  2001:9:10:56::100
```

config ap syslog host specific

特定のアクセス ポイントの syslog サーバを設定するには、**config ap syslog host specific** コマンドを使用します。

config ap syslog host specific *ap_nameip_address*

構文の説明

ap_name	Cisco Lightweight アクセス ポイント。
ip_address	syslog サーバの IPv4/IPv6 アドレス。

コマンド デフォルト

syslog サーバの IP アドレスのデフォルト値は 0.0.0.0 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。
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。

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。

使用上のガイドライン

デフォルトでは、各アクセス ポイントの syslog サーバ IP アドレスは 0.0.0.0 で、これはまだサーバが設定されていないことを示しています。このデフォルト値を使用すると、グローバル アクセス ポイント syslog サーバの IP アドレスがアクセス ポイントにプッシュされます。

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、Syslog サーバを設定する例を示します。

```
(Cisco Controller) >config ap syslog host specific 0.0.0.0
```

次に、IPv6 アドレスを使用して特定の AP に syslog サーバを設定する例を示します。

```
(Cisco Controller) > config ap syslog host specific AP3600 2001:9:10:56::100
```

config ap tcp-mss-adjust

特定のアクセス ポイントまたはすべてのアクセス ポイントで TCP 最大セグメント サイズ（MSS）を有効または無効にするには、**config ap tcp-mss-adjust** コマンドを使用します。

config ap tcp-mss-adjust {**enable** | **disable**} {*cisco_ap* | **all**} *size*

構文の説明

enable	アクセス ポイントで TCP 最大セグメント サイズを有効にします。
disable	アクセス ポイントで TCP 最大セグメント サイズを無効にします。
cisco_ap	Cisco Lightweight アクセス ポイント名。
all	すべてのアクセス ポイントを指定します。
size	最大セグメント サイズ。 • IPv4：536 ～ 1363 の値を指定します。 • IPv6：1220 ～ 1331 の値を指定します。 （注） CAPWAP v6 AP では、1220 未満または 1331 より大きい TCP MSS 値は無効です。

（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。

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 IPv6 だけをサポートしています。

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。

使用上のガイドライン

この機能を有効にすると、アクセス ポイントがデータ パスの無線クライアントへの TCP パケットとデータ パスの無線クライアントからの TCP パケットをチェックします。これらのパケットの MSS が設定した値または CAPWAP トンネルのデフォルト値よりも大きい場合、アクセス ポイントは MSS を、設定された新しい値に変更します。

次に、セグメント サイズが 1200 バイトであるアクセス ポイント cisco_ap1 で TCP MSS を有効にする例を示します。

```
(Cisco Controller) > config ap tcp-mss-adjust enable cisco_ap1 1200
```

config ap telnet

アクセス ポイントで Telnet 接続を有効にするには、**config ap telnet** コマンドを使用します。

config ap telnet {**enable** | **disable** | **default**} *cisco_ap* | *all*

構文の説明

enable	アクセス ポイントで Telnet 接続を有効にします。
disable	アクセス ポイントで Telnet 接続を無効にします。
default	アクセス ポイントの特定の Telnet 設定をグローバル Telnet 設定に置き換えます。
cisco_ap	Cisco Lightweight アクセス ポイント名。
all	すべてのアクセス ポイント。

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。

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。

使用上のガイドライン

- Cisco Lightweight アクセス ポイントは、すべてのネットワーク操作に関して、およびハードウェア リセットが発生した場合に、Cisco WLC と関連付けられます。
- Telnet は、Cisco Aironet 1810 OEAP、1810W、1830、1850、2800、および 3800 シリーズの AP ではサポートされていません。

次に、アクセス ポイント cisco_ap1 で Telnet 接続を有効にする例を示します。

```
(Cisco Controller) >config ap telnet enable cisco_ap1
```

次に、アクセス ポイント cisco_ap1 で Telnet 接続を無効にする例を示します。

```
(Cisco Controller) > config ap telnet disable cisco_ap1
```

config ap tertiary-base

Cisco Lightweight アクセス ポイントのターシャリ Cisco WLC を設定するには、**config ap tertiary-base** コマンドを使用します。

config ap tertiary-base *controller_name Cisco_AP*［*controller_ip_address*］

構文の説明

controller_name	Cisco WLC の名前。
Cisco_AP	Cisco Lightweight アクセス ポイント名。
controller_ip_address	（任意）アクセスポイントの接続先モビリティグループの外部にバックアップ コントローラが配置されている場合は、プライマリ、セカンダリ、またはターシャリ Cisco WLC の IP アドレスを指定する必要があります。 （注） OfficeExtend アクセス ポイントの場合は、Cisco WLC に対して名前と IP アドレスの両方を入力する必要があります。入力しないと、アクセスポイントはこの Cisco WLC に join できません。

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。
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

OfficeExtend アクセス ポイントは、Cisco WLC を見つけるために一般的なブロードキャストまたは無線（OTAP）検出プロセスを使用しません。OfficeExtend アクセス ポイントは設定された Cisco WLC にだけ接続しようとするため、1 つまたは複数のコントローラを設定する必要があります。

Cisco Lightweight アクセス ポイントは、すべてのネットワーク操作に関して、およびハードウェア リセットが発生した場合に、Cisco WLC と関連付けられます。

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、アクセス ポイントのターシャリ Cisco WLC を設定する例を示します。

```
(Cisco Controller) > config ap tertiary-base SW_1 AP02 10.0.0.0
```

次に、Cisco AP のアクセス ポイントのターシャリ Cisco WLC IPv6 アドレスを設定する例を示します。

```
(Cisco Controller) > config ap tertiary-base SW_1 AP2 2001:DB8:0:1::1
```

関連コマンド

show ap config general

config ap tftp-downgrade

Lightweight アクセス ポイントを Autonomous アクセス ポイントにダウングレードするために使用される設定を指定するには、**config ap ftp-downgrade** コマンドを使用します。

config ap tftp-downgrade *tftp_ip_addressfilename Cisco_AP*

構文の説明

tftp_ip_address	TFTP サーバの IP アドレスです。
filename	TFTP サーバ上のアクセス ポイント イメージ ファイルのファイル名。
Cisco_AP	アクセス ポイント名。

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。

次に、アクセス ポイント ap1240_102301 をダウングレードするための設定方法を示します。

```
(Cisco Controller) >config ap ftp-downgrade 209.165.200.224 1238.tar ap1240_102301
```

config ap username

ユーザ名とパスワードを特定のアクセス ポイントまたはすべてのアクセス ポイントにアクセスするように割り当てるには、**config ap username** コマンドを使用します。

config ap username *user_id* **password** *passwd* ［**all** | *ap_name*］

構文の説明

user_id	管理者ユーザ名。
passwd	管理者パスワード。
all	（任意）すべてのアクセス ポイントを指定します。
ap_name	特定のアクセス 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。

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、特定のアクセス ポイントにユーザ名およびパスワードを割り当てる例を示します。

```
(Cisco Controller) > config ap username jack password blue la204
```

次に、すべてのアクセス ポイントに同じユーザ名とパスワードを割り当てる例を示します。

```
(Cisco Controller) > config ap username jack password blue all
```

config ap venue

アクセス ポイントに対して 802.11u ネットワークの場所の情報を設定するには、**config ap venue** コマンドを使用します。

config ap venue {**add***venue_name venue-group venue-type lang-code cisco-ap* | **delete**}

構文の説明

add	場所の情報を追加します。
venue_name	場所の名前。
venue_group	場所グループのカテゴリ。場所グループ マッピングの詳細については次の表を参照してください。
venue_type	場所のタイプ。この値は指定された場所グループによって異なります。場所グループ マッピングについては次の表を参照してください。
lang_code	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）。
cisco_ap	アクセス ポイントの名前。
deletes	場所の情報を削除します。

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。

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、cisco-ap1 という名前のアクセス ポイントの場所の詳細を設定する例を示します。

```
(Cisco Controller) > config ap venue add test 11 34 eng cisco-ap1
```

この表には、場所グループごとに異なる場所のタイプが示されます。

表 *2：*場所グループのマッピング

場所グループの名前	値	グループの場所のタイプ
未指定	0	
アセンブリ	1	• 0：未指定のアセンブリ • 1：アリーナ • 2：スタジアム • 3：乗客ターミナル（たとえば、空港、バス、フェリー、電車の駅） • 4：円形劇場 • 5：アミューズメントパーク • 6：礼拝所 • 7：会議場 • 8：図書館 • 9：博物館 • 10：レストラン • 11：シアター • 12：バー • 13：喫茶店 • 14：動物園または水族館 • 15：緊急対応センター

場所グループの名前	値	グループの場所のタイプ
ビジネス	2	• 0：未指定のビジネス • 1：医師または歯科医師のオフィス • 2：銀行 • 3：消防署 • 4：警察署 • 6：郵便局 • 7：専門家のオフィス • 8：研究および開発施設 • 9：弁護士のオフィス
教育機関	3	• 0：未指定の教育機関 • 1：小学校 • 2：中学校 • 3：大学
工場および産業	4	• 0：未指定の工場および産業 • 1：工場
機関	5	• 0：未指定の公共機関 • 1：病院 • 2：長期看護施設（療養所、ホスピスなど） • 3：アルコールおよび薬物のリハビリテーション センター • 4：グループ ホーム • 5：刑務所または拘置所

場所グループの名前	値	グループの場所のタイプ
商業	6	• 0：未指定の商業施設 • 1：小売店 • 2：食料品店 • 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
住居	7	• 0：未指定の居住施設 • 1：私邸 • 2：ホテルまたはモーテル • 3：寄宿舎 • 4：宿泊施設
倉庫	8	未指定の倉庫
公共施設、その他	9	0：未指定の公共施設およびその他
乗り物	10	• 0：未指定の乗り物 • 1：自動車またはトラック • 2：飛行機 • 3：バス • 4：フェリー • 5：船またはボート • 6：電車 • 7：モーター バイク

場所グループの名前	値	グループの場所のタイプ
アウトドア	11	• 0：未指定のアウトドア • 1：自治体メッシュ ネットワーク • 2：都市公園 • 3：休憩施設 • 4：交通管制施設 • 5：バス停留所 • 6：売店

config ap wlan

Cisco Lightweight アクセス ポイント無線に対して無線 LAN オーバーライドを有効または無効にするには、**config ap wlan** コマンドを使用します。

config ap wlan {**enable** | **disable**} {**802.11a** | **802.11b**} *wlan_id cisco_ap*

構文の説明

enable	アクセス ポイントで無線 LAN オーバーライドを有効にします。
disable	アクセス ポイントで無線 LAN オーバーライドを無効にします。
802.11a	802.11a ネットワークを指定します。
802.11b	802.11b ネットワークを指定します。
wlan_id	無線 LAN に割り当てられている Cisco ワイヤレス LAN コントローラ ID。
cisco_ap	Cisco Lightweight アクセス ポイント名。

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。

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、AP03 802.11a で無線 LAN オーバーライドを有効にする例を示します。

```
(Cisco Controller) > config ap wlan 802.11a AP03
```

config atf 802.11

config atf 802.11 コマンドを使用することにより、ネットワーク レベル、AP グループ レベル、または AP 無線レベルで Cisco Air Time Fairness を設定します。

config atf 802.11{**a** | **b**} {**mode** {**disable** | **monitor** | **enforce-policy**} {[*ap-group-name*] | [*ap-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。
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 をモニタ モードで設定するには、次のコマンドを入力します。

```
(Cisco Controller) >config atf 802.11a mode monitor
```

- 802.11a ネットワークで通信時間の最適化を有効にするには、次のコマンドを入力します。

```
(Cisco Controller) >config atf 802.11a optimization enable
```

config atf policy

Cisco Air Time Fairness（ATF）ポリシーを設定するには、**config atf policy** コマンドを使用します。

config atf policy {{ **create** *policy-id policy-name policy-weight*} | {**modify** { **weight** *policy-weight policy-name*} | {**client-sharing** {**enable** | **disable**} *policy-name*}} | { **delete** *policy-name*}}

構文の説明

create	通信時間ポリシーを作成します。
modify	通信時間ポリシーを変更します。
delete	通信時間ポリシーを削除します。
client-sharing {**enable** | **disable** *policy-name*}	指定したポリシー名の Client Fair Sharing を有効または無効にします。
policy-id	ポリシー ID（1 ～ 511）。
policy-name	Cisco ATF ポリシーの名前。
policy-weight	ポリシー ウェイト（5 ー 100）。

コマンド履歴

リリース	変更内容
8.1.122.0	このコマンドが追加されました。
8.2	**client-sharing** {**enable** | **disable**} オプションが追加されました。

次に、Cisco ATF ポリシーを作成する例を示します。

```
(Cisco Controller) >config atf policy create 2 test-policy 70
```

config auth-list add

認可済みアクセス ポイント エントリを作成するには、**config auth-list add** コマンドを使用します。

config auth-list add {**mic** | **ssc**} *AP_MAC* [*AP_key*]

構文の説明

mic	アクセス ポイントに製造元がインストールした証明書があることを指定します。
ssc	アクセス ポイントに自己署名証明書があることを指定します。
AP_MAC	Cisco Lightweight アクセス ポイントの MAC アドレス。
AP_key	（任意）20 バイトまたは 40 桁に等しいキー ハッシュ値。

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。

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、MAC アドレス 00:0b:85:02:0d:20 で製造元がインストールした証明書によって許可済みアクセス ポイント エントリを作成する例を示します。

```
(Cisco Controller) > config auth-list add 00:0b:85:02:0d:20
```

関連コマンド

config auth-list delete

config auth-list ap-policy

config auth-list ap-policy

アクセス ポイントの認可ポリシーを設定するには、**config auth-list ap-policy** コマンドを使用します。

config auth-list ap-policy {**authorize-ap** {**enable** | **disable**} | **ssc** {**enable** | **disable**}}

構文の説明

authorize-ap enable	許可ポリシーを有効にします。
authorize-ap disable	AP 許可ポリシーを無効にします。
ssc enable	自己署名証明書を持つ AP の接続を許可します。
ssc disable	自己署名証明書を持つ AP の接続を禁止します。

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。

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、アクセス ポイントの許可ポリシーを有効にする例を示します。

```
(Cisco Controller) > config auth-list ap-policy authorize-ap enable
```

次に、自己署名証明書を持つアクセス ポイントの接続を有効にする例を示します。

```
(Cisco Controller) > config auth-list ap-policy ssc disable
```

関連コマンド

config auth-list delete

config auth-list add

config auth-list delete

アクセス ポイント エントリを削除するには、**config auth-list delete** コマンドを使用します。

config auth-list delete *AP_MAC*

構文の説明

AP_MAC	Cisco Lightweight 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。

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、MAC アドレス 00:1f:ca:cf:b6:60 のアクセス ポイント エントリを削除する例を示します。

```
(Cisco Controller) > config auth-list delete 00:1f:ca:cf:b6:60
```

関連コマンド

config auth-list delete

config auth-list add

config auth-list ap-policy

config auto-configure voice

WLAN での音声展開を自動設定するには、**config auto-configure voice** コマンドを使用します。

config auto-configure voice cisco *wlan_id* **radio** {**802.11a** | **802.11b** | **all**}

構文の説明

cisco	シスコ エンドポイントの音声展開用の自動設定 WLAN。
wlan_id	1 ～ 512 の無線 LAN 識別子（両端の値を含む）。
radio	WLAN で無線用に音声展開を自動設定します。
802.11a	WLAN で 802.11 a 用に音声展開を自動設定します。
802.11b	WLAN で 802.11 b 用に音声展開を自動設定します。
all	WLAN ですべての無線用に音声展開を自動設定します。

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

このコマンドを設定すると、すべての WLAN と無線が自動的に無効になります。設定が完了すると、WLAN と無線の以前の状態が復元されます。

次に、WLAN ですべての無線用に音声展開を自動設定する例を示します。

```
(Cisco Controller) >config auto-configure voice cisco 2 radio all
Warning! This command will automatically disable all WLAN's and Radio's.
 It will be reverted to the previous state once configuration is complete.
 Are you sure you want to continue? (y/N)y


Auto-Configuring these commands in WLAN for Voice..
 wlan qos 2 platinum
 - Success
 wlan call-snoop enable 2
 - Success
 wlan wmm allow 2
 - Success
 wlan session-timeout 2 86400
 - Success
 wlan peer-blocking disable 2
 - Success
 wlan security tkip hold-down 0 2
 - Success
 wlan exclusionlist 2 disable
 - Success
 wlan mac-filtering disable 2
 - Success
 wlan dtim 802.11a 2 2
```

```
 - Success
 wlan dtim 802.11b 2 2
 - Success
 wlan ccx aironetIeSupport  enabled 2
 - Success
 wlan channel-scan defer-priority 4 enable 2
 - Success
 wlan channel-scan defer-priority 5 enable 2
 - Success
 wlan channel-scan defer-priority 6 enable 2
 - Success
 wlan channel-scan defer-time 100 2
 - Success
wlan load-balance allow disable 2
 - Success
 wlan mfp client enable 2
 - Success
 wlan security wpa akm  cckm enable 2
 - Success
 wlan security wpa akm cckm timestamp-tolerance  5000 2
 - Success
 wlan band-select allow disable 2
 - Success
*********************************************

Auto-Configuring these commands for Voice - Radio 802.11a.

 advanced 802.11a edca-parameter optimized-voice
 - Success
 802.11a cac voice acm enable
 - Success
 802.11a cac voice max-bandwidth 75
 - Success
 802.11a cac voice roam-bandwidth 6
 - Success
 802.11a cac voice cac-method load-based
 - Success
 802.11a cac voice sip disable
 - Success
 802.11a tsm enable
 - Success
 802.11a exp-bwreq  enable
 - Success
 802.11a txPower global auto
 - Success
 802.11a channel global auto
 - Success
 advanced 802.11a channel dca interval 24
 - Success
 advanced 802.11a channel dca anchor-time 0
 - Success
 qos protocol-type platinum dot1p
 - Success
 qos dot1p-tag platinum 6
 - Success
 qos priority platinum voice voice besteffort
 - Success
 802.11a beacon period 100
 - Success
 802.11a dtpc enable
 - Success
 802.11a Coverage Voice RSSI Threshold -70
 - Success
 802.11a txPower global min 11
```

```
  - Success
 advanced eap eapol-key-timeout 250
 - Success
 advanced 802.11a voice-mac-optimization disable
 - Success
802.11h channelswitch enable 1
 - Success
Note: Data rate configurations are not changed.
It should be changed based on the recommended values after analysis.
*********************************************

Auto-Configuring these commands for Voice - Radio 802.11b.
 advanced 802.11b edca-parameter optimized-voice
 - Success
 802.11b cac voice acm enable
 - Success
 802.11b cac voice max-bandwidth 75
 - Success
 802.11b cac voice roam-bandwidth 6
 - Success
 802.11b cac voice cac-method load-based
 - Success
 802.11b cac voice sip disable
 - Success
 802.11b tsm enable
 - Success
 802.11b exp-bwreq  enable
 - Success
 802.11b txPower global auto
  - Success
 802.11b channel global auto - Success
 advanced 802.11b channel dca interval 24
 - Success
 advanced 802.11b channel dca anchor-time 0
 - Success
 802.11b beacon period 100
 - Success
 802.11b dtpc enable
 - Success
 802.11b Coverage Voice RSSI Threshold -70
 - Success
 802.11b preamble short
 - Success
advanced 802.11a voice-mac-optimization disable
 - Success
Note: Data rate configurations are not changed.
It should be changed based on the recommended values after analysis.
```

config avc profile create

新しい Application Visibility and Control（AVC）プロフィルを作成するには、**config avc profile create** コマンドを使用します。

config avc profile *profile_name* **create**

構文の説明

profile_name	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。
create	新しい AVC プロファイルを作成します。

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
7.4	このコマンドが導入されました。

使用上のガイドライン

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。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。

次に、新しいポート プロファイルを作成する例を示します。

```
(Cisco Controller) > config avc profile avcprofile1 create
```

関連コマンド

config avc profile delete

config avc profile rule

config wlan avc

show avc profile

show avc applications

show avc statistics

debug avc error

debug avc events

config avc profile delete

Application Visibility and Control（AVC）プロフィルを削除するには、**config avc profile delete** コマンドを使用します。

config avc profile *profile_name* **delete**

構文の説明

profile_name	AVC プロファイルの名前。
delete	AVC プロファイルを削除します。

コマンド デフォルト

AVC プロファイルは削除されません。

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。

次に、AVC プロファイルを削除する例を示します。

```
(Cisco Controller) > config avc profile avcprofile1 delete
```

関連コマンド

config avc profile create

config avc profile rule

config wlan avc

show avc profile summary

show avc profile detailed

debug avc error

debug avc events

config avc profile rule

Application Visibility and Control（AVC）プロフィルのルールを設定するには、**config avc profile rule** コマンドを使用します。

config avc profile *profile_name* **rule** {**add** | **remove**} **application** *application_name* {**drop** | **mark** *dscp*}

構文の説明

profile_name	AVC プロファイルの名前。
rule	AVC プロファイルのルールを設定します。
add	AVC プロファイルのルールを作成します。
remove	AVC プロファイルのルールを削除します。
application	ドロップまたはマークする必要のあるアプリケーションを指定します。
application_name	アプリケーションの名前。ライセンス名は最大 32 文字の英数字で、大文字と小文字を区別します。
drop	選択したアプリケーションに対応するアップストリームおよびダウンストリーム パケットをドロップします。
mark	ドロップダウン リストで指定した DiffServ コード ポイント（DSCP）の値を使用して、選択したアプリケーションに対応するアップストリームおよびダウンストリーム パケットをマークします。DSCP 値を使用して、QoS レベルに基づいて Differentiated Services を提供できます。
dscp	インターネット上で QoS を定義するために使用されるパケット ヘッダー コード。範囲は 0 ～ 63 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
7.4	このコマンドが導入されました。

次に、AVC プロファイルのルールを設定する例を示します。

```
(Cisco Controller) > config avc profile avcprofile1 rule add application gmail mark 10
```

関連コマンド

config avc profile delete

config avc profile create

config wlan avc

show avc profile

show avc applications

show avc statistics

debug avc error

debug avc events

config band-select cycle-count

帯域幅選択プローブ サイクル カウントを設定するには、**config band-select cycle-count** コマンドを使用します。

config band-select cycle-count *count*

構文の説明

count	1 ～ 10 の間のサイクル カウントの値。

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。

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、帯域幅選択のプローブ サイクルカウントを 8 に設定する例を示します。

```
(Cisco Controller) > config band-select cycle-count 8
```

関連コマンド

config band-select cycle-threshold

config band-select expire

config band-select client-rssi

config band-select cycle-threshold

新しいスキャン サイクルの時間のしきい値を設定するには、**config band-select cycle-threshold** コマンドを使用します。

config band-select cycle-threshold *threshold*

構文の説明

threshold	1 ～ 1000 ミリ秒のサイクルしきい値の値。

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。

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、しきい値が 700 ミリ秒の新しいスキャン サイクルの時間のしきい値を設定する例を示します。

```
(Cisco Controller) > config band-select cycle-threshold 700
```

関連コマンド

config band-select cycle-count

config band-select expire

config band-select client-rssi

config band-select expire

帯域幅選択に対してエントリの期限切れを設定するには、**config band-select expire** コマンドを使用します。

config band-select expire {**suppression** | **dual-band**} *seconds*

構文の説明

suppression	抑制の期限切れを帯域幅選択に設定します。
dual-band	デュアル バンドの期限切れを帯域幅選択に設定します。
seconds	• 10 ～ 200 秒の抑制の値。 • 10 ～ 300 秒のデュアル バンドの値。

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。

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、抑制の期限切れを 70 秒に設定する例を示します。

```
(Cisco Controller) > config band-select expire suppression 70
```

関連コマンド

config band-select cycle-threshold

config band-select client-rssi

config band-select cycle-count

config band-select client-rssi

帯域幅選択に対して、クライアントの Received Signal Strength Indicator（RSSI）のしきい値を設定するには、**config band-select client-rssi** コマンドを使用します。

config band-select client-rssi *rssi*

構文の説明

rssi	20 ～ 90 のプローブに応答するクライアント RSSI の最小 dBM。

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。

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、帯域幅選択の RSSI しきい値を 70 に設定する例を示します。

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

関連コマンド

config band-select cycle-threshold

config band-select expire

config band-select cycle-count

config boot

Cisco ワイヤレス LAN コントローラのブート オプションを変更するには、**config boot** コマンドを使用します。

config boot {**primary** | **backup**}

構文の説明

primary	アクティブとしてプライマリ イメージを設定します。
backup	アクティブとしてバックアップ イメージを設定します。

コマンド デフォルト

デフォルトのブート オプションは **primary** 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。

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。

使用上のガイドライン

各 Cisco ワイヤレス LAN コントローラは、プライマリの、最後にロードされたオペレーティング システムイメージ（OS）をブートオフしたり、バックアップの、以前にロードされた OS イメージをブートオフしたりできます。

次に、LAN コントローラがプライマリの、最後にロードされたイメージをブートオフできるように、プライマリ イメージをアクティブとして設定する例を示します。

```
(Cisco Controller) > config boot primary
```

次に、LAN コントローラがバックアップの、以前にロードされた OS イメージをブートオフできるように、バックアップ イメージをアクティブとして設定する例を示します。

```
(Cisco Controller) > config boot backup
```

関連コマンド

show boot

config call-home contact email address

Call Home 連絡先の電子メール アドレスを設定するには、**config call-home contact-email-addr** コマンドを使用します。

config call-home contact-email-addr *email-address*

構文の説明

email-address	Call Home 連絡先の電子メール アドレス。

コマンド履歴

リリース	変更内容
8.2	このコマンドが導入されました。

次に、Call Home 連絡先の電子メール アドレスを追加する例を示します。

```
(Cisco Controller) >config call-home contact-email-addr device1@example1.com
```

config call-home events

Call Homeイベント レポートを有効または無効にするには、**call-home events** コマンドを使用します。

config call-home events {**enable** | **disable**}

構文の説明

enable	Call Homeイベント レポートを有効にします。
disable	Call Homeイベント レポートを無効にします。

コマンド デフォルト

Enable

コマンド履歴

リリース	変更内容
8.2	このコマンドが導入されました。

次に、Call Home イベント レポートを無効にする例を示します。

```
(Cisco Controller) > config call-home events disable
```

config call-home http-proxy ipaddr

レポートの HTTP プロキシ アドレスを設定するには、**config call-home http-proxy ipaddr** コマンドを使用します。

config call-home http-proxy ipaddr *ip-address* **port** *port*

構文の説明

ip-address	HTTP プロキシ IP アドレス。
port	HTTP プロキシ ポート番号。

コマンド履歴

リリース	変更内容
8.2	このコマンドが導入されました。

次に、HTTP プロキシ IP アドレスを使用して Call Home を設定する例を示します。

```
(Cisco Controller) >config call-home http-proxy ipaddr 209.165.200.224 port 773
```

config call-home http-proxy ipaddr 0.0.0.0

レポートの HTTP プロキシ設定をリセットするには、**config call-home http-proxy ipaddr 0.0.0.0** コマンドを使用します。

config call-home http-proxy ipaddr *0.0.0.0*

構文の説明

0.0.0.0	HTTP プロキシ設定をリセットします。

コマンド履歴

リリース	変更内容
8.2	このコマンドが導入されました。

次に、Call Home HTTP プロキシ設定をリセットする例を示します。

```
(Cisco Controller) >config call-home http-proxy ipaddr 0.0.0.0
```

config call-home profile

Call Home プロファイルの作成および更新するには、**config call-home profile** コマンドを使用します。

config call-home profile {**create** | **update** } *profile-name* {**sm-license-data** | **all** | **call-home-data**}{**short-text** | **long-text** | **xml** } *url*

構文の説明

create	Call Home プロファイルを作成します
update	Call Home プロファイルを更新します
sm-license-data	スマートライセンス レポート プロファイルを設定します。
all	すべてのモジュールのレポート プロファイルを設定します。
call-home-data	Call Home データ レポート プロファイルを設定します。
short-text	ショートテキスト形式のデータ レポートを設定します。
long-text	ロングテキスト形式のデータ レポートを設定します。
xml	XML 形式のデータ レポートを設定します。
url	URL 名

コマンド履歴

リリース	変更内容
8.2	このコマンドが導入されました。

次に、XML 形式の Call Home レポート プロファイルを作成する例を示します。

```
(Cisco Controller) > config call-home profile create example-profile sm-license-data xml
 internal.example.com
```

config call-home profile delete

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

config call-home profile delete *profile-name*

構文の説明

profile-name	Call Home プロファイルは削除されます。

コマンド履歴

リリース	変更内容
8.2	このコマンドが導入されました。

次に、Call Home プロファイルを削除する例を示します。

```
(Cisco Controller) > config call-home profile delete example-profile
```

config call-home profile status

ユーザ プロファイルを有効または無効にするには、**config call-home profile status** コマンドを使用します。

config call-home profile status {**enable** | **disable**}

構文の説明

enable	Call Home プロファイルのステータスを有効にします。
disable	Call Home プロファイルのステータスを無効にします。

コマンド履歴

リリース	変更内容
8.2	このコマンドが導入されました。

次に、Call Home プロファイルを無効にする例を示します。

```
(Cisco Controller) >config call-home profile status disable
```

config call-home reporting

データ レポートのプライバシー レベルを設定するには、**config call-home reporting data-privacy level** コマンドを使用します。

config call-home reporting data-privacy level {**normal** | **high**}**hostname** ホスト名

構文の説明

normal	すべての標準レベル コマンドをスクラビング処理します。
high	標準レベル コマンドと IP ドメイン名および IP アドレスのコマンドをスクラビング処理します。
hostname	すべての高レベル コマンドとホスト名のコマンドをスクラビング処理します。

コマンド履歴

リリース	変更内容
8.2	このコマンドが導入されました。

次に、標準プライバシー レベルを設定する例を示します。

```
(Cisco Controller) >config call-home reporting data-privacy- level normal hostname
internal.example.com
```

config call-home tac-profile

TAC プロファイルを有効または無効にするには、**config call-home tac-profile status** コマンドを使用します。

config call-home tac-profile status {**enable** | **disable**}

構文の説明

enable	Call Home TAC プロファイルを有効にします。
disable	Call Home TAC プロファイルを無効にします。

コマンド デフォルト

Enable

コマンド履歴

リリース	変更内容
8.2	このコマンドが導入されました。

次に、Call Home TAC プロファイルを無効にする例を示します。

```
(Cisco Controller) >config call-home tac-profile status disable
```

config cdp

コントローラ上に Cisco Discovery Protocol（CDP）を設定するには、**config cdp** コマンドを使用します。

config cdp {**enable** | **disable** | **advertise-v2** {**enable** | **disable**} | **timer***seconds* | **holdtime** *holdtime_interval*}

構文の説明

enable	コントローラで CDP をイネーブルにします。
disable	コントローラで CDP をディセーブルにします。
advertise-v2	CDP バージョン 2 のアドバタイズメントを設定します。
timer	CDP メッセージが生成される間隔を設定します。
seconds	CDP メッセージが生成される間隔。範囲は 5 ～ 254 秒です。
holdtime	生成された CDP パケット内の存続可能時間の値としてアドバタイズされる時間を設定します。
holdtime_interval	最大ホールドタイマー値。範囲は 10 ～ 255 秒です。

コマンド デフォルト

CDP タイマーのデフォルト値は 60 秒です。

CDP 保持時間のデフォルト値は 180 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。

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、CDP 最大ホールドタイマーを 150 秒に設定する例を示します。

```
(Cisco Controller) > config cdp timer 150
```

関連コマンド

config ap cdp

show cdp

show ap cdp

config certificate

Secure Sockets Layer（SSL）証明書を設定するには、**config certificate** コマンドを使用します。

config certificate {**generate** {**csr-webadmin** | **csr-webauth** | **webadmin** | **webauth**}

構文の説明

generate	認証証明書生成の設定を指定します。
csr-webadmin	新しい Web 管理証明書署名要求を作成します。
csr-webauth	新しい Web 認証署名要求を作成します。
webadmin	新しい Web 管理証明書を生成します。
webauth	新しい Web 認証証明書を生成します。

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。
8.3	このコマンドはリリース 8.3 で新しいキーワードによって機能が拡張されました。

次に、新しい Web 管理 SSL 証明書を生成する例を示します。

```
(Cisco Controller) > config certificate generate webadmin
Creating a certificate may take some time. Do you wish to continue? (y/n)
```

config certificate lsc

ローカルで有効な証明書（LSC）を設定するには、**config certificate lsc** コマンドを使用します。

config certificate lsc {**enable** | **disable** | **ca-server** *http://url:port/path* | **ca-cert** {**add** | **delete**} | **subject-params** *country state city orgn dept email* | **other-params** *keysize*} | **ap-provision** {**auth-list** {**add** | **delete**} *ap_mac* | **revert-cert** *retries*}

構文の説明

enable	コントローラ上で LSC 証明書をイネーブルにします。
disable	コントローラ上で LSC 証明書をディセーブルにします。
ca-server	認証局（CA）サーバ設定を指定します。
http://url:port/path	CA サーバのドメイン名または IP アドレス。
ca-cert	CA 証明書データベースの設定を指定します。
add	CA サーバから CA 証明書を取得し、コントローラの証明書データベースに追加します。
delete	コントローラの証明書データベースから CA 証明書を削除します。
subject-params	デバイス証明書の設定を指定します。
country state city orgn dept email	認証局の国、州、市、組織、部門、および電子メール。 （注） Common Name（CN）は、現在の MIC/SSC 形式である *Cxxxx-MacAddr* を使用して、アクセスポイント上で自動的に生成されます。ここで、*xxxx* は製品番号です。
other-params	デバイスの証明書キーのサイズ設定を指定します。
keysize	384 ～ 2048 の値（ビット単位）。デフォルト値は 2048 です。
ap-provision	アクセスポイントプロビジョニングリストの設定を指定します。

auth-list	プロビジョニング リストの許可設定を指定します。
ap_mac	プロビジョニング リストに追加する、またはプロビジョニング リストから削除するアクセス ポイントの MAC アドレス。
revert-cert	デフォルトの証明書に戻る前にアクセス ポイントが LSC を使用してコントローラへの接続を試行する回数。
retries	0 ～ 255 の値。デフォルト値は 3 です。 （注） 再試行回数を 0 に設定した場合、アクセス ポイントが LSC 使用によるコントローラへの join に失敗すると、このアクセス ポイントはデフォルトの証明書を使用したコントローラへの join を試みません。初めて LSC を設定する場合は、ゼロ以外の値を設定することが推奨されます。

コマンド デフォルト

keysize のデフォルト値は 2048 ビットです。*retries* のデフォルト値は 3 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 つの CA サーバだけを設定できます。別の CA サーバを設定するには、**config certificate lsc ca-server delete** コマンドを使用して設定済みの CA サーバを削除してから、別の CA サーバを設定します。

アクセス ポイント プロビジョニング リストを設定する場合は、AP プロビジョニングを有効にしたときに（手順8）プロビジョニング リストのアクセス ポイントだけがプロビジョニングされます。アクセス ポイント プロビジョン リストを設定しない場合、コントローラに接続する MIC または SSC 証明書を持つすべてのアクセス ポイントが LSC でプロビジョニングされます。

次に、LSC 機能を有効にする例を示します。

```
(Cisco Controller) >config certificate lsc enable
```

次に、認証局（CA）サーバ設定の LSC 設定をイネーブルにする例を示します。

```
(Cisco Controller) >config certificate lsc ca-server http://10.0.0.1:8080/caserver
```

次に、CA サーバから CA 証明書を取得し、コントローラの証明書データベースにそれを追加する例を示します。

```
(Cisco Controller) >config certificate lsc ca-cert add
```

次に、2048 ビットのキー サイズの LSC 証明書を設定する例を示します。

```
(Cisco Controller) >config certificate lsc keysize 2048
```

config certificate ssc

自己署名証明書（SSC）で証明書を設定するには、**config certificate ssc** コマンドを使用します。

config certificate ssc hash validation {**enable** | **disable**}

構文の説明

hash	SSC のハッシュ キーを設定します。
validation	SSC 証明書のハッシュ検証を設定します。
enable	SSC 証明書のハッシュ検証をイネーブルにします。
disable	SSC証明書のハッシュ検証をディセーブルにします。

コマンド デフォルト

SSC 証明書は、デフォルトでは有効になっています。

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。

使用上のガイドライン

SSC ハッシュ検証をイネーブルにすると、AP は仮想コントローラの SSC 証明書を検証します。AP が SSC 証明書を検証するときに、仮想コントローラのハッシュ キーが、フラッシュに保存されるハッシュ キーと一致するかどうかが確認されます。一致が見つかると、検証は成功し、APはRun状態に移行します。一致がない場合、検証は失敗し、APはコントローラから切断され、ディスカバリ プロセスを再起動します。デフォルトでは、ハッシュ検証は有効です。AP は仮想コントローラに関連付ける前に、フラッシュの仮想コントローラのハッシュ キーが必要です。SSC のハッシュ検証をディセーブルにすると、AP はハッシュ検証をバイパスし、Run 状態に直接移動します。

APS は物理コントローラに関連付けることが可能で、ハッシュ キーをダウンロードし、次に仮想コントローラに関連付けます。APが物理コントローラに関連付けられている場合に、ハッシュ検証がディセーブルであると、ハッシュ検証なしで仮想コントローラを接続します。

次に、SSC 証明書のハッシュ検証を有効にする例を示します。

```
(Cisco Controller) > config certificate ssc hash validation enable
```

関連コマンド

show certificate ssc

show mobility group member

config mobility group member hash

config certificate

show certificate compatibility

show certificate lsc

show certificate summary

show local-auth certificates

config certificate use-device-certificate webadmin

Web 管理にデバイス証明書を使用するには、**config certificate use-device-certificate webadmin** コマンドを使用します。

config certificate use-device-certificate webadmin

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。

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、Web 管理にデバイス証明書を使用する例を示します。

```
(Cisco Controller) > config certificate use-device-certificate webadmin
Use device certificate for web administration. Do you wish to continue? (y/n) y
Using device certificate for web administration.
Save configuration and restart controller to use new certificate.
```

関連コマンド

config certificate

show certificate compatibility

show certificate lsc

show certificate ssc

show certificate summary

show local-auth certificates

config client ccx clear-reports

クライアントのレポート情報をクリアするには、**config client ccx clear-reports** コマンドを使用します。

config client ccx clear-reports *client_mac_address*

構文の説明

client_mac_address	クライアントの 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、クライアントの MAC アドレス 00:1f:ca:cf:b6:60 のレポート情報をクリアする例を示します。

```
(Cisco Controller) >config client ccx clear-reports 00:1f:ca:cf:b6:60
```

config client ccx clear-results

コントローラ上のテスト結果をクリアするには、**config client ccx clear-results** コマンドを使用します。

config client ccx clear-results *client_mac_address*

構文の説明

client_mac_address	クライアントの 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、クライアントの MAC アドレス 00:1f:ca:cf:b6:60 のテスト結果をクリアする例を示します。

```
(Cisco Controller) >config client ccx clear-results 00:1f:ca:cf:b6:60
```

config client ccx default-gw-ping

デフォルトのゲートウェイ pingテストの実行要求をクライアントに送信するには、**config client ccx default-gw-ping** コマンドを使用します。

config client ccx default-gw-ping *client_mac_address*

構文の説明

client_mac_address	クライアントの 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。

使用上のガイドライン

このテストでは、クライアントは診断チャネルを使用する必要はありません。

次に、クライアント 00:0b:85:02:0d:20 に要求を送信して、デフォルト ゲートウェイの ping テストを実行する例を示します。

```
(Cisco Controller) >config client ccx default-gw-ping 00:0b:85:02:0d:20
```

config client ccx dhcp-test

DHCP テストの実行要求をクライアントに送信するには、**config client ccx dhcp-test** コマンドを使用します。

config client ccx dhcp-test *client_mac_address*

構文の説明

client_mac_address	クライアントの 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。

使用上のガイドライン

このテストでは、クライアントは診断チャネルを使用する必要はありません。

次に、クライアント 00:E0:77:31:A3:55 に要求を送信して、DHCP テストを実行する例を示します。

```
(Cisco Controller) >config client ccx dhcp-test 00:E0:77:31:A3:55
```

config client ccx dns-ping

ドメイン ネーム システム（DNS）サーバ IP アドレス ping テストの実行要求をクライアントに送信するには、**config client ccx dns-ping** コマンドを使用します。

config client ccx dns-ping *client_mac_address*

構文の説明

client_mac_address	クライアントの 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。

使用上のガイドライン

このテストでは、クライアントは診断チャネルを使用する必要はありません。

次に、クライアントに要求を送信して、DNS サーバの IP アドレスの ping テストを実行する例を示します。

```
(Cisco Controller) >config client ccx dns-ping 00:E0:77:31:A3:55
```

config client ccx dns-resolve

指定されたホスト名に対するドメイン ネーム システム（DNS）名前解決テストの実行要求をクライアントに送信するには、**config client ccx dns-resolve** コマンドを使用します。

config client ccx dns-resolve *client_mac_address host_name*

構文の説明

client_mac_address	クライアントの MAC アドレス。
host_name	クライアントのホスト名。

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

このテストでは、クライアントは診断チャネルを使用する必要はありません。

次に、クライアント 00:E0:77:31:A3:55 に要求を送信して、指定したホスト名に対して DNS 名前解決テストを実行する例を示します。

```
(Cisco Controller) >config client ccx dns-resolve 00:E0:77:31:A3:55 host_name
```

config client ccx get-client-capability

機能情報の送信要求をクライアントに送信するには、**config client ccx get-client-capability** コマンドを使用します。

config client ccx get-client-capability *client_mac_address*

構文の説明

client_mac_address	クライアントの 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、クライアント 172.19.28.40 に機能情報の送信要求を送信する例を示します。

```
(Cisco Controller) >config client ccx get-client-capability 172.19.28.40
```

config client ccx get-manufacturer-info

製造元情報の送信要求をクライアントに送信するには、**config client ccx get-manufacturer-info** コマンドを使用します。

config client ccx get-manufacturer-info *client_mac_address*

構文の説明

client_mac_address	クライアントの 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、クライアント 172.19.28.40 に製造元情報を送信するように要求する例を示します。

```
(Cisco Controller) >config client ccx get-manufacturer-info 172.19.28.40
```

config client ccx get-operating-parameters

現在の動作パラメータの送信要求をクライアントに送信するには、**config client ccx get-operating-parameters** コマンドを使用します。

config client ccx get-operating-parameters *client_mac_address*

構文の説明

client_mac_address	クライアントの 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、クライアント 172.19.28.40 に現在の動作パラメータの送信要求を送信する例を示します。

```
(Cisco Controller) >config client ccx get-operating-parameters 172.19.28.40
```

config client ccx get-profiles

プロファイルの送信要求をクライアントに送信するには、**config client ccx get-profiles** コマンドを使用します。

config client ccx get-profiles *client_mac_address*

構文の説明

client_mac_address	クライアントの 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、クライアント 172.19.28.40 にプロファイルの詳細の送信要求を送信する例を示します。

```
(Cisco Controller) >config client ccx get-profiles 172.19.28.40
```

config client ccx log-request

特定のクライアントデバイスのCisco Client Extensions（CCX）ログ要求を設定するには、**config client ccx log-request** コマンドを使用します。

config client ccx log-request {**roam** | **rsna** | **syslog**} *client_mac_address*

構文の説明

roam	（任意）クライアント CCX ローミング ログを指定する要求を指定します。
rsna	（任意）クライアント CCX RSNA ログを指定する要求を指定します。
syslog	（任意）クライアント CCX システム ログを指定する要求を指定します。
client_mac_address	クライアントの 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、クライアント CCS システム ログの指定要求を指定する例を示します。

```
(Cisco Controller) >config client ccx log-request syslog 00:40:96:a8:f7:98
Tue Oct 05 13:05:21 2006
SysLog Response LogID=1: Status=Successful
Event Timestamp=121212121212
Client SysLog = 'This is a test syslog 2'
Event Timestamp=121212121212
Client SysLog = 'This is a test syslog 1'
Tue Oct 05 13:04:04 2006
SysLog Request LogID=1
```

次に、クライアント CCX ローミング ログを指定する例を示します。

```
(Cisco Controller) >config client ccx log-request roam 00:40:96:a8:f7:98
Thu Jun 22 11:55:14 2006
Roaming Response LogID=20: Status=Successful
Event Timestamp=121212121212
Source BSSID=00:40:96:a8:f7:98, Target BSSID=00:0b:85:23:26:70,
Transition Time=100(ms)
Transition Reason: Unspecified Transition Result: Success
Thu Jun 22 11:55:04 2006
Roaming Request LogID=20
Thu Jun 22 11:54:54 2006
Roaming Response LogID=19: Status=Successful
Event Timestamp=121212121212
Source BSSID=00:40:96:a8:f7:98, Target BSSID=00:0b:85:23:26:70,
Transition Time=100(ms)
Transition Reason: Unspecified Transition Result: Success
```

```
Thu Jun 22 11:54:33 2006  Roaming Request LogID=19
```

次に、クライアント CCX RSNA ログを指定する例を示します。

```
(Cisco Controller) >config client ccx log-request rsna 00:40:96:a8:f7:98
Tue Oct 05 11:06:48 2006
RSNA Response LogID=2: Status=Successful
Event Timestamp=242424242424
Target BSSID=00:0b:85:23:26:70
RSNA Version=1
Group Cipher Suite=00-x0f-ac-01
Pairwise Cipher Suite Count = 2
Pairwise Cipher Suite 0 = 00-0f-ac-02
Pairwise Cipher Suite 1 = 00-0f-ac-04
AKM Suite Count = 2
KM Suite 0 = 00-0f-ac-01
KM Suite 1 = 00-0f-ac-02
SN Capability = 0x1
PMKID Count = 2
PMKID 0 = 01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16
PMKID 1 = 0a 0b 0c 0d 0e 0f 17 18 19 20 1a 1b 1c 1d 1e 1f
802.11i Auth Type: EAP_FAST
RSNA Result: Success
```

config client ccx send-message

メッセージをクライアントに送信するには、**config client ccx send-message** コマンドを使用します。

config client ccx send-message *client_mac_address message_id*

構文の説明

client_mac_address	クライアントの MAC アドレス。

message_id

次のいずれかを含むメッセージ タイプ。

- 1：SSID が無効です。
- 2：ネットワーク設定が無効です。
- 3：WLANの信頼性に不一致があります。
- 4：ユーザの資格情報が間違っています。
- 5：サポートにお問い合わせください。
- 6：問題は解決されました。
- 7：問題は解決されていません。
- 8：もう一度後で作業を行ってください。
- 9：示された問題を修正してください。
- 10：ネットワークにより、トラブルシューティングが拒否されました。
- 11：クライアント レポートを取得中です。
- 12：クライアント ログを取得中です。
- 13：取得が完了しました。
- 14：アソシエーション テストを開始します。
- 15：DHCP テストを開始します。
- 16：ネットワーク接続テストを開始します。
- 17：DNS ping テストを開始します。
- 18：名前解決テストを開始します。
- 19：802.1X 認証テストを開始します。
- 20：クライアントを特定のプロファイルにリダイレクトしています。
- 21：テストが完了しました。
- 22：テストに合格しました。
- 23：テストに失敗しました。
- 24：通常の操作を再開するには、診断チャネル操作をキャンセルするか、WLAN プロファイルを選択してください。

	• 25：クライアントにより、ログの取得が拒否されました。 • 26：クライアントにより、クライアントレポートの取得が拒否されました。 • 27：クライアントにより、テスト要求が拒否されました。 • 28：無効なネットワーク（IP）設定です。 • 29：ネットワークで機能停止または問題が発生しています。 • 30：予定された保守期間です。 （次ページに続く）
message_type（続き）	• 31：WLAN セキュリティ方式が正しくありません。 • 32：WLAN 暗号化方式が正しくありません。 • 33：WLAN 認証方式が正しくありません。

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、メッセージ user-action-required を使用して、クライアント MAC アドレス 172.19.28.40 にメッセージを送信する例を示します。

```
(Cisco Controller) >config client ccx send-message 172.19.28.40 user-action-required
```

config client ccx stats-request

統計要求を送信するには、**config client ccx stats-request** コマンドを使用します。

config client ccx stats-request *measurement_duration* {**dot11** | **security**} *client_mac_address*

構文の説明

measurement_duration	秒単位の測定期間。
dot11	（任意）dot11 カウンタを指定します。
security	（任意）セキュリティカウンタを指定します。
client_mac_address	クライアントの 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、dot11 カウンタの設定を指定する例を示します。

```
(Cisco Controller) >config client ccx stats-request 1 dot11 00:40:96:a8:f7:98
Measurement duration = 1
dot11TransmittedFragmentCount       = 1
dot11MulticastTransmittedFrameCount = 2
dot11FailedCount                    = 3
dot11RetryCount                     = 4
dot11MultipleRetryCount             = 5
dot11FrameDuplicateCount            = 6
dot11RTSSuccessCount                = 7
dot11RTSFailureCount                = 8
dot11ACKFailureCount                = 9
dot11ReceivedFragmentCount          = 10
dot11MulticastReceivedFrameCount    = 11
dot11FCSErrorCount                  = 12
dot11TransmittedFrameCount          = 13
```

config client ccx test-abort

現在のテストの中止要求をクライアントに送信するには、**config client ccx test-abort** コマンドを使用します。

config client ccx test-abort *client_mac_address*

構文の説明

client_mac_address	クライアントの 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。

使用上のガイドライン

一度に保留できるテストは 1 つだけです。

次に、クライアントに要求を送信して、現在のテストの設定を中止する例を示します。

```
(Cisco Controller) >config client ccx test-abort 11:11:11:11:11:11
```

config client ccx test-association

アソシエーション テストの実行要求をクライアントに送信するには、**config client ccx test-association** コマンドを使用します。

config client ccx test-association *client_mac_address ssid bssid* **802.11**{**a** | **b** | **g**} *channel*

構文の説明

client_mac_address	クライアントの MAC アドレス。
ssid	ネットワーク名。
bssid	Basic SSID。
802.11a	802.11a ネットワークを指定します。
802.11b	802.11b ネットワークを指定します。
802.11g	802.11g ネットワークを指定します。
channel	チャネル番号。

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 MAC アドレス 00:0E:77:31:A3:55 に要求を送信して、基本 SSID アソシエーション テストを実行する例を示します。

```
(Cisco Controller) >config client ccx test-association 00:E0:77:31:A3:55 ssid bssid
802.11a
```

config client ccx test-dot1x

802.1x テストの実行要求をクライアントに送信するには、**config client ccx test-dot1x** コマンドを使用します。

config client ccx test-dot1x *client_mac_address profile_id bssid* **802.11** {**a** | **b** | **g**} *channel*

構文の説明

client_mac_address	クライアントの MAC アドレス。
profile_id	テスト プロファイル名。
bssid	Basic SSID。
802.11a	802.11a ネットワークを指定します。
802.11b	802.11b ネットワークを指定します。
802.11g	802.11g ネットワークを指定します。
channel	チャネル番号。

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、クライアントに要求を送信して、プロファイル名 profile_01 で 802.11b テストを実行する例を示します。

```
(Cisco Controller) >config client ccx test-dot1x 172.19.28.40 profile_01 bssid 802.11b
```

config client ccx test-profile

プロファイル リダイレクト テストの実行要求をクライアントに送信するには、**config client ccx test-profile** コマンドを使用します。

config client ccx test-profile *client_mac_address profile_id*

構文の説明

client_mac_address	クライアントの MAC アドレス。
profile_id	テスト プロファイル名。 （注） *profile_id* には、必ずクライアント レポートが有効なクライアント プロファイルのプロファイル ID 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、クライアントに要求を送信して、プロファイル名 profile_01 でプロファイル リダイレクト テストを実行する例を示します。

```
(Cisco Controller) >config client ccx test-profile 11:11:11:11:11:11 profile_01
```

config client deauthenticate

クライアントを接続解除するには、**config client deauthenticate** コマンドを使用します。

config client deauthenticate {*MAC* | *IPv4/v6_address* | *user_name*}

構文の説明

MAC	Client MAC address.
IPv4/v6_address	IPv4 または IPv6 アドレス。
user_name	クライアント 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
7.6	このコマンドは、リリース 7.6 以前のリリースで導入されました。

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、MAC アドレスを使用してクライアントを認証解除する例を示します。

```
(Cisco Controller) >config client deauthenticate 11:11:11:11:11:11
```

config client location-calibration

リンク集約を設定するには、**config client location-calibration** コマンドを使用します。

config client location-calibration {**enable** *mac_address interval* | **disable** *mac_address*}

構文の説明

enable	（任意）クライアントのロケーション調整をイネーブルにするよう指定します。
mac_address	クライアントの MAC アドレス。
interval	秒単位の測定間隔。
disable	（任意）クライアントのロケーション調整をディセーブルにするよう指定します。

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。

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、45 秒の測定間隔で、クライアント 37:15:85:2a のクライアント ロケーション調整を無効にする例を示します。

```
(Cisco Controller) >config client location-calibration enable 37:15:86:2a:Bc:cf 45
```

config client profiling delete

クライアント プロファイルを削除するには、**config client profiling** コマンドを使用します。

config client profiling delete {*mac_address*}

構文の説明

mac_address	クライアントの MAC アドレス。

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。

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、クライアント プロファイルを削除する例を示します。

```
(Cisco Controller) >config client profiling delete 37:15:86:2a:Bc:cf
```

（注） 上記のコマンドを実行すると、デバイス タイプが「Unknown」に変更されます。クライアントは削除されませんが、代わりにクライアントのプロファイル情報が削除され、クライアントは依然として関連付けられているために保持されます。Cisco WLC のアーキテクチャ上の制限により、CLI の確認メッセージは表示されません。

config cloud-services cmx

CMX クラウド サービスを有効または無効にするには、**config cloud-services cmx** コマンドを使用します。

config cloud-services cmx {**enable**|**disable**}

構文の説明

enable	CMX クラウド サービスを有効にします。
disable	CMX クラウド サービスを無効にします。

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
8.3	このコマンドが導入されました。

次に、CMX クラウド サービスを有効にする例を示します。

```
(Cisco Controller) > config cloud-services cmx enable
```

config cloud-services server url

クラウド サーバの URLを設定するには、**config cloud-services server url** コマンドを使用します。

config cloud-services server url *url*

構文の説明		
	url	クラウド サーバの URL 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
8.3	このコマンドが導入されました。

次に、クラウド サーバの URL を設定する例を示します。

```
(Cisco Controller) >config cloud-services server url www.example.com
```

config cloud-services server id-token

クラウドサーバの ID トークンを設定するには、 **config cloud-services server id-token** コマンドを使用します。

config cloud-services server id-token *id-token*

構文の説明

id-token	クラウドサーバの ID トークンを入力します。

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
8.3	このコマンドが導入されました。

次に、クラウド サーバの ID トークンを設定する例を示します。

```
(Cisco Controller) >config cloud-services server id-token dzypisQ2#bo$iAQM
```

config coredump

クラッシュ後のコントローラによるコア ダンプ ファイルの生成を有効または無効にするには、**config cordump** コマンドを使用します。

config coredump {**enable** | **disable**}

構文の説明

enable	コントローラによるコア ダンプ ファイルの生成をイネーブルにします。
disable	コントローラによるコア ダンプ ファイルの生成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。

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、クラッシュ後のコントローラによるコア ダンプ ファイルの生成を有効にする例を示します。

```
(Cisco Controller) > config coredump enable
```

関連コマンド

config coredump ftp

config coredump username

show coredump summary

config coredump ftp

クラッシュ後に FTP サーバにコントローラのコア ダンプ ファイルを自動的にアップロードするには、**config coredump ftp** コマンドを使用します。

config coredump ftp *server_ip_address filename*

構文の説明

server_ip_address	コントローラがコア ダンプ ファイルを送信する FTP サーバの IP アドレス。
filename	コントローラのコア ダンプ ファイルに割り当てられた名前。

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。
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。

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。

使用上のガイドライン

このコマンドを使用するには、コントローラが FTP サーバに到達できる必要があります。

次に、*core_dump_controller* という名前のコア ダンプ ファイルをネットワーク アドレス *192.168.0.13* で FTP サーバにアップロード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 coredump ftp 192.168.0.13 core_dump_controller
```

関連コマンド

config coredump

config coredump username

show coredump summary

config coredump username

クラッシュ後にコントローラのコア ダンプ ファイルをアップロードするときの FTP サーバのユーザ名とパスワードを指定するには、**config coredump username** コマンドを使用します。

config coredump username *ftp_username* **password** *ftp_password*

構文の説明

ftp_username	FTP サーバ ログイン ユーザ名。
ftp_password	FTP サーバ ログイン パスワード。

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

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。

使用上のガイドライン

このコマンドを使用するには、コントローラが FTP サーバに到達できる必要があります。

次に、コア ダンプ ファイル アップロードに対して、FTP サーバにユーザ名 *admin* とパスワード *adminpassword* を指定する例を示します。

```
(Cisco Controller) > config coredump username admin password adminpassword
```

関連コマンド

config coredump ftp

config coredump

show coredump summary

config country

コントローラの国コードを設定するには、**config country** コマンドを使用します。

config country *country_code*

構文の説明

country_code	2 文字または 3 文字の国コード。

コマンド デフォルト

us（米国の国コード）。

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。

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。

使用上のガイドライン

Cisco WLC は、ネットワーク管理者または資格のある IP プロフェッショナルがインストールしてください。その際、正しい国コードを選択する必要があります。インストール後は、法的な規制基準を遵守するためおよび、適切なユニット機能を保証するために、ユニットへのアクセスはパスワードで保護する必要があります。最新の国コードおよび規制区域については、関連する製品マニュアルを参照してください。

サポートされている国のリストを表示するには、**show country** コマンドを使用できます。

次に、コントローラの国コードを DE に設定する例を示します。

```
(Cisco Controller) >config country DE
```

config cts

Cisco WLC で Cisco TrustSec を有効または無効にするには、**config cts** コマンドを使用します。

config cts {**enable** | **disable**}

構文の説明

enable	Cisco WLC で Cisco TrustSec を有効にします。
disable	Cisco WLC で Cisco TrustSec を無効にします。

コマンド デフォルト

デフォルトでは、Cisco TrustSec は無効状態になっています。

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。

config cts ap

AP でのインライン タギングとセキュリティ グループ アクセス コントロール リスト（SGACL）適用を設定するには、**config cts ap** コマンドを使用します。

config cts ap{**inline-tagging** | **sgacl-enforcement**} {**enable** | **disable**} {*ap-name* | **all**}

構文の説明

inline-tagging	すべての AP または特定の AP でのインライン タギングを設定します。
sgacl-enforcement	すべての AP または特定の AP での SGACL 適用を設定します。
enable	指定した機能を有効にします。
disable	指定した機能を無効にします。
ap-name	指定した機能を設定する必要がある AP の名前。
all	Cisco WLC に関連付けられているすべての AP の指定した機能を設定します。

コマンド デフォルト

デフォルトでは、インライン タギングと SGACL 適用の両方が無効状態になっています。

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。

使用上のガイドライン

- インライン タギングは、FlexConnect モードの AP でのみサポートされます。
- インライン タギングは、Flex + ブリッジ 802.11ac Lightweight AP ではサポートされていません。
- インライン タギングと、SGACL のダウンロードや適用は、5508、WiSM2、8510、7510、および vWLC の各 Cisco WLC ではサポートされていません。
- すべての AP に対して SGACL 適用を有効にすると、Cisco TrustSec オーバーライドが有効になっている AP を除くすべての AP に設定が適用されます。

次に、*cisco-flex-ap* という名前の AP でインライン タギングを有効にする例を示します。

```
(Cisco Controller) >config cts ap inline-tagging enable cisco-flex-ap
```

次に、*cisco-flex-ap* という名前の AP で SGACL 適用を有効にする例を示します。

```
(Cisco Controller) >config cts ap sgacl-enforcement enable cisco-flex-ap
```

config cts inline-tag

Cisco WLC の Cisco TrustSec インライン タギングを設定するには、**config cts inline-tag** コマンドを使用します。

config cts inline-tag {**enable** | **disable**}

構文の説明

inline-tag	Cisco WLC のインライン タギングを設定します。
enable	インライン タギングを有効にします。
disable	インライン タギングを無効にします。

コマンド デフォルト

デフォルトでは、インライン タギングは無効状態になっています。

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。

使用上のガイドライン

インライン タギングは、5508、WiSM2、8510、7510、および vWLC の各 Cisco WLC ではサポートされていません。

config cts ap override

AP の Cisco TrustSec オーバーライドを設定するには、**config cts ap override** コマンドを使用します。

config cts ap override {**enable** | **disable**} {*ap-name*}

構文の説明

enable	対応する AP の CTS オーバーライドを有効にします。
disable	対応する AP の CTS オーバーライドを無効にします。
ap-name	CTS オーバーライドを設定する必要がある AP の名前。

コマンド デフォルト

デフォルトでは、AP の CTS オーバーライドは無効状態になっています。

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。

使用上のガイドライン

すべての AP に対して SGACL の適用を有効にすると、CTS オーバーライドが有効になっている AP を除くすべての AP に設定が適用されます。

次に、*my-cisco-ap* という名前の AP で CTS オーバーライドを有効にする例を示します。

```
(Cisco Controller) >config cts ap override enable my-cisco-ap
```

config cts device-id

Cisco TrustSec デバイス ID を設定するには、**config cts device-id** コマンドを使用します。

config cts device-id *device-id* **password** *password*

構文の説明

device-id	CTS デバイス ID。
password	CTS デバイス ID のパスワード。

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
8.4	このコマンドが導入されました。

次に、CTS デバイス ID を設定する例を示します。

```
(Cisco Controller) > config cts device-id wlc-8540 password Cisco123
```

config cts refresh

Cisco TrustSec 環境データまたはセキュリティ グループ タグ（SGT）ポリシーを更新するには、**config cts refresh** コマンドを使用します。

config cts refresh {**environment-data**} | {**policy sgt** {**all** | *sgt-tag*}}

構文の説明

environment-data	CTS 環境データを更新します。
policy sgt	SGT ポリシーを更新します。
all	すべての SGT ポリシーを更新します。
sgt-tag	更新する CTS SGT タグ（整数）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、SGT ポリシー（*Default-65535*）を更新する例を示します。

```
(Cisco Controller) > config cts refresh policy sgt 65535
```

config cts sxp ap connection delete

すべての AP または特定の AP の SXPv4 接続ピアを削除するには、**config cts sxp ap connection delete** コマンドを使用します。

config cts sxp ap connection delete *ip-addr* {*cisco-ap* | **all**}

構文の説明

ip-addr	SXPv4 接続ピアの IP アドレス。
cisco-ap	AP の名前。
all	設定をすべての AP に適用します。

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
8.4	このコマンドが導入されました。

config cts sxp ap connection peer

すべての AP または特定の AP の SXPv4 ピア接続を設定するには、**config cts sxp ap connection peer** コマンドを使用します。

config cts sxp ap connection peer *ip-addr***password** {**default** | **none**} **mode** {**both** | **listener** | **speaker**} {*cisco-ap* | **all**}

構文の説明

ip-addr	SXPv4 接続ピアの IP アドレス。
password	SXPv4 ピア接続のパスワードを設定します。
default	MD5 暗号化にデフォルト パスワードを使用します。
none	パスワードの暗号化なしで SXPv4 を設定します。
time-in-seconds	SXPv4 接続の失敗後に接続を再試行するまでの時間。
mode	SXPv4 接続のモードを設定します。
both	デバイスを SXP のスピーカーとリスナーの両方として設定します。
listener	デバイスを SXP リスナーとして設定します。
speaker	デバイスを SXP スピーカーとして設定します。
cisco-ap	AP の名前。
all	対応する Cisco WLC に関連付けられているすべての AP に設定を適用します。

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
8.4	このコマンドが導入されました。

次に、Cisco WLC に関連付けられたすべての AP に対して、デフォルト パスワードによる SXPv4 ピア接続と、リスナー モードとスピーカー モードの両方での動作を設定する例を示します。

```
(Cisco Controller) > config cts sxp ap connection peer 10.165.200.224 password default
mode both all
```

config cts sxp ap default password

すべての AP または特定の AP の SXPv4 接続のデフォルト パスワードを設定するには、**config cts sxp ap default password** コマンドを使用します。

config cts sxp ap default password *password* {*cisco-ap* | **all**}

構文の説明

password	SXPv4 接続のデフォルト パスワード。
cisco-ap	AP の名前。
all	対応する Cisco WLC に関連付けられているすべての AP に設定を適用します。

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
8.4	このコマンドが導入されました。

config cts sxp ap listener

SXPv4 リスナー モードのパラメータを設定するには、**config cts sxp ap listener** コマンドを使用します。

config cts sxp ap listener hold-time *min-hold-time max-hold-time* {*cisco-ap* | **all**}

構文の説明

min-hold-time	SXPv4 接続の最小保留時間。
max-hold-time	SXPv4 接続の最大保留時間。
cisco-ap	SXPv4 を設定する必要がある AP の名前。
all	Cisco WLC に関連付けられているすべての AP に対して SXPv4 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
8.4	このコマンドが導入されました。

config cts sxp ap reconciliation period

SXPv4 接続調整期間を設定するには、**config cts sxp ap reconciliation period** コマンドを使用します。

config cts sxp ap reconciliation period *time-in-seconds* {*cisco-ap* | **all**}

構文の説明

time-in-seconds	SXPv4 接続が調整されるまでの時間間隔。有効な範囲は 0 ～ 64000 秒です。
cisco-ap	AP の名前。
all	Cisco WLC に関連付けられているすべての AP に設定を適用します。

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
8.4	このコマンドが導入されました。

config cts sxp ap retry period

SXPv4 接続再試行の間隔を設定するには、**config cts sxp ap retry period** コマンドを使用します。

config cts sxp ap retry period *time-in-seconds* {*cisco-ap* | **all**}

構文の説明

time-in-seconds	SXPv4 接続の失敗後に接続を再試行するまでの時間。有効な範囲は 0 ～ 64000 秒です。
cisco-ap	AP の名前。
all	対応する Cisco WLC に関連付けられているすべての AP に設定を適用します。

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
8.4	このコマンドが導入されました。

config cts sxp ap speaker

SXPv4 スピーカー モードのパラメータを設定するには、**config cts sxp ap speaker** コマンドを使用します。

config cts sxp ap speaker hold-time *time-in-seconds* {*cisco-ap* | **all**}

構文の説明

time-in-seconds	保持時間間隔（秒単位）。有効な範囲は 1 ～ 65534 秒です。
cisco-ap	SXPv4 を設定する必要がある AP の名前。
all	対応する Cisco WLC に関連付けられているすべての AP に対して SXPv4 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
8.4	このコマンドが導入されました。

config cts sxp

Cisco WLC で Cisco TrustSec SXP を有効または無効にするには、**config cts sxp** コマンドを使用します。

config cts sxp {**enable** | **disable**}

構文の説明

enable	Cisco WLC で Cisco TrustSec SXP を有効にします。
disable	Cisco WLC で Cisco TrustSec SXP 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。

config cts sxp connection

Cisco WLC での CTS SXP 接続を設定するには、**config cts sxp connection** コマンドを使用します。

config cts sxp connection {**delete** | **peer**} *ipv4-addr*

構文の説明

delete	SXP 接続を削除します。
peer	Cisco WLC が接続されるネクストホップスイッチを設定します。
ipv4-addr	SXP 接続の IPv4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。

config cts sxp default password

CTS SXP のデフォルト パスワードを設定するには、**config cts sxp default password** コマンドを使用します。

config cts sxp default password *password*

構文の説明

password	SXP メッセージの MD5 認証用のデフォルト パスワード。パスワードには、少なくとも 6 文字が必要です。

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。

config cts sxp retry period

CTS SXP 接続再試行の間隔を設定するには、**config cts sxp retry period** コマンドを使用します。

config cts sxp retry period *time-in-seconds*

構文の説明

time-in-seconds	CTS SXP 接続の失敗後に接続を再試行するまでの時間。有効な範囲は 0 ～ 64000 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。

config cts sxp version

CTS SXP 接続のバージョンを設定するには、**config cts sxp version** コマンドを使用します。

config cts sxp version *version-1-or-2*

構文の説明

version-1-or-2	SXP のバージョンを入力します。有効な値は 1 と 2 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
8.4	このコマンドが導入されました。

config cts sxp

コントローラで Cisco TrustSec SXP（CTS）接続を設定するには、**config cts sxp** コマンドを使用します。

config cts sxp {**enable** | **disable** | **connection** {**delete** | **peer**} | **default password** *password* | **retry period** *time-in-seconds*}

構文の説明

enable	コントローラで CTS 接続を有効にします。
disable	コントローラで CTS 接続を無効にします。
connection	コントローラで CTS 接続を設定します。
delete	コントローラで CTS 接続を削除します。
peer	コントローラが接続されるネクストホップスイッチを設定します。
ip-address	ピアの IPv4アドレスのみ。
default password	SXP メッセージの MD5 認証のデフォルト パスワードを設定します。
password	SXP メッセージの MD5 認証用のデフォルト パスワード。パスワードには、少なくとも 6 文字が必要です。
retry period	SXP 再試行期間を設定します。
time-in-seconds	接続の失敗後に CTS の接続を再試行するまでの時間。

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 では、TrustSec SXP の設定で IPv4 のみがサポートされています。

次に、コントローラで CTS を有効にする例を示します。

```
(Cisco Controller) > config cts sxp enable
```

次に、CTS 接続のピアを設定する例を示します。

```
> config cts sxp connection peer 209.165.200.224
```

関連コマンド

debug cts sxp

config custom-web ext-webauth-mode

カスタム Web 認証ページに対する外部 URL Web ベースのクライアント認可を設定するには、**config custom-web ext-webauth-mode** コマンドを使用します。

config custom-web ext-webauth-mode {**enable** | **disable**}

構文の説明

enable	外部 URL Web ベースのクライアント認証をイネーブルにします。
disable	外部 URL Web ベースのクライアント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。

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、外部 URL Web ベースのクライアント認証を有効にする例を示します。

```
(Cisco Controller) > config custom-web ext-webauth-mode enable
```

関連コマンド

config custom-web redirectUrl

config custom-web weblogo

config custom-web webmessage

config custom-web webtitle

config custom-web ext-webauth-url show custom-web

config custom-web ext-webauth-url

カスタム Web 認証ページに対する完全な外部 Web 認証 URL を設定するには、**config custom-web ext-webauth-url** コマンドを使用します。

config custom-web ext-webauth-url *URL*

構文の説明

URL	Web ベースのクライアント認証に使用される URL。

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。

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、Web ベースのクライアント認証に、完全な外部 Web 認証 URL http://www.AuthorizationURL.com/ を設定する例を示します。

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

関連コマンド

config custom-web redirectUrl

config custom-web weblogo

config custom-web webmessage

config custom-web webtitle

config custom-web ext-webauth-mode show custom-web

config custom-web ext-webserver

外部 Web サーバを設定するには、**config custom-web ext-webserver** コマンドを使用します。

config custom-web ext-webserver {**add** *index IP_address* | **delete** *index*}

構文の説明

add	外部 Web サーバを追加します。
index	外部 Web サーバ リストの外部 Web サーバ インデックス。インデックスは 1 から 20 までの数にしてください。
IP_address	外部 Web サーバの IP アドレス。
delete	外部 Web サーバを削除します。

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。
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。

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、外部 Web サーバ 2 のインデックスを、外部 Web サーバの IP アドレス 192.23.32.19 に追加する例を示します。

```
(Cisco Controller) > config custom-web ext-webserver add 2 192.23.32.19
```

関連コマンド

config custom-web redirectUrl

config custom-web weblogo

config custom-web webmessage

config custom-web webtitle

config custom-web ext-webauth-mode

config custom-web ext-webauth-url

show custom-web

config custom-web logout-popup

カスタムWeb認証のログアウトポップアップを有効または無効にするには、**config custom-web logout-popup** コマンドを使用します。

config custom-web logout-popup {**enable** | **disable**}

構文の説明

enable	カスタム Web 認証のログアウト ポップアップをイネーブルにします。このページは、ログインの成功後、またはカスタム Web 認証ページのリダイレクト後に表示されます。
disable	カスタム Web 認証のログアウト ポップアップ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。

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、カスタム Web 認証のログアウト ポップアップを無効にする例を示します。

```
(Cisco Controller) > config custom-web logout-popup disable
```

関連コマンド

config custom-web redirectUrl

config custom-web weblogo

config custom-web webmessage

config custom-web webtitle

config custom-web ext-webauth-url show custom-web

config custom-web qrscan-bypass-opt

QR スキャン バイパス認証オプションを設定するには、**config custom-web qrscan-bypass-opt** コマンドを使用します。

config custom-web qrscan-bypass-opt *timer count*

構文の説明

timer	一時的にトラフィックをバイパスする期間を設定します。値の範囲は 5 ～ 60 です。
count	クライアントが再参加する前にトラフィックをバイパスできる回数を設定します。値の範囲は 1 ～ 9 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
8.4	このコマンドが導入されました。

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、カスタム QR スキャン バイパス タイマーを 60 に設定し、クライアントが再参加する前の回数を 3 に設定する例を示します。

```
(Cisco Controller) > config custom-web qrscan-bypass-opt 60 3
```

config custom-web radiusauth

RADIUS Web 認証方式を設定するには、**config custom-web radiusauth** コマンドを使用します。

config custom-web radiusauth {**chap** | **md5chap** | **pap**}

構文の説明

chap	RADIUS Web 認証方式をチャレンジ ハンドシェイク認証プロトコル（CHAP）に設定します。
md5chap	RADIUS Web 認証方式を Message Digest 5 CHAP（MD5 CHAP）に設定します。
pap	RADIUS Web 認証方式をパスワード認証プロトコル（PAP）に設定します。

コマンド デフォルト

なし

コマンド履歴

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

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、RADIUS Web 認証方式を MD5-CHAP に設定する例を示します。

```
(Cisco Controller) > config custom-web radiusauth md5chap
```

関連コマンド

config custom-web redirectUrl

config custom-web webmessage

config custom-web webtitle

config custom-web ext-webauth-mode

config custom-web ext-webauth-url

show custom-web

config custom-web redirectUrl

カスタム Web 認証ページのリダイレクト URL を設定するには、**config custom-web redirectUrl** コマンドを使用します。

config custom-web redirectUrl *URL*

構文の説明

URL	指定したアドレスにリダイレクトされるURL。

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。

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、abc.com にリダイレクトされる URL を設定する例を示します。

```
(Cisco Controller) > config custom-web redirectUrl abc.com
```

関連コマンド

config custom-web weblogo

config custom-web webmessage

config custom-web webtitle

config custom-web ext-webauth-mode

config custom-web ext-webauth-url

show custom-web

config custom-web sleep-client

Web 認証されたスリープ状態のクライアントを削除するには、**config custom-web sleep-client** コマンドを使用します。

config custom-web sleep-client delete *mac_address*

構文の説明

delete	Web 認証されたスリープ状態のクライアントを、そのクライアントの MAC アドレスの使用して削除します。
mac_address	スリープ状態のクライアントの MAC アドレス。

コマンド デフォルト

Web 認証されたスリープ状態のクライアントは削除されません。

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。

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、Web 認証されたスリープ状態のクライアントを削除する例を示します。

```
(Cisco Controller) > config custom-web sleep-client delete 0:18:74:c7:c0:90
```

config custom-web webauth-type

Web 認証のタイプを設定するには、**config custom-web webauth-type** コマンドを使用します。

config custom-web webauth-type {**internal** | **customized** | **external**}

構文の説明

internal	Web 認証タイプを internal に設定します。
customized	Web 認証タイプを customized に設定します。
external	Web 認証タイプを external に設定します。

コマンド デフォルト

デフォルトの Web 認証タイプは **internal** 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。

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。

Web 認証タイプを internal に設定する例を示します。

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

関連コマンド

config custom-web redirectUrl

config custom-web webmessage

config custom-web webtitle

config custom-web ext-webauth-mode

config custom-web ext-webauth-url

show custom-web

config custom-web weblogo

カスタム Web 認証ページの Web 認証ロゴを設定するには、**config custom-web weblogo** コマンドを使用します。

config custom-web weblogo {**enable** | **disable**}

構文の説明

enable	Web 認証のロゴ設定をイネーブルにします。
disable	Web認証のロゴ設定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。

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、Web 認証ロゴを有効にする例を示します。

```
(Cisco Controller) > config custom-web weblogo enable
```

関連コマンド

config custom-web redirectUrl

config custom-web webmessage

config custom-web webtitle

config custom-web ext-webauth-mode

config custom-web ext-webauth-url

show custom-web

config custom-web webmessage

カスタム Web 認証ページのカスタム Web 認証メッセージを設定するには、**config custom-web webmessage** コマンドを使用します。

config custom-web webmessage *message*

構文の説明

message	Web 認証のメッセージ テキスト。

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。

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、Web 認証のメッセージのテキスト Thisistheplace を設定する例を示します。

```
(Cisco Controller) > config custom-web webmessage Thisistheplace
```

関連コマンド

config custom-web redirectUrl

config custom-web weblogo

config custom-web webtitle

config custom-web ext-webauth-mode

config custom-web ext-webauth-url

show custom-web

config custom-web webtitle

カスタム Web 認証ページの Web 認証タイトル テキストを設定するには、**config custom-web webtitle** コマンドを使用します。

config custom-web webtitle *title*

構文の説明

title	Web 認証のカスタム タイトル テキスト。

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。

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、Web 認証のカスタム タイトル テキスト Helpdesk を設定する例を示します。

```
(Cisco Controller) > config custom-web webtitle Helpdesk
```

関連コマンド

config custom-web redirectUrl

config custom-web weblogo

config custom-web webmessage

config custom-web ext-webauth-mode

config custom-web ext-webauth-url

show custom-web

config database size

ローカル データベースを設定するには、**config database size** コマンドを使用します。

config database size *count*

構文の説明

count	512 ～ 2040 のデータベース サイズ値

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。

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。

使用上のガイドライン

show database コマンドを使用して、ローカル データベースの設定を表示します。

次に、ローカル データベースのサイズを設定する例を示します。

```
(Cisco Controller) > config database size 1024
```

関連コマンド

show database

config dhcp

内部 DHCP を設定するには、**config dhcp** コマンドを使用します。

config dhcp {**address-pool** *scope start end* | **create-scope** *scope* | **default-router** *scope router_1* [*router_2*] [*router_3*] | **delete-scope** *scope* | **disable** *scope* | **dns-servers** *scope dns1* [*dns2*] [*dns3*] | **domain** *scope domain* | **enable** *scope* | **lease** *scope lease_duration* | **netbios-name-server** *scope wins1* [*wins2*] [*wins3*] | **network***scope network netmask*}

config dhcpopt-82 remote-id {*ap_mac* | *ap_mac*:*ssid* | *ap-ethmac* | *apname:ssid* | *ap-group-name* | *flex-group-name* | *ap-location* | *apmac-vlan_id* | *apname-vlan_id* | *ap-ethmac-ssid* }

構文の説明

address-pool *scope start end*	割り当てるアドレス範囲を設定します。スコープ名およびアドレス範囲の最初と最後のアドレスを指定する必要があります。
create-scope *name*	新規 DHCP スコープを作成します。スコープ名を指定する必要があります。
default-router *scope router_1* [*router_2*] [*router_3*]	指定されたスコープのデフォルト ルータを設定し、ルータの IP アドレスを指定します。オプションで、セカンダリおよびターシャリ ルータの IP アドレスを指定できます。
delete-scope *scope*	指定された DHCP スコープを削除します。
disable *scope*	指定された DHCP スコープをディセーブルにします。
dns-servers *scope dns1* [*dns2*] [*dns3*]	指定されたスコープのネーム サーバを設定します。少なくとも 1 つのネーム サーバを指定する必要があります。オプションでセカンダリおよびターシャリ ネーム サーバを指定できます。
domain *scope domain*	DNS ドメイン名を設定します。スコープ名およびドメイン名を指定する必要があります。
enable *scope*	指定された DHCP スコープをイネーブルにします。
lease *scope lease_duration*	指定されたスコープのリース期間（秒）を設定します。

netbios-name-server *scope wins1* [*wins2*] [*wins3*]	NetBIOS ネーム サーバを設定します。スコープ名およびネームサーバのIPアドレスを指定する必要があります。オプションで、セカンダリおよびターシャリ ネーム サーバの IP アドレスを指定できます。
network *scope network netmask*	network および netmask を設定します。スコープ名、ネットワーク アドレス、およびネットワーク マスクを指定する必要があります。
opt-82 remote-id	DHCP オプション 82 リモート ID フィールド フォーマットを設定します。 DHCP オプション 82 では、DHCP を使用してネットワーク アドレスを割り当てる場合のセキュリティが強化されます。コントローラは DHCP リレー エージェントとして機能し、信頼できないソースからの DHCP クライアント要求を回避します。コントローラは、要求を DHCP サーバに転送する前に、クライアントからの DHCP 要求にオプション 82 情報を追加します。
ap_mac	DHCP オプション 82 ペイロードへのアクセス ポイントの MAC アドレス。
ap_mac:*ssid*	DHCP オプション 82 ペイロードへのアクセス ポイントの MAC アドレスと SSID。
ap-ethmac	AP Ethernet MAC アドレスとしてのリモート ID 形式。
apname:ssid	AP 名としてのリモート ID の形式: SSID。
ap-group-name	AP グループ名としてのリモート ID 形式。
flex-group-name	FlexConnect グループ名としてのリモート ID 形式。
ap-location	AP ロケーションとしてのリモート ID 形式。
apmac-vlan_id	AP 無線の MAC アドレスとしてのリモート ID の形式: VLAN_ID。
apname-vlan_id	AP 名としてのリモート ID の形式: VLAN_ID。
ap-ethmac-ssid	AP Ethernet MAC としてのリモート ID の形式: SSID のアドレス。

コマンド デフォルト

ap-group-name のデフォルト値は「default-group」であり、ap-location のデフォルト値は「default location」です。

ap-group-name と flex-group-name がヌルの場合は、システム MAC がリモート ID フィールドとして送信されます。

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

show dhcp コマンドを使用して、内部 DHCP 設定を表示します。

次に、スコープ 003 の DHCP リースを設定する例を示します。

```
(Cisco Controller) >config dhcp lease 003
```

config dhcp opt-82 format

DHCPオプション 82 の形式を設定するには、**config dhcp opt-82 format** を使用します。

config dhcp opt-82 format{*binary* | *ascii*}

構文の説明

binary	DHCP オプション 82 の形式をバイナリとして指定します。
ascii	DHCP オプション 82 の形式を ASCII として指定します。

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、DHCP オプション 82 ペイロードの形式を設定する例を示します。

```
(Cisco Controller) > config dhcp opt-82 format binary
```

config dhcp opt-82 remote-id

DHCPオプション 82 ペイロードの形式を設定するには、**config dhcp opt-82 remote-id** を使用します。

config dhcp opt-82 remote-id {*ap_mac* | *ap_mac:ssid* | *ap-ethmac* | *apname:ssid* | *ap-group-name* | *flex-group-name* | *ap-location* | *apmac-vlan-id* | *apname-vlan-id* | *ap-ethmac-ssid*}

構文の説明

ap_mac	アクセス ポイントの無線 MAC アドレスを DHCP オプション 82 ペイロードに対して指定します。
ap_mac:ssid	アクセス ポイントの無線 MAC アドレスと SSID を DHCP オプション 82 ペイロードに対して指定します。
ap-ethmac	アクセス ポイントのイーサネット MAC アドレスを DHCP オプション 82 ペイロードに対して指定します。
apname:ssid	アクセス ポイントの AP 名と SSID を DHCP オプション 82 ペイロードに対して指定します。
ap-group-name	AP グループ名を DHCP オプション 82 ペイロードに対して指定します。
flex-group-name	FlexConnect グループ名を DHCP オプション 82 ペイロードに対して指定します。
ap-location	AP の場所を DHCP オプション 82 ペイロードに対して指定します。
apmac-vlan-id	アクセス ポイントの無線 MAC アドレスと VLAN ID を DHCP オプション 82 ペイロードに対して指定します。
apname-vlan-id	AP 名とその VLAN ID を DHCP オプション 82 ペイロードに対して指定します。
ap-ethmac-ssid	アクセス ポイントのイーサネット MAC アドレスと SSID を DHCP オプション 82 ペイロードに対して指定します。

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、DHCP オプション 82 ペイロードのリモート ID を設定する例を示します。

```
(Cisco Controller) > config dhcp opt-82 remote-id apgroup1
```

config dhcp proxy

DHCP パケットを変更するレベルを指定するには、**config dhcp proxy** コマンドを使用します。

config dhcp proxy {**enable** | **disable** {**bootp-broadcast** [**enable** | **disable**]}

構文の説明

enable	コントローラは制限なしで DHCP パケットを変更できます。
disable	DHCP パケット変更をリレー レベルまで削減します。
bootp-broadcast	DHCP BootP ブロードキャスト オプションを設定します。

コマンド デフォルト

DHCP は有効になっています。

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。

使用上のガイドライン

show dhcp proxy コマンドを使用して、DHCP プロキシ処理のステータスを表示します。

サードパーティ WGB サポートを有効にするには、**config wlan passive-client enable** コマンドを入力して、ワイヤレス LAN 上でパッシブ クライアント機能を有効にする必要があります。

次に、DHCP パケット情報を無効にする例を示します。

```
(Cisco Controller) >config dhcp proxy disable
```

次に、DHCP BootP ブロードキャスト オプションを有効にする例を示します。

```
(Cisco Controller) >config dhcp proxy disable bootp-broadcast enable
```

config dhcp timeout

DHCP タイムアウト値を設定するには、**config dhcp timeout** コマンドを使用します。WLAN が DHCP required 状態に設定されている場合は、このタイマーが、クライアントが DHCP 経由で DHCP リースを取得するまで WLC が待機する時間を制御します。

config dhcp timeout *timeout-value*

構文の説明

timeout-value	5～120 秒の範囲のタイムアウト値。

コマンド デフォルト

デフォルトのタイムアウト値は 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。

次に、DHCP のタイムアウトを 10 秒に設定する例を示します。

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

config dx

Cisco WLC でのデータ公開を設定するには、**config dx** コマンドを使用します。

config dx {**enable | disable**}

構文の説明

enable	Cisco WLC でのデータ公開を有効にします。
disable	Cisco WLC でのデータ公開を無効にします。

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。

config exclusionlist

除外リスト エントリを作成または削除するには、**config exclusionlist** コマンドを使用します。

config exclusionlist {**add** *MAC* [*description*] | **delete** *MAC* | **description** *MAC* [*description*]}

構文の説明

config exclusionlist	除外リストを設定します。
add	ローカル除外リスト エントリを作成します。
delete	ローカル除外リスト エントリを削除します。
description	除外リスト エントリの説明を指定します。
MAC	ローカル除外リスト エントリの MAC アドレス。
description	（任意）除外されたエントリの説明（最大 32 文字）。

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。

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、MAC アドレス *xx:xx:xx:xx:xx:xx* のローカル除外リスト エントリを作成する例を示します。

```
(Cisco Controller) > config exclusionlist add xx:xx:xx:xx:xx:xx lab
```

次に、MAC アドレス *xx:xx:xx:xx:xx:xx* のローカル除外リスト エントリを削除する例を示します。

```
(Cisco Controller) > config exclusionlist delete xx:xx:xx:xx:xx:xx lab
```

関連コマンド

show exclusionlist

config fabric

ファブリックの有効または無効にするには、**config fabric** コマンドを使用します。

config fabric enable disable

構文の説明		
	enable	ファブリックを有効にします。
	disable	ファブリ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
8.5	このコマンドが導入されました。

例

次に、ファブリックを有効にする例を示します。

```
config fabric enable
```

config fabric vnid create name

ファブリックの仮想拡張 LAN（VXLAN）ネットワーク識別子（VNID）とサブネットを設定するには、**config fabric vnid create name** コマンドを使用します。

config fabric vnid create name *interface-name* **l2-vnid** *l2-vnid* **ip** *network-ip* **subnet** *subnet* **l3-vnid** *l3-vnid*

構文の説明

interface-name	インターフェイスの名前。
l2-vnid	レイヤ 2 VNID。
L2 vnid	レイヤ 2 VNID の値。
ip	IP アドレス。
network-ip	ネットワーク IP アドレス。
subnet	サブネット アドレス。
subnet	ネットワークのサブネットのアドレス。
L3 vnid	レイヤ 3 VNID の値。
l3-vnid	レイヤ 3 VNID。

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
8.5	このコマンドが導入されました。

使用上のガイドライン

サブネットと VNID の組み合わせは、重複なしの 1 対 1 になることが予期されています。

RADIUS オーバーライドまたは WLAN での VNID の設定には VNID 名を使用できます。

ゲスト ファブリック VNID またはサブネットは、エンタープライズ ファブリック VNID またはサブネットと重複できません。

例

次に、ファブリック VNID およびサブネットを設定する例を示します。

```
config fabric vnid create name vnid1 l2-vnid l2-vn ip 10.10.1.3 subnet 255.255.255.223
l3-vnid l3-vn
```

config fabric control-plane enterprise-fabric

マップ サーバの IP アドレスと事前共有キーを設定するには、**config fabric control-plane enterprise-fabric ip** コマンドを使用します。

config fabric control-plane enterprise-fabric {add |delete}{primary | secondary} ip *ip-address* **preshared-key** *pre-shared-key*

構文の説明

ip-address	マップサーバのIPアドレス。
pre-shared-key	事前共有キー。

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
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

AP は、このコマンドを使用して設定されるマップ サーバでファブリックの一部となっている必要があります。最大2つのIPアドレスを使用できます。2つのIPアドレスの場合、アクティブ - アクティブ モードになります。

関連付けられているマップ サーバを削除するには、**config fabric control-plane enterprise-fabric delete ip***ip-address* コマンドを使用します。

例

次に、マップ サーバの IP アドレスと事前共有キーを設定する例を示します。

```
config fabric control-plane enterprise-fabric add primary ip 10.1.1.1 preshare-key secret
```

config fabric control-plane guest-fabric

ファブリック WLAN で使用されるゲスト マップ サーバの IP アドレスと事前共有キーを設定するには、**config fabric control-plane guest-fabric** コマンドを使用します。

config fabric control-plane guest-fabric {add |delete}{primary | secondary} ip *ip-address* **preshared-key** *pre-shared-key*

構文の説明

ip-address	マップ サーバの IP アドレス。
pre-shared-key	事前共有キー。

コマンド デフォルト

エンタープライズ ファブリック マップ サーバが使用されます。

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。

使用上のガイドライン

最大 2 つの IP アドレスを使用できます。2 つの IP アドレスの場合、アクティブ - アクティブ モードになります。

例

次に、ゲスト マップ サーバの IP アドレスと事前共有キーを設定する例を示します。

```
config fabric control-plane guest-fabric add primary ip 10.2.1.1 preshared-key guest
```

config flexconnect [ipv6] acl

FlexConnect アクセス ポイントに設定されたアクセス コントロール リストを適用するには、**config flexconnect [ipv6] acl** コマンドを使用します。IPv6 の FlexConnect ACL を設定するには、**ipv6** キーワードを使用します。

config flexconnect［**ipv6**］ **acl** ｛**apply** ｜ **create** ｜ **delete**｝ *acl_name*

構文の説明

ipv6	IPv6 の FlexConnect ACL を設定するには、このオプションを使用します。このオプションを使用しない場合は、IPv4 の FlexConnect ACL が設定されます。
apply	ACL をデータ パスに適用します。
create	ACL を作成します。
delete	ACL を削除します。
acl_name	最大 32 文字の英数字による ACL 名。

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。
8.8	IPv6 ACL オプションが追加されました。

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、FlexConnect アクセス ポイントに設定された IPv4 の ACL を適用する例を示します。

```
(Cisco Controller) >config flexconnect acl apply acl1
```

config flexconnect [ipv6] acl rule

FlexConnect アクセス ポイントにアクセス コントロール リスト（ACL）ルールを設定するには、**config flexconnect** [**ipv6**] **acl rule** コマンドを使用します。

config flexconnect ［**ipv6**］ **acl rule** ｛**action** *rule_name rule_index* ｛**permit** ｜ **deny**｝ ｜ **add** *rule_name rule_index* ｜ **change index** *rule_name old_index new_index* ｜ **delete** *rule_name rule_index* ｜ **destination address** *rule_name rule_index ip_address netmask* ｜ **destination port range** *rule_name rule_index start_port end_port* ｜ **direction** *rule_name rule_index* ｛**in** ｜ **out** ｜ **any**｝ ｜ **dscp** *rule_name rule_index dscp* ｜ **protocol** *rule_name rule_index protocol* ｜ **source address** *rule_name rule_index ip_address netmask* ｜ **source port range** *rule_name rule_index start_port end_port* ｜ **swap index** *rule_name index_1 index_2*｝

構文の説明

ipv6	IPv6 の FlexConnect ACL ルールを設定するには、このオプションを使用します。このオプションを使用しない場合は、IPv4 の FlexConnect ACL ルールが設定されます。
action	アクセスを許可するか拒否するかを設定します。
rule_name	最大 32 文字の英数字による ACL 名。
rule_index	1 ～ 32 のルールのインデックス。
permit	ルールのアクションを許可します。
deny	ルールのアクションを拒否します。
add	新規ルールを追加します。
change	ルールのインデックスを変更します。
index	ルールのインデックスを指定します。
delete	ルールを削除します。
destination address	ルールの宛先 IP アドレスとネットマスクを設定します。
ip_address	ルールの IP アドレス。
netmask	ルールのネットマスク。
start_port	開始ポート番号（0 ～ 65535）。
end_port	終了ポート番号（0 ～ 65535）。

direction	ルールの方向（in、out、またはany）を設定します。
in	ルールの方向を in に設定します。
out	ルールの方向を out に設定します。
any	ルールの方向を any に設定します。
dscp	ルールの DSCP を設定します。
dscp	0 ～ 63 の数値または **any**。
protocol	ルールの DSCP を設定します。
protocol	0 ～ 255 の数値または **any**。
source address	ルールの送信元 IP アドレスとネットマスクを設定します。
source port range	ルールの送信元ポート範囲を設定します。
swap	ルールの2つのインデックスを入れ替えます。
index_1	交換する最初のインデックス。
index_2	最初のインデックスと交換するルールインデックス。

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。
8.8	IPv6 ACL オプションが追加されました。

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、アクセスを許可するよう ACL を設定する例を示します。

```
(Cisco Controller) >config flexconnect acl rule action lab1 4 permit
```

config flexconnect [ipv6] acl url-domain

FlexConnect ACL の URL ドメイン ベース ルールを設定するには、**config flexconnect acl** [**ipv6**] **url-domain** コマンドを使用します。

config flexconnect ［**ipv6]acl url-domain**{**action** *acl-name index action* |**add** *acl-name index*|**delete** *acl-name index*|**url** *acl-name index url-name*}

構文の説明

ipv6	IPv6 の FlexConnect ACL の URL ドメイン ベース ルールを設定するには、このオプションを使用します。このオプションを使用しない場合は、IPv4 の FlexConnect ACL ルールが設定されます。
action *acl-name index action*	FlexConnect ACL ルールのアクション（アクセスの許可または拒否）を設定します。
add *acl-name index*	FlexConnect ACL に URL ドメインに追加します。
delete *acl-name index*	FlexConnect ACL から URL ドメインを削除します。
url *acl-name index url-name*	FlexConnect ACL の URL 名を設定します。

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。
8.8	IPv6 ACL オプションが追加されました。

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、IPv6 の FlexConnect ACL の URL ベース ルールを設定する例を示します。

```
(Cisco Controller) >config flexconnect ipv6 acl url-domain action acls-to-allow 2 permit
```

config flexconnect arp-caching

FlexConnect AP でローカルに切り替えられる WLAN を使用している場合にクライアントの ARP エントリをキャッシュに保存するには、**config flexconnect arp-caching** コマンドを使用します。

config flexconnect arp-caching {**enable** } **disable**}

構文の説明

arp-caching enable	クライアントの ARP エントリをキャッシュに保存し、ローカルに切り替えられる WLAN のクライアントに代わって応答するようにアクセス ポイントに指示します。
arp-caching disable	ARP キャッシュを無効にします。

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。

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。

例

次に、FlexConnect AP でローカルに切り替えられる WLAN を使用している場合にプロキシ ARP を適用する例を示します。

```
(Cisco Controller) >config flexconnect arp-caching enable
```

config flexconnect avc profile

FlexConnect の Application Visibility and Control（AVC）プロファイルのルールを設定するには、**config flexconnect avc profile** コマンドを使用します。

config flexconnect avc profile *profilename* {**create | delete**} | **apply** | **rule** {**addapplication** *app-name* {**drop** | {**mark** *dscp-value*}}} | {**remove application** *app-name*}

構文の説明

proflie-name	AVC プロファイルの名前。入力できる範囲は英数字で 0 ～ 32 文字です。
create	AVC プロファイルを作成します。
delete	AVC プロファイルを削除します。
apply	AVC プロファイルを適用します。
rule	AVC プロファイルのルールを設定します。
add application	AVC プロファイルのルールを追加します。
app-name	アプリケーションの名前。入力できる範囲は英数字で 0 ～ 32 文字です。
drop	パケットをドロップするルールを追加します。
mark	特定の DiffServ コード ポイント（DSCP）によってパケットをマークするルールを追加します。
dscp-value	パケット マーキングの DSCP 値。範囲は 0 ～ 63 です。
remove application	AVC プロファイル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
8.1	このコマンドが導入されました。

次に、FlexConnect プロファイルを作成する例を示します。

```
(Cisco Controller) >config flexconnect avc profile profile1 create
```

config flexconnect fallback-radio-shut

イーサネット リンクが動作していないときのアクセス ポイントの無線インターフェイスを設定するには、**config flexconnect fallback-radio-shut** コマンドを使用します。

config flexconnect fallback-radio-shut {**disable** | **enable delay** *delay-in-sec*}

構文の説明

disable	無線インターフェイスのシャットダウンを無効にします。
enable	無線インターフェイスのシャットダウンを有効にします。
delay	インターフェイスの遅延（この後に無線インターフェイスがシャットダウンされる）を指定します。
delay-in-sec	遅延時間（秒単位）。

コマンド デフォルト

無線インターフェイスのシャットダウンは無効になっています。

コマンド履歴

リリース	変更内容
7.6	このコマンドが導入されました。

使用上のガイドライン

無線インターフェイスのシャットダウンを有効にする場合のみ、遅延時間を指定できます。

次に、5 秒間の遅延時間後の無線インターフェイス シャットダウンを有効にする例を示します。

```
(Cisco Controller) >config flexconnect fallback-radio-shut enable delay 5
```

config flexconnect group

FlexConnect グループを追加、削除、または設定するには、**config flexconnect group** コマンドを使用します。

config flexconnect group *group_name* {**add** | **delete** | **ap** {**add** | **delete**} *ap-mac* | **radius** {**ap** {**authority** {**id** *hex_id* | **info** *auth_info*} | **disable** | **eap-fast** {**enable** | **disable**} | **enable** | **leap** {**enable** | **disable**} | **pac-timeout** *timeout* | **server-key** {**auto** | *key*} | **user** {**add** {*username password*} | **delete** *username*}}} | **server auth** {**add** | **delete**} {**primary** | **secondary**} *server_index IP_address auth_port secret*} | **predownload** {**disable** | **enable**} | **master** *ap_name* | **slave** {**retry-count** *max_count* | **ap-name** *cisco_ap*} | **start** {**primary backup abort**} | **local-split** {**wlan** *wlan_id* **acl** *acl_name* {**enable** | **disable**}} | **multicast overridden-interface** {**enable** | **disable**} | **vlan** {**add** *vlan_id* **acl** *in-aclname out-aclname* | **delete** *vlan_id* } | **web-auth wlan** *wlan_id* **acl** *acl_name* {**enable** | **disable**} | **web-policy acl** {**add** | **delete**} *acl_name*}

config flexconnect group *group_name* **radius ap** {**eap-cert download** | **eap-tls** {**enable** | **disable**} | **peap** {**enable** | **disable**}}

config flexconnect group *group_name* **policy acl** {**add** | **delete**} *acl_name*

`config flexconnect group` *group_name* {add | delete}`http-proxy ipaddress` *ip-address* `port` *port -no*

構文の説明

group_name	グループ名。
add	FlexConnect グループを追加します。
delete	FlexConnect グループを削除します。
ap	FlexConnect グループにアクセス ポイントを追加または削除します。
add	FlexConnect グループにアクセス ポイントを追加します。
delete	FlexConnect グループからアクセス ポイントを削除します。
ap_mac	アクセス ポイントの MAC アドレス。
radius	FlexConnect グループのクライアント認証用に RADIUS サーバを設定します。
ap	FlexConnect グループのクライアント認証用にアクセス ポイント ベースの RADIUS サーバを設定します。

authority	拡張認証プロトコル - セキュアトンネル経由の柔軟な認証（EAP-FAST）権限パラメータを設定します。
id	ローカル EAP-FAST サーバの権限識別子を設定します。
hex_id	16 進数文字で表したローカル EAP-FAST サーバの権限識別子。最大 32 文字の 16 進数の偶数を入力できます。
info	テキスト形式のローカル EAP-FAST サーバの権限識別子を設定します。
auth_info	テキスト形式のローカル EAP-FAST サーバの権限識別子。
disable	AP ベースの RADIUS サーバを無効にします。
eap-fast	拡張認証プロトコル - セキュアトンネル経由の柔軟な認証（EAP-FAST）権限を有効または無効にします。
enable	EAP-FAST 認証を有効にします。
disable	EAP-FAST 認証を無効にします。
enable	AP ベースの RADIUS サーバを有効にします。
leap	Lightweight Extensible Authentication Protocol（LEAP）認証を有効または無効にします。
disable	LEAP 認証を無効にします。
enable	LEAP 認証をイネーブルにします。
pac-timeout	EAP-FAST Protected Access Credential（PAC）タイムアウト パラメータを設定します。
timeout	PAC タイムアウト（日数単位）。範囲は 2 ～ 4095 です。値 0 は無効であることを示します。
server-key	EAP-FAST サーバ キーを設定します。サーバ キーは、PAC の暗号化と暗号化解除に使用されます。
auto	ランダム サーバ キーを自動的に生成します。
key	FlexConnect グループの効率的なアップグレードを無効にするキー。

user	AP ベースの RADIUS サーバでユーザ リストを管理します。
add	ユーザを追加します。最大 100 人のユーザを設定できます。
username	大文字と小文字を区別し、英数字で最大24文字のユーザ名。
password	ユーザのパスワード
delete	ユーザを削除します。
server	外部 RADIUS サーバを設定します。
add	外部 RADIUS サーバを追加します。
delete	外部 RADIUS サーバを削除します。
primary	外部プライマリ RADIUS サーバを設定します。
secondary	外部セカンダリ RADIUS サーバを設定します。
server_index	RADIUS サーバのインデックス。
IP_address	RADIUS サーバの IP アドレスです。
auth_port	RADIUS サーバのポート アドレスです。
secret	RADIUS サーバのインデックス。
predownload	FlexConnect グループの効率的な AP アップグレードを設定します。アクセス ポイントをリセットしたり、ネットワーク接続を切断したりせずに、コントローラからアクセス ポイントにアップグレード イメージをダウンロードできます。
disable	FlexConnect グループの効率的なアップグレードを無効にします。
enable	FlexConnect グループの効率的なアップグレードを有効にします。
master	マスター AP として FlexConnect グループのアクセス ポイントを手動で指定します。
ap_name	アクセス ポイント名。
slave	スレーブ AP として FlexConnect グループのアクセス ポイントを手動で指定します。

retry-count	スレーブ アクセス ポイントがマスターからイメージをプレダウンロードを試みる回数を設定します。
max_count	スレーブ アクセス ポイントがマスターからイメージをプレダウンロードを試みる最大回数。
ap_name	手動で設定したマスターをオーバーライドします。
cisco_ap	マスター アクセス ポイントの名前。
start	FlexConnect グループのプレダウンロード イメージ アップグレードを開始します。
primary	FlexConnect グループのプレダウンロードのプライマリ・イメージのアップグレードを開始します。
backup	FlexConnect グループのプレダウンロードのバックアップ イメージのアップグレードを開始します。
abort	FlexConnect グループのプレダウンロード イメージ アップグレードを中断します。
local-split	WLAN 単位で、FlexConnect AP グループにローカル スプリット ACL を設定します。
wlan	FlexConnect AP グループにローカル・スプリット ACL の WLAN を設定します。
wlan_id	1 ～ 512 の無線 LAN 識別子。
acl	WLAN 単位で、FlexConnect AP グループにローカル スプリット ACL を設定します。
acl_name	ACL の名前
multicast overridden-interface	ローカルにスイッチされたクライアントの上書きインターフェイスで、レイヤ 2 ブロードキャスト ドメイン間のマルチキャストを設定します。
vlan	FlexConnect グループに VLAN を設定します。
add	FlexConnect グループに VLAN を追加します。
vlan_id	VLAN 識別番号。

in-acl	最大 32 文字の英数字による着信 ACL 名。
out-acl	最大 32 文字の英数字による発信 ACL 名。
delete	FlexConnect グループから VLAN を削除。
web-auth	外部 Web 認証の FlexConnect ACL を設定します。
wlan	FlexConnect ACL を設定する無線 LAN を指定します。
wlan_id	1 ～ 512 の無線 LAN 識別子。
cisco_ap	FlexConnect アクセス ポイントの名前。
acl	FlexConnect ACL を設定します。
web-policy	Web ポリシー FlexConnect ACL を設定します。
add	FlexConnect グループに Web ポリシー FlexConnect ACL を追加します。
delete	FlexConnect グループから Web ポリシー FlexConnect ACL を削除します
eap-cert download	EAP ルートおよびデバイス証明書をダウンロードします。
eap-tls	EAP-Transport Layer Security（EAP-TLS）認証を有効または無効にします。
peap	Protected Extensible Authentication Protocol（PEAP）認証を有効または無効にします。
policy acl	FlexConnect グループのポリシー ACL を設定します。
http-proxy ipaddress	HTTP プロキシ サーバを設定します。
ip-address	FlexGroup の HTTP プロキシの IP アドレス。
port-no	FlexGroup の HTTP プロキシのポート番号。

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。

使用上のガイドライン

最大 100 個のクライアントを追加できます。

リリース 7.4 以降では、RADIUS サーバでサポートされている最大数は 100 です。

次に、MAC アドレス 192.12.1.2 に対して FlexConnect グループを追加する例を示します。

```
(Cisco Controller) >config flexconnect group 192.12.1.2 add
```

次に、サーバのインデックス番号が 1 である FlexConnect グループのプライマリ サーバとして RADIUS サーバを追加する例を示します。

```
(Cisco Controller) >config flexconnect group 192.12.1.2 radius server add primary 1
```

次に、WLAN の FlexConnect AP グループにローカル スプリット ACL を有効にする例を示します。

```
(Cisco Controller) >config flexconnect group flexgroup1 local-split wlan 1 acl flexacl1
 enable
```

config flexconnect group vlan

FlexConnect グループの VLAN を設定するには、**config flexconnect group vlan** コマンドを使用します。

config flexconnect group *group_name* **vlan** {**add** *vlan-id* **acl** *in-aclname out-aclname* | **delete** *vlan-id*}

構文の説明

group_name	FlexConnect グループ名。
add	FlexConnect グループの VLAN を追加します。
vlan-id	VLAN ID。
acl	アクセス コントロール リストを指定します。
in-aclname	インバウンド ACL の名前。
out-aclname	アウトバウンド ACL の名前。
delete	FlexConnect グループから VLAN を削除。

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。

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、FlexConnect グループ myflexacl の VLAN ID 1 を追加する例を示します。この例では、インバウンド ACL の名前は in-acl、アウトバウンド ACL の名前は out-acl です。

```
(Cisco Controller) >config flexconnect group vlan myflexacl vlan add 1 acl in-acl out-acl
```

configflexconnectgroup*group-name*dhcpoverridden-interface

FlexConnect グループの DHCP 優先インターフェイスを有効または無効にするには、**config flexconnect group** *group-name* **dhcp overridden-interface** コマンドを使用します。

config flexconnect group *group-name* **dhcp overridden-interface** {**enable** | **disable**}

構文の説明

overridden-interface	FlexConnect グループの DHCP 優先インターフェイス。
group-name	FlexConnect グループの名前。
enable	ローカルで切り替えられるクライアントの DHCP ブロードキャストを有効にするようにアクセス ポイントに指示します。
disable	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
8.0	このコマンドが導入されました。

例

次に、ローカルに切り替えられるクライアントの DHCP ブロードキャストを有効にする例を示します。

```
(Cisco Controller) >config flexconnect
  group flexgroup dhcp overridden-interface enable
```

config flexconnect group web-auth

FlexConnect グループの Web-Auth ACL を設定するには、**config flexconnect group web-auth** コマンドを使用します。

config flexconnect group *group_name* **web-auth wlan** *wlan-id* **acl** *acl-name* {**enable** | **disable**}

構文の説明

group_name	FlexConnect グループ名。
wlan-id	WLAN ID。
acl-name	ACL 名です。
enable	FlexConnect グループの Web-Auth ACL を有効にします。
disable	FlexConnect グループの Web-Auth ACL を無効にします。

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。

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、FlexConnect グループ myflexacl の Web-Auth ACL webauthacl を有効にする例を示します。

```
(Cisco Controller) >config flexconnect group myflexacl web-auth wlan 1 acl webauthacl
enable
```

config flexconnect group web-policy

FlexConnect グループの Web ポリシー ACL を設定するには、**config flexconnect group web-policy** コマンドを使用します。

config flexconnect group *group_name* **web-policy acl** {**add** | **delete**} *acl-name*

構文の説明

group_name	FlexConnect グループ名。
add	Web ポリシー ACL を追加します。
delete	Web ポリシー ACL を削除します。
acl-name	Web ポリシー ACL の名前。

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。

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、FlexConnect グループ myflexacl に Web ポリシー ACL mywebpolicyacl を追加する例を示します。

```
(Cisco Controller) >config flexconnect group myflexacl web-policy acl add mywebpolicyacl
```

config flexconnect join min-latency

接続時に最短の遅延のコントローラを選択するようアクセスポイントを有効または無効にするには、**config flexconnect join min-latency** コマンドを使用します。

config flexconnect join min-latency {**enable** | **disable**} *cisco_ap*

構文の説明

enable	接続時に最短の遅延のコントローラを選択するようアクセス ポイントを有効にします。
disable	接続時に最短の遅延のコントローラを選択するようアクセス ポイントを無効にします。
cisco_ap	Cisco Lightweight アクセス ポイント。

コマンド デフォルト

アクセス ポイントは、接続時に最短の遅延のコントローラを選択できません。

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。

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。

使用上のガイドライン

この機能を有効にすると、アクセスポイントは検出要求と検出応答の間の時間を計算し、最初に応答したコントローラに join します。このコマンドは、次のコントローラ リリースでのみサポートされています。

- Cisco 2500 シリーズ コントローラ
- Cisco 5500 シリーズ コントローラ
- Cisco Flex 7500 シリーズ コントローラ
- Cisco 8500 シリーズ コントローラ
- Cisco ワイヤレス サービス モジュール 2

この設定は、コントローラの HA 設定よりも優先され、OEAP アクセスポイントにのみ適用されます。

次に、接続時に遅延の最も少ないコントローラをアクセス ポイントが選択できるようにする例を示します。

```
(Cisco Controller) >config flexconnect join min-latency enable CISCO_AP
```

config flexconnect office-extend

OfficeExtend アクセス ポイントの FlexConnect モードを設定するには、**config flexconnect office-extend** コマンドを使用します。

config flexconnect office-extend {{**enable** | **disable**} *cisco_ap* | **clear-personalssid-config** *cisco_ap*}

構文の説明

enable	アクセス ポイントに対して OfficeExtend モードを有効にします。
disable	アクセス ポイントに対して OfficeExtend モードを無効にします。
clear-personalssid-config	アクセス ポイントのパーソナル SSID だけをクリアします。
cisco_ap	Cisco Lightweight アクセス ポイント。

コマンド デフォルト

アクセス ポイントで FlexConnect モードを有効にした場合は、OfficeExtend モードが自動的に有効になります。

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

現時点では、WPLUS ライセンスにより Cisco 5500 シリーズのコントローラに接続された Cisco Aironet 1130 シリーズおよび 1140 シリーズのアクセス ポイントだけを OfficeExtend アクセス ポイントとして設定できます。

アクセス ポイントに対して OfficeExtend モードを有効にした場合は、不正なアクセス ポイントの検出が自動的に無効になります。多くの場合、室内環境に導入された OfficeExtend アクセス ポイントは、大量の不正なデバイスを検出します。**config rogue detection** コマンドを使用して、特定のアクセス ポイントまたはすべてのアクセス ポイントの不正検出を有効または無効にできます。

アクセス ポイントに対して OfficeExtend モードを有効にした場合は、DTLS データ暗号化が自動的に有効になります。ただし、**config ap link-encryption** コマンドを使用して、特定のアクセス ポイントまたはすべてのアクセス ポイントの DTLS データ暗号化を有効または無効にできます。

アクセス ポイントに対して OfficeExtend モードを有効にした場合は、Telnet および SSH アクセスが自動的に無効になります。ただし、**config ap telnet** または **config ap ssh** コマンドを使用して、特定のアクセス ポイントの Telnet または SSH アクセスを有効または無効にできます。

アクセスポイントに対して OfficeExtend モードを有効にした場合は、リンク遅延が自動的に有効になります。ただし、**config ap link-latency** コマンドを使用して、コントローラに現在関連

付けられている特定のアクセス ポイントまたはすべてのアクセス ポイントのリンク遅延を有効または無効にできます。

次に、アクセス ポイント Cisco_ap の office-extend を有効にする例を示します。

```
(Cisco Controller) >config flexconnect office-extend enable Cisco_ap
```

次に、アクセス ポイント Cisco_ap のアクセス ポイントのパーソナル SSID だけをクリアする例を示します。

```
(Cisco Controller) >config flexconnect office-extend clear-personalssid-config Cisco_ap
```

config flow

NetFlow モニタおよびエクスポータを設定するには、**config flow** コマンドを使用します。

config flow {**add** | **delete**} **monitor** *monitor_name* {**exporter** *exporter_name* | **record**{*ipv4_client_app_flow_record* | *ipv4_client_src_dst_flow_record*}

構文の説明

add	エクスポータに NetFlow モニタを関連付けるか、NetFlow モニタに NetFlow レコードを関連付けます。
delete	エクスポータから NetFlow モニタの関連付けを解除するか、NetFlow モニタから NetFlow レコードの関連付けを解除します。
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。
exporter	NetFlow エクスポータを設定します。
exporter_name	NetFlow エクスポータの名前。モニタ名は最大 32 文字の英数字で、大文字と小文字が区別されます。エクスポータ名にスペースを含めることはできません。
record	NetFlow モニタに NetFlow レコードを関連付けます。
ipv4_client_app_flow_record	パフォーマンスを向上させる既存のレコード テンプレート。
ipv4_client_src_dst_flow_record	カバレッジを改善する拡張レコード テンプレート。

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

エクスポータは、IP トラフィック情報のテンプレートをエクスポートするネットワーク エンティティです。Cisco WLC は、エクスポータとして機能します。Cisco WLC の NetFlow レコードには、クライアントの MAC アドレス、クライアントの送信元 IP アドレス、WLAN ID、データの入力および出力バイト、入力および出力パケット、入力および出力 DiffServ コードポイント（DSCP）など、指定されたフローのトラフィックに関する情報が含まれています。

次に、NetFlow モニタおよびエクスポータを設定する例を示します。

```
(Cisco Controller) > config flow add monitor monitor1 exporter exporter1
```

config guest-lan

無線 LAN を作成したり、削除したり、有効または無効にしたりするには、**config guest-lan** コマンドを使用します。

config guest-lan {**create** | **delete**} *guest_lan_id interface_name* | {**enable** | **disable**} *guest_lan_id*

構文の説明

create	有線 LAN の設定を作成します。
delete	有線 LAN の設定を削除します。
guest_lan_id	1～5 の LAN 識別子。
interface_name	最大 32 文字の英数字のインターフェイス名。
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。

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。

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、LAN ID 16 の無線 LAN を有効にする例を示します。

```
(Cisco Controller) > config guest-lan enable 16
```

関連コマンド

show wlan

config guest-lan custom-web ext-webauth-url

Web ログインページにアクセスする前にゲストユーザを外部サーバにリダイレクトするには、**config guest-lan custom-web ext-webauth-url** コマンドを使用します。

config guest-lan custom-web ext-webauth-url *ext_web_url guest_lan_id*

構文の説明

ext_web_url	外部サーバの URL。
guest_lan_id	1 ～ 5 のゲスト 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。

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、LAN ID 16 の無線 LAN を有効にする例を示します。

```
(Cisco Controller) > config guest-lan custom-web ext-webauth-url
http://www.AuthorizationURL.com/ 1
```

関連コマンド

config guest-lan

config guest-lan create

config guest-lan custom-web login_page

config guest-lan custom-web global disable

グローバル カスタム Web 設定ではなくゲスト LAN 固有のカスタム Web 設定を使用するには、**config guest-lan custom-web global disable** コマンドを入力します。

config guest-lan custom-web global disable *guest_lan_id*

構文の説明

guest_lan_id	1 ～ 5 のゲスト 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。

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。

使用上のガイドライン

config guest-lan custom-web global enable *guest_lan_id* コマンドを入力すると、カスタム Web 認証の設定がグローバル レベルで使用されます。

次に、ゲスト LAN ID 1 のグローバル Web 設定を無効にする例を示します。

```
(Cisco Controller) > config guest-lan custom-web global disable 1
```

関連コマンド

config guest-lan

config guest-lan create

config guest-lan custom-web ext-webauth-url

config guest-lan custom-web login_page

config guest-lan custom-web webauth-type

config guest-lan custom-web login_page

カスタマイズされた Web ログイン ページに有線ゲスト ユーザがログインできるようにするには、**config guest-lan custom-web login_page** コマンドを使用します。

config guest-lan custom-web login_page *page_name guest_lan_id*

構文の説明

page_name	カスタマイズされた Web ログイン ページの名前。
guest_lan_id	1 ～ 5 のゲスト 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。

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、ゲスト LAN ID 1 の Web ログイン ページ custompage1 をカスタマイズする例を示します。

```
(Cisco Controller) > config guest-lan custom-web login_page custompage1 1
```

関連コマンド

config guest-lan

config guest-lan create

config guest-lan custom-web ext-webauth-url

config guest-lan custom-web webauth-type

有線ゲスト ユーザの Web ログイン ページを定義するには、**config guest-lan custom-web webauth-type** コマンドを使用します。

config guest-lan custom-web webauth-type {**internal** | **customized** | **external**} *guest_lan_id*

構文の説明

internal	コントローラのデフォルト Web ログイン ページを表示します。これはデフォルト値です。
customized	以前に設定されたカスタム Web ログイン ページを表示します。
external	以前に設定された URL へユーザをリダイレクトします。
guest_lan_id	1 ～ 5 のゲスト LAN 識別子。

コマンド デフォルト

コントローラの Web ログイン ページのデフォルト設定は internal 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。

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、ゲスト LAN ID 1 の内部として WebAuth タイプでゲスト LAN を設定する例を示します。

```
(Cisco Controller) > config guest-lan custom-web webauth-type internal 1
```

関連コマンド

config guest-lan

config guest-lan create

config guest-lan custom-web ext-webauth-url

config guest-lan ingress-interface

レイヤ 2 アクセス スイッチ経由で有線ゲスト クライアントとコントローラの間のパスを提供する、有線ゲスト VLAN の入力インターフェイスを設定するには、**config guest-lan ingress-interface** コマンドを入力します。

config guest-lan ingress-interface *guest_lan_id interface_name*

構文の説明

guest_lan_id	1 ～ 5 のゲスト LAN 識別子（両端の値を含む）。
interface_name	インターフェイス名。

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、ゲスト LAN ID 1 およびインターフェイス名 guest01 を使用して有線ゲスト クライアントとコントローラの間にパスを提供する例を示します。

```
(Cisco Controller) > config guest-lan ingress-interface 1 guest01
```

関連コマンド

config interface guest-lan

config guest-lan create

config guest-lan interface

コントローラから有線ゲストトラフィックを送信する出力インターフェイスを設定するには、**config guest-lan interface** コマンドを入力します。

config guest-lan interface *guest_lan_id interface_name*

構文の説明

guest_lan_id	1 ～ 5 のゲスト LAN 識別子。
interface_name	インターフェイス名。

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、ゲスト LAN ID 1 およびインターフェイス名 guest01 のコントローラからゲストトラフィックを送信する出力インターフェイスを設定する例を示します。

```
(Cisco Controller) > config guest-lan interface 1 guest01
```

関連コマンド

config ingress-interface guest-lan

config guest-lan create

config guest-lan mobility anchor

モビリティ アンカーを追加または削除するには、**config guest-lan mobility anchor** コマンドを使用します。

config guest-lan mobility anchor {**add** | **delete**} *Guest LAN Id IP addr*

構文の説明

add	WLANにモビリティ アンカーを追加します。
delete	WLAN からモビリティ アンカーを削除します。
Guest LAN Id	1 ～ 5 のゲスト LAN 識別子。
ip-addr	WLAN をアンカーするメンバースイッチの IPv4 または IPv6 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。
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、WAN ID 4 のモビリティ アンカーおよびアンカー IP *192.168.0.14* を削除する例を示します。

```
(Cisco Controller) > config guest-lan mobility anchor delete 4 192.168.0.14
```

config guest-lan nac

ゲストLANの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有効または無効にするには、**config guest-lan nac** コマンドを使用します。

config guest-lan nac ｛**enable** | **disable**｝ *guest_lan_id*

構文の説明

enable	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	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。
guest_lan_id	1 ～ 5 のゲスト 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、ゲスト LAN ID 3 の NAC アウトオブバンド サポートを有効にする例を示します。

```
(Cisco Controller) > config guest-lan nac enable 3
```

関連コマンド

show nac statistics

show nac summary

config wlan nac

debug nac

config guest-lan security

有線ゲスト LAN のセキュリティ ポリシーを設定するには、**config guest-lan security** コマンドを使用します。

config guest-lan security {**web-auth** {**enable** | **disable** | **acl** | **server-precedence**} *guest_lan_id* | **web-passthrough** {**acl** | **email-input** | **disable** | **enable**} *guest_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。
guest_lan_id	1～5 の LAN 識別子。
web-passthrough	認証不要の Web キャプティブ ポータルを設定します。
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。

コマンド デフォルト

有線ゲスト LAN のデフォルトのセキュリティ ポリシーは Web 認証です。

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。

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、ゲスト LAN ID 1 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 guest-lan security web-auth enable 1
```

関連コマンド

config ingress-interface guest-lan

config guest-lan create

config interface guest-lan

config interface 3g-vlan

3G/4G-VLAN インターフェイスを設定するには、**config interface 3g-vlan** コマンドを使用します。

config interface 3g-vlan *interface-name* {**enable** | **disable**}

構文の説明

interface-name **enable**	指定された 3G/4G-VLAN インターフェイスを有効にします。
interface-name **disable**	指定された 3G/4G-VLAN インターフェイスを無効にします。

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
8.1	このコマンドが導入されました。

次に、3G/4G-VLAN トンネル インターフェイスを設定する例を示します。

```
(Cisco Controller) > config interface 3g-vlan vlan-int enable
```

config interface acl

インターフェイスのアクセス コントロール リストを設定するには、**config interface acl** コマンドを使用します。

config interface acl {**ap-manager** | **management** | *interface_name*} {*ACL* | **none**}

構文の説明

ap-manager	アクセス ポイントのマネージャ インターフェイスを設定します。
management	管理インターフェイスを設定します。
interface_name	インターフェイス名。
ACL	最大 32 文字の英数字の ACL 名。
none	何も指定しません。

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

Cisco 2100 シリーズ ワイヤレス LAN コントローラの場合、外部 Web サーバに対して無線 LAN で事前認証 ACL を設定する必要があります。この ACL は、Web ポリシーで無線 LAN 事前認証 ACL として設定する必要があります。ただし、Cisco 4400 シリーズ ワイヤレス LAN コントローラの場合は事前認証 ACL を設定する必要はありません。

次に、アクセス コントロール リストを [None] の値で設定する例を示します。

```
(Cisco Controller) > config interface acl management none
```

config interface address

インターフェイスのアドレス情報を設定するには、**config interface address** コマンドを使用します。

config interface address {**ap-manager** *IP_address netmask gateway* | **management** *IP_address netmask gateway* | **service-port** *IP_address netmask* | **virtual** *IP_address* | **dynamic-interface** *IP_address dynamic_interface netmask gateway* | **redundancy-management** *IP_address* **peer-redundancy-management** *IP_address* }

構文の説明

ap-manager	アクセス ポイントのマネージャ インターフェイスを指定します。
IP_address	IP アドレス（IPv4 のみ）。
netmask	ネットワーク マスク。
gateway	ゲートウェイの IP アドレス。
management	管理インターフェイスを指定します。
service-port	アウトオブバンド サービス ポート インターフェイスを指定します。
virtual	バーチャル ゲートウェイ インターフェイスを指定します。
interface-name	*interface-name* パラメータでインターフェイスを指定します。
interface-name	インターフェイス名。
redundancy-management	冗長管理インターフェイスの IP アドレスを設定します。
peer-redundancy-management	ピア冗長管理インターフェイスの IP 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。

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。

使用上のガイドライン

Cisco 5500 シリーズ コントローラの場合は、AP マネージャ インターフェイスを設定する必要はありません。管理インターフェイスは、デフォルトで AP マネージャ インターフェイスとして動作します。

このコマンドは、IPv4 アドレスだけに適用されます。

両方のコントローラの管理インターフェイスが同じサブネット上にあることを確認します。両方のコントローラの冗長管理の IP アドレスが同じであるようにします。同様に、両方のコントローラのピア冗長管理の IP アドレスが同じであるようにします。

次に、IP アドレス 209.165.201.31、ネットワーク マスク 255.255.0.0、およびゲートウェイ アドレス 209.165.201.30 によってアクセス ポイントのマネージャ インターフェイスを設定する例を示します。

```
(Cisco Controller) > config interface address ap-manager 209.165.201.31 255.255.0.0
209.165.201.30
```

次に、コントローラの冗長管理インターフェイスを設定する例を示します。

```
(Cisco Controller) > config interface address redundancy-management 209.4.120.5
peer-redundancy-management 209.4.120.6
```

次に、仮想インターフェイスを設定する例を示します。

```
(Cisco Controller) > config interface address virtual 192.0.2.1
```

関連コマンド

show interface

config interface address redundancy-management

コントローラの管理インターフェイス IP アドレス、サブネット、およびゲートウェイを設定するには、**config interface address redundancy-management** コマンドを使用します。

config interface address redundancy-management *IP_address netmask gateway*

構文の説明

IP_address	アクティブ コントローラの管理インターフェイス IP アドレス。
netmask	ネットワーク マスク。
gateway	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

このコマンドにより、キープアライブが失敗したときのアクティブ/スタンバイの到達可能性を確認できます。。

次に、コントローラの管理 IP アドレスを設定する例を示します。

```
(Cisco Controller) > config interface address redundancy-management 209.165.201.31
255.255.0.0 209.165.201.30
```

関連コマンド

config redundancy mobilitymac

config redundancy interface address peer-service-port

config redundancy peer-route

config redundancy unit

config redundancy timer

show redundancy timers

show redundancy summary

debug rmgr

debug rsyncmgr

config interface ap-manager

管理または動的インターフェイスでアクセスポイントのマネージャ機能を有効または無効にするには、**config interface ap-manager** コマンドを使用します。

config interface ap-manager {**management** | *interface_name*} {**enable** | **disable**}

構文の説明

management	管理インターフェイスを指定します。
interface_name	動的インターフェイス名。
enable	動的インターフェイスでアクセス ポイントのマネージャ機能をイネーブルにします。
disable	動的インターフェイスでアクセス ポイントのマネージャ機能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

管理インターフェイスに対して動的 AP 管理を有効または無効にするには **management** オプションを使用します。Cisco 5500 シリーズ コントローラの場合、管理インターフェイスはデフォルトで AP マネージャ インターフェイスのように動作します。必要に応じて、管理インターフェイスを AP マネージャ インターフェイスとして無効にし、別の動的インターフェイスを AP マネージャとして作成できます。

動的インターフェイスに対してこの機能を有効にした場合、動的インターフェイスは AP マネージャ インターフェイスとして設定されます（1 つの物理ポートに対して 1 つの AP マネージャ インターフェイスだけが許可されます）。AP マネージャ インターフェイスとして指定された動的インターフェイスは WLAN インターフェイスとして使用できません。

次に、アクセス ポイントのマネージャ myinterface を無効にする例を示します。

```
(Cisco Controller) > config interface ap-manager myinterface disable
```

config interface create

有線ゲスト ユーザ アカウントのダイナミック インターフェイス（VLAN）を作成するには、**config interface create** コマンドを使用します。

config interface create *interface_name vlan-id*

構文の説明

interface_name	インターフェイス名。
vlan-id	VLAN 識別番号。

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、lab2 および VLAN ID 6 という名前のインターフェイスによってダイナミック インターフェイスを作成する例を示します。

```
(Cisco Controller) > config interface create lab2 6
```

config interface delete

ダイナミック インターフェイスを削除するには、**config interface delete** コマンドを使用します。

config interface delete *interface-name*

構文の説明

interface-name	*interface-name*インターフェイス名。

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、VLAN501 という名前のダイナミック インターフェイスを削除する例を示します。

```
(Cisco Controller) > config interface delete VLAN501
```

config interface dhcp management

管理インターフェイスで DHCP オプションを設定するには、**config interface dhcp management** コマンドを使用します。

config interface dhcp management {**option-82** {**bridge-mode-insertion** {**enable** | **disable**} | **enable** | **disable** | **linksel** {**enable** | **disable** | **relaysrc** *interface-name*} | **vpnsel** {**enable** | **disable** | **vpnid** *vpn-id* | **vrfname** *vrf-name*}} | **primary** *primary-dhcp_server* [**secondary** *secondary-dhcp_server*] | **proxy-mode** {**enable** | **disable** | **global**} }

構文の説明

option-82	インターフェイスで DHCP オプション 82 を設定します。
bridge-mode-insertion	DHCP オプション 82 挿入をブリッジモードで設定します。
disable	機能を無効にします。
enable	機能を有効にします。
linksel	ダイナミック インターフェイスまたは管理インターフェイスでリンク選択サブオプション 5 を設定します。
relaysrc	リレー送信元でリンク選択サブオプション 5 を設定します。
interface-name	DHCP サーバから到達可能な既存の WLC インターフェイスの名前。
vpnid	VPN 選択サブオプション 151 VPN ID を設定します。
vpn-id	oui:vpn-index 形式 xxxxxx:xxxxxxxx の VPN ID。
vrfname	VPN 選択サブオプション 151 VPF 名を設定します。
vrf-name	VRF 名（長さ 7 の文字列）。
primary	プライマリ DHCP サーバを指定します。
primary-dhcp-server	サーバの IP アドレス。
secondary	（任意）セカンダリ DHCP サーバを指定します。
secondary-dhcp-server	サーバの IP アドレス。

proxy-mode	インターフェイスで DHCP プロキシ モードを設定します。
global	インターフェイスでグローバル DHCP プロキシ モードを使用します。
disable	（任意）インターフェイスで DHCP プロキシ モードをディセーブルにします。
global	（任意）インターフェイスでグローバル DHCP プロキシ モードを使用します。

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。
8.0	新しいキーワード **linksel** と **vpnsel** が追加されました。 このコマンドは、このリリースから IPv6 をサポートしています。

使用上のガイドライン

IPv6 の場合は DHCP プロキシがサポートされず、無効モードで機能します。

次に、管理インターフェイスでオプション 82 を設定する例を示します。

```
(Cisco Controller) > config interface dhcp management option-82 enable
```

関連コマンド

config dhcp
config dhcp proxy
config interface dhcp
config wlan dhcp_server
debug dhcp
debug dhcp service-port
debug disable-all
show dhcp
show dhcp proxy
show interface

config interface dhcp

config interface dhcp コマンドを入力して、管理インターフェイスまたはダイナミック インターフェイスでブリッジ モードの DHCP オプション 82 挿入を設定します。

config interface dhcp {**management** | **dynamic-interface** *dynamic-interface-name*} **option-82 bridge-mode-insertion** {**enable** | **disable**}

構文の説明

management	管理インターフェイス
dynamic-interface	ダイナミック インターフェイス
dynamic-interface-name	ダイナミック インターフェイス名。
option-82	インターフェイスの DHCP オプション 82
bridge-mode-insertion	ブリッジ モード挿入を設定する場合。

コマンド デフォルト

ブリッジ モードの DHCP オプション 82 挿入は無効になっています。

コマンド履歴

リリース	変更内容
8.0	このリリースで、ブリッジモード挿入パラメータが導入されました。

config interface dhcp dynamic-interface

OpenDNS サーバ IP を使用する（または使用しない）ためにインターフェイスで DHCP オプション 6 オーバーライドを設定するには、**config interface dhcp dynamic-interface** コマンドを使用します。

config interface dhcp dynamic-interface *intf-name* **option-6-opendns** { **enable** | **disable** }

構文の説明

intf-name	インターフェイス名。
enable	インターフェイスで DHCP オプション 6 オーバーライドを有効にして、OpenDNS IP アドレスをデフォルトにします。
disable	インターフェイスで DHCP オプション 6 オーバーライドを無効にします。DHCP 提供の DNS IP が使用されます。

コマンド デフォルト

なし

コマンド モード

Controller Config >

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 IP を使用するためにインターフェイスで DHCP オプション 6 オーバーライドを設定する例を示します。

```
(Cisco Controller) > config interface dhcp management option-6-opendns enable
```

config interface dhcp management option-6-opendns

OpenDNS サーバ IP を使用するためにインターフェイスで DHCP オプション 6 オーバーライドを設定するには、**config interface dhcp management option-6-opendns** コマンドを使用します。

config interface dhcp management option-6-opendns{**enable** | **disable**}

構文の説明

enable	インターフェイスで DHCP オプション 6 オーバーライドを有効にして、OpenDNS IP アドレスをデフォルトにします。
disable	インターフェイスで DHCP オプション 6 オーバーライドを無効にして、DHCP 提供の DNS IP を使用します。

コマンド デフォルト

DHCP オプション 6 オーバーライドは有効になっていません。

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。

例

次に、OpenDNS サーバ IP を使用するためにインターフェイスで DHCP オプション 6 オーバーライドを設定する例を示します。

```
(Cisco Controller) > config interface dhcp management option-6-opendns enable
```

config interface address

インターフェイス アドレスを設定するには、**config interface address** コマンドを使用します。

config interface address {**dynamic-interface** *dynamic_interface netmask gateway* | **management** | **redundancy-management** *IP_address* **peer-redundancy-management** | **service-port** *netmask* | **virtual**} *IP_address*

構文の説明

dynamic-interface	コントローラの動的インターフェイスを設定します。
dynamic_interface	コントローラの動的インターフェイス。
IP_address	インターフェイスの IP アドレス。
netmask	インターフェイスのネットマスク。
gateway	インターフェイスのゲートウェイ。
management	管理インターフェイスの IP アドレスを設定します。
redundancy-management	冗長管理インターフェイスの IP アドレスを設定します。
peer-redundancy-management	ピア冗長管理インターフェイスの IP アドレスを設定します。
service-port	アウトバンドサービス ポートを設定します。
virtual	仮想ゲートウェイ インターフェイスを設定します。

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。

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。

使用上のガイドライン

両方のコントローラの管理インターフェイスが同じサブネット上にあることを確認します。両方のコントローラの冗長管理 IP アドレスが同じであることと、両方のコントローラのピア冗長管理 IP アドレスが同じであることを確認します。

次に、コントローラの冗長管理インターフェイスを設定する例を示します。

```
(Cisco Controller) >config interface address redundancy-management 209.4.120.5
peer-redundancy-management 209.4.120.6
```

次に、仮想インターフェイスを設定する例を示します。

```
(Cisco Controller) > config interface address virtual 1.1.1.1
```

関連コマンド

show interface group summary

show interface summary

config interface guest-lan

ゲスト LAN VLAN を有効または無効にするには、**config interface guest-lan** コマンドを使用します。

config interface guest-lan *interface_name* {*enable* | *disable*}

構文の説明

interface_name	インターフェイス名。
enable	ゲスト LAN をイネーブルにします。
disable	ゲスト LAN 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、myinterface という名前のインターフェイスでゲスト LAN 機能を有効にする例を示します。

```
(Cisco Controller) > config interface guest-lan myinterface enable
```

関連コマンド

config guest-lan create

config interface hostname

仮想ゲートウェイ インターフェイスのドメイン ネーム システム（DNS）ホスト名を設定するには、**config interface hostname** コマンドを使用します。

config interface hostname virtual *DNS_host*

構文の説明

virtual	完全記述DNS名の指定された仮想アドレスを使用する仮想ゲートウェイ インターフェイスを指定します 仮想ゲートウェイ IP アドレスは、任意の架空で未割り当ての IP アドレス（192.0.2.1 など）であり、レイヤ 3 Security Manager と Mobility Manager で使用されます。
DNS_host	DNS ホスト名。

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、完全修飾 DNS ホスト名 DNS_Host の指定された仮想アドレスを使用する仮想ゲートウェイ インターフェイスを設定する例を示します。

```
(Cisco Controller) > config interface hostname virtual DNS_Host
```

config interface nasid

インターフェイスのネットワーク アクセス サーバの ID（NAS-ID）を設定するには、**config interface nasid** コマンドを使用します。

config interface nasid {*NAS-ID* | **none**} *interface_name*

構文の説明

NAS-ID	インターフェイスのネットワーク アクセス サーバの 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。
interface_name	最大 32 文字の英数字のインターフェイス名。

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。

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。

使用上のガイドライン

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、インターフェイスの NAS-ID を設定する例を示します。

```
(Cisco Controller) > config interface nasid
```

関連コマンド

config wlan nasid

config wlan apgroup

config interface nat-address

1 対 1 マッピング ネットワーク アドレス変換（NAT）を使用しているルータまたは他のゲートウェイ デバイスの背後に Cisco 5500 シリーズ コントローラを設置するには、**config interface nat-address** コマンドを使用します。

config interface nat-address {**management** | **dynamic-interface** *interface_name*} {{**enable** | **disable**} | {**set** *public_IP_address*}}

構文の説明

management	管理インターフェイスを指定します。
dynamic-interface *interface_name*	動的インターフェイス名を指定します。
enable	インターフェイスで 1 対 1 マッピング NAT をイネーブルにします。
disable	インターフェイスで 1 対 1 マッピング NAT をディセーブルにします。
public_IP_address	外部 NAT 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

これらの NAT コマンドは、Cisco 5500 シリーズ コントローラ専用であり、管理インターフェイスが動的 AP 管理用に設定されている場合にだけ使用できます。

これらのコマンドは、1 対 1 マッピング NAT での使用に対してだけサポートされています。各プライベート クライアントはグローバル アドレスに対して直接的かつ固定的にマッピングされます。クライアントのグループを単一の IP アドレスで表すために送信元ポート マッピングを使用する 1 対多 NAT はサポートされません。

次に、管理インターフェイスで 1 対 1 マッピング NAT を有効にする例を示します。

```
(Cisco Controller) > config interface nat-address management enable
```

次に、管理インターフェイスで外部 NAP IP アドレス 10.10.10.10 を設定する例を示します。

```
(Cisco Controller) > config interface nat-address management set 10.10.10.10
```

config interface port

インターフェイスに物理ポートをマップするには（リンク集約トランクが設定されていない場合）、**config interface port** コマンドを使用します。

config interface port {**management** | *interface_name* | **redundancy-management**} *primary_port* [*secondary_port*]

構文の説明

management	管理インターフェイスを指定します。
interface_name	インターフェイス名。
redundancy-management	冗長性管理インターフェイスを指定します。
primary_port	プライマリ物理ポート番号。
secondary_port	（任意）セカンダリ物理ポート番号。

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

Cisco 5500 シリーズ コントローラ以外のすべてのコントローラに対して **management** オプションを使用できます。

次に、LAb02 インターフェイスのプライマリ ポート番号を 3 に設定する例を示します。

```
(Cisco Controller) > config interface port lab02 3
```

config interface quarantine vlan

いずれかの動的インターフェイスで検疫 VLAN を設定するには、**config interface quarantine vlan** コマンドを使用します。

config interface quarantine vlan *interface-name vlan_id*

構文の説明

interface-name	インターフェイスの名前。
vlan_id	VLAN 識別番号。 （注） 隔離処理を無効にするには、0 と入力します。

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、VLAN ID 10 がある隔離インターフェイスで隔離 VLAN を設定する例を示します。

```
(Cisco Controller) > config interface quarantine vlan quarantine 10
```

config interface url-acl

インターフェイスのアクセス コントロール リストを設定するには、**config interface url-acl** コマンドを使用します。

config interface url-acl {**management** | *interface_name*} {*acl-name* | **none**}

構文の説明

management	管理インターフェイスを設定します。
interface_name	インターフェイス名。
acl-name	最大 32 文字の英数字の ACL 名。
none	インターフェイスで設定されている ACL 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
8.3	このコマンドが導入されました。

次に、インターフェイスの URL ACL を設定する例を示します。

```
(Cisco Controller) >config interface url-acl management test
```

config interface vlan

インターフェイスの VLAN ID を設定するには、**config interface vlan** コマンドを使用します。

config interface vlan {**ap-manager** | **management** | *interface-name* | **redundancy-management**} *vlan*

構文の説明

ap-manager	アクセスポイントのマネージャ インターフェイスを設定します。
management	管理インターフェイスを設定します。
interface_name	インターフェイス名。
vlan	VLAN 識別番号。
redundancy-management	冗長性管理インターフェイスを指定します。

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

システム冗長性管理インターフェイスが冗長性ポートにマッピングされている場合は、冗長性管理 VLAN を変更できません。まず冗長性管理ポートを設定する必要があります。

次に、管理インターフェイスの VLAN ID 10 を設定する例を示します。

```
(Cisco Controller) > config interface vlan management 10
```

config interface group mdns-profile

インターフェイス グループに mDNS（マルチキャスト DNS）プロファイルを設定するには、**config interface group mdns-profile** コマンドを使用します。

config interface group mdns-profile {**all** | *interface-group-name*} {*profile-name* | **none**}

構文の説明

all	すべてのインターフェイス グループに mDNS プロファイルを設定します。
interface-group-name	mDNS プロファイルが関連付けられる必要のあるインターフェイス グループの名前。インターフェイス グループ名では大文字と小文字が区別され、最大 32 文字のの英数字を使用できます。
profile-name	mDNS プロファイルの名前。
none	インターフェイス グループから既存の mDNS プロファイルを削除します。インターフェイス グループに mDNS プロファイルを設定することはできません。

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

mDNS プロファイルが WLAN に関連付けられている場合は、エラーが表示されます。

次に、インターフェイス グループ floor1 に mDNS プロファイルを設定する例を示します。

```
(Cisco Controller) > config interface group mdns-profile floor1 profile1
```

関連コマンド

config mdns query interval

config mdns service

config mdns snooping

config interface mdns-profile

config mdns profile

config wlan mdns

show mdns profile

show mnds service

clear mdns service-database

debug mdns all

debug mdns error

debug mdns detail

debug mdns message

config interface mdns-profile

インターフェイスに mDNS（マルチキャスト DNS）プロファイルを設定するには、**config interface mdns-profile** コマンドを使用します。

config interface mdns-profile {**management** | **all** インターフェイス名} {プロファイル名 | **none**}

構文の説明

management	管理インターフェイスの mDNS プロファイルを設定します。
all	すべてのインターフェイスの mDNS プロファイルを設定します。
interface-name	mDNS プロファイルを設定しなければならないインターフェイスの名前。インターフェイス名は最大 32 文字の英数字で、大文字と小文字を区別します。
profile-name	mDNS プロファイルの名前。
none	インターフェイスから既存の mDNS プロファイルを削除します。インターフェイスに mDNS プロファイルを設定することはできません。

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

mDNS プロファイルが WLAN に関連付けられている場合は、エラーが表示されます。

次に、インターフェイス lab 1 に mDNS プロファイルを設定する例を示します。

```
(Cisco Controller) > config interface mdns-profile lab1 profile1
```

関連コマンド

config mdns query interval

config mdns service

config mdns snooping

config mdns profile

config interface group mdns-profile

config wlan mdns

show mdns profile

show mnds service

clear mdns service-database

debug mdns all

debug mdns error

debug mdns detail

debug mdns message

config icons delete

フラッシュからアイコンを削除するには、WLANコンフィギュレーションモードで**config icons delete** コマンドを使用します。

config icons delete{ *filename* | **all** }

構文の説明

filename	削除するアイコンの名前。
all	システムからすべてのアイコン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 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 8.2	このコマンドが導入されました。

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、フラッシュからアイコンを削除する例を示します。

```
Cisco Controller > config icons delete image-1
```

config icons file-info

アイコン パラメータを設定するには、WLAN コンフィギュレーション モードで **config icons file-info** コマンドを使用します。

config icons file-info *filename file-type lang-code width height*

構文の説明

filename	アイコンのファイル名。最大 32 文字を使用できます。
file-type	アイコンのファイル名のタイプまたは拡張子。最大 32 文字を使用できます。
lang-code	アイコンの言語コード。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*）。
width	アイコンの幅。有効な範囲は 1 ～ 65535 です。
height	アイコンの高さ。有効な範囲は 1 ～ 65535 です。

コマンド デフォルト

なし

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 8.2	このコマンドが導入されました。

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、アイコン パラメータを設定する例を示します。

```
Cisco Controller > config icons file-info ima png eng 300 200
```

config ipv6 disable

Cisco WLC で IPv6 をグローバルに無効にするには、**config ipv6 disable** コマンドを使用します。

config ipv6 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。

使用上のガイドライン

このコマンドを使用すると、コントローラは、すべての IPv6 パケットを廃棄し、クライアントは IPv6 アドレスを受信しません。

次に、コントローラで IPv6 を無効にする例を示します。

```
(Cisco Controller) >config ipv6 disable
```

config ipv6 enable

Cisco WLC で IPv6 をグローバルに有効にするには、**config ipv6 enable** コマンドを使用します。

config ipv6 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、Cisco WLC で IPv6 を有効にする例を示します。

```
(Cisco Controller) >config ipv6 enable
```

config ipv6 acl

Cisco ワイヤレス LAN コントローラで IPv6 ACL を作成または削除し、ACL をデータ パスに適用し、IPv6 ACL のルールを設定するには、**config ipv6 acl** コマンドを使用します。

config ipv6 acl [**apply** | **cpu** | **create** | **delete** | **rule**]
config ipv6 acl apply *name*
config ipv6 acl cpu {*name* | **none**}
config ipv6 acl create *name*
config ipv6 acl delete *name*
config ipv6 acl rule [**action** | **add** | **change** | **delete** | **destination** | **direction** | **dscp** | **protocol** | **source** | **swap**]
config ipv6 acl rule action *name index* {**permit** | **deny**}
config ipv6 acl rule add *name index*
config ipv6 acl rule change index *name old_index new_index*
config ipv6 acl rule delete *name index*
config ipv6 acl rule destination {**address** *name index ip_address prefix-len* | **port range** *name index* }
`config ipv6 acl rule direction` ***name index*** `{in | out | any}`
config ipv6 acl rule dscp *name dscp*
config ipv6 acl rule protocol *name index protocol*
config ipv6 acl rule source {**address** *name index ip_address prefix-len* | **port range** *name index start_port end_port*}
config ipv6 acl rule swap index *name index_1index_2*

構文の説明

apply *name*	IPv6 ACL を適用します。IPv6 ACL 名には最大 32 文字の英数字で使用できます。
cpu *name*	IPv6 ACL を CPU に適用します。
cpu none	IPV6 ACL を使用しない場合は、none を設定します。
create	IPv6 ACL を作成します。
delete	IPv6 ACL を削除します。
rule（**action**）（*name*）（*index*）	IPv6 ACL のルール（アクセスの許可または拒否）を設定します。IPv6 ACL 名には最大 32 文字の英数字を使用でき、IPv6 ACL ルール インデックスには 1 ー 32 を指定できます。
{**permit** | **deny**}	IPv6 ルールのアクションを許可または拒否します。
add *name index*	新しいルールおよびルール インデックスを追加します。
change *name old_index new_index*	ルールのインデックスを変更します。
delete *name index*	ルールおよびルール インデックスを削除します。

destination address *name index ip_addr prefix-len*	ルールの宛先 IP アドレスとプレフィックス長（0 ー 128）を設定します。
destination port *name index*	ルールの宛先ポート範囲を設定します。IPv6 ACL 名を入力し、その ACL のルール インデックスを設定します。
direction *name index* {**in** | **out** | **any**}	ルールの方向（in、out、または any）を設定します。
dscp *name index dscp*	ルールの DSCP を設定します。DSCP のルール インデックスの場合は、0 ー 63 の数字または **any** を選択してください。
protocol *name index protocol*	ルールのプロトコルを設定します。名前を入力し、次のインデックスを設定します：0 ー 255 または **any**
source address *name index ip_address prefix-len*	ルールの送信元 IP アドレスとネットマスクを設定します。
source port range *name index start_port end_port*	ルールの送信元ポート範囲を設定します。
swap index *name index_1 index_2*	ルールの 2 つのインデックスを入れ替えます。

コマンド デフォルト

ACL を追加すると、**config ipv6 acl cpu** はデフォルトで **enabled** 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。。
8.0	このコマンドが更新され、 **cpu** および **none** キーワードと *ipv6_acl_name* 変数が追加されました。

使用上のガイドライン

Cisco 2100 シリーズ ワイヤレス LAN コントローラの場合、外部 Web サーバに対して無線 LAN で事前認証 ACL を設定する必要があります。この ACL は、Web ポリシーで無線 LAN 事前認証 ACL として設定する必要があります。ただし、Cisco 4400 シリーズ ワイヤレス LAN コントローラの場合は事前認証 ACL を設定する必要はありません。

次に、アクセスを許可するよう IPv6 ACL を設定する例を示します。

```
(Cisco Controller) >config ipv6 acl rule action lab1 4 permit
```

次に、インターフェイス ACL を設定する例を示します。

```
(Cisco Controller) > config ipv6 interface acl management IPv6-Acl
```

関連コマンド

show ipv6 acl detailed

show ipv6 acl cpu

config ipv6 capwap

Cisco ワイヤレス LAN コントローラで CAPWAP AP の IPv6 の CAPWAP UDPLite を有効または無効にするには、**config ipv6 capwap** コマンドを使用します。

config ipv6 capwap udplite {**enable** | **disable**} [**all** | **<Cisco AP>**]

構文の説明

udplite	CAPWAP UDP Lite の IPv6 を設定します。
enable	IPv6 の CAPWAP UDP Lite を有効にします。
disable	IPv6 の CAPWAP UDP Lite を無効にします。
all	すべての Cisco AP で IPv6 の CAPWAP UDP Lite を有効または無効にします。
<Cisco AP>	ユーザが定義した Cisco AP で IPv6 の CAPWAP UDP Lite を有効または無効にします。

コマンド デフォルト

config ipv6 capwap udplite コマンドは、デフォルトでは **enabled** に設定されています。

コマンド履歴

リリース	変更内容
8.0	このコマンドはリリース 8.0 で導入されました。

使用上のガイドライン

- IPv6 の CAPWAP UDP Lite の設定は、IPv6 トンネルを使用してコントローラに接続されている AP だけに適用されます。
- IPv4 トンネルを使用して WLC に接続されている AP の場合、IPv6 の CAPWAP UDPLite のコマンドは、グローバル設定にも AP ごとにも適用されません。
- IPv6 には UDP の完全なペイロード チェックサムが必要です。これにより、パフォーマンスが影響を受けます。影響を最小限に抑えるために、データ トラフィックには UDPLite（ヘッダー チェックサムだけが必要）が使用され、制御トラフィックには UDP が使用されます。
- UDP Lite の使用はファイアウォールに影響します。中間ファイアウォールは、UDP Lite プロトコル（プロトコル ID 136）のパケットを許可するように設定する必要があります。
- UDP Lite をオフにすると、パケット処理においてパフォーマンス上の問題が発生します。
- UDP から UDPLite へ、またはその逆に変更する場合、AP は参加解除と再参加を強制されます。

次に、すべての Cisco AP または特定の Cisco AP で IPv6 の CAPWAP UDP Lite を設定する例を示します。

```
(Cisco Controller) >config ipv6 capwap udplite enable all
Changing AP's IPv6 Capwap UDP Lite mode will cause the AP to rejoin.
Are you sure you want to continue? (y/n)
```

config ipv6 interface

IPv6 システム インターフェイスを設定するには、**config ipv6 interface** コマンドを使用します。

config ipv6 interface {**acl** | **address** | **slaac**}

config ipv6 interface acl management *acl_name*

config ipv6 interface address {**management primary** *ipv6_address prefix_length ipv6_gateway_address* | **service-port** *ipv6_address prefix-length*}

config ipv6 interface slacc service-port［**enable** | **disable**］

構文の説明

acl	インターフェイスのアクセス コントロール リストで IPv6 を設定します。
management	管理インターフェイスを設定します。
acl_name	管理 ACL の IPv6 ACL 名を入力します。最大 32 文字の英数字で指定できます。
address	インターフェイスのアドレス情報で IPv6 を設定します。
management	管理インターフェイスを設定します。
primary	インターフェイスのプライマリ IPv6 アドレスを設定します。
ipv6_address	IPv6 アドレス情報でインターフェイスを設定します。
prefix_length	IPv6 プレフィックス長を設定します。プレフィックス長の範囲は 1 ー 127 です。
ipv6_gateway_address	リンク層 IPv6 ゲートウェイ アドレスを設定します。
service-port	アウトオブバンド サービス ポートで IPv6 を設定します。
ipv6_address	IPv6 アドレス情報でインターフェイスを設定します。
prefix_length	IPv6 プレフィックス長を設定します。プレフィックス長の範囲は 1 ー 127 です。

slacc	インターフェイスでSLAACオプションを設定します。
service-port	アウトオブバンド サービス ポートで IPv6 を設定します。
enable	SLAAC オプションを有効にします。
disable	SLAAC オプションを無効にします。

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	このコマンドはリリース 8.0 で導入されました。

次に、IPv6 ACL 管理インターフェイスを設定する例を示します。

```
(Cisco Controller) >config ipv6 interface acl management Test_ACL
```

次に、IPv6 アドレスとプライマリ インターフェイスを設定する例を示します。

```
(Cisco Controller) > config ipv6 interface address management primary 2001:9:10:56::44
64 fe80::aea0:16ff:fe4f:2244
```

関連コマンド

show interface detailed management

show ipv6 interface summary

config ipv6 interface multicast

IPv6 マルチキャストを設定するには、**config ipv6 multicast** コマンドを使用します。

config ipv6 multicast mode {**unicast** | **multicast** *ipv6_address*}

構文の説明

mode	コントローラを AP マルチキャストまたはブロードキャスト IPv6 トラフィック転送モードに設定します。
unicast	マルチキャスト/ブロードキャスト IPv6 パケットは、AP へのユニキャスト CAPWAP トンネルにカプセル化されます。
multicast	マルチキャスト/ブロードキャスト IPv6 パケットは、AP へのマルチキャスト CAPWAP トンネルにカプセル化されます。
ipv6_address	IPv6 マルチキャスト アドレスを設定します。

コマンド デフォルト

- Cisco WLC 8500 および Cisco WLC 2500 ではマルチキャストがデフォルトで有効になっています。
- Cisco WLC 5500 ではユニキャストがデフォルトで有効になっています。

コマンド履歴

リリース	変更内容
8.0	このコマンドはリリース 8.0 で導入されました。

使用上のガイドライン

ありません。

次に、アクセスを許可するように Cisco WLC で IPv6 マルチキャストを設定する例を示します。

```
(Cisco Controller) >config ipv6 multicast 2001:DB8:0000:0000:0000:0000:0000:0001
```

次に、アクセスを許可するように Cisco WLC で IPv6 ユニキャストを設定する例を示します。

```
(Cisco Controller) > config ipv6 multicast mode unicast
```

関連コマンド

show network summary

config ipv6 neighbor-binding

シスコのワイヤレス LAN コントローラでネイバー バインディング テーブルを設定するには、**config ipv6 neighbor-binding** コマンドを使用します。

config ipv6 neighbor-binding {**timers** {**down-lifetime** *down_time* | **reachable-lifetime** *reachable_time* | **stale-lifetime** *stale_time* } | { **ra-throttle** {**allow at-least** *at_least_value*} | **enable** | **disable** | **interval-option** { **ignore** | **passthrough** | **throttle** } | **max-through** {*no_mcast_RA* | **no-limit**} | **throttle-period** *throttle_period*} }

構文の説明

timers	ネイバー バインディング テーブルのタイムアウト タイマーを設定します。
down-lifetime	ダウン ライフタイムを設定します。
down_time	秒単位のダウン ライフタイム。指定できる範囲は 0 ～ 86400 です。デフォルトは 30 秒です。
reachable-lifetime	到達可能なライフタイムを設定します。
reachable_time	秒単位の到達可能なライフタイム。指定できる範囲は 0 ～ 86400 です。デフォルトは 300 秒です。
stale-lifetime	古いライフタイムを設定します。
stale_time	秒単位の古いライフタイム。指定できる範囲は 0 ～ 86400 です。デフォルトは 86400 秒です。
ra-throttle	IPv6 RA スロットリング オプションを設定します。
allow	スロットル期間ごとに、ルータ 1 台あたりのマルチキャスト RA の数を指定します。
at_least_value	スロットリング前のルータからのマルチキャスト RA 数。有効な範囲は 0 ～ 32 です。デフォルトは 1 です。
enable	IPv6 RA スロットリングをイネーブルにします。
disable	IPv6 RA スロットリングをディセーブルにします。

interval-option	RFC3775 間隔オプションで RA の動作を調整します。
ignore	間隔オプションが、スロットリングに影響しないことを示します。
passthrough	RFC3775 間隔オプションですべての RA が転送されることを示します（デフォルト）。
throttle	RFC3775 間隔オプションですべての RA がスロットルされることを示します。
max-through	スロットル期間ごとに、VLANあたりのスロットルされない RA の数を指定します。
no_mcast_RA	スロットルを適用にする VLAN のマルチキャスト RA の数。vlan のデフォルト マルチキャスト RA は、10 です。
no-limit	VLAN レベルで、上限を設定しません。
throttle-period	スロットル期間を設定します。
throttle_period	秒単位のスロットル期間の長さ。範囲は 10 ～ 86400 秒です。デフォルトは 600 秒です。

コマンド デフォルト

このコマンドは、デフォルトでディセ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、ネイバー バインディング テーブルを設定する例を示します。

```
(Cisco Controller) >config ipv6 neighbor-binding ra-throttle enable
```

関連コマンド

show ipv6 neighbor-binding

config ipv6 na-mcast-fwd

ネイバー アドバタイズメント マルチキャスト転送を設定するには、**config ipv6 na-mcast-fwd** コマンドを使用します。

config ipv6 na-mcast-fwd {**enable** | **disable**}

構文の説明

enable	ネイバーアドバタイズメントマルチキャスト転送を有効にします。
disable	ネイバーアドバタイズメントマルチキャスト転送を無効にします。

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
7.5	このコマンドが導入されました。

使用上のガイドライン

ネイバー アドバタイズメント マルチキャスト転送を有効にすると、有線またはワイヤレスからのすべての未承認マルチキャスト ネイバー アドバタイズメントがワイヤレスに転送されなくなります。

ネイバー アドバタイズメント マルチキャスト転送を無効にすると、コントローラの IPv6 重複アドレス検出（DAD）が影響を受けます。

次に、ネイバー アドバタイズメント マルチキャスト転送を設定する例を示します。

```
(Cisco Controller) >config ipv6 na-mcast-fwd enable
```

config ipv6 ns-mcast-fwd

ノンストップ マルチキャスト キャッシュ ミス転送を設定するには、**config ipv6 ns-mcast-fwd** コマンドを使用します。

config ipv6 ns-mcast-fwd {**enable** | **disable**}

構文の説明

enable	キャッシュ ミス時のノンストップ マルチキャスト転送を有効にします。
disable	キャッシュ ミス時のノンストップ マルチキャスト転送を無効にします。

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、ノンストップ マルチキャスト転送を設定する例を示します。

```
(Cisco Controller) >config ipv6 ns-mcast-fwd enable
```

config ipv6 ra-guard

AP でクライアントから発信されるルータアドバタイズメント（RA）パケットのフィルタ処理を設定するには、**config ipv6 ra-guard** コマンドを使用します。

config ipv6 ra-guard ap {**enable** | **disable**}

構文の説明

enable	AP で RA ガードを有効にします。
disable	AP で RA ガ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。

次に、IPv6 RA ガードを有効にする例を示します。

```
(Cisco Controller) >config ipv6 ra-guard enable
```

関連コマンド

show ipv6 ra-guard

config ipv6 route

IPv6 ネットワーク ルートを追加または削除するには、**config ipv6 route** コマンドを使用します。

config ipv6 route {**add** *network_ipv6_addr prefix-len ipv6_gw_addr* | **delete** *network _ipv6 addr* }

構文の説明

add	IPv6 ネットワーク ルートを追加します。
network_ipv6_addr	ネットワークの IPv6 アドレスを入力します。
prefix-len	ネットワークのプレフィックス長を入力します。
ipv6_gw_addr	システム インターフェイスを設定します。
delete	IPv6 ネットワーク ルートを削除します。
network_ipv6_addr	ネットワークの IPv6 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
8.0	このコマンドはリリース 8.0 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、異なるネットワークから IPv6 経由でサービス インターフェイスにアクセスするための IPv6 ネットワーク ルートを追加および削除するために使用されます。
- IPv6 ルートの追加中は、IPv6 ゲートウェイ アドレスがリンク ローカル スコープ（FE80::/64）である必要があります。

次に、IPv6 ルートを追加する例を示します。

```
(Cisco Controller) > config ipv6 route add 3010:1111:2222:abcd:abcd:abcd:abcd:1111 64
fe80::6616:8dff:fed3:c0cf
```

次に、IPv6 ルートを削除する例を示します。

```
(Cisco Controller) > config ipv6 route delete 2001:9:5:90::115
```

関連コマンド

show ipv6 route summary