

Web 認証プロキシの設定例

内容

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[WLC の設定](#)

[PAC ファイルの設定](#)

[事前認証 ACL の作成](#)

[クイック変更：Web ブラウザの設定](#)

[確認](#)

[トラブルシューティング](#)

概要

このドキュメントでは、プロキシ設定と連携するため Web 認証を設定する方法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。

- ワイヤレス LAN コントローラの基本設定
- Web 認証セキュリティ

使用するコンポーネント

このドキュメントの情報は、Cisco Wireless LAN Controller バージョン 7.0 以降に基づくものです。

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、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

設定

ネットワーク上でプロキシ サーバを維持するネットワーク管理者は、最初にプロキシ サーバに web トラフィックを送信し、その後インターネットにトラフィックをリレーします。クライアントとプロキシ サーバ間の接続では、ポート 80 以外の TCP ポートを通信に使用できます。このポ

ートは通常、TCP ポート 3128 または 8080 です。デフォルトでは、Web認証はポート80でのみリッスンします。したがって、HTTP GETがコンピュータを離れると、プロキシポートに送信されますが、コントローラによってドロップされます。

このセクションでは、プロキシ設定と連携するために Web 認証を設定する方法について説明します。

1. プロキシ ポートをリッスンするため、シスコワイヤレス LAN コントローラ (WLC) を設定します。
2. 仮想 IP アドレスを直接返すには、プロキシの自動設定 (PAC) ファイルを設定します。
3. Web 認証をする前にクライアントが PAC ファイルをダウンロードできるようにするには、事前認証のアクセスコントロール リスト (ACL) を作成します。

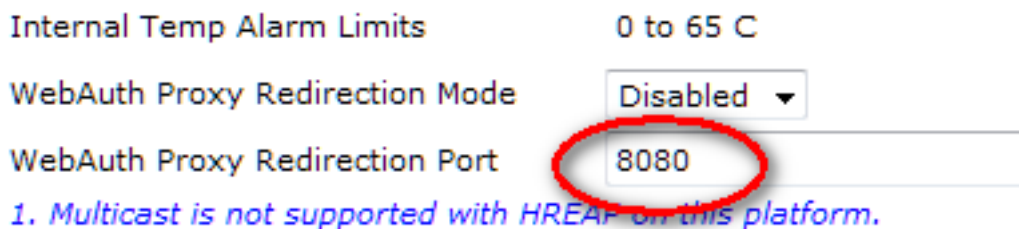
応急処置として、192.0.2.1 を返すように Web ブラウザを手動で設定可能です。

これらの各プロセスの詳細は、次のサブセクションで示します。

WLC の設定

この手順では、コントローラがリッスンするポートを、プロキシ サーバがリッスンしているポートに変更する方法について説明します。

1. [Controller] > [General] ページに移動します。

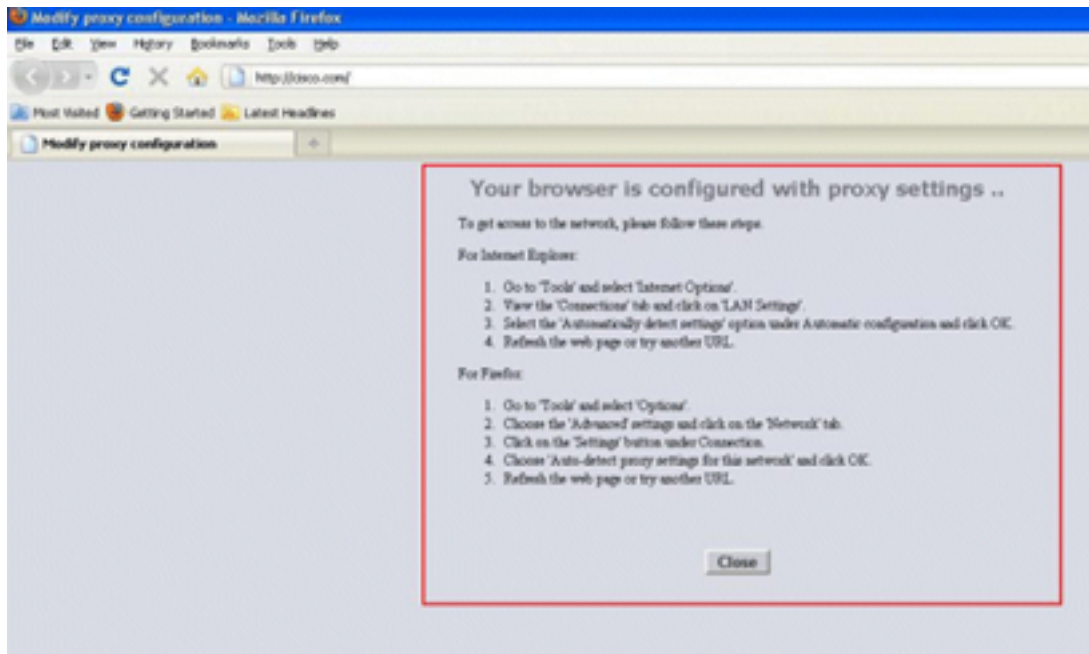


The screenshot shows the configuration page for the WLC. The 'Internal Temp Alarm Limits' is set to '0 to 65 C'. The 'WebAuth Proxy Redirection Mode' is set to 'Disabled' in a dropdown menu. The 'WebAuth Proxy Redirection Port' is set to '8080' in a text input field, which is circled in red. Below the input field, there is a blue note: '1. Multicast is not supported with HREAP on this platform.'

2. [WebAuth Proxy Redirection Port] フィールドで、WLC がクライアント リダイレクトを行うためにリッスンするポートを入力します。
3. [WebAuth Proxy Redirection Mode] ドロップダウン リストから [Disabled] または [Enabled] を選択します。

[Disabled] を選択すると、パススルーまたは認証用の通常の Web 認証のページがクライアントに表示されます。したがってプロキシを使用する場合は、192.0.2.1 (または WLC で使用される他の仮想 IP アドレス) に対してプロキシを使用しないようにすべてのクライアント ブラウザを設定する必要があります。 「[Web ブラウザを設定する](#)」を参照してください。

[Enabled] を選択すると、WLC ではデフォルトでポート 80、8080、および 3128 をリッスンするため、[WebAuth Proxy Redirection Port] テキスト フィールドにこれらのポートを入力する必要はありません。クライアントがこれらのポートで HTTP GET を送信すると、これらのポートには、プロキシ設定を自動に変更するように求める画面が表示されます。



4. 設定を保存します。

5. コントローラをリブートします。

つまり、WLC がリッスンするポートを定義するには、[WebAuth Proxy Redirection Port] にポート番号を入力します。リダイレクションモードが有効化されると、クライアントはプロキシ設定画面にリダイレクトされ、自動プロキシ設定を行うように、Webプロキシ自動発見 (WPAD) または PAC ファイルを動的にプッシュすることを求められます。無効化されると、クライアントは通常の Web 認証ページにリダイレクトされます。

PAC ファイルの設定

WLC の仮想 IP アドレスは、Web 認証がユーザを適切に認証するために「direct」に戻される必要があります。Direct とはプロキシサーバが要求をプロキシしないことであり、クライアントは IP アドレスに直接到達するためのアクセス許可を持つことを意味します。通常、これは WPAD または PAC ファイル内のプロキシサーバ上で、プロキシサーバ管理者によって設定されます。次に PAC ファイルの設定例を示します。

```
function FindProxyForURL(url, host) {
    // our local URLs from the domains below example.com don't need a proxy:
    if (shExpMatch(host, "*.example.com"))
    if (shExpMatch(host, "192.0.2.1"))    <-- (Line states return 1.1.1 directly)
    {
        return "DIRECT";
    }

    // URLs within this network are accessed through
    // port 8080 on fastproxy.example.com:
    if (isInNet(host, "10.0.0.0", "255.255.248.0"))
    {
        return "PROXY fastproxy.example.com:8080";
    }

    // All other requests go through port 8080 of proxy.example.com.
    // should that fail to respond, go directly to the WWW:
    return "PROXY proxy.example.com:8080; DIRECT";
}
```

事前認証 ACL の作成

事前認証 ACL は Web 認証サービス セット識別子 (SSID) で発行されます。これにより、クライアントが Web 認証にログインする前に、ワイヤレス クライアントは PAC ファイルをダウンロードできます。事前認証 ACL は、PAC ファイルが存在するポートのみへのアクセスを許可する必要があります。プロキシ ポートへのアクセスによって、クライアントは Web 認証なしでインターネットに到達できるようになります。

1. コントローラ上に ACL を作成するには、[Security] > [Access Control List] に移動します。
2. PAC ダウンロード ポート上でプロキシへのトラフィックを双方向で許可するルールを作成します。

General										
Access List Name		ACL1								
Deny Counters		0								
Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction	Number of Hits	
1	Permit	0.0.0.0 /	192.168.0.4 /	TCP	Any	8081	Any	Any	0	
		0.0.0.0 /	255.255.255.255 /							
2	Permit	192.168.0.4 /	0.0.0.0 /	TCP	8081	Any	Any	Any	0	
		255.255.255.255 /	0.0.0.0 /							

注：プロキシHTTPポートを許可しないでください。

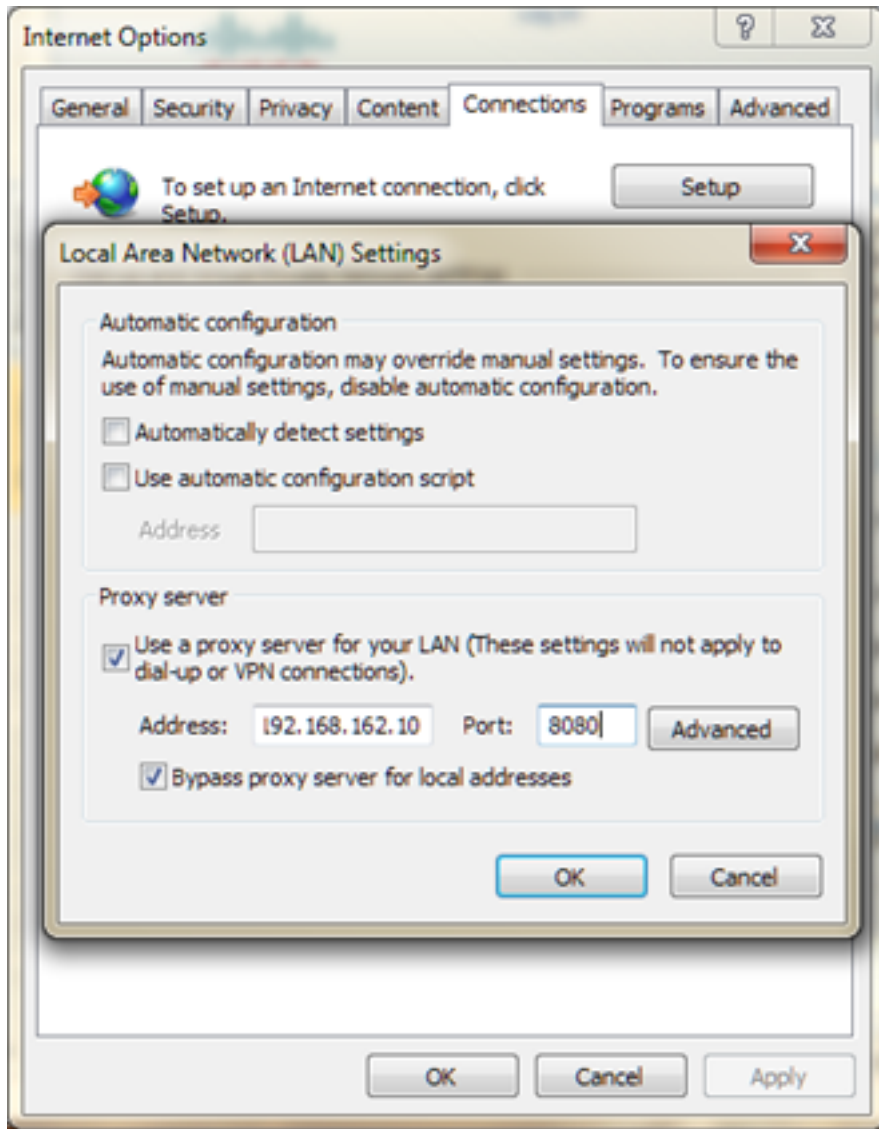
3. コントローラの WLAN 設定で、作成したばかりの ACL を事前認証 ACL として選択することを忘れないでください。

The screenshot shows the configuration page for WLAN settings. At the top, there are tabs for 'General', 'Security', 'QoS', and 'Advanced'. Under the 'Security' tab, there are sub-tabs for 'Layer 2', 'Layer 3', and 'AAA Servers'. The 'AAA Servers' sub-tab is selected. In this view, 'Layer 3 Security' is set to 'None'. There are several radio button options: 'Web Policy' (checked), 'Authentication' (selected), 'Passthrough', 'Conditional Web Redirect', 'Splash Page Web Redirect', and 'On MAC Filter failure' (with a blue '11' next to it). At the bottom, 'Preauthentication ACL' is set to 'ACL1' via a dropdown menu, and 'Over-ride Global Config' is set to 'Enable' via a checkbox.

クイック変更：Web ブラウザの設定

この手順では、クライアントの Web ブラウザが 192.0.2.1 に直接到達するように手動で例外を設定する方法について説明します。

1. Internet Explorer で、[Tools] > [Internet] オプションに移動します。
2. [Connections] タブをクリックし、次に [LAN Settings] ボタンをクリックします。
3. [Proxy server] エリアで [Use a proxy server for your LAN] チェック ボックスをオンにし、サーバのリッスンする IP アドレスおよびポートを入力します。



4. [Advanced] ボタンをクリックし、[Exceptions] 領域で WLC の仮想 IP アドレスを入力します。

Servers

Type	Proxy address to use	Port
HTTP:	192.168.162.10	
Secure:		
FTP:		
Socks:		

Use the same proxy server for all protocols

Exceptions

Do not use proxy server for addresses beginning with:

192.0.2.1

Use semicolons (;) to separate entries.

確認

現在、この設定に使用できる確認手順はありません。

トラブルシューティング

現在、この設定に関する特定のトラブルシューティング情報ははありません。