

## MAC 認証バイパス

- MAC 認証バイパス (1ページ)
- •WLAN の 802.11 セキュリティの設定(GUI) (3ページ)
- •WLANの 802.11 セキュリティの設定(CLI) (4ページ)
- 外部認証用の AAA の設定 (5ページ)
- ローカル認証用の AAA の設定(GUI) (6 ページ)
- ローカル認証用の AAA の設定(CLI) (7 ページ)
- ローカル認証用の MAB の設定 (8 ページ)
- 外部認証用の MAB の設定(GUI) (9ページ)
- 外部認証用の MAB の設定(CLI) (9ページ)

### MAC 認証バイパス

MAC 認証バイパス(MAB)機能を使用し、クライアント MAC アドレスに基づいてクライア ントを許可するように 組み込みワイヤレスコントローラを設定できます。

MABを有効にすると、組み込みワイヤレスコントローラはクライアントIDとしてMACアドレスを使用します。認証サーバーには、ネットワークアクセスを許可されたクライアントMACアドレスのデータベースがあります。クライアントの検出後、組み込みワイヤレスコントローラはクライアントからのパケットを待機します。組み込みワイヤレスコントローラは、MACアドレスに基づくユーザー名とパスワードを含むRADIUSアクセス/要求フレームを認証サーバーに送信します。認証が成功すると、組み込みワイヤレスコントローラはクライアントにネットワークへのアクセス権を付与します。認証が失敗した場合、ゲストWLANが設定されていれば、組み込みワイヤレスコントローラはゲストWLANにポートを割り当てます。

MAC 認証バイパスで認証されたクライアントは再認証できます。再認証プロセスは、認証さ れたクライアントの場合と同じです。再認証の間、ポートは前に割り当てられた WLAN のま まです。再認証が成功すると、組み込みワイヤレスコントローラは同じ WLAN でポートを保 持します。再認証が失敗した場合、ゲスト WLAN が設定されていれば、組み込みワイヤレス コントローラはゲスト WLAN にポートを割り当てます。

### MABの設定に関する注意事項

- •MABの設定に関する注意事項は、802.1x認証の注意事項と同じです。
- MACアドレスで認可された後にポートで MAB を無効にしても、ポートステートに影響 はありません。
- ・ポートが未許可ステートであり、クライアント MAC アドレスが認証サーバーデータベー スにない場合、ポートは未許可ステートのままです。ただし、クライアント MAC アドレ スがデータベースに追加されると、スイッチは MAC 認証バイパス機能を使用してポート を再認証できます。
- ポートが認証ステートにない場合、再認証が行われるまでポートはこのステートを維持します。
- MABによって接続されているにもかかわらず非アクティブなホストのタイムアウト時間 を設定できます。有効な範囲は1~65535秒です。

(注) ユーザーに対して wlan-profile-name が設定されている場合、ゲストユーザー認証はその WLAN からのみ許可されます。

ユーザーに対して wlan-profile-name が設定されていない場合、すべての WLAN でゲストユー ザー認証が許可されます。

クライアントを SSID1 に接続するが、MAC フィルタリングを使用して SSID2 には接続しない 場合は、ポリシープロファイルで aaa-override を設定してください。

次の例では、MAC アドレスが 1122.3344.0001 のクライアントが WLAN に接続しようとする と、要求がローカル RADIUS サーバーに送信され、属性リスト(FILTER\_1および FILTER\_2) にクライアントの MAC アドレスが存在するかどうかがチェックされます。クライアントの MAC アドレスが属性リスト(FILTER\_1)にリストされている場合、クライアントは、RADIUS サーバーから ssid 属性として返される WLAN(WLAN\_1)に接続できます。クライアントの MAC アドレスが属性リストにリストされていない場合、そのクライアントは拒否されます。

ローカル RADIUS サーバーの設定

```
!Configures an attribute list as FILTER_2
aaa attribute list FILTER_2
!Defines an attribute type that is to be added to an attribute list.
attribute type ssid "WLAN_2"
!Username with the MAC address is added to the filter
username 1122.3344.0002 mac aaa attribute list FILTER_2
```

! aaa attribute list FILTER\_1 attribute type ssid "WLAN\_1" username 1122.3344.0001 mac aaa attribute list FILTER 1

#### **Controller Configuration**

! Sets authorization to the local radius server aaa authorization network MLIST MACFILTER local

!A WLAN with the SSID WLAN\_2 is created and MAC filtering is set along with security
parameters.
wlan WLAN\_2 2 WLAN\_2
mac-filtering MLIST\_MACFILTER
no security wpa
no security wpa wpa2 ciphers
!WLAN with the SSID WLAN 1 is created and MAC filtering is set along with security

parameters. wlan WLAN\_1 1 WLAN\_1 mac-filtering MLIST\_MACFILTER no security wpa no security wpa wpa2 ciphers aes no security wpa akm dot1x security web-auth security web-auth ! Policy profile to be associated with the above WLANS wireless profile policy MAC FILTER POLICY

#### wireless profile policy MAC\_FILTER\_POLICY aaa-override vlan 504 no shutdown

### WLAN の 802.11 セキュリティの設定(GUI)

手順

- ステップ1 [Configuration] > [Tags & Profiles] > [WLANs] を選択します。
- ステップ2 [Add] をクリックして WLAN を作成します。

[Add WLAN] ページが表示されます。

- ステップ3 [Security] タブで次の設定を行えます。
  - ・レイヤ2
  - Layer3
  - AAA
- ステップ4 [Layer2] タブで次の設定を行えます。
  - a) [Layer2 Security Mode] を次のオプションから選択します。
    - [None]: レイヤ2セキュリティなし。
    - [WPA + WPA2] : Wi-Fi Protected Access<sub> $\circ$ </sub>
    - Static WEP:静的 WEP 暗号化パラメータ。
  - b) 必要に応じて、[MAC Filtering] を有効にしますMAC フィルタリングは、MAC 認証バイパス(MAB) とも呼ばれます。

- c) [Protected Management Frame] セクションの [PMF] で、[Disabled]、[Optional]、または [Required] を選択します。デフォルトでは、PMF は無効になっています。
- d) [WPA Parameters] セクションで、必要に応じて次のオプションを選択します。
  - WPA Policy
  - WPA2 Policy
  - WPA2 Encryption
- e) [Auth Key Mgmt] のオプションを選択します。
- f) AP 間の [Fast Transition] の適切なステータスを選択します。
- g) 分散システム経由の高速移行を有効にするには、[Over the DS] チェック ボックスをオンに します。
- h) [Reassociation Timeout] の値(秒単位)を入力します。これは、高速移行の再アソシエー ションがタイムアウトするまでの時間です。
- i) [Save & Apply to Device] をクリックします。
- ステップ5 [Layer3] タブで次の設定を行えます。
  - a) Web ポリシーを使用するには、[Web Policy] チェック ボックスをオンにします。
  - b) 必要な [Webauth Parameter Map] 値をドロップダウンリストから選択します。
  - c) 必要な [Authentication List] 値をドロップダウンリストから選択します。
  - d) [Show Advanced Settings] セクションで、[On Mac Filter Failure] チェック ボックスをオンに します。
  - e) [Conditional Web Redirect] と [Splash Web Redirect] を有効にします。
  - f) ドロップダウンリストから適切な IPv4 および IPv6 ACL を選択します。
  - g) [Save & Apply to Device] をクリックします。
- ステップ6 [AAA] タブで次の設定を行えます。
  - a) ドロップダウンから認証リストを選択します。
  - b) WLAN でローカル EAP 認証を有効にするには、[Local EAP Authentication] チェック ボック スをオンにします。また、必要な [EAP Profile Name] をドロップダウンリストから選択し ます。
  - c) [Save & Apply to Device] をクリックします。

### WLAN の 802.11 セキュリティの設定(CLI)

WLANの 802.11 セキュリティを設定するには、次の手順に従います。

手順		
	コマンドまたはアクション	目的
ステップ1	wlan profile-name wlan-id ssid	WLAN プロファイルを設定します。
	例:	
	Device(config)# wlan ha-wlan-dotlx-test 3 ha-wlan-dotlx-test	
ステップ2	security dot1x authentication-list auth-list-name	dot1x セキュリティ用のセキュリティ認 証リストを有効にします。
	例:	
	Device(config-wlan)# security dot1x authentication-list default	
ステップ3	no shutdown	WLAN をイネーブルにします。
	例:	
	Device(config-wlan)# no shutdown	

## 外部認証用のAAAの設定

外部認証用に AAA を設定するには、次の手順に従います。

	コマンドまたはアクション	目的
ステップ1	radius server server-name	Radius サーバーを設定します。
	例:	
	Device(config)# radius server ISE	
ステップ2	address {ipv4	Radius サーバーのアドレスを指定しま
	<b>ipv6</b> } <i>radius-server-ip-address</i> <b>auth-port</b> <i>auth-port-no</i> <b>acct-port</b> <i>acct-port-no</i>	-j-,
	. נילו	
	<pre>Device(config-radius-server)# address ipv4 9.2.58.90 auth-port 1812 acct-port 1813</pre>	
ステップ3	key key	サーバーごとの暗号キーを設定しま
	例:	す。
	Device(config-radius-server)# key any123	
ステップ4	exit	コンフィギュレーションモードに戻り
	例:	ます。

	コマンドまたはアクション	目的
	Device(config-locsvr-da-radius)# exit	
ステップ5	aaa local authentication default authorization default	デフォルトのローカル認証および許可 を選択します。
	例: Device(config)# aaa local authentication default authorization default	
ステップ6	aaa new-model 例: Device(config)# aaa new-model	AAA認証モデルを作成します。新しい アクセス制御コマンドと機能を有効に します。
ステップ <b>1</b>	aaa session-id common 例: Device(config)# aaa session-id common	コモン セッション ID を作成します。
ステップ8	aaa authentication dot1x default group radius 例: Device(config)# aaa authentication dot1x default group radius	デフォルトの dot1x 方式の認証を設定 します。
ステップ <b>9</b>	aaa authorization network default group radius 例: Device(config)# aaa authorization network default group radius	ネットワークサービスに対する認証を 設定します。
ステップ10	dot1x system-auth-control 例: Device(config)# dot1x system-auth-control	SysAuthControl を有効にします。

# ローカル認証用の AAA の設定(GUI)

- ステップ1 [Configuration] > [Tags & Profiles] > [WLANs] を選択します。
- ステップ2 [Wireless Networks] ページで [Add] をクリックします。
- ステップ3 表示される [Add WLAN] ウィンドウで、[Security] > [AAA] を選択します。
- ステップ4 [Authentication List] ドロップダウンから値を選択します。

- **ステップ5** WLAN でローカル EAP 認証を有効にするには、[Local EAP Authentication] チェック ボックス をオンにします。
- ステップ6 [EAP Profile Name] ドロップダウンから値を選択します。
- ステップ7 [Save & Apply to Device] をクリックします。

## ローカル認証用の AAA の設定(CLI)

ローカル認証用に AAA を設定するには、次の手順に従います。

	コマンドまたはアクション	目的
ステップ1	aaa authentication dot1x default local 例: Device(config)# aaa authentication dot1x default local	デフォルトのローカルRADIUSサーバー を使用するように設定します。
ステップ <b>2</b>	aaa authorization network default local 例: Device(config)# aaa authorization network default local	ネットワークサービスに対する認証を設 定します。
ステップ3	aaa authorization credential-download default local 例: Device(config)# aaa authorization credential-download default local	ローカル サーバーからログイン情報を ダウンロードするようにデフォルトデー タベースを設定します。
ステップ4	username mac-addressmac 例: Device(config)# username abcdabcdabcd mac	ユーザー名を使用したMACフィルタリ ングには、 <b>username</b> <i>abcdabcdabcd</i> <b>mac</b> コマンドを使用します。
ステップ5	aaa local authentication default authorization default 例: Device(config)# aaa local authentication default authorization default	ローカル認証方式リストを設定します。
ステップ6	aaa new-model 例: Device(config)# aaa new-model	AAA 認証モデルを作成します。新しい アクセス制御コマンドと機能を有効にし ます。

	コマンドまたはアクション	目的
ステップ <b>1</b>	aaa session-id common	コモン セッション ID を作成します。
	例:	
	Device(config)# aaa session-id common	

## ローカル認証用の MAB の設定

ローカル認証用に MAB を設定するには、次の手順に従います。

#### 始める前に

AAA ローカル認証を設定します。

**username** *mac-address* **mac** コマンドを使用して、WLAN 設定(ローカル認証)のユーザー名を 設定します。

(注)

MAC アドレスの形式は、abcdabcdabcd にする必要があります。

	コマンドまたはアクション	目的
ステップ1	wlan profile-name wlan-id	WLAN の名前と ID を指定します。
	例:	
	wlan CR1_SSID_mab-local-default 1 CR1_SSID_mab-local-default	
ステップ2	mac-filtering default	WLAN の MAC フィルタリング サポー
	例:	トを設定します。
	Device(config-wlan)# mac-filtering default	
ステップ3	no security wpa	WPA セキュリティを無効にします。
	例:	
	Device(config-wlan)# no security wpa	
ステップ4	no security wpa akm dot1x	dot1x に対するセキュリティの AKM を
	例:	ディセーブルにします。
	Device(config-wlan)# no security wpa akm dot1x	
ステップ5	no security wpa wpa2	WPA2 セキュリティを無効にします。
	例:	

	コマンドまたはアクション	目的
	<pre>Device(config-wlan)# no security wpa wpa2</pre>	
ステップ6	no security wpa wpa2 ciphers aes	AESのWPA2暗号化をディセーブルに します。
	191 :	
	<pre>Device(config-wlan)# no security wpa wpa2 ciphers aes</pre>	
ステップ1	no shutdown	WLAN をイネーブルにします。
	例:	
	Device(config-wlan)# no shutdown	

## 外部認証用の MAB の設定(GUI)

#### 始める前に

AAA 外部認証を設定します。

#### 手順

- ステップ1 [Configuration] > [Wireless] > [WLANs] の順に選択します。
- ステップ2 [Wireless Networks] ページで WLAN の名前をクリックします。
- ステップ3 [Edit WLAN] ウィンドウで [Security] タブをクリックします。
- ステップ4 [Layer2] タブで、[MAC Filtering] チェック ボックスをオンにして機能を有効にします。
- **ステップ5** MAC フィルタリングを有効にした状態で、ドロップダウンリストから [Authorization List] を選択します。
- ステップ6 設定を保存します。

### 外部認証用の MAB の設定(CLI)

外部認証用に MAB を設定するには、次の手順に従います。

#### 始める前に

AAA 外部認証を設定します。

I

ステップ1       Wian wlan-name wlan-id ssid-name       WLAN の名前とID を指定します。         例:       wlan CR1_SSID_mab-ext-radius 3       WLAN の名前とID を指定します。         ステップ2       mac-filtering list-name       MAC フィルタリングパラメータをします。ここで、ewlc-radius はlist- の例です         フテップ3       no security wpa       MAC フィルタリングパラメータを します。ここで、ewlc-radius はlist- の例です         ステップ3       no security wpa       WPA セキュリティを無効にします         ステップ4       no security wpa akm dot1x       dot1x に対するセキュリティの AK ディセーブルにします。         例:       Device(config-wlan) # no security wpa akm dot1x       dot1x に対するセキュリティの AK ディセーブルにします。         ステップ5       no security wpa wpa2       WPA2 セキュリティを無効にします         例:       Device(config-wlan) # no security wpa wpa2       オブション。WLAN でMAC フィル ングを使用する際のデリミタを設定 す。         ステップ6       mab request format attribute {1 groupsize size separator separator [lowercase] uppercase]   2 {0 7  LINE} LINE password   32 vlan access-vlan} 例:       オブション。WLAN でMAC フィル ングを使用する際のデリミタを設定 す。         例:       Device(config) # mab request format attribute 1 groupsize 4 separator       1: MAB 要求に使用するユーザー名 と指定します。         groupsize size: グルーブごとの 16 の桁数を指定します。 EGUり 文字は、 マ、セミュロン、およびピリオドで lowercase: ニーザー名を小文字で l = =		コマンドまたはアクション	目的
例: wlan CR1_SSID_mab-ext-radius 3 CR1_SSID_mab-ext-radiusMAC フィルタリングパラメータを します。ここで、ewle-radiusはlist- の例: Device (config-wlan) # mac-filtering ewlo-radiusステップ3no security wpa Ml: Device (config-wlan) # no security wpaWPA セキュリティを無効にしますステップ4no security wpa akm dot1x Ml: Device (config-wlan) # no security wpadot1x に対するセキュリティのAK ディセーブルにします。ステップ5no security wpa wpa2 Ml: Device (config-wlan) # no security wpaWPA2 セキュリティを無効にしますステップ5no security wpa wpa2 Ml: Device (config-wlan) # no security wpaオブション。WLANでMACフィル グン化します。ステップ5no security mat attribute { 1 groupsize size separator separator [lowercase] uppercase]   2 (0   7   LINE) LINE password   32 vlan access-vlan} 例: Device (config) # mab request format attribute 1 groupsize 4 separatorオブション。WLANでMACフィル ングを使用する際のデリミタを設定 す。 ここで、各変数は次のように定義さ す。 ここで、各変数は次のように定義さ す。 ここで、各変数は次のように定義さ す。 ここで、各変数は次のように定義さ す。 ここで、各変数は次のように定義さ す。 ここで、各変数は次のように定義さ す。 ここで、各変数は次のように定義さ す。 ここで、各変数は次のように定義さ す。 ここで、各変数は次のように定義さ 方法を指定します。 なんーブごとの 16 の桁数を指定します。G切り文字は、 マ、セミコロン、およびピリオドで しwercase: ユーザー名を小文字で します	ステップ1	wlan wlan-name wlan-id ssid-name	WLAN の名前と ID を指定します。
wlan CR1_SSID_mab-ext-radius         ステップ2       mac-filtering list-name 例: Device (config-wlan) # mac-filtering ewlc-radius       MAC フィルタリングパラメータを します。ここで、ewlc-radiusはlist- の例です         ステップ3       no security wpa 例: Device (config-wlan) # no security wpa       WPA セキュリティを無効にします         ステップ4       no security wpa akm dot1x 例: Device (config-wlan) # no security wpa akm dot1x       dot1x に対するセキュリティのAK ディセーブルにします。         ステップ5       no security wpa wpa2 例: Device (config-wlan) # no security wpa akm dot1x       dot1x に対するセキュリティを無効にします         ステップ5       no security wpa wpa2 例: Device (config-wlan) # no security wpa akm dot1x       オブション。WLANでMACフィル クリンにします。         ステップ5       mab request format attribute [1 groupsize size separator separator [lowercase] uppercase]   2 (0   7   LINE) LINE password   32 vlan access-vlan} 例: Device (config) # mab request format attribute 1 groupsize 4 separator       オブション。WLANでMACフィル ングを使用する際のデリミタを設定 す。 ここで、各変数は次のように定義さ す。         1: MAB要求に使用するユーザー名 を指定します。 groupsize size : グループごとの 16 の桁数を指定します。 て効な値の範 1 ~ 12 です。       separator separator : グループを広 方法を指定します。 て効な値の範 1 ~ 12 です。		例:	
ステップ2       mac-filtering list-name       MAC フィルタリングパラメータをします。ここで、ewlc-radius はlist- の例です         Aテップ3       no security wpa       MAC フィルタリングパラメータを します。ここで、ewlc-radius はlist- の例です         ステップ3       no security wpa       WPA セキュリティを無効にします         例: Device (config-wlan) # no security wpa       WPA セキュリティを無効にします         ステップ5       no security wpa akm dot1x       dot1x に対するセキュリティのAK ディセーブルにします。         例: Device (config-wlan) # no security wpa akm dot1x       dot1x に対するセキュリティを無効にします         ステップ5       no security wpa wpa2       WPA2 セキュリティを無効にします         例: Device (config-wlan) # no security wpa wpa2       オプション。WLANでMACフィル ングを使用する際のデリミタを設定 す。         ステップ6       mab request format attribute {1 groupsize size separator separator [lowercase   uppercase]   2 {0   7   LINE   LINE password   32 vlan access-vlan} 例: Device (config) # mab request format attribute 1 groupsize 4 separator       オプション。WLANでMACフィル ングを使用するユーザー名 を指定します。 groupsize size : グループごとの 16 の桁数を指定します。反明り文字は、 マ、セミコロン、およびピリオドで lowercase : ユーザー名を小文字で: l. **t		wlan CR1_SSID_mab-ext-radius 3 CR1_SSID_mab-ext-radius	
例:       Device (config-wlan) # mac-filtering ewic-radius       します。ここで、ewic-radius はlist-o例です         ステップ3       no security wpa       WPA セキュリティを無効にします         例:       Device (config-wlan) # no security wpa       dot1x に対するセキュリティのAK         ステップ4       no security wpa akm dot1x       dot1x に対するセキュリティのAK         例:       Device (config-wlan) # no security wpa       dot1x に対するセキュリティのAK         ステップ5       no security wpa wpa2       dot1x に対するセキュリティを無効にします         例:       Device (config-wlan) # no security wpa       wPA2 セキュリティを無効にします         ステップ6       mab request format attribute {1 groupsize xize separator separator [lowercase]       オプション。WLANでMACフィル ングを使用する際のデリミタを設定す。         の:       Device (config) # mab request format attribute 1 groupsize 4 separator       1: MAB 要求に使用するユーザー名を指定します。の所数を指定します。有効な値の領1 ~ 12 です。         groupsize size: グループごとの16       の桁数を指定します。区切り文字に、マ、セミコロン、およびピリオドマレーナを区方法を指定します。区切り文字でも       カメンパーナを区方式を行ってもの、たちまのでもの、アクトックを図り、マイト・	ステップ2	mac-filtering list-name	MACフィルタリングパラメータを設定
Device (config-wlan) # mac-filtering ewlo-radius     の例です       ステッブ3     no security wpa 例: Device (config-wlan) # no security wpa     WPA セキュリティを無効にします       ステッブ4     no security wpa akm dot1x 例: Device (config-wlan) # no security wpa akm dot1x     dot1x に対するセキュリティの AK ディセーブルにします。       ステッブ5     no security wpa wpa2 例: Device (config-wlan) # no security wpa wpa2     WPA2 セキュリティを無効にします       ステッブ6     mab request format attribute {1 groupsize size separator separator [lowercase] uppercase]  2 {0  7   LINE} LINE password   32 vlan access-vlan} 例: Device (config) # mab request format attribute 1 groupsize 4 separator     オプション。WLAN でMAC フィル ングを使用する際のデリミタを設定 す。 ここで、各変数は次のように定義さ す。       1: MAB要求に使用するユーザー名 を指定します。有効な値の範 1 ~ 12 です。     separator separator : グループざとの 16 の桁数を指定します。反切り文字は、 マ、セミュロン、およびビリオドで		例:	します。ここで、ewlc-radius は list-name
ステップ3no security wpa 例: Device (config-wlan) # no security wpaWPA セキュリティを無効にしますステップ4no security wpa akm dot1x 例: Device (config-wlan) # no security wpa akm dot1xdot1x に対するセキュリティのAK ディセーブルにします。ステップ5no security wpa wpa2 例: Device (config-wlan) # no security wpa wpa2WPA2 セキュリティを無効にしますステップ5mab request format attribute {1 groupsize size separator separator [lowercase   uppercase]   2 (0  7) LINE } LINE password   32 vlan access-vlan } 例: Device (config) # mab request format attribute 1 groupsize 4 separatorオプション。WLAN でMAC フィル ングを使用する際のデリミタを設定 す。 ここで、各変数は次のように定義さ す。 1: MAB 要求に使用するユーザー名 を指定します。有効な値の範 1 ~ 12 です。groupsize size : グループごとの 16 の桁数を指定します。反切り文字は、 マ、セミュロン、およびビリオドで Levieseparator separator : グループを区 方法を指定します。区切り文字は、 マ、セミュロン、およびビリオドで Levie		Device(config-wlan)# mac-filtering ewlc-radius	(7)例(())
例: Device(config-wlan) # no security wpadot1x に対するセキュリティのAK ディセーブルにします。ステップ4no security wpa akm dot1x 例: Device(config-wlan) # no security wpa akm dot1xdot1x に対するセキュリティのAK ディセーブルにします。ステップ5no security wpa wpa2 例: Device(config-wlan) # no security wpa wpa2WPA2 セキュリティを無効にしますステップ6mab request format attribute {1 groupsize size separator separator [lowercase] uppercase]   2 {0   7   LINE } LINE password   32 vlan access-vlan} 例: Device(config) # mab request format attribute 1 groupsize 4 separatorオプション。WLAN でMAC フィル ングを使用する際のデリミタを設定 す。 ここで、各変数は次のように定義さ す。 1: MAB 要求に使用するユーザー名 を指定します。 groupsize size : グループごとの 16 の桁数を指定します。互切り文字は、 マ、セミコロン、およびピリオドで lowercase : ユーザー名を小文字で i. + t	ステップ3	no security wpa	WPA セキュリティを無効にします。
Device (config-wlan) # no security wpaステップ4no security wpa akm dot1x 例: Device (config-wlan) # no security wpa akm dot1xdot1x に対するセキュリティのAK ディセーブルにします。ステップ5no security wpa wpa2 例: Device (config-wlan) # no security wpa wpa2WPA2 セキュリティを無効にします。ステップ6mab request format attribute {1 groupsize size separator separator [lowercase] uppercase]   2 {0   7   LINE } LINE password   32 vlan access-vlan } 例: Device (config) # mab request format attribute 1 groupsize 4 separatorオプション。WLAN でMAC フィル ングを使用する際のデリミタを設定 す。 ここで、各変数は次のように定義さ す。 1: MAB 要求に使用するユーザー名 を指定します。 groupsize size : グループごとの 16 の桁数を指定します。 有効な値の範 1 ~ 12 です。separator separator : グループごとの 16 の桁数を指定します。 回り文字は、 マ、セミコロン、およびピリオドで l キオ		例:	
ステップ4       no security wpa akm dot1x       dot1x に対するセキュリティのAK         例:       Device (config-wlan) # no security wpa akm dot1x       dot1x に対するセキュリティのAK         ステップ5       no security wpa wpa2       WPA2 セキュリティを無効にします。         例:       Device (config-wlan) # no security wpa wpa2       WPA2 セキュリティを無効にします。         ステップ6       mab request format attribute {1 groupsize size separator separator [lowercase] uppercase]   2 {0 [7   LINE} LINE password   32 vlan access-vlan}       オプション。WLAN でMACフィルングを使用する際のデリミタを設定 す。         例:       Device (config) # mab request format attribute 1 groupsize 4 separator       エーザー名を指定します。         1:       MAB 要求に使用するユーザー名を指定します。有効な値の範1 ~ 12 です。       separator separator : グループごとの 16 の桁数を指定します。回り文字は、マ、セミコロン、およびピリオドで         の桁数を指定します。回り文字は、マ、セミコロン、およびピリオドで       Ister       マーザー名を小文字でまします。		Device(config-wlan)# no security wpa	
例: Device (config-wlan) # no security wpa akm dot1xディセーブルにします。ステップ5no security wpa wpa2 例: Device (config-wlan) # no security wpa wpa2WPA2 セキュリティを無効にしますステップ6mab request format attribute {1 groupsize size separator separator [lowercase   uppercase]   2 {0   7   LINE } LINE password   32 vlan access-vlan} 例: Device (config) # mab request format attribute 1 groupsize 4 separatorオブション。WLAN でMAC フィル ングを使用する際のデリミタを設定 す。 ここで、各変数は次のように定義さ す。 	ステップ4	no security wpa akm dot1x	dot1x に対するセキュリティの AKM を
Device (config-wlan) # no security wpa akm dot1xWPA2 セキュリティを無効にしますステップ5no security wpa wpa2 例: Device (config-wlan) # no security wpa wpa2WPA2 セキュリティを無効にしますステップ6mab request format attribute {1 groupsize size separator separator [lowercase   uppercase]   2 {0   7   LINE } LINE password   32 vlan access-vlan } 例: Device (config) # mab request format attribute 1 groupsize 4 separatorオプション。WLAN でMAC フィル ングを使用する際のデリミタを設定 す。 ここで、各変数は次のように定義さ す。 1: MAB 要求に使用するユーザー名 を指定します。 groupsize size : グループごとの 16 の桁数を指定します。有効な値の範 1 ~ 12 です。groupsize size : グループごとの 16 の桁数を指定します。区切り文字は、 マ、セミコロン、およびピリオドで します		例:	ディセーブルにします。
ステップ5no security wpa wpa2 例: Device (config-wlan) # no security wpaWPA2 セキュリティを無効にしますステップ6mab request format attribute {1 groupsize size separator separator [lowercase   uppercase]   2 {0   7   LINE } LINE password   32 vlan access-vlan } 例: Device (config) # mab request format attribute 1 groupsize 4 separatorオプション。WLAN でMAC フィル ングを使用する際のデリミタを設定 す。 ここで、各変数は次のように定義さ す。 1 : MAB 要求に使用するユーザー名 を指定します。 groupsize size : グループごとの 16 の桁数を指定します。有効な値の範 1 ~ 12 です。の桁数を指定します。区切り文字は、 マ、セミコロン、およびピリオドで しwercase : ユーザー名を小文字でき します		Device(config-wlan)# no security wpa akm dot1x	
例: Device(config-wlan)# no security wpaオプション。WLANでMACフィル ングを使用する際のデリミタを設定 す。ステップ6mab request format attribute {1 groupsize 	ステップ5	no security wpa wpa2	WPA2 セキュリティを無効にします。
Device (config-wlan) # no security wpa wpa2         ステップ6         mab request format attribute {1 groupsize size separator separator [lowercase   uppercase]   2 {0   7   LINE } LINE password   32 vlan access-vlan}         例:         Device (config) # mab request format attribute 1 groupsize 4 separator         I: MAB 要求に使用するユーザー名を指定します。         groupsize size : グループごとの 16 の桁数を指定します。有効な値の範1 ~ 12 です。         separator separator : グループを区方法を指定します。区切り文字は、マ、セミコロン、およびピリオドでい         iowercase : ユーザー名を小文字でまします。		例:	
<pre>ステップ6 mab request format attribute {1 groupsize size separator separator [lowercase   uppercase]   2 {0   7   LINE } LINE password   32 vlan access-vlan} 例: Device (config) # mab request format attribute 1 groupsize 4 separator</pre> T: MAB 要求に使用するユーザー名を指定します。有効な値の範 1 ~ 12 です。 Separator : グループごとの 16 の桁数を指定します。有効な値の範 1 ~ 12 です。 Separator : グループごとの 16 の桁数を指定します。回り文字は、マ、セミコロン、およびピリオドでは Let t		Device(config-wlan)# no security wpa wpa2	
Ø:ここで、各変数は次のように定義さす。Device (config) # mab request format attribute 1 groupsize 4 separatorここで、各変数は次のように定義さす。1: MAB要求に使用するユーザー名 を指定します。1: MAB要求に使用するユーザー名 を指定します。groupsize size : グループごとの 16 の桁数を指定します。有効な値の範 1 ~ 12 です。の桁数を指定します。有効な値の範 1 ~ 12 です。separator separator : グループを区 方法を指定します。Separator separator : グループを区 方法を指定します。しますーザー名を小文字でき します	ステップ6	mab request format attribute {1 groupsize size separator separator [lowercase   uppercase]   2 {0   7   LINE} LINE password   32 ylan access-ylan}	オプション。WLAN でMACフィルタリ ングを使用する際のデリミタを設定しま す。
Device (config) # mab request format attribute 1 groupsize 4 separator       1: MAB要求に使用するユーザー名を         2       を指定します。         groupsize size : グループごとの16       の桁数を指定します。有効な値の範         1 ~ 12 です。       separator : グループを区         方法を指定します。区切り文字は、       マ、セミコロン、およびピリオドで         lowercase : ユーザー名を小文字でき       します		例:	ここで、各変数は次のように定義されま す。
groupsize size : グループごとの 16         の桁数を指定します。有効な値の範         1 ~ 12 です。         separator separator : グループを区         方法を指定します。区切り文字は、         マ、セミコロン、およびピリオドで         lowercase : ユーザー名を小文字でき         します		Device(config)# mab request format attribute 1 groupsize 4 separator	1:MAB要求に使用するユーザー名形式 を指定します。
<b>separator</b> separator : グループを区 方法を指定します。区切り文字は、 マ、セミコロン、およびピリオドで <b>lowercase</b> : ユーザー名を小文字で します			<b>groupsize</b> <i>size</i> :グループごとの 16 進数 の桁数を指定します。有効な値の範囲は 1 ~ 12 です。
<b>lowercase</b> :ユーザー名を小文字で します			<b>separator</b> <i>separator</i> : グループを区切る 方法を指定します。区切り文字は、コン マ、セミコロン、およびピリオドです。
			<b>lowercase</b> : ユーザー名を小文字で指定 します。

		コマンドまたはアクション	目的
			<b>uppercase</b> :ユーザー名を大文字で指定 します。
			2: すべてのMAB要求に使用するグロー バルパスワードを指定します。
			0:暗号化されていないパスワードを指 定します。
			7:非表示のパスワードを指定します。
			<b>LINE</b> :暗号化されたパスワードまたは 暗号化されていないパスワードを指定し ます。
			<i>password</i> :回線パスワード。
			32: NAS-Identifier 属性を指定します。
			<b>vlan</b> : VLAN を指定します。
			<b>access-vlan</b> :設定されたアクセスVLAN を指定します。
	ステップ1	no security wpa wpa2 ciphers aes 例: Device(config-wlan)# no security wpa wpa2 ciphers aes	AES の WPA2 暗号化をディセーブルに します。
-	ステップ8	no shutdown	WLAN をイネーブルにします。
		例: Device(config-wlan)# no shutdown	

I

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては 、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている 場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容につい ては米国サイトのドキュメントを参照ください。