ISE の簡素化と拡張

- セキュリティ設定用のユーティリティ （1 ページ）
- ローカルおよび中央 Web 認証のキャプティブ ポータル バイパスの設定 （4 ページ）
- DHCP オプション 55 および 77 の ISE への送信 （6 ページ）
- キャプティブ ポータル （9 ページ）

セキュリティ設定用のユーティリティ

この章では、次のコマンドを使用してすべての RADIUS サーバー側設定を行う方法について説明します。

wireless-default radius server *ip* **key** *secret*

この簡易設定オプションは次の機能を提供します。

- ネットワークサービスの AAA 認証、Web 認証および Dot1x の認証を設定します。
- デフォルトの認証を使用してローカル認証を有効にします。
- CWA のデフォルトのリダイレクト ACL を設定します。
- 仮想 IP でグローバルパラメータマップを作成し、キャプティブ バイパス ポータルを有効にします。
- RADIUS サーバーの設定時に、デフォルト ケースのすべての AAA 設定を行います。
- WLAN では、メソッドリストの設定がデフォルトで仮定されます。
- デフォルトで RADIUS アカウンティングを有効にします。
- デフォルトで RADIUS アグレッシブ フェールオーバーを無効にします。
- RADIUS 要求のタイムアウトをデフォルトで 5 秒に設定します。
- キャプティブ バイパス ポータルを有効にします。

このコマンドは、次の設定をバックグラウンドで行います。

```
aaa new-model
aaa authentication webauth default group radius
```

```
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting identity default start-stop group radius
!
aaa server radius dynamic-author
 client <IP> server-key cisco123
!
radius server RAD_SRV_DEF_<IP>
 description Configured by wireless-default
 address ipv4 <IP> auth-port 1812 acct-port 1813
 key <key>
!
aaa local authentication default authorization default
aaa session-id common
!
ip access-list extended CISCO-CWA-URL-REDIRECT-ACL-DEFAULT
remark " CWA ACL to be referenced from ISE "
deny udp any any eq domain
deny tcp any any eq domain
deny udp any eq bootps any
deny udp any any eq bootpc
deny udp any eq bootpc any
deny ip any host <IP>
permit tcp any any eq www
!
parameter-map type webauth global
  captive-bypass-portal
  virtual-ip ipv4 192.0.2.1
  virtual-ip ipv6 1001::1
!
wireless profile policy default-policy-profile
   aaa-override
   local-http-profiling
   local-dhcp-profiling
   accounting
```

このため、設定ガイドの内容をすべて調べなくても、簡易な設定要件を満たすようにワイヤレス 組み込みワイヤレスコントローラを設定することができます。

複数の RADIUS サーバーの設定

RADIUS サーバーを設定するには、次の手順を実行します。

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** **例：** `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wireless-default radius server** *ip* **key** *secret* **例：** `Device(config)# wireless-default radius server 9.2.58.90 key cisco123`	RADIUS サーバーを設定します。 （注） 最大 10 個の RADIUS サーバーを設定できます。

	コマンドまたはアクション	目的
ステップ 3	**end** 例： デバイス(config)# **end**	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

AAA および RADIUS サーバーの設定の確認

AAA サーバーの詳細を表示するには、次のコマンドを使用します。

```
Device# show run aaa
!
aaa new-model
aaa authentication webauth default group radius
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa accounting Identity default start-stop group radius
!
aaa server radius dynamic-author
 client 9.2.58.90 server-key cisco123
!
radius server RAD_SRV_DEF_9.2.58.90
 description Configured by wireless-default
 address ipv4 9.2.58.90 auth-port 1812 acct-port 1813
 key cisco123
!
aaa local authentication default authorization default
aaa session-id common
!
!
ip access-list extended CISCO-CWA-URL-REDIRECT-ACL-DEFAULT
remark " CWA ACL to be referenced from ISE "
deny udp any any eq domain
deny tcp any any eq domain
deny udp any eq bootps any
deny udp any any eq bootpc
deny udp any eq bootpc any
deny ip any host 9.2.58.90
permit tcp any any eq www
!
parameter-map type webauth global
  captive-bypass-portal
  virtual-ip ipv4 192.0.2.1
  virtual-ip ipv6 1001::1
!
wireless profile policy default-policy-profile
   aaa-override
   local-http-profiling
   local-dhcp-profiling
   accounting
```

（注） このユーティリティに新しいコマンドを追加すると **show run aaa** の出力が変わる場合があります。

ローカルおよび中央 Web 認証のキャプティブ ポータル バイパスの設定

キャプティブ バイパスについて

WISPr は、ユーザーが異なるワイヤレス サービス プロバイダ間をローミングできるようにするドラフト プロトコルです。一部のデバイス（Apple iOS デバイスなど）には、指定の URL に対する HTTP WISPr 要求に基づいて、デバイスがインターネットに接続するかどうかを決定するときに使用するメカニズムが搭載されています。このメカニズムは、インターネットへの直接接続が不可能なときにデバイスが自動的に Web ブラウザを開くために使用されます。これにより、ユーザーがインターネットにアクセスするために、自身の認証情報を提供することが可能となります。実際の認証は、デバイスが新しい SSID に接続するたびにバックグラウンドで実行されます。

クライアントデバイス（Apple iOS デバイス）は、WISPr 要求を組み込みワイヤレスコントローラに送信します。コントローラはユーザーエージェントの詳細をチェックし、組み込みワイヤレスコントローラでの Web 認証代行受信により HTTP リクエストをトリガーします。ユーザーエージェントによって提供される iOS バージョンおよびブラウザの詳細の確認後、クライアントは、組み込みワイヤレスコントローラによってキャプティブポータル設定のバイパスを許可され、インターネットにアクセスできます。

この HTTP 要求は、他のページ要求がワイヤレスクライアントによって実行されると、組み込みワイヤレスコントローラでの Web 認証代行受信をトリガーします。この代行受信によって Web 認証プロセスが発生し、プロセスは正常に完了します。Web 認証がいずれかの 組み込みワイヤレスコントローラ スプラッシュページ機能で使用されている場合（設定された RADIUS サーバーが URL を指定）、WISPr 要求が非常に短い間隔で発信されるため、スプラッシュページは表示されず、いずれかのクエリが指定のサーバーに到達可能になるとただちに、バックグラウンドで実行されている Web リダイレクションまたはスプラッシュページ表示プロセスがキャンセルされます。そして、デバイスによってページ要求が処理され、スプラッシュページ機能は中断されます。

たとえば、Apple は iOS 機能を導入して、キャプティブ ポータルがある場合のネットワーク アクセスを容易にしました。この機能では、ワイヤレス ネットワークへの接続に関する Web 要求を送信することにより、キャプティブ ポータルの存在を検出します。この要求は、Apple iOS バージョン 6 以前の場合は http://www.apple.com/library/test/success.html に、Apple iOS バージョン 7 以降の場合は複数の該当するターゲット URL に送信されます。応答が受信されると、インターネット アクセスが使用可能であると見なされ、それ以上の操作は必要ありません。応答が受信されない場合、インターネット アクセスはキャプティブ ポータルによってブロックされたと見なされ、Apple の Captive Network Assistant（CNA）が疑似ブラウザを自動起動して管理ウィンドウでポータル ログインを要求します。ISE キャプティブ ポータルへのリダイレクト中に、CNA が切断される場合があります。 組み込みワイヤレスコントローラは、この疑似ブラウザがポップアップ表示されないようにします。

現在、WISPr検出プロセスをバイパス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るようになりました。それによって、ユーザーが、ユーザーコンテキストでスプラッシュページのロードを引き起こす Web ページを要求したときに、バックグラウンドで WISPr 検出を実行せずに、Web 認証代行受信だけが行われるようにすることができます。

LWA および CWA における WLAN のキャプティブ バイパスの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Security]** > **[Web Auth]** の順に選択します。

ステップ 2 [Webauth Parameter Map] タブで、パラメータ マップ名をクリックします。[Edit WebAuth Parameter] ウィンドウが表示されます。

ステップ 3 [Captive Bypass Portal] チェックボックスをオンにします。

ステップ 4 [Update & Apply to Device] をクリックします。

LWA および CWA内の WLAN におけるキャプティブ バイパスの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル設定モードを開始します。
ステップ 2	**parameter-map type webauth** *parameter-map-name* 例： `Device(config)# parameter-map type webauth WLAN1_MAP`	パラメータ マップを作成します。 *parameter-map-name* は 99 文字を超えないようにする必要があります。
ステップ 3	**captive-bypass-portal** 例： `Device(config)# captive-bypass-portal`	キャプティブ バイパスを設定します。
ステップ 4	**wlan** *profile-name wlan-id ssid-name* 例：	WLAN の名前と ID を指定します。 • *profile-name* は、最大 32 文字の英数字からなる WLAN 名です。

	コマンドまたはアクション	目的
	`Device(config)# wlan WLAN1_NAME 4 WLAN1_NAME`	• *wlan-id* はワイヤレス LAN の ID です。有効な範囲は 1 ～ 512 です。 • *ssid-name* は、最大 32 文字の英数字からなる SSID です。
ステップ 5	**security web-auth** 例： `Device(config-wlan)# security web-auth`	WLAN の Web 認証を有効にします。
ステップ 6	**security web-auth parameter-map** *parameter-map-name* 例： `Device(config-wlan)# security web-auth parameter-map WLAN1_MAP`	パラメータ マップをマッピングします。 （注） パラメータ マップが WLAN に関連付けられていない場合は、グローバル パラメータ マップの設定と見なされます。
ステップ 7	**end** 例： `Device(config-wlan)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

DHCP オプション 55 および 77 の ISE への送信

DHCP オプション 55 および 77 について

DHCP センサーは、ネイティブおよびリモート プロファイリングのために、ISE で次の DHCP オプションを使用します。

- **オプション 12**：ホスト名
- **オプション 6**：クラス ID

これと一緒に、次のオプションをプロファイリングのために ISE に送信する必要があります。

- **オプション 55**：パラメータ要求リスト
- **オプション 77**：ユーザー クラス

DHCP オプション 55 および 77 を ISE に送信するための設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Tags & Profiles]** > **[Policy]** を選択します。

ステップ 2 [Policy Profile] ページで、[Add] をクリックして [Add Policy Profile] ウィンドウを表示します。

ステップ 3 [Access Policies] タブをクリックし、[RADIUS Profiling] チェックボックスと [DHCP TLV Caching] チェックボックスをオンにして、WLANで RADIUS プロファイリングと DHCP TLV キャッシングを設定します。

ステップ 4 [Save & Apply to Device] をクリックします。

DHCP オプション 55 および 77 を ISE に送信するための設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wireless profile policy** *profile-policy* 例： `Device(config)# wireless profile policy rr-xyz-policy-1`	WLAN ポリシー プロファイルを設定し、ワイヤレス ポリシー コンフィギュレーション モードを開始します。
ステップ 3	**dhcp-tlv-caching** 例： `Device(config-wireless-policy)# dhcp-tlv-caching`	WLAN で DHCP TLV キャッシングを設定します。
ステップ 4	**radius-profiling** 例： `Device(config-wireless-policy)# radius-profiling`	WLAN でクライアント RADIUS プロファイリングを設定します。
ステップ 5	**end** 例： `Device(config-wireless-policy)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

EAP 要求のタイムアウトの設定（GUI）

以下の手順に従って、GUI を使用して EAP 要求タイムアウトを設定します。

手順

ステップ 1 **[Configuration]** > **[Security]** > **[Advanced EAP]** を選択します。

ステップ 2 [EAP-Identity-Request Timeout] フィールドで、デバイスがローカル EAP を使用してワイヤレスクライアントに EAP ID 要求を送信する際の試行時間（秒単位）を指定します。

ステップ 3 [EAP-Identity-Request Max Retries] フィールドで、デバイスがローカル EAP を使用してワイヤレスクライアントに EAP ID 要求を再送信する際の最大試行回数を指定します。

ステップ 4 [EAP Max-Login Ignore Identity Response] を [Enabled] 状態に設定して、同じユーザー名を使用してデバイスに接続できるクライアントの数を制限します。同じデバイス上の異なるクライアント（PDA、ラップトップ、IP フォンなど）から最大 8 台までログインできます。デフォルトの状態は [Disabled] です。

ステップ 5 [EAP-Request Timeout] フィールドで、デバイスがローカル EAP を使用してワイヤレスクライアントに EAP 要求を送信する際の試行時間（秒単位）を指定します。

ステップ 6 [EAP-Request Max Retries] フィールドで、デバイスがローカル EAP を使用してワイヤレスクライアントに EAP 要求を再送信する際の最大試行回数を指定します。

ステップ 7 [EAPOL-Key Timeout] フィールドで、デバイスがローカル EAP を使用してワイヤレスクライアントに LAN 経由で EAP キーを送信する際の試行時間（秒単位）を指定します。

ステップ 8 [EAPOL-Key Max Retries] フィールドで、デバイスがローカル EAP を使用してワイヤレスクライアントに LAN 経由で EAP キーを送信する際の最大試行回数を指定します。

ステップ 9 [EAP-Broadcast Key Interval] フィールドで、クライアントに使用されるブロードキャスト暗号キーのローテーションの時間間隔を指定し、[Apply] をクリックします。

（注） EAP ブロードキャストキー間隔を新しい期間に設定した後、変更を有効にするには、WLAN をシャットダウンまたは再起動する必要があります。WLAN がシャットダウンまたは再起動し、設定されたタイマー値が期限切れになると、M5 および M6 パケットが交換されます。

EAP 要求のタイムアウトの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 2	**wireless wps client-exclusion dot1x-timeout** 例： `Device(config)# wireless wps client-exclusion dot1x-timeout`	タイムアウト時および応答がない場合の除外を有効にします。 デフォルトでは、この機能は有効です。 無効にするには、コマンドの先頭に **no** を付けます。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

ワイヤレスセキュリティでの EAP 要求タイムアウトの設定（CLI）

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	0 - 20 1 - 120 } **wireless security dot1x request** {**retries** | **timeout** 例： `Device(config)# wireless security dot1x request timeout 60`	EAP 要求の再送信タイムアウト値を秒単位で設定します。
ステップ 3	**end** 例： `Device(config)# end`	特権 EXEC モードに戻ります。また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

キャプティブ ポータル

キャプティブ ポータル設定

この機能を使用すると、AP に基づき同じ SSID に対して、複数の Web 認証 URL（外部のキャプティブ URL を含む）を設定できます。デフォルトの設定では、グローバル URL が認証に使用されます。オーバーライド オプションは、WLAN および AP レベルで使用できます。

優先順位は次のとおりです。

- AP
- WLAN
- グローバル コンフィギュレーション

キャプティブ ポータルの設定の制約事項

- この設定は、スタンドアロン コントローラでのみサポートされています。
- エクスポート アンカー設定はサポートされていません。

キャプティブポータルの設定（GUI）

手順

ステップ 1 **[Configuration]** > **[Tags & Profiles]** > **[WLANs]** を選択します。

ステップ 2 [Add] をクリックします。

ステップ 3 [General] タブで、[Profile Name]、[SSID]、および [WLAN ID] を入力します。

ステップ 4 [Security] > [Layer2] タブで、[WPA Policy]、[AES]、および [802.1x] チェックボックスをオフにします。

ステップ 5 [Security] > [Layer3] タブで、[Web Auth Parameter Map] ドロップダウンリストからパラメータマップを選択し、[Authentication List] ドロップダウンリストから認証リストを選択します。

ステップ 6 [Security] > [AAA] タブの [Authentication List] ドロップダウンリストから認証リストを選択します。

ステップ 7 [Apply to Device] をクリックします。

ステップ 8 **[Configuration]** > **[Security]** > **[Web Auth]** の順に選択します。

ステップ 9 [Web Auth Parameter Map] を選択します。

ステップ 10 [General] タブで、[Maximum HTTP connections]、[Init-State Timeout(secs)] を入力し、[Type] ドロップダウンリストから [webauth] を選択します。

ステップ 11 [Advanced] タブの [Redirect to external server] 設定で、**Redirect for log-in server** と入力します。

ステップ 12 [Update & Apply] をクリックします。

キャプティブ ポータルの設定

手順

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**wlan** {*profile-name* | **shutdown**} *network-name* 例： `Device(config)# wlan edc6 6 edc`	WLANプロファイルを設定します。すべてのWLANを有効または無効にし、WLAN IDを作成します。プロファイル名と SSID ネットワーク名には、最大 32 文字の英数字を使用できます。
ステップ 3	**ip** {**access-group** | **verify**} **web** *IPv4-ACL-Name* 例： `Device(config-wlan)# ip access-group web CPWebauth`	WLAN の Web ACL を設定します。 （注） この操作を実行する前に、WLANを無効にしておく必要があります。
ステップ 4	**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 5	**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 AKM をディセーブルにします。
ステップ 6	**no security wpa wpa2 ciphers aes** 例： `Device(config-wlan)# no security wpa wpa2 ciphers aes`	AES の WPA2 暗号化を無効にします。

ステップ 7	**security web-auth** {**authentication-list** *authentication-list-name* | **authorization-list** *authorization-list-name* | **on-macfilter-failure** | **parameter-map** *parameter-map-name*}
	例：
	`Device(config-wlan)# security web-auth authentication-list cp-webauth`
	`Device(config-wlan)# security web-auth parameter-map parMap6`
		WLAN の Web 認証を有効にします。ここで、各変数は次のように定義されます。
		• **authentication-list**
		authentication-list-name：IEEE 802.1x の認証リストを指定します。
		• **authorization-list**

	コマンドまたはアクション	目的
		authorization-list-name：IEEE 802.1x のオーバーライド認可リストを指定します。 • **on-macfilter-failure**：MAC フィルタの失敗における Web 認証を有効にします。 • **parameter-map** *parameter-map-name*：パラメータ マップを設定します。 （注） **security web-auth** を有効にすると、デフォルトの **authentication-list** とグローバルの **parameter-map** がマッピングされます。これは、明示的に記述されていない認証リストとパラメータマップに適用されます。
ステップ 8	**no shutdown** 例： `Device(config-wlan)# no shutdown`	WLAN をイネーブルにします。
ステップ 9	**exit** 例： `Device(config-wlan)# exit`	WLAN 設定を終了します。
ステップ 10	**parameter-map type webauth** *parameter-map-name* 例： `Device(config)# parameter-map type webauth parMap6`	パラメータ マップを作成し、parameter-map webauth コンフィギュレーション モードを開始します。
ステップ 11	**parameter-map type webauth** *parameter-map-name* 例： `Device(config)# parameter-map type webauth parMap6`	パラメータ マップを作成し、parameter-map webauth コンフィギュレーション モードを開始します。
ステップ 12	**type webauth** 例： `Device(config-params-parameter-map)# type webauth`	webauth タイプ パラメータを設定します。

	コマンドまたはアクション	目的
ステップ 13	**timeout init-state sec** <*timeout-seconds*> 例： `Device(config-params-parameter-map)# timeout inti-state sec 3600`	WEBAUTH のタイムアウトを秒単位で設定します。タイムアウト（秒単位）パラメータの有効な範囲は 60 ～ 3932100 秒です。
ステップ 14	**redirect for-login** <*URL-String*> 例： `Device(config-params-parameter-map)# redirect for-login https://172.16.100.157/portal/login.html`	ログイン時のリダイレクト用の URL 文字列を設定します。
ステップ 15	**exit** 例： `Device(config-params-parameter-map)# exit`	パラメータ設定を終了します。
ステップ 16	**wireless tag policy** *policy-tag-name* 例： `Device(config)# wireless tag policy policy_tag_edc6`	ポリシータグを設定し、ポリシータグコンフィギュレーションモードを開始します。
ステップ 17	**wlan** *wlan-profile-name* **policy** *policy-profile-name* 例： `Device(config-policy-tag)# wlan edc6 policy policy_profile_flex`	WLAN プロファイルにポリシー プロファイルをアタッチします。
ステップ 18	**end** 例： `Device(config-policy-tag)# end`	設定を保存し、コンフィギュレーションモードを終了して、特権 EXEC モードに戻ります。

キャプティブ ポータル設定：例

次に、複数の AP を異なるロケーションに配置して同じ SSID をブロードキャストするものの、クライアントを異なるリダイレクト ポータルにリダイレクトする例を示します。

異なるリダイレクトポータルを指す複数のパラメータ マップを設定するには、次のようにします。

```
parameter-map type webauth parMap1
type webauth
timeout init-state sec 21600
redirect for-login
https://172.16.12.3:8080/portal/PortalSetup.action?portal=cfdbce00-2ce2-11e8-b83c-005056a06b27
redirect portal ipv4 172.16.12.3
!
```

```
!
parameter-map type webauth parMap11
type webauth
timeout init-state sec 21600
redirect for-login
https://172.16.12.4:8443/portal/PortalSetup.action?portal=094e7270-3808-11e8-9797-02421e4cae0c
redirect portal ipv4 172.16.12.4
!
```

これらのパラメータ マップを異なる WLAN に関連付けます。

```
wlan edc1 1 edc
ip access-group web CPWebauth
no security wpa
no security wpa akm dot1x
no security wpa wpa2 ciphers aes
security web-auth
security web-auth authentication-list cp-webauth
security web-auth parameter-map parMap11
no shutdown
wlan edc2 2 edc
ip access-group web CPWebauth
no security wpa
no security wpa akm dot1x
no security wpa wpa2 ciphers aes
security web-auth
security web-auth authentication-list cp-webauth
security web-auth parameter-map parMap1
no shutdown
```

（注） すべての WLAN に同じ SSID があります。

WLAN を異なるポリシー タグに関連付けます。

```
wireless tag policy policy_tag_edc1
wlan edc1 policy policy_profile_flex
wireless tag policy policy_tag_edc2
wlan edc2 policy policy_profile_flex
```

これらのポリシー タグを目的の AP に割り当てます。

```
ap E4AA.5D13.14DC
policy-tag policy_tag_edc1
site-tag site_tag_flex
ap E4AA.5D2C.3CAC
policy-tag policy_tag_edc2
site-tag site_tag_flex
```

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。