

# FQDN ACL のコンバージしたアクセス ワイヤレス コントローラ ( 5760/3850/3650 ) BYOD クライアント Onboarding

## 目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[DNS は ACL プロセスフローを基づかせていました](#)

[設定](#)

[WLC の設定](#)

[ISE 設定](#)

[確認](#)

[参考資料](#)

## 概要

この資料は Web 認証/クライアントの間に特定のドメインリストにアクセスを許可するために DNS によって基づくアクセス リスト ( ACL ) の使用のための設定例を、完全修飾ドメイン名 ( FQDN ) ドメインリスト持って来ますコンバージしたアクセスコントローラのあなた自身のデバイス ( BYOD ) 提供状態を記述したものです。

## 前提条件

### 要件

この資料は基本的な中央 Web 認証 ( CWA ) を設定する方法を既にこれである facilitate BYOD に FQDN ドメインリストの使用を示すちょうど付加知っていると仮定します。 CWA および ISE BYOD 設定例はこの資料の終わりに参照されます。

### 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。  
Cisco Identity Services Engine ソフトウェア リリース 1.4

Cisco WLC 5760 ソフトウェア リリース 3.7.4

## DNS は ACL プロセスフローを基づかせていました

リダイレクト ACL 名前を戻す Identity Services Engine ( ISE ) に ( ACL の名前はどのトラフィックが ISE にリダイレクトされるべきで、どれが判別するのが常であり、 ) FQDN ドメインリスト名前 ( 認証の前にアクセスを可能にされるべきコントローラの FQDN URL リストにマッピング

グされる ACL の名前は )、フローそのようにあります:

1. ワイヤレス LAN コントローラ ( WLC ) は Access Point ( AP ) に URL のための DNS スヌーピングを有効にするために capwap ペイロードを送信します。
2. AP はクライアントからの DNS クエリのためにスヌーピングします。ドメイン名が許可された URL と一致する場合、AP は DNS サーバに要求を、待っています DNS サーバからの応答を転送し、ために DNS 応答を解析し、解決される最初の IP アドレスだけと転送して下さい。ドメイン名が一致する場合、DNS 応答はクライアントに戻って ( 修正なしで ) あるように転送されます。
3. ドメイン名が一致すれば、最初の解決される IP アドレスは capwap ペイロードの WLC に送信されます。WLC は次のアプローチを使用して AP から得た解決される IP アドレスの FQDN ドメインリストに暗黙のうちにマッピングされる ACL をアップデートします: 解決される IP アドレスは FQDN ドメインリストへのマッピングされた ACL の各ルールの宛先アドレスとして追加されます。またその逆にもそれから ACL を否定する割り当てからの反転する ACL gets の各ルールはクライアントに適用されます。注: このメカニズムを使うとリダイレクト ACL ルールを反転させることがトラフィックは ISE にリダイレクトする必要があることを意味する割り当てへそれらを変更することに起因するので CWA リダイレクト ACL にドメインリストをマッピングすることができません。Therefore FQDN ドメインリストは設定部品の別途の「permit ip any any」ACL にマッピングされます。ネットワーク admin がリストの cisco.com URL で FQDN ドメインリストを設定し、次の ACL にそのドメインリストをマッピングしたことをそのポイントを明白にするために、仮定して下さい:

```
ip access-list extended FQDN_ACL
permit ip any any
```

cisco.com を要求しているクライアントに AP は IP アドレス 72.163.4.161 にドメイン名 cisco.com を変換し、contoller に送信します、ACL は下記にとしてあるために修正され、クライアントに適用されます:

```
ip access-list extended FQDN_ACL
deny ip any host 72.163.4.161
```

4. クライアントが HTTP 「GET」 要求を送信する時: クライアントは ACL 割り当てトラフィックリダイレクトされます。否定された IP アドレスによって HTTP トラフィックは許可されません。
5. アプリケーションがクライアントでダウンロードされ、プロビジョニングが完了した、ISE サーバは WLC に CoA セッション 終端を送信します。
6. クライアントが WLC から非認証されれば、AP はクライアント 1 人あたりのスヌーピングのためのフラグを取除き、スヌーピングをディセーブルにします。

## 設定

### WLC の設定

1. リダイレクト ACL を作成して下さい:  
およびどのトラフィックがリダイレクトする必要があるかこの ACL がどのトラフィックが ISE にべきではないか定義するのに使用されています ( ACL で否定される ) リダイレクトす

る ( ACL で許可されて ) 。

```
ip access-list extended REDIRECT_ACL
deny udp any eq bootps any
deny udp any any eq bootpc
deny udp any eq bootpc any
deny udp any any eq domain
deny udp any eq domain any
deny ip any host 10.48.39.228
deny ip host 10.48.39.228 any
permit tcp any any eq www
permit tcp any any eq 443
```

このアクセス リストで 10.48.39.228 は ISE サーバのIPアドレスです。

2. FQDN ドメインリストを設定して下さい:このリストはクライアントが提供するか、または CWA 認証の前にアクセスできるドメイン名が含まれています。

```
passthru-domain-list URLS_LIST
match play.google.*.*
match cisco.com
```

3. permit ip any any でアクセス リストを URLS\_LIST と結合されるために設定して下さい:  
この ACL はクライアント ( スタンドアロン FQDN ドメインリストを追加できません ) に実際の IPアクセスリストを適用する必要があるので必要 FQDN ドメインリストにマッピングされるためにです。

```
ip access-list extended FQDN_ACL
permit ip any any
```

4. FQDN\_ACL に URLS\_LIST ドメインリストをマッピングして下さい:

```
access-session passthru-access-group FQDN_ACL passthru-domain-list URLS_LIST
```

5. Onboarding CWA SSID を設定して下さい:  
この SSID はクライアント中央 Web 認証のために使用され、クライアント プロビジョニング、FQDN\_ACL および REDIRECT\_ACL は ISE によってこの SSID に適用されます

```
wlan byod 2 byod
aaa-override
accounting-list rad-acct
client vlan VLAN0200
mac-filtering MACFILTER
nac
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
no shutdown
```

この SSID 設定 **MACFILTER** メソッドリストで ISE 半径グループを指すメソッドリストはあり、**radacct** は同じ ISE 半径グループを指すアカウント方式リストです。

この例で使用されるメソッドリスト 設定の要約:

```
aaa group server radius ISEGroup
server name ISE1

aaa authorization network MACFILTER group ISEGroup

aaa accounting network rad-acct start-stop group ISEGroup
```

```
radius server ISE1
  address ipv4 10.48.39.228 auth-port 1812 acct-port 1813
  key 7 112A1016141D5A5E57
```

```
aaa server radius dynamic-author
  client 10.48.39.228 server-key 7 123A0C0411045D5679
  auth-type any
```

## ISE 設定

このセクションは CWA ISE 設定部品について詳しく知っているのと、ISE 設定ですほぼ同じ仮定します次の修正と。

ワイヤレス CWA MAC アドレス 認証 バイパス ( MAB ) 認証結果は CWA リダイレクト URL と共に次の属性を戻す必要があります:

```
cisco-av-pair = fqdn-acl-name=FQDN_ACL
cisco-av-pair = url-redirect-acl=REDIRECT_ACL
```

FQDN\_ACL がある一方、ドメインリストおよび REDIRECT\_ACL にマッピングされる IP アクセスリストの名前は標準 CWA リダイレクト アクセスリストです。

Therefore CWA MAB 認証結果は下記のように設定された次であるはずはです:

The screenshot shows the ISE configuration interface. The top section is titled "Web Redirection (CWA, MDM, NSP, CPP)" and is checked. Below it, there are three input fields: "Centralized Web Auth" (dropdown menu), "ACL" (text box containing "REDIRECT\_ACL"), and "Value" (text box containing "Sponsored Guest Portal (defau..."). There are two checkboxes: "Display Certificates Renewal Message" (checked) and "Static IP/Host name" (unchecked). The bottom section is titled "Advanced Attributes Settings" and shows a configuration entry: "Cisco:cisco-av-pair" (dropdown menu) followed by an equals sign, "fqdn-acl-name=FQDN\_ACL" (dropdown menu), and a plus sign.

## 確認

FQDN ドメインリストがコマンドの下のクライアント 使用に追加されることを確認するため:

```
show access-session mac <client_mac> details
```

許可されたドメイン名を示すコマンド 出力の例:

```
5760-2#show access-session mac 60f4.45b2.407d details
  Interface:  Capwap7
  IIF-ID:  0x41BD400000002D
```

Wlan SSID: byod  
AP MAC Address: f07f.0610.2e10  
MAC Address: 60f4.45b2.407d  
IPv6 Address: Unknown  
IPv4 Address: 192.168.200.151  
Status: Authorized  
Domain: DATA  
Oper host mode: multi-auth  
Oper control dir: both  
Session timeout: N/A  
Common Session ID: 0a30275b58610bdf0000004b  
Acct Session ID: 0x00000005  
Handle: 0x42000013  
Current Policy: (No Policy)  
Session Flags: Session Pushed

Server Policies:

**FQDN ACL: FQDN\_ACL**  
**Domain Names: cisco.com play.google.\*.\***

URL Redirect: https://bruiser.wlaaan.com:8443/portal/gateway?sessionId=0a30275b58610bdf0000004b&portal=27963fb0-e96e-11e4-a30a-005056bf01c9&action=cwa&token=fcc0772269e75991be7f1ca238cbb035

URL Redirect ACL: REDIRECT\_ACL

Method status list: empty

## 参考資料

[WLC と ISE での中央 Web 認証の設定例](#)

[BYOD 無線インフラストラクチャー 設計](#)

[Chromebook オンボーディング用の ISE 2.1 を設定する](#)