Cisco Identity Services Engine 用のユニバーサル ワイヤレス コントローラ設定

セキュア アクセスを実現するハウツー ガイド シリーズ

作成者:Hosuk Won

日付:2015 年 11 月

目次

はじめに

Cisco Identity Services Engine とは

Cisco Identity Services Engine（ISE）は、包括的でセキュアな、有線、ワイヤレスおよびバーチャル プライベート ネットワーク（VPN）アクセスを実現するオールインワン型エンタープライズ ポリシー制御製品です。

Cisco ISE は、RADIUS ベースの単一製品でありながら、ポリシーの包括的な管理と適用の集中制御ポイントとして機能します。Cisco ISE 固有のアーキテクチャにより、企業はネットワーク、ユーザ、およびデバイスから状況に応じた情報をリアルタイムで収集できるようになります。管理者は、プロアクティブなガバナンスの意思決定にその情報を使用できます。Cisco ISE は Cisco Secure Access の重要なコンポーネントです。

Cisco Secure Access は、ネットワーク インフラストラクチャに統合された高度なネットワーク アクセス コントロールとアイデンティティのソリューションです。ソリューション内のすべてのコンポーネントが統合システムとして十分に吟味かつ厳密にテストされた、実証済みの有効なソリューションです。

Cisco ワイヤレス コントローラ

オーバーレイ ネットワーク アクセス コントロール ソリューションとは異なり、Cisco Secure Access では、アクセス レイヤ デバイス（スイッチ、ワイヤレス コントローラなど）が適用時に使用されます。Web 認証用の URL リダイレクトなど、一般にはアプライアンスやその他のオーバーレイ デバイスによって処理されていた機能をアクセス デバイス自体が処理するようになりました。

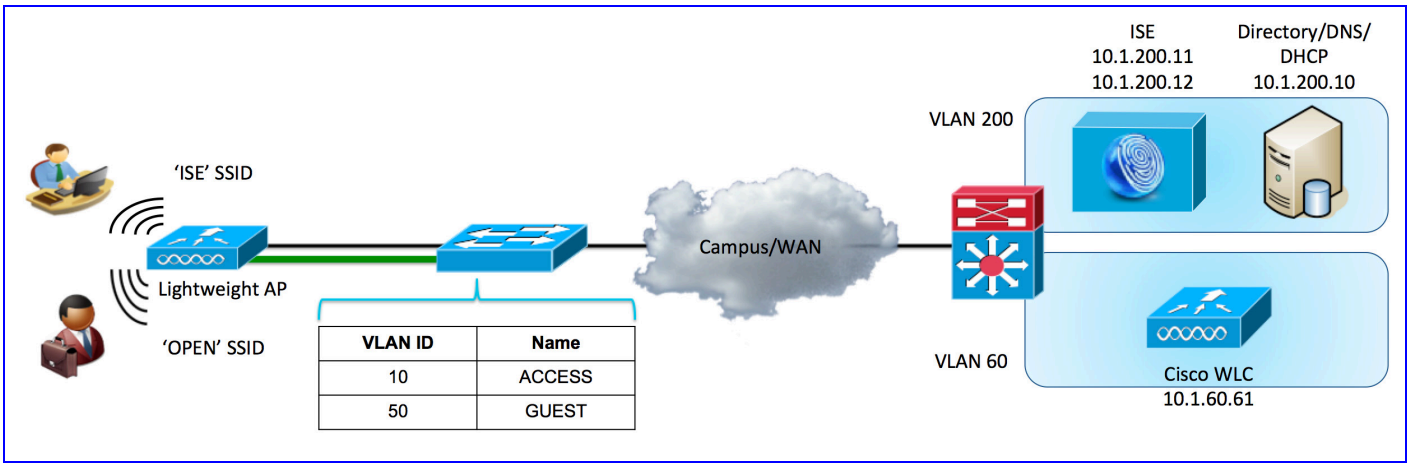
Cisco Secure Access は、IEEE 802.1X と VLAN 制御などの標準ベースのアイデンティティおよび適用モデルを組み合わせるだけでなく、URL リダイレクト、名前付きアクセス コントロール リスト（AireSpace ACL）、セキュリティ グループ タグ（SGT）、デバイス プロファイリング、ゲストと Web の認証サービス、ポスチャ評価、ネットワークへのアクセス前とアクセス時のモバイル デバイスのコンプライアンス検証を行うモバイル デバイス管理（MDM）の大手ベンダーとの統合など、さらに多くの高度なアイデンティティおよび適用機能も備えています。

このマニュアルについて

次の項では、Cisco® ワイヤレス LAN コントローラ（WLC）の汎用設定について説明します。これらの推奨設定は、すべての導入環境で使用できるベスト プラクティスとして編集されており、どの導入タイプを選択しても、導入のどの段階でも、一貫して使用できます。

次の図は、コンポーネントの全体的なレイアウトを示します。アクセス VLAN は 2 つあります。従業員ユーザ用の ACCESS VLAN と、ゲスト ユーザ用の GUEST VLAN です。このドキュメントには BYOD、ポスチャ アセスメント、プロファイリングなどの ISE のポリシー設定は含まれていませんが、記載されている設定はこのような操作の基準を定めています。

図 1 コンポーネント



付録には、最小限の変更でコピー アンド ペーストできる設定例があります。また、FlexConnect モード WLAN/AP および自動アンカー モードで設定された WLAN に関連する追加設定も付録にあります。

設定

初期設定

このセクションでは、CLI ベースの構成ツールを使用した、WLC の初期ブートストラップを扱います。

表 1.　初期設定

オプション	値
管理インターフェイスの IP（Management Interface IP）	10.1.60.61
管理インターフェイスのマスク（Management Interface Mask）	255.255.255.0
管理インターフェイスのゲートウェイ（Management Interface Gateway）	10.1.60.1
管理インターフェイスの VLAN ID（Management Interface VLAN ID）	0（タグなし）
管理インターフェイスのポート番号（Management Interface Port Number）	1
仮想ゲートウェイ IP（Virtual Gateway IP）	192.0.2.1
モビリティ/RF グループ名（Mobility/RF Group Name）	メイン（Main）
NTP サーバの IP（NTP Server IP）	10.1.60.1

注：初期設定は事前設定のない新しい WLC に適用されます。ISE 関連の設定を既存の設定を持つ WLC に追加する場合は、「コントローラ設定」セクションに進みます。

手順 1　WLC のコンソール ポートに接続するか、vWLC の仮想コンソールを使用します。次の設定を参照して、WLC のブートストラップを行います。

```
(Cisco Controller)

Welcome to the Cisco Wizard Configuration Tool
Use the '-' character to backup

Would you like to terminate autoinstall? [yes]:yes
AUTO-INSTALL: process terminated -- no configuration loaded

System Name [Cisco_91:e2:64] (31 characters max):
Enter Administrative User Name (24 characters max): admin
Enter Administrative Password (3 to 24 characters): ********
Re-enter Administrative Password                : ********
```

```
Service Interface IP Address Configuration [static][DHCP]:dhcp

Enable Link Aggregation (LAG) [yes][NO]: no

Management Interface IP Address: 10.1.60.61
Management Interface Netmask: 255.255.255.0
Management Interface Default Router: 10.1.60.1
Management Interface VLAN Identifier (0 = untagged): 0
Management Interface Port Num [1 to 8]: 1
Management Interface DHCP Server IP Address: 10.1.100.100

Virtual Gateway IP Address: 192.0.2.1

Mobility/RF Group Name: Main

Network Name (SSID): EXAMPLE

Configure DHCP Bridging Mode [yes][NO]: no

Allow Static IP Addresses [YES][no]: no

Configure a RADIUS Server now? [YES][no]: no
Warning! The default WLAN security policy requires a RADIUS server.
Please see documentation for more details.

Enter Country Code list (enter 'help' for a list of countries) [US]:us

Enable 802.11b Network [YES][no]: yes
Enable 802.11a Network [YES][no]: yes
Enable 802.11g Network [YES][no]: yes
Enable Auto-RF [YES][no]: yes

Configure a NTP server now? [YES][no]: yes
Enter the NTP server's IP address: 10.1.60.1
Enter a polling interval between 3600 and 604800 secs: 3600

Configuration correct? If yes, system will save it and reset.[yes][NO]: yes
```

Cisco WLC の仮想ゲートウェイ アドレスを 192.0.2.1 に設定することを推奨します。使用するアドレスは、ドメイン ネーム システム（DNS）でマッピングされる完全修飾ドメイン名（FQDN）を使用した非ルーテッド IP にする必要があります。この FQDN/IP アドレスを、CA によって生成された証明書に追加する必要があります。この設定により、ユーザが WLC の仮想ゲートウェイにリダイレクトされたときに「証明書を信頼できません（untrusted certificate）」のエラーが表示されなくなります。

手順 2 WLC のリセット後に、WLC の残りの設定を行います。このガイドでは、以降のセクションに GUI と CLI ベースの設定が両方とも記載されています。

注：初期化中に設定された「EXAMPLE」という名前の SSID はこのガイドでは使用されません。WLC のリセット後に次のコマンドを実行することで削除できます。

```
(WLC) >config wlan delete 1
```

コントローラ コンフィギュレーション

このセクションでは、コントローラに関連する設定について扱います。これには、エンドポイント デバイス用のインターフェイスおよび VLAN の設定と、グローバル コントローラ設定が含まれます。

表 2. インターフェイスの設定

オプション	従業員	ゲスト
[インターフェイス名（Interface Name）]	ACCESS	GUEST
VLAN ID（Admin. VLAN ID）	10	50
ダイナミック IP（Dynamic IP）	10.1.10.61	10.1.50.61
サブネット マスク	255.255.255.0	255.255.255.0
ゲートウェイ	10.1.10.1	10.1.50.1
DHCP サーバ（DHCP Server）	10.1.200.10	10.1.200.10
[ポート（Port）]	1	1

手順 3 ダイナミック インターフェイスを設定します。GUI の場合は、[コントローラ（Controller）] → [インターフェイス（Interfaces）] に移動します。

```
(WLC) >config interface create ACCESS 10
(WLC) >config interface create GUEST 50
```

手順 4 上で作成したダイナミック インターフェイスの物理ポートを割り当てます。この例では、すべてのインターフェイスが同じ物理インターフェイスに割り当てられ、トランキングを利用します。

```
(WLC) >config interface port ACCESS 1
(WLC) >config interface port GUEST 1
```

手順 5 インターフェイスに IP アドレスを設定します。

```
(WLC) >config interface address dynamic-interface ACCESS 10.1.10.61 255.255.255.0 10.1.10.1
(WLC) >config interface address dynamic-interface GUEST 10.1.50.61 255.255.255.0 10.1.50.1
```

手順 6 ユーザ インターフェイス用の DHCP サーバを設定します。

```
(WLC) >config interface dhcp dynamic-interface ACCESS primary 10.1.200.10
(WLC) >config interface dhcp dynamic-interface GUEST primary 10.1.200.10
```

手順 7 DHCP プロキシをグローバルに無効にし、ルータの SVI を使用して DHCP 要求を DHCP サーバに転送します。GUI の場合は、[コントローラ(Controller)] → [詳細設定(Advanced)] → [DHCP] に移動します。

```
(WLC) >config dhcp proxy disable
```

注:DHCP プロキシが無効になっている場合、WLC は DHCP 要求を上流に位置するルータにブリッジします。上流に位置するルータは、DHCP サーバの「ip helper-address」を使用して設定し、プロファイリングのための ISE PSN ノードとして設定する必要があります。WLC デバイス センサーは ISE の DHCP 属性を取得できますが、DHCP オプションの属性などの複数の DHCP 属性は欠落します。上流に位置するルータを設定して DHCP 要求を ISE ノードに転送することで、ISE はプロファイリングのための追加の DHCP 情報を収集することができます。

手順 8 (オプション)高速 SSID 変更機能を有効にして、デュアル SSID 導入のために異なる SSID からの Apple デバイスの遷移に対応します。GUI の場合は、[コントローラ(Controller)] → [全般(General)] に移動します。

```
(WLC) >config network fast-ssid-change enable
```

注:コントローラ上で高速 SSID 変更が有効になっているときは、クライアントは SSID 間で移動することができます。クライアントが異なる SSID の新しいアソシエーションを送信すると、コントローラの通信テーブルのクライアント エントリがクリアされてから、新しい SSID にクライアントが追加されます。高速 SSID 変更が無効のときは、コントローラは一定の遅延時間が経過した後でクライアントに新しい SSID への移動を許可するため、デュアル SSID BYOD 導入でのユーザ エクスペリエンスに影響が出ます。

セキュリティ設定

このセクションでは、RADIUS サーバや ACL を含む、セキュリティ関連の設定について扱います。RADIUS サーバは、既存の RADIUS 設定を上書きしないように 11 と 12 の ID 値を使用します。

手順 9 RADIUS 認証サーバを作成します。この例では、2 つの ISE ノード、10.1.200.11 と 10.1.200.12 があります。CoA が有効になっており、タイムアウトは 5 秒に設定されています(デフォルトは 2 秒)。RADIUS によるデバイス管理は無効になっており、これらの RADIUS サーバはネットワーク ユーザ認証専用です。GUI 設定の場合は、[セキュリティ(Security)] → [AAA] → [RADIUS] → [認証(Authentication)] → [新規…(New…)] に移動します。

```
(WLC) >config radius auth add 11 10.1.200.11 1812 ascii ISEc0ld
(WLC) >config radius auth disable 11
(WLC) >config radius auth management 11 disable
(WLC) >config radius auth retransmit-timeout 11 5
(WLC) >config radius auth rfc3576 enable 11
(WLC) >config radius auth enable 11

(WLC) >config radius auth add 12 10.1.200.12 1812 ascii ISEc0ld
(WLC) >config radius auth disable 12
(WLC) >config radius auth management 12 disable
(WLC) >config radius auth retransmit-timeout 12 5
(WLC) >config radius auth rfc3576 enable 12
(WLC) >config radius auth enable 12
```

手順 10 （オプション）Calling-Station-ID フィールドで送信される MAC アドレスの形式が ISE と一致することを確認します。これはデフォルトの設定です。

```
(WLC) >config radius auth mac-delimiter hyphen
```

手順 11 （オプション）追加情報を使用して RADIUS Called-Station-ID 属性の形式を設定します。デフォルト形式は APMAC:SSID です。この属性のオプションは、WLC コードのバージョンによって異なります。このフィールドは、エンドポイントで初期認証に関連付けられた AP ロケーション情報を使用した、ロケーションベースの認証を実現するために使用されます。

```
(WLC) >config radius callStationIdType ap-macaddr-ssid
```

注：これは、WiFi の三角測量を使用したエンドポイント ロケーションを使用する MSE ロケーション統合とは異なります。

手順 12 RADIUS フォールバック モードを設定して、オンラインに戻ったときにプライマリ ISE ノードが使用されるようにします。このオプションがない場合、プライマリ サーバがオンラインに戻っても第 2 サーバまたは第 3 サーバが使用されます。GUI の場合、[セキュリティ（Security）] → [AAA] → [RADIUS] → [フォールバック（Fallback）] に移動します。

```
(WLC) >config radius fallback-test username RADIUS-TEST
(WLC) >config radius fallback-test mode active
```

注：**アクティブ**を選択すると、Cisco WLC は使用可能なバックアップ サーバからより低い優先順位を持つサーバへの復帰を実行します。サーバを選択するために、RADIUS プローブ メッセージを使用して、非アクティブとしてマークされているサーバがオンラインに戻っているかどうかを事前に判断します。コントローラは、すべてのアクティブな RADIUS 要求に対して、すべての非アクティブ サーバを無視します。**パッシブ** モードを選択すると、Cisco WLC は外部のプローブ メッセージを使用せずに、使用可能なバックアップ サーバからより低い優先順位を持つサーバへの復帰を実行します。コントローラは、しばらくの間非アクティブなすべてのサーバを無視し、後で RADIUS メッセージの送信が必要になったときに再試行します。

手順 13 （オプション）この間隔は、アクティブ モード フォールバックの場合のプローブ間隔またはパッシブ モード フォールバックの場合の非アクティブ時間を指定します。デフォルト値は 300 秒です。

```
(WLC) >config radius fallback-test mode interval 300
```

手順 14 RADIUS アグレッシブ フェールオーバー メカニズムを無効にして、RADIUS サーバがエラーでデッドとしてマーキングされないようにします。

```
(WLC) >config radius aggressive-failover disable
```

注：WLC でアグレッシブ フェールオーバー機能が有効になっている場合、WLC は AAA サーバを「応答なし」としてマークするには過剰にアグレッシブになります。この機能を有効にしない理由の 1 つは、サイレント破棄を設定している場合、特定のクライアントにのみ AAA サーバが応答しなくなる可能性があるためです。また、有効な証明書を持つ他の有効なクライアントに応答する可能性もあります。WLC はこの場合も AAA サーバを「応答なし」および「機能停止」としてマークする可能性があります。この問題を解決するには、アグレッシブ フェールオーバー機能を無効にします。この機能を無効にした場合、RADIUS サーバからの応答の受信に 3 回連続で失敗したクライアントがある場合にのみ、コントローラが次の AAA サーバにフェールオーバーします。

手順 15 RADIUS アカウンティング サーバを作成します。GUI の場合は、[セキュリティ（Security）] → [AAA] → [RADIUS] → [アカウンティング（Accounting）] → [新規…（New…）] に移動します。

```
(WLC) >config radius acct add 11 10.1.200.11 1813 ascii ISEc0ld
(WLC) >config radius acct disable 11
(WLC) >config radius acct retransmit-timeout 11 5
(WLC) >config radius acct enable 11

(WLC) >config radius acct add 12 10.1.200.12 1813 ascii ISEc0ld
(WLC) >config radius acct disable 12
(WLC) >config radius acct retransmit-timeout 12 5
(WLC) >config radius acct enable 12
```

手順 16 ACL_WEBAUTH_REDIRECT ACL を作成します。GUI の場合は、[セキュリティ（Security）] → [アクセス コントロール リスト（Access Control Lists）] → [アクセス コントロール リスト（Access Control Lists）] → [新規…（New…）] に移動します。

```
(WLC) >config acl delete ACL_WEBAUTH_REDIRECT
(WLC) >config acl create ACL_WEBAUTH_REDIRECT
(WLC) >config acl rule add ACL_WEBAUTH_REDIRECT 1
(WLC) >config acl rule action ACL_WEBAUTH_REDIRECT 1 permit
(WLC) >config acl rule protocol ACL_WEBAUTH_REDIRECT 1 6
(WLC) >config acl rule source port range ACL_WEBAUTH_REDIRECT 1 0 65535
(WLC) >config acl rule destination address ACL_WEBAUTH_REDIRECT 1 10.1.200.12 255.255.255.255
(WLC) >config acl rule destination port range ACL_WEBAUTH_REDIRECT 1 8443 8444

(WLC) >config acl rule add ACL_WEBAUTH_REDIRECT 1
(WLC) >config acl rule action ACL_WEBAUTH_REDIRECT 1 permit
(WLC) >config acl rule protocol ACL_WEBAUTH_REDIRECT 1 6
(WLC) >config acl rule source address ACL_WEBAUTH_REDIRECT 1 10.1.200.12 255.255.255.255
(WLC) >config acl rule source port range ACL_WEBAUTH_REDIRECT 1 8443 8444
(WLC) >config acl rule destination port range ACL_WEBAUTH_REDIRECT 1 0 65535

(WLC) >config acl rule add ACL_WEBAUTH_REDIRECT 1
(WLC) >config acl rule action ACL_WEBAUTH_REDIRECT 1 permit
(WLC) >config acl rule protocol ACL_WEBAUTH_REDIRECT 1 6
(WLC) >config acl rule source port range ACL_WEBAUTH_REDIRECT 1 0 65535
(WLC) >config acl rule destination address ACL_WEBAUTH_REDIRECT 1 10.1.200.12 255.255.255.255
(WLC) >config acl rule destination port range ACL_WEBAUTH_REDIRECT 1 8905 8905

(WLC) >config acl rule add ACL_WEBAUTH_REDIRECT 1
(WLC) >config acl rule action ACL_WEBAUTH_REDIRECT 1 permit
(WLC) >config acl rule protocol ACL_WEBAUTH_REDIRECT 1 6
(WLC) >config acl rule source address ACL_WEBAUTH_REDIRECT 1 10.1.200.12 255.255.255.255
(WLC) >config acl rule source port range ACL_WEBAUTH_REDIRECT 1 8905 8905
(WLC) >config acl rule destination port range ACL_WEBAUTH_REDIRECT 1 0 65535

(WLC) >config acl rule add ACL_WEBAUTH_REDIRECT 1
(WLC) >config acl rule action ACL_WEBAUTH_REDIRECT 1 permit
(WLC) >config acl rule protocol ACL_WEBAUTH_REDIRECT 1 6
(WLC) >config acl rule source port range ACL_WEBAUTH_REDIRECT 1 0 65535
```

```
(WLC) >config acl rule destination address ACL_WEBAUTH_REDIRECT 1 10.1.200.11 255.255.255.255
(WLC) >config acl rule destination port range ACL_WEBAUTH_REDIRECT 1 8443 8444

(WLC) >config acl rule add ACL_WEBAUTH_REDIRECT 1
(WLC) >config acl rule action ACL_WEBAUTH_REDIRECT 1 permit
(WLC) >config acl rule protocol ACL_WEBAUTH_REDIRECT 1 6
(WLC) >config acl rule source address ACL_WEBAUTH_REDIRECT 1 10.1.200.11 255.255.255.255
(WLC) >config acl rule source port range ACL_WEBAUTH_REDIRECT 1 8443 8444
(WLC) >config acl rule destination port range ACL_WEBAUTH_REDIRECT 1 0 65535

(WLC) >config acl rule add ACL_WEBAUTH_REDIRECT 1
(WLC) >config acl rule action ACL_WEBAUTH_REDIRECT 1 permit
(WLC) >config acl rule protocol ACL_WEBAUTH_REDIRECT 1 6
(WLC) >config acl rule source port range ACL_WEBAUTH_REDIRECT 1 0 65535
(WLC) >config acl rule destination address ACL_WEBAUTH_REDIRECT 1 10.1.200.11 255.255.255.255
(WLC) >config acl rule destination port range ACL_WEBAUTH_REDIRECT 1 8905 8905

(WLC) >config acl rule add ACL_WEBAUTH_REDIRECT 1
(WLC) >config acl rule action ACL_WEBAUTH_REDIRECT 1 permit
(WLC) >config acl rule protocol ACL_WEBAUTH_REDIRECT 1 6
(WLC) >config acl rule source address ACL_WEBAUTH_REDIRECT 1 10.1.200.11 255.255.255.255
(WLC) >config acl rule source port range ACL_WEBAUTH_REDIRECT 1 8905 8905
(WLC) >config acl rule destination port range ACL_WEBAUTH_REDIRECT 1 0 65535

(WLC) >config acl rule add ACL_WEBAUTH_REDIRECT 1
(WLC) >config acl rule action ACL_WEBAUTH_REDIRECT 1 permit
(WLC) >config acl rule protocol ACL_WEBAUTH_REDIRECT 1 17
(WLC) >config acl rule source port range ACL_WEBAUTH_REDIRECT 1 0 65535
(WLC) >config acl rule destination port range ACL_WEBAUTH_REDIRECT 1 53 53

(WLC) >config acl rule add ACL_WEBAUTH_REDIRECT 1
(WLC) >config acl rule action ACL_WEBAUTH_REDIRECT 1 permit
(WLC) >config acl rule protocol ACL_WEBAUTH_REDIRECT 1 17
(WLC) >config acl rule source port range ACL_WEBAUTH_REDIRECT 1 53 53
(WLC) >config acl rule destination port range ACL_WEBAUTH_REDIRECT 1 0 65535
```

手順 17　（オプション）必要に応じて、DNS ACL エントリをリダイレクト ACL に追加できます。これにより、エンドポイントが NSP プロセス中に Google Play ストアにアクセスできるようになります。

```
(WLC) >config acl url-domain add play.google.com ACL_WEBAUTH_REDIRECT
(WLC) >config acl url-domain add android.clients.google.com ACL_WEBAUTH_REDIRECT
(WLC) >config acl url-domain add www.googleapis.com ACL_WEBAUTH_REDIRECT
(WLC) >config acl url-domain add ggpht.com ACL_WEBAUTH_REDIRECT
(WLC) >config acl url-domain add android.pool.ntp.org ACL_WEBAUTH_REDIRECT
(WLC) >config acl url-domain add market.android.com ACL_WEBAUTH_REDIRECT
(WLC) >config acl url-domain add mtalk.google.com ACL_WEBAUTH_REDIRECT
(WLC) >config acl url-domain add gvt1.com ACL_WEBAUTH_REDIRECT
```

注：英語以外の言語設定を使用するクライアント デバイスに対応するために、ドメインの追加が必要になる場合もあります。最大で 20 のドメイン エントリを ACL ごとに追加できます。

手順 18　ACL をデータ パスに適用します。

```
(WLC) >config acl apply ACL_WEBAUTH_REDIRECT
```

注：クライアントがリダイレクト状態（POSTURE_REQ、CWA、クライアント プロビジョニングなど）の場合、WLC のデフォルトの動作では DHCP/DNS 以外のすべてのトラフィックがブロックされます。（Cisco ISE から受信される url-redirect-acl AV ペアで呼び出される）ACL_WEBAUTH_REDIRECT ACL がクライアントに適用され、クライアントは ACL で特に許可されているリソースにのみ到達できます。

手順 19　BLACKHOLE ACL を作成します。

```
(WLC) >config acl delete BLACKHOLE
(WLC) >config acl create BLACKHOLE
(WLC) >config acl rule add BLACKHOLE 1
(WLC) >config acl rule action BLACKHOLE 1 permit
(WLC) >config acl rule protocol BLACKHOLE 1 6
(WLC) >config acl rule source port range BLACKHOLE 1 0 65535
(WLC) >config acl rule destination address BLACKHOLE 1 10.1.200.12 255.255.255.255
(WLC) >config acl rule destination port range BLACKHOLE 1 8444 8444

(WLC) >config acl rule add BLACKHOLE 1
(WLC) >config acl rule action BLACKHOLE 1 permit
(WLC) >config acl rule protocol BLACKHOLE 1 6
(WLC) >config acl rule source address BLACKHOLE 1 10.1.200.12 255.255.255.255
(WLC) >config acl rule source port range BLACKHOLE 1 8444 8444
(WLC) >config acl rule destination port range BLACKHOLE 1 0 65535

(WLC) >config acl rule add BLACKHOLE 1
(WLC) >config acl rule action BLACKHOLE 1 permit
(WLC) >config acl rule protocol BLACKHOLE 1 6
(WLC) >config acl rule source port range BLACKHOLE 1 0 65535
(WLC) >config acl rule destination address BLACKHOLE 1 10.1.200.11 255.255.255.255
(WLC) >config acl rule destination port range BLACKHOLE 1 8444 8444

(WLC) >config acl rule add BLACKHOLE 1
(WLC) >config acl rule action BLACKHOLE 1 permit
(WLC) >config acl rule protocol BLACKHOLE 1 6
(WLC) >config acl rule source address BLACKHOLE 1 10.1.200.11 255.255.255.255
(WLC) >config acl rule source port range BLACKHOLE 1 8444 8444
(WLC) >config acl rule destination port range BLACKHOLE 1 0 65535

(WLC) >config acl rule add BLACKHOLE 1
(WLC) >config acl rule action BLACKHOLE 1 permit
(WLC) >config acl rule protocol BLACKHOLE 1 17
(WLC) >config acl rule source port range BLACKHOLE 1 0 65535
(WLC) >config acl rule destination port range BLACKHOLE 1 53 53

(WLC) >config acl rule add BLACKHOLE 1
(WLC) >config acl rule action BLACKHOLE 1 permit
(WLC) >config acl rule protocol BLACKHOLE 1 17
(WLC) >config acl rule source port range BLACKHOLE 1 53 53
(WLC) >config acl rule destination port range BLACKHOLE 1 0 65535
```

手順 20　ACL をデータ パスに適用します。

```
(WLC) >config acl apply BLACKHOLE
```

WLAN の設定

このセクションでは、従業員のデバイスのためのセキュアな WLAN に関連する設定について扱います。これには、WLAN 設定が含まれています。WLAN は、既存の WLAN 設定を上書きしないように 11 と 12 の ID 値を使用します。この例では、2 つの WLAN を設定します。

- 「ISE」は WLAN ID 11 のセキュアな WLAN で、従業員アクセスとシングル SSID BYOD フローのために使用されます。
- 「OPEN」は WLAN ID 12 のオープンな WLAN で、ゲスト アクセスのために使用されます。

表 3.

オプション	セキュアな WLAN	オープンな WLAN
WLAN ID	11	12
WLAN 名（WLAN Name）	ISE	[オープン（OPEN）]
SSID	ISE	[オープン（OPEN）]
インターフェイス（Interface）	ACCESS	GUEST
L2 セキュリティ	WPA/WPA2 & 802.1X	MAC フィルタリング（MAC Filtering）
L3 セキュリティ	なし	なし
RADIUS 認証サーバ（RADIUS Auth Server）	11 および 12（11 & 12）	11 および 12（11 & 12）
RADIUS アカウンティング サーバ（RADIUS Acct Server）	11 および 12（11 & 12）	11 および 12（11 & 12）
RADIUS 中間アカウンティング（RADIUS Interim ACCT）	[有効（Enabled）]	[有効（Enabled）]
暫定アップデート間隔（Interim Update Interval）	0 秒	0 秒
AAA オーバーライド	[有効（Enabled）]	[有効（Enabled）]
アイドル タイムアウト	180 秒	180 秒
NAC	NAC_RADIUS	NAC_RADIUS
デバイス センサー	DHCP および HTTP（DHCP & HTTP）	DHCP および HTTP（DHCP & HTTP）

手順 21 WLAN ID 11 を使用して ISE WLAN を作成します。GUI の場合は、[WLAN（WLANs）] → [新規作成（Create New）] → [実行（Go）] に移動します。

```
(WLC) >config wlan create 11 ISE ISE
```

手順 22 以前に作成したインターフェイス「ISE」を WLAN に割り当てます。

```
(WLC) >config wlan interface 11 ACCESS
```

注：WLC に WLAN が追加されている場合は、WPA および 802.1X ですでに有効になっています。

手順 23 以前に作成した RADIUS 認証およびアカウンティング サーバを WLAN に割り当てます。

```
(WLC) >config wlan radius_server auth add 11 11
(WLC) >config wlan radius_server auth add 11 12
(WLC) >config wlan radius_server acct add 11 11
(WLC) >config wlan radius_server acct add 11 12
```

手順 24 エンドポイントの中間アカウンティング更新を設定します。次の設定は、8.x コードに適用されます。

```
(WLC) >config wlan radius_server acct interim-update 0 11
(WLC) >config wlan radius_server acct interim-update enable 11
```

注：7.6 コードの場合は、中間アカウンティングを無効にします。無効にされていても、WLC はエンドポイントのモビリティ イベントのアカウンティング更新を送信します。

```
(WLC) >config wlan radius_server acct interim-update disable 11
```

注：その他の以前のバージョン用です。

```
(WLC) >config wlan radius_server acct interim-update 3600 11
(WLC) >config wlan radius_server acct interim-update enable 11
```

手順 25 ISE からの AuthZ 属性を受け入れるように WLAN を設定します。

```
(WLC) >config wlan aaa-override enable 11
```

手順 26 （オプション）アイドル タイムアウトを設定します。

```
(WLC) >config wlan usertimeout 180 11
```

手順 27 WLAN の NAC RADIUS を有効にします。

```
(WLC) >config wlan nac radius enable 11
```

手順 28 http および dhcp のデバイス センサーを有効にします。

```
(WLC) >config wlan profiling radius all enable 11
```

手順 29 セキュアな WLAN を有効にします。

```
(WLC) >config wlan enable 11
```

手順 30 WLAN ID 12 を使用して OPEN WLAN を作成します。

```
(WLC) >config wlan create 12 OPEN OPEN
```

手順 31 以前に作成したインターフェイス「GUEST」を WLAN に割り当てます。

```
(WLC) >config wlan interface 12 GUEST
```

手順 32 オープン WLAN の L2 セキュリティを無効にします。

```
(WLC) >config wlan security wpa disable 12
```

手順 33 CWA の MAC フィルタリングを有効にします。

```
(WLC) >config wlan mac-filtering enable 12
```

手順 34 以前に作成した RADIUS 認証およびアカウンティング サーバを WLAN に割り当てます。

```
(WLC) >config wlan radius_server auth add 12 11
(WLC) >config wlan radius_server auth add 12 12
(WLC) >config wlan radius_server acct add 12 11
(WLC) >config wlan radius_server acct add 12 12
```

手順 35 エンドポイントの中間アカウンティング更新を設定します。次の設定は、8.x コードに適用されます。

```
(WLC) >config wlan radius_server acct interim-update 0 12
(WLC) >config wlan radius_server acct interim-update enable 12
```

注:7.6 コードの場合は、中間アカウンティングを無効にします。無効にされていても、WLC はエンドポイントのモビリティ イベントのアカウンティング更新を送信します。

```
(WLC) >config wlan radius_server acct interim-update disable 12
```

注:その他の以前のバージョン用です。

```
(WLC) >config wlan radius_server acct interim-update 3600 12
(WLC) >config wlan radius_server acct interim-update enable 12
```

手順 36 ISE からの AuthZ 属性を受け入れるように WLAN を設定します。

```
(WLC) >config wlan aaa-override enable 12
```

手順 37 セッションのタイムアウトを設定します。

```
(WLC) >config wlan session-timeout 12 1800
```

手順 38 アイドル タイムアウトを設定します。

```
(WLC) >config wlan usertimeout 180 12
```

手順 39 (オプション)オープン WLAN に必要なその他のパラメータを設定します。

```
(WLC) >config wlan chd 12 disable
(WLC) >config wlan ccx AironetIeSupport disable 12
(WLC) >config wlan dhcp_server 12 0.0.0.0 required
```

手順 40 WLAN の NAC RADIUS を有効にします。

```
(WLC) >config wlan nac radius enable 12
```

手順 41 http および dhcp のデバイス センサーを有効にします。

```
(WLC) >config wlan profiling radius all enable 12
```

手順 42 オープン WLAN を有効にします。

```
(WLC) >config wlan enable 12
```

管理設定

このセクションでは、全般的なコントローラの管理に関連する設定について扱います。これには、キャプティブ ポータル バイパス、および HTTPS リダイレクトの設定が含まれます。

手順 43 キャプティブ ポータル バイパスを有効にして、Apple デバイスを WLAN に関連付けたときにポップアップするミニ ブラウザを無効にします。これは、WLC が再起動された後に有効になります。この設定の GUI はありません。

```
(WLC) >config network web-auth captive-bypass enable
```

手順 44 (オプション)8.x コードで HTTPS リダイレクトを有効にします。GUI の場合は、[管理(Management)] → [HTTP-HTTPS] → [HTTPS リダイレクション(HTTPS Redirection)] → [有効(Enabled)] に移動します。

```
(WLC) >config network web-auth https-redirect enable
```

注:コントローラの負荷が増え、有効にされているときに WLC が扱うことができる Web 認証セッションが減るため、実稼働環境では推奨されません。

手順 45 設定を保存します。

```
(WLC) >save config
```

手順 46 コントローラをリロードして、キャプティブ ポータル バイパス設定を有効にします。

```
(WLC) >reset system
```

付録 A: サンプル設定

8.x コードを実行する WLC 用の設定

以前のバージョンの WLC 用の設定は、各 WLAN 設定の下にある中間アカウンティング設定を除いて同じです。以前のバージョン用の適切な設定については、ドキュメントのメイン セクションを参照してください。

```
config interface create ACCESS 10
config interface create GUEST 50
config interface port ACCESS 1
config interface port GUEST 1
config interface address dynamic-interface ACCESS 10.1.10.61 255.255.255.0 10.1.10.1
config interface address dynamic-interface GUEST 10.1.50.61 255.255.255.0 10.1.50.1
config interface dhcp dynamic-interface ACCESS primary 10.1.200.10
config interface dhcp dynamic-interface GUEST primary 10.1.200.10
config dhcp proxy disable

config radius auth add 11 10.1.200.11 1812 ascii ISEc0ld
config radius auth disable 11
config radius auth management 11 disable
config radius auth retransmit-timeout 11 5
config radius auth rfc3576 enable 11
config radius auth enable 11
config radius auth add 12 10.1.200.12 1812 ascii ISEc0ld
config radius auth disable 12
config radius auth management 12 disable
config radius auth retransmit-timeout 12 5
config radius auth rfc3576 enable 12
config radius auth enable 12

config radius fallback-test username RADIUS-TEST
config radius fallback-test mode active
config radius aggressive-failover disable

config radius acct add 11 10.1.200.11 1813 ascii ISEc0ld
config radius acct disable 11
config radius acct retransmit-timeout 11 5
config radius acct enable 11
config radius acct add 12 10.1.200.12 1813 ascii ISEc0ld
config radius acct disable 12
config radius acct retransmit-timeout 12 5
config radius acct enable 12

config acl delete ACL_WEBAUTH_REDIRECT
config acl create ACL_WEBAUTH_REDIRECT
config acl rule add ACL_WEBAUTH_REDIRECT 1
config acl rule action ACL_WEBAUTH_REDIRECT 1 permit
config acl rule protocol ACL_WEBAUTH_REDIRECT 1 6
config acl rule source port range ACL_WEBAUTH_REDIRECT 1 0 65535
config acl rule destination address ACL_WEBAUTH_REDIRECT 1 10.1.200.12 255.255.255.255
config acl rule destination port range ACL_WEBAUTH_REDIRECT 1 8443 8444
config acl rule add ACL_WEBAUTH_REDIRECT 1
config acl rule action ACL_WEBAUTH_REDIRECT 1 permit
config acl rule protocol ACL_WEBAUTH_REDIRECT 1 6
config acl rule source address ACL_WEBAUTH_REDIRECT 1 10.1.200.12 255.255.255.255
config acl rule source port range ACL_WEBAUTH_REDIRECT 1 8443 8444
config acl rule destination port range ACL_WEBAUTH_REDIRECT 1 0 65535
config acl rule add ACL_WEBAUTH_REDIRECT 1
config acl rule action ACL_WEBAUTH_REDIRECT 1 permit
config acl rule protocol ACL_WEBAUTH_REDIRECT 1 6
config acl rule source port range ACL_WEBAUTH_REDIRECT 1 0 65535
config acl rule destination address ACL_WEBAUTH_REDIRECT 1 10.1.200.12 255.255.255.255
config acl rule destination port range ACL_WEBAUTH_REDIRECT 1 8905 8905
config acl rule add ACL_WEBAUTH_REDIRECT 1
```

```
config acl rule action ACL_WEBAUTH_REDIRECT 1 permit
config acl rule protocol ACL_WEBAUTH_REDIRECT 1 6
config acl rule source address ACL_WEBAUTH_REDIRECT 1 10.1.200.12 255.255.255.255
config acl rule source port range ACL_WEBAUTH_REDIRECT 1 8905 8905
config acl rule destination port range ACL_WEBAUTH_REDIRECT 1 0 65535
config acl rule add ACL_WEBAUTH_REDIRECT 1
config acl rule action ACL_WEBAUTH_REDIRECT 1 permit
config acl rule protocol ACL_WEBAUTH_REDIRECT 1 6
config acl rule source port range ACL_WEBAUTH_REDIRECT 1 0 65535
config acl rule destination address ACL_WEBAUTH_REDIRECT 1 10.1.200.11 255.255.255.255
config acl rule destination port range ACL_WEBAUTH_REDIRECT 1 8443 8444
config acl rule add ACL_WEBAUTH_REDIRECT 1
config acl rule action ACL_WEBAUTH_REDIRECT 1 permit
config acl rule protocol ACL_WEBAUTH_REDIRECT 1 6
config acl rule source address ACL_WEBAUTH_REDIRECT 1 10.1.200.11 255.255.255.255
config acl rule source port range ACL_WEBAUTH_REDIRECT 1 8443 8444
config acl rule destination port range ACL_WEBAUTH_REDIRECT 1 0 65535
config acl rule add ACL_WEBAUTH_REDIRECT 1
config acl rule action ACL_WEBAUTH_REDIRECT 1 permit
config acl rule protocol ACL_WEBAUTH_REDIRECT 1 6
config acl rule source port range ACL_WEBAUTH_REDIRECT 1 0 65535
config acl rule destination address ACL_WEBAUTH_REDIRECT 1 10.1.200.11 255.255.255.255
config acl rule destination port range ACL_WEBAUTH_REDIRECT 1 8905 8905
config acl rule add ACL_WEBAUTH_REDIRECT 1
config acl rule action ACL_WEBAUTH_REDIRECT 1 permit
config acl rule protocol ACL_WEBAUTH_REDIRECT 1 6
config acl rule source address ACL_WEBAUTH_REDIRECT 1 10.1.200.11 255.255.255.255
config acl rule source port range ACL_WEBAUTH_REDIRECT 1 8905 8905
config acl rule destination port range ACL_WEBAUTH_REDIRECT 1 0 65535
config acl rule add ACL_WEBAUTH_REDIRECT 1
config acl rule action ACL_WEBAUTH_REDIRECT 1 permit
config acl rule protocol ACL_WEBAUTH_REDIRECT 1 17
config acl rule source port range ACL_WEBAUTH_REDIRECT 1 0 65535
config acl rule destination port range ACL_WEBAUTH_REDIRECT 1 53 53
config acl rule add ACL_WEBAUTH_REDIRECT 1
config acl rule action ACL_WEBAUTH_REDIRECT 1 permit
config acl rule protocol ACL_WEBAUTH_REDIRECT 1 17
config acl rule source port range ACL_WEBAUTH_REDIRECT 1 53 53
config acl apply ACL_WEBAUTH_REDIRECT

config acl delete BLACKHOLE
config acl create BLACKHOLE
config acl rule add BLACKHOLE 1
config acl rule action BLACKHOLE 1 permit
config acl rule protocol BLACKHOLE 1 6
config acl rule source port range BLACKHOLE 1 0 65535
config acl rule destination address BLACKHOLE 1 10.1.200.12 255.255.255.255
config acl rule destination port range BLACKHOLE 1 8444 8444
config acl rule add BLACKHOLE 1
config acl rule action BLACKHOLE 1 permit
config acl rule protocol BLACKHOLE 1 6
config acl rule source address BLACKHOLE 1 10.1.200.12 255.255.255.255
config acl rule source port range BLACKHOLE 1 8444 8444
config acl rule destination port range BLACKHOLE 1 0 65535
config acl rule add BLACKHOLE 1
config acl rule action BLACKHOLE 1 permit
config acl rule protocol BLACKHOLE 1 6
config acl rule source port range BLACKHOLE 1 0 65535
config acl rule destination address BLACKHOLE 1 10.1.200.11 255.255.255.255
config acl rule destination port range BLACKHOLE 1 8444 8444
config acl rule add BLACKHOLE 1
config acl rule action BLACKHOLE 1 permit
config acl rule protocol BLACKHOLE 1 6
config acl rule source address BLACKHOLE 1 10.1.200.11 255.255.255.255
config acl rule source port range BLACKHOLE 1 8444 8444
config acl rule destination port range BLACKHOLE 1 0 65535
config acl rule add BLACKHOLE 1
config acl rule action BLACKHOLE 1 permit
config acl rule protocol BLACKHOLE 1 17
config acl rule source port range BLACKHOLE 1 0 65535
config acl rule destination port range BLACKHOLE 1 53 53
```

```
config acl rule add BLACKHOLE 1
config acl rule action BLACKHOLE 1 permit
config acl rule protocol BLACKHOLE 1 17
config acl rule source port range BLACKHOLE 1 53 53
config acl rule destination port range BLACKHOLE 1 0 65535
config acl apply BLACKHOLE

config wlan create 11 ISE ISE
config wlan interface 11 ACCESS
config wlan radius_server auth add 11 11
config wlan radius_server auth add 11 12
config wlan radius_server acct add 11 11
config wlan radius_server acct add 11 12
config wlan radius_server acct interim-update 0 11
config wlan radius_server acct interim-update enable 11
config wlan aaa-override enable 11
config wlan usertimeout 180 11
config wlan nac radius enable 11
config wlan profiling radius all enable 11
config wlan enable 11

config wlan create 12 OPEN OPEN
config wlan interface 12 GUEST
config wlan security wpa disable 12
config wlan mac-filtering enable 12
config wlan radius_server auth add 12 11
config wlan radius_server auth add 12 12
config wlan radius_server acct add 12 11
config wlan radius_server acct add 12 12
config wlan radius_server acct interim-update 0 12
config wlan radius_server acct interim-update enable 12
config wlan aaa-override enable 12
config wlan session-timeout 12 1800
config wlan usertimeout 180 12
config wlan chd 12 disable
config wlan ccx AironetIeSupport disable 12
config wlan dhcp_server 12 0.0.0.0 required
config wlan nac radius enable 12
config wlan profiling radius all enable 12
config wlan enable 12

config network web-auth captive-bypass enable

save config
```

WLC に接続された Cisco IOS スイッチ インターフェイスの設定

```
description WLC Port 1
switchport trunk encapsulation dot1q
switchport trunk native vlan 60
switchport mode trunk
```

Cisco IOS スイッチ SVI の設定

```
interface vlan 10
 description ACCESS
 ip address 10.1.10.1 255.255.255.0
 ip helper-address 10.1.200.10
 ip helper-address 10.1.200.11
interface vlan 50
 description GUEST
 ip address 10.1.50.1 255.255.255.0
 ip helper-address 10.1.200.10
 ip helper-address 10.1.200.11
```

付録 B：設計に関する考慮事項

FlexConnect AP および WLAN

以前は H-REAP モードと呼ばれていた FlexConnect モードは、通常はブランチ オフィスで導入される特定の WLAN のために AP がローカルでユーザ トラフィックを切り替えられるようにします。これにより、ワイヤレストラフィックをブランチ オフィス内に留まらせることができます。この設計では、FlexConnect が有効になっている WLAN にエンドポイントが関連付けられると、エンドポイントは LAP からコントローラまでの CAPWAP トンネル内で認証を行います。ただし、認証が行われた後は、トラフィックは中央ワイヤレス コントローラ経由ではなく、LAP からローカル LAN にローカルに切り替えられます。ISE との統合と FlexConnect モード AP は、WLC v7.5 からサポートされています。ただし、統合には特定の設定が必要です。WLAN および AP の FlexConnect モードへの設定の他に、リダイレクト ACL も FlexConnect ACL として再作成し、FlexConnect グループまたは個々の AP にダウンロードする必要があります。

まず、ACL_WEBAUTH_REDIRECT および BLACKHOLE FlexConnect ACL を作成します。

```
config flexconnect acl create ACL_WEBAUTH_REDIRECT
config flexconnect acl rule add ACL_WEBAUTH_REDIRECT 1
config flexconnect acl rule action ACL_WEBAUTH_REDIRECT 1 permit
config flexconnect acl rule protocol ACL_WEBAUTH_REDIRECT 1 6
config flexconnect acl rule source port range ACL_WEBAUTH_REDIRECT 1 0 65535
config flexconnect acl rule destination address ACL_WEBAUTH_REDIRECT 1 10.1.200.12 255.255.255.255
config flexconnect acl rule destination port range ACL_WEBAUTH_REDIRECT 1 8443 8444
config flexconnect acl rule add ACL_WEBAUTH_REDIRECT 1
config flexconnect acl rule action ACL_WEBAUTH_REDIRECT 1 permit
config flexconnect acl rule protocol ACL_WEBAUTH_REDIRECT 1 6
config flexconnect acl rule source address ACL_WEBAUTH_REDIRECT 1 10.1.200.12 255.255.255.255
config flexconnect acl rule source port range ACL_WEBAUTH_REDIRECT 1 8443 8444
config flexconnect acl rule destination port range ACL_WEBAUTH_REDIRECT 1 0 65535
config flexconnect acl rule add ACL_WEBAUTH_REDIRECT 1
config flexconnect acl rule action ACL_WEBAUTH_REDIRECT 1 permit
config flexconnect acl rule protocol ACL_WEBAUTH_REDIRECT 1 6
config flexconnect acl rule source port range ACL_WEBAUTH_REDIRECT 1 0 65535
config flexconnect acl rule destination address ACL_WEBAUTH_REDIRECT 1 10.1.200.12 255.255.255.255
config flexconnect acl rule destination port range ACL_WEBAUTH_REDIRECT 1 8905 8905
config flexconnect acl rule add ACL_WEBAUTH_REDIRECT 1
config flexconnect acl rule action ACL_WEBAUTH_REDIRECT 1 permit
config flexconnect acl rule protocol ACL_WEBAUTH_REDIRECT 1 6
config flexconnect acl rule source address ACL_WEBAUTH_REDIRECT 1 10.1.200.12 255.255.255.255
config flexconnect acl rule source port range ACL_WEBAUTH_REDIRECT 1 8905 8905
config flexconnect acl rule destination port range ACL_WEBAUTH_REDIRECT 1 0 65535
config flexconnect acl rule add ACL_WEBAUTH_REDIRECT 1
config flexconnect acl rule action ACL_WEBAUTH_REDIRECT 1 permit
config flexconnect acl rule protocol ACL_WEBAUTH_REDIRECT 1 6
config flexconnect acl rule source port range ACL_WEBAUTH_REDIRECT 1 0 65535
config flexconnect acl rule destination address ACL_WEBAUTH_REDIRECT 1 10.1.200.11 255.255.255.255
config flexconnect acl rule destination port range ACL_WEBAUTH_REDIRECT 1 8443 8444
config flexconnect acl rule add ACL_WEBAUTH_REDIRECT 1
config flexconnect acl rule action ACL_WEBAUTH_REDIRECT 1 permit
config flexconnect acl rule protocol ACL_WEBAUTH_REDIRECT 1 6
config flexconnect acl rule source address ACL_WEBAUTH_REDIRECT 1 10.1.200.11 255.255.255.255
config flexconnect acl rule source port range ACL_WEBAUTH_REDIRECT 1 8443 8444
config flexconnect acl rule destination port range ACL_WEBAUTH_REDIRECT 1 0 65535
config flexconnect acl rule add ACL_WEBAUTH_REDIRECT 1
config flexconnect acl rule action ACL_WEBAUTH_REDIRECT 1 permit
config flexconnect acl rule protocol ACL_WEBAUTH_REDIRECT 1 6
config flexconnect acl rule source port range ACL_WEBAUTH_REDIRECT 1 0 65535
config flexconnect acl rule destination address ACL_WEBAUTH_REDIRECT 1 10.1.200.11 255.255.255.255
```

```
config flexconnect acl rule destination port range ACL_WEBAUTH_REDIRECT 1 8905 8905
config flexconnect acl rule add ACL_WEBAUTH_REDIRECT 1
config flexconnect acl rule action ACL_WEBAUTH_REDIRECT 1 permit
config flexconnect acl rule protocol ACL_WEBAUTH_REDIRECT 1 6
config flexconnect acl rule source address ACL_WEBAUTH_REDIRECT 1 10.1.200.11 255.255.255.255
config flexconnect acl rule source port range ACL_WEBAUTH_REDIRECT 1 8905 8905
config flexconnect acl rule destination port range ACL_WEBAUTH_REDIRECT 1 0 65535
config flexconnect acl rule add ACL_WEBAUTH_REDIRECT 1
config flexconnect acl rule action ACL_WEBAUTH_REDIRECT 1 permit
config flexconnect acl rule protocol ACL_WEBAUTH_REDIRECT 1 17
config flexconnect acl rule source port range ACL_WEBAUTH_REDIRECT 1 0 65535
config flexconnect acl rule destination port range ACL_WEBAUTH_REDIRECT 1 53 53
config flexconnect acl rule add ACL_WEBAUTH_REDIRECT 1
config flexconnect acl rule action ACL_WEBAUTH_REDIRECT 1 permit
config flexconnect acl rule protocol ACL_WEBAUTH_REDIRECT 1 17
config flexconnect acl rule source port range ACL_WEBAUTH_REDIRECT 1 53 53
config flexconnect acl apply ACL_WEBAUTH_REDIRECT

config flexconnect acl create BLACKHOLE
config flexconnect acl rule add BLACKHOLE 1
config flexconnect acl rule action BLACKHOLE 1 permit
config flexconnect acl rule protocol BLACKHOLE 1 6
config flexconnect acl rule source port range BLACKHOLE 1 0 65535
config flexconnect acl rule destination address BLACKHOLE 1 10.1.200.12 255.255.255.255
config flexconnect acl rule destination port range BLACKHOLE 1 8444 8444
config flexconnect acl rule add BLACKHOLE 1
config flexconnect acl rule action BLACKHOLE 1 permit
config flexconnect acl rule protocol BLACKHOLE 1 6
config flexconnect acl rule source address BLACKHOLE 1 10.1.200.12 255.255.255.255
config flexconnect acl rule source port range BLACKHOLE 1 8444 8444
config flexconnect acl rule destination port range BLACKHOLE 1 0 65535
config flexconnect acl rule add BLACKHOLE 1
config flexconnect acl rule action BLACKHOLE 1 permit
config flexconnect acl rule protocol BLACKHOLE 1 6
config flexconnect acl rule source port range BLACKHOLE 1 0 65535
config flexconnect acl rule destination address BLACKHOLE 1 10.1.200.11 255.255.255.255
config flexconnect acl rule destination port range BLACKHOLE 1 8444 8444
config flexconnect acl rule add BLACKHOLE 1
config flexconnect acl rule action BLACKHOLE 1 permit
config flexconnect acl rule protocol BLACKHOLE 1 6
config flexconnect acl rule source address BLACKHOLE 1 10.1.200.11 255.255.255.255
config flexconnect acl rule source port range BLACKHOLE 1 8444 8444
config flexconnect acl rule destination port range BLACKHOLE 1 0 65535
config flexconnect acl rule add BLACKHOLE 1
config flexconnect acl rule action BLACKHOLE 1 permit
config flexconnect acl rule protocol BLACKHOLE 1 17
config flexconnect acl rule source port range BLACKHOLE 1 0 65535
config flexconnect acl rule destination port range BLACKHOLE 1 53 53
config flexconnect acl rule add BLACKHOLE 1
config flexconnect acl rule action BLACKHOLE 1 permit
config flexconnect acl rule protocol BLACKHOLE 1 17
config flexconnect acl rule source port range BLACKHOLE 1 53 53
config flexconnect acl rule destination port range BLACKHOLE 1 0 65535
config flexconnect acl apply BLACKHOLE
```

作成した後は、FlexConnect AP に追加します。

```
config ap flexconnect policy acl add ACL_WEBAUTH_REDIRECT AP_NAME
config ap flexconnect policy acl add BLACKHOLE AP_NAME
```

注: FlexConnect モードでは、ローカル認証などの追加設定がサポートされますが、これらのオプションは ISE 統合の一部としてテストされていません。また、このドキュメントでは個々の AP を使用した必要な設定について扱いますが、通常は FlexConnect グループを設定して AP の設定を管理する方が簡単です。ISE による FlexConnect モード AP ローカル スイッチング導入の場合は、次の警告にも注意してください。

- FlexConnect を利用しているエンドポイントが、ISE ノードにアクセスできる必要があります
- FlexConnect ACL は DNS ACL をサポートしていません
- ローカルに切り替えられたトラフィックの TrustSec はサポートされません

FlexConnect エンドポイント セッションには FlexConnect ACL が適用されますが、古いバージョンの WLC では、同じ ACL 名がすでにある通常の ACL がない FlexConnect ACL の適用に失敗する場合があります。少なくとも、WLC に登録された通常の ACL 名を付ける必要があります。その場合は、単純に次のように空の ACL を作成します。

```
config acl create ACL_WEBAUTH_REDIRECT
config acl apply ACL_WEBAUTH_REDIRECT

config acl create BLACKHOLE
config acl apply BLACKHOLE
```

自動アンカーされた WLAN

お客様はセキュリティを強化するために、自動アンカー（AKA ゲストトンネリング）を設定して、ゲスト WLAN トラフィックを DMZ にあるアンカー コントローラにトンネリングすることがよくあります。これは、ISE 中央 WebAuth でサポートされる設定です。ただし、これを機能させるには特定の設定が必要です。これは、アンカー コントローラ WLAN で RADIUS アカウンティング サーバを無効にする必要があることを除いて、通常は自動アンカー設定に設定できます。OPEN WLAN がアンカーされていることを前提とした、アンカー コントローラでの WLAN 設定の例を示します。

```
config wlan create 12 OPEN OPEN
config wlan interface 12 GUEST
config wlan security wpa disable 12
config wlan mac-filtering enable 12
config wlan radius_server auth disable 12
config wlan radius_server acct disable 12
config wlan radius_server acct interim-update disable 12
config wlan aaa-override enable 12
config wlan session-timeout 12 1800
config wlan usertimeout 180 12
config wlan chd 12 disable
config wlan ccx AironetIeSupport disable 12
config wlan dhcp_server 12 0.0.0.0 required
config wlan nac radius enable 12
config wlan profiling radius all enable 12
config wlan enable 12
```

注: 前の例では RADIUS 設定が無効になっていますが、アンカー コントローラはモビリティ メッセージの外部コントローラによって中継された ISE からセッションに適用する ACL 名を受信します。アンカー コントローラ設定にリダイレクト ACL を含めて、外部コントローラによって呼び出されたときにユーザ セッションに適用できるようにすることが必要です。