ConvergedAccessConsolidatedQuickReference Templates for Wireless LAN

This document describes the CLI configuration templates for basic and known Layer 2 and Layer 3 WLANs configurations. The configuration templates are used for the lab recreations and customer initial installations of Cisco Catalyst 3850 Series Switches.

- Prerequisites, page 1
- Configuration Templates for Layer 2 Security, page 2
- Configuration Templates for Layer 3 Security, page 4

Prerequisites

- We recommend that you have a basic knowledge and understanding of Converged Access Release 3.3 or later.
- Switch Virtual Interfaces (SVIs) and DHCP pools or snooping must be configured.

Supported Platforms and Releases

This document is not restricted to specific software and hardware versions.

Note The information in this document refers to devices in a specific lab environment. Descriptions of the devices is provided with default configuration values. If you are on a live network, you must understand the potential impact of all the commands.

Configuration Templates for Layer 2 Security

Open WLAN No Security Template

The following is the template for Open WLAN No Security:

```
wlan 1 name testwlan ssid testwlan
client vlan 20
no security wpa
no shutdown
```

Static Wired Equivalent Privacy Template

The following is the template for Static Wired Equivalent Privacy (WEP):

```
wlan staticWEP 6 staticWEP
client vlan 79
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
security static-wep-key encryption 40 ascii 0 Cisco 1
session-timeout 1800
no shutdown
```

MAC Filter - Local Database Template

The following is the template for MAC Filter - Local Database:

```
username 24770319eB75 mac

aaa new-model
aaa authorization network test_mac local

wlan macfiltering 6 macfiltering
client vlan Vlan7
mac-filtering test_mac
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
no shutdown
```

MAC Filter - External RADIUS Template

The following is the template for MAC Filter - External RADIUS:

```
aaa new-model
aaa group server radius wcm_rad

server name RAD_EXT
subscriber mac-filtering security-mode mac
mac-delimiter colon

radius server RAD_EXT
address ipv4 x.x.x.x auth-port 1812 acct-port 1813
key cisco
```

```
aaa authorization network wcm_macfilter group wcm_rad

wlan macfiltering 1 macfiltering
client vlan Vlan7
mac-filtering wcm_macfilter
no security wpa
no security wpa akm dot1x
no security wpa wpa2
no security wpa wpa2 ciphers aes
no shutdown
```

Wireless Protected Access 2 Pre-Shared Key Template

The following is a template for Wireless Protected Access 2 (WPA2) Pre-Shared Key (PSK):

```
wlan wpa2psk 1 wpa2psk
client vlan 20
no security wpa akm dot1x
security wpa akm psk set-key ascii 0 Cisco123
no shutdown
```

802.1x Local Extensible Authentication Protocol Authentication Template

The following is the template for 802.1x Local Extensible Authentication Protocol (EAP):

```
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 TestCONVERGEDACCESS 1 TestCONVERGEDACCESS
 client vlan VLAN0080
 ip dhcp server 192.0.2.14
 local-auth PEAPProfile
```

802.1x on External RADIUS Template

The following is the template for 802.1x on External RADIUS:

```
aaa new-model
  !
  !
  aaa group server radius ACS
   server name ACS
  !
  aaa authentication dot1x ACS group ACS
```

```
  radius server ACS
   address ipv4 203.0.113.50 auth-port 1645 acct-port 1646
   key Cisco123


dot1x system-auth-control

wlan EAPFAST 4 EAPFAST
   client vlan VLAN0020
   security dot1x authentication-list ACS
   session-timeout 1800
   no shutdown
```

Configuration Templates for Layer 3 Security

Web Passthrough Template

The following is the template for Web Passthrough:

```
parameter-map type webauth global
 type consent
 virtual-ip ipv4 192.0.2.1
 !
 !
 parameter-map type webauth web
 type consent


 wlan Webauth 9 Webauth
  client vlan VLAN0020
  no security wpa
  no security wpa akm dot1x
  no security wpa wpa2
  no security wpa wpa2 ciphers aes
  security web-auth
  security web-auth parameter-map web
  session-timeout 1800
```

Local Authentication Template

The following is the template for Local Web Authentication:

```
 aaa new-model
 aaa authentication login wcm_local local
 aaa authorization network default local
 aaa authorization credential-download default local
 username test password 0 test12345
 parameter-map type webauth global
         virtual-ip ipv4 1.1.1.1
 parameter-map type webauth test_web
            type webauth
            banner    c test webauth c
 ip http server
 ip http authentication local
 ip http secure-server

 wlan local_webauth 11 local_webauth
  client vlan 263
  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
```

Web Authentication with External RADIUS Authentication Template

The following is the template for Web Authentication and External RADIUS Authentication:

```
radius server ise
       address ipv4 192.0.2.119 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 type webauth global
          virtual-ip ipv4 1.1.1.1
parameter-map type webauth test_web
           type webauth
           banner    c test webauth c
wlan local_webauth 11 local_webauth
 client vlan 263
 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 ext_ise
 security web-auth parameter-map test_web
 no shutdown
```

External Web Authentication Template

The following is the template for External Web Authentication:

```
//Parameter Map   //
       parameter-map type webauth test_web
       type webauth
       redirect for-login https: //192.0.2.119:8443 /guestportal
/portals/external_webauth/portal.jsp

       redirect portal ipv4 192.0.2.119

           redirect on-success <url> //Optional//
       redirect on-failure <url> //Optional//

       banner

//Pre auth ACL//
 ip access-lists extended preauth_ise
       10 permit udp any eq bootps any
       20 permit udp any any eq bootpc
       30 permit udp any eq bootpc any
       40 permit udp any any eq domain
       50 permit udp any eq domain any
       60 permit ip any host 192.0.2.119
       70 permit ip host 192.0.2.119 any
wlan external_webauth 11 external_webauth
 client vlan 263
 ip access-group web preauth_ise
 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 ext_ise
 security web-auth parameter-map test_web
 no shutdown
```

Customized Local Web Authentication Template

The following is the template for Customized Web Authentication with Local Authentication:

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

 Example of flash content:
Device# 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
```

Auto Anchor Web Authentication Template

The following is the template for Auto Anchor Web Authentication:

```
 //Verify//
 show wireless mobility summary
 <snip>

IP               Public IP        Group Name       Multicast IP     Link Status
-------------------------------------------------------------------------------
```

```
192.168.100.8    -               CONVERGEDACCESS    0.0.0.0          UP   : UP
192.168.100.15   192.168.100.15   5760                                UP   : UP

 radius server ise
               address ipv4 192.0.2.119 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 convergedaccess_guest 3 convergedaccess_guest
  client vlan 254
  mobility anchor 192.0.2.8   //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 convergedaccess_guest 3 convergedaccess_guest
  client vlan 254
  mobility anchor 192.0.2.8 //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
```