```
no captive-portal-cert
captive-portal-cert ServerCert2
```

Using the WebUI to Configure Split Tunnel Captive Portal

1. Navigate to the **Configuration > Security > Authentication > L3 Authentication** window.
2. Select **Captive Portal Authentication Profile**.
3. Enter the name for a new captive portal authentication profile in the text box, then click **Add**.
4. Double click on the new profile name to launch the **Captive Portal Profile Authentication > your_profile_name** window.
   a. Enable user login and/or guest login, and configure other parameters as desired. (For a complete description of these parameters, see Table 7).
   b. Click **Apply**.
5. Select the Server Group under the captive portal authentication profile you just configured.
   a. Use the drop-down list to select your server group (for example **radius)**.
   b. Click **Apply**.
6. Navigate to **Security > Access Control > User Roles Tab > Add Role** and create the new user-role "splitcp-logon".
7. Assign the pre-defined firewall policy "logon-control" to position one and the policy "captiveportal" to position two for this user role.
8. Assign the captive portal profile created in step 3.
   a. Select the **AAA Profiles** tab.
   b. Click **Add** at the bottom of the AAA Profile Summary and enter the profile name you created in step 3. Click **Add**.
   c. Double click on the AAA profile you just created.
   d. Select **splitcp-logon** from the **Initial Role** drop-down list.
   e. Click **Apply**.
9. Navigate to the **Configuration > Wireless > AP Configuration** window. Select either the AP Group or AP Specific tab. Click **Edit** for the applicable AP group name or AP name.
10. In the **Profiles** list, expand the **Wireless LAN** menu, then select **Virtual AP**.
11. Select **NEW** from the **Add a profile** drop-down list to create a new virtual AP profile. Enter a name for the virtual AP profile and then click **Add**.
    a. In the Profile Details window for the Virtual APs, select your recently created AAA profile from the **AAA Profile** drop-down list. A pop-up window displays the configured AAA profile parameters. Click **Apply** in the pop-up window.
    b. From the **SSID profile** drop-down list, select **NEW**.
    c. Enter the name for the SSID profile.
    d. Enter the Network Name for the SSID.
    e. Click **Apply** in the pop-up window.
    f. At the bottom of the Profile Details window, click **Apply**.
12. Click the new virtual AP name, in the Profiles list or in the Profile Details window, to its display configuration parameters.
    a. Select the **Virtual AP enable** check box.
    b. Select **split-tunnel** from the **Forward mode** drop-down list.
    c. In the **VLAN** section, select the ID number of the VLAN to which users are assigned (for example, **20**).

d. Click **Apply**.

Using the CLI to Configure Split Tunnel Captive Portal

1. Create a captive portal profile, assigning the post-captive portal role and server group.

```
aaa authentication captive-portal <CP_Profile_name>
   default-role "rapuser"
   server-group "radius"
```

2. Create a pre-captive portal user-role (initial-role) and then apply the captive portal profile created in step 1.

```
user-role splitcp-logon
    captive-portal <CP_Profile_name>
    session-acl logon-control
    session-acl captiveportal
```

3. Apply the pre-captive portal role (created in step 2) to the AAA profile as the initial-role.

```
aaa profile <AAA_Profile_name>
   initial-role "splitcp-logon"
   aaa authentication dot1x default
!
```

4. Create an SSID profile.

```
wlan ssid-profile <SSID_Profile_name>
   essid "split-tunnel-cp"
   opmode wpa2-psk-aes
   wpa-passphrase <some_wpa_passphrase>
```

5. Create a Virtual AP profile and apply the AAA profile and SSID profile to it.

```
wlan virtual-ap <Virtual-AP_Profile_name>
   vlan 30
   aaa-profile <AAA_Profile_name>
   ssid-profile <SSID_Profile_name>
   forward-mode split-tunnel
```

6. Apply this configuration to the ap-group/ap-name

```
ap-group <AP_Group_Name>
   virtual-ap <Virtual-AP_Profile_name>
```

Modifying Guest Captive Portal User Role

When you define a captive portal guest login role, users are assigned to that role after guest login from captive portal. Typically this role allows guest users to obtain DHCP from corporate networks as well as all other traffic (such as DNS, DHCP, ICMP) routed on their local network to the remote AP. If user's defined role is not specified in the AAA profile, the standard *guest* role is applied to the user.

Using the WebUI to modify and apply the split-tunnel captive portal guest role

1. Navigate to the **Configuration > Security > Authentication > L3 Authentication** window.
2. Create a new role "splitcp-guest".
3. Add firewall policies to this role by selecting Add to create a new firewall policy that permits DHCP, route src-nat HTTP, HTTPS, DNS and ICMP traffic.
4. Click Apply (at the bottom right of the window) to apply this firewall policy to the user role.
5. Navigate to Captive portal configuration **Security > Authentication > L3 Authentication** and select a role from the **Default Guest Role** drop-down list.

Using the CLI to create a split-tunnel captive portal guest role

Using the CLI to create split-tunnel captive portal guest role.

1. Create a firewall policy.

```
ip access-list session splitcp-guest
   any any svc-dhcp permit
   any any svc-dns route src-nat
   any any svc-icmp route src-nat
   any any svc-http route src-nat
   any any svc-https route src-nat
!
```

2. Apply firewall policy to user role

```
user-role splitcp-guest
session-acl splitcp-guest
!
```

3. Apply this role to default-guest-role of captive portal profile.

```
aaa authentication captive-portal "PROFILE_NAME"
default-guest-role "splitcp-guest"
   guest-logon
```

Captive Portal Configuration Parameters

Table 7 describes the configuration parameters on the WebUI Captive Portal Authentication profile window.

In the CLI, you configure these options with the **aaa authentication captive-portal** commands.

Table 7 *Captive Portal Authentication Profile Parameters*

Parameter	Description
Default role	Role assigned to the Captive Portal user upon login. When both user and guest logon are enabled, the default role applies to the user logon; users logging in using the guest interface are assigned the default-guest-role. The Policy Enforcement Firewall license must be installed. Default: guest
default-guest-role	Role assigned to the Captive Portal guest users that logon using the guest interface are assigned this role by default. The Policy Enforcement Firewall license must be installed.
Redirect Pause	Time, in seconds, that the system remains in the initial welcome page before redirecting the user to the final web URL. If set to 0, the welcome page displays until the user clicks on the indicated link. Default: 10 seconds.
User Login	Enables Captive Portal with authentication of user credentials. Default: enabled
Guest Login	Enables Captive Portal logon without authentication. Default: disabled
Logout popup window	Enables a pop-up window with the Logout link for the user to logout after logon. If this is disabled, the user remains logged in until the user timeout period has elapsed or the station reloads. Default: enabled
Use HTTP for authentication	Use HTTP protocol on redirection to the Captive Portal page. If you use this option, modify the captiveportal policy to allow HTTP traffic. Default: Disabled (HTTPS is used)

Table 7 *Captive Portal Authentication Profile Parameters (Continued)*

Parameter	Description
Logon wait minimum wait	Minimum time, in seconds, the user will have to wait for the logon page to pop up if the CPU load is high. This works in conjunction with the Logon wait CPU utilization threshold parameter. Default: 5 seconds.
Logon wait maximum wait	Maximum time, in seconds, the user will have to wait for the logon page to pop up if the CPU load is high. This works in conjunction with the Logon wait CPU utilization threshold parameter. Default: 10 seconds.
Logon wait CPU utilization threshold	CPU utilization percentage above which the Logon wait interval is applied when presenting the user with the logon page. Default: 60%
Max authentication failures	Maximum number of authentication failures before the user is blacklisted. Default: 0
Show FQDN	Allows the user to see and select the fully-qualified domain name (FQDN) on the login page. Default: disabled
Use CHAP	Use CHAP protocol. You should not use this option unless instructed to do so by an Aruba representative. Default: PAP
Sygate-on-demand-agent	Enables client remediation with Sygate-on-demand-agent (SODA). Default: disabled
Login page	URL of the page that appears for the user logon. This can be set to any URL. Default: /auth/index.html
Welcome page	URL of the page that appears after logon and before redirection to the web URL. This can be set to any URL. Default: /auth/welcome.html
Show Welcome Page	Enables the display of the welcome page. If this option is disabled, redirection to the web URL happens immediately after logon. Default: Enabled
Proxy Server Configuration	Configures IP address and port number for proxy server. **NOTE**: This option is only available in the base operating system. Default: N/A
Adding switch ip address in redirection URL	Sends the controller's IP address in the redirection URL when external captive portal servers are used. An external captive portal server can determine the controller from which a request originated by parsing the 'switchip' variable in the URL. Default: disabled