NGWC – Configure PSK and 802.1X SSID
3850 and 5760

Viten Patel – RTP Wireless TAC
CCIE # 37808
May 14, 2012
Agenda

• Configure SSID using PSK security
• Configure SSID using 802.1X security
SSID – PSK security

• Using GUI
  • Go to Configuration > WLANS > New
SSID – PSK security

- Using GUI
- Enter the WLAN ID, SSID and Profile Name and hit Apply
SSID – PSK security

- Using GUI

- Click on the WLANs tab which will bring you back to the summary page. The SSID will be tied to VLAN 1 and will be disabled by default.
SSID – PSK security

• Using GUI

• Click on the SSID to edit the configuration. Assign the correct interface/VLAN, enable the status and set the pre-shared key to be used (PSK) and hit apply.
SSID – PSK security

• Using GUI
SSID – PSK security

• Using CLI

wlan viten_psk 14 viten_psk  #profile name, WLAN id and SSID name
client vlan Viten  #Set the client interface/VLAN
no security wpa akm dot1x  #disable dot1x which is set by default
security wpa akm psk set-key ascii 0 test12345  #set the pre-shared key
session-timeout 1800  #session timeout which is set by default
no shutdown  #enable the SSID

• Note: the default commands are hidden. For example, the above SSID uses WPA2/ AES and the command which enables that is hidden since that is the default method

security wpa wpa2 ciphers aes
SSID – PSK security

• Viewing Client Details

• Click on Monitor > Clients and click on the mac address

![Image of Wireless Controller interface with Client Details expanded and a client entry displayed]
## SSID – PSK security

- Viewing Client Details

<table>
<thead>
<tr>
<th><strong>Client Properties</strong></th>
<th><strong>AP Properties</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Mac Address</td>
<td>AP Address</td>
</tr>
<tr>
<td>IPv4 Address</td>
<td>AP Name</td>
</tr>
<tr>
<td>IPv6 Address</td>
<td>AP Type</td>
</tr>
<tr>
<td>User Name</td>
<td>Wlan Profile</td>
</tr>
<tr>
<td>Port Number</td>
<td>Status</td>
</tr>
<tr>
<td>Interface</td>
<td>Association ID</td>
</tr>
<tr>
<td>VLAN ID</td>
<td>802.11 Authentication</td>
</tr>
<tr>
<td>CCX Version</td>
<td>Reason Code</td>
</tr>
<tr>
<td>E2E Version</td>
<td>Status Code</td>
</tr>
<tr>
<td>Mobility Role</td>
<td>CF Pollable</td>
</tr>
<tr>
<td>Policy Manager State</td>
<td>CF Pollable Request</td>
</tr>
<tr>
<td>Management Frame Protection</td>
<td>Short Preamble</td>
</tr>
<tr>
<td>Uptime (sec)</td>
<td>PBCC</td>
</tr>
<tr>
<td>Power Save Mode</td>
<td>Channel Agility</td>
</tr>
<tr>
<td>Current TxRateSet</td>
<td>Re-Authentication Timeout</td>
</tr>
<tr>
<td>Data RateSet</td>
<td>Remaining Re-Authentication Timeout</td>
</tr>
</tbody>
</table>

- Viewing Client Details

- Viewing AP Properties
SSID – 802.1X security

• Adding RADIUS server
  • Define RADIUS server(s)
  • Create RADIUS group(s)
  • Create Method list to call under the SSID
SSID – 802.1X security

• Define RADIUS Server(s)
• Click on Configuration > Security
SSID – 802.1X security

• Define RADIUS Server(s)
• Click on RADIUS > Servers > New
SSID – 802.1X security

- Define RADIUS Server(s)
- Add details for the RADIUS server and hit apply
SSID – 802.1X security

• Define RADIUS Group(s)

• Under the SECURITY tab, click on Server Groups > Radius > New
SSID – 802.1X security

• Define RADIUS Group(s)

• Name the Server Group and you will see a list of available RADIUS servers. In this example RADIUS server ‘ISE’ is the only server which was added. Select the RADIUS server(s) which need to be the part of this server group and add them as assigned servers.
SSID – 802.1X security

• Method Lists
  
  SECURITY > AAA > Method Lists
  
  There are 4 types of method lists but for 802.1X authentication, Method List type ‘Authentication’ is needed. Click new to create a new list.
SSID – 802.1X security

• Method Lists

• Name the method list, select the type (for layer 2 802.1X authentication select dot1x) and select group type (here the group ‘ISE_group’ which was previously created shows up in the available server group list).
SSID – 802.1X security

• Method Lists

• Method list summary page
SSID – 802.1X security

- WLAN Config
- Wireless > WLAN > WLANs > New
SSID – 802.1X security

- WLAN Config

![WLAN Configuration Screen](image-url)
SSID – 802.1X security

• WLAN Config

• Set the layer 2 authentication to dot1x
SSID – 802.1X security

• WLAN Config

• Under the AAA servers tab select the appropriate method list. For example the method list which was created earlier ‘Viten_dot1x’.
SSID – 802.1X security

• CLI

• aaa authentication dot1x Viten_dot1x group ISE_Group

  # Viten_dot1x is the method list which calls the RADIUS server group ‘ISE_Group’

• aaa group server radius ISE_Group

  server name ISE

  # Define the RADIUS server group and select the RADIUS server(s)

• radius server ISE

  address ipv4 192.168.154.119 auth-port 1813 acct-port 1812

  key ww-wireless

  # Define the RADIUS server for example server named ‘ISE’
SSID – 802.1X security

• CLI

• Wlan configs

wlan Viten_dot1x 15 Viten_dot1x
client vlan Viten
security dot1x authentication-list Viten_dot1x
session-timeout 1800
no shutdown
Debug and Show commands

- Debug aaa authentication
- Debug radius authentication
- Debug client mac-address <mac>
- Show run aaa
- Show wireless client mac-address <mac> detail
Thank You

Viten Patel (CCIE #37808)
Cisco Wireless TAC