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

目次

概要

このドキュメントは、WLC 環境の Web 認証問題のトラブルシューティングに役立つヒントについて説明します。

前提条件

要件

次の項目に関する知識が推奨されます。

- コントロールのナレッジおよびワイヤレスアクセスポイント（CAPWAP）のプロビジョニング。
- Lightweight アクセスポイント（LAP）および基本動作のための WLC を設定する方法のナレッジ。
- Web 認証の基本的な知識および WLCs の Web 認証を設定する方法を。 WLCs の Web 認証を設定する方法の情報に関してはワイヤレス LAN コントローラ Web 認証の設定例を参照して下さい。

使用するコンポーネント

この資料に記載されている情報はファームウェア バージョン 8.3.121 を実行する WLC 5500 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。

関連製品

この資料もこのハードウェアによって使用することができます:

- Cisco 5500 シリーズ ワイヤレス コントローラ
- Cisco 8500 シリーズ ワイヤレス コントローラ
- Cisco 2500 シリーズ ワイヤレス コントローラ
- Cisco Airespace 3500 シリーズ WLAN コントローラ
- Cisco Airespace 4000 シリーズ ワイヤレス LAN コントローラ
- Cisco Flex 7500 シリーズ Wireless Controller
- Cisco Wireless Services Module 2（WiSM2）

WLC での Web 認証

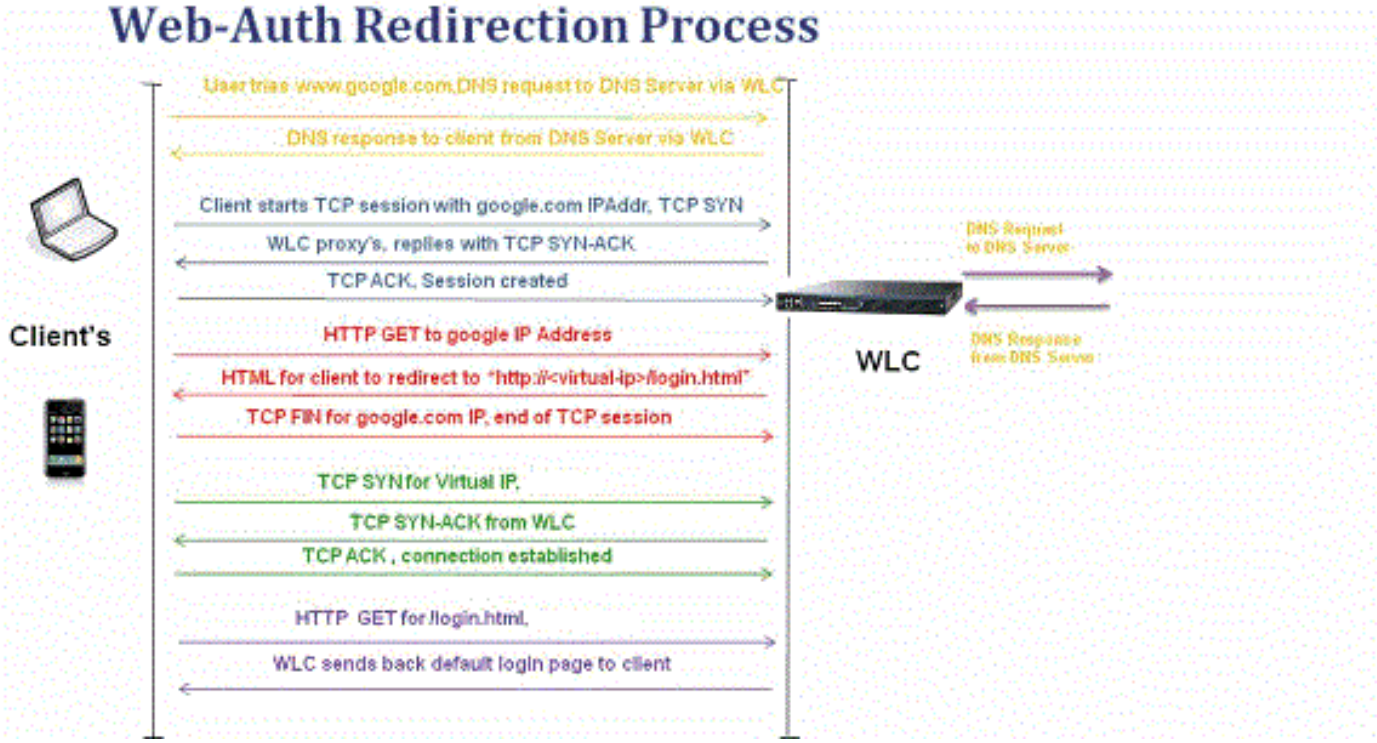
Web 認証はそのクライアントが前auth Access Control List（ACL）によって許可されるトラフィックの例外を正しく有効なユーザ名およびパスワードに供給するまでコントローラが IP トラフィックを、特定のクライアントからの DHCP 関連のパケット ドメイン ネーム システム（DNS）関連のパケットを除いて、許可しますレイヤ3 セキュリティ機能です。 Web 認証はクライアントが認証の前に IP アドレスを得ることを可能にする唯一のセキュリティポリシーです。 それはサプリカントまたはクライアントユーティリティ用の必要なしにシンプル認証認証方法です。 Web 認証は WLC 上でローカルに実行することも、RADIUS サーバ経由で実行することもできます。 一般に、Web 認証はゲスト アクセス ネットワークを展開する場合に使用されます。

Web 認証は、クライアントからの最初の TCP HTTP（ポート 80）GET パケットをコントローラがインターセプトしたときに開始されます。 クライアントの Web ブラウザがそこまで到達するには、クライアントがまず IP アドレスを取得し、Web ブラウザのために URL の IP アドレスへの変換（DNS 解決）を行う必要があります。 これによって、Web ブラウザが HTTP GET を送信する IP アドレスを認識できます。

WLAN で Web 認証が設定されている場合、コントローラは認証プロセスが完了するまで、クライアントからの DHCP および DNS トラフィックを除くすべてのトラフィックをブロックします。 クライアントが TCPポート 80 に最初の HTTP GET を送信 するとき、コントローラは処理のための https://192.0.2.1/login.html にクライアントを（設定されるこれがバーチャルIP なら）リダイレクトします。 このプロセスは最終的にログイン Web ページを起動します。

> **注:** Web 認証のために外部 Webサーバを使用するとき、WLC プラットフォームは外部 Webサーバのための事前認証 ACL を必要とします。

このセクションでは、Web 認証のリダイレクトの手順を詳しく説明します。



- Web ブラウザを開き、たとえば、http://www.google.com などの URL を入力します。 クライアントは、宛先の IP を取得するため、この URL の DNS 要求を送信します。 WLC は DNS サーバに DNS 要求を渡し、DNS サーバは無線クライアントにそれから転送される、宛先 www.google.com の IP アドレスが含まれている DNS 応答と応答を返します。
- 続いて、クライアントは宛先 IP アドレスを使用して TCP 接続を開始しようとします。 Www.google.com の IP アドレスを宛先とする TCP SYN パケットが送信されます。
- WLC にはクライアント用に設定されたルールがあるため、www.google.com のプロキシとして機能します。 WLC は、www.google.com の IP アドレスを送信元とする TCP SYN-ACK パケットをクライアントに戻します。 クライアントは三方 TCP ハンドシェイクを完了するために TCP ACK パケットを送返し、TCP 接続は十分に確立されます。
- クライアントは、宛先が www.google.com である HTTP GET パケットを送信します。 WLC が、このパケットをインターセプトして、リダイレクト処理用に送信します。 HTTP アプリケーション ゲートウェイは、HTML 本文を準備し、クライアントから要求された HTTP GET への応答として返します。 この HTML によって、クライアントが WLC のデフォルト Web ページ URL (http://<Virtual-Server-IP>/login.html など) に誘導されます。
- クライアントは IP アドレスの TCP 接続を、たとえば www.google.com 切断します。
- この場合クライアントは http:// <virtualip>/login.html に行きたいと思い、従って WLC のバーチャル IP アドレスの TCP 接続を開くことを試みます。 (ここにバーチャルIP である) それは WLC にのための TCP 同期信号 パケットを 192.0.2.1 送信 します。
- WLC は、TCP SYN-ACK で応答し、クライアントは WLC に TCP ACK を返して、ハンドシェイクが完了します。
- クライアントは 192.0.2.1 に Login ページを要求するために送信される /login.html のための HTTP GET を送信 します。
- この要求は WLC の Webサーバまで許可され、サーバは Login ページ デフォルトと応答を返します。 クライアントは、ブラウザ ウィンドウでログイン ページを受信し、ユーザはブラウザでログインできます。

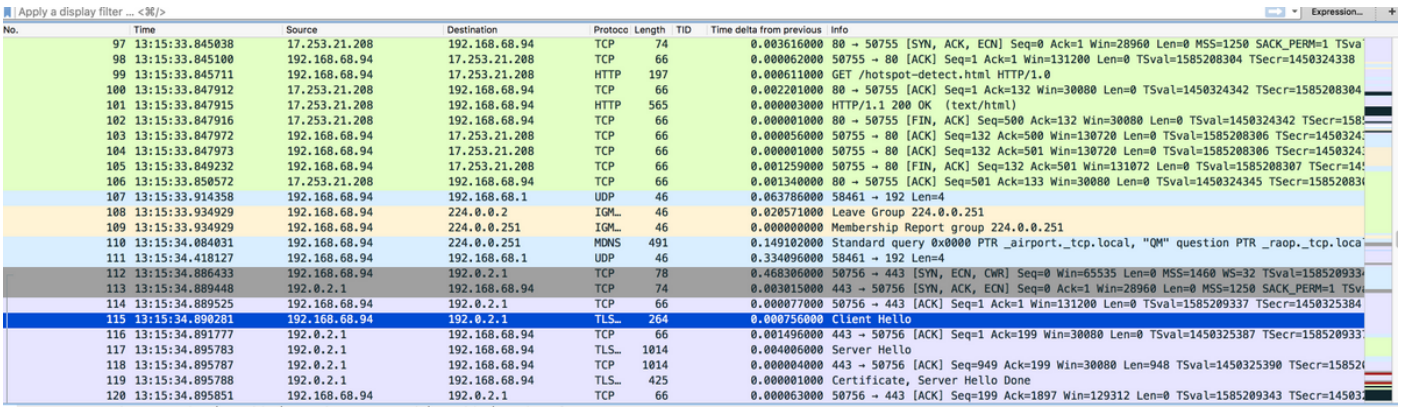
この例では、クライアントの IP アドレスは 192.168.68.94 です。 クライアントはアクセスしていた Webサーバに URL を、10.1.0.13 解決しました。 見てわかるように、クライアントは TCP 接続を開始するために 3方向ハンドシェイクをし、次にパケット 96 から開始する HTTP GET パ

ケットを送信 しました（00 は HTTP パケットです）。 これはユーザによって（要求された URL から）推測できるように誘発されませんでしたが、オペレーティング システムによって自動化された門脈検出誘発でした。 コントローラはコード 200 のパケットおよび応答を代行受信します。 コード 200 のパケットには、次のように、リダイレクト URL が含まれています。

```
<HTML><HEAD>
<TITLE> Web Authentication Redirect</TITLE>
<META http-equiv="Cache-control" content="no-cache">
<META http-equiv="Pragma" content="no-cache">
<META http-equiv="Expires" content="-1">
<META http-equiv="refresh" content="1;
URL=https://192.0.2.1/login.html?redirect=http://captive.apple.com/hotspot-detect.html">
</HEAD></HTML>
```

それは 3方向ハンドシェイクを通してそれから TCP 接続を切断します。

クライアントはそれから 192.0.2.1 にコントローラのバーチャル IP アドレスである、それを送信する リダイレクト URL への HTTPS 接続を開始します。 SSL トンネルを開始するため、クライアントはサーバ証明書を検証するか、または無視する必要があります。 この例では、証明書が自己署名証明書であるため、クライアントはそれを無視します。 ログイン Web ページがこの SSL トンネルを経由して送信されます。 パケット 112 はトランザクションを始めます。



No.	Time	Source	Destination	Protocol	Length	TID	Time delta from previous	Info
97	13:15:33.845038	17.253.21.208	192.168.68.94	TCP	74		0.003616000	80 → 50755 [SYN, ACK, ECN] Seq=0 Ack=1 Win=28960 Len=0 MSS=1250 SACK_PERM=1 TSva
98	13:15:33.845100	192.168.68.94	17.253.21.208	TCP	66		0.000062000	50755 → 80 [ACK] Seq=1 Ack=1 Win=131200 Len=0 TSval=1585208304 TSecr=1450324338
99	13:15:33.845711	192.168.68.94	17.253.21.208	HTTP	197		0.000611000	GET /hotspot-detect.html HTTP/1.0
100	13:15:33.847912	17.253.21.208	192.168.68.94	TCP	66		0.002201000	80 → 50755 [ACK] Seq=1 Ack=132 Win=30080 Len=0 TSval=1450324342 TSecr=1585208304
101	13:15:33.847915	17.253.21.208	192.168.68.94	HTTP	565		0.000003000	HTTP/1.1 200 OK (text/html)
102	13:15:33.847916	17.253.21.208	192.168.68.94	TCP	66		0.000001000	80 → 50755 [FIN, ACK] Seq=500 Ack=132 Win=30080 Len=0 TSval=1450324342 TSecr=158
103	13:15:33.847972	192.168.68.94	17.253.21.208	TCP	66		0.000056000	50755 → 80 [ACK] Seq=132 Ack=500 Win=130720 Len=0 TSval=1585208306 TSecr=1450324
104	13:15:33.847973	192.168.68.94	17.253.21.208	TCP	66		0.000001000	50755 → 80 [ACK] Seq=132 Ack=501 Win=130720 Len=0 TSval=1585208306 TSecr=1450324
105	13:15:33.849232	192.168.68.94	17.253.21.208	TCP	66		0.001259000	50755 → 80 [FIN, ACK] Seq=132 Ack=501 Win=131072 Len=0 TSval=1585208307 TSecr=14
106	13:15:33.850572	17.253.21.208	192.168.68.94	TCP	66		0.001340000	80 → 50755 [ACK] Seq=501 Ack=133 Win=30080 Len=0 TSval=1450324345 TSecr=158520836
107	13:15:33.914358	192.168.68.94	192.168.68.1	UDP	46		0.063786000	58461 → 192 Len=4
108	13:15:33.934929	192.168.68.94	224.0.0.2	IGM…	46		0.020571000	Leave Group 224.0.0.251
109	13:15:33.934929	192.168.68.94	224.0.0.251	IGM…	46		0.000000000	Membership Report group 224.0.0.251
110	13:15:34.084031	192.168.68.94	224.0.0.251	MDNS	491		0.149102000	Standard query 0x0000 PTR _airport._tcp.local, "QM" question PTR _raop._tcp.loca
111	13:15:34.418127	192.168.68.94	192.168.68.1	UDP	46		0.334096000	58461 → 192 Len=4
112	13:15:34.886433	192.168.68.94	192.0.2.1	TCP	78		0.468306000	50756 → 443 [SYN, ECN, CWR] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=158520933
113	13:15:34.889448	192.0.2.1	192.168.68.94	TCP	74		0.003015000	443 → 50756 [SYN, ACK, ECN] Seq=0 Ack=1 Win=28960 Len=0 MSS=1250 SACK_PERM=1 TSv
114	13:15:34.889525	192.168.68.94	192.0.2.1	TCP	66		0.000077000	50756 → 443 [ACK] Seq=1 Ack=1 Win=131200 Len=0 TSval=1585209337 TSecr=1450325384
115	13:15:34.890281	192.168.68.94	192.0.2.1	TLS…	264		0.000756000	Client Hello
116	13:15:34.891777	192.0.2.1	192.168.68.94	TCP	66		0.001496000	443 → 50756 [ACK] Seq=1 Ack=199 Win=30080 Len=0 TSval=1450325387 TSecr=158520933
117	13:15:34.895783	192.0.2.1	192.168.68.94	TLS…	1014		0.004006000	Server Hello
118	13:15:34.895787	192.0.2.1	192.168.68.94	TCP	1014		0.000004000	443 → 50756 [ACK] Seq=949 Ack=199 Win=30080 Len=948 TSval=1450325390 TSecr=15852
119	13:15:34.895788	192.0.2.1	192.168.68.94	TLS…	425		0.000001000	Certificate, Server Hello Done
120	13:15:34.895851	192.168.68.94	192.0.2.1	TCP	66		0.000063000	50756 → 443 [ACK] Seq=199 Ack=1897 Win=129312 Len=0 TSval=1585209343 TSecr=14503

WLC のバーチャル IP アドレスのためのドメイン名を設定するオプションがあります。 仮想 IP アドレスにドメイン名を設定する場合、このドメイン名は、クライアントからの HTTP GET パケットへの応答の際の HTTP OK パケットの中でコントローラから返されます。 それからこのドメイン名のための DNS 解決を行わなければなりません。 それが DNS 解決から IP アドレスを得れば、コントローラの仮想インターフェイスで設定される IP アドレスであるその IP アドレスの TCP セッションを開くように試みます。

最終的に、Webページはクライアントにトンネルによって通じ、ユーザは Secure Sockets Layer（SSL）トンネルによって username/password を送返します。

次の 3 つの方法のいずれかによって、Web 認証が実行されます。

- 内部 Webページ（デフォルト）を使用して下さい。 デフォルト Web ページの使用の詳細については、「デフォルト Web 認証ログイン ページの選択」を参照してください。
- カスタマイズされた Login ページを使用して下さい。 カスタマイズされた Login ページを使用する方法に関する詳細についてはカスタマイズされた Web 認証ログイン ページを作成することを参照して下さい。
- 外部 Webサーバからの Login ページを使用して下さい。 外部 Web サーバが提供するログイン ページの使用の詳細については、「外部 Web サーバが提供するカスタマイズした Web 認証ログインページの使用」を参照してください。

注：
-カスタマイズされた Web 認証バンドルにファイル名のための 30 文字までの制限があります。 バンドル内のすべてのファイル名が 30 文字以内であることを確認する。

Web 認証が WLAN で有効に なればまた CPU ACL ルールがあれば前に、クライアント ベース Web 認証ルールは- WLC リリース 7.0 から…クライアントが WebAuth_Reqd 状態で非認証である限り高い優先順位を常に優先し。 クライアントが RUN 状態になると、CPU ACL ルールが適用されます。

-従って、CPU ACL が WLC で有効に なれば、これらの状態に仮想インターフェイス IP のための割り当てルールが（ANY 方向で）必要となります:
- CPU ACL に割り当てが両方向のためのすべてのルールない時。
-そこに割り当てをすべて支配して下さい存在 して、そこにまた高い優先順位のポート 443 または 80 のための拒否ルールを存在 した場合。

-バーチャルIP のための割り当てルールは TCP プロトコルおよびポート 80 のため secureweb が有効に なる場合 secureweb が無効に なれば、またはポート 443 はずですである。 これは、CPU ACL が設定されている場合に、クライアントの仮想インターフェイス IP アドレスへのアクセスが、正常認証をポストできるようにするために必要です。

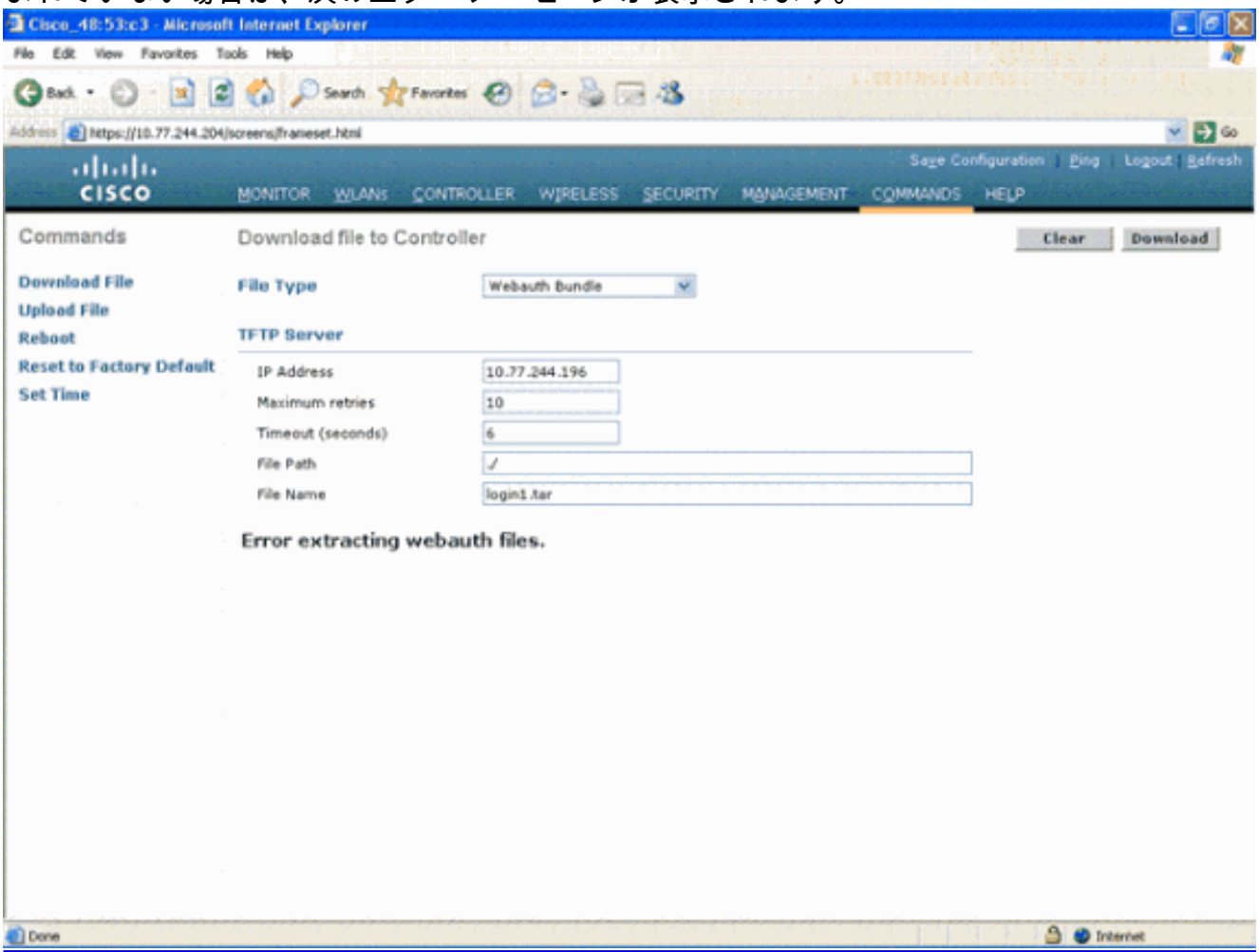
Web 認証のトラブルシューティング

Web 認証を設定した後、そして機能が予想通り動作しなかったら、これらのステップを完了して下さい:

1. クライアントが IP アドレスを取得しているかどうかを確認します。 そうでなかったら、ユーザは**必要とし、**WLAN のチェックボックスを与えます無線クライアントに静的IP アドレスを **DHCP の**チェックを外すことができます。 これによって、アクセス ポイントの割り当てが見込まれます。
2. プロセスの次のステップは、Web ブラウザでの URL の DNS 解決です。 WLAN クライアントが、Web 認証用に設定された WLAN に接続したとき、クライアントは DHCP サーバから IP アドレスを取得します。 ユーザはブラウザを開始し、Web サイトのアドレスを入力します。 クライアントは、DNS 解決を実行して Web サイトの IP アドレスを取得します。 ここで、クライアントがその Web サイトにアクセスしようとすると、WLC はクライアントの HTTP Get セッションをインターセプトし、ユーザを Web 認証ログイン ページにリダイレクトします。
3. したがって、リダイレクションが機能するように、クライアントが DNS 解決を実行できることを確認します。 Microsoft Windows では、Command ウィンドウを開くために Start > Run の順に選択 し、**CMD を**入力し、「nslookup www.cisco.com」をし、IP アドレスがもどって来るかどうか参照して下さい。 MAC/Linux では、ターミナル ウィンドウを開き、「nslookup www.cisco.com」をし、IP アドレスがもどって来るかどうか参照して下さい。信じればクライアントは DNS 解決を、できます次のいずれか得ません:URL の IP アドレスを入力して下さい（たとえば、http://www.cisco.com は http://198.133.219.25) です。ワイヤレスアダプタを通って解決する必要がある（非実在）IP アドレスを入力することを試みて下さい。この URL の入力によって、Web ページが起動される場合、 DNS の問題である可能性が最も高くなります。 証明書の問題である可能性もあります。 コントローラは、デフォルトで、自己署名証明書を使用し、ほとんどの Webブラウザは使用に対して警告します。
4. カスタマイズされた Webページとの Web 認証に関しては、カスタマイズされた Webページのための HTML コードが適切であることを確認して下さい。 サンプル Web 認証スクリプ

トは、シスコのソフトウェア ダウンロードからダウンロードできます。 たとえば、5508 人のコントローラのために、**製品 > ワイヤレス > ワイヤレス LAN コントローラ > スタンドアロン コントローラを > Cisco 5500 シリーズ ワイヤレス LAN コントローラ > シャーシ > ワイヤレス LAN コントローラ Web 認証バンドルの Cisco 5508 ワイヤレス LAN コントローラ > ソフトウェア**選択し、**webauth_bundle.zip ファイルを**ダウンロードして下さい。ユーザのインターネット ブラウザがカスタマイズされたログイン ページにリダイレクトされるときに、次のパラメータが URL に追加されます。ap_mac -無線ユーザが準であるアクセス ポイントの MAC アドレス。switch_url -ユーザーの資格情報が掲示する必要があるコントローラの URL。リダイレクト-認証が正常だった後ユーザがリダイレクトされる URL。ステータス・コード-コントローラの Web 認証サーバから戻るステータス スコード。wlan -無線ユーザが準である WLAN SSID。次のステータス コードが使用できます。ステータス スコード 1 -「既にログオンされています。 特にアクションは必要ありません。」ステータス スコード 2 -「ウェブ ポータルに対して認証するために設定されません。 特にアクションは必要ありません。」ステータス スコード 3 -「規定 されるユーザー名は現時点で使用することができません。 あるいは、そのユーザ名はすでにシステムにログインしている可能性があります。」ステータス スコード 4 -「除かれました」。ステータス スコード 5 -「である無効入力したユーザネームおよびパスワード組み合せ。 再試行してください。"

5. WLC にアップロードされる前にカスタマイズされた Webページで書かれる必要があるピクチャ .tar ファイルにおよびすべてのファイルは組み込む必要があります。 .tar バンドルに含まれているファイルのが login.html であることを確認して下さい。 login.html ファイルが含まれていない場合は、次のエラー メッセージが表示されます。



カスタマイズされた Web 認証ウィンドウの作成方法については、「ワイヤレス LAN コントローラの Web 認証の設定例」の「カスタマイズされた Web 認証のガイドライン」セクションを参照してください。**注:** 大容量ファイルと長い名前のファイルでは、抽出エラーが起こ

ります。 画像は .jpg フォーマットをお勧めします。
6. WLC のカスタマイズされた Web ページは本質的に HTML スクリプトであるため、クライアント ブラウザで、**Scripting** オプションがブロックされていないことを確認します。
7. WLC の**仮想インターフェイス**に**ホスト名**を設定した場合、仮想インターフェイスのホスト名に対して DNS 解決が使用できることを確認します。 **注:** 仮想インターフェイスに **DNS ホスト名**を割り当てるには、WLC GUI で [Controller] > [Interfaces] メニューの順に移動します。
8. 場合によっては、クライアント コンピュータにインストールされているファイアウォールによって Web 認証ログイン ページがブロックされることがあります。 ログイン ページへのアクセスを試みる前に、ファイアウォールをディセーブルにしてください。 Web 認証が完了した後は、ファイアウォールを再びイネーブルにしても問題ありません。
9. トポロジー/ソリューション ファイアウォールはネットワークによって決まる Webauth サーバ置くことができますとクライアントの間に。 各ネットワークの設計または実装ソリューションと同様に、エンドユーザはネットワークのファイアウォールにおいて次のポートが許可されていることを確認する必要があります。

10. Web 認証が実行されるには、クライアントはまず、WLC で適切な WLAN と関連付けられる必要があります。 クライアントが WLC に関連付けられているかどうかを確認するには、WLC で [Monitor] > [Clients] メニューの順に移動します。 クライアントが有効な IP アドレスを持っているかどうか確認します。
11. Web 認証が完了するまで、クライアント ブラウザのプロキシ設定をディセーブルにします。
12. デフォルトのWeb 認証方式は Password Authentication Protocol （ PAP ）です。 RADIUS サーバで PAP 認証が機能するように許可されていることを確認します。 クライアント認証の状態を確認するために、RADIUS サーバからのデバッグ メッセージとログ メッセージを確認します。 WLC の**すべての**コマンド RADIUSサーバからのデバッグを表示するために**デバッグ AAA を**使用できます。
13. コンピュータのハードウェア ドライバを製造業者の Web サイトから取得した最新コードにアップデートします。
14. サプリカント（ラップトップのプログラム ）の設定を確認します。
15. Windows に組み込みの Windows Zero Config サプリカントを使用する場合： ユーザが最新のパッチをインストールしてもらうことを確認して下さい。サプリカントのデバッグを実行して下さい。
16. クライアントで、EAPOL （ WPA+WPA2 ）を起動すれば RASTLS は Command ウィンドウから記録 します。 Start > Run > cmd の順に選択 して下さい:
    ```
    netsh ras set tracing eapol enable
          netsh ras set tracing rastls enable
    ```
    ログをディセーブルにするには同じコマンドを実行しますが、enable の部分を disable に置き換えます。 XP の場合は、すべての口グは、C:\Windows\tracing に置かれます。
17. ログイン Web ページがまだない場合は、次の出力を 1 台のクライアントから収集して分析します。
    ```
    debug client <mac_address in format xx:xx:xx:xx:xx:xx>
    debug dhcp message enable
    debug aaa all enable
    debug dot1x aaa enable
    debug mobility handoff enable
    ```
18. これらのステップを完了した後問題が解決されない場合、これらのデバッグを収集し、サービス リクエストを開くために[サポート ケース マネージャを](#)使用して下さい。
    ```
    debug pm ssh-appgw enable
    debug pm ssh-tcp enable
    ```

```
debug pm rules enable
debug emweb server enable
debug pm ssh-engine enable packet <client ip>
```

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 LAN コントローラを使用した外部 Web 認証の設定例
- テクニカル サポートとドキュメント – Cisco Systems