WLAN コントローラでの Web 認証

目次

はじめに

このドキュメントでは、ワイヤレス LAN コントローラ（WLC）での Web 認証プロセスについて説明します。

前提条件

要件

WLC 設定に関する基本的な知識があることをお勧めします。

使用するコンポーネント

このドキュメントの情報は、すべての WLC ハードウェア モデルに基づいています。

本書の情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。稼働中のネットワークで作業を行う場合、コマンドの影響について十分に理解したうえで作業してください。

Web 認証の内部プロセス

Web 認証のセキュリティ機能としての位置付け

Web 認証（WebAuth）はレイヤ 3 セキュリティです。これは、ブラウザを実行する任意のステーションで機能する使いやすいセキュリティを提供します。また、事前共有キー（PSK）セキュリティ（レイヤ 2 セキュリティ ポリシー）と組み合わせることもできます。 ただし、WebAuth と PSK を組み合わせることはあまりなく、かえって使いづらくなる面もありますが、クライアントトラフィックを暗号化できるというメリットがあります。WebAuth は、暗号化のない認証方法です。

WLC Software リリース 7.4 を同時に設定できる場所にインストールするまで、WebAuth は 802.1x/RADIUS（リモート認証ダイヤルイン ユーザ サービス）と設定できません。ただし、クライアントは、dot1x と Web 認証の両方を実行する必要があります。ゲスト向けではなく、従業員向けのWebポータル（802.1xを使用するユーザ）を追加するためのものです。 従業員またはゲストの Web ポータルの dot1x に対するオールインワンの Service Set Identifier（SSID）はありません。

WebAuth の動作の仕組み

802.11 認証プロセスはオープンであるため、認証および関連付けを問題なく行うことができます。その後、関連付けられますが、WLC **RUN**状態ではありません。Web認証が有効になっている場合は、**WEBAUTH_REQD**のままになり、ネットワークリソースにアクセスできません（pingなし等）。 オプションでDNSサーバのアドレスを含むDHCP IPアドレスを受信する必要があります。

有効な URL をブラウザに入力する必要があります。クライアントは、DNS プロトコルを介して URL の名前解決を行います。次に、クライアントは、その HTTP 要求を Web サイトの IP アドレスに送信します。WLC は、その要求をインターセプトし、Web サイトの IP アドレスをスプーフする webauth ログイン ページを返します。外部 WebAuth の場合、WLC は、Web サイト IP アドレスを含む HTTP 応答を送信し、ページが移動されたことを示します。ページは、WLC により使用される外部 Web サーバに移動されます。認証されると、すべてのネットワーク リソースにアクセスできるようになり、デフォルトでは（WLC で強制リダイレクトが設定されていない場合）、要求された URL にリダイレクトされます。 要約すると、WLCではクライアントがDNSを解決し、IPアドレスを**WEBAUTH_REQD**状態で自動的に取得できます。

ヒント：WLCでポート80の代わりに別のポートを監視する場合は、**config network web-auth-port <port number>**を使用して、このポートでリダイレクトを作成することもできます。たとえば、ポート 2002 を使用する Access Control Server（ACS）Web インターフェイスやその他の同様のアプリケーションです。

HTTPSリダイレクションに関する注意:デフォルトでは、7.x以前のバージョンでは、WLCはHTTPSトラフィックをリダイレクトしませんでした。つまり、ブラウザを開いてHTTPSアドレスを入力しても、何も起こりません。HTTPSで提供されたログインページにリダイレクトするには、HTTPアドレスを入力する必要があります。

バージョン8.0以降では、CLIコマンド**config network web-auth https-redirect enable**を使用して、HTTPSトラフィックのリダイレクションを有効にできます。

多数のHTTPS要求が送信される場合、WLCではリソースが消費されることに注意してください。この機能のスケーラビリティが強化されたWLCバージョン8.7より前では、この機能を使用しないことをお勧めします。また、この場合、証明書警告は避けられないことに注意してください。実際、クライアントがURL(https://www.cisco.comなど)を要求しても、WLCは仮想インターフェイスのIPアドレスに対して発行された独自の証明書を提示します。これはクライアントが要求したURL/IPアドレスと一致せず、クライアントがブラウザで例外を強制しない限り、証明書は信頼されません。

8.7より前のWLCソフトウェアリリースのパフォーマンス低下を示す指標：

Web認証	**達成レート**
3 URL:HTTP	140/秒
1番目のURL:HTTP 2番目と3番目のURL - HTTPS	20/秒
3つのURL:HTTPS（大規模導入）	1/秒
3 URL:HTTPS（最大100クライアント）	10/秒

このパフォーマンステーブルでは、3つのURLは次のように呼ばれます。

- エンドユーザが入力した元のURL（ユーザが参照するWebサイト）
- WLCがブラウザを
- 最終クレデンシャルの送信

パフォーマンステーブルは、3つのURLがすべてHTTPの場合、3つのURLがすべてHTTPSの場合、またはクライアントがHTTPからHTTPSに移動する場合（より一般的なシナリオ）にWLCのパフォーマンスを示します。

内部ページで内部（ローカル）WebAuth を動作させる方法

動作中のダイナミック インターフェイスで WLAN を設定する必要がある場合、クライアントは、DHCP を介して DNS サーバ IP アドレスを受信する必要もあります。任意の webauth を設定する前に、WLAN が正しく機能し、DNS 要求（nslookup）の名前解決を行うことができ、Web ページを表示できることをテストしておく必要があります。これで、Web 認証をレイヤ 3 セキュリティ機能として設定できます。たとえば、ローカル データベースまたは外部 RADIUS サーバでユーザを作成できます。詳細については、「ワイヤレス LAN コントローラ（WLC）上の Web 認証の設定例」を参照してください。

カスタム ページでカスタムのローカル WebAuth を設定する方法

カスタム **webauth** は、[Security] タブから **redirectUrl** を使用して設定できます。これにより、入力する特定の Web ページに強制的にリダイレクトされます。ユーザが認証されると、クライアントが要求したオリジナル URL がオーバーライドされ、リダイレクトが割り当てられているページが表示されます。

カスタム機能を使用すると、デフォルトのログイン ページではなく、カスタム HTML ページを使用できます。HTML およびイメージ ファイル バンドルがコントローラにアップロードされます。アップロード ページで、tar 形式の webauth バンドルを探します。通常、PicoZip により、WLC の互換性がある tar が作成されます。WebAuth バンドルの例については、「ワイヤレス コントローラ WebAuth バンドルのソフトウェアのダウンロード」ページを参照してください。WLC に適したリリースを選択する必要があります。既存のバンドルをカスタマイズすることをお勧めします。バンドルを最初から作成しないでください。

バージョンやバグにより異なりますが、**カスタム webauth** にはいくつかの制限事項があります。これを次に示します。

- .tarファイルサイズ（5 MB以下）
- .tar のファイル数
- ファイルのファイル名の長さ（30 文字以内）

カスタマー パッケージが機能しない場合、シンプル カスタム パッケージを使用してみてください。次に、機能しなかったカスタマー パッケージに合わせて、ファイル数や設定などを徐々に変更します。これは、問題の特定に役立ちます。カスタム ページを設定する方法については、『シスコ ワイヤレス LAN コントローラ設定ガイド リリース 7.0』の「カスタマイズされた Web 認証ログイン ページの作成」を参照してください。

グローバル設定をオーバーライドする手法

各 WLAN を **override global config** コマンドで設定して、各 WLAN の WebAuth タイプを設定します。つまり、別の WLAN のカスタム内部/デフォルト WebAuth で内部/デフォルト WebAuth を使用できます。これにより、WLAN ごとに異なるカスタム ページを設定できます。同じバンドルのすべてのページを組み合わせ、WLC にアップロードする必要があります。次に、各 WLAN で override global config コマンドを使用してカスタム ページを設定し、バンドル内のすべてのファイルからログイン ページとして使用するファイルを選択できます。各 WLAN で、バンドル内の異なるログイン ページを選択できます。

リダイレクションの問題

HTML バンドルには、リダイレクションを可能にする変数があります。ここに強制リダイレクション URL を含めないでください。カスタム WebAuth でリダイレクション問題が発生した場合、バンドルをチェックすることをお勧めします。WLC GUI に += を使用するリダイレクト URL を入力すると、バンドル内で定義されている URL でオーバーライドされるか、これに追加されます。たとえば、WLC GUI で、[redirectURL] フィールドに www.cisco.com を設定します。バンドルでは、次のように表示されます。redirectURL+='www.google.com'。 **+=** は、無効な URL である www.cisco.comwww.google.com にユーザをリダイレクトします。

外部ページで外部（ローカル）Web 認証を動作させる方法

すでに簡単に説明したように、外部 WebAuth サーバは、ログイン ページの外部リポジトリです。ユーザ クレデンシャルは、WLC により認証されます。外部 Web サーバでは、特定または異なるログイン ページを使用が許可されるだけです。次に、外部 WebAuth で実行されるステップを示します。

1. クライアント（エンド ユーザ）が Web ブラウザを開き、URL を入力します。

2. このクライアントが認証されず、外部 Web 認証が使用される場合、WLC は、このユーザを外部 Web サーバ URL にリダイレクトします。つまり、WLC は、Web サイトのスプーフ IP アドレスで HTTP リダイレクトをクライアントに送信し、外部サーバ IP アドレスを示します。外部 Web 認証ログイン URL には、カスタマーがスイッチ Web サーバへの問い合わせに必要な AP_Mac_Address、client_url（www.website.com）、action_URL などのパラメータが付加されます。

3. 外部 Web サーバ URL は、ユーザをログイン ページに送信します。次に、ユーザは、事前認証アクセス コントロール リスト（ACL）を使用して、サーバにアクセスできます。ACLは、4400シリーズとWism1を除くすべてのWLCモデルに必要です。

4. ログイン ページはユーザ クレデンシャルの入力を受け取り、WLC Web サーバの **action_URL**（http://192.0.2.1/login.html など）に要求を送信して戻します。これが入力パラメータとしてカスタマーのリダイレクト URL に提供されます。ここで、192.0.2.1 は、スイッチの仮想インターフェイス アドレスです。

5. WLC Web サーバは、認証のためにユーザ名とパスワードを送信します。

6. WLC は RADIUS サーバ要求を開始するか、WLC 上のローカル データベースを使用してユーザを認証します。

7. 認証が成功した場合、WLC Web サーバは、設定されたリダイレクト URL またはクライアントが入力した URL にユーザを転送します。

8. 認証が失敗した場合、WLC Web サーバはカスタマー ログイン URL にユーザをリダイレクトして戻します。

   注：このドキュメントでは、仮想IPの例として192.0.2.1を使用します。192.0.2.xの範囲はルーティング不能であるため、仮想IPに使用することを推奨します。古いドキュメントでは、「1.1.1.x」を参照することもあれば、これがデフォルト設定として使用されているWLCで設定されているものもあります。ただし、このIPはルーティング可能な有効なIPアドレスであるため、代わりに192.0.2.xサブネットが推奨されます。

注：アクセスポイント(AP)がFlexConnectモードの場合、**事前認証**ACLは関係ありません。認証されないクライアントに Web サーバへのアクセスを許可するには、Flex ACL を使用できます。「ワイヤレス LAN コントローラを使用した外部 Web 認証の設定例」を参照してください。

Web パススルー

これは、内部 Web 認証の一種です。Web パススルーでは、警告またはアラート ステートメントを示すページが表示され、クレデンシャル プロンプトは表示されません。ユーザは、[ok] をクリックします。E メール入力を有効にできるので、ユーザは E メール アドレスを入力できます。この E メールはユーザ名として使用されます。ユーザが接続されると、アクティブ クライアント リストがチェックされます。ユーザ名として入力された E メール アドレスでユーザがリストされているか確認されます。詳細については、「Wireless LAN Controller Web Passthrough Configuration Example」を参照してください。

条件付き Web リダイレクト

条件付き Web リダイレクトを有効にすると、802.1X 認証が正常に完了した後に、ユーザは条件付きで特定の Web ページにリダイレクトされます。リダイレクト ページ、および、RADIUS サーバでリダイレクトを実行する条件を指定できます。条件には、有効期限に達した場合やユーザが使用/アクセスを継続するための料金を支払う必要がある場合に使用されるユーザ パスワードを含めることができます。RADIUS サーバから Cisco AV ペア url-redirect が返された場合、ユーザがブラウザを開くと、指定された URL にリダイレクトされます。さらにサーバから Cisco AV ペア url-redirect-acl も返された場合は、指定された ACL が、そのクライアントの事前認証 ACL としてインストールされます。クライアントはこの時点で完全に認証されていないと見なされ、事前認証 ACL によって許可されるトラフィックのみを送信できます。指定されている URL でクライアントが特定の操作 (パスワードの変更や料金の支払いなど) を完了した後で、クライアントは再度認証を行う必要があります。RADIUS サーバから url-redirect が返されない場合、クライアントは完全に認証されたものと見なされ、トラフィックを渡すことを許可されます。

注：条件付きWebリダイレクト機能は、802.1xまたはWPA+WPA2レイヤ2セキュリティ用に設定されたWLANでのみ使用できます。

RADIUS サーバを設定した後は、コントローラ GUI または CLI のいずれかを使用して、コントローラ上で条件付き Web リダイレクトを設定できます。次の詳細手順を示したガイドを参照してください。「GUI を使用して Web リダイレクトを設定」および「CLI を使用して Web リダイレクトを設定」。

スプラッシュ ページ Web リダイレクト

スプラッシュ ページ Web リダイレクトを有効にすると、802.1X 認証が正常に完了した後に、ユーザは特定の Web ページにリダイレクトされます。ユーザは、リダイレクト後、ネットワークにフル アクセスできます。RADIUS サーバでリダイレクト ページを指定できます。RADIUS サーバから Cisco AV ペア url-redirect が返された場合、ユーザがブラウザを開くと、指定された URL にリダイレクトされます。クライアントは、この段階で完全に認証され、RADIUS サーバが url-redirect を返さなくても、トラフィックを渡すことができます。

注：スプラッシュページWebリダイレクト機能は、802.1xまたはWPA+WPA2レイヤ2セキュリティ用に設定されたWLANでのみ使用できます。

RADIUS サーバを設定した後は、コントローラ GUI または CLI のいずれかを使用して、コントローラ上でスプラッシュ ページ Web リダイレクトを設定できます。

MAC フィルタ失敗時の WebAuth

レイヤ 2 セキュリティ メニューで MAC フィルタを設定する必要があります。ユーザが MAC アドレスで正常に検証されると、直接 run 状態に移行します。これに失敗すると、WEBAUTH_REQD 状態に移行し、通常の Web 認証が発生します。

注：これは、Webパススルーではサポートされていません。詳細については、機能拡張要求に関するアクティビティCSCtw73512 .

中央 Web 認証

中央 Web 認証は、WLC がサービスをホストしない状況で使用されます。これらの違いは、クライアントが ISE Web ポータルに送信され、WLC の 192.0.2.1 を介さないということです。ログイン ページおよびポータル全体は外部に配置されます。

中央 Web 認証は、RADIUS ネットワーク アドミッション コントロール（NAC）を WLAN の詳細設定で有効にし、MAC フィルタを有効にしている場合に発生します。

全体的な概念としては、WLC は、RADIUS 認証（通常は MAC フィルタ用）を ISE に送信し、ISE は、**redirect-url** 属性値（AV）ペアで応答します。次に、ISE が認可変更（CoA）要求で許可するまで、ユーザは POSTURE_REQD 状態になります。同様のことは、Posture または Central WebAuth でも発生します。中央 WebAuth は、WPA-Enterprise/802.1x には対応しません。これは、拡張認証プロトコル（EAP）の場合のようにゲスト ポータルが暗号化キーのセッションキーを返すことができないためです。

外部ユーザ認証（RADIUS）

これは、WLC がクレデンシャルを処理する場合、またはレイヤ 3 Web ポリシーが有効な場合のみローカル WebAuth で有効です。ユーザは、WLC でローカルに、または RADIUS を介して外部的に認証できます。

WLC は次の順にユーザのクレデンシャルをチェックします。

1. いずれの場合でも、独自のデータベースが参照されます。
2. そこでユーザが見つからない場合、ゲスト WLAN で設定されている RADIUS サーバがチェックされます。
3. 次に、グローバル RADIUS サーバで、**ネットワーク ユーザ**がチェックされる RADIUS サーバがチェックされます。

この 3 番目のポイントは非常に重要で、WLAN の RADIUS を設定しない場合に通常行われますが、ユーザがコントローラで見つからない場合でも、RADIUS でチェックされるので注意してください。これは、ネットワーク ユーザがグローバル リストの RADIUS サーバでチェックされるためです。

WLC は、パスワード認証プロトコル（PAP）、チャレンジ ハンドシェイク認証プロトコル（CHAP）または EAP-MD5（メッセージ ダイジェスト 5）でユーザを RADIUS サーバに認証できます。 これは、グローバル パラメータで、GUI または CLI から設定できます。

GUI から：[Controller] [Web RADIUS Authentication] に移動します。

CLI から：config custom-web RADIUSauth <pap|chap|md5chap>

注：NACゲストサーバはPAPのみを使用します。

有線ゲスト WLAN の設定方法

設定は簡単で、ワイヤレス ゲスト設定とほぼ同じです。設定には、1 つまたは 2 つのコントローラを使用できます（一方がオートアンカーの場合のみ）。

有線ゲストユーザを配置するVLANとして、たとえばVLAN 50上のVLANを選択します。有線ゲストがインターネットにアクセスする場合は、VLAN 50に設定されたスイッチ上のポートにラップトップを接続します。このVLAN 50が許可され、WLCトランクポートを経由の経由ので2 つの

WLC（アンカーと外部）を使用する場合、この有線ゲスト VLAN は、アンカーではなく、外部 WLC（WLC1）に接続する必要があります。その後、WLC1はDMZ WLC（アンカー、名前 WLC2）へのトラフィックのトンネリングを処理し、ルーテッドネットワークのトラフィックを解放します。

次に、有線ゲスト ユーザ アクセスを設定する 5 つのステップを示します。

1. **有線ゲスト ユーザ アクセス用の動的インターフェイス（VLAN）を設定します。**

   WLC1で、ダイナミックインターフェイスVLAN50を作成します。**インターフェイス設定**ページで、[**ゲストLAN**]ボックスをオンにします。次に、[IP address] および [gateway] などのフィールドが非表示になります。WLCがこのインターフェイスについて認識する必要があるのは、トラフィックがVLAN 50からルーティングされることだけです。これらのクライアントは有線ゲストです。

2. **ゲスト ユーザ アクセス用の有線 LAN を作成します。**

   コントローラで、インターフェイスは、WLAN に関連付けられる場合に使用されます。ここでは、本社コントローラで WLAN を作成します。[WLANs] に移動し、[New] をクリックします。[WLAN Type] で [Guest LAN] を選択します。

   [Profile Name] および [WLAN SSID] で、この WLAN を識別する名前を入力します。これらの名前を変更できますが、スペースを含めることはできません。WLAN という名前が使用されますが、このネットワーク プロファイルはワイヤレス ネットワーク プロファイルには関連しません。

   [General] タブは、次の 2 つのドロップダウン リストを提供します。[Ingress] および [Egress]。[Ingress] は、ユーザが送信される VLAN です（VLAN 50）。[Egress] は、ユーザの送信先の VLAN です。

   [Ingress] では、[VLAN50] を選択します。

   [Egress] の VLAN は異なります。使用するコントローラが 1 つだけの場合、別の動的インターフェイス（ここでは標準（ゲスト LAN ではありません））を作成する必要があります。有線ユーザはこのインターフェイスに送信されます。この場合、DMZ コントローラに送信します。そのため、[Egress] インターフェイスでは、[Management Interface] を選択します。

   このゲスト LAN「WLAN」の**セキュリティ** モードは WebAuth です。これは許容範囲です。[OK] をクリックして検証します。

3. **外部コントローラ（本社）を設定します。**

   [WLAN list] から、[Guest LAN] 行の最後にある [Mobility Anchor] をクリックして、DMZ コントローラを選択します。ここでは、両方のコントローラがお互いを認識していることを前提としています。お互いが認識されていない場合は、[Controller] > [Mobility Management] > [Mobility group] に移動し、WLC1にDMZWLCを追加します。次に、DMZに**WLC1**を追加します。コントローラは、それぞれ異なるモビリティ グループにある必要があります。同じ場

合、基本セキュリティ規則に違反します。

4. **アンカー コントローラ（DMZ コントローラ）を設定します。**

   本社コントローラの準備は完了しています。DMZ コントローラを準備する必要があります。DMZ コントローラに Web ブラウザ セッションを開き、[WLANs] に移動します。新規 WLAN を作成してください。[WLAN Type] で [Guest LAN] を選択します。

   [Profile Name] および [WLAN SSID] で、この WLAN を識別する名前を入力します。本社コントローラと同じ値を入力します。

   [Ingress] インターフェイスは、[None] です。ただし、トラフィックは Ethernet over IP（EoIP）トンネルを介して受信されるので、これは重要ではありません。そのため、入力インターフェイスは指定する必要はありません。

   [Egress] インターフェイスは、クライアント送信に使用されるインターフェイスです。たとえば、**DMZ VLAN**はVLAN 9です。DMZWLCでVLAN 9の標準ダイナミックインターフェイスを作成し、出力インターフェイスとして**VLAN 9**を選択します。

   モビリティ アンカー トンネルの終端を設定する必要があります。[WLAN list] から、[Mobility Anchor for Guest LAN] を選択します。トラフィックをローカル コントローラ DMZWLC に送信します。これで、両端の準備ができました。

5. **ゲスト LAN を調整します。**

   両端の WLAN 設定を調整することもできます。ただし、設定は両端で同じにする必要があります。たとえば、[WLAN Advanced] タブで、WLC1 の [Allow AAA override] をクリックした場合、DMZWLC でも同じチェックボックスをオンにする必要があります。いずれかの WLAN の選択が異なる場合、トンネルは切断されます。DMZWLC はトラフィックを拒否します。debug mobility を実行すると確認できます。

   すべての値は、実際には DMZWLC から取得されます。たとえば、IP アドレスや VLAN 値などです。WLC1 側を個別に設定し、要求を WLCDMZ にリレーします。

ログイン ページ用の証明書

このセクションでは、WebAuth ページで独自の証明書を使用する場合、または 192.0.2.1 WebAuth URL を表示せず、指定 URL を表示する場合に必要なプロセスについて説明します。

コントローラの Web 認証用の証明書のアップロード

GUI（[WebAuth] [Certificate]）または CLI（転送タイプ webauthcert）を介して、証明書をコントローラにアップロードできます。認証局（CA）で作成した証明書でも、サードパーティの公式証明書でも、.pem 形式でなければなりません。送信前に、証明書のキーを入力する必要もあります。

アップロード後、証明書を有効にするには、リブートする必要があります。リブート後、GUI の WebAuth 証明書ページに移動すると、アップロードした証明書の詳細（有効期間など）が示され

ます。 重要なフィールドは、証明書に発行される名前である、Common Name（CN）です。このフィールドについては、このドキュメントの「コントローラ上の認証局などの証明書」セクションで説明します。

リブートして、証明書の詳細を確認すると、WebAuth のログイン ページで新しいコントローラ証明書が提供されます。ただし、次の 2 つの状況が発生します。

1. 証明書の発行元が、確実に信頼できる主要ルート CA のいずれかである場合は問題ありません。たとえば、VeriSign です。ただし、通常、Verisign サブ CA や非ルート CA により署名されます。記載されている CA が信頼できるかどうかは、ブラウザで証明書ストアをチェックできます。

2. 小規模な企業/CA から取得した証明書は、すべてのコンピュータで信頼されません。企業/CA 証明書をクライアントに提供し、可能であれば、いずれかのルート CA がその証明書を発行します。最後に、「Certificate has been ised by CA x > CA x certificate has been issued by CA y > CA y certificate has been issued by this trusted root CA」などのチェーンが表示されます。 最終的には、クライアントが信頼する CA に到達します。

コントローラ上の認証局などの証明書

「this certificate is not trusted」という警告を削除するには、コントローラのコントローラ証明書を発行したCAの証明書も入力する必要があります。次に、コントローラは、両方の証明書（コントローラの証明書および CA 証明書）を提供します。 CA 証明書は、信頼できる CA であるか、CA を確認できるリソースが必要です。信頼できる CA に送信される CA 証明書のチェーンを構築できます。

チェーン全体を同じファイルに保存する必要があります。つまり、ファイルには、次のような内容が含まれます。

```
BEGIN CERTIFICATE ------ device certificate*   END CERTIFICATE ------ BEGIN
CERTIFICATE ------ intermediate CA certificate* END CERTIFICATE ------ BEGIN
CERTIFICATE ------ Root CA certificate* END CERTIFICATE ------
```

証明書を URL に一致させる方法

WebAuth URL は自身を認証するために 192.0.2.1 に設定され、証明書が発行されます（これは、WLC 証明書の CN フィールドです）。 たとえば、WebAuth URLを「myWLC.com」に変更する場合は、**仮想インターフェイス設定**(192.0.2.1インターフェイス)に移動し、仮想DNSホスト名（myWLC.comなど）を入力できます。これにより、URL バーの 192.0.2.1 が置換されます。この名前は解決できる必要があります。スニファ トレースは、どのように機能するかを示しますが、WLC がログイン ページを送信すると、WLC は myWLC.com アドレスを示し、クライアントはその DNS で名前を解決します。この名前は192.0.2.1として解決する必要があります。つまり、WLCの管理に名前を使用する場合は、WebAuthに別の名前を使用する必要があります。つまり、WLC 管理 IP アドレスにマッピングされる myWLC.com を使用する場合、myWLCwebauth.com など、WebAuth に別の名前を使用する必要があります。

証明書の問題のトラブルシューティング

このセクションでは、証明書問題をトラブルシューティングの確認方法および確認内容について説明します。

確認方法

OpenSSL (Windows の場合 OpenSSL Win32 を検索) をダウンロードして、インストールできます。この URL が、WebAuth ページが DNS でリンクされている URL である場合、設定を行わずに、bin ディレクトリに移動して、openssl s_client –connect www.mywebauthpage.com:443 を使用できます。この例については、このドキュメントの「確認内容」セクションを参照してください。

証明書でプライベートCAを使用する場合は、ローカルマシンのディレクトリにルートCA証明書を配置し、openssslオプション**-CApath**を使用する必要があります。中間CAがある場合は、同じディレクトリに配置する必要があります。

証明書に関する一般的な情報を取得して確認するには、次のコマンドを使用します。

```
openssl x509 -in certificate.pem -noout -text
openssl verify certificate.pem
```

openssl:

```
openssl x509 -in certificate.der -inform DER -outform PEM -out certificate.pem
```

確認内容

接続時にクライアントに送信される証明書を確認できます。デバイス証明書を確認します。CN は、Web ページが到達できる URL である必要があります。デバイス証明書の「issued by」行を参照します。これは、セカンド証明書の CN と一致する必要があります。また、このセカンド証明書の「issued by」は次の証明書の CN と一致する必要があり、これ以降も証明書の「issued by」と次の証明書の CN が一致する必要があります。一致しない場合、チェーンは確立されません。ここで示される OpenSSL 出力では、openssl でデバイス証明書を確認できないことがわかります。これは、「issued by」が、提供された CA 証明書の名前と一致しないためです。

SSL の出力

```
Loading 'screen' into random state - done CONNECTED(00000760) depth=0 /O=
<company>.ac.uk/OU=Domain Control Validated/CN=<company>.ac.uk verify error:
num=20:unable to get local issuer certificate verify return:1 depth=0 /O=
<company>.ac.uk/OU=Domain Control Validated/CN=<company>.ac.uk verify error:
num=27:certificate not trusted verify return:1 depth=0 /O=<company>.ac.uk/OU=
Domain Control Validated/CN=<company>.ac.uk verify error:num=21:
unable to verify the first certificate verify return:1 --- Certificate chain
0 s:/O=<company>.ac.uk/OU=
Domain Control Validated/CN=<company>.ac.uki:/C=US/ ST=
Arizona/L=Scottsdale/O=.com/OU=http://certificates.gocompany.com/repository/CN=
Secure Certification Authority/serialNumber=079
692871 s:/C=US/O=Company/OU=Class 2 Certification Authority
i:/C=US/O=Company/OU=Class 2 Certification Authority --- Server certificate

BEGIN CERTIFICATE-----
MIIE/zCCA+egAwIBAgIDRc2iMA0GCSqGSIb3DQEBBQUAMIHKMQswCQYDVQQGEwJV
output cut*
YMaj/NACviEU9J3iot4sfreCQSKkBmjH0kf/Dg1l0kmdSbc=

END CERTIFICATE-----
subject=/O=<company>.ac.uk/OU=Domain Control Validated/CN=<company>c.ac.uk
issuer=/C=US/ST=Arizona/L=Scottsdale/O=.com/OU=http://certificates.
```

```
.com/repository/CN=Secure Certification Authority/serialNumber=0
7969287 --- No client certificate CA names sent --- SSL handshake has read
2476 bytes and written 322 bytes --- New, TLSv1/SSLv3, Cipher is AES256-SHA
Server public key is 1024 bit Compression: NONE Expansion: NONE SSL-Session:

Protocol : TLSv1
Cipher : AES256-SHA
Session-ID: A32DB00A7AB7CD1CEF683980F3696C2BBA31A1453324F711F50EF4B86A4A7F03

Session-ID-ctx:Master-Key: C95E1BDAC7B1A964ED7324955C985CAF186B92EA34CD69E10
5F95D969D557E19
939C6A77C72350AB099B3736D168AB22

Key-Arg : None
Start Time: 1220282986
Timeout : 300 (sec)
Verify return code: 21 (unable to verify the first certificate)
---
```

また、証明書をコントローラにアップロードできないという問題が発生する可能性があります。この場合、有効期間、CA などは問題ではありません。これを確認するには、最初に、トリビアル ファイル転送プロトコル (TFTP) 接続を確認し、構成ファイルを転送します。次に、debug transfer all enable コマンドを入力すると、証明書のインストールが問題であることがわかります。この原因は、証明書で使用されるキーが正しくないことが考えられます。また、証明書のフォーマットが正しくない、または壊れていることも考えられます。

証明書の内容を確実に有効な証明書と比較することをお勧めします。これにより、LocalkeyID 属性ですべての 0 (発生済み) が表示されるか確認できます。 この場合、証明書を再変換する必要があります。OpenSSL では、.pem から .p12 に変換し、目的のキーで .pem を再発行できる 2 つのコマンドがあります。

準備：証明書とキーを含む .pem を受け取った場合、キーの部分をコピー/ペーストします。---- BEGIN KEY ---- until ------- END KEY ------ を .pem から「key.pem」にコピー/ペーストします。

1. **openssl pkcs12 -export -in certificate.pem -inkey key.pem -out newcert.p12**?キーが表示されます。check123 と入力します。

2. **openssl pkcs12 -in newcert.p12 -out workingnewcert.pem -passin pass:check123 -passout pass:check123**：これにより、パスワード **check123** で .pem を使用できます。

トラブルシューティングを行うその他の状況

このドキュメントでは**モビリティ アンカー**については説明していませんが、**アンカー ゲスト**の場合、モビリティ エクスチェンジが正しく発生し、クライアントがアンカーに到達することを確認します。WebAuth 問題が発生した場合、アンカーでトラブルシューティングを行う必要があります。

次に、トラブルシューティングできる一般的な問題をいくつか示します。

- **ユーザをゲスト WLAN に関連付けることができない。**

  これは、WebAuth に関連するものです。クライアント設定、WLAN のセキュリティ設定、これが有効にされているかどうか、無線がアクティブで機能しているかどうかなどを確認します。

- **ユーザが IP アドレスを取得できない。**

  ゲスト アンカーの場合、これは多くの場合、外部およびアンカーが同じ方法で設定されていない場合に発生します。それ以外の場合、DHCP 設定や接続などを確認します。他の WLAN が同じ DHCP サーバを正常に使用できるかどうかを確認します。これは、WebAuth とは関係ありません。

- **ユーザがログイン ページにリダイレクトされない。**

  これは、一般的な症状ですが、より正確に説明します。この問題が発生する状況は次の 2 つあります。

  ユーザがリダイレクトされない（ユーザが URL を入力しても、WebAuth ページにアクセスできない）。 この場合、次のことを確認します。

  有効な DNS サーバが DHCP（**ipconfig /all**）を介してクライアントに割り当てられている。

  クライアント(**nslookup** www.website.com)からDNSに到達できることを確認します。

  リダイレクトされる有効な URL をユーザが入力している。

  ユーザがポート 80 の HTTP URL にアクセスしている（たとえば、http://localhost:2002 で ACS にアクセスするには、ポート 2002 ではなくポート 80 に送信されるまでリダイレクトされません）。

  ユーザは、192.0.2.1 に正しくリダイレクトされるが、ページ自体が表示されない。

  これは、通常、WLC 問題（バグ）またはクライアント側の問題です。クライアントがいくつかのファイアウォールまたはブロッキング ソフトウェアまたはポリシーを使用している可能性があります。また、Web ブラウザでプロキシを設定している可能性もあります。

  推奨事項：スニファ トレースをクライアント PC で使用します。ワイヤレス アダプタで実行し、WLC が応答しリダイレクトするか示す Wireshark 以外、特殊なワイヤレス ソフトウェアは必要ありません。この問題には 2 つの原因が考えられます。WLC から応答がないか、WebAuth ページの SSL ハンドシェイクに問題があるかのいずれかです。SSL ハンドシェイク問題については、ユーザ ブラウザで SSLv3 が許可されているかどうか（一部では SSLv2 のみ許可）、また証明書検証での頻度を確認できます。

  共通して、DNS なしで Web ページが表示されるかどうかを確認するには、http://192.0.2.1 を手動で入力します。実際、http://6.6.6.6 を入力しても効果は同じです。WLC は、入力された IP アドレスをリダイレクトします。そのため、http://192.0.2.1 と入力しても、Web リダイレクションは回避されません。https:// 192.0.2.1(secure)と入力すると、WLCがHTTPSトラフィックをリダイレクトしないため、これは機能しません（デフォルトでは、バージョン 8.0以降では実際に可能です）。 リダイレクトせずにページを直接ロードする最良の方法は、https://192.0.2.1/login.html を入力することです。

- **ユーザが認証できない。**

このドキュメントで認証について説明しているセクションを参照してください。RADIUS でローカルにクレデンシャルを確認します。

- **ユーザが WebAuth を介して正常に認証できるが、その後インターネットにアクセスできない**。

  WLAN のセキュリティから WebAuth を削除し、オープン WLAN を使用する必要があります。次に、Web や DNS などにアクセスできます。ここでも問題が発生する場合、WebAuth 設定も削除して、インターフェイス設定を確認します。

詳細については、次のサイトを参照してください。「ワイヤレス LAN コントローラ（WLC）上の Web 認証のトラブルシューティング」

HTTP プロキシ サーバとその動作方法

HTTP プロキシ サーバを使用できます。192.0.2.1 がプロキシ サーバを通過しない例外をクライアントのブラウザに追加する必要がある場合、プロキシ サーバのポート（通常は 8080）で HTTP トラフィックに対する WLC リッスンを作成できます。

この状況を理解するには、HTTP プロキシの動作を認識する必要があります。これは、ブラウザでのクライアント側の設定内容（IP アドレスおよびポート）です。

ユーザが Web サイトにアクセスする場合、通常、DNS で名前が IP に解決され、Web ページから Web サーバに要求されます。このプロセスは、常に、ページの HTTP 要求をプロキシに送信します。プロキシは、必要に応じて DNS を処理し、Web サーバに転送します（ページがプロキシでキャッシュされていない場合）。 記述は、クライアントとプロキシ間のみです。プロキシが実際の Web ページを取得するかどうかは、クライアントとは関係ありません。

次に、Web 認証プロセスを示します。

- ユーザが URL を入力します。
- クライアント PC がプロキシ サーバに送信します。
- WLC がインターセプトし、プロキシ サーバ IP をスプーフします。192.0.2.1へのリダイレクトでPCに応答する

この段階で、PC が設定されていない場合、プロキシに 192.0.2.1 WebAuth ページが要求されるので、機能しません。PC は、192.0.2.1 例外を作成する必要があります。次に、HTTP 要求を 192.0.2.1 に送信し、WebAuth に進みます。認証されると、すべての通信が再びプロキシを通過します。例外設定は、通常、プロキシ サーバの設定同様、ブラウザにあります。次のメッセージが表示されます。「Don't use proxy for those IP addresses」

WLC リリース 7.0 以降の場合、**webauth proxy redirect** は、グローバル WLC 設定オプションで有効にできます。有効にされると、WLC は、クライアントがプロキシを手動で使用するように設定されているか確認します。この場合、クライアントは、正常に機能するようにプロキシ設定を変更する方法を示すページにリダイレクトされます。WebAuth プロキシ リダイレクトは、さまざまなポートで機能するように設定でき、中央 Web 認証に対応します。

WebAuth プロキシ リダイレクションの例については、「Web Authentication Proxy on a Wireless LAN Controller Configuration Example」を参照してください。

HTTPS ではなく HTTP での Web 認証

HTTPS ではなく HTTP で Web 認証にログインできます。HTTP でログインする場合、証明書アラートは受け取りません。

WLC リリース 7.2 よりも前のコードでは、WLC の HTTPS 管理を無効にし、HTTP 管理をそのままにしておく必要があります。ただし、この場合、HTTP を介した WLC の Web 管理だけが許可されます。

WLC リリース 7.2 のコードでは、**config network web-auth secureweb disable** コマンドを使用して無効にします。この場合、管理ではなく、Web 認証の HTTPS だけが無効になります。これにはコントローラのリブートが必要です。

WLC リリース 7.3 以降のコードでは、GUI および CLI を介してのみ WebAuth の HTTPS を有効/無効にできます。

関連情報

- ワイヤレス LAN コントローラの Web 認証の設定例
- ワイヤレス コントローラ WebAuth バンドルのソフトウェアのダウンロード
- カスタマイズされた Web 認証ログイン ページの作成
- ワイヤレス LAN コントローラを使用した外部 Web 認証の設定例
- ワイヤレス LAN コントローラの Web パススルーの設定例
- GUI を使用した Web リダイレクトの設定
- CLI を使用した Web リダイレクトの設定
- ワイヤレス LAN コントローラ (WLC) 上の Web 認証のトラブルシューティング
- ワイヤレス LAN コントローラ上の Web 認証プロキシの設定例
- Requests for Comments (RFC)
- テクニカル サポートとドキュメント – Cisco Systems