

Web 認証プロキシの設定例

目次

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[表記法](#)

[設定](#)

[WLC の設定](#)

[PAC ファイルを設定する](#)

[事前認証 ACL を作成する](#)

[手っ取り早い解決策： Web ブラウザを設定する](#)

[確認](#)

[トラブルシューティング](#)

[関連情報](#)

概要

このドキュメントでは、プロキシ設定を使用するように 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 認証のセキュリティ

使用するコンポーネント

このドキュメントの情報は、シスコ ワイヤレス LAN コントローラ バージョン 7.0 以降に基づくものです。

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。

表記法

ドキュメント表記の詳細は、『[シスコテクニカルティップスの表記法](#)』を参照してください。

設定

プロキシサーバのあるネットワークのネットワーク管理者は、まずにプロキシサーバに Web トラフィックを送信し、プロキシサーバが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、通信にポート 80 以外の TCP ポートを使用できます。このポートは通常は TCP ポート 3128 または 8080 です。デフォルトで、Web 認証はポート 80 だけをリッスンします。そのため、コンピュータから送信される HTTP GET は、プロキシポートに向かいますが、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、プロキシ設定を使用するように Web 認証を設定する方法について説明します。

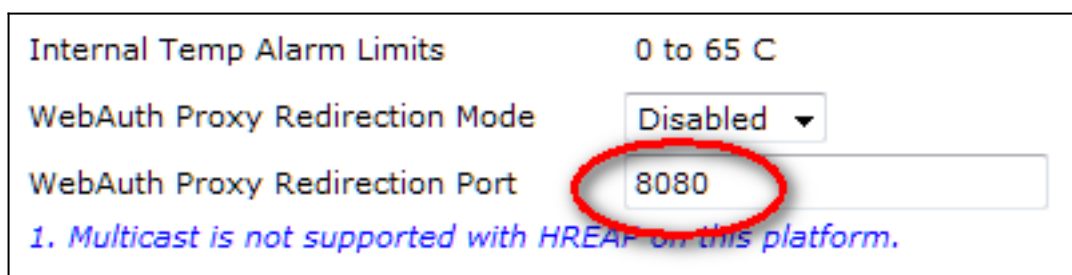
1. プロキシポートをリッスンするために Cisco Wireless LAN Controller (WLC) を設定します。
 2. 仮想 IP アドレスを直接返すように Proxy Auto-Configuration (PAC) ファイルを設定します。
 3. Web 認証の前にクライアントで PAC ファイルをダウンロードできるようにするために、事前認証のアクセスコントロールリスト (ACL) を作成します。
- 手っ取り早い解決策として、1.1.1.1 を返すように Web ブラウザを手動で設定できます。

これらのプロセスそれぞれの詳細は、次のサブセクションにあります。

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するポートに変更する方法について説明します。

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



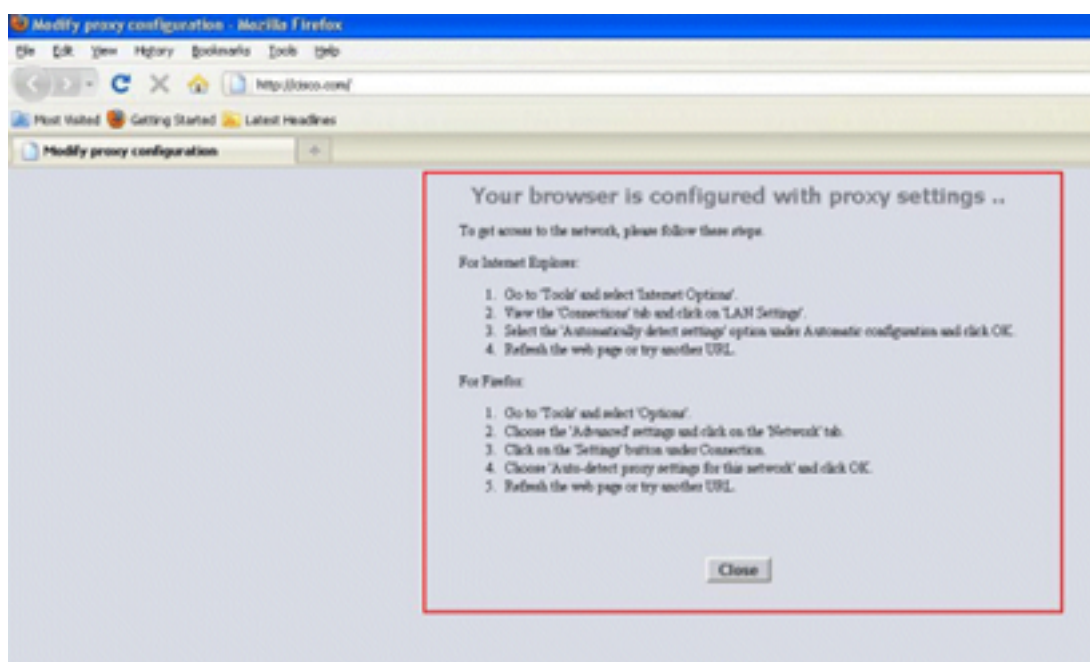
The screenshot shows a configuration page for a Cisco Wireless LAN Controller. The 'WebAuth Proxy Redirection Port' field is highlighted with a red circle and contains the value '8080'. The 'WebAuth Proxy Redirection Mode' is set to 'Disabled'. A note below the fields states: '1. Multicast is not supported with HREAP on this platform.'

2. [WebAuth Proxy Redirection Port] フィールドで、クライアントのリダイレクトのために WLC で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、1.1.1.1 (または WLC で使用他の仮想 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。「[手っ取り早い解決策： 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 を送信する場合、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ためには [WebAuth Proxy Redirection Port] にポート番号を入力します。リダイレクション モードが有効になっている場合は、プロキシ設定画面にクライアントがリダイレクトされ、自動プロキシ設定のために Web Proxy Auto-Discovery (WPAD) または PAC ファイルが動的にプッシュされることを予期します。無効の場合、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 ファイルを設定する

Web 認証でユーザを正しく認証するには、WLC の仮想 IP アドレスが「直接」返される必要があります。「直接」とは、プロキシ サーバが要求のプロキシ処理を行わず、クライアントがこの IP アドレスに直接到達するアクセス許可を持つことを意味します。これは通常、プロキシ サーバの管理者によってプロキシ サーバの WPAD または PAC ファイルに設定されます。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, "1.1.1.1")) <-- (Line states return 1.1.1 directly)
{
    return "DIRECT";
}
}
```

```
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, "1.1.1.1")) <-- (Line states return 1.1.1 directly)
{
    return "DIRECT";
}
}
```

事前認証 ACL を作成する

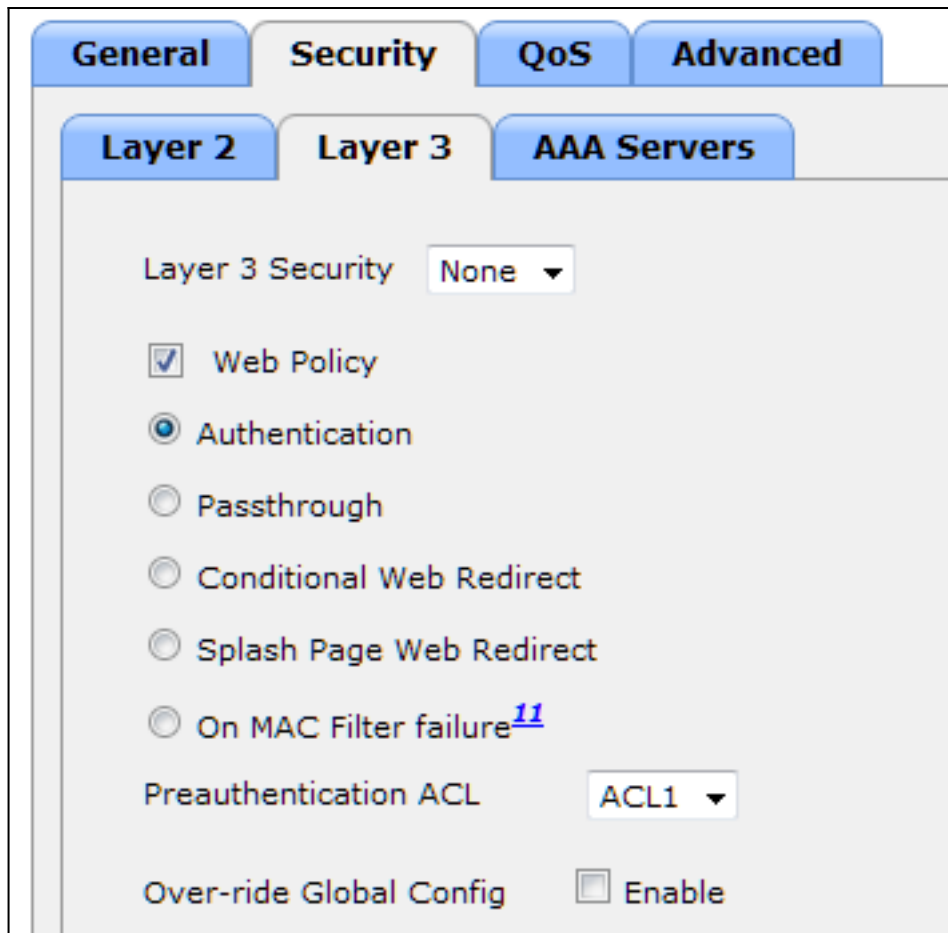
ワイヤレス クライアントが Web 認証にログインする前に、クライアントで PAC ファイルをダウンロードできるように Web 認証サービス セット識別子 (SSID) に事前認証 ACL を配置します。事前認証 ACL は PAC ファイルにあるポートにのみアクセスを許可する必要があります。プロキシ ポートへのアクセスは、クライアントが Web 認証なしでインターネットに到達できるようにします。

1. コントローラに 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 ポートでプロキシへの両方向のトラフィックを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 ポートは許可しません。

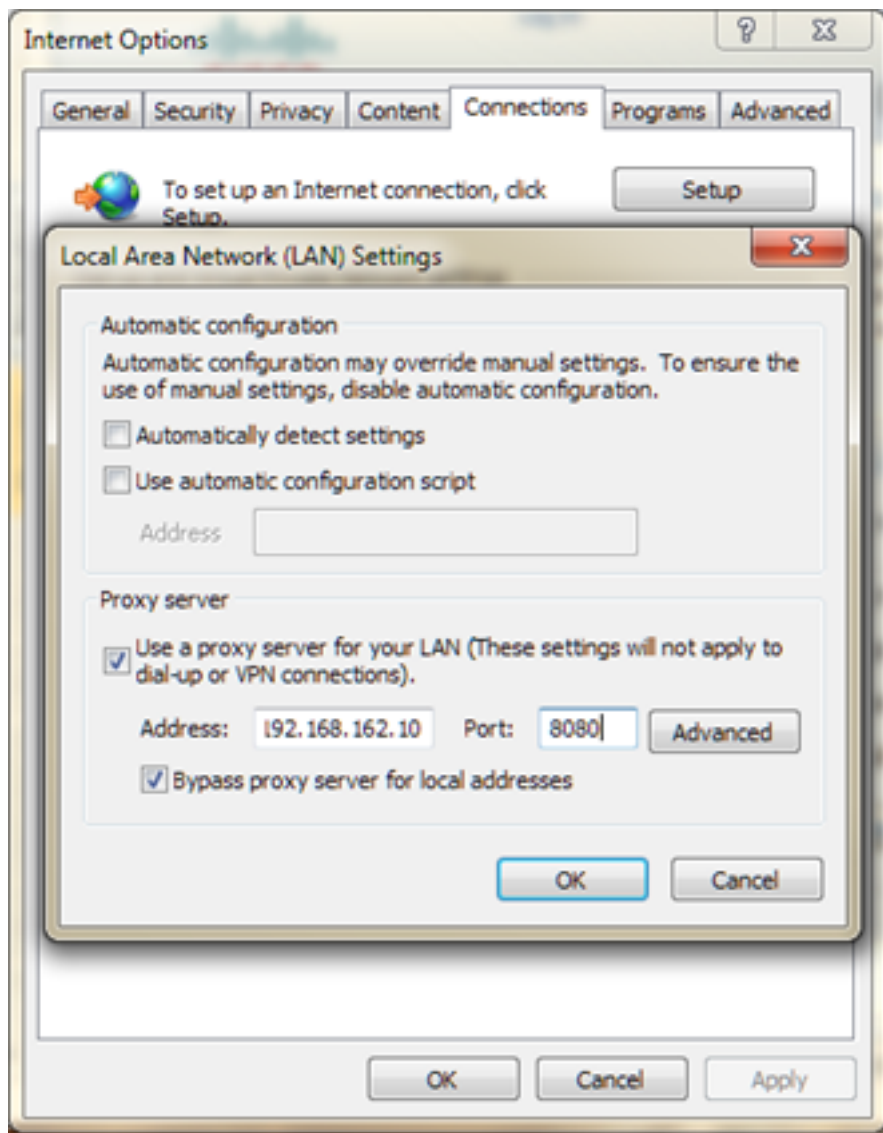
3. コントローラの WLAN 設定で、作成したばかりの ACL を事前認証 ACL として選択することを忘れないでください。



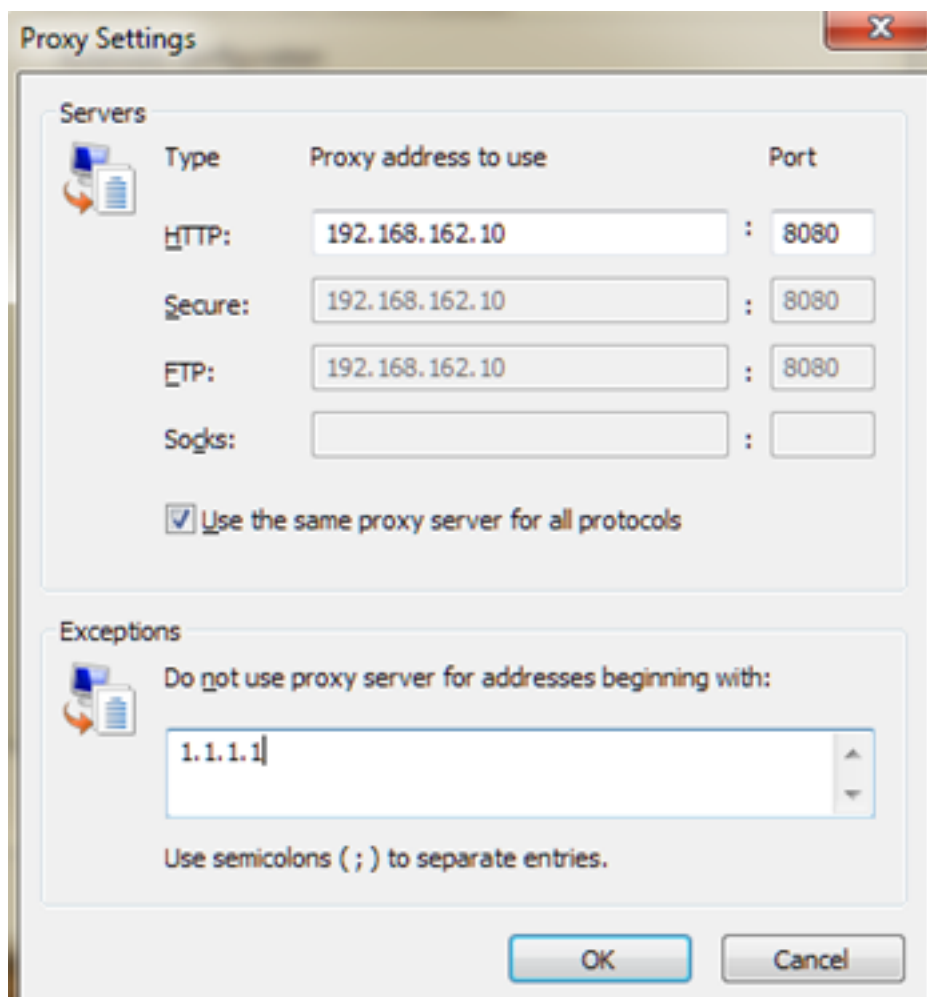
手っ取り早い解決策：Web ブラウザを設定する

この手順では、クライアントの Web ブラウザが 1.1.1.1 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 Options] の順に選択します。
2. [Connections] タブをクリックしてから [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] 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。



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

現在のところ、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ありません。

関連情報

- [テクニカル サポートとドキュメント – Cisco Systems](#)