How do I create a custom Captive Portal for public access?

Information

Introduction

Feature Notes

Environment

Network Topology

Configuration Steps

Answer

Product and Software: This article applies to all Aruba controllers and ArubaOS version 2.5 and later.

Introduction
The Aruba built-in Captive Portal login pages were designed to provide the means to authenticate users through a username/password combination and/or to provide guest access by prompting guest users for their email address.

Prompting users to identify themselves is based on the Aruba controller firewall design where a user is initially placed in a "logon" role that highjacks his web access and presents him with the Captive Portal page. After identifying himself, the user is moved to a different role that grants the appropriate web access.

To provide users with a Captive Portal page that requires no user entry, but just a button to accept Internet use terms conditions, we must work around these requirements.

Assumptions
The following assumptions apply to the configuration example:

- A valid Policy Enforcement Firewall (PEF) license is installed.
- The software version on the controller is 3.x.
- The VLAN 100 and DHCP servers of the Captive Portal users are already defined.
- The SSID profile "public" with essid "public" is already defined.

Implementation
To configure an Aruba controller to present a custom captive portal that requires no user information entry, follow these steps:

Step1: Ensure that the "captiveportal" ACL contains the following rules.
(config) #ip access-list session captiveportal
user alias mswitch svc-http dst-nat 8080
user alias mswitch svc-https dst-nat 8081
user any svc-http dst-nat 8080
user any svc-https dst-nat 8081

Step 2: Ensure that the "logon-control" ACL contains the following rules.
(config) # ip access-list session logon-control
user any udp 68 deny
any any svc-icmp permit
any any svc-dns permit
any any svc-dhcp permit

Step 3: Define a new captive portal profile "public-cp".
(config)# aaa authentication captive-portal "public-cp"
no user-logon
guest-logon
no logout-popup-window
no enable-welcome-page

Step 4: Define the captive portal initial role "cp-logon" to use the captive portal profile defined in the previous step.
(config) #user-role cp-logon
captive-portal public-cp
session-acl logon-control
session-acl captiveportal

Step 5: Define an AAA profile "public" that uses the captive portal initial role defined in the previous step.
(config) # aaa profile "public"
initial-role "cp-logon"
authentication-dot1x "default-psk" (only if pre-shared key is used)

Step 6: Define a new virtual ap profile "vap-public" for the captive portal users.
(config) #wlan virtual-ap "vap-public"
ssid-profile "public" (Assumed to be already defined)
vlan 100 (Assumed to be already defined)
aaa-profile "public" (Defined in the previous step)

Step 7: Define the Captive Portal ACL and Role "guest" to control Internet access.
(config) #ip access-list session guest
user any udp 68 deny
any any svc-dhcp permit
user any svc-dns permit
user any svc-http permit
user any svc-https permit
user any svc-icmp permit
!
(config) #user-role guest
session-acl guest

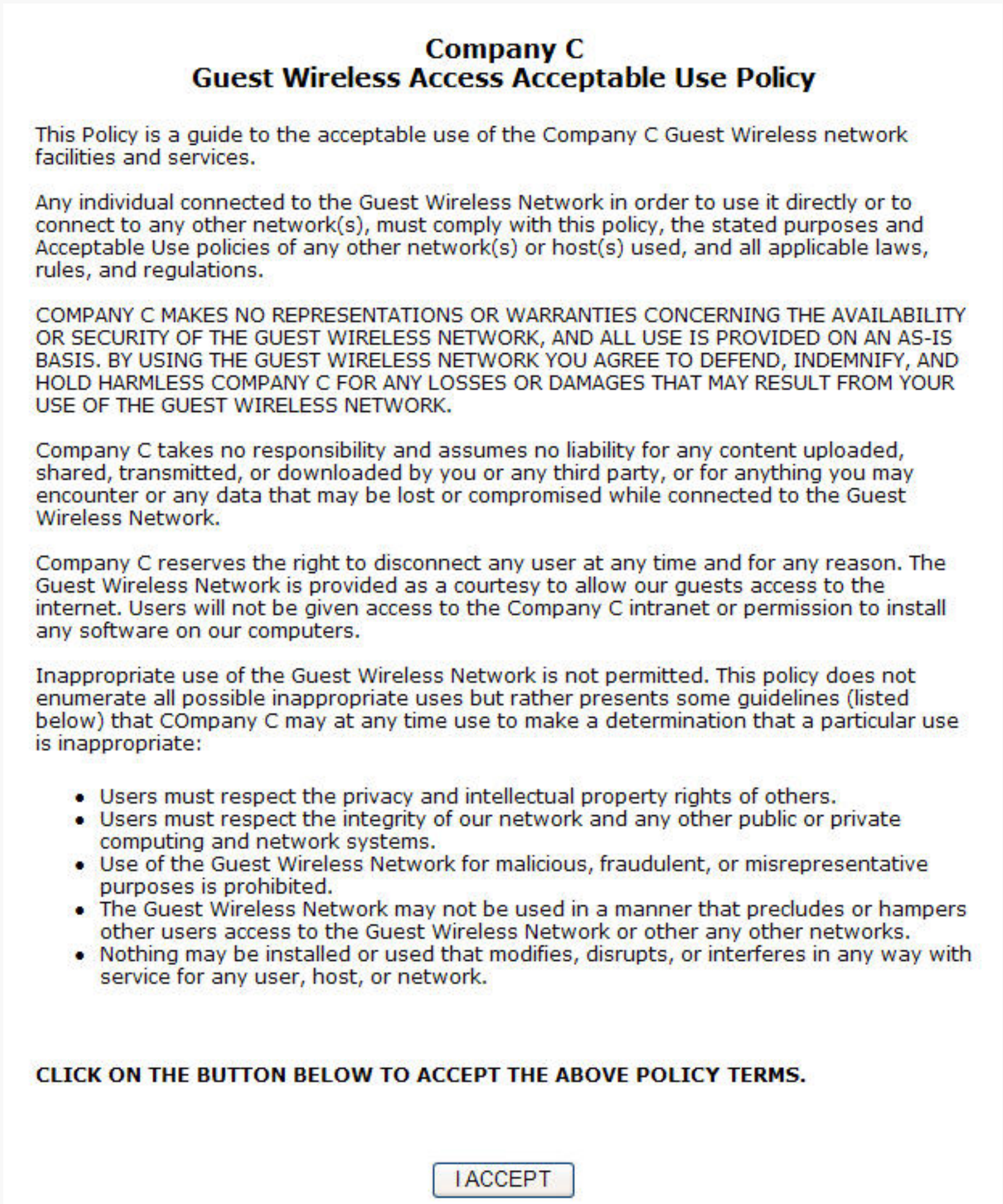
Step 8: Create your custom captive portal page that uses the FORM POST defined in the template provided below:

```
<META HTTP-EQUIV="Content-Type" CONTENT="text/html; charset=iso-8859-1">
<!DOCTYPE HTML PUBLIC"-//W3C//DTD HTML 4.01 Transitional//EN">
<html>
<head>
<title>Public wireless Internet access</title>

<style type="text/css">
body {
font-family: Verdana, Arial, Helvetica, sans-serif;
font-size: 12px;
background-color: #FFFFFF;
margin: 10px;
padding: 10px;
}
h1 { font-size: 16px; font-weight: bold; }
h2 { font-size: 14px; font-weight: bold; }
p, ul, li, input { }
</style>
</head>
<body>
<h1 align="center">Company C<br/>Guest Wireless Access Acceptable Use Policy</h1>
<p>
This Policy is a guide to the acceptable use of the Company C Guest Wireless network facilities and services.
<br/><br/>
Any individual connected to the Guest Wireless Network in order to use it directly or to connect to any other network(s), must comply with this policy, the stated purposes and Acceptable Use policies of any other network(s) or host(s) used, and all applicable laws, rules, and regulations.
<br/><br/>
COMPANY C MAKES NO REPRESENTATIONS OR WARRANTIES CONCERNING THE AVAILABILITY OR SECURITY OF THE GUEST WIRELESS NETWORK, AND ALL USE IS PROVIDED ON AN AS-IS BASIS. BY USING THE GUEST WIRELESS NETWORK YOU AGREE TO DEFEND, INDEMNIFY, AND HOLD HARMLESS COMPANY C FOR ANY LOSSES OR DAMAGES THAT MAY RESULT FROM YOUR USE OF THE GUEST WIRELESS NETWORK.
<br/><br/>
Company C takes no responsibility and assumes no liability for any content uploaded, shared, transmitted, or downloaded by you or any third party, or for anything you may encounter or any data that may be lost or compromised while connected to the Guest Wireless Network.
<br/><br/>
Company C reserves the right to disconnect any user at any time and for any reason. The Guest Wireless Network is provided as a courtesy to allow our guests access to the internet. Users will not be given access to the Company C intranet or permission to install any software on our computers.
<br/><br/>
Inappropriate use of the Guest Wireless Network is not permitted. This policy does not enumerate all possible inappropriate uses but rather presents some guidelines (listed below) that COmpany C may at any time use to make a determination that a particular use is inappropriate:
</p>
<ul>
<li>Users must respect the privacy and intellectual property rights of others.</li>
<li>Users must respect the integrity of our network and any other public or private computing and network systems.</li>
<li>Use of the Guest Wireless Network for malicious, fraudulent, or misrepresentative purposes is prohibited.</li>
<li>The Guest Wireless Network may not be used in a manner that precludes or hampers other users access to the Guest Wireless Network or other any other networks.</li>
<li>Nothing may be installed or used that modifies, disrupts, or interferes in any way with service for any user, host, or network.</li>
</ul>
<br><br>
<b>CLICK ON THE BUTTON BELOW TO ACCEPT THE ABOVE POLICY TERMS.</b></font></div>
<div align="center">
<br><br><br>
<form name="form1" method="post" action="/auth/index.html/u">
<span class="bodytext">
<input type="hidden" id="email" name="email" type="text" value="user@company.com" class="text" accesskey="e" />
<input type="hidden" name="cmd" value="authenticate" />
<input type="submit" name="Login" value="I ACCEPT" class="button" />
</span>
</form>
</div>
</body>
```

</html

Here is a screenshot that of the corresponding Captive Portal page:



Company C
Guest Wireless Access Acceptable Use Policy

This Policy is a guide to the acceptable use of the Company C Guest Wireless network facilities and services.

Any individual connected to the Guest Wireless Network in order to use it directly or to connect to any other network(s), must comply with this policy, the stated purposes and Acceptable Use policies of any other network(s) or host(s) used, and all applicable laws, rules, and regulations.

COMPANY C MAKES NO REPRESENTATIONS OR WARRANTIES CONCERNING THE AVAILABILITY OR SECURITY OF THE GUEST WIRELESS NETWORK, AND ALL USE IS PROVIDED ON AN AS-IS BASIS. BY USING THE GUEST WIRELESS NETWORK YOU AGREE TO DEFEND, INDEMNIFY, AND HOLD HARMLESS COMPANY C FOR ANY LOSSES OR DAMAGES THAT MAY RESULT FROM YOUR USE OF THE GUEST WIRELESS NETWORK.

Company C takes no responsibility and assumes no liability for any content uploaded, shared, transmitted, or downloaded by you or any third party, or for anything you may encounter or any data that may be lost or compromised while connected to the Guest Wireless Network.

Company C reserves the right to disconnect any user at any time and for any reason. The Guest Wireless Network is provided as a courtesy to allow our guests access to the internet. Users will not be given access to the Company C intranet or permission to install any software on our computers.

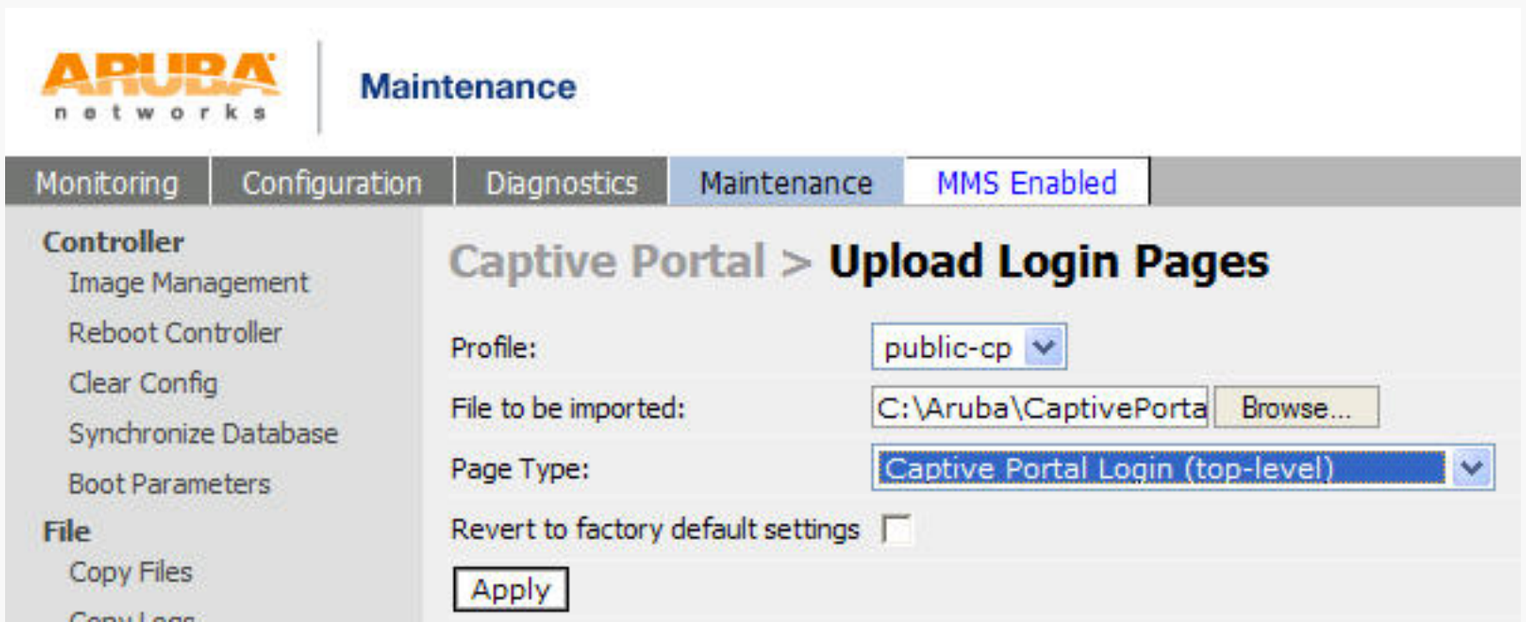
Inappropriate use of the Guest Wireless Network is not permitted. This policy does not enumerate all possible inappropriate uses but rather presents some guidelines (listed below) that COmpany C may at any time use to make a determination that a particular use is inappropriate:

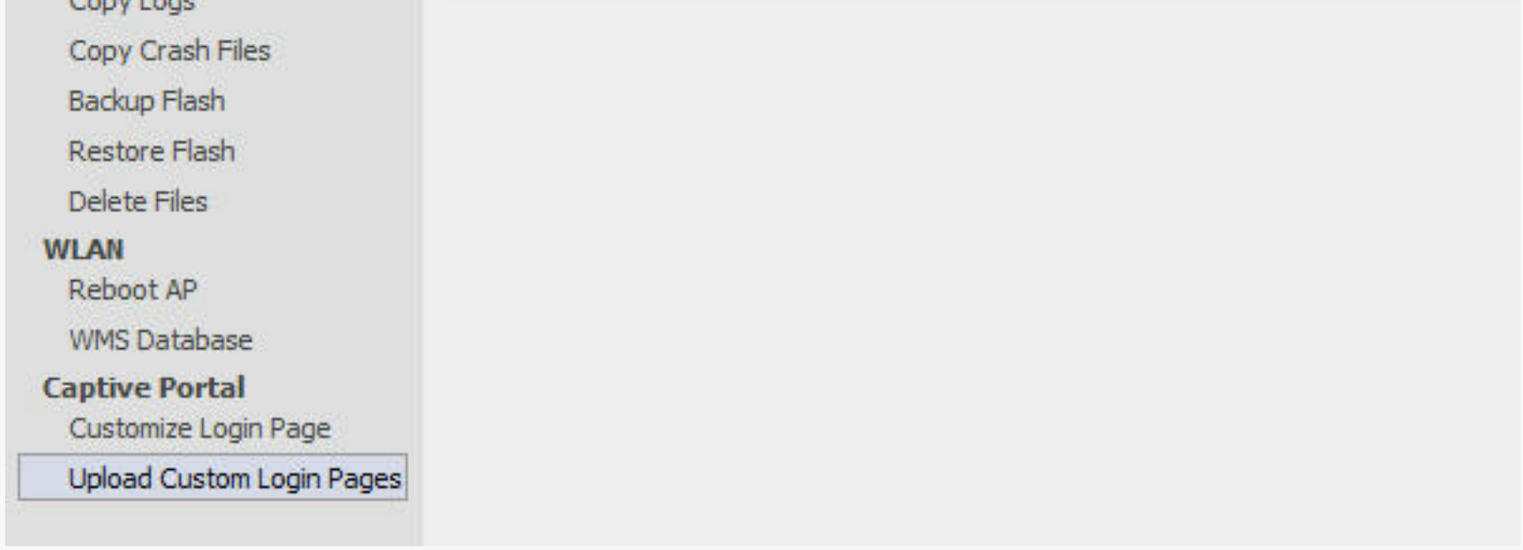
- Users must respect the privacy and intellectual property rights of others.
- Users must respect the integrity of our network and any other public or private computing and network systems.
- Use of the Guest Wireless Network for malicious, fraudulent, or misrepresentative purposes is prohibited.
- The Guest Wireless Network may not be used in a manner that precludes or hampers other users access to the Guest Wireless Network or other any other networks.
- Nothing may be installed or used that modifies, disrupts, or interferes in any way with service for any user, host, or network.

CLICK ON THE BUTTON BELOW TO ACCEPT THE ABOVE POLICY TERMS.

I ACCEPT

Step 9: Upload the custom captive portal page to the controller via the WebUI as per the following screenshot:





Important Notes

1. The email string "user@company.com" in the FORM POST could be customized to reflect the user name that will appear in the controller user table.
2. The Captive Portal role will always be "guest" since we are leveraging a "hidden" guest access.
3. In the case where multiple Captive Portal pages are desired, each with its own role and username displayed in the controller user table, a few amendments are need to the above steps:

3.1 Change the captive portal profile to disable guest access and enable user logon:
(config)# aaa authentication captive-portal "public-cp"
user-logon
no guest-logon
no logout-popup-window
no enable-welcome-page
3.2 Add a username, password, and desired role to the controller Internal DB.
example: user1 passwd1 role1
3.3 Define the new role "role1" with the appropriate ACLs.
3.4 Ensure that the AAA profile makes use of the Internal DB as the authentication server.
3.5 Modify the FORM POST in the captive portal login page as follows:

```
<form name="form1" method="post" action="/auth/index.html/u">
<span class="bodytext">
<input type="hidden" name="user" id="user" type="text" value="user1" class="text" accesskey="u" />
<input type="hidden" id="password" name="password" type="text" value="passwd1" class="text" accesskey="p" />
<input type="hidden" name="cmd" value="authenticate" />
<input type="submit" name="Login" value="I ACCEPT" class="button" />
</span>
</form>
```

User-table before and after clicking the "I ACCEPT" button:

```
(A800) #show user

Users
-----
IP MAC Name Role Age(d:h:m) Auth VPN link AP name Roaming Essid/Bssid/Phy Profile
---------- ------------ ------ ---- ---------- ---- -------- ------- ------- --------------- -------
10.168.84.14 00:13:02:20:4b:43 cp-logon 00:00:00 00:0b:86:cb:5a:5c Associated public/00:0b:86:35:a5:c0/g public

User Entries: 1/1

(A800) #
(A800) #show user-table

Users
-----
IP MAC Name Role Age(d:h:m) Auth VPN link AP name Roaming Essid/Bssid/Phy Profile
---------- ------------ ------ ---- ---------- ---- -------- ------- ------- --------------- -------
10.168.84.14 00:13:02:20:4b:43 user1 role1 00:00:00 Web 00:0b:86:cb:5a:5c Associated public/00:0b:86:35:a5:c0/g public
```

Verification

Troubleshooting

How To Doc

Related Links

Original article ID 154

Feedback

Was this article helpful?
Yes No