WiNG 5 Feature Guide

Integrating with 3rd Party Captive Portals

Published: April 2017

Extreme Networks, Inc.
Phone / +1 408.579.2800
Toll-free / +1 888.257.3000

www.extremenetworks.com

P/N XXXXX-XX

Contents

Overview

This guide will focus on integrating WiNG 5 Captive Portal service with 3rd party Captive Portal solutions. In such scenarios WiNG 5 Controllers or Access Points will provide capture and redirection of the guest user to the external Captive Portal Server, which can provide different types of access, like RADIUS authentication, guest self-registration, secure onboarding etc. WiNG5 architecture is very flexible and allows to integrate with virtually any guest access scenario.

It is assumed that the reader is familiar with main WiNG 5 concepts and WiNG 5 Captive Portal in general, which are covered in the "*WiNG5 How To Captive Portals*" guide.

Externall Hosted Pages

The captive portal login, registration, welcome, failed and agreement pages can be hosted on an external HTTP server. This is useful for large scale deployments when complex customized pages need to be deployed or external captive portal is providing registration, billing and guest analytics services.

To enable externally hosted pages the web page source in the captive portal policy is set to Externally Hosted and the URLs are defined for each page type. The URL can include the IPv4 address or FQDN of the server hosting each page as well as the path and page name.

There are few important things that need special care when using externally hosted pages:

1. Captive Portal Policy mappings and server mode selection

   The principle is the same as when using internally hosted captive portal pages, i.e. the important decision to make is to choose centralized vs Distributed architecture approach, or in other words select if the Wireless Controller or Cluster or Wireless Controllers will perform capture and redirection, or each Access Point will perform capture and redirection right from the edge of the network.

2. DNS Whitelist

   By default, a captive portal will only permit limited access to the network for unauthenticated devices. To permit access to the externally hosted pages a DNS whitelist policy must be defined and assigned to the captive portal policy. The DNS whitelist can include the IPv4 addresses and/or hostnames of the external hosts that needs to be allowed for guest authentication. This provides a walled garden for unauthenticated devices as it permits access only to the web servers used for guest onboarding until the user has been granted full access to the guest network.

3. Client-side scripting on the Captive Portal pages

   Client-side scripts (e.g. JavaScript, PHP) are used to pass information to a WiNG 5 device that is doing capture and redirection. Client-side script will be invoked after the client will submit an HTML form (for example it can be username and password combination or a full form with user details for guest self-registration). After the script is executed on the client side, the client will send an HTTP POST message to the WiNG 5 device that is doing capture and redirection providing information from the HTML form that in turn will invoke an action depending on the access type. This guide will cover common use-case scenarios.

4. Additional information that WiNG 5 device can pass to the external server when performing client redirection inside the HTTP GET request (Query tags)

   For example, client MAC address, IP address, RF Domain of the Access Point, SSID name, etc.

DNS Whitelist

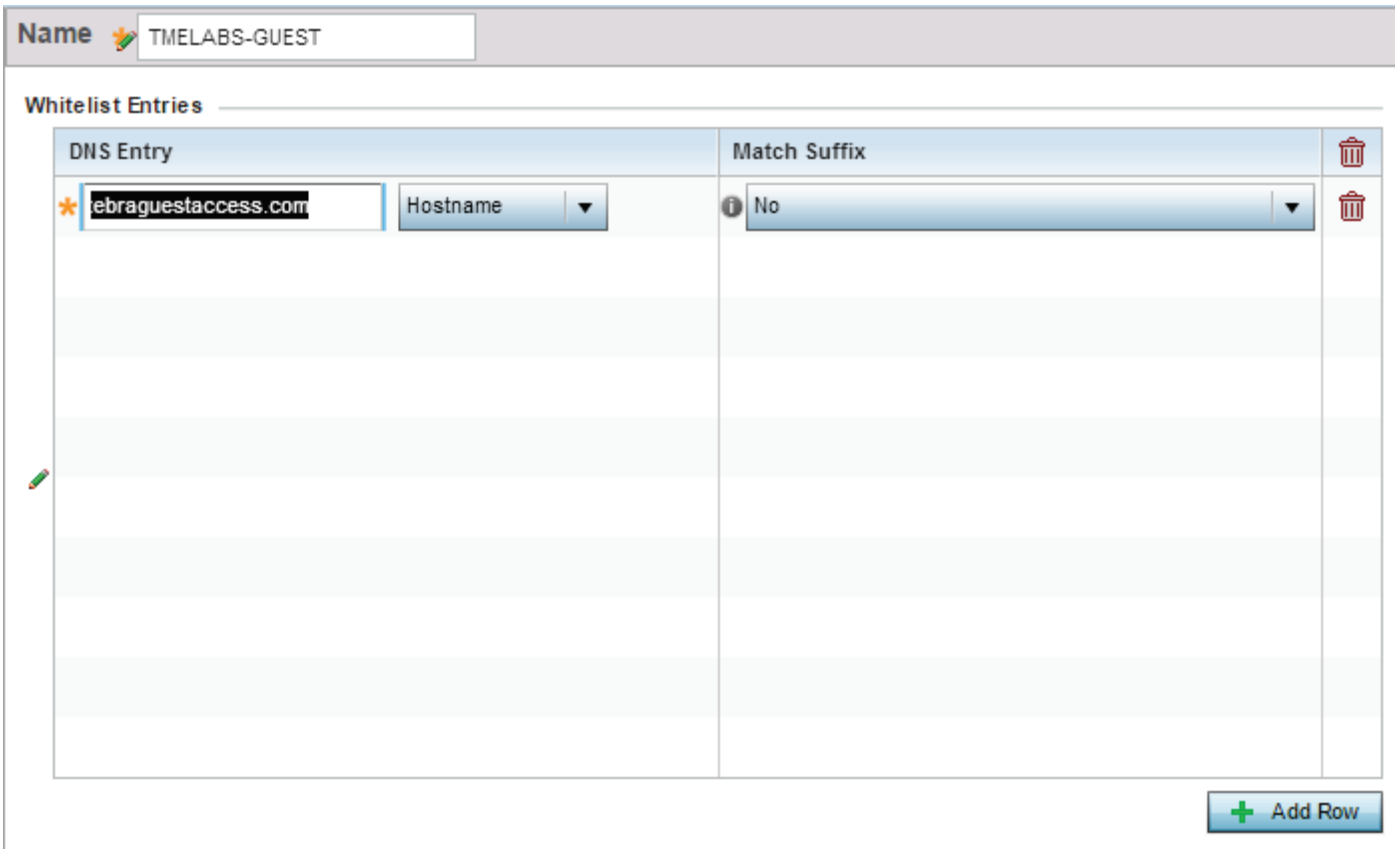
The DNS Whitelist policy includes the IP addresses or FQDNs of one or more HTTP servers hosting the customized content. Once assigned captive portal users sessions can be re-directed to the permitted external hosts. Access to non-permitted hosts will still be denied. This capability is often referred to as a **walled garden**.

DNS Whitelist must permit all externally hosted pages, as well as all other referenced sites inside captive portal pages, for example advertisements portals, images from external sources, social wifi login portals for Facebook/Google login etc.

Note
DNS ALG in the firewall policy must be enabled for DNS whitelist to work.

GUI Configuration

Configuration -> Services -> Captive Portals -> DNS Whitelist -> Add:



CLI Configuration

```
!
dns-whitelist TMELABS-GUEST
 permit portal.extremeguestaccess.com
 permit extreme.com
 permit fbcdn.net suffix
 permit akamaihd.net suffix
!
```

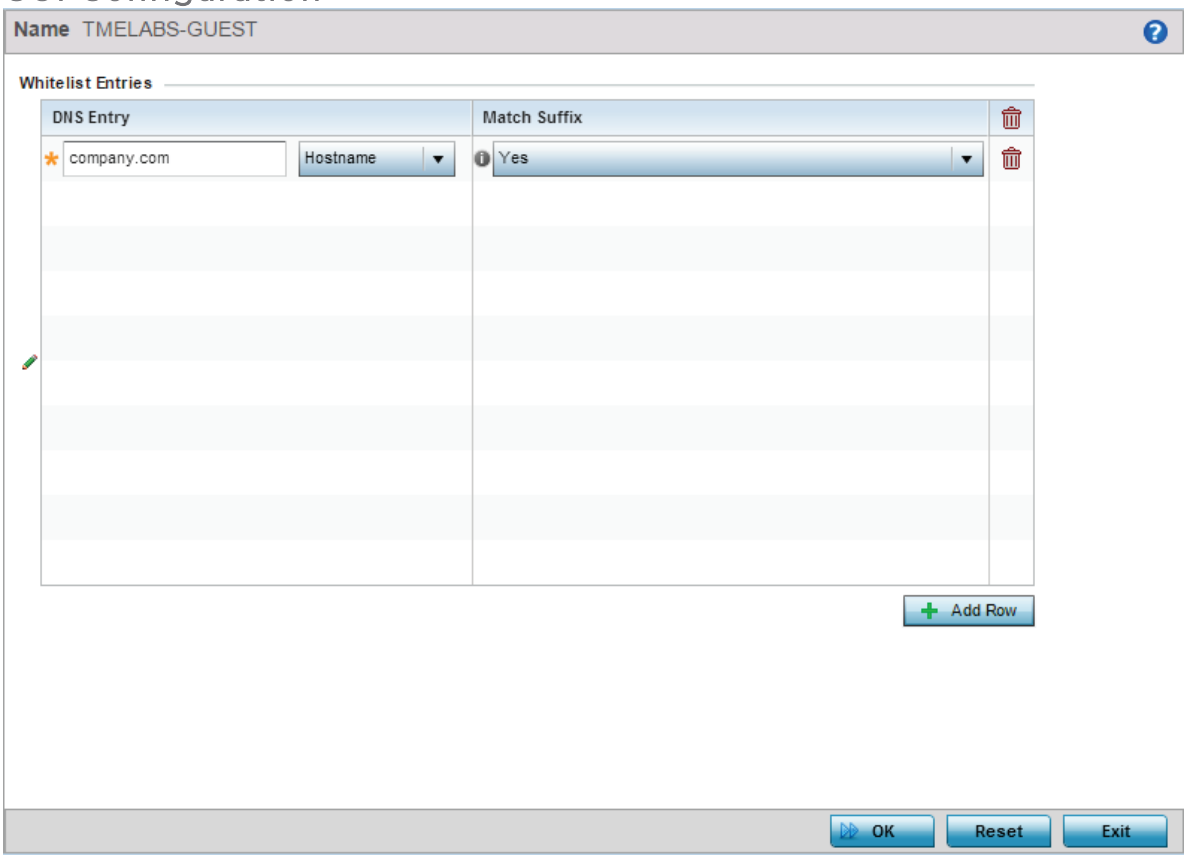
DNS Whitelist Suffix Options

WiNG 5 DNS Whitelist implementation allows usage of FQDN suffix to summarize permit rules.

For example, if the requirement is to permit all the front pages of the customer with domain name company.com which may include multiple sites like login.company.com, shop.company.com, news.company.com etc, then all these entries can be summarized using Match Suffix option.

The example below will allow all the FQDNs that will include company.com as a suffix, or a wildcard of *.company.com:

GUI Configuration



CLI Configuration

```
!
dns-whitelist TMELABS-GUEST
 permit company.com suffix
!
```

Scripting on the Captive Portal Pages

Terms & Agreement (access-type no-auth & terms agreement)

With access-type configured as no-auth and terms-agreement enabled, a device that is performing capture and redirection (an Access Point or a Controller) will redirect unauthenticated guest user to the agreement page specified under Captive Portal policy:

```
!
captive-portal EXTERNAL-TERMS-AGREEMENT
 access-type no-auth
 terms-agreement
 webpage-location external
 webpage external agreement http://192.168.10.5:880/agreement.html
 use dns-whitelist WALLED-GARDEN
!
dns-whitelist WALLED-GARDEN
 permit 192.168.10.5
!
```

During redirection WiNG 5 device will ask the client to add this additional information as a minimum to the HTTP GET request to the captive portal pages:

```
http://portal.guestaccess.com/agreement.html?hs_server=1.1.1.1&Qv=it_qpmjdz=FYU.UD@bbb_qpmjdz=@dmjfou_njou=
23:9912375@dmjfou_nbd=21.5B.8E.C8.C5.DG@ttje=BMQIBOFU@bq_nbd=95.35.9E.7B.33.81
```

In the above example client will attach hs_server address ("hotspot server" or IP/FQDN of the WiNG 5 device that is doing capture and redirection) and Qv variable (identifier of unique client session) to the HTTP GET request when being redirected to the external Web server.

This information need to be captured later on to maintain communication with WiNG captive portal. Additionally it is required to inform the WiNG 5 Captive Portal that guest user has acknowledged terms and conditions. In order to do this it is necessary to either:

a. Provide the user with a HTML page where they can tick the box that the user agrees to the terms & conditions and click submit.
b. Create PHP/Java script on the external web server's page to prepare HTML form and automatically POST the content from client's browser on the user's behalf to the WiNG 5 captive portal server.

Sample javascript to get hs_server and Qv variables can be found in the default internal agreement.html page.

Sample JavaScript to get QV variable and hs_server:

```
<script>
// function to get the query parameter value from URL query string.
function getQueryVariable(variable) {
  var query = window.location.search.substring(1);
  var vars = query.split(/[?&]/);
  for (var i=0;i<vars.length;i++) {
    var pair = vars[i].split("=");
    if (pair[0] == variable) {
        if (pair[0] == "Qv") {
            return vars[i].substr(3, vars[i].length);
        }
        return pair[1];
    }
  }
  return "";
}

var user = getQueryVariable("user");
if (user != "") {
        var user_dec = decodeURIComponent(user);
        document.getElementById('user').innerHTML = 'Welcome ' + user_dec;
}

function getCurrTime(){
    document.getElementById('frmLogin').elements['f_curr_time'].value = Math.floor(new Date().getTime() /
1000);
}

var hs_server = "NONE";
var port = 880;
var postToUrl = "/cgi-bin/hslogin.cgi";
hs_server = getQueryVariable("hs_server");
Qv = getQueryVariable("Qv");
cpstats_iframe = "http://cpstats." + hs_server + "/cp_stats.html";
postToUrl = ":" + port + postToUrl;

document.getElementById("f_hs_server").value = hs_server;
document.getElementById("f_Qv").value = Qv;
document.getElementById("frmLogin").action = "http://" + hs_server + postToUrl;
</script>
```

A sample HTML form can also be found in default agreement.html page that prepares the form for the client and initiates an HTTP POST from the client when the user is clicking "I Agree" button:

Sample HTML form to silently initiate HTTP POST after user presses "I Agree" button:

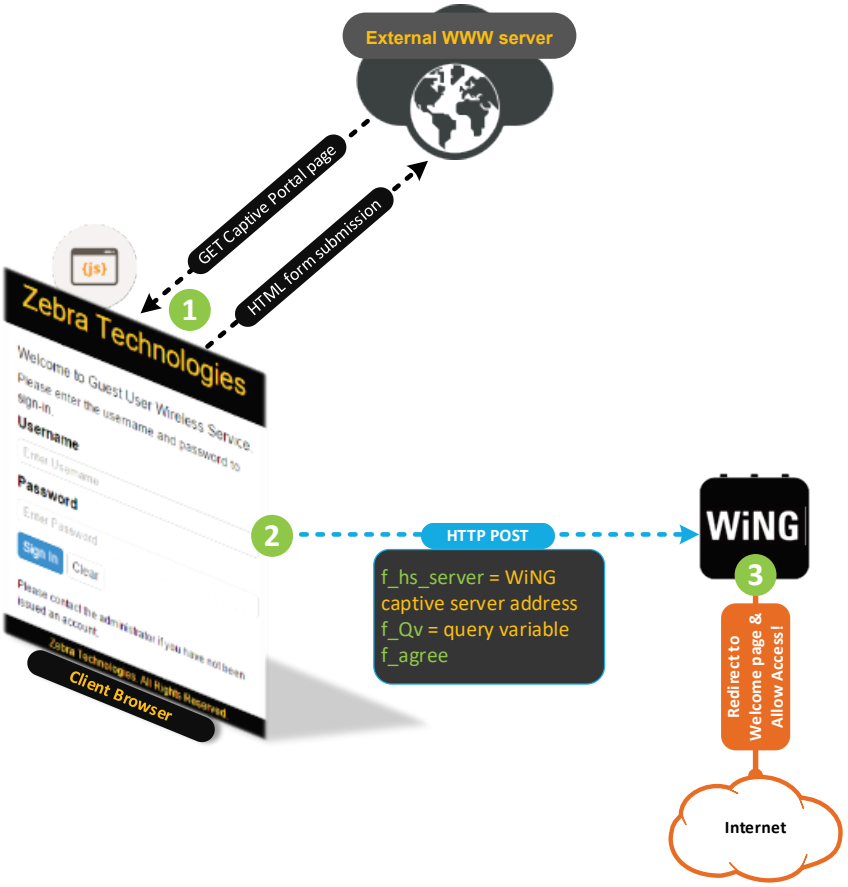
```
Sample HTML form to silently initiate HTTP POST after user presses "I Agree" button:
<form name="frmLogin" id="frmLogin" action="/cgi-bin/hslogin.cgi" method="POST" >
  <input size="20" name="f_agree" id="f_agree" type="hidden">
  <input size="64" name="f_hs_server" id="f_hs_server" type="hidden">
  <input name="f_curr_time" id="f_curr_time" type="hidden">

  <input name="f_Qv" id="f_Qv" type="hidden">

  <dl class="ta-c">
   <input name="submit" value="I Agree" type="submit" class="btn primary" onclick="getCurrTime();">
  </dl>
</form>
```

After the user will click on "I Agree" button in the browser Javascript shown above will send HTTP POST message on behalf of the user to the WiNG 5 device running Captive Portal server that will contain f_hs_server, f_Qv, f_agree variables.

An Access Point or Controller running Captive Portal server will open firewall for the user upon receiving the HTTP POST message with contents specified above and put the captive portal session status to “Success”. User is then redirected to the Welcome page.



RADIUS authentication (access-type radius)

With access-type configured as radius, a device that is performing capture and redirection (an Access Point or a Controller) will redirect unauthenticated guest user to the login page specified under Captive Portal policy:

```
!
captive-portal EXT-RADIUS
 webpage-location external
 webpage external login http://192.168.10.5:880/login.html
 webpage external welcome https://www.extreme.com
 webpage external fail http://192.168.10.5:880/fail.html
 use aaa-policy CENTRALIZED-RADIUS
 use dns-whitelist EXT-RADIUS
!
aaa-policy CENTRALIZED-RADIUS
 authentication server 1 host 140.101.4.17 secret 0 helloextreme
!
dns-whitelist EXT-RADIUS
 permit 192.168.10.5
!
```

Upon redirection WiNG 5 device will ask the client to add this information as a minimum to the HTTP GET request when fetching portal pages:

```
http://portal.guestaccess.com/login.html?hs_server=1.1.1.1&Qv=it_qpmjdz=FYU.UD@bbb_qpmjdz=@dmjfou_njou=23:9
912375@dmjfou_nbd=21.5B.8E.C8.C5.DG@ttje=BMQIBOFU@bq_nbd=95.35.9E.7B.33.81
```

In the above example client will attach hs_server address ("hotspot server" or IP/FQDN of the WiNG 5 device that is doing capture and redirection) and Qv variable (identifier of unique client session) to the HTTP GET request when being redirected to the external Web server.

This information need to be captured later on to maintain communication with WiNG captive portal. Additionally, it is required to inform the WiNG 5 Captive Portal that the guest user has acknoledged. In order to do this it is necessary to either:

a. Provide the user with a form where they can enter their credentials and click submit (this should be used with RADIUS access type).
b. Create PHP/Java script on the external web server's page to prepare HTML form and automatically POST the content from client's browser on the user's behalf to the WiNG 5 captive portal server.

Sample javascript to get hs_server and Qv variables can be found in the default internal agreement.html page (before the <body> tag)

Sample JavaScript to get Qv variable, f_hs_server, f_user and f_pass variables:

```
<script>
// function to get the query parameter value from URL query string.
function getQueryVariable(variable) {
  var query = window.location.search.substring(1);
  var vars = query.split(/[?&]/);
  for (var i=0;i<vars.length;i++) {
    var pair = vars[i].split("=");
    if (pair[0] == variable) {
        if (pair[0] == "Qv") {
            return vars[i].substr(3, vars[i].length);
        }
        return pair[1];
    }
  }
  return "";
}

var user = getQueryVariable("user");
if (user != "") {
        var user_dec = decodeURIComponent(user);
        document.getElementById('user').innerHTML = 'Welcome ' + user_dec;
}

function clear(){
  document.getElementById('f_user').value = "";
  document.getElementById('f_pass').value = "";
return true;
}

var hs_server = "NONE";
var port = 880;
var postToUrl = "/cgi-bin/hslogin.cgi";
hs_server = getQueryVariable("hs_server");
Qv = getQueryVariable("Qv");
cpstats_iframe = "http://cpstats." + hs_server + "/cp_stats.html";
postToUrl = ":" + port + postToUrl;
document.getElementById("f_hs_server").value = hs_server;
document.getElementById("f_Qv").value = Qv;
document.getElementById("frmLogin").action = "http://" + hs_server + postToUrl;
</script>
```

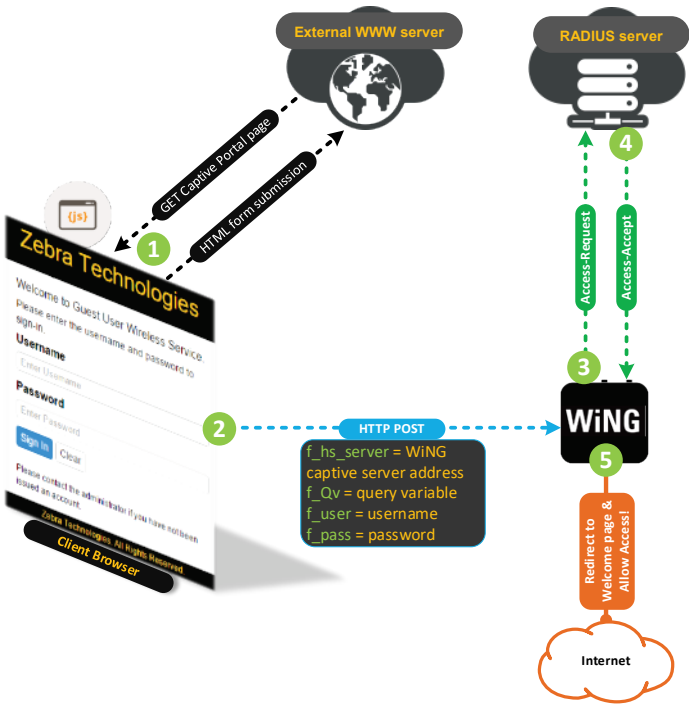
Additionally an HTML form should be included into the login page to get f_user and f_pass variables using the above script, as the user will submit his username and password. After pressing Submit button client will send an HTTP POST to the WiNG 5 Captive Portal that will contain f_hs_server, f_Qv, f_user and f_pass variables:

Sample HTML form to ask the visitor for username and password:

```
<form name="frmLogin" id="frmLogin" action="/cgi-bin/hslogin.cgi" method="POST" onReset="return clear()">
 <div class="normal-login show">
 <dl>
  <dt>Username</dt>
  <dd>
    <input class="control" name="f_user" id="f_user" type="text" placeholder="Enter Username">
  </dd>
  <dt>Password</dt>
  <dd>
    <input class="control" name="f_pass" id="f_pass" type="password" placeholder="Enter Password">
  </dd>
  </dl>
  <input size="64" name="f_hs_server" id="f_hs_server" type="hidden">
  <input name="f_curr_time" id="f_curr_time" type="hidden">
  <input name="f_Qv" id="f_Qv" type="hidden">
  <input name="submit" value="Sign In" type="submit" class="btn primary" onclick="getCurrTime();">
  <input name="reset" value="Clear" type="reset" class="btn default">
  </div>
</form>
```

After client submits the form with username and password the above javascript will initiate an HTTP POST from the client to the hs_server address (can be a virtual hostname defined under captive portal policy, can be IP address of the WiNG 5 device that performed redirection or a shadow IP 1.1.1.1 if this is an Access Point without SVI available).

After WiNG5 Captive Portal server will receive an HTTP POST it will initiate RADIUS Access-Request (by default using PAP, can be also CHAP/MSCHAP/MSCHAPv2) to the RADIUS Server defined in the AAA policy. After receiving RADIUS Access-Accept WiNG 5 device will open the firewall for this particular client and will change session to “Success” state.



Guest Self-Registration (access-type radius)

In a more complex scenario with guest user self-registration using external portals and external user database MAC authentication can be used along with Captive Portal redirection as a fallback mechanism. This approach will provide a one-time registration and seamless guest user handoff when the client is roaming to another Access Point or even trying to connect at another location.

It is assumed that all the components of this deployment scenario are external (Captive Portal web server, RADIUS server and Guest User Database).

In such scenarios a typical flow begins with the client starting MAC authentication against a centralized RADIUS server to perform a check against User database whether or not it is a returning user with existing user record.

If MAC authentication fails, then the user will be redirected to the Captive Portal landing page. When redirecting an Access Point or a Controller that performs redirection will typically ask the client to attach client MAC address into the GET request as a Query String.

This will allow external web pages to add client MAC address information silently into the HTML form, which will then be submitted to the user database along with the rest of the user registration details, like e-mail address, Name, mobile phone number, etc.

After the user will submit a HTML form it would be necessary to include a client side script that would do a HTTP POST to WiNG Captive Portal server (hs_server + f_Qv) with f_user and f_pass variables both set to client's MAC address.

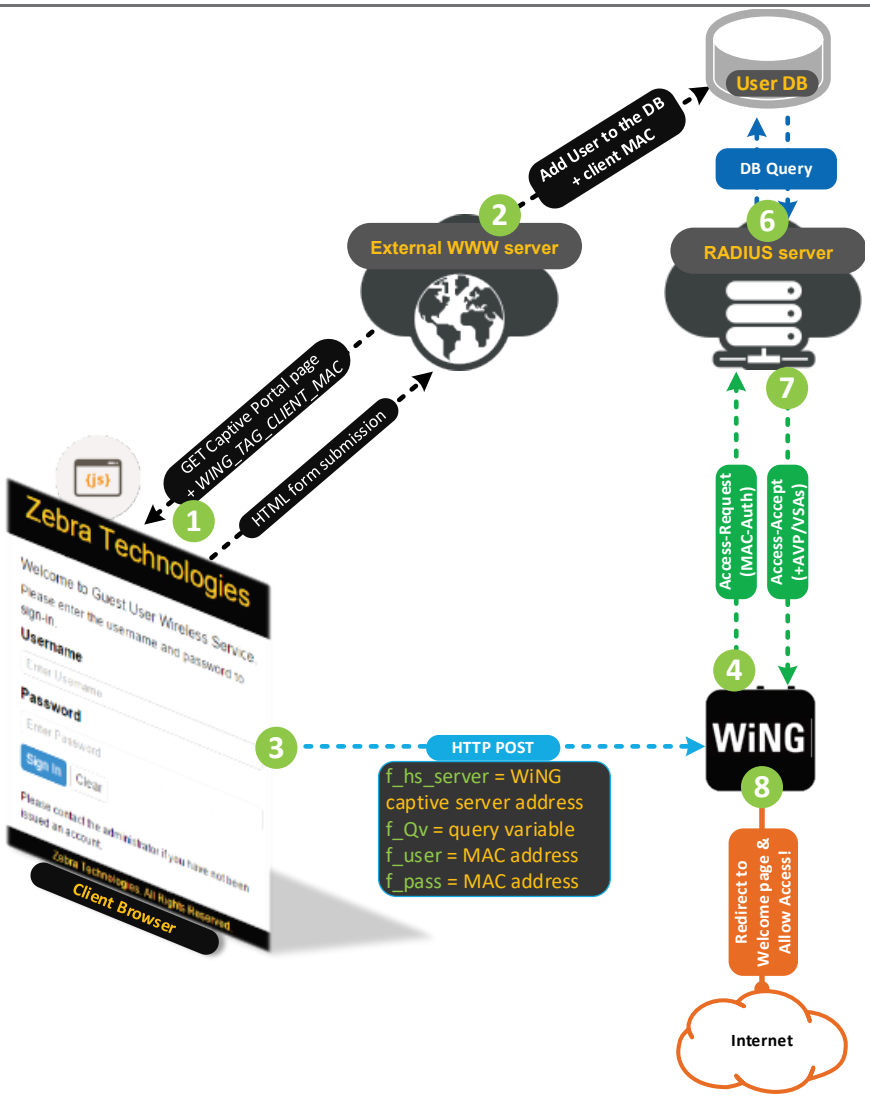
At this point an Access Point or a Controller running Captive Portal server will initiate a RADIUS Access-Request message to configured centralized RADIUS and perform MAC Authentication.

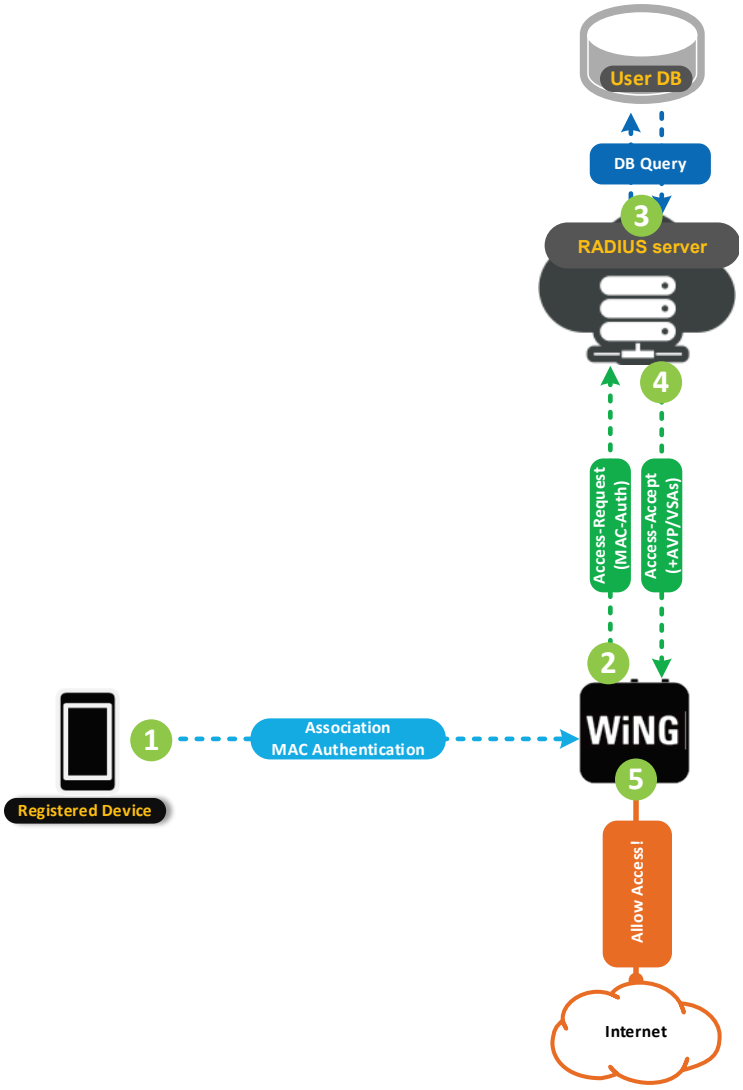
Along with receiving Access-Accept centralized RADIUS may also be configured to provide IETF or Vendor Specific attributes for example to assign a VLAN, provide application policy name for AVC feature, radius group name to assign a user a particular role using Role-Based Firewall, etc. As a final step upon successful MAC authentication WiNG Captive Portal will open firewall for this client and redirect the client to the configured Welcome page.

In case connecting guest user already exists in the centralized user database the flow would skip presenting Captive Portal landing page, as the first MAC authentication would be a success (client's MAC is present in the db) and therefore an Access Point will allow access (optionally assigning vlan and policies received from attributes from the RADIUS Access-Accept message).

For the scenario example configuration would include following statements:

```
!
wlan Guest
 ssid Guest
 vlan $GUEST
 bridging-mode local
 encryption-type none
 authentication-type mac
 use aaa-policy EXT-RADIUS
 use captive-portal EXT-REGISTRATION
 captive-portal-enforcement fall-back
!
captive-portal EXT-REGISTRATION
 webpage-location external
 webpage external login http://guestlogin.company.com:880/login.html
 webpage external welcome https://www.guestlogin.company.com:880/welcome.html
 webpage external fail http://guestlogin.company.com:880/fail.html
 use aaa-policy CENTRALIZED-RADIUS
 use dns-whitelist EXT-REG-SERVER
!
aaa-policy CENTRALIZED-RADIUS
 authentication server 1 host 140.101.4.17 secret 0 wingsecure
!
dns-whitelist EXT-RADIUS
 permit company.com suffix
!
```





WiNG Query Tags available with External Pages

A WiNG 5 device that is doing capture and redirection can attach various different query tags on behalf of the client when doing HTTP redirection to any external page. These tags can be used at the external web server to catch different information to be used for authentication, analytics or other purposes, like for example presenting a page in different language based on the RF_DOMAIN tag received, etc.

WiNG 5 Query Tags:	
WING_TAG_CLIENT_IP	Captive portal client IPv4 address
WING_TAG_CLIENT_MAC	Captive portal client MAC address
WING_TAG_WLAN_SSID	Captive portal client SSID
WING_TAG_AP_MAC	Captive portal client AP MAC address
WING_TAG_AP_NAME	Captive portal client AP Hostname
WING_TAG_RF_DOMAIN	Captive portal client RF Domain
WING_TAG_CP_SERVER	Captive portal server address (hs_server value)
WING_TAG_USERNAME	Captive portal authentication username
WING_TAG_USERTYPE	Captive portal usertype (new/return/refresh)

In the example below the external Web Server needs to catch MAC and IPv4 address of the client that is trying to associate (to check with the user database if any record exists for the user) and RF Domain where the client is currently associated:

```
!
captive-portal EXT-RADIUS
 webpage-location external
 webpage external login
http://192.168.10.5:880/login.html?client_mac=WING_TAG_CLIENT_MAC&client_ip=WING_TAG_CLIENT_IP&site=WING_TA
G_RF_DOMAIN
 webpage external welcome https://www.extremenetworks.com
 webpage external fail http://192.168.10.5:880/fail.html
 use aaa-policy INT
!
```

Note

Each web page type may have different Query Tags configured.

As a result when client gets redirected the URL will contain these additional tags in the Query String:

```
http://192.168.10.5:880/login.html?client_mac=10-4A-7D-B7-B4-CF&client_ip=192.168.70.126&site=home-
udolni&hs_server=1.1.1.1&Qv=it_qpmjdz=FYU.SBEJVT@bbb_qpmjdz=JOU@dmjfou_njou=23:9912375@dmjfou_nbd=21.5B.8E.
C8.C5.DG@ttje=BMQIBOFU@bq_nbd=95.35.9E.7B.33.81
```

Captive Portal Server FQDN

WiNG 5 device that performs capture and redirection of the wireless client will add hs_server address to the client's HTTP GET request. By default WiNG 5 device will use either its own IPv4 address (if Switch Virtual Interface is available in the guest user VLAN) or a shadow IPv4 address of 1.1.1.1 when no SVI is available in the guest user VLAN:

Note
SVI is the same as "interface vlan <x>" command in cli context.

SVI is not available in the guest VLAN:

```
http://192.168.10.5:880/login.html?client_mac=10-4A-7D-B7-B4-CF&client_ip=192.168.70.126&site=home-
udolni&hs_server=1.1.1.1&Qv=it_qpmjdz=FYU.SBEJVT@bbb_qpmjdz=JOU@dmjfou_njou=23:9912375@dmjfou_nbd=21.5B.8E.
C8.C5.DG@ttje=BMQIBOFU@bq_nbd=95.35.9E.7B.33.81
```

SVI is present in the guest VLAN:

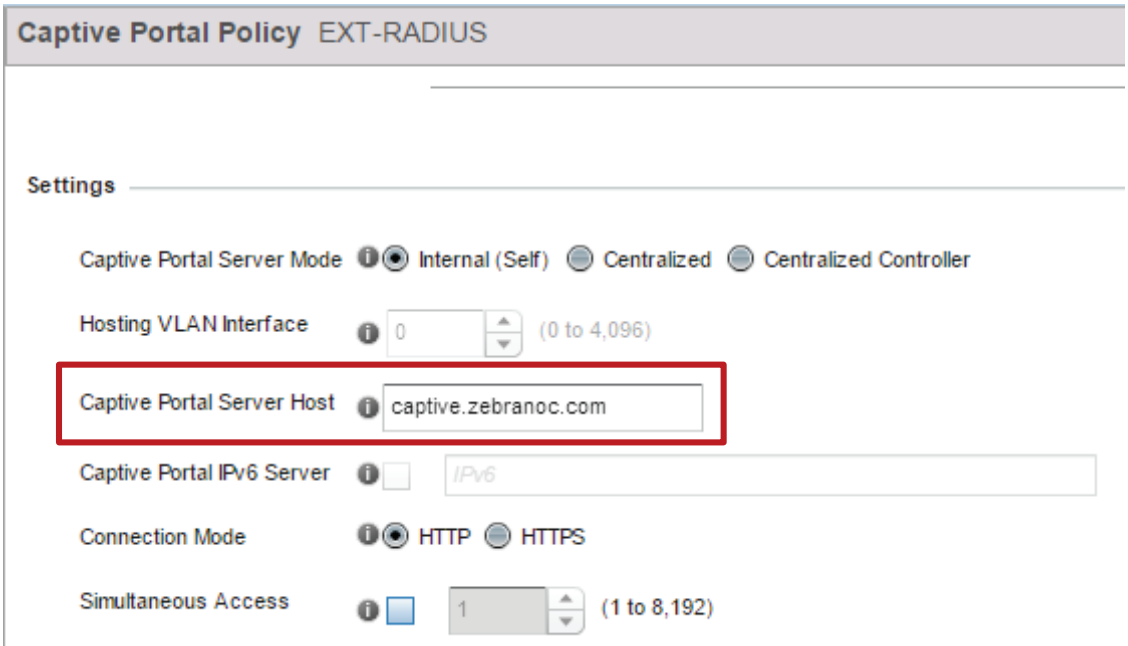
```
http://192.168.10.5:880/login.html?client_mac=10-4A-7D-B7-B4-CF&client_ip=192.168.70.126&site=home-
udolni&hs_server=192.168.70.235&Qv=it_qpmjdz=FYU.SBEJVT@bbb_qpmjdz=JOU@dmjfou_njou=23:9912375@dmjfou_nbd=21
.5B.8E.C8.C5.DG@ttje=BMQIBOFU@bq_nbd=95.35.9E.7B.33.81
```

It is possible to define a virtual FQDN for redirection if desired to present a hostname rather than IP address inside the client's GET request. Virtual Hostname will be automatically captured by the WiNG 5 device and translated to the shadow IP address 1.1.1.1 or real IPv4 address of an SVI (if available in the guest VLAN) using L2 NAT. Virtual Hostname must not be resolvable by available DNS servers:

Note
Available only in Self and Centralized-Controller modes

GUI Configuration

Configuration -> Services -> Captive Portals -> <NAME>



CLI Configuration

```
!
captive-portal EXT-RADIUS
 server host captive.extremenoc.com
 webpage-location external
 webpage external login
http://192.168.10.5:880/login.html?client_mac=WING_TAG_CLIENT_MAC&client_ip=WING_TAG_CLIENT_IP&site=WING_TA
G_RF_DOMAIN
 webpage external welcome https://www.extremenetworks.com
 webpage external fail http://192.168.10.5:880/fail.html
 use aaa-policy REDUNDANT-AAA
!
```

Sample HTTP GET from redirected client

```
http://192.168.10.5:880/login.html?client_mac=10-4A-7D-B7-B4-CF&client_ip=192.168.70.126&site=home-
udolni&hs_server=captive.extremenoc.com&Qv=it_qpmjdz=FYU.SBEJVT@bbb_qpmjdz=JOU@dmjfou_njou=23:9912375@dmjfo
u_nbd=21.5B.8E.C8.C5.DG@ttje=BMQIBOFU@bq_nbd=95.35.9E.7B.33.81
```

Logout FQDN

By default if a user closes the welcome page or the web-browser is in privacy mode, there is now way for the user to logout from the captive portal

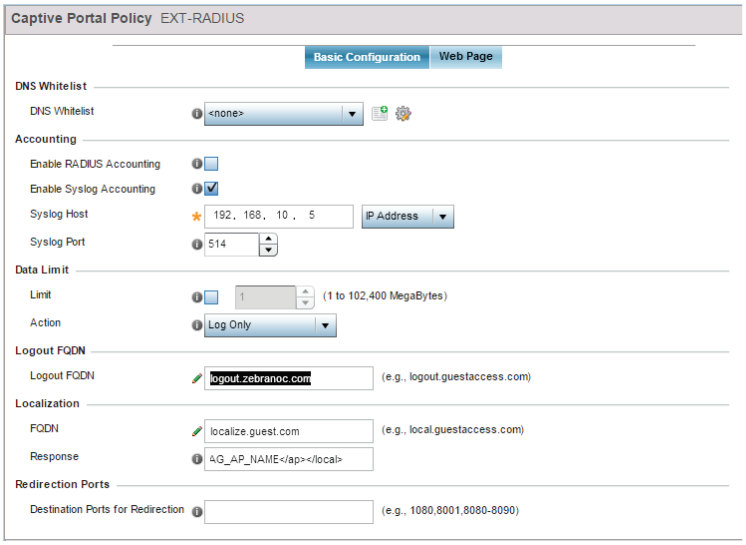
A user session will stay alive until the inactivity timeout period expires

Logout FQDN allows administrators to define an explicit logout URL that captive portal users can enter to disconnect from a WiNG 5 captive portal.

It is useful for paid public Hotspot deployments when service providers charge users for Internet access but can also be used for guest / visitor access

GUI Configuration

Configuration -> Services -> Captive Portals -> <NAME>



CLI Configuration

```
!
captive-portal EXT-RADIUS
 server host captive.extremenoc.com
 webpage-location external
 webpage external login
http://192.168.10.5:880/login.html?client_mac=WING_TAG_CLIENT_MAC&client_ip=WING_TAG_CLIENT_IP&site=WING_TA
G_RF_DOMAIN
 webpage external welcome https://www.extremenetworks.com
 webpage external fail http://192.168.10.5:880/fail.html
 use aaa-policy REDUNDANT-AAA
 logout-fqdn logout.extremenoc.com
!
```

Localization FQDN

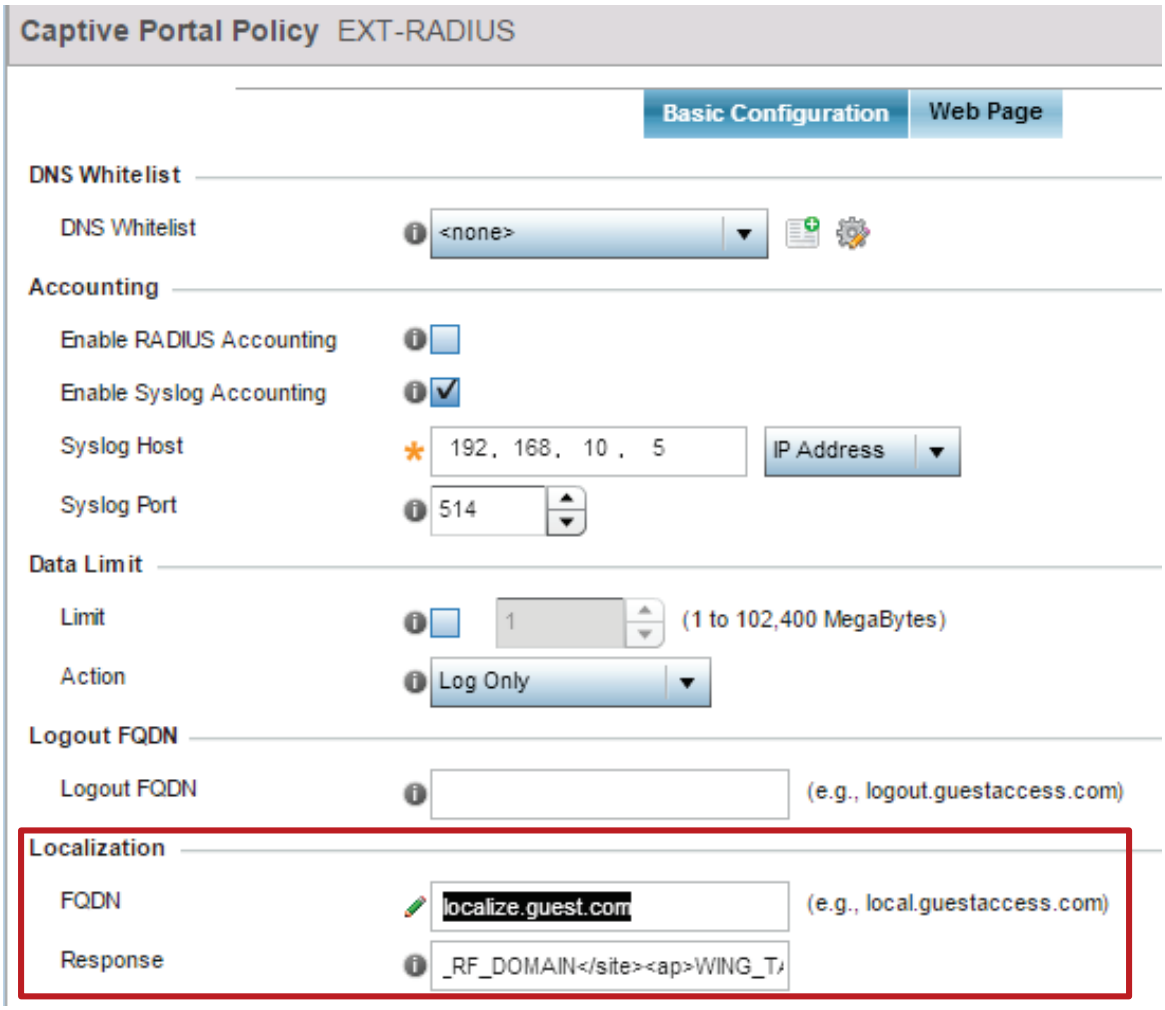
Starting from WiNG 5.8.1.0 release it is possible to define a Localization FQDN inside the Captive Portal Policy. It is useful when integrating with 3rd party application running on a smartphone (i.e. Android or iOS device for example) in order to pass information to the client about where it is located (region/store/brand).

This info can be used later to inform the application to fetch only certain information, for example show only items that are on stock in this particular store, or show map information for a particular branch where client is in etc.

How it works:

- Client will run an application that will initiate HTTP GET request to the configured localization URL

GUI Configuration

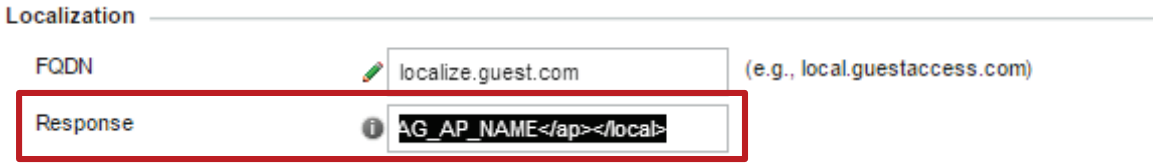


CLI Configuration

```
!
captive-portal EXT-RADIUS
 server host captive.extremenoc.com
 webpage-location external
 webpage external login
http://192.168.10.5:880/login.html?client_mac=WING_TAG_CLIENT_MAC&client_ip=WING_TAG_CLIENT_IP&site=WING_TA
G_RF_DOMAIN
 webpage external welcome https://www.extremenetworks.com
 webpage external fail http://192.168.10.5:880/fail.html
 use aaa-policy INT
 localization fqdn localize.guest.com
!
```

- An Access Point will intercept this request and respond back to the client with localization data as configured in the Captive Portal policy

GUI Configuration

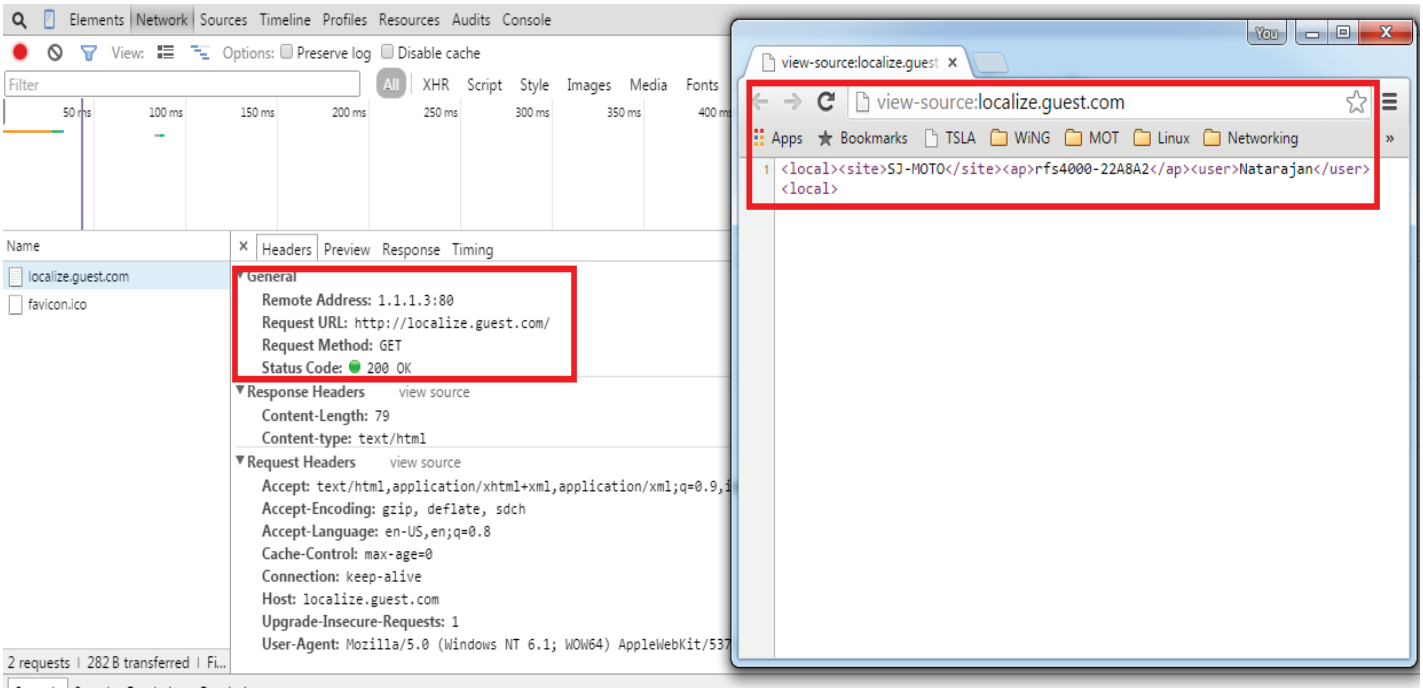


CLI Configuration

```
!
captive-portal EXT-RADIUS
 server host captive.extremenoc.com
 webpage-location external
 webpage external login
http://192.168.10.5:880/login.html?client_mac=WING_TAG_CLIENT_MAC&client_ip=WING_TAG_CLIENT_IP&site=WING_TA
G_RF_DOMAIN
 webpage external welcome https://www.extremenetworks.com
 webpage external fail http://192.168.10.5:880/fail.html
 use aaa-policy INT
 localization fqdn localize.guest.com
 localization response
<local><site>WING_TAG_RF_DOMAIN</site><ap>WING_TAG_AP_NAME</ap><ssid>WING_TAG_WLAN_SSID</ssid><client-
ip>WING_TAG_CLIENT_IP</client-ip></local>
!
```

Available Query Response Tags:	
WING_TAG_CLIENT_IP	Captive portal client IPv4 address
WING_TAG_CLIENT_MAC	Captive portal client MAC address
WING_TAG_WLAN_SSID	Captive portal client SSID
WING_TAG_AP_MAC	Captive portal client AP MAC address
WING_TAG_AP_NAME	Captive portal client AP Hostname
WING_TAG_RF_DOMAIN	Captive portal client RF Domain
WING_TAG_CP_SERVER	Captive portal server address (hs_server value)
WING_TAG_USERNAME	Captive portal authentication username
WING_TAG_USERTYPE	Captive portal usertype (new/return/refresh)

- Localization FQDN will be translated via L2 NAT to a shadow IP address of 1.1.1.3, for example:



Session and Data Usage Logging

Accounting

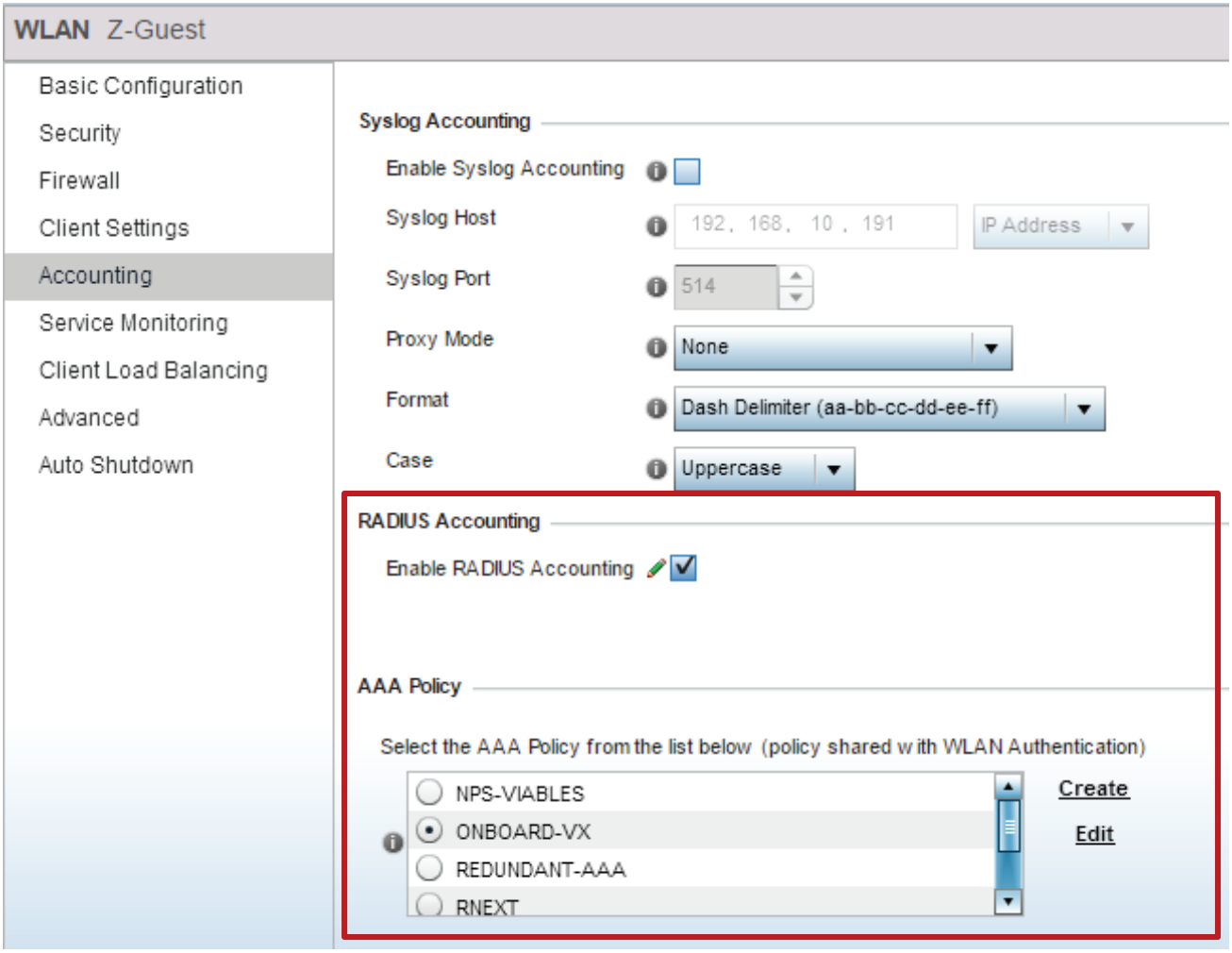
When it comes to Captive Portals in many countries it is required to have logging of user sessions and destinations visited and have all accounting information written into a centralized location. Additionally, RADIUS Accounting is typically used in situations when billing services are provided to track data and time usage for each user session .WiNG 5 supports multiple ways of capturing accounting information for users:

Per WLAN

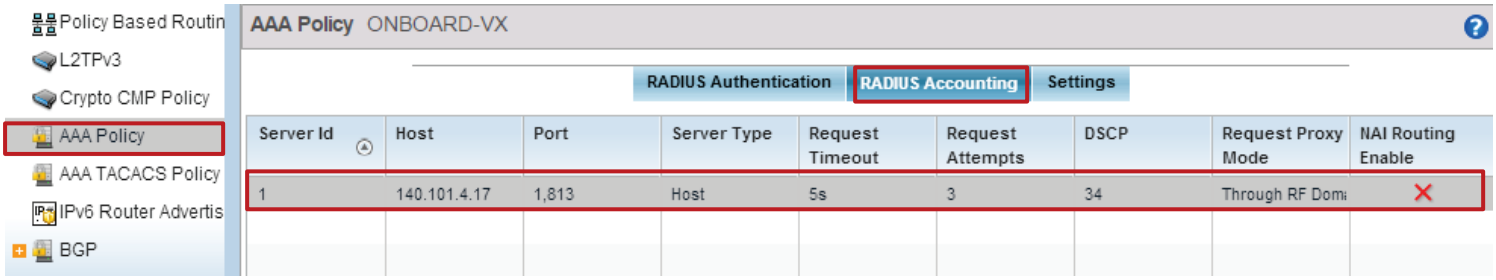
Accounting information is captured when the client associates and is not relevant to the captive portal authentication state. It is useful when captive portal is a fallback authentication method (MAC authentication being the primary), i.e. when wireless client may skip visiting captive portal pages.

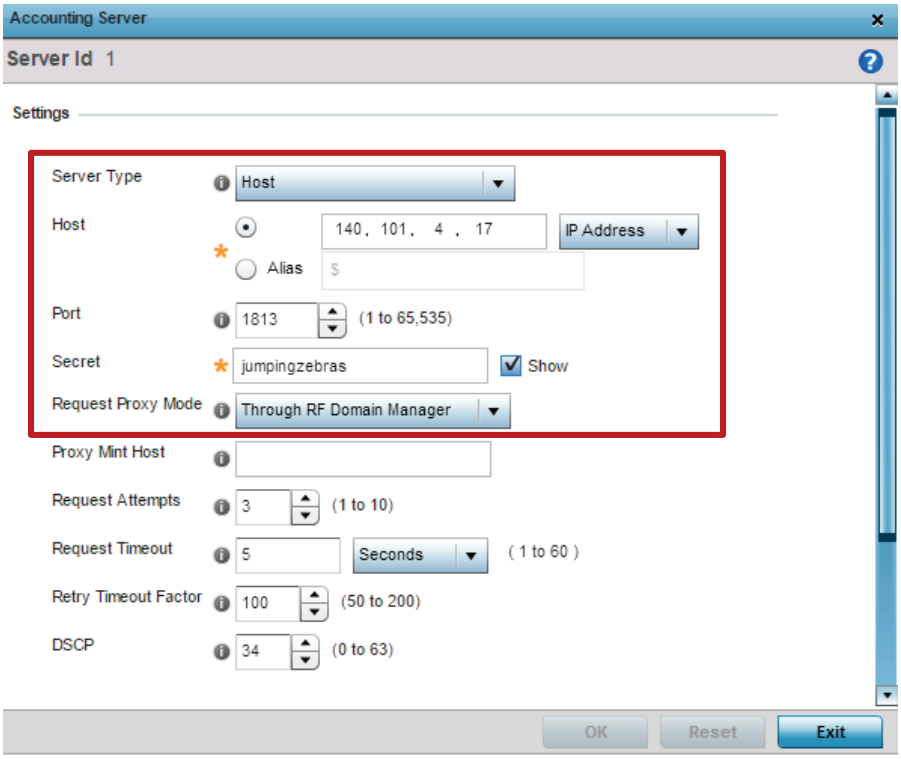
GUI Configuration

Configuration -> Wireless -> Wireless LANs -> <Name> -> Accounting



Accounting server must be defined in the AAA Policy that is assigned to the Wireless LAN:





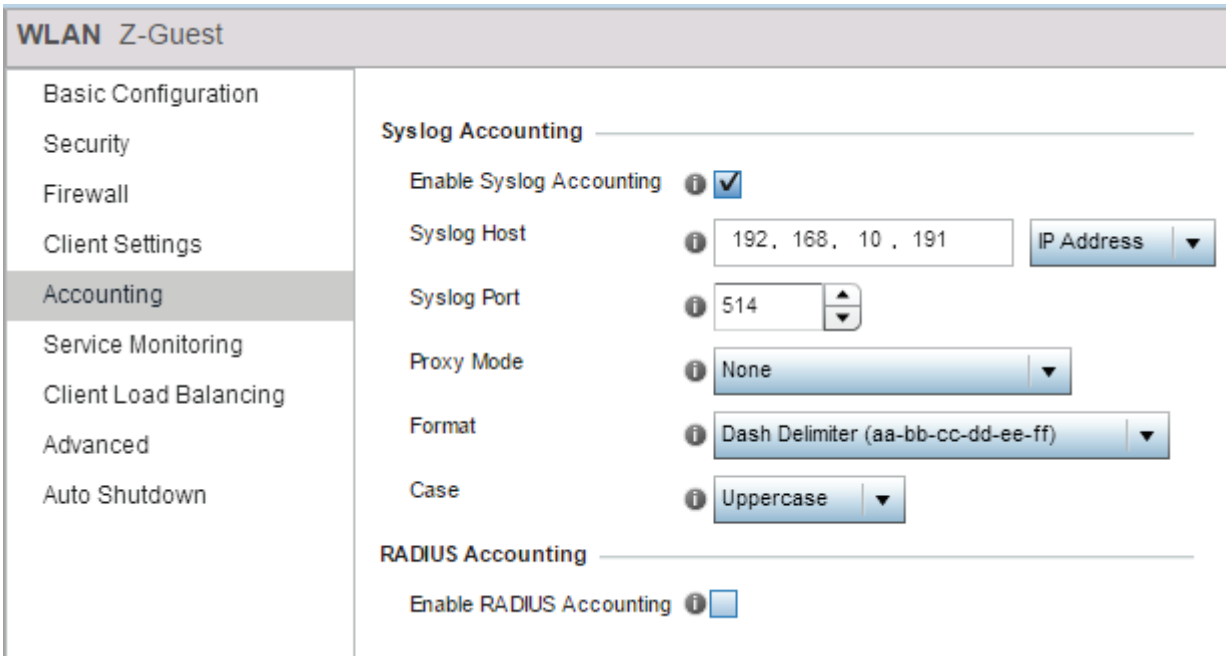
CLI Configuration

```
CLI Configuration
!
wlan Z-Guest
 ssid Z-Guest
 vlan $GUEST
 bridging-mode local
 encryption-type none
 authentication-type mac
 accounting radius
 accounting wait-client-ip
 use aaa-policy ONBOARD-VX
 use captive-portal Z-GUEST
 captive-portal-enforcement fall-back
!
aaa-policy ONBOARD-VX
 authentication server 1 host 140.101.4.17 secret 0 helloextreme
 accounting server 1 host 140.101.4.17 secret 0 helloextreme
 accounting server 1 proxy-mode through-rf-domain-manager
 accounting type start-interim-stop
 accounting interim interval 60
!
```

Syslog Accounting

GUI Configuration

Configuration -> Wireless -> Wireless LANs -> <Name> -> Accounting



CLI Configuration

Note

Additional configuration options available in CLI only

```
!
wlan Z-Guest
 ssid Z-Guest
 vlan $GUEST
 bridging-mode local
 encryption-type none
 authentication-type mac
 radio-resource-measurement
 accounting syslog host 192.168.10.5
 accounting wait-client-ip
 use aaa-policy INT
 use captive-portal UPLOAD-TEST
 captive-portal-enforcement fall-back
!
```

Example Output

```
Dec 28 18:55:57  ACCT-START User-Name:BC-3B-AF-85-F0-70 IPv4-Address:192.168.95.70 Session-Id:38571
Calling-Station:BC-3B-AF-85-F0-70 Called-Station:B4-C7-99-CA-EC-E2
Dec 28 18:55:56  ACCT-STOP User-Name:BC-3B-AF-85-F0-70 IPv4-Address:192.168.95.70 Session-Id:38570 Calling-
Station:BC-3B-AF-85-F0-70 Called-Station:B4-C7-99-CA-BF-35 Packets-In:26 Packets-Out:19 Bytes-In:6690
Bytes-Out:4424
```

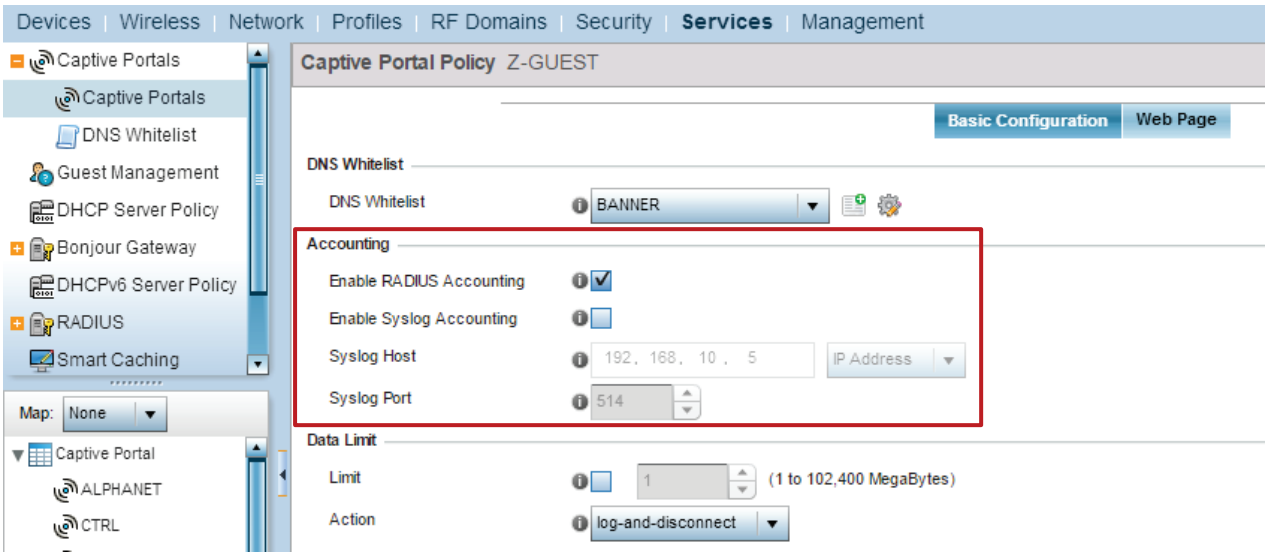
Per Captive Portal Policy

Accounting information is captured when the client authenticates through a Captive Portal. It is useful when captive portal is used a main client authentication method, without prior MAC authentication.

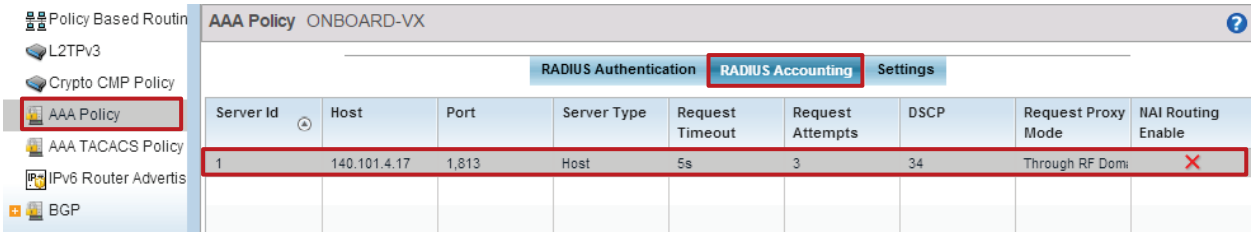
RADIUS Accounting

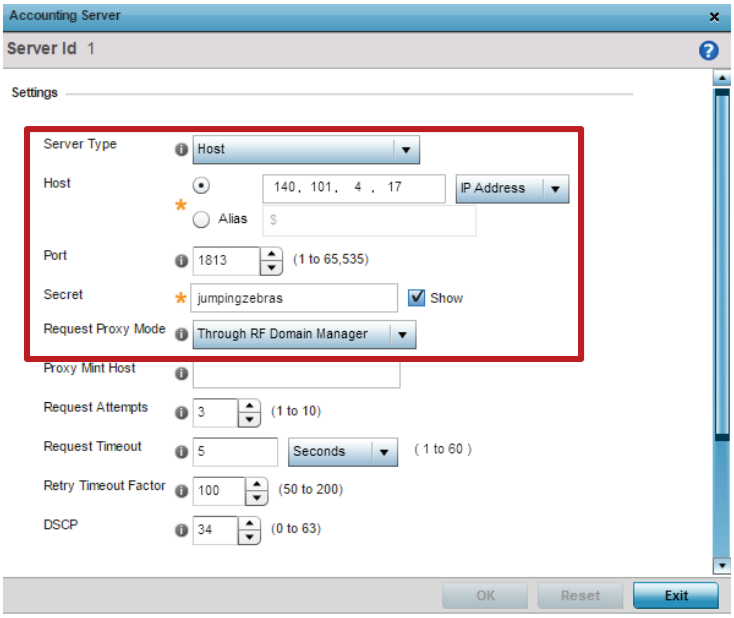
GUI Configuration

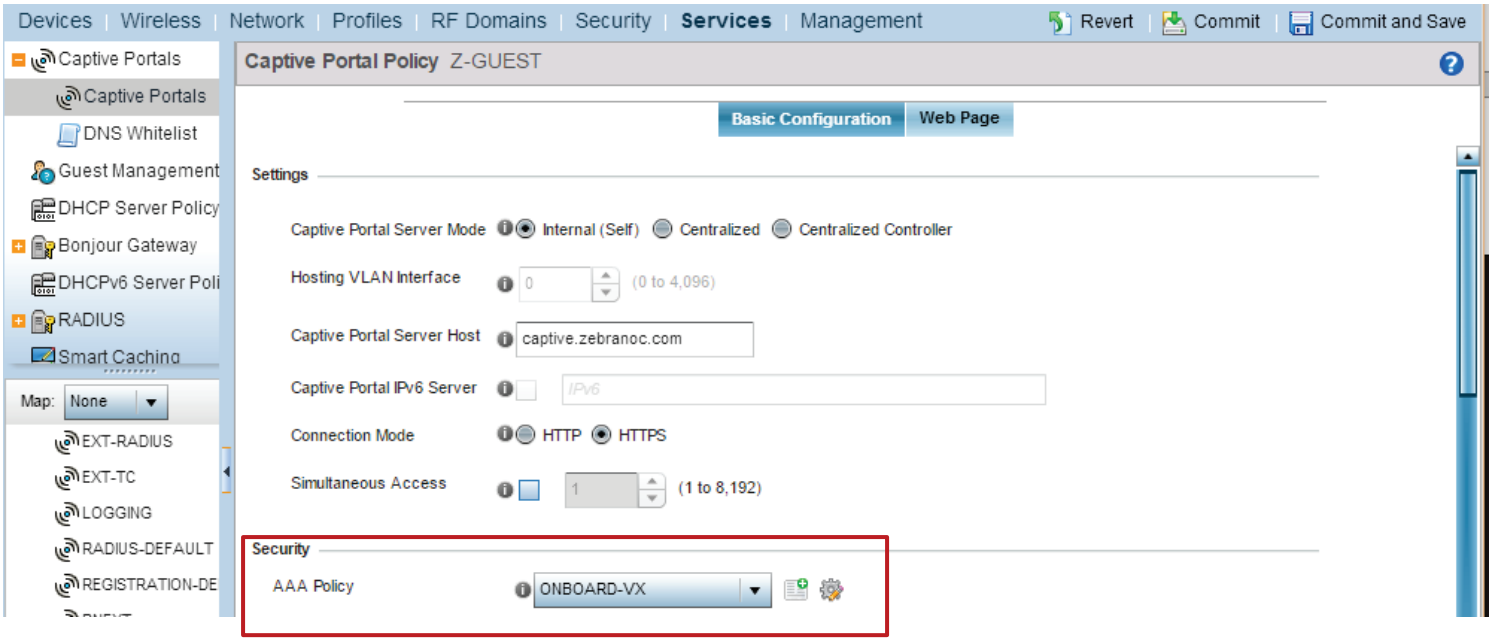
Services -> Captive Portals -> <Name> -> Accounting



Accounting server must be defined in the AAA Policy that is assigned to the Captive Portal Policy.







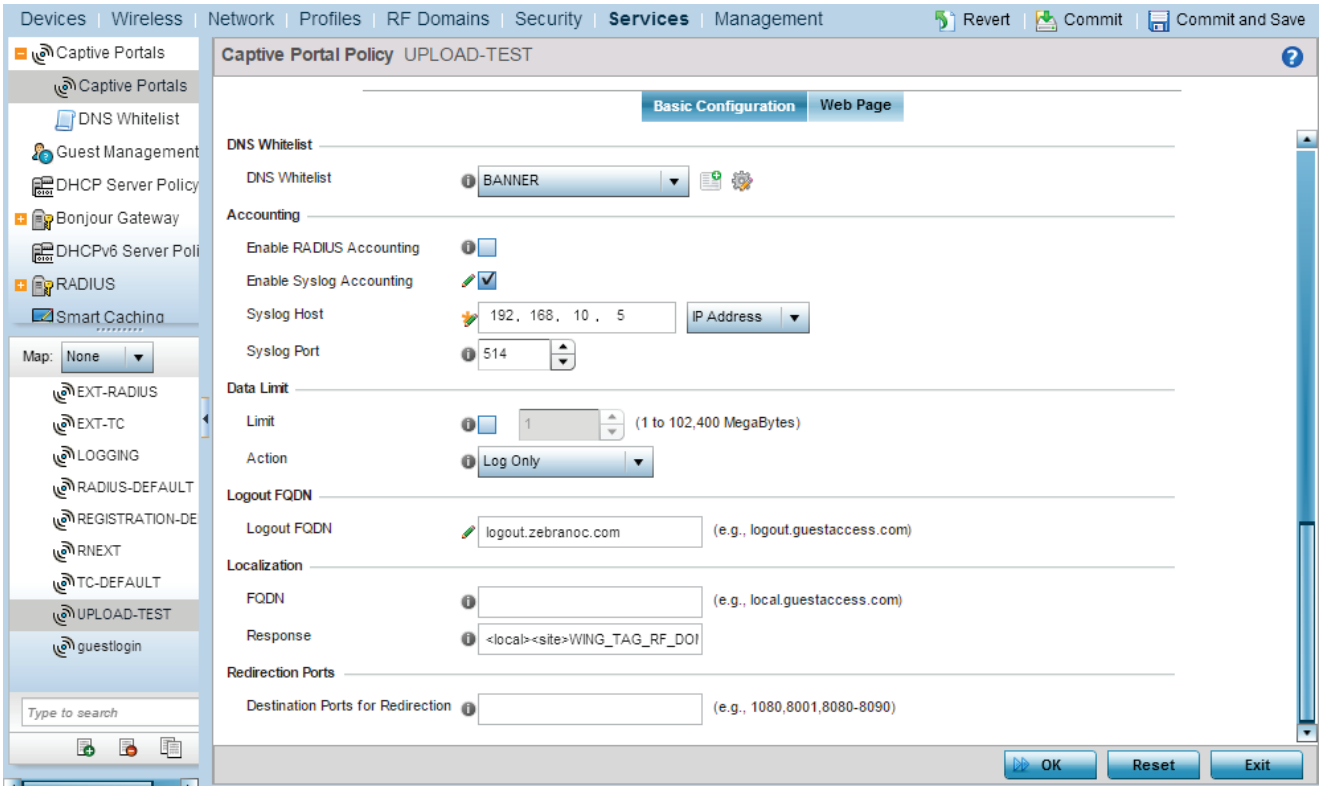
CLI Configuration

```
!
aaa-policy ONBOARD-VX
 authentication server 1 host 140.101.4.17 secret 0 helloextreme
 accounting server 1 host 140.101.4.17 secret 0 helloextreme
 accounting server 1 proxy-mode through-rf-domain-manager
 accounting type start-interim-stop
 accounting interim interval 60
!
captive-portal Z-GUEST
 access-type registration
 connection-mode https
 server host captive.extremenoc.com
 oauth
 oauth client-id Google 55848734804-ija3kti4o36b1esmjtgbotid177ks6bd.apps.googleusercontent.com Facebook
1576296242634490
 accounting radius
 use aaa-policy ONBOARD-VX
 use dns-whitelist BANNER
 webpage-auto-upload
 logout-fqdn logout.deaflyz.com
 bypass captive-portal-detection
!
```

Syslog Accounting

GUI Configuration

Services -> Captive Portals -> <Name> -> Accounting



CLI Configuration

```
!
captive-portal UPLOAD-TEST
 access-type registration
 connection-mode https
 server host captive.extremenoc.com
 oauth
 oauth client-id Google 55848734804-ija3kti4o36b1esmjtgbotid177ks6bd.apps.googleusercontent.com Facebook
1576296242634490
 accounting syslog host 192.168.10.5
 use aaa-policy INT
 use dns-whitelist BANNER
 webpage-auto-upload
 logout-fqdn logout.deaflyz.com
 bypass captive-portal-detection
!
```

Example Output

```
Feb  6 20:01:25  ACCT-STOP User-Name:nexus IP-Address:192.168.70.102 Session-Id:24 Calling-Station:64-BC-
0C-6A-D9-5B Packets-In:12865 Packets-Out:11643 Bytes-In:2983234 Bytes-Out:6011243
Feb  6 20:01:20  ACCT-UPDATE User-Name:nexus IP-Address:192.168.70.102 Session-Id:24 Calling-Station:64-BC-
0C-6A-D9-5B Packets-In:12492 Packets-Out:11173 Bytes-In:2784739 Bytes-Out:5937241
Feb  6 20:00:20  ACCT-START User-Name:nexus IP-Address:192.168.70.102 Session-Id:24 Calling-Station:64-BC-
0C-6A-D9-5B
```

Information logged – RADIUS Accounting

Accounting information is sent to the server when a user connects and disconnects from a WLAN and may also be periodically forwarded during the session (Interim updates). RADIUS accounting information can be used to track individual user's network usage for billing purposes as well as be used as a tool for gathering statistic for general network monitoring.

When network access is granted to the user by the Wireless Controller, an **Accounting-Request** message with the **Acct-Status-Type** field set to Start is forwarded by the Wireless Controller to the RADIUS server to signal the start of the user's network access. Start records typically contain the user's identification, network address, point of attachment and a unique session identifier. Optionally periodic Accounting-Request messages with the Acct-Status-Type field set to Interim Update may be sent by the WiNG 5 AP or Controller to the RADIUS server to update it on the status of an active session. Interim records typically convey the current session duration and information on current data usage. When the user's session is closed, the AP forwards an Accounting-Request message with the Acct-Status-Type field set to Stop. This provides information on the final usage in terms of time, packets transferred, data transferred and reason for disconnect and other information related to the user's network access.

In each **Accounting-Request** message the following Vendor Specific Attributes (VSAs) will be present.

Vendor Code	Attribute Number	Description
388	18	IP address of the WiNG 5 device that is forwarding a RADIUS Accounting packet. Applicable to Accounting-Request packets.
388	17	Hostname of the WiNG 5 device sending RADIUS Accounting packet. Applicable to Accounting-Request packets.
388	19	MAC Address of the WiNG 5 device sending RADIUS Accounting packet. Applicable to Accounting-Request packets
388	32	RF Domain name. Applicable to Accounting-Request packets.

Attribute Name	Type	RFC	Description
User-Name	1	RFC 2865	The User-Name attribute is forwarded in the Accounting-Request and indicates the name of the user.
NAS-IP-Address	4	RFC 2865	The NAS-IP-Address attribute is forwarded in the Accounting-Request and indicates the IP Address of the Wireless Controller or Access Point.
NAS-Port	5	RFC 2865	The NAS-Port attribute is forwarded in the Accounting-Request and indicates the association index of the user on the Wireless Controller or Access Point.
Class	25	RFC 2865	The Class attribute is optionally forwarded in the Access-Accept and should be sent unmodified by the client to the accounting server as part of the Accounting-Request packet if accounting is supported.
Called-Station-Id	30	RFC 2865	The Called-Station-Id attribute is forwarded in the Accounting-Request and indicates the BSSID and ESSID that the user is associated with. The Wireless Controller or Access Point will forward the attribute value using the following formatting: XX-XX-XX-XX-XX-XX:ESSID.
Calling-Station-Id	31	RFC 2865	The Calling-Station-Id attribute is forwarded in the

			Accounting-Request and indicates the MAC address of the user. The Wireless Controller or Access Point will forward the attribute value using the following formatting: XX-XX-XX-XX-XX-XX.
NAS-Identifier	32	RFC 2865	The NAS-Identifier attribute is forwarded in the Accounting-Request and indicates the hostname or user defined identifier of the Wireless Controller or Access Point.
Acct-Status-Type	40	RFC 2866	The Acct-Status-Type attribute is forwarded in the Accounting-Request and indicates whether the Accounting-Request marks the status of the accounting update. Supported values include Start, Stop and Interim-Update.
Acct-Delay-Time	41	RFC 2866	The Acct-Delay-Time attribute is forwarded in the Accounting-Request and indicates how many seconds the Wireless Controller or Access Point has been trying to send the accounting record for. This value is subtracted from the time of arrival on the server to find the approximate time of the event generating this Accounting-Request.
Acct-Input-Octets	42	RFC 2866	The Acct-Input-Octets attribute is forwarded in the Accounting-Request and indicates how many octets have been received from the user over the course of the connection. This attribute may only be present in Accounting-Request records where the Acct-Status-Type is set to Stop.
Acct-Output-Octets	43	RFC 2866	The Acct-Output-Octets attribute is forwarded in the Accounting-Request and indicates how many octets have been forwarded to the user over the course of the connection. This attribute may only be present in Accounting-Request records where the Acct-Status-Type is set to Stop.
Acct-Session-Id	44	RFC 2866	The Acct-Session-Id attribute is forwarded in the Accounting-Request and provides a unique identifier to make it easy to match start, stop and interim records in an accounting log file.
Account-Authentic	45	RFC 2866	The Account-Authentic attribute is forwarded in the Accounting-Request and indicates how the user was authenticated. When RADIUS accounting is enabled the Wireless Controller or Access Point will set this value to RADIUS.
Acct-Session-Time	46	RFC 2866	The Acct-Session-Time attribute is forwarded in the Accounting-Request and indicates how many seconds the user has received service for. This attribute may only be present in Accounting-Request records where the Acct-Status-Type is set to Stop.

HTTP URL logging (Syslog or JSON)

If there is a requirement to log all the visited URLs for each client it is possible to send capture and send this information either to an external Syslog server or using outbound HTTP API stream in json format. This function is based on tracking client's HTTP requests, therefore it is limited to HTTP traffic only, since SSL traffic is encrypted.

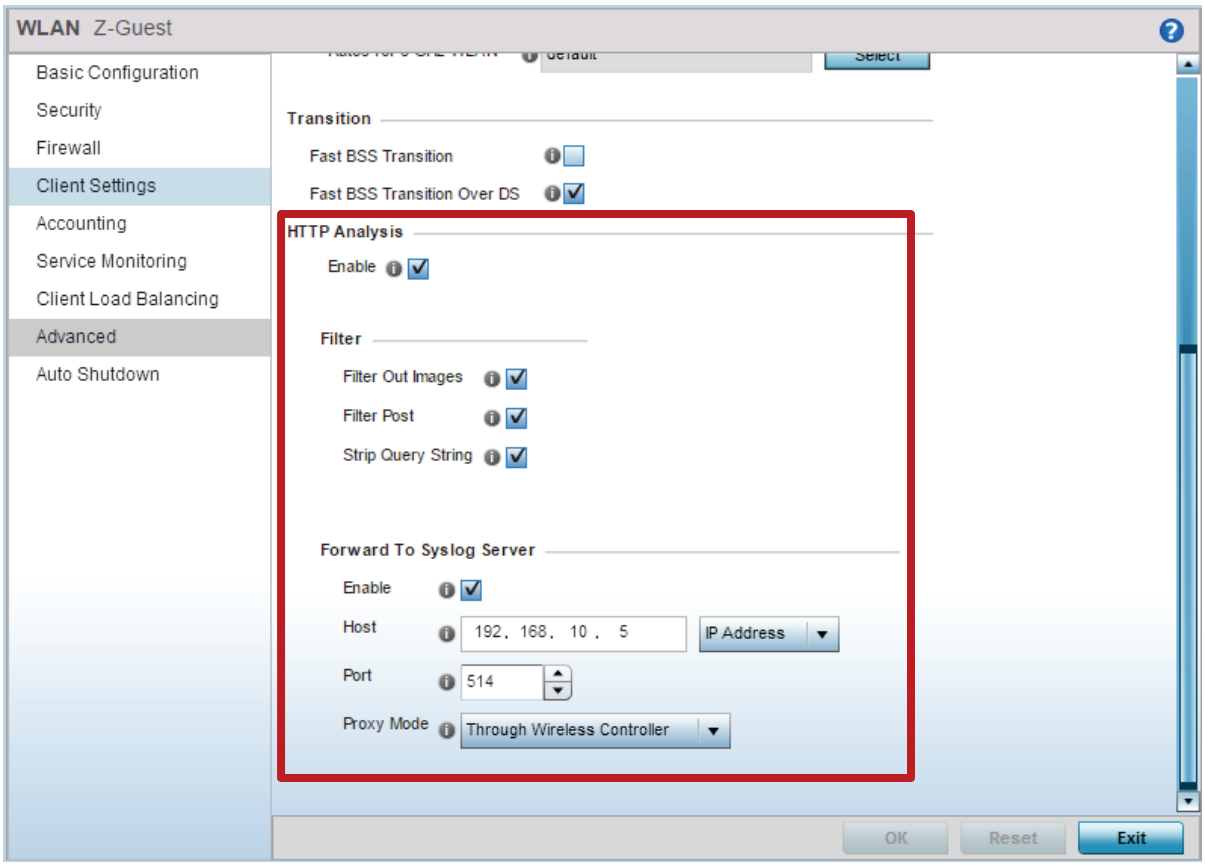
Additionally, it is also possible to filter out GET request for images, HTTP POST messages and strip Query Strings.

HTTP URL Logging to an external SYSLOG

URL logging to external Syslog server is managed entirely from the WLAN configuration context. Syslog port is configurable, additionally info feed can be proxied via RF Domain Manager or the adopting Controller through MiNT.

GUI Configuration

Configuration -> Wireless -> Wireless LANs -> <WLAN Name> -> Advanced



CLI Configuration

```
!
wlan Z-Guest
 ssid Z-Guest
 vlan $GUEST
 bridging-mode local
 encryption-type none
 authentication-type mac
 radio-resource-measurement
 use aaa-policy INT
 use captive-portal UPLOAD-TEST
 captive-portal-enforcement fall-back
 registration device-OTP group-name GUESTS expiry-time 4320
 registration external host 140.101.4.17
 use ip-access-list out BROADCAST-MULTICAST-CONTROL
 use mac-access-list out PERMIT-ARP-AND-IPv4
 http-analyze syslog host 192.168.10.5 port 514 proxy-mode through-controller
 http-analyze
 http-analyze filter query-string
 http-analyze filter images
 http-analyze filter post
!
```

Example Output

```
Dec 28 19:17:08 URL_INFO RF-Domain:EMEATECH Client:40-83-DE-8D-D7-A4 Wlan:guest-access
Url:http://90.182.119.35/generate_204
Dec 28 18:50:20 URL_INFO RF-Domain:EMEATECH Client:BC-3B-AF-85-F0-70 Wlan:ONBOARDING
Url:http://www.google.com/client_204?ct=clpit&cad=429047995:1
Dec 28 19:50:55 URL_INFO RF-Domain:EMEATECH Client:00-1D-0F-B2-A1-64 Wlan:SC
Url:http://liveupdate.symantecliveupdate.com/sesc$20virus$20definitions$20win64$20$28x64$29$20v11_microdefs
b.curdefs_symalllanguages_livetri.zip
```

HTTP URL Logging using HTTP JSON stream

In addition to Syslog URL logging it is possible to establish an HTTP stream in JSON format to an external server (for example RetailNext).

HTTP Analytics data is forwarded in MiNT to the VX or NX controller (MiNT port 60) and afterwards VX or NX controller will upload them to the external server using compressed JSON format over an HTTPS socket. The user needs to specify the URL of the External Server and the username and password for authentication. Some amount of data is cached and aggregated before the data is uploaded to the external server.

Feature supported on NX9XXX or VX9000 controllers only.

The data is uploaded to the external engine as an array of JSON objects. The keys used for the objects is described in the following table.

mu_mac	MAC address of the wireless client on which the HTTP request originated
ap_mac	MAC address of the Access Point where the HTTP request originated
ap_name	Hostname of the Access Point where the HTTP request originated
rf_domain	RF Domain name where the HTTP request originated
wlan_name	WLAN name where client was associated
timestamp	Time the packet was received (Epoch time in seconds)
url	URL of the request
body	Optional body of the HTTP request
method	HTTP method – POST, GET, PUT, HEAD etc

Additionally following HTTP Headers will be forwarded and encoded in JSON:

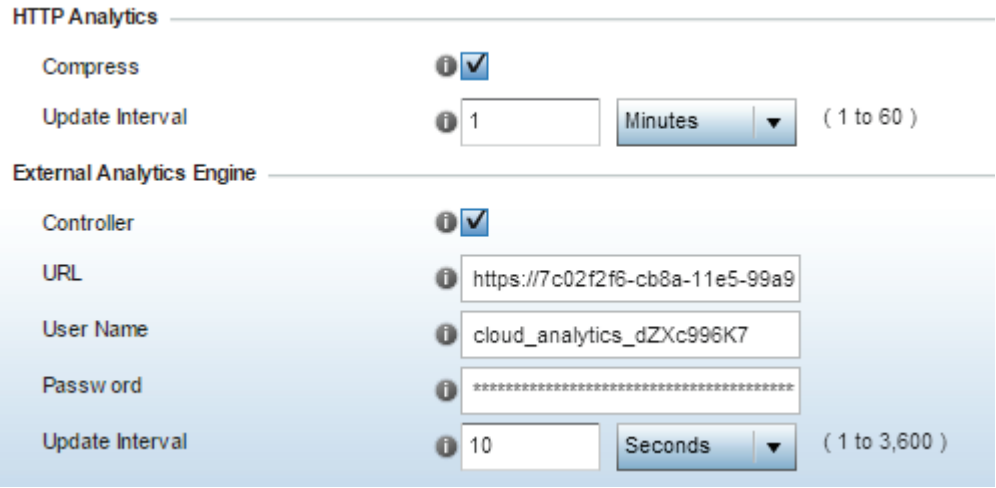
- Host
- Referrer
- User-Agent

Sample Output

```
[{"mu_mac": "01:02:03:04:05:06", "method": "POST", "url":"http://www.amazon.com/gp/prime/handlebuy-
box.html/ref=dp_start-bbf_1_glance", "body":
"sessionid=192950285002746 30&ASIN=B004TGO6RY&isMerchantExclusive=0&merchantID=ATVPDKIKX0
DER&nodeID=228013&offerListingID=mFfPAnruz88M%2BebaqepobfL9h%2BbmWdLsNowVaMO1i
SXfnx1kTLstEIawFz0Uec7XX4usFjsIa2pTyVtLVuH1wgE0RFWuFLa%", "ap_mac": "aa:bb:cc:dd:ee:ff","ap_name": "ap7532-
1", "rf_domain": "store-1", "wlan_name": "guest-access"}]
```

GUI Configuration

Profile -> Profile Name -> Management



CLI Configuration (VX/NX controller profile level)

```
!
 http-analyze external-server url https://7c02f2f6-cb8a-11e5-99a9-00000d252588.h-a.wifiops.io/WiNG
 http-analyze external-server username cloud_analytics_dZXc996K7
 http-analyze external-server password 6xJheYtCnJfhW
 no http-analyze external-server validate-server-certificate
 http-analyze external-server update-interval 60
 http-analyze compress
!
```

Application Visibility and Control

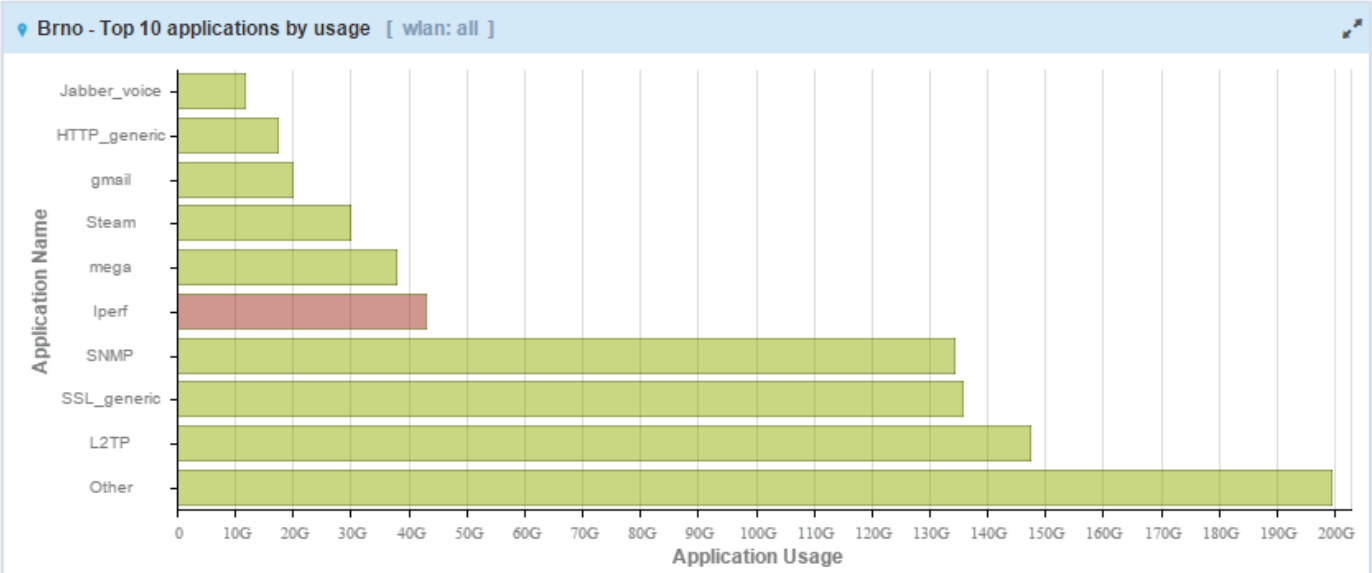
WiNG Access Points can provide additional layer 7 visibility and control by leveraging the AVC feature and built-in Deep Packet Inspection engine (DPI). This will allow to inspect guest user traffic and detect applications that each wireless client is using and apply access rules or different QoS priorities.

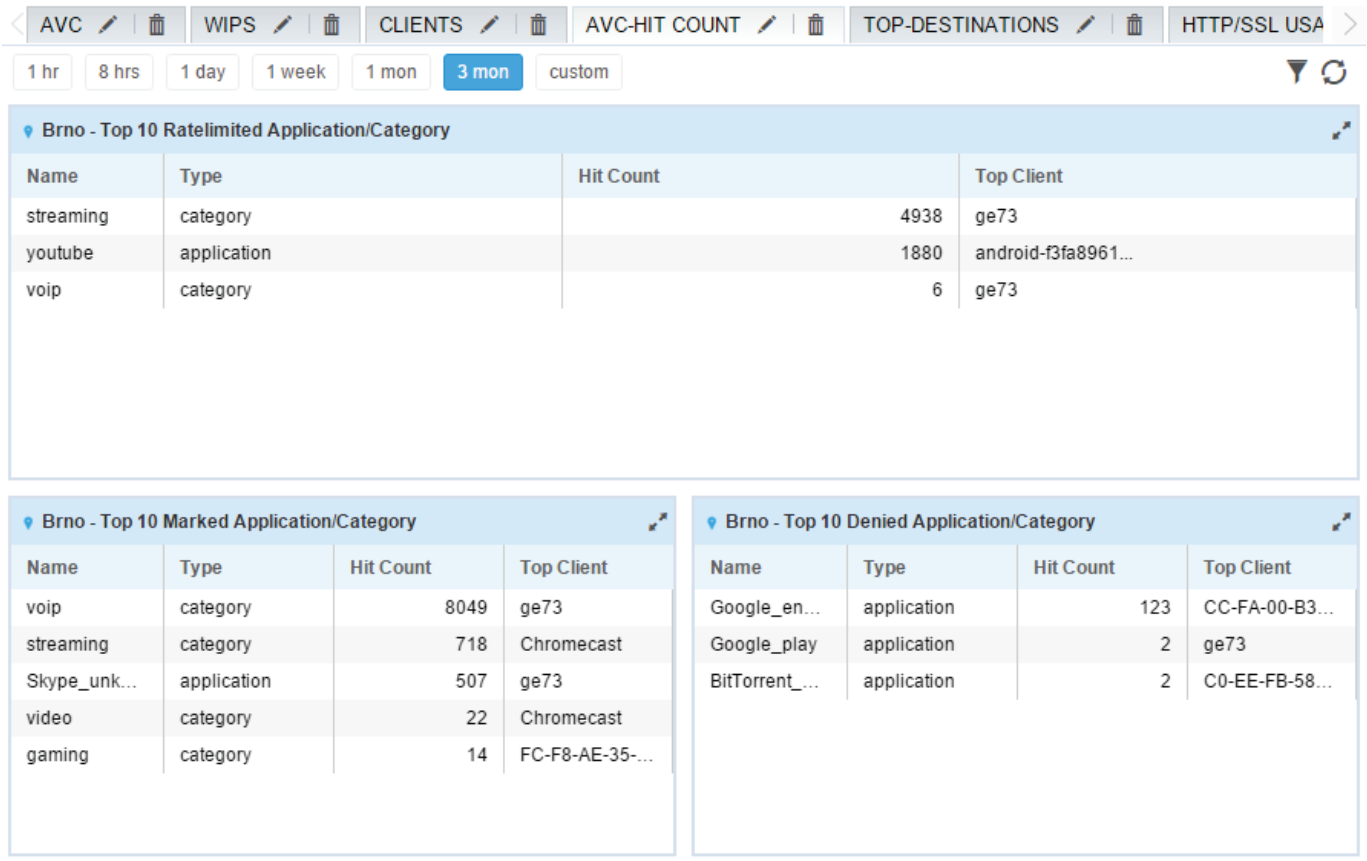
Note

Refer to *Application Visibility and Control How To* for detailed configuration instructions

Brno - All Applications by usage [wlan: all]

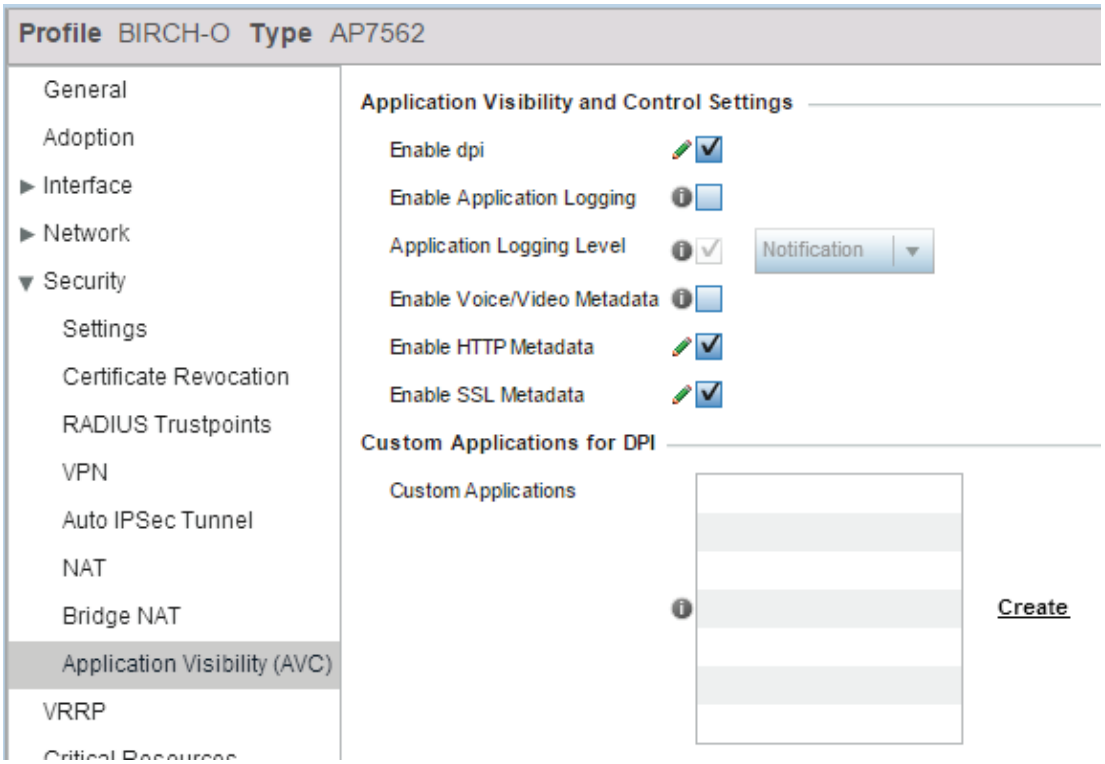
Application...	Category	Usage ↓	Total Clients	Top Client
HTTP_generic	web	3.60 GB	7	android-9c588660...
Silverlight	streaming	2.38 GB	1	Chromecast
Google_en...	web	1.76 GB	7	Chromecast
youtube	streaming	1.33 GB	4	ZCZ09TMECGJ864
dropbox	filetransfer	941 MB	1	android-a660809d...
facebook	social networking	785 MB	5	android-a660809d...
itunes	streaming	540 MB	1	Marias-iPad
googledocs	business	291 MB	4	android-9c588660...
MPEG	streaming	227 MB	2	android-9c588660...
FTP_data	filetransfer	221 MB	0	NA
instagram	mobile	168 MB	3	android-a660809d...
Skype for B...	business	134 MB	0	NA
gmail	mail	110 MB	6	ZCZ09TMECGJ864





Extreme AVC: HTTP / SSL top 10 destinations Visited or by Usage

Starting from WiNG 5.8.2.0 release on certain AP and controller platforms it is possible to enable HTTP and SSL metadata analysis using built-in DPI engine and log information.



NSight will provide visibility on the top 10 destinations visited or top 10 destinations by traffic usage. Information is available for any time period on a per RF Domain / AP / client basis.

1 hr | 8 hrs | 1 day | 1 week | **1 mon** | 3 mon | custom

Brno - Top Destinations Visited [proto: All]

Destination	Application	Category	Usage	# Hits	Top Client
outlook.com	SSL_generic	tunnel	96.8 MB	6959	android-9c588...
*.moxx-mobility.com	SSL_generic	tunnel	32.0 MB	3693	40-83-DE-94-...
clients4.google.com	Google_encry...	web	4.36 GB	3690	android-d14a...
Unknown destination	SSL_generic	tunnel	8.99 GB	3577	ZCZ09TMECG...
outlook.office365.com	SSL_generic	tunnel	135 MB	2274	ZCZ09TMECG...
www.googleapis.com	Google_encry...	web	122 MB	2175	24-DB-ED-45-...
android.clients.google.com	SSL_generic	tunnel	56.2 MB	2148	android-a660...
clients3.google.com	Google_encry...	web	39.0 MB	2050	CC-FA-00-B3-...
upload.drive.google.com	gmail	mail	15.6 GB	1735	ZCZ09TMECG...
api.vk.com	HTTP_generic	web	10.1 MB	1571	Marias-iPad

Brno - Top Destinations By Usage [proto: All]

Destination	Application	Category	Usage	# Hits	Top Client
upload.drive.google.com	gmail	mail	15.6 GB	1735	ZCZ09TMECG...
Unknown destination	SSL_generic	tunnel	8.99 GB	3577	ZCZ09TMECG...
r13---sn-2gb7ln76.c.doc-0-0-sj.sj.google...	googledocs	business	8.60 GB	4	android-9c588...
clients4.google.com	Google_encry...	web	4.36 GB	3690	android-d14a...
spynet2.microsoft.com	SSL_generic	tunnel	4.30 GB	36	FC-F8-AE-35-...
*.vo.msecnd.net	SSL_generic	tunnel	4.30 GB	24	android-a660...
localhost.localdomain	SSL_generic	tunnel	3.61 GB	65	ZCZ09TMECG...
fg.v4.b1.download.windowsupdate.com	HTTP_generic	web	2.90 GB	2	00-26-82-95-7...
cn800.airwatchportals.com	SSL_generic	tunnel	2.57 GB	82	EMEATECHLAB
au.v4.download.windowsupdate.com	HTTP_generic	web	2.41 GB	169	ZCZ09TMECG...

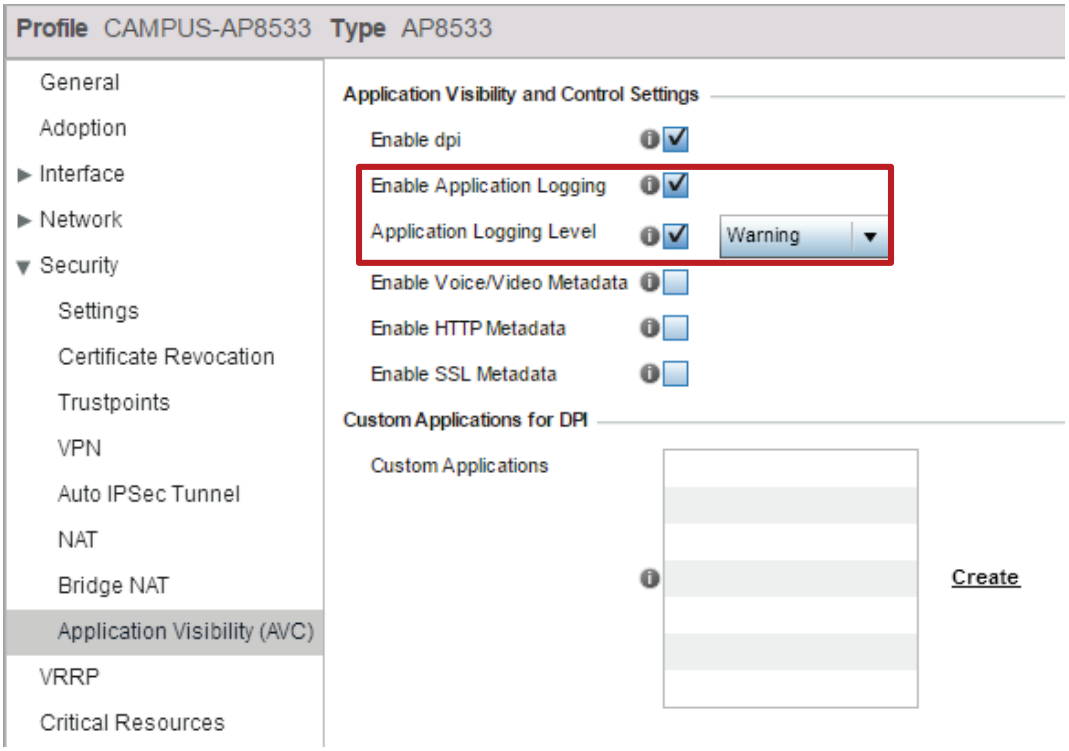
DPI Logging

In certain situations, in some countries it might be necessary to retain data amount all the communication that is happening on the public guest network. In such cases it is possible to utilize Deep Packet Inspection logging in order to obtain information about each firewall flow for each guest client.

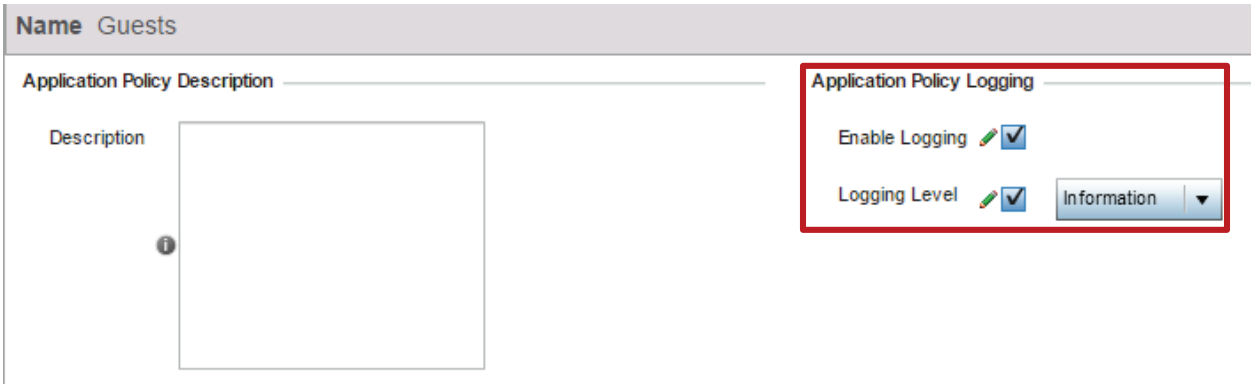
DPI logging can be **global** or per **Application Policy**.

GUI Configuration

Profile -> Profile Name -> Security -> Application Visibility (AVC)



Network -> Application Policy -> <Name>



CLI Configuration (Device Profile Level)

```
!
profile ap8533 CAMPUS-AP8533
 no mint mlcp vlan
 trustpoint https extremenoc
 interface radio1
  wlan TMELABS-GUEST bss 1 primary
 interface radio2
  wlan TMELABS-GUEST bss 1 primary
 interface radio3
 interface ge1
  switchport mode access
  switchport access vlan 1
 interface ge2
 interface vlan1
  ip address dhcp
  ip dhcp client request options all
 interface pppoe1
 use firewall-policy default
 use captive-portal server TMELABS-GUEST
 logging on
 service pm sys-restart
 router ospf
 dpi
 dpi logging on
 dpi logging level errors
!
```

CLI Configuration (Application Policy Level)

```
!
application-policy Guests
 logging on
 logging level informational
!
```

An example of the DPI message can be found below:

```
Mar 28 13:51:47 2016: %DATAPLANE-3-: Matched application 823:SSL_generic category tunnel Src MAC:<10-68-3F-
70-FD-10> Dst MAC:<5C-0E-8B-1A-DF-88> EtherType:0x0800 Src IP:192.168.70.197 Dst IP:172.217.18.68 Proto:6
Src Port:40923 Dst Port:443 .
Mar 28 13:51:47 2016: %DATAPLANE-3-: Matched application 239:DNS category network management Src MAC:<10-
68-3F-70-FD-10> Dst MAC:<5C-0E-8B-1A-DF-88> EtherType:0x0800 Src IP:192.168.70.197 Dst IP:208.67.222.222
Proto:17 Src Port:29629 Dst Port:53 .
Mar 28 13:51:43 2016: %DATAPLANE-3-: Matched application 600:HTTP_generic category web Src MAC:<5C-0E-8B-
1A-DF-88> Dst MAC:<64-BC-0C-6A-D9-5B> EtherType:0x8100 Src IP:69.28.57.172 Dst IP:192.168.70.102 Proto:6
Src Port:80 Dst Port:38168 .
Mar 28 13:51:43 2016: %DATAPLANE-3-: Matched application 600:HTTP_generic category web Src MAC:<5C-0E-8B-
1A-DF-88> Dst MAC:<64-BC-0C-6A-D9-5B> EtherType:0x8100 Src IP:69.28.57.172 Dst IP:192.168.70.102 Proto:6
Src Port:80 Dst Port:48093 .
Mar 28 13:51:37 2016: %DATAPLANE-3-: Matched application 600:HTTP_generic category web Src MAC:<5C-0E-8B-
1A-DF-88> Dst MAC:<64-BC-0C-6A-D9-5B> EtherType:0x8100 Src IP:69.28.57.172 Dst IP:192.168.70.102 Proto:6
Src Port:80 Dst Port:47212 .
Mar 28 13:51:37 2016: %DATAPLANE-3-: Matched application 600:HTTP_generic category web Src MAC:<5C-0E-8B-
1A-DF-88> Dst MAC:<64-BC-0C-6A-D9-5B> EtherType:0x8100 Src IP:69.28.57.172 Dst IP:192.168.70.102 Proto:6
Src Port:80 Dst Port:37651 .
Mar 28 13:51:36 2016: %DATAPLANE-3-: Matched application 278:IGMP category network management Src MAC:<CC-
C7-60-1C-AB-C8> Dst MAC:<01-00-5E-00-00-16> EtherType:0x0800 Src IP:192.168.70.81 Dst IP:224.0.0.22 Proto:2
.
Mar 28 13:51:47 2016: %DATAPLANE-3-: Matched application 823:SSL_generic category tunnel Src MAC:<10-68-3F-
70-FD-10> Dst MAC:<5C-0E-8B-1A-DF-88> EtherType:0x0800 Src IP:192.168.70.197 Dst IP:172.217.18.68 Proto:6
Src Port:40923 Dst Port:443 .
```

Event System Policy

Certain events related to the Captive Portal activity can be captured and processed at the external Syslog server or sent out as an SNMP trap.

```
VX(config-event-system-policy-<POLICY-NAME>)#show context include-factory | include captive

 event captive-portal inactivity-timeout syslog on snmp off forward-to-switch off email off
 event captive-portal session-timeout syslog on snmp off forward-to-switch off email off
 event captive-portal no-service-page-sent syslog on snmp off forward-to-switch off email off
 event captive-portal server-monitor-state-change syslog on snmp off forward-to-switch off email off
 event captive-portal vlan-switch syslog on snmp off forward-to-switch off email off
 event captive-portal client-disconnect syslog on snmp off forward-to-switch off email off
 event captive-portal client-removed syslog on snmp off forward-to-switch off email off
 event captive-portal auth-success syslog on snmp off forward-to-switch off email off
 event captive-portal allow-access syslog on snmp off forward-to-switch off email off
 event captive-portal data-limit-exceed syslog on snmp off forward-to-switch off email off
 event captive-portal auth-failed syslog on snmp off forward-to-switch off email off
```

Verification and Troubleshooting

Remote-Debug Captive Portal

Starting from WiNG 5.8.1 release new remote-debug functionality allows an administrator to perform a live troubleshooting on captive portal related events filtered by specific client at certain location or an AP.

```
VX-1#remote-debug captive-portal rf-domain udolni clients 64-BC-0C-6A-D9-5B max-events 999 duration 999
events all
Printing up to 999 messages from each remote system for up to 999 seconds. Use Ctrl-C to abort
[ap7532-1] 22:47:59.346: client:Hotspot client IP: 192.168.70.102, vlan: 70, Mac: 64-BC-0C-6A-D9-5B
(hs_main.c:2371)
[ap7532-1] 22:47:59.346: client:Hotspot client 64-BC-0C-6A-D9-5B is being redirected on wlan 2 and vlan 70
(hs_main.c:2388)
[ap7532-1] 22:47:59.346: client:cpstats server: login.extremenoc.com for client 64-BC-0C-6A-D9-5B
(hs_main.c:647)
[ap7532-1] 22:47:59.346: client:ap_mac: 74-67-F7-06-FC-BD, ssid: Z-GUEST-VOUCHERS, server:
login.extremenoc.com, client 64-BC-0C-6A-D9-5B (
>>> client redirection:
[ap7532-1] 22:47:59.346: client:mu_mac: 64-BC-0C-6A-D9-5B redirect url: https://login.extremenoc.com:444
/login.html?hs_server=logi
[ap7532-1] %%%%>22:48:11.283: client:failed to resolve IPv4 address of interface vlan 70, client 64-BC-0C-
6A-D9-5B (utils.c:83)
>>> client credentials submitted via POST and RADIUS Access-Request sent:
[ap7532-1] 22:48:11.302: client:hotspot auth request received for 64-BC-0C-6A-D9-5B (extif.c:1012)
[ap7532-1] 22:48:11.302: client:handle forwarded auth request message for client[nexus:64-BC-0C-6A-D9-5B]
(extif.c:477)
[ap7532-1] 22:48:11.302: radius:aaa-policy EXT-RADIUS user: nexus mac: 64-BC-0C-6A-D9-5B
server_is_candidate: 1 0 0 0 0 0 (radius.c:4784)
[ap7532-1] 22:48:11.304: radius:access-req sent to 140.101.4.17:1812 (attempt 1) for 64-BC-0C-6A-D9-5B
(user:nexus) (radius.c:2996)
>>> receiving RADIUS attributes along with Access-Accept:
[ap7532-1] 22:48:11.359: radius:rx Vlan-Tag 70 for 64-BC-0C-6A-D9-5B (radius.c:1405)
[ap7532-1] 22:48:11.360: radius:rx Session-Start-Time [06:02:2016-19:58] for 64-BC-0C-6A-D9-5B
(radius.c:1689)
[ap7532-1] 22:48:11.361: radius:rx Session-Expiry-Time [07:02:2016-19:58] for 64-BC-0C-6A-D9-5B
(radius.c:1722)
[ap7532-1] 22:48:11.362: radius:rx Client-Group-Name [RADIUS-CAPTIVE-GUESTS] for 64-BC-0C-6A-D9-5B
(radius.c:1824)
[ap7532-1] 22:48:11.362: radius:rx Session-Timeout 3571 for 64-BC-0C-6A-D9-5B (radius.c:1331)
[ap7532-1] 22:48:11.362: radius:rx info->data_bytes_remaining 1073236022 for 64-BC-0C-6A-D9-5B
(radius.c:1798)
[ap7532-1] 22:48:11.362: radius:rx Downlink-Rate-Limit 1000 for 64-BC-0C-6A-D9-5B (radius.c:1264)
[ap7532-1] 22:48:11.362: radius:rx Uplink-Rate-Limit 1000 for 64-BC-0C-6A-D9-5B (radius.c:1267)
[ap7532-1] 22:48:11.362: radius:rx info->data_limit_bytes 1073741824 for 64-BC-0C-6A-D9-5B (radius.c:1788)
[ap7532-1] 22:48:11.362: radius:rx access-accept for 64-BC-0C-6A-D9-5B (radius.c:3493)
>>> Captive Portal opens firewall and allows access:
[ap7532-1] 22:48:11.364: client:Forwarding hs-auth-response to hsd with status Success for 64-BC-0C-6A-D9-
5B (extif.c:234)
[ap7532-1] 22:48:11.364: client:change fdb hotspot auth state for client 64-BC-0C-6A-D9-5B (extif.c:975)
[ap7532-1] 22:48:11.364: client:hotspot session timeout 3571 for client 64-BC-0C-6A-D9-5B (extif.c:1031)
[ap7532-1] 22:48:11.364: client:hotspot auth success received for mu 64-BC-0C-6A-D9-5B (extif.c:1107)
[ap7532-1] 22:48:11.364: client:adding client 64-BC-0C-6A-D9-5B to hotspot user cache (usercache.c:339)
>>> RADIUS Accounting starts:
[ap7532-1] 22:48:11.364: client:hotspot acct request received for 64-BC-0C-6A-D9-5B (extif.c:1142)
[ap7532-1] 22:48:11.365: radius:radius acct 1 is_wired 0 for 64-BC-0C-6A-D9-5B (accounting.c:1455)
[ap7532-1] 22:48:11.365: radius:assigning id 122 to pending accounting request for 64-BC-0C-6A-D9-5B
(accounting.c:1469)
```

General Captive Portal Troubleshooting Q&A

Q: Wireless Client is not being redirected to the landing page, is this a bug?

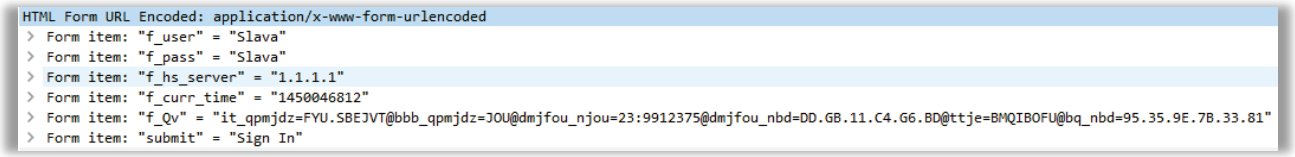
A: Most likely not. Verify and make sure the following checks out:

1. Client can resolve names via configured DNS server and client can reach internet / external networks under normal conditions without Captive Portal.
2. Captive Portal server is assigned to the device that should perform client capture and redirection. In "Self" mode captive portal server should be assigned to the Access Point profile, in "Centralized" or "Centralized-Controller" mode Captive Portal server should be assigned to the Wireless Controller.
3. Captive Portal server mode matched the architecture selected. I.e. "Self" mode should only be used when Captive Portal server is running in a distributed architecture on each Access Point. "Centralized" mode should be used on a single controller with real IP address or FQDN of the controller. "Centralized-controller" mode should be used whenever a cluster of controllers is deployed with virtual hostname.
4. If Centralized-controller mode is used SVI must be present in the Guest User VLAN with an IPv4 address to perform capture and redirection.
5. DNS whitelist must contain FQDNs or IP addresses of all the external web servers as permit rules. Additionally all the contents of the pages that refer to external sources (like ads or videos) must also be allowed in the DNS whitelist.
6. IP Access Lists assigned inbound direction on the Guest WLANs allow communication to captive portal server address on ports 444 (https mode) or 880 (http mode). In case captive portal server is running on the Access Point without any SVI in the Guest User VLAN, communication to an IP address 1.1.1.1 should be allowed.

Q: Client is able to get to landing page and submit data, but Captive Portal on the AP/Controller still block access to the client.

A: Check the following:

1. Make sure client side script is present to allow a client to make a HTTP POST and submit user credentials or terms&agreement accept to the captive portal server. Verify by taking a packet capture filtered by the client's IP address and look into the contents of HTTP POST. For example:



2. Run remote-debug captive-portal command from the CLI with client MAC as a filter and monitor the messages reported when client presses Submit or Login button.