

# 目次

[概要](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[レイヤ2 セキュリティ](#)

[WLAN ノー・セキュリティを開いて下さい](#)

[静的な Wired Equivalent Privacy \( WEP \)](#)

[MAC フィルタ-ローカルデータベース](#)

[MAC フィルタ-外部 Radius](#)

[ワイヤレスによって保護されるアクセス 2 \( WPA2 \) 事前共有キー \( PSK \)](#)

[802.1X ローカル Extensible Authentication Protocol \( EAP \) 認証 \( ローカル RADIUS として使用される NGWC \)](#)

[外部 Radius の 802.1X](#)

[レイヤ3 セキュリティ](#)

[Web パススルー](#)

[Web 認証 ローカル認証](#)

[外部 RADIUS 認証 \( ISE \) を用いる Web 認証](#)

[外部 Web 認証](#)

[ローカル認証を用いるカスタマイズされた Web 認証](#)

[オート固定 Web 認証](#)

## 概要

この資料は基本的な、既知レイヤ2 およびレイヤ3 Wireless LAN ( WLAN ) コンフィギュレーションにクイックレファレンス CLI コンフィギュレーションテンプレートを提供したものです。基礎テンプレートは Cisco 次世代 ワイヤリング クローゼット ( NGWC ) に速いのにコピー アンド ペーストします 5760 および 3850 ワイヤレス LAN コントローラ ( WLC ) ラボ レクリエーション および顧客 初期インストール提供されます。

## 前提条件

### 要件

Cisco は NGWC リリース 3.3 またはそれ以降のナレッジがあることを推奨します。スイッチ 仮想インターフェイス ( SVIs ) ことが期待されますおよび DHCP プール/スヌーピングは最良の方法ごとに前もって構成されます。

### 使用するコンポーネント

このドキュメントは、特定のソフトウェアやハードウェアのバージョンに限定されるものではありません。

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、クリアな（デフォルト）設定で作業を開始しています。ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。

## レイヤ 2 セキュリティ

### WLAN ノー・セキュリティを開いて下さい

### 静的な Wired Equivalent Privacy ( WEP )

### MAC フィルタ-ローカルデータベース

### MAC フィルタ-外部 Radius

### ワイヤレスによって保護されるアクセス 2 ( WPA2 ) 事前共有キー ( PSK )

### 802.1X ローカル Extensible Authentication Protocol ( EAP ) 認証 ( ローカル RADIUS として使用される NGWC )

```
user-name test
  privilege 15
  password 0 cisco
  type network-user description pass=cisco
aaa new-model
aaa authentication dot1x default local
aaa authorization credential-download author_list local
aaa authentication dot1x authen_list local
aaa local authentication authen_list authorization author_list
dot1x system-auth-control
eap profile PEAPProfile
method ?
  fast      EAP-FAST method allowed
  gtc       EAP-GTC method allowed
  leap      EAP-LEAP method allowed
  md5       EAP-MD5 method allowed
  mschapv2  EAP-MSCHAPV2 method allowed
  peap      EAP-PEAP method allowed
  tls       EAP-TLS method allowed

method peap
method mschapv2
wlan TestNGWC 1 TestNGWC
  client vlan VLAN0080
```

```
ip dhcp server 192.168.80.14
local-auth PEAPProfile
```

## 外部 Radius の 802.1X

```
user-name test
 privilege 15
 password 0 cisco
 type network-user description pass=cisco
aaa new-model
aaa authentication dot1x default local
aaa authorization credential-download author_list local
aaa authentication dot1x authen_list local
aaa local authentication authen_list authorization author_list
dot1x system-auth-control
eap profile PEAPProfile
```

### method ?

```
fast          EAP-FAST method allowed
gtc           EAP-GTC method allowed
leap         EAP-LEAP method allowed
md5          EAP-MD5 method allowed
mschapv2     EAP-MSCHAPV2 method allowed
peap         EAP-PEAP method allowed
tls          EAP-TLS method allowed
```

```
method peap
```

```
method mschapv2
```

```
wlan TestNGWC 1 TestNGWC
 client vlan VLAN0080
 ip dhcp server 192.168.80.14
 local-auth PEAPProfile
```

## レイヤ 3 セキュリティ

### Web パススルー

```
user-name test
 privilege 15
 password 0 cisco
 type network-user description pass=cisco
aaa new-model
aaa authentication dot1x default local
aaa authorization credential-download author_list local
aaa authentication dot1x authen_list local
aaa local authentication authen_list authorization author_list
dot1x system-auth-control
eap profile PEAPProfile
```

### method ?

```
fast          EAP-FAST method allowed
gtc           EAP-GTC method allowed
leap         EAP-LEAP method allowed
md5          EAP-MD5 method allowed
mschapv2     EAP-MSCHAPV2 method allowed
peap         EAP-PEAP method allowed
tls          EAP-TLS method allowed
```

```
method peap
```

```
method mschapv2
```

```
wlan TestNGWC 1 TestNGWC
```

```
client vlan VLAN0080
ip dhcp server 192.168.80.14
local-auth PEAPProfile
```

## Web 認証 ローカル認証

```
user-name test
 privilege 15
 password 0 cisco
 type network-user description pass=cisco
aaa new-model
aaa authentication dot1x default local
aaa authorization credential-download author_list local
aaa authentication dot1x authen_list local
aaa local authentication authen_list authorization author_list
dot1x system-auth-control
eap profile PEAPProfile
```

### method ?

```
fast      EAP-FAST method allowed
gtc       EAP-GTC method allowed
leap      EAP-LEAP method allowed
md5       EAP-MD5 method allowed
mschapv2  EAP-MSCHAPV2 method allowed
peap      EAP-PEAP method allowed
tls       EAP-TLS method allowed
```

```
method peap
method mschapv2
wlan TestNGWC 1 TestNGWC
 client vlan VLAN0080
 ip dhcp server 192.168.80.14
 local-auth PEAPProfile
```

## 外部 RADIUS認証 ( ISE ) を用いる Web 認証

```
user-name test
 privilege 15
 password 0 cisco
 type network-user description pass=cisco
aaa new-model
aaa authentication dot1x default local
aaa authorization credential-download author_list local
aaa authentication dot1x authen_list local
aaa local authentication authen_list authorization author_list
dot1x system-auth-control
eap profile PEAPProfile
```

### method ?

```
fast      EAP-FAST method allowed
gtc       EAP-GTC method allowed
leap      EAP-LEAP method allowed
md5       EAP-MD5 method allowed
mschapv2  EAP-MSCHAPV2 method allowed
peap      EAP-PEAP method allowed
tls       EAP-TLS method allowed
```

```
method peap
method mschapv2
wlan TestNGWC 1 TestNGWC
 client vlan VLAN0080
 ip dhcp server 192.168.80.14
 local-auth PEAPProfile
```

## 外部 Web 認証

```
user-name test
 privilege 15
 password 0 cisco
 type network-user description pass=cisco
aaa new-model
aaa authentication dot1x default local
aaa authorization credential-download author_list local
aaa authentication dot1x authen_list local
aaa local authentication authen_list authorization author_list
dot1x system-auth-control
eap profile PEAPProfile
method ?
 fast      EAP-FAST method allowed
 gtc       EAP-GTC method allowed
 leap      EAP-LEAP method allowed
 md5       EAP-MD5 method allowed
 mschapv2  EAP-MSCHAPV2 method allowed
 peap      EAP-PEAP method allowed
 tls       EAP-TLS method allowed

method peap
method mschapv2
wlan TestNGWC 1 TestNGWC
 client vlan VLAN0080
 ip dhcp server 192.168.80.14
 local-auth PEAPProfile
```

## ローカル認証を用いるカスタマイズされた Web 認証

```
ip http server
ip device tracking

aaa new-model
aaa authentication login local_webauth local
aaa authorization network default local
aaa authorization credential-download default local

username <username> password 0 <password>
```

FTP Configuration for file transfer:

```
ip ftp username <username>
ip ftp password <password>
```

Upload custom html files to flash: with command:

```
5760# copy ftp://x.x.x.x/webauth_login.html flash:
```

Example of flash content:

```
w-5760-2#dir flash:
```

```
Directory of flash:/
```

```
64649  -rw-      1164   Oct 7 2013 04:36:23 +00:00  webauth_failure.html
64654  -rw-      2047   Oct 7 2013 13:32:38 +00:00  webauth_login.html
64655  -rw-      1208   Oct 7 2013 04:34:12 +00:00  webauth_success.html
64656  -rw-        900   Oct 7 2013 04:35:00 +00:00  webauth_expired.html
64657  -rw-     96894   Oct 7 2013 05:05:09 +00:00  web_auth_logo.png
64658  -rw-     23037   Oct 7 2013 13:17:58 +00:00  web_auth_cisco.png
```

64660 -rw- 2586 Oct 7 2013 13:31:27 +00:00 web\_auth\_aup.html

```
parameter-map type webauth global
virtual-ip ipv4 1.1.1.1
```

```
parameter-map type webauth custom
type webauth
redirect on-success http://www.cisco.com
banner text ^C CC global ip for redirect ^C
custom-page login device flash:webauth_login.html
custom-page success device flash:webauth_success.html
custom-page failure device flash:webauth_failure.html
custom-page login expired device flash:webauth_expired.html
```

```
wlan cisco 1 cisco
client vlan Vlanx
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
security web-auth
security web-auth authentication-list local_webauth
security web-auth parameter-map custom
session-timeout 1800
no shutdown
```

## オート固定 Web 認証

//Verify//

**show wireless mobility summary**

<snip>

IP	Public IP	Group Name	Multicast IP	Link Status
192.168.100.8	-	ngwc	0.0.0.0	UP : UP
192.168.100.15	192.168.100.15	5760		UP : UP

```
radius server ise
address ipv4 192.168.154.119 auth-port 1812 acct-port 1813
key Cisco123
```

```
aaa group server radius rad_ise
server name ise
```

```
aaa authentication login ext_ise group rad_ise
parameter-map webauth global
virtual-ip ipv4 1.1.1.1
parameter-map type webauth test_web
type webauth
banner
```

WLAN configs on the Foreign 5760

```
wlan ngwc_guest 3 ngwc_guest
client vlan 254
mobility anchor 192.168.100.8 //Anchor
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
```

```
security web-auth
security web-auth authentication-list wcm_local
security web-auth parameter-map test_web
no shutdown
```

WLAN configs on the Anchor 5760

```
wlan ngwc_guest 3 ngwc_guest
client vlan 254
mobility anchor 192.168.100.8 //Local
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
security web-auth
security web-auth authentication-list rad_ise
security web-auth parameter-map test_web
no shutdown
```