AireOS のある ISE ワイヤレス CWA とホットスポット フローおよび次世代 WLC を設定する

目次

概要

この資料に Cisco AireOS および Generation（NGWC）次のワイヤレス LAN コントローラ（WLCs）で Identity Services Engine （ISE）の 3 つのゲスト ユース ケースを設定する方法を記述されています。

前提条件

要件

次の項目に関する知識が推奨されます。

- Ciscoワイヤレス LAN コントローラ（およびコンバージしたアクセス統一される）
- Identity Services Engine（ISE）

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco Identity Services Engine バージョン 2.1
- Ciscoワイヤレス LAN コントローラ 5508 実行 8.0.121.0
- 次世代 03.06.04.E を実行するワイヤレス コントローラ（NGWC） Catalyst 3850(WS-C3850-24P)

設定

ネットワーク図

この資料でカバーされるステップは統一され、コンバージしたアクセス WLCs の典型的なコンフィギュレーションを ISE のゲスト フローをサポートするために説明します。

統一しました 5508 WLC を設定して下さい

WLC 観点からの ISE で、設定される使用例に関係なくそれはすべて認証およびアカウンティング サーバとして ISE に（AAA 上書きするおよび RADIUS NAC と）イネーブルになっている MAC フィルタリングそのポイントと開いた SSID に接続するワイヤレス エンド ポイントから開始します。 これは ISE が ISE のゲスト ポータルにリダイレクトの正常な適用のための WLC に動的に必要な属性を押すことができるようにします。

グローバル コンフィギュレーション

1. 認証およびアカウンティング サーバとして ISE をグローバルに追加して下さい。

   - **セキュリティ > AAA > 認証**にナビゲート し、『New』 をクリック して下さい

   - ISE サーバIP および共有秘密を入力して下さい
   - **RFC 3676**（許可または CoA サポートの変更）**の**サーバステータスおよび**サポートがイネーブルになった**に両方セットであることを確認して下さい。
   - サーバタイムアウト デフォルトで AireOS の下で WLCs は 2 秒を過します。 ネットワーク

特性（レイテンシー、ISE および WLC、異なる場所の等）によっては不必要なフェールオーバー イベントを避けるために少なくとも 5 秒にサーバタイムアウトを高めることは有利かもしれません。
- [Apply] をクリックします。
- あれば設定するべき複数のポリシー Services ノード（PSN）は追加サーバエントリを作成することを続行します。

注: この特定の設定例は 2 つの ISE 例が含まれています

- **セキュリティ > AAA > RADIUS > アカウンティング**にナビゲート し、『New』 をクリックして下さい
- ISE サーバIP および共有秘密を入力して下さい
- サーバステータスがイネーブルになったに設定されるようにして下さい
- サーバタイムアウトを必要ならば高めて下さい（デフォルトは 2 秒です）。

2. フォールバック設定。

統一された環境でサーバタイムアウトが引き起こされれば WLC は次の設定されたサーバに進みます。 次に WLAN からの行で。 他が利用可能ではない場合 WLC はグローバル な Servers リストの次の 1 つを選択します。 多重サーバが SSID プライマリ サーバがオンラインでもフェールオーバーが発生するで（プライマリ、セカンダリ、等） WLC デフォルトでセカンダリ例に永久に認証および（または）アカウンティング トラフィックを送信 し続ける設定される時。

この動作イネーブル フォールバックを軽減するため。 **セキュリティ > AAA > RADIUS > フォールバック**へのナビゲート。 デフォルトの動作は消えています。 サーバ イベントから回復唯一の方法は admin 介入を必要とします（グローバルにサーバの管理状態を跳ねて下さい）。

フォールバックを有効に するために 2 つのオプションがあります:

- **受動**-パッシブモードでは、サーバが WLC 認証要求に応答しなければ、WLC は非アクティブキューにサーバを移動し、タイマー（秒オプションの間隔）を設定します。 タイマーが切れるとき、WLC はサーバ実際のステータスに関係なくアクティブなキューにサーバを移動します。 認証要求がサーバはまだあることを（意味するタイムアウト イベント）という結果にサーバエントリが非アクティブ キューに終ればおよびタイマーが再度移動される再度作動すれば。 サーバが正常に応答を返す場合、アクティブなキューに残ります。 ここの構成可能値は 180 から 3600 秒から行きます。

- **アクティブ**-アクティブ モードでは、サーバが WLC 認証要求に応答しないとき、WLC はデッドようにサーバを示し、そして非活動的なサーバ プールにサーバを移動し、そのサーバが応答するまでプローブ メッセージを定期的に送信 し始めます。 サーバが応答した場合、WLC は停止状態のサーバをアクティブなプールに移動し、プローブ メッセージの送信を停止します。

このモードで WLC は秒（3600）にユーザ名およびプローブ間隔をへの 180 入力するように要求します。

注: WLC プローブは認証の成功を必要としません。 いずれにしても、成功したのか失敗した認証はアクティブなキューにサーバを促進する十分であるサーバレスポンスとみなされます。

ゲストの Service Set Identifier （ SSID ）を設定して下さい:

- WLAN タブにナビゲートし、新しいオプションを『Go』 をクリック します作成して下さい:

- Profile Name および SSID 名前を入力して下さい。 [Apply] をクリックします。
- General タブの下で使用されるべきインターフェイスかインターフェイス グループを選択して下さい（ゲスト VLAN）。

- **セキュリティ > レイヤ2 > レイヤ2 セキュリティ**の下で **Mac フィルタリング** チェックボックスを『None』 を選択 し、有効に して下さい。

- **AAA サーバ** タブ一定認証およびアカウンティング サーバの下でプライマリおよびセカンダリサーバを**イネーブルに設定し、**選択します。

- **暫時アップデート**: これはこのフローに利点を追加しないオプショナルコンフィギュレーションです。 それを有効に することを好む場合 WLC 8.x かより高いコードを実行する必要があります:

無効: 機能は完全に無効です。

0 間隔とイネーブルにされる: WLC は ISE にクライアントのモバイル ステーション制御 Block（MSCB）エントリ（IE に変更がある度にアカウンティング更新を送ります。 IPv4 か IPv6 アドレス 指定または変更、クライアント ローミング イベント、等は）追加定期的なアップデート送信されません。

設定された暫時間隔とイネーブルにされる: このモードで WLC はクライアントの MSCB エントリ変更に ISE に通知を送信 し、また設定された 間隔で追加定期的にアカウンティング通知を送信 します（あらゆる変更に関係なく）。

- Advanced タブ イネーブルの下で **AAA 上書きを許可すれば NAC 状態**の下で **NAC を**『RADIUS』 を選択 して下さい。 これは WLC が ISE から来る属性値ペア（AVP）を加えるようにします。
- SSID General タブにナビゲートし、**イネーブルになった**に SSID ステータスを設定して下さい

- 変更を**加えて下さい**。

リダイレクト ACL を設定して下さい

この ACL は ISE によって参照され、どんなトラフィックがリダイレクトされ、どんなトラフィックが許可されるか判別します。

- **Security タブ > アクセス・コントロール・リスト**に行き、『New』 をクリック して下さい
- これは ACL の例です

この ACL は TCPポート 8443 上の DNS サービスおよび ISE ノードに出入してアクセスを許可する必要があります。 トラフィックの他は ISE のゲスト門脈 URL にリダイレクトされることを意味する暗黙の deny が下部のにあります。

HTTPS リダイレクト

この機能は AireOS バージョン 8.0.x でサポートされ、が、活動化しますデフォルトで消えます。 HTTPS サポートを有効に するために WLC **管理 > HTTP-HTTPS > HTTPS リダイレクション**に行き、それを**イネーブルにするか、**または適用します CLI のこのコマンドを設定して下さい:

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

HTTPS リダイレクトの後の証明書警告はイネーブルになっています

https リダイレクトがイネーブルになっていた後、ユーザはリダイレクトの間に証明書信頼問題に直面するかもしれません。 これはコントローラに有効なチェーン証明書があっても、そしてこの証明書がサード パーティによって信頼される認証局によって署名しても見られます。 理由は WLC でインストールされる証明書が仮想インターフェイス ホスト名-か IP アドレスに発行されることです。 クライアントが https を試す時: //cisco.com は、ブラウザ証明書が cisco.com に発行されると期待します。 ただし、なぜならクライアントが発行する GET を代行受信ことはできる WLC それは最初に WLC が SSL ハンドシェイク フェーズの間に仮想インターフェイス 証明書を示す HTTPS セッションを設定する必要があります。 SSL ハンドシェイクの間に示される証明書がクライアントがアクセスすることを試みているオリジナル Webサイトに発行されなかったのでこれによりブラウザは警告を表示します（IE。 cisco.com は WLC の仮想インターフェイス ホスト名に反対しました）。 異なるブラウザすべての異なる Certificate エラーメッセージが同じ問題に関連するのを見るかもしれません。

積極的なフェールオーバー

この機能は AireOS WLCs でデフォルトでイネーブルになっています。 積極的なフェールオーバーがイネーブルになっているとき、WLC は Radius タイムアウト イベントが 1 人のクライアントに影響を与えた後無理解、それ次の設定された AAAサーバに進むと同時に AAAサーバを示します。

機能がディセーブルにされるとき WLC は次のサーバに RADIUS タイムアウト イベントが少なくとも 3 人のクライアントセッションと発生するときだけ失敗します。 この機能はこのコマンドによってディセーブルにされるかもしれません（このコマンドにリブートが必要となりません）:

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

機能の現在のステータスを確認するため:

```
(Cisco Controller) >show radius summary

Vendor Id Backward Compatibility..... Disabled
Call Station Id Case..... lower
Acct Call Station Id Type..... Mac Address
Auth Call Station Id Type..... AP's Radio MAC Address:SSID
Extended Source Ports Support..... Enabled
Aggressive Failover..... Disabled
```

捕虜バイパス

これを誘発するために他のエンド ポイントが十分に可能なブラウザを起動させる間、捕虜門脈を検出するために捕虜 Network Assistant（チャンネル利用不可）メカニズムをサポートするおよび自動起動は通常制御ウィンドウの疑似ブラウザによってログオン ページこれをしますエンド ポイント。 チャンネル利用不可が疑似ブラウザを起動させるエンド ポイントに関しては ISE 捕虜ポータルにリダイレクトされたとき、これはフローを壊すかもしれません。 これは一般的に Apple IOSデバイスに影響を与え、デバイス登録、VLAN DHCPRlease、準拠性 チェック、先祖などを

必要とするフローで特に悪影響をもたらします

使用中のフローの複雑な状況によっては捕虜バイパスを有効に することを推奨するかもしれません。 そのようなシナリオでは、WLC はチャンネル利用不可門脈ディスカバリ メカニズムを無視し、クライアントはリダイレクト プロセスを開始するためにブラウザを開く必要があります。

機能のステータスを確認して下さい:

```
(Cisco Controller) >show network summary

Web Auth CMCC Support ..................... Disabled
Web Auth Redirect Ports ................... 80,3128
Web Auth Proxy Redirect  .................. Disable
Web Auth Captive-Bypass   ................. Disabled
Web Auth Secure Web  ...................... Enable
Web Auth Secure Redirection  .............. Enable
```

この機能型を有効に するためこのコマンド:

```
(Cisco Controller) >config network web-auth captive-bypass enable
Web-auth support for Captive-Bypass will be enabled.

You must reset system for this setting to take effect.
```

WLC は実施される変更のためにリセット システム（再起動）が必要であるユーザに警告します。

この時点で**提示ネットワーク要約は**イネーブルになられているように機能を示しますが、実施される変更のために WLC は再起動する必要があります。

コンバージしました設定して下さい 3850 NGWC

グローバル コンフィギュレーション

1. **認証およびアカウンティング サーバとして ISE をグローバルに追加して下さい**

   - **設定 > Security > RADIUS > サーバ**にナビゲート し、『New』 をクリック して下さい
   - 環境条件を反映する ISE **サーバのIPアドレス**、**共有秘密**、**サーバタイムアウトを**および**リトライ回数を**入力して下さい。
   - **RFC 3570**（CoA サポート）**のサポートが**イネーブルになっていることを確認して下さい。
   - セカンダリサーバ エントリを追加するためにプロセスを繰り返して下さい。
2. **ISE のサーバグループを作成して下さい**

   - **設定 > Security > サーバグループ**にナビゲート し、『New』 をクリック して下さい
   - 名前をグループに割り当て、分に**デッド タイム**値を入力して下さい。 これはアクティブなサーバ リストに再度促進される前にコントローラが非アクティブ キューでサーバを保存すること時間です。
   - 利用可能な Servers リストそれらをから割り当てられたサーバ カラムに追加して下さい。
3. **グローバルに Dot1x を有効に して下さい**

   - **設定 > AAA > メソッドリスト > 一般**にナビゲート し、**Dot1x システム Auth 制御を**有効に し

て下さい

4. **メソッドリストを設定して下さい**

- **設定 > AAA > メソッドリスト > 認証**にナビゲート し、新しいメソッド リストを作成して下さい。 この場合それは型 Dot1x およびグループ ISE_Group （ 前の手順で作成されるグループ）です。 それからヒットは**適用します**

- （**設定 > AAA > メソッドリスト > アカウンティング**）説明および（**設定 > AAA > メソッドリスト > 許可**）のために同じを許可して下さい。 彼らはこのようになる必要があります

5. **許可 MAC フィルタ方式を作成して下さい。**

これは SSID 設定以降から呼出されます。

- **AAA > メソッドリスト > 許可は Configuration>** にナビゲート し、『New』 をクリック します。
- **メソッドリスト名前を**入力して下さい。 **= ネットワーク**および**グループ タイプ グループ**『Type』 を選択 しました。
- 割り当てられた Server Groups フィールドに ISE_Group を追加して下さい。

SSID 設定

1. **ゲスト SSID を作成して下さい**

- **設定 > ワイヤレス > WLAN** にナビゲート し、『New』 をクリック して下さい
- WLAN ID、SSID および Profile Name を入力し、『Apply』 をクリック して下さい。
- インターフェイス/インターフェイス グループの下の SSID 設定でゲスト VLAN レイヤ3 インターフェイスを選択しなさい。

- **セキュリティ > レイヤ2** の下で『None』 を選択 すれば **Mac フィルタリング**の隣で前もって設定した Mac フィルタ メソッドリスト名前を入力して下さい（MacFilterMethod）。
- **セキュリティ > AAAサーバ** タブの下で適切な認証およびアカウンティング方式リスト（ISE_Method）を選択して下さい。

- **Advanced タブ** イネーブルの下で **AAA 上書き**および **NAC 状態を許可して下さい。** 設定の他は各によって配置の要件（セッション タイムアウト、クライアント 除外、サポート、Aironet Extension のための等）調節する必要があります。

- General タブに設定しますイネーブルになったにステータスをナビゲートして下さい。 それからヒットは**適用します。**

リダイレクト ACL構成

この ACL は最初の MAB 要求に応じて access-accept で ISE 以降によって参照されます。
NGWC はどんなトラフィックが許可する必要があるかそれをリダイレクトするべきどんなトラフィックをか判別するのに使用し。

- **設定 > Security > ACL > アクセス・コントロール・リスト**にナビゲート し、『Add New』 をクリック して下さい。
- 拡張を選択し、ACL 名前を入力して下さい。
- このピクチャは典型的なリダイレクト ACL の例を示します:

  注: 10 ラインはオプションです。 これは通常トラブルシューティングのために提案します 追加されます。 この ACL は DHCP、DNS サービスとまた ISE サーバ ポート TCP 8443(Deny ACE へのアクセスを許可する必要があります)。 HTTP および HTTPS トラフィックはリダイレクトされます (割り当て ACE)。

Command Line Interface （ CLI) 設定

前の手順で説明されているすべての設定はまた CLI によって適用します。

グローバルにイネーブルになっている 802.1X

```
dot1x system-auth-control
```

グローバル な AAA設定

```
aaa new-model
!
aaa authentication dot1x ISE_Method group ISE_Group
aaa authorization network ISE_Method group ISE_Group
aaa accounting Identity ISE_Method start-stop group ISE_Group
!
aaa server radius dynamic-author
 client 14.36.157.210 server-key *****
 client 14.36.157.21 server-key *****
 auth-type any
!
radius server ISE1
 address ipv4 14.36.157.210 auth-port 1812 acct-port 1813
 timeout 5
 retransmit 2
 key *****
!
radius server ISE2
 address ipv4 14.36.157.21 auth-port 1812 acct-port 1813
 timeout 5
 retransmit 2
 key *****
!
!
aaa group server radius ISE_Group
 server name ISE2
 server name ISE1
 deadtime 10
 mac-delimiter colon
!
```

Wlan 設定

```
 wlan Guest 1 Guest
```

```
 aaa-override
 accounting-list ISE_Method
 client vlan VLAN0301
 mac-filtering MacFilterMethod
 nac
 no security wpa
 no security wpa akm dot1x
 no security wpa wpa2
 no security wpa wpa2 ciphers aes
 security dot1x authentication-list ISE_Method
 no security ft over-the-ds
 session-timeout 28800
 no shutdown
```

リダイレクト ACL 例

```
3850#show ip access-lists Guest_Redirect
Extended IP access list Guest_Redirect
    10 deny icmp any any
    20 deny udp any any eq bootps
    30 deny udp any any eq bootpc
    40 deny udp any any eq domain
    50 deny tcp any host 14.36.157.210 eq 8443
    60 deny tcp any host 14.36.157.21 eq 8443
    70 permit tcp any any eq www
    80 permit tcp any any eq 443
```

HTTP および HTTPS サポート

```
3850#show run | inc http
ip http server
ip http secure-server
```

注: HTTP 上の WLC へのアクセスを制限するために ACL を適用する場合リダイレクションに影響を与えます。

ISE の設定

この資料で説明されているこのセクションがすべての使用例をサポートするために ISE で必要な設定を説明します。

よくある ISE コンフィギュレーション タスク

1. ISE への ログオンおよび **Administration > ネットワークリソース > ネットワークデバイス**へのナビゲートはおよび『Add』 をクリック します
2. WLC およびデバイス **IP アドレス**に関連付けられる**名前を**入力して下さい。
3. **RADIUS認証設定**ボックスをチェックし、WLC 側で設定される**共有秘密を**入力して下さい。 次に [Submit] をクリックします。

4. **ポリシー > 認証**へのおよび MAB の下のナビゲートは**使用**の下でそれを『Edit』 をクリッ

ク し、確認します: **ユーザがなければ内部エンド ポイントは続くために**オプション設定されます（デフォルトでそこにあるはずです）。

使用例 1: 各ユーザ接続のゲスト認証を用いる CWA

フロー概要

1. 無線ユーザはゲスト SSID に接続します。
2. WLC は AAAサーバとして ISE を使用して MAC アドレスに基づいてエンド ポイントを認証します。
3. ISE は 2 つの属性値ペア（AVP）との access-accept 戻り、: URL リダイレクトおよび URL リダイレクト ACL。 WLC がエンド ポイント セッションにこの AVP を適用すれば、ステーションは DHCP 必須に CENTRAL_WEB_AUTH に IP アドレスをつかめばそれとどまります移行し。 このステップで WLC はクライアントの http/https トラフィックをリダイレクトし始めて準備ができています。
4. エンドユーザは Webブラウザを開発し、HTTP または HTTPS トラフィックが生成されれば、WLC は ISE ゲスト ポータルにユーザをリダイレクトします。
5. ゲスト信任状をプロンプト表示するゲスト ポータルへのユーザ gets（この場合スポンサー作成される）入力するために。
6. 信任状検証に ISE は AUP ページを表示し、クライアントが受け入れれば、ダイナミック CoA 型 Re-authenticate WLC に送信されます。
7. WLC はモバイル ステーションに非認証を発行しないで MAC フィルタリング認証を再処理します。 これはエンド ポイントにシームレスであるはずです。
8. 再認証イベントが起これば ISE は承認ポリシーを再評価し、前の正常なゲスト認証イベントがあったので今回エンド ポイントは割り当てアクセスを可能になります。

このプロセスはユーザが SSID に接続する度にそれ自身を繰り返されます。

設定

1. ISE へのナビゲートおよび**作業センター > ゲスト アクセス**へのナビゲートは **> > ゲスト ポータル** > 選択します**後援されたゲスト ポータルを設定します**（または新しい門脈型後援ゲストを作成して下さい）。
2. **ゲスト デバイス登録**の下で設定はすべてのオプションのチェックを外し、『SAVE』 をクリック します。

3. [Policy] > [Policy Elements] > [Results] > [Authorization] > [Authorization Profiles] に移動します。 [Add] をクリックします。

4. このプロファイルは最初の MAC 認証バイパス（MAB）要求に応じて WLC にリダイレクト **URL** およびリダイレクト URL **ACL** 押下げられます。

- チェックされる **Web リダイレクション（CWA、MDM、NSP、CPP）が中央集中型 Web Auth を**選択したら、そしてリダイレクト ACL 名前を **ACL** フィールドの下で入力し、**値**の下で**後援されたゲスト Portal（default）**選択して下さい（または前の手順で作成される他のどの特定のポータルも）。

プロファイルは類似したこのピクチャの 1 つを検知 する必要があります。 それから『SAVE』 をクリック して下さい。

あると同時にページの一番下に属性詳細は WLC に属性値 Pairs（AVPs）押されます

5. **ポリシー > 許可**にナビゲート し、新しいルールを追加して下さい。 このルールは WLC からの最初の MAC 認証要求に応じてリダイレクト プロセスを誘発するものです。（この場合 **Wireless_Guest_Redirect と**呼出される）。

6. **条件**の下で**ライブラリから既存の条件を**『SELECT』 を選択 して下さい、そして**条件名**の下で**複合条件（COBOL）を**選択して下さい。 **Wireless_MAB と**呼ばれるあらかじめ定義された複合条件（COBOL）を選択して下さい。

> **注:** この条件はアクセス要求によって起こされる形式で期待される 2 つの RADIUS特性で WLC（MAC 認証 bypass> のための特定の要求を示すコール <present NAS-Port-Type= IEEE 802.11 Check< = すべてのワイヤレス requests> およびサービス タイプで構成されています）

7. 結果の下で、**規格 > CWA_Redirect**（前の手順で作成される許可プロファイル）を選択して下さい。 それから『Done』 をクリック し、**保存して下さい**

8. **CWA_Redirect** ルールの終わりにナビゲート し、矢印をの隣で**編集します**クリックして下さい。 それから**上で重複を**選択して下さい。

9. 一度セッションが ISE の CoA（この場合 Wireless_Guest_Access）に再認証されるこれがそのポリシー エンド ポイント一致であるので名前を修正して下さい。

10. **Wireless_MAB** 複合条件（COBOL）の隣で **+** 状態を拡張する記号クリックすれば **Wireless_MAB** 状態の終りまでに**属性/値を**『Add』 をクリック して下さい。

11. の下で「属性」を選択しました**ネットワーク アクセス > UseCase 等号ゲスト フローを**選択して下さい

12. **権限**の下で **PermitAccess を**選択して下さい。 それから『Done』 をクリック し、**保存して下さい**

2 つのポリシーはこれに類似したに検知 する必要があります:

使用例 2: ゲスト認証を 1 日 1 回実施するデバイス登録を用いる CWA。

フロー概要

1. 無線ユーザはゲスト SSID に接続します。
2. WLC は AAAサーバとして ISE を使用して MAC アドレスに基づいてエンド ポイントを認証します。
3. ISE は 2 つの属性値ペア（AVP）との access-accept 戻り、（URL リダイレクトおよび URL リダイレクト ACL）。
4. WLC がエンド ポイント セッションにこの AVP を適用すれば、ステーションは DHCP 必須に CENTRAL_WEB_AUTH に IP アドレスをつかめばそれとどまります移行し。 このステップで WLC はクライアントの http/https トラフィックをリダイレクトし始めて準備ができています。

5. エンドユーザは Webブラウザを開発し、HTTP または HTTPS トラフィックが生成されれば、WLC は ISE ゲスト ポータルにユーザをリダイレクトします。
6. ユーザがゲスト ポータルに着けばスポンサー作成された信任状を入力するために、彼はプロンプト表示されます。
7. 信任状検証に ISE は特定の（前もって構成された）エンド ポイント識別グループ（デバイス登録）にこのエンド ポイントを追加します。
8. AUP ページはクライアントが受け入れれば、ダイナミック CoA 型再認証します表示され。WLC に送信されます。
9. モバイル ステーションに非認証を発行しないで MAC フィルタリング認証を再処理する WLC。 これはエンド ポイントにシームレスであるはずです。
10. 再認証イベントが起これば ISE は承認ポリシーを再評価します。 エンド ポイントが権限エンド ポイント識別グループ ISE のメンバーであるので今回は制限無しでアクセスを受け入れます戻します。
11. エンド ポイントがステップ 6 で登録されていたので、それがユーザもどって来るたびに、彼はネットワークで ISE から手動で取除かれる、またはエンド ポイント パージ ポリシーは条件を満たすエンド ポイントをフラッシュすることを実行しますまで許可されます。

この Lab Scenario では、認証は 1 日 1 回実施されます。 使用されたエンド ポイント識別グループのすべてのエンド ポイントを毎日取除く再認証トリガーはエンド ポイント パージ ポリシーです。

> **注:** 最後の AUP 承認以来の経過時間に基づいてゲスト認証イベントを実施することは可能性のあるです。 これは 1 日 1 回ゲスト ログオンをより頻繁に実施する必要がある場合オプションであるかもしれません（例で 4 時間毎に）。

設定

1. **作業センター > ゲスト アクセス**への ISE ナビゲートで **> > ゲスト ポータル** > 選択します**後援されたゲスト ポータルを設定して下さい**（または新しい門脈型後援ゲストを作成して下さい）。
2. **ゲスト デバイス登録**設定の下でオプションが**自動的にデバイスが**チェックされる**ゲストを登録する**ことを確認して下さい。 [Save] をクリックします。

3. **作業センター > ゲスト アクセス**へのナビゲートは **> > ゲスト型設定するか**、またはちょうどポータルのゲスト デバイス登録設定の下で規定 されるショートカットをクリックします。

4. スポンサー ユーザがゲスト アカウントを作成するとき、彼はそれにゲスト型を割り当てます。 各々の個々のゲスト型は異なるエンド ポイント識別 Group.To にこれらのゲストユーザ向けに割り当てるデバイスがに追加する必要があるエンド ポイント識別グループを選択するゲスト型をスポンサー使用属する登録されていたエンド ポイントがある場合があります（この使用例はウィークリー（デフォルト）に基づいています）。

5. **ログオン オプション**の下のゲスト型で、**ゲスト デバイス登録に**廃棄メニュー **エンド ポイント識別グループ**からエンド ポイント グループを選択して下さい

6. [Policy] > [Policy Elements] > [Results] > [Authorization] > [Authorization Profiles] に移動します。 [Add] をクリックします。

7. このプロファイルは最初の MAC 認証バイパス（MAB）要求に応じて WLC にリダイレクト **URL** およびリダイレクト URL **ACL** 押下げられます。

- チェックされる **Web リダイレクション（CWA、MDM、NSP、CPP）が中央集中型 Web Auth を**選択したら、そしてリダイレクト ACL 名前を **ACL** フィールドの下で入力し、このフロー（**CWA_DeviceRegistration**）に**値**の下で作成されるポータルを選択して下さい。

8. **ポリシー > 許可**にナビゲート し、新しいルールを追加して下さい。 このルールは WLC からの最初の MAC 認証要求に応じてリダイレクト プロセスを誘発するものです。（この場合 **Wireless_Guest_Redirect と**呼出される）。

9. **条件**の下で**ライブラリから既存の条件を**『SELECT』 を選択 しました、そして**条件名**の下で**複合条件（COBOL）を**選択して下さい。 **Wireless_MAB と**呼ばれるあらかじめ定義された複合条件（COBOL）を選択して下さい。

10. 結果の下で、**規格 > CWA_DeviceRegistration**（前の手順で作成される許可プロファイル）を選択して下さい。 それから『Done』 をクリック し、**保存して下さい**

11. これが再認証イベントから戻った後エンド ポイントが見つけるポリシーであるので上記のポリシーを複写して下さい名前を修正して下さい（Wireless_Guest_Access と呼ばれる）。

12. **識別グループ**の下でボックスを**詳述し、エンド ポイント識別グループを**選択し、ゲスト Type（GuestEndpoints）の下で参照したグループを選択します。

13. 結果の下で **PermitAccess を**選択して下さい。 変更を『Done』 をクリック し、**保存して下さい**。

14. エンド ポイント パージ ポリシー作成すれば GuestEndpoint グループ毎日をクリアする。

- **Administration > アイデンティティ管理 > 設定 > エンド ポイント パージ**へのナビゲート
- **パージ** ルールの下で経過時間が 30 日より大きい場合デフォルトで 1 つがあるはずですトリガー GuestEndpoints その削除。
- （デフォルトが取除かれたら） GuestEndpoints のための現在のポリシーを修正するか、または新しいものを作成して下さい。 パージ ポリシーが明確な時間を毎日実行することに注目して下さい。

この場合条件は経過日数の GuestEndpoints のメンバー 1 日以下です

使用例 3: HostSpot ポータル

フロー概要

1. 無線ユーザはゲスト SSID に接続します。
2. WLC は AAAサーバとして ISE を使用して MAC アドレスに基づいてエンド ポイントを認証します。
3. ISE は 2 つの属性値ペア（AVP）との access-accept を戻します: URL リダイレクトおよび URL リダイレクト ACL。
4. WLC がエンド ポイント セッションにこの AVP を適用すれば、ステーションは DHCP 必須に CENTRAL_WEB_AUTH に IP アドレスをつかめばそれとどまります移行し。 このステップで WLC はクライアントの http/https トラフィックをリダイレクトして準備ができています。
5. エンドユーザは Webブラウザを開発し、HTTP または HTTPS トラフィックが生成されれば、WLC は ISE ホットスポット ポータルにユーザをリダイレクトします。
6. ポータルでユーザがインターネット接続規定を受け入れるためにプロンプト表示されれば。
7. ISE は構成されたエンドポイント識別グループにエンド ポイント MAC アドレス（エンドポ

イントID）を追加します。
8. そのポリシー Services ノード（PSN）は WLC に要求を発行しますダイナミック CoA タイプ Admin **リセットを**処理します。
9. WLC が着信 CoA を処理することを終わればクライアントに非認証を発行します（接続はクライアントがもどって来ることができるように）かかる時間の損失です。
10. クライアントが再接続すれば、新しいセッションはそうそこにです ISE 側のセッション継続作成されません。 認証が新しいスレッドとして処理されることを意味します。
11. エンド ポイントが構成されたエンドポイント識別グループに追加される、およびエンド ポイントはそのグループの一部であるかどうか確認する承認ポリシーがあるので、新しい認証はこのポリシーと一致します。 結果はゲスト ネットワークにフル アクセスです。
12. ユーザはエンド ポイント識別オブジェクトがエンド ポイント パージ ポリシーの結果として ISE データベースから削除されなければ AUP を再度受け入れなければならないべきではありません。

設定

1. 登録ににこれらのデバイスを移動するために新しいエンド ポイント識別グループを作成して下さい。 **グループ化し、> エンド ポイント識別グループは作業センター > ゲスト アクセス > 識別**にクリックしますナビゲート します 。

- グループ名（この場合 HotSpot_Endpoints）を入力して下さい。 説明を追加すれば親 グループは必要ではないです。

2. **作業センター > ゲスト アクセス**へのナビゲートは **> > ゲスト ポータル** > 選択します**ホットスポット ポータル（デフォルト）を設定します。**

3. 門脈設定を拡張すればエンド ポイント識別グループの下で**エンド ポイント識別グループ**の下で **HostSpot_Endpoints** グループを選択して下さい。 これは特定のグループに登録されているデバイスを送ります。

4.変更を**保存して下さい。**

5. 許可プロファイルを作成して下さい WLC によって起きる MAB 認証にホットスポット ポータルを呼出す。

- **ポリシー > ポリシー要素 > 結果 > 許可 > 許可プロファイル**にナビゲート し、1 つを作成して下さい（HotSpotRedirect）。
- **Web リダイレクション（CWA、MDM、NSP、CPP）が**チェックされたら**ホットスポットを**選択し、そして ACL フィールド（Guest_Redirect）のリダイレクト ACL 名前を入力し、ように値選定された正しいポータル（**ホットスポット ポータル（デフォルト）**）。

6. WLC からの最初の MAB 要求に HotSpotRedirect 結果を誘発する承認ポリシーを作成して下さい。

- **ポリシー > 許可**にナビゲート し、新しいルールを追加して下さい。 このルールは WLC からの最初の MAC 認証要求に応じてリダイレクト プロセスを誘発するものです。（この場合 **Wireless_HotSpot_Redirect と**呼出される）。
- **条件**の下で**ライブラリから既存の条件を**『SELECT』 を選択 して下さい、そして**条件名**の下で**複合条件（COBOL）を**選択して下さい
- 結果の下で、**規格** > **HotSpotRedirect**（前の手順で作成される許可プロファイル）を選択し

て下さい。 それから『Done』 をクリック し、**保存して下さい**
7. 第 2 承認ポリシーを作成して下さい。

- これが再認証イベントから戻った後エンド ポイントが見つけるポリシーであるので上記のポリシーを複写して下さい名前を修正して下さい（Wireless_HotSpot_Access と呼ばれる）。
- 次に**識別グループ**の下でボックスを**詳述しましたり**、先に作成した**エンド ポイント識別グループを**およびグループを選択します（**HotSpot_Endpoints**）。
- 結果の下で **PermitAccess を**選択して下さい。 変更を『Done』 をクリック し、**保存して下さい**。

8. その経過時間すばらしいより 5 日でパージ ポリシーをオフ エンド ポイント設定して下さい。

- **Administration > アイデンティティ管理 > 設定 > エンド ポイント パージ**にナビゲート すればパージの下でルールは新しいものを作成します。
- **識別グループ詳細**ボックスの下で**エンド ポイント識別グループ > HotSpot_Endpoints を**選択して下さい
- **条件**の下で**新しい状態 (Advanced オプション**）を『Create』 をクリック して下さい。
- の下で属性を選択します *ENDPOINTPURGE* を選択して下さい*: ElapsedDays GREATERTHAN* 5 日

確認

使用例 1

1. ユーザはゲスト SSID に接続します。
2. 彼はブラウザを開き、HTTPトラフィックが生成されるとすぐ、ゲスト ポータルは表示されます。
3. ゲストユーザが AUP を認証し、受け入れれば、成功ページは表示されます。
4. 再認証 CoA は送信されます (クライアントに対して透過的)。
5. エンド ポイント セッションはネットワークへのフルアクセスと再認証されます。
6. どのそれに続くゲスト接続でもネットワークにアクセス権を得る前にゲスト認証を取得しなければなりません。

ISE RADIUS ライブ ログからのフロー:

使用例 2

1. ユーザはゲスト SSID に接続します。
2. 彼はブラウザを開き、HTTPトラフィックが生成されるとすぐ、ゲスト ポータルは表示されます。
3. ゲストユーザが AUP を認証し、受け入れれば、デバイスは登録されています。
4. 成功ページは表示され、再認証 CoA は送信されます (クライアントに対して透過的)。
5. エンド ポイント セッションはネットワークへのフルアクセスと再認証されます。
6. どのそれに続く突風接続 9s でもゲスト認証を実施しないで許しましたエンド ポイントが構成されたエンドポイント識別グループにそれでもある限り。

ISE RADIUS ライブ ログからのフロー:

使用例 3

1. ユーザはゲスト SSID に接続します。
2. 彼はブラウザを開き、HTTPトラフィックが生成されるとすぐ、AUP ページは表示されます。
3. ゲストユーザが AUP を受け入れれば、デバイスは登録されています。
4. 成功ページは表示され、Admin リセット CoA は送信されます（クライアントに対して透過的）。
5. エンド ポイントはネットワークにフルアクセスと再接続します。
6. どのそれに続く突風接続でも AUP 承認を（他では設定されなければ）のための実施しないで許可されますエンド ポイントが構成されたエンドポイント識別グループに残る限り。

AireOS の FlexConnect ローカル スイッチング

FlexConnect ローカル スイッチングが設定されるときネットワーク Admin はそれを確認する必要があります:

- リダイレクト ACL は FlexConnect ACL で設定されます。
- リダイレクト ACL は **FlexConnect** タブの下の AP 自体によるポリシーとしていずれにしても **> WebAuthentication 外部 ACL > ポリシー** > 選択し、リダイレクト ACL を『Apply』 をクリック します適用されました

または FlexConnect グループへポリシーを ACL は追加することによってに属します（**ワイヤレス > FlexConnect グループは >** 正しいグループ **> ACL マッピング > ポリシーを**選択し、リダイレクト ACL を『Add』 をクリック します選択します）

ポリシー ACL 付加は FlexConnect グループの AP メンバーに設定された ACL を押下げるために WLC を誘発します。 これをする失敗は Web リダイレクト問題という結果に終ります。

外部固定シナリオ

自動固定では（外部–固定）シナリオ次のファクトを強調表示することは重要です:

- リダイレクト ACL は外部および固定 WLC で定義される必要があります。 それが固定だけで実施される時でさえ。
- レイヤ2 認証は外部 WLC によって常に処理されます。 これはすべての RADIUS認証として設計フェーズの間に重要（またトラブルシューティングのために）であり、説明トラフィックは ISE と外部 WLC の間に発生します。

- リダイレクト AVP がクライアントセッションに適用されれば外部 WLC はモビリティ ハンドオフ メッセージを通して固定のクライアントセッションをアップデートします。
- この時点で固定 WLC は前もって構成されたリダイレクト ACL を使用してリダイレクトを実施し始めます。
- アカウンティングは固定 WLC SSID で完全に固定から来る ISE の方に（同じ認証イベントを参照する）両方行く説明更新を避けるために外部消し。
- URL によって基づく ACL は外部固定シナリオでサポートされません。

トラブルシューティング

AireOS およびコンバージしたアクセス両方 WLC のよくある壊された状態

1. **クライアントはゲスト SSID に加入することができません**

「**詳述されるクライアントを XX 表示して下さい: xx: xx: xx: xx: XX は**」クライアントが**開始**で接続されることを明らかにします。 通常これはその属性を適用することができない WLC のインジケータ AAAサーバ戻りです。

リダイレクト ACL 名前が ISE 一致によって WLC のあらかじめ定義された ACL の名前を丁度押したことを確認して下さい。

同じプリンシパルは WLC（VLAN ID、インターフェイス名、Airespace ACL、等）に押下げるために ISE を設定したという他のどの属性にも適用されます。 次にクライアントは DHCP および CENTRAL_WEB_AUTH にそれから移行する必要があります。

2. **リダイレクト AVP はクライアント セッションに適用されますが、リダイレクトははたらいていません**

リダイレクト ACL および URL リダイレクト属性がクライアント セッションに適用されることクライアントの Policy Manager 状態が SSID のための設定された動的インターフェイスに従って有効なIP アドレスの CENTRAL_WEB_AUTH であるまたことを確認すれば。

ACL をリダイレクトして下さい

AIreOS WLCs でリダイレクトは ACL あらゆるあらゆるトリガー リダイレクトされるべきトラフィックの他はっきりとリダイレクトするべきではない両方向および暗黙の deny IP の TCPポート 8443 の DNS および ISE のようなトラフィックを認める必要があります。

コンバージしたアクセスでロジックは反対です。 拒否 ACE バイパスは割り当て ACE がリダイレクトを誘発する間、リダイレクトします。 こういうわけでそれは割り当て TCPポート 80 および 443 に明示的に推奨されます。

ゲスト VLAN からのポート 8443 上の ISE へのアクセスを確認して下さい。 すべてが設定観点からよく検知 すれば進む最も簡単な方法はクライアントのワイヤレスアダプタの背後にあるキャプチャをつかみ、リダイレクトがどこに壊れるか確認することです。

- DNS resoultion は起こりますか。
- TCP 3 方法ハンドシェイクは要求されたページに対して終わりますか。
- WLC はクライアントの後でリダイレクト操作を始めます GET を戻しますか。
- 8443 上の ISE に対する TCP 3 方法ハンドシェイクは完了しますか。

3. **クライアントはゲスト フローの終わりに ISE の後でネットワークにアクセスすることが押しました VLANの変更をできません**

クライアントがフロー再認証しなさいゲスト認証が（ポスト CoA 起こった後） VLANの変更が押下げられれば（前にリダイレクト状態）の始めに IP アドレスをつかんだら、DHCP リリースを強制する唯一の方法はフローによってが Javaアプレットを通して（ポスチャ エージェントなしで）あるゲストで/更新しますモバイルデバイスではたらかせない。

これは VLAN Y.の IP アドレスを VLAN X でクライアントにブラックホール化される残します。 これはソリューションを計画している間考慮する必要があります。

4. **ISE はリダイレクトの間にゲスト クライアント ブラウザので「HTTP 500 Internal エラー、Radius セッション見つけられなかった」をメッセージ示します**

これは通常 ISE のセッション ロスのインジケータです（セッションは終了されました）。 これのためのもっとも一般的な原因は固定 WLC で外部固定が配置されたら設定しました説明してい

ます。 固定で説明するこのディセーブルを固定し、外部ハンドル認証および説明を残すため。

5.クライアント切断は切断されている残るか、または別の SSID に ISE のホットスポット ポータルの AUP を受け入れた後接続し。

これはそのこのフロー（リセットされる CoA Admin）に原因を関連する許可（CoA）のダイナミック変更によるホットスポットで WLC ワイヤレス ステーションに deauth を発行すると期待されるかもしれません。 非認証が起こったが、場合によってはクライアントが非authenitcate イベントに応じて別の好まれた SSID に接続する後ワイヤレス エンド ポイントの大半に SSID に戻る問題がありません。 オリジナル SSID にスタックするべき無線クライアントまで防ぐためにあるまたは別の利用可能な（好まれた） SSID にことができませんと同時に何も ISE か WLC からこれを接続するためにする。

この場合無線ユーザはホットスポット SSID に戻って手動で接続する必要があります。

AireOS WLC

(Cisco Controller) >debug client <MAC addr>
デバッグ クライアントはクライアント ステート マシン変更に関連する一組のコンポーネントをデバッグするために設定します。

(Cisco Controller) >debug client <MAC addr>
デバッグ AAA コンポーネント

(Cisco Controller) >debug client <MAC addr>
これは MAB か Dot1X SSID によって接続するユーザの量によって影響リソースであるかもしれません。 デバッグ レベルのこれらのコンポーネントは WLC と ISE 間の AAA トランザクションを記録し、画面で RADIUSパケットを印刷します。

これは ISE が期待された属性を提供しないかもしれないことまたは WLC がそれらを正しく処理しなければ重要です。

WebAuth リダイレクト

(Cisco Controller) >debug client <MAC addr>
これが WLC が正常にリダイレクトを引き起こして いることを確認するのに使用することができます。 これはリダイレクトがデバッグからのようにどのようにの見える必要があるか例です:

(Cisco Controller) >debug client <MAC addr>

NGWC

デバッグ クライアントはクライアント ステート マシン変更に関連する一組のコンポーネントをデバッグするために設定します。

(Cisco Controller) >debug client <MAC addr>
このコンポーネントは画面で RADIUSパケットを（認証およびアカウンティング）印刷します。

これは ISE は権限 AVP をまた CoA は正しく送信 されて、処理されていることを確認するために提供することを確認する必要があるとき便利であり。

```
(Cisco Controller) >debug client <MAC addr>
```

これは無線クライアントが複雑であるところすべての AAA 遷移 (認証、許可およびアカウンティング)。 これは WLC が AVP を正しく解析し、クライアントセッションに適用することを確認して重要です。

```
(Cisco Controller) >debug client <MAC addr>
```

これは NGWC のリダイレクト問題を疑うときイネーブルになったできます。

```
(Cisco Controller) >debug client <MAC addr>
```

ISE

RADIUS ライブ ログ

最初の MAB 要求が ISE で正しく処理され、その ISE が期待された属性を押し戻すことを確認して下さい。 **> ライブ ログはオペレーション > RADIUS** にナビゲート し、クライアントMAC を使用して**エンドポイントID** の下で出力をフィルタリングします。 認証イベントがあったら、受諾の一部として押される結果を『Details』 をクリック し、次に確認して下さい。

tcpdump

この機能は ISE と WLC 間の RADIUSパケット交換より深い調べが必要なとき使用することができます。 こうすれば ISE が WLC 側こととをのデバッグを有効に しないで access-accept の正しい属性を送信 すると証明できます。 **オペレーション**に TCDDump ナビゲートを使用しているキャプチャを開始するため **> 解決するため > 診察道具 >General ツール > TCPDump。**

これは TCPDump によってキャプチャされる正しいフローの例です

最初の MAB 要求 (上記のスクリーン ショットの第 2 パケット) に応じて送信 される AVP はここにあります。

```
(Cisco Controller) >debug client <MAC addr>
```

エンド ポイント デバッグ:

政策決定を含む ISE プロセスにより深い潜る必要があれば、門脈選択、ゲスト認証、CoA 処理、等はこれにアプローチする最も簡単な方法デバッグ レベルに完全なコンポーネントを設定しなければならないかわりに **Endpoit デバッグを**有効に することです。

これを、ナビゲート **オペレーション**に有効に するため **> > DiagnosticTools > 汎用ツール > エンド ポイント デバッグ解決します。**

エンド ポイント デバッグ ページで、エンド ポイント MAC アドレスを入力し、『Start』 をクリック して下さい問題を作り直すこと準備ができた場合。

デバッグが停止したらデバッグ 出力をダウンロードするためにエンドポイントID を識別するリンクをクリックして下さい。

関連情報

TAC 推薦する AireOS のビルド

Ciscoワイヤレス コントローラ設定ガイド、リリース 8.0。

Cisco Identity Services Engine 管理者ガイド、リリース 2.1

Identity Services Engine を搭載するユニバーサル NGWC ワイヤレス設定