

ワイヤレスLANコントローラ(WLC)でのWeb認証のトラブルシューティング

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[関連製品](#)

[WLCでのWeb認証](#)

[Web認証のトラブルシューティング](#)

[関連情報](#)

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)環境でWeb認証の問題をトラブルシューティングするための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あることが推奨されます。

- Control and Provisioning of Wireless Access Points(CAPWAP)。
- 基本動作用にLightweightアクセスポイント(LAP)とWLCを設定する方法
- Web認証に関する基本的な知識とWLCでのWeb認証の設定方法。

WLCでWeb認証を設定する方法については、『[ワイヤレスLANコントローラのWeb認証の設定例](#)』を参照してください。

使用するコンポーネント

このドキュメントの情報は、ファームウェアバージョン 8.3.121 が稼働する WLC 5500 に基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

関連製品

このドキュメントは、次のハードウェアでも使用できます。

- 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、事前認証アクセスコントロールリスト(ACL)で許可されたトラフィックを除き、有効なユーザ名とパスワードを正しく入力するまで、特定のクライアントからのIPトラフィック(DHCP関連パケット/ドメインネームシステム(DNS)関連パケットを除く)をコントローラで許可しないようにするレイヤ3セキュリティ機能です。Web 認証は、認証の前にクライアントが IP アドレスを取得することを許可する唯一のセキュリティ ポリシーです。これは、サブリカントやクライアント ユーティリティを必要としない簡単な認証方式です。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。

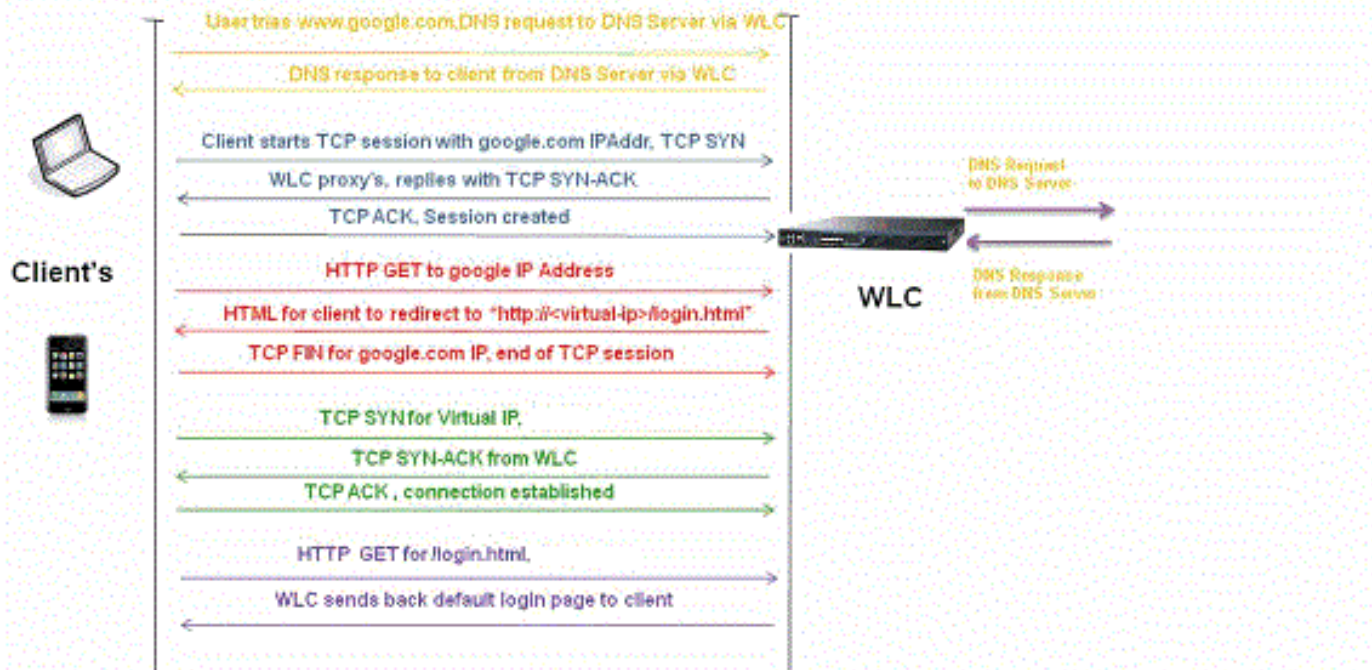
Web 認証は、クライアントからの最初の TCP HTTP (ポート 80) GET パケットをコントローラがインターセプトしたときに開始されます。クライアントのWebブラウザがそこまで到達するには、クライアントはまずIPアドレスを取得し、WebブラウザのURLからIPアドレスへの変換 (DNS解決) を行う必要があります。これによって、Web ブラウザが HTTP GET を送信する IP アドレスを認識できます。

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。クライアントが最初のHTTP GETをTCPポート80に送信すると、コントローラは処理のためにクライアントを<https://192.0.2.1/login.html> (これが設定されている仮想IPである場合) に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認証に外部Webサーバを使用する場合、WLCプラットフォームには外部Webサーバ用の事前認証ACLが必要です。

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-Auth Redirection Process



- Web ブラウザを開き、たとえば、`http://www.example.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 要求を DNS サーバに渡し、DNS サーバは宛先 `www.example.com` の IP アドレスを含む DNS 応答を返します。この応答はワイヤレスクライアントに転送されます。
- 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.example.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.example.com のプロキシとして機能します](#)。WLC は、[www.example.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、3ウェイ TCP ハンドシェイクを完了するために TCP ACK パケットを返信し、TCP 接続が完全に確立されます。
- クライアントは、宛先が `www.example.com` である HTTP GET パケットを送信します。WLC は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 により、クライアントは WLC のデフォルト Web ページの URL (たとえば、`http://<Virtual-Server-IP>/login.html`。) に転送されます。
- クライアントは、たとえば [www.example.com](#) などの IP アドレスとの TCP 接続を閉じます。
- 次に、クライアントは [http://<virtualip>/login.html](#) に移動するため、WLC の仮想 IP アドレスを使用して TCP 接続を開こうとします。192.0.2.1 (ここでは仮想 IP) の TCP SYN パケットを WLC に送信します。
- WLC は TCP SYN-ACK で返答し、クライアントはハンドシェイクを完了するために、TCP ACK を WLC に戻します。

- クライアントは、ログインページを要求するために、192.0.2.1宛ての/login.html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、サーバはデフォルトのログインページで応答します。クライアントは、ユーザがログインできるブラウザウィンドウでログインページを受け取ります。

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、アクセスしたWebサーバ10.1.0.13へのURLを解決しました。このように、クライアントは3ウェイハンドシェイクを実行してTCP接続を開始し、パケット96 (00はHTTPパケット) で始まるHTTP GETパケットを送信しました。これはユーザによってトリガーされたのではなく、オペレーティングシステム(OS)によるポータルサイトの自動検出トリガーでした (要求されたURLから推測できます)。コントローラはパケットを代行受信し、コード200で応答します。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">
</HEAD></HTML>
```

次に、3ウェイハンドシェイクによってTCP接続を閉じます。

次に、クライアントはリダイレクトURLへのHTTPS接続を開始し、リダイレクトURLはコントローラの仮想IPアドレスである192.0.2.1に送信します。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。トランザクションは、パケット 112 から始まります。

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 TSval=0
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	192.168.68.94	192.168.68.94	TCP	66		0.000001000	80 -> 50755 [FIN, ACK] Seq=500 Ack=132 Win=30080 Len=0 TSval=1450324342 TSecr=1585208304
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=1450324342
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=1450324342
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=1450324342
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=1585208304
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	224.0.0.251	IGMP	46		0.020571000	Leave Group 224.0.0.251
109	13:15:33.934929	192.168.68.94	224.0.0.251	IGMP	46		0.000000000	Membership Report group 224.0.0.251
110	13:15:34.004031	192.168.68.94	224.0.0.251	MDNS	491		0.149102000	Standard query 0x0000 PTR _airport._tcp.local, "QM" question PTR _raop._tcp.local
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, CWI] Seq=0 Win=65535 Len=0 MSS=1460 WS=32 TSval=1585209337 TSecr=1450325384
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 TSval=0
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=1585209337
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=1585209337
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=1450325384

WLCの仮想IPアドレス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。次に、このドメイン名に対してDNS解決を実行する必要があります。DNS解決からIPアドレスを取得すると、そのIPアドレス (コントローラの仮想インターフェイスに設定されたIPアドレス) を使用してTCPセッションを

開こうとします。

最終的に、Webページはトンネルを介してクライアントに渡され、ユーザはSecure Sockets Layer(SSL)トンネルを介してユーザ名とパスワードを返信します。

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ページを使用します (デフォルト)。
- カスタマイズされたログインページを使用します。
- 外部Webサーバからのログインページを使用します。



注 :

- カスタマイズされたWeb認証バンドルには、ファイル名に対して最大30文字の制限があります。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。

- WLCリリース7.0以降、WLANでWeb認証がイネーブルにされていて、CPU ACLルールもある場合、クライアントがWebAuth_Reqd状態で認証されていない限り、クライアントベースのWeb認証ルールが常に優先されます。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。

- したがって、CPU ACLがWLCで有効になっている場合、次の条件では仮想インターフェイスIPの許可ルールが (任意の方向に) 必要です。

- CPU ACL に、両方向の allow ALL ルールがない場合。

- allow ALL ルールがあるが、より優先順位の高い、ポート 443 または 80 に対する DENY ルールがある場合。

- 仮想IPの許可ルールは、TCPプロトコルとポート80 (securewebが無効の場合)、またはポート443 (securewebが有効の場合) に対して設定する必要があります。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、機能が期待どおりに動作しない場合は、次の手順を実行します。

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。そうでない場合は、WLANのDHCP Requiredチェックボックスのチェックマークを外して、ワイヤレスクライアントに固定IPアドレスを割り当てます。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、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。

- 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、Start > Runの順に選択し、CMDと入力してコマンドウィンドウを開き、「nslookup www.cisco.com」を実行してIPアドレスが返されるかどうかを確認します。

Mac/Linuxでターミナルウィンドウを開き、nslookup www.cisco.comを実行して、IPアドレスが返されるかどうかを確認します。

クライアントがDNS解決を取得しないと考えられる場合は、次のいずれかを実行できます。

- URLのIPアドレスを入力します(たとえば、<http://www.cisco.com>は<http://192.168.219.25>)。
- ワイヤレスアダプタを介して解決する必要がある(存在しない)IPアドレスを入力してみてください。

このURLを入力すると、Webページが表示されますか。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ブラウザはその使用を警告します。

- カスタマイズされたWebページを使用したWeb認証では、カスタマイズされたWebページのHTMLコードが適切であることを確認します。

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コントローラの場合は、Products > Wireless > Wireless LAN Controller > Standalone Controllers > Cisco 5500 Series Wireless LAN Controllers > Cisco 5508 Wireless LAN Controller > Software on Chassis > Wireless Lan Controller Web Authentication Bundleの順に選択し、webauth_bundle.zipファイルをダウンロードします。

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、次のパラメータがURLに追加されます。

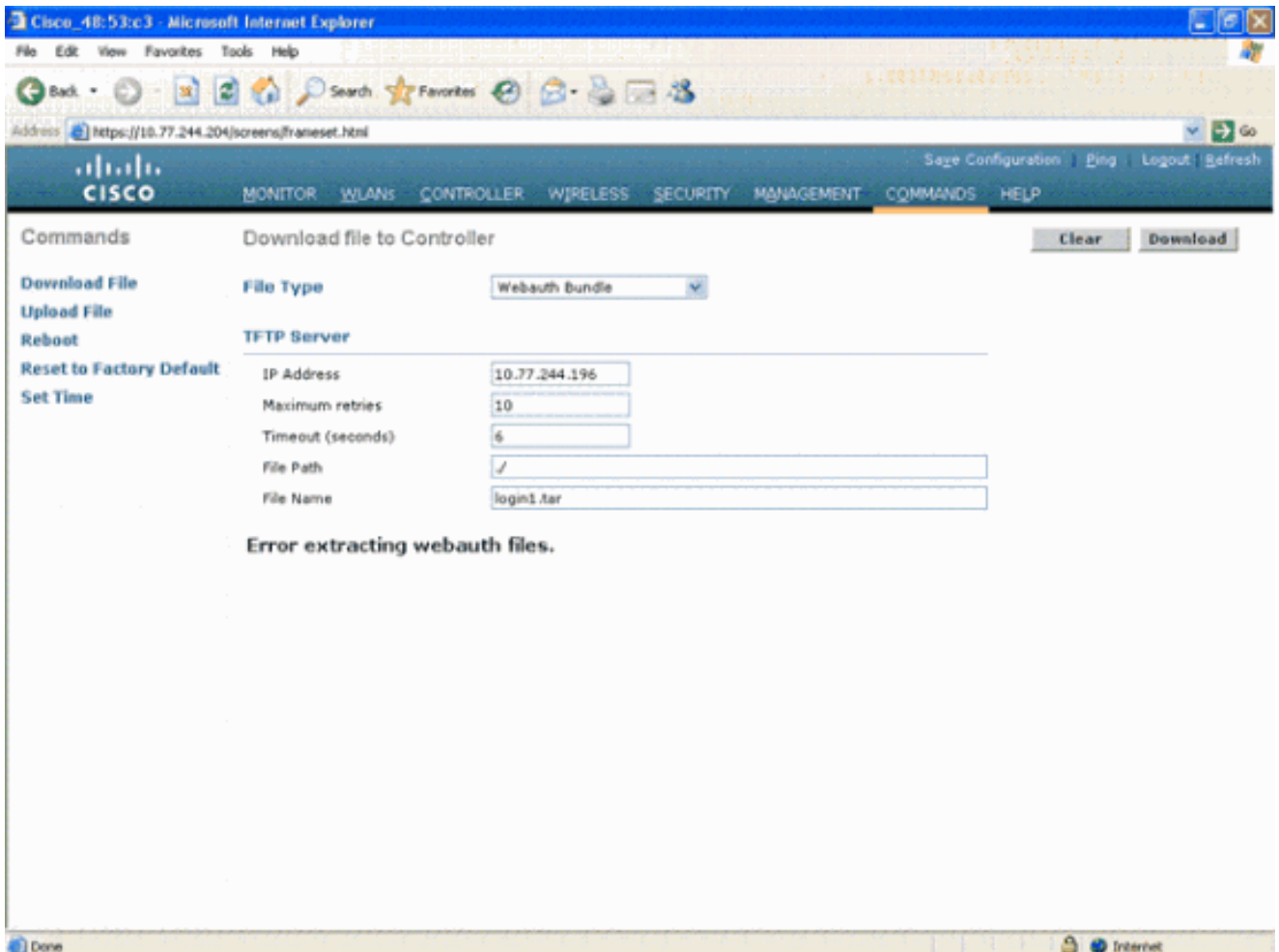
- ap_mac : ワイヤレスユーザが関連付けられているアクセスポイントのMACアドレス。
- switch_url : ユーザクレデンシャルをポストするコントローラのURL。
- redirect : 認証が成功した後にユーザがリダイレクトされるURL。
- statusCode : コントローラのWeb認証サーバから返されるステータスコード。
- wlan : ワイヤレスユーザが関連付けられているWLAN SSID。

次のステータスコードが使用できます。


- ステータスコード1 - すでにログインしています。ユーザ側でこれ以上の操作は必要ありません。
- ステータスコード2 - Webポータルに対して認証するように設定されていません。ユーザ側でこれ以上の操作は必要ありません。
- ステータスコード3 - 指定されたユーザ名は現在使用できません。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か。


- ステータスコード4 – 除外されました。
 - ステータスコード5：入力したユーザ名とパスワードの組み合わせが無効です。
5. カスタマイズされたWebページに表示する必要があるすべてのファイルと画像は、WLCにアップロードする前に.tarファイルにバンドルする必要があります。.tarバンドルに含まれているファイルの1つがlogin.htmlであることを確認します。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：サイズの大きいファイルや名前の長いファイルでは、書き出しエラーが発生する可能性があります。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から

 Controller > Interfacesメニューに移動します。

- 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。
- トポロジ/ソリューションファイアウォールは、ネットワークに応じて、クライアントと Web認証サーバの間に配置できます。実装された各ネットワーク設計/ソリューションについて、エンドユーザは、これらのポートがネットワークファイアウォールで許可されていることを確認する必要があります。

プロトコル	ポート
HTTP/HTTPS トラフィック	TCP ポート 80/443
CAPWAP データ/コントロール トラフィック	UDP ポート 5247/5246
LWAPP データ/コントロール トラフィック (リリース 5.0 以前)	UDP ポート 12222/12223
EOIP パケット	IP プロトコル 97
モビリティ	UDP ポート 16666 (非セキュア) UDP ポート 16667 (セキュア IPSEC トンネル)

- Web認証を実行するには、クライアントをWLC上の適切なWLANに最初に関連付ける必要があります。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。
- 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。
- デフォルトのWeb認証方式は、パスワード認証プロトコル(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でdebug aaa allコマンドを使用すると、RADIUSサーバからのデバッグを表示できます。
- コンピュータのハードウェアドライバを製造元のWebサイトから最新のコードに更新します。
- サブリカント (ラップトップのプログラム) の設定を確認します。
- Windows に組み込みの Windows Zero Config サブリカントを使用する場合：
 - ユーザに最新のパッチがインストールされていることを確認します。
 - サブリカントでデバッグを実行します。
- クライアントで、コマンドウィンドウからEAPOL(WPA+WPA2)とRASTLSログを有効にします。Start > Run > CMDの順に選択します。

```
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、すべてのログはC:\Windows\tracingにあります。

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. これらの手順を実行しても問題が解決しない場合は、次のデバッグ情報を収集し、[Support Case Manager](#)を使用してサービスリクエストをオープンします。

```
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](#)
- [シスコのテクニカルサポートとダウンロード](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。