Technical Guide

ecCLOUD AuthPort Configuration

Released: 2024-12-12

Table of Contents

1. Introduction

This technical guide is aimed at helping readers learn how to enable and configure settings for “AuthPort”, an add-on available on ecCLOUD. The purpose of AuthPort is to allow ecCLOUD users to manage network access and regulate network usage of their wireless clients.

With AuthPort, ***authentication, authorization, and accounting (AAA) of wireless clients*** can be performed using ecCLOUD’s built-in authentication server and account database. The “AuthPort” add-on available on ecCLOUD only supports RADIUS feature with ***username/password*** authentication. It means that "AuthPort" on ecCLOUD contains RADIUS server function. The authentication format of RADIUS supports Open, Personal and Enterprise (802.1x) (PEAP and EAP-TTLS).

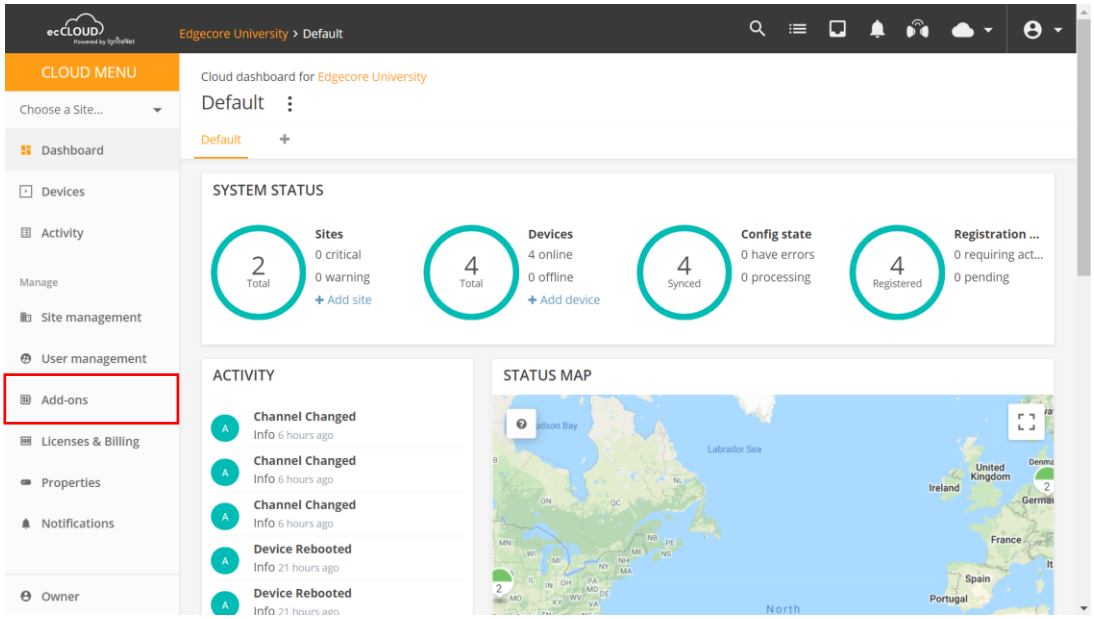
A ***captive portal editor*** is also included in AuthPort for easy captive portal customization, and multiple captive portals can be saved.After enabling AuthPort from the “Add-ons” page, it can then be enabled in configuration settings of each SSID, and the desired captive portal can be selected subsequently. Thus, wireless clients that associate to an SSID with AuthPort enabled will be presented the selected captive portal for login.

Accounts used for login via the captive portal should be pre-generated in AuthPort by ecCLOUD users, and each account is linked to a self-defined ***service plan***, which specifies constraints on network usage. Thus, service plans should be added before accounts can be created. In this way, network usage of wireless clients can be governed by the service plans associated with the accounts they log in with.

2. Enable AuthPort from Add-Ons Page

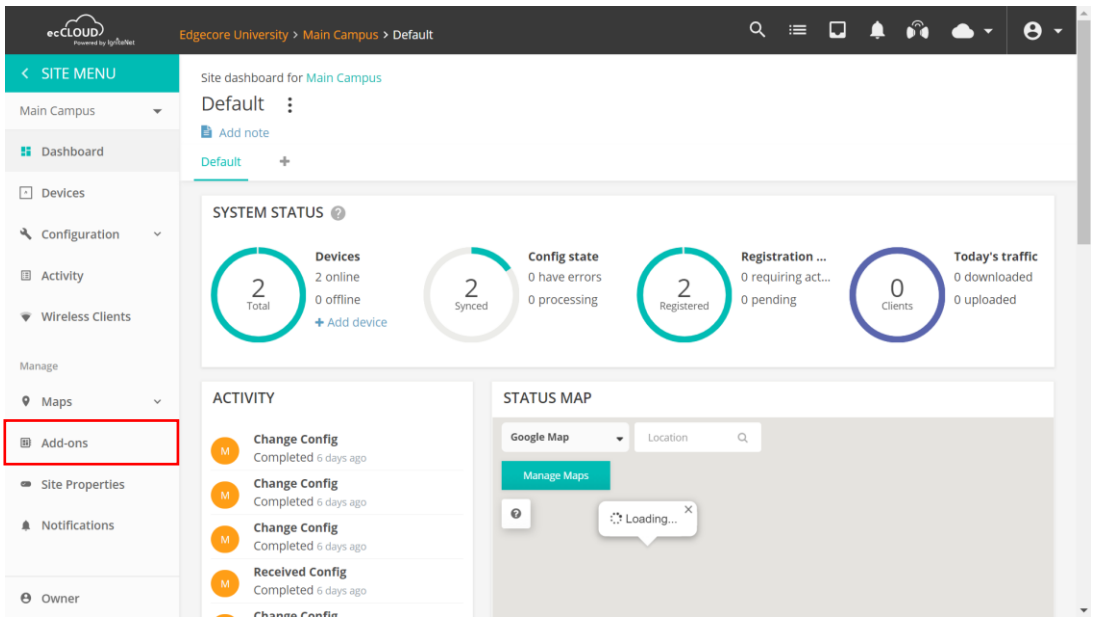
AuthPort can be enabled at the cloud level or at the site level depending on the deployment scenario. If enabled at the cloud level, AuthPort will be enabled for all the sites under this cloud at once. If you would like to enable AuthPort for only certain sites, please go to these sites and enable this add-on from the Add-ons page at the site level.

a. To enable AuthPort at the cloud level, click on "**Add-ons**" on the Cloud Menu

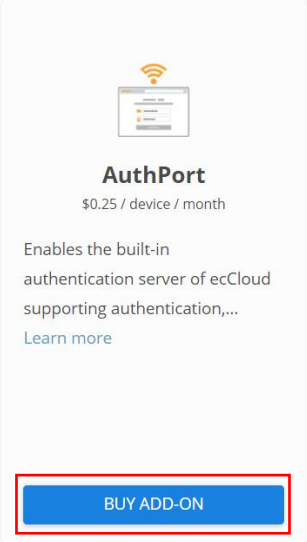


Or

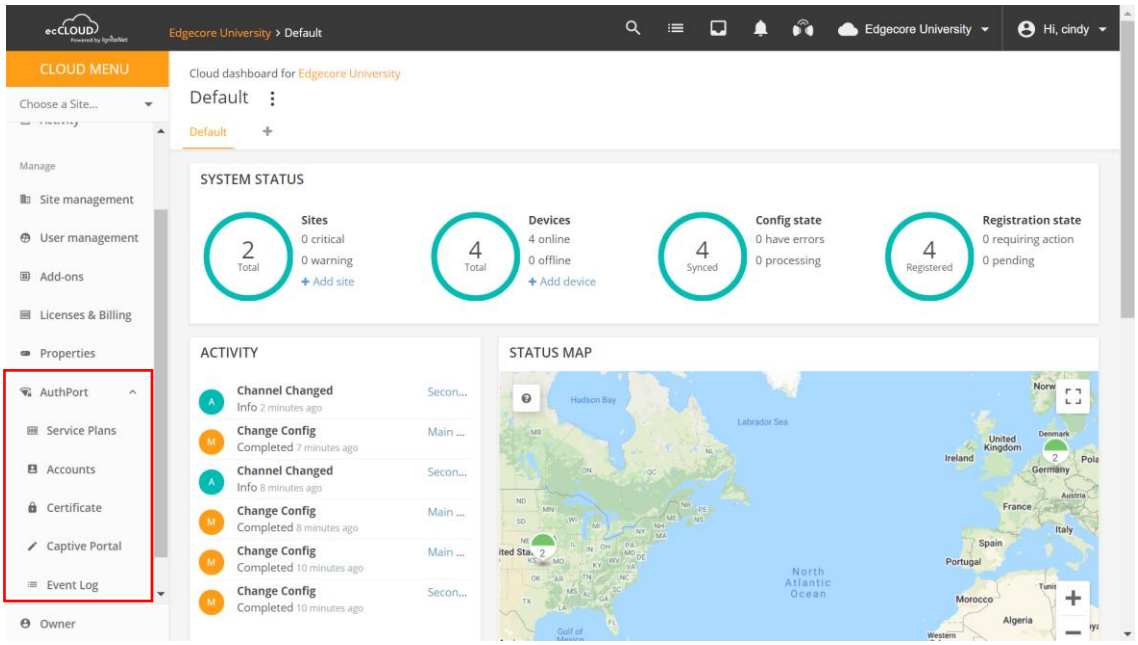
To enable AuthPort for a site, go to the site and click on **"Add-ons"** on the Site Menu



b. On the Add-ons page, find AuthPort and click on "**BUY ADD-ON**". Follow on-screen instructions to confirm purchase.



c. Once the purchase is completed, AuthPort will appear on the Cloud Menu under Manage. Clicking on AuthPort reveals a submenu.

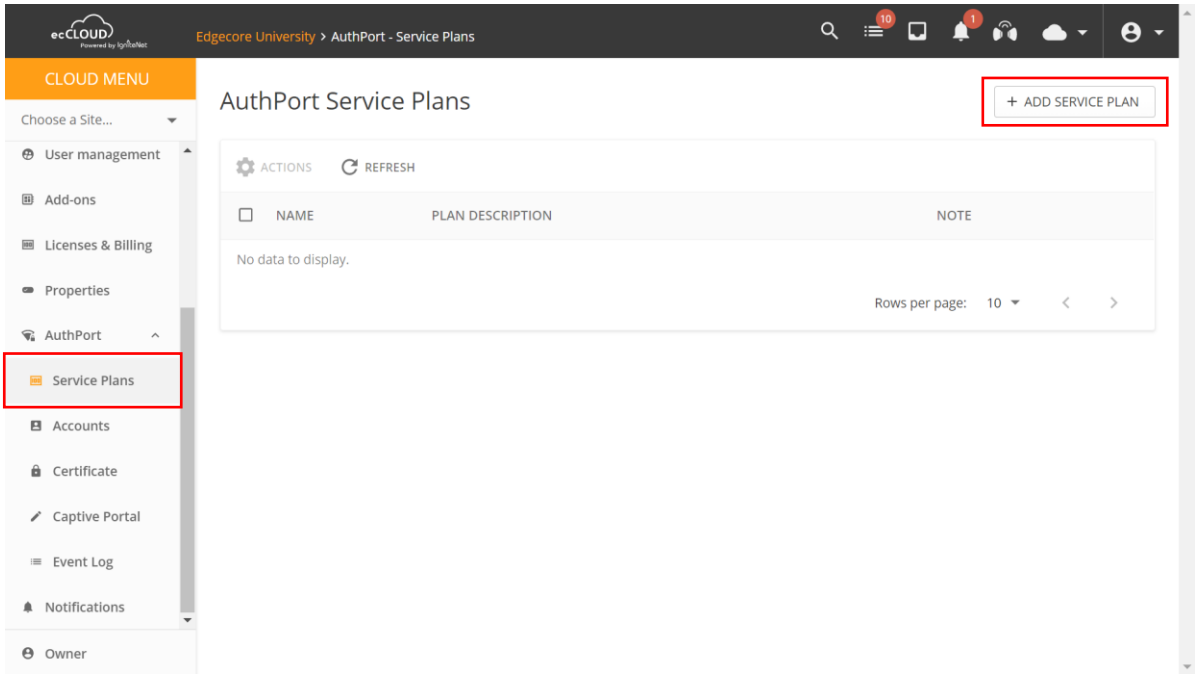


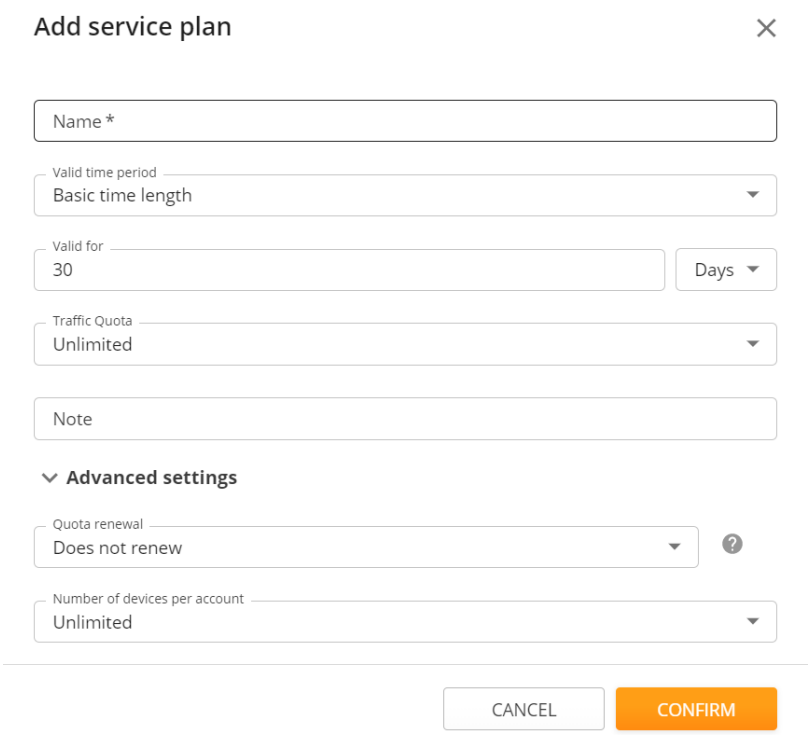
3. Configure AuthPort Settings: Add Service Plans and Generate Accounts

On the AuthPort submenu, first add at least one service plan. In a service plan, time, data and/or device number constraints can be specified as desired. Once one or more service plans have been added, accounts can then be generated where each account links to a specific service plan.

3.1 Add Service Plans

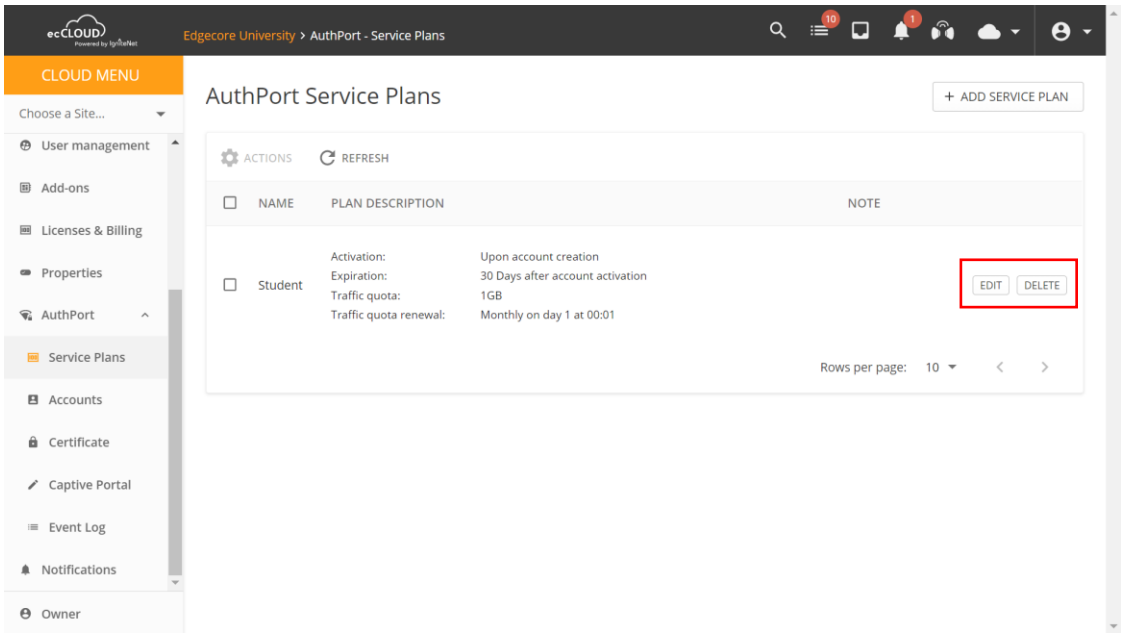
a. Go to "**Cloud Menu > AuthPort > Service Plan**" and click on "**ADD SERVICE PLAN**"





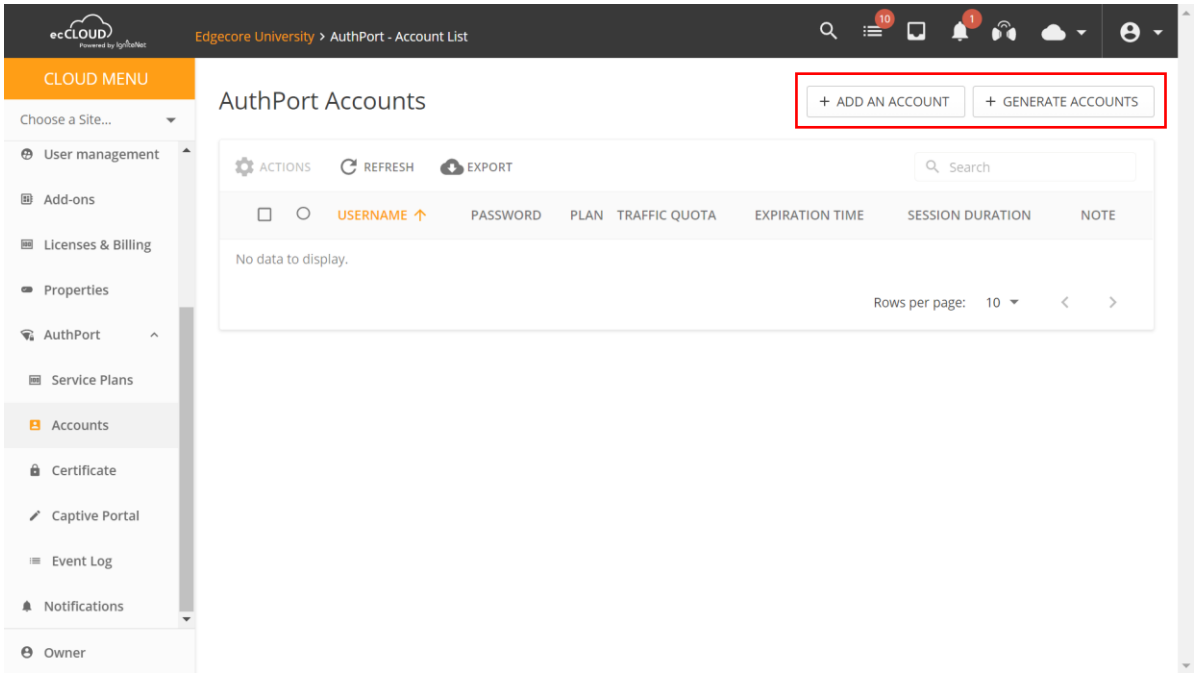
- **Name**: Name of the service plan.
- **Valid time period**: The time period during which the account is valid.
    - Select "**Basic time length**" if you want the account to be valid for a certain time duration, and you can define the time duration in seconds, minutes, hours or days in the field "Valid for" below.
    - Select "**Custom**" if you want to the account to be activated at a specific time, and the account can also expire at certain time or after a time duration. For account activation, select "Activate upon account creation" for the account to be activated at the same time it's created; select "Activate before" for the account to be activated before a specific date and time as defined in the next field. For account expiration, select "Does not expire" for the account to remain valid unless it has reached the defined traffic quota (see below for description of traffic quota), if any; select "Expires in" for the account to expire after a certain time period as defined in the next field; or select "Expires on" for the account to expire on a specific date and at a specific time.
- **Traffic quota**:
    - Select "**Custom**" to define a data cap for the account to become invalid once the cap is reached.
    - Select "**Unlimited**" to allow the account to enjoy unlimited data usage.
- **Quota renewal**: If configured, the defined traffic quota can be renewed daily, weekly or monthly for the account within the time frame set.
- **Number of devices per account**: Select "Custom" for the account to be shared by only a limited number of devices as defined in the next field; select "Unlimited" for the account to be shared by

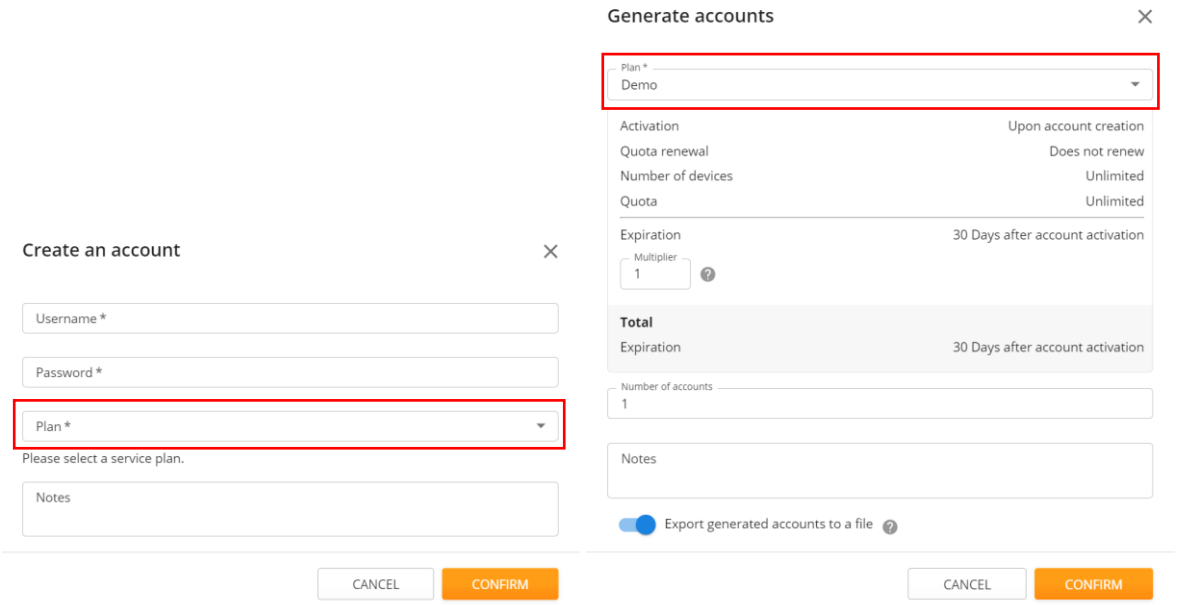
Once a service plan has been added, it can be edited or deleted from this page.



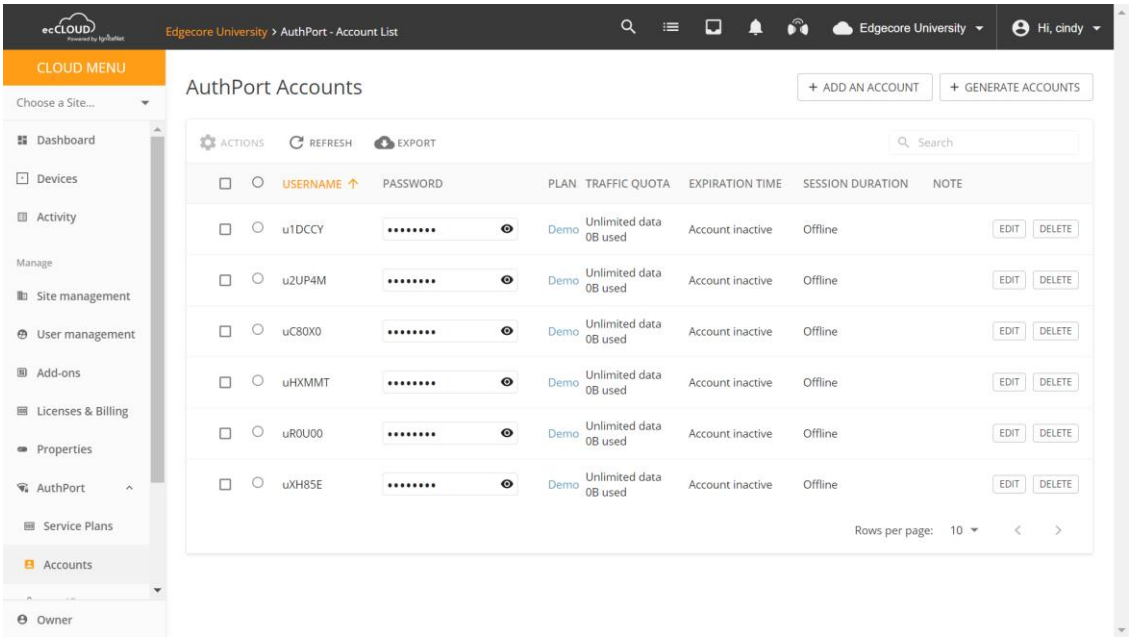
3.2 Generate Accounts

a. Go to "**Cloud Menu > AuthPort > Accounts**", and click on "**ADD AN ACCOUNT**" to add one account or "**GENERATE ACCOUNTS**" to add multiple accounts. Note that a service plan has to be selected when generating accounts.



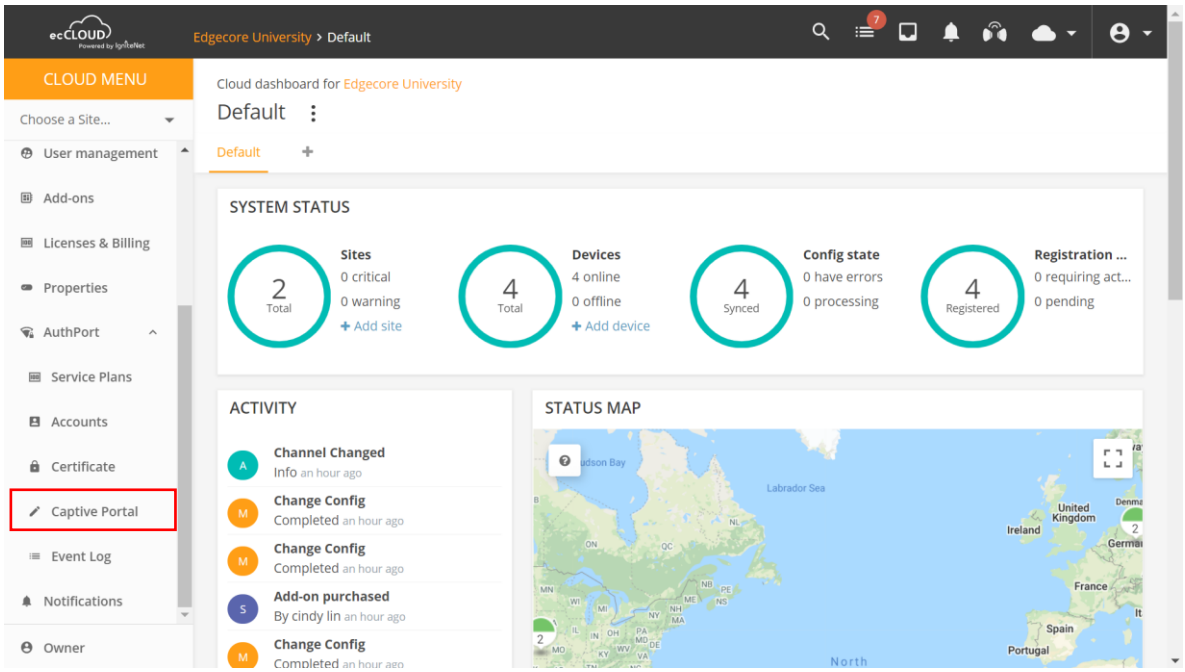


b. Once accounts have been generated, they will appear on the same page.

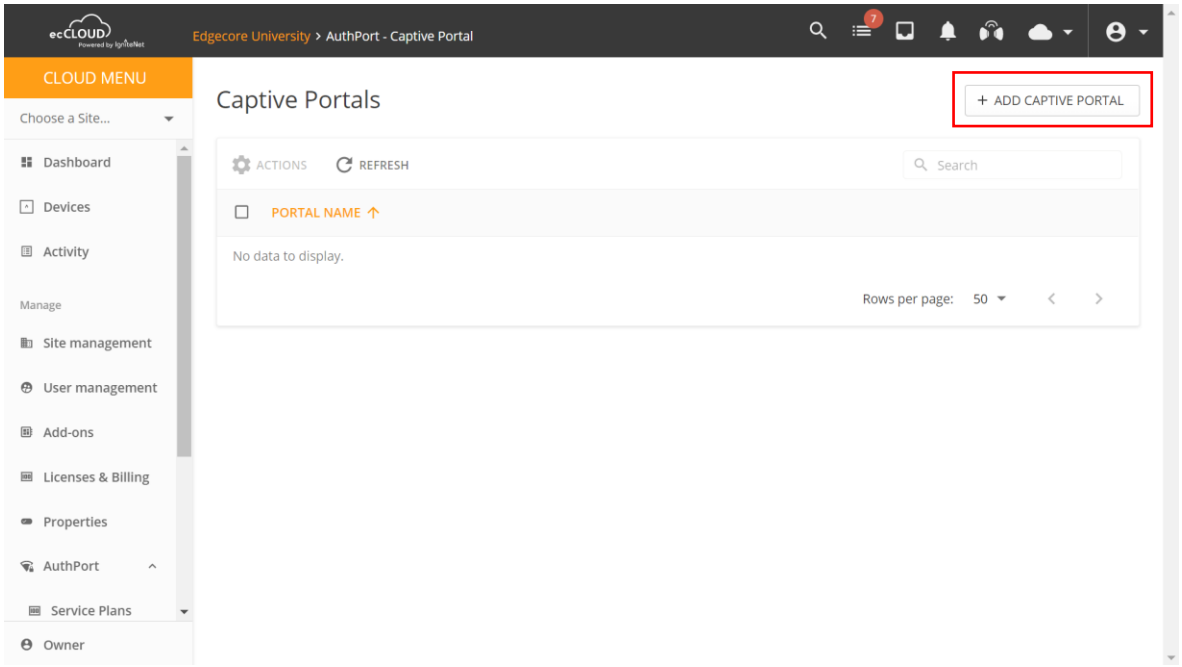


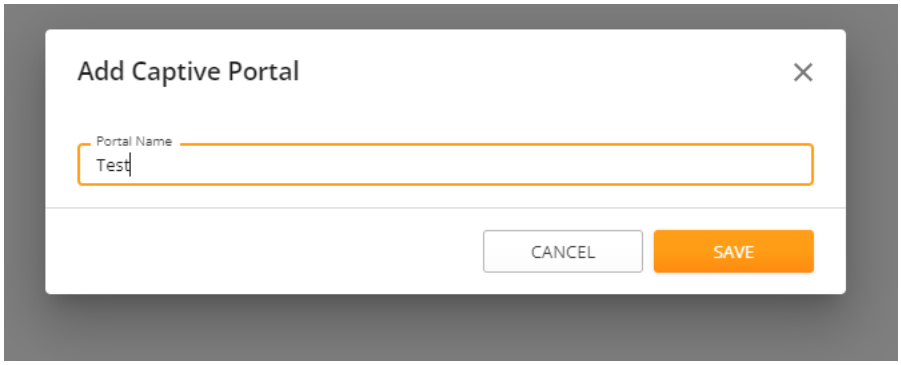
4. Configure AuthPort Settings: Add Customized Captive Portals

a. On the "**AuthPort**" submenu, click on "**Captive Portal**".

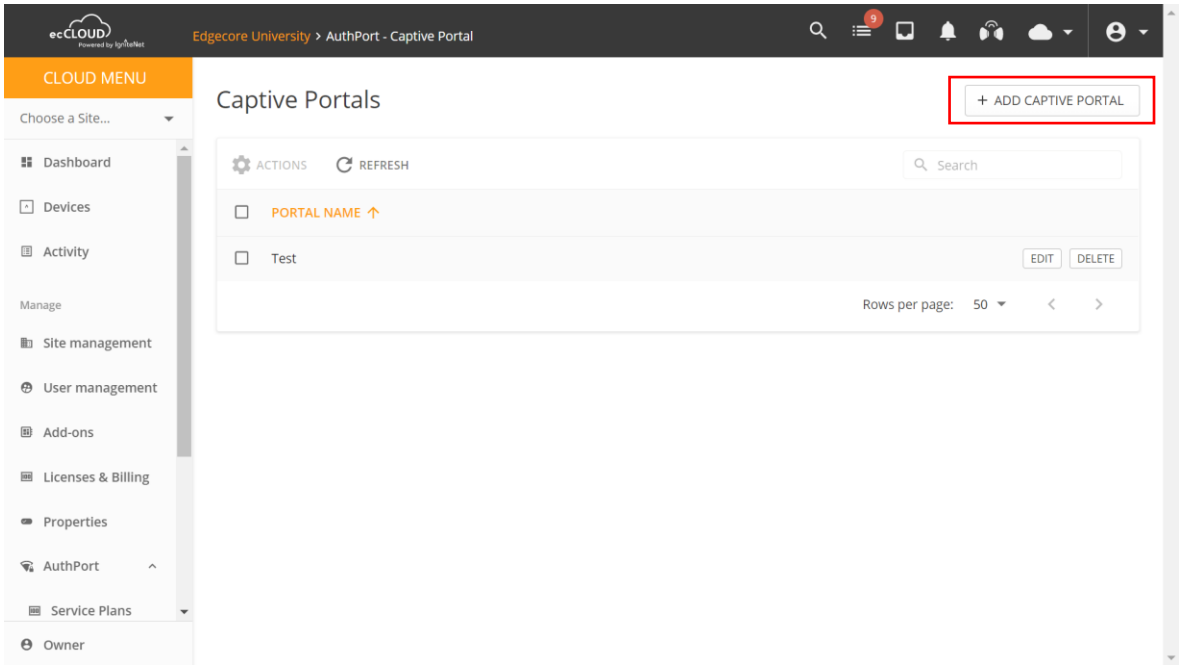


b. Once on the Captive Portal page, click on "**ADD CAPTIVE PORTAL**" to add a new captive portal to begin customizing it.

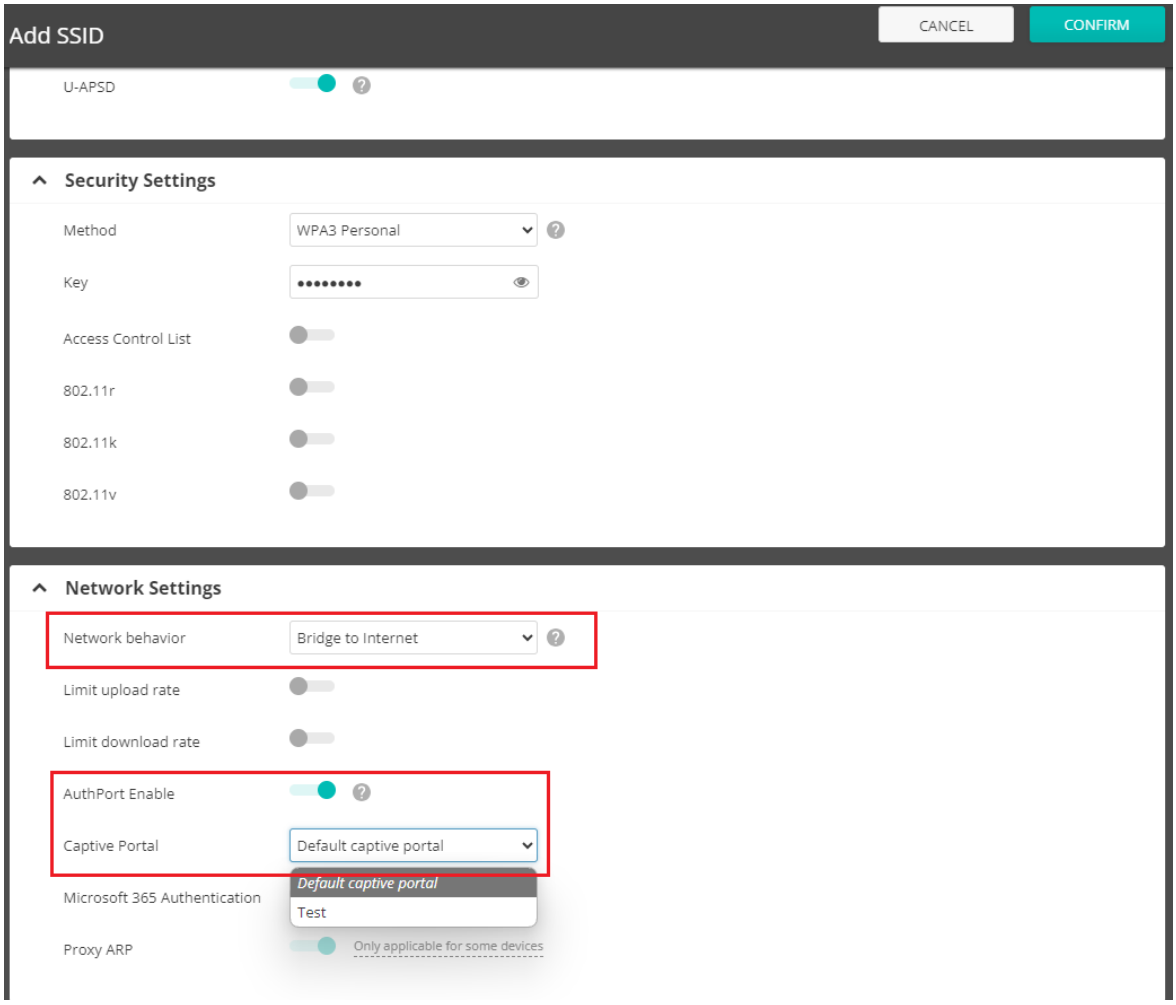




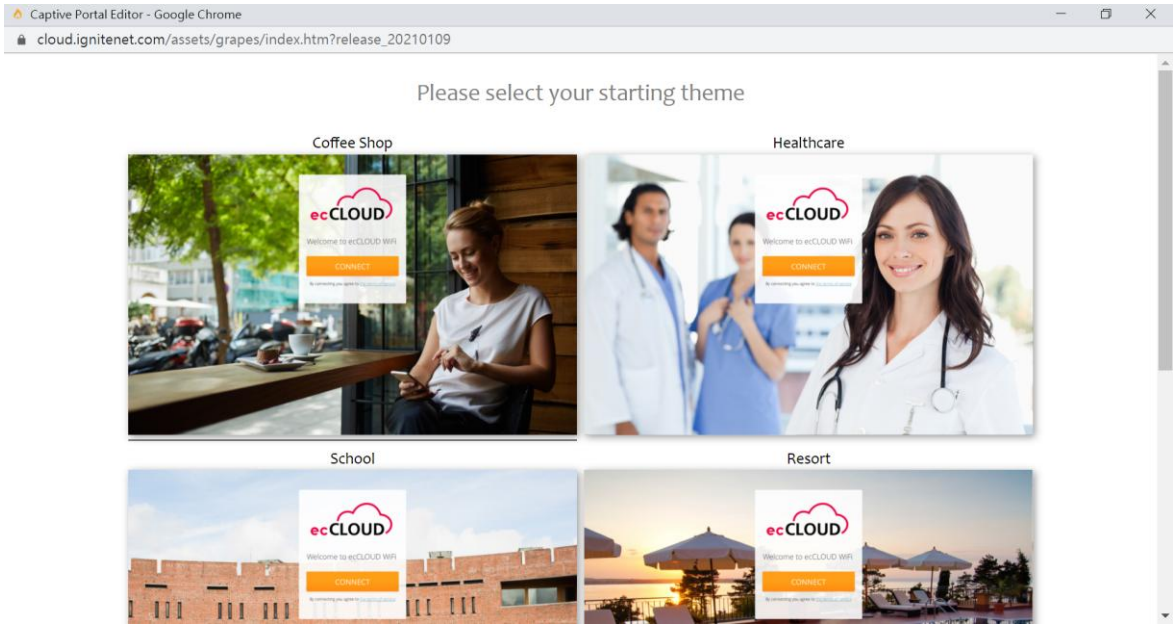
If there are existing captive portals, they can also be edited or deleted from this page.



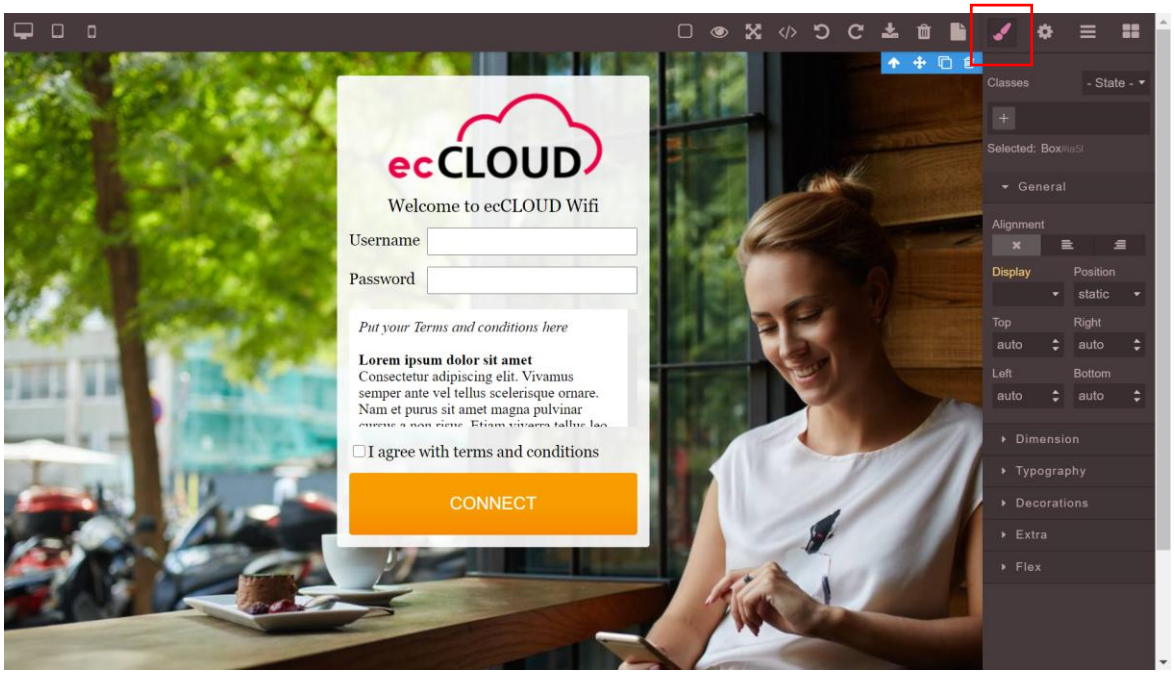
Captive portals can also be added from any SSID configuration page. Once AuthPort is enabled, the Captive Portal option will be revealed, and new captive portals can be added by clicking on "**ADD NEW PORTAL**".


Add SSID
CANCEL
CONFIRM
U-APSD
Security Settings
Method
WPA3 Personal
Key
Access Control List
802.11r
802.11k
802.11v
Network Settings
Network behavior
Bridge to Internet
Limit upload rate
Limit download rate
AuthPort Enable
Captive Portal
Default captive portal
Default captive portal
Test
Microsoft 365 Authentication
Proxy ARP
Only applicable for some devices

c. Captive Portal Editor will appear as a pop-up window. Choose one of the starting themes to begin customizing the new captive portal.



d. Use Style Manager to modify the attributes of the selected HTML object.



See Table 1 below for descriptions of each attribute category.

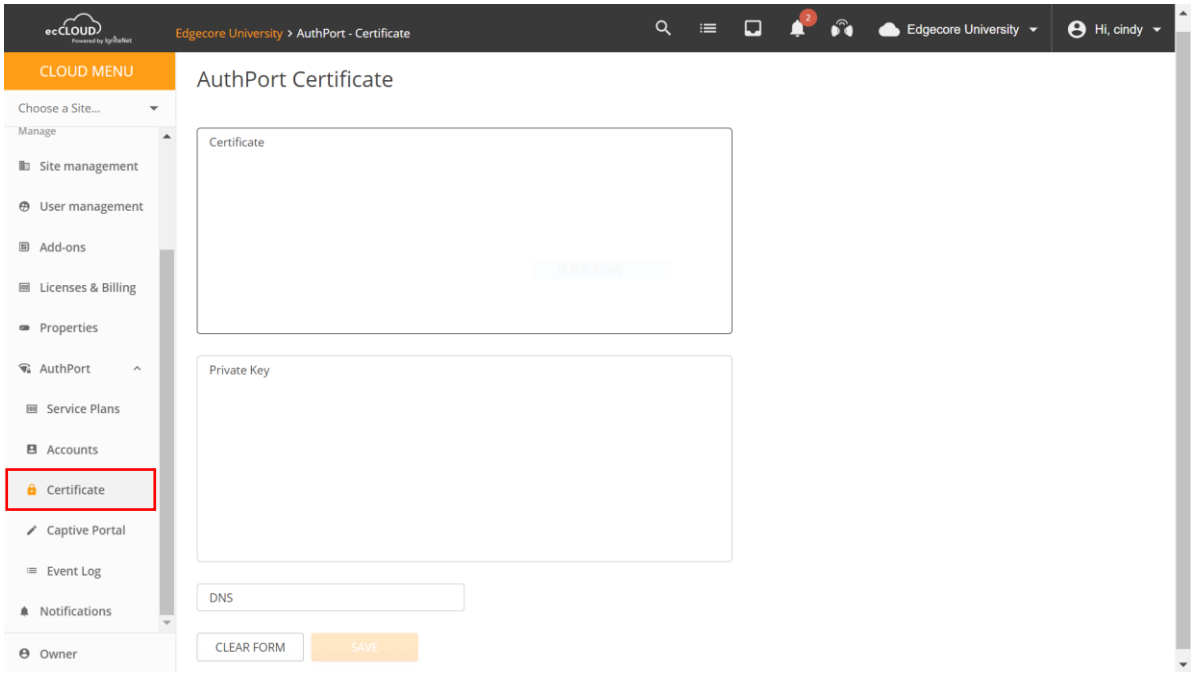
Table 1

Attribute Category	**Description**
Class	This tells you what kind of component it is
General	configure alignment and display position
Dimension	Modify component dimension
Typography	Edit font, size, text align, text decoration
Decorations	Select background color, border width/styler/color
Extra	Add transition, edit perspective, transform (rotate, scale)
Flex	Edit flex effect

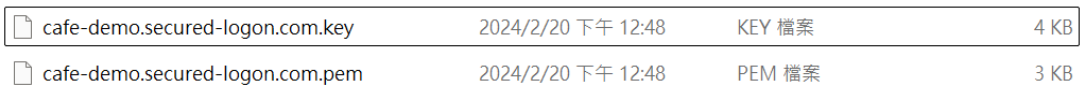
5. Configure AuthPort Settings: Upload an SSL Certificate

When AuthPort is enabled, we recommend submitting a valid SSL certificate to help make the captive portal redirection experience smooth for your wireless clients. If no SSL certificate is uploaded or if a suspicious SSL certificate is uploaded, they may see a security warning upon captive portal detection.

a. Click on "**Certificate**" on the "**AuthPort**" submenu



b. Open your Private key and SSL certificate file in Notepad.



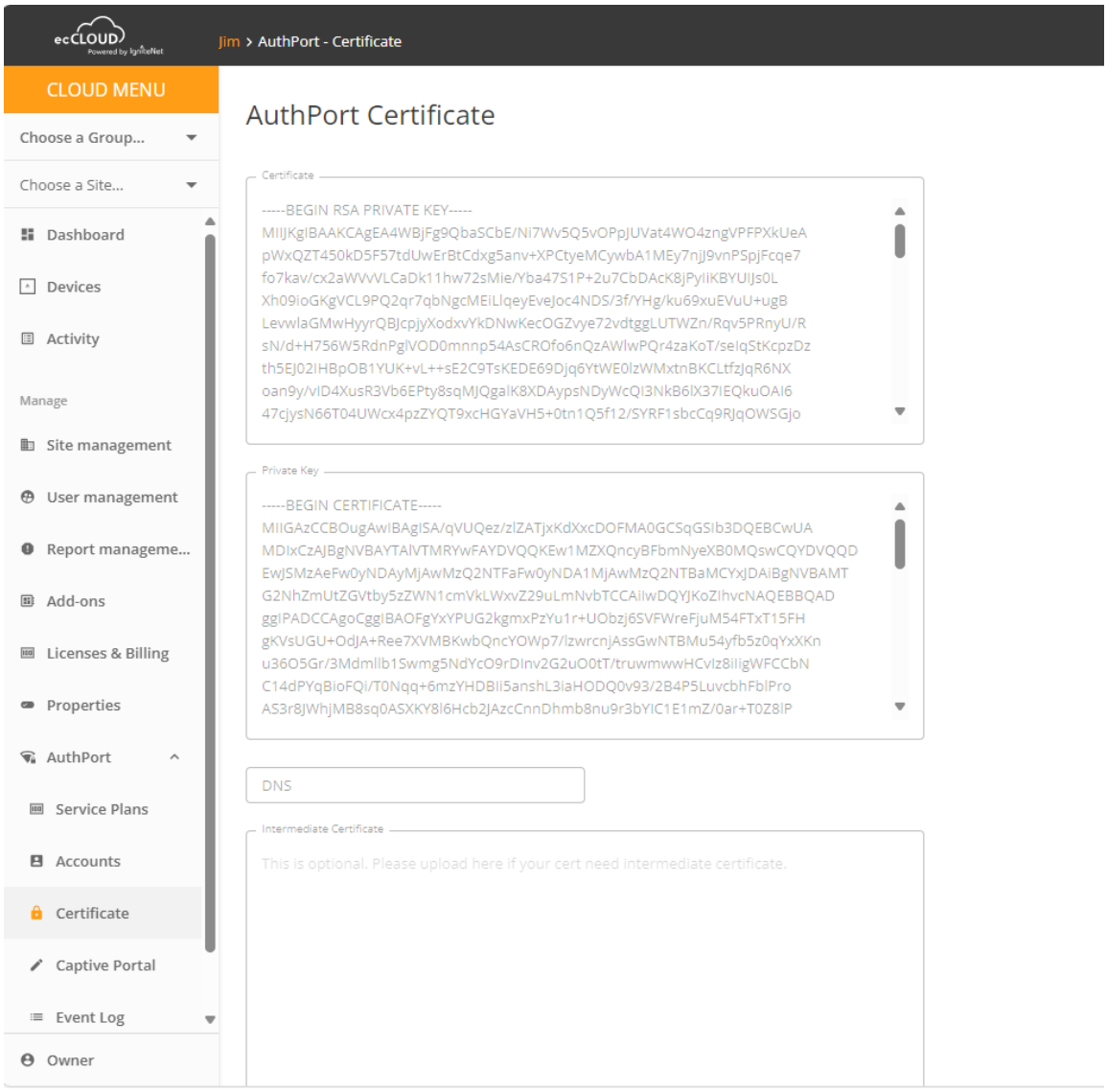
SSL Certificate:

```
-----BEGIN CERTIFICATE-----
MIIGAzCCBOugAwIBAgISA/qVUQez/z1ZATjxKdXxcDOFMA0GCSqGSIb3DQEBCwUA
MDIxCzAJBgNVBAYTA1VTMRYwFAYDVQQKEw1MZXQncyBFbmNyeXB0MQswCQYDVQQD
EwJSMzAeFw0yNDAyMjAwMzQ2NTFaFw0yNDA1MjAwMzQ2NTBaMCYxJDAiBgNVBAMT
G2NhZmUtZGVtby5zZWN1cmVkLWxvZ29uLmNvbTCCAiIwDQYJKoZIhvcNAQEBBQAD
ggIPADCCAgoCggIBAOFgYxYPUG2kgmxPzYu1r+UObzj6SVFWreFjuM54FTxT15FH
gKVsUGU+OdJA+Ree7XVMBKwbQncYOWp7/1zwrcnjAssGwNTBMu54yfb5z0qYxXKn
u36O5Gr/3Mdm11b1Swmg5NdYcO9rDInv2G2uO0tT/truwmwwHCvIz8iIigWFCCbN
C14dPYqBioFQi/T0Nqq+6mzYHDBIi5anshL3iaHODQ0v93/2B4P5LuvcbhFb1Pro
AS3r8JWhjMB8sq0ASXKY816Hcb2JAzcCnnDhmb8nu9r3bYIC1E1mZ/0ar+T0Z81P
0bDf3fh++e1uUXZz4JVTg9Jp56eeALAkTn6Op0MwFpcDOK+M2iqE/7HiKkrSnKcw
87YeRCdNiBwaTgdWFCvry/vrBNgvU7ChAxOvQ46umLVhNJc1jMbZwSgi7X8yakej
V6Gp/cv7yA+F7rEd1W+hD7cvLKjCUIGpSvFwwMqbDQ81nECNzZAepV9+yBEJLjgC
OuO3I8rDeuk9OFFnMeKc2WEE/cXBxmG1R+ftLZ9UOX9dv0mERdbG3AqvUSaj1kho
6HbulxyhiFs0Yrg/xUO9ghoQVXxJHCz/qIqPieceiPgfQwX5N96kAoWDEq5w43sE
WVSrwvz6SUSmDNaRs+YzuLBthXMeb1C2T9Lmh/A+UbjEJqbeHynqgNdvujpZAgMB
AAGjggIdMIICGTAOBgNVHQ8BAf8EBAMCBaAwHQYDVR01BBYwFAYIKwYBBQUHAwEG
CCsGAQUFBwMCMAwGA1UdEwEB/wQCMAAwHQYDVR0OBBYEFKd+i0k74cL+7ybvz1zn
k8HXiLSMMB8GA1UdIwQYMBaAFBQusxe3WFbLr1AJQOYfr52LFMLGMFUGCCsGAQUF
BwEBBEkwRzAhBggrBgEFBQcwAYYVaHR0cDovL3IzLm8ubGVuY3Iub3JnMCIGCCsG
AQUFBzAChhZodHRwOi8vcjMuaS5sZW5jci5vcmcvMCYGA1UdEQQfMB2CG2NhZmUt
ZGVtby5zZWN1cmVkLWxvZ29uLmNvbTATBgNVHSAEDDAKMAgGBmeBDAECATCCAQQG
CisGAQQB1nkCBAIEgfUEgfIA8AB2AEiw42vapkc0D+VqAvqdMOscUgHLVt0sgdm7
v6s52IRzAAABjcTWjhUAAAQDAEcwRQIgVZ34DMQrv9NmhgyagwjATJ5BTzJU0CfK
3tCG8Ysq2nMCIQCxdYDB8M4zKRtHg8UhGSkp+fk1XLnQyfre2dulutr0hgB2AHb/
iD8KtvuVUcJhzPWHujS0pM27KdxoQgqf5mdMWjp0AAABjcTWjnkAAAQDAEcwRQIh
AJypjVREW7zwBOJtJ9BKrPur9svYGc4nsyMOMUEpsmf1AiBXzwENHhFz3A5n8Sk/
Lj4YVBQdnGwYoHMIYco1Ui9qkzANBgkqhkiG9w0BAQsFAAOCAQEAmknY1SzgQtSy
RAFNquFC3OdO+CfiXUtyuC2NQpoF/ZmiAHLXX4H11x1/Ns1AugMW2n9oeIYTDIM+
I/DyQWKRUdgN9ydP1d5NtGY1uGdpCk2myB+nkhAji7LKeWvbnn0GGWpPL16/kH3Z
FwBtDyyRr3kNCvCQCaPHDiPX6Pj9JZyV81KGfwq+rAQmDqLTmYqsD1TsPFz6j1Jn
40kHHgHV2nZrcJ8HwGbbgJT94DLVwPoPtRODy/SECTMM6IZJchj0WmydWWJkvgRR
V1C0HCeb5gi85TL9PepFG1CK1ggiGHCBFT9o/tzckE3gH4ZzkL+Pv+2Fg21sYxn1
```

Private key:

```
-----BEGIN RSA PRIVATE KEY-----
MIIJKgIBAAKCAgEA4WBjFg9QbaSCbE/Ni7Wv5Q5vOPpJUVat4WO4zngVPFPXkUeA
pWxQZT450kD5F57tdUwErBtCdxg5anv+XPCtyeMCywbA1MEy7njJ9vnPSpjFcqe7
fo7kav/cx2aWVvVLCaDk11hw72sMie/Yba47S1P+2u7CbDAcK8jPyIiKBYUIJs0L
Xh09ioGKgVCL9PQ2qr7qbNgcMEiLlqeyEveJoc4NDS/3f/YHg/ku69xuEVuU+ugB
LevwlaGMwHyyrQBJcpjyXodxvYkDNwKecOGZvye72vdtggLUTWZn/Rqv5PRnyU/R
sN/d+H756W5RdnPg1VOD0mnnp54AsCROfo6nQzAW1wPQr4zaKoT/seIqStKcpzDz
th5EJ02IHBp0B1YUK+vL++sE2C9TsKEDE69Djq6YtWE01zWMxtnBKCLtfzJqR6NX
oan9y/vID4XusR3Vb6EPty8sqMJQga1K8XDAypsNDyWcQI3NkB61X37IEQkuOAI6
47cjysN66T04UWcx4pzZYQT9xcHGYaVH5+0tn1Q5f12/SYRF1sbcCq9RJqOWSGjo
du6XHKGIWzRiuD/FQ72CGhBVfEkcLP+oio+J5x6I+B9DBfk33qQChYMSrnDjewRZ
VKvC/PpJRKYM1pGz5jO4sG2Fcx5vULZP0uaH8D5RuMQmpt4fKeqA12+6O1kCAwEA
AQKCAgA2FXpRveUQGq1Nrqz1vPjz383i/3T+tu1NLDAaJAj8jCYr79u4VtDIKvGX
Og5Mk8/qGQ75+iSuDbshiZXV2c/qpbZy4DEAHUjKn2PgB7yt6xFe3U+KJGI+Jx51
H4IuZfjW26xu3QN1AOxmYY8vauNBxWtgQHGZosXv3+W0+sccYfs9zHDQ6fVtun5x
X9HmO4Cu4tfAvO+uyons41tCX/LASIErS/p506GkEvUm1qQ3OCH9QBWgXoFCdx0e
yA3cpDf77yYidyBdWnbSCafZ8NmDXNagykWWMHWgCVY1D/Vr3RbW4XexmVdcHaR9
VwLniRE45Gy63r0/pRQHMP9BMZyDeKooWpzJVfs7gQMzzefUUqSSjQqv8LI4YCwF
LCee3CcKm7l3vYGqa47F3gaXivUg/1+CaxwApkRIz5+qk4t21aPqSB3gxpjbqnb6
PR+v0pc9CzxZ1uW26EzUTEiH+FqzwzsOtbJkgiL8IRigBTf0r/MGdx5hW4UBitwl
FQCwkBBbfWXJRmJTSyANCSMdkSBEPdLvmG9j9xIR688Yo0YidNwIFzCHvDvv/th4
h6D8gZj5HF+RIPwpY5jgijghxxOD1NnNmLrOmQET1ojQQArrOdiQhk9HY7jRu14h
r6yC8kUhXOeRQjb+3a1eCo396gkAH8QtSjANTmonUq3s3pfDHQKCAQEA+8xrVVj7
G6hdpngaAZt9oaciAbZfrP1kv88XNbuZ8m40YOmgXk5vWdfTGbcauBtmCT46Cx2R
wJd+ArKDTshjFXHf07F8Ik7butigKpa4dxHoMm21aMTyd+NIqDEXK8PMGg6Oqe0P
fSnyJQQBqpz0KNugiYpOshXYhF1QNWDs3JPWaHCUHcB+HXnhvDUq91zkeC/gUJmZ
WPIhJ93AgVaQfFbMG8J+xN9SVHB1Rz7Fz9hRiMfrFzCcxjG1Ng18pZO0nHEh/SQt
6LmJb1/a8wrHM8ETh1RTeI7XxntscGS+g6bMeq3QnNhJ+kGhaxRDyzwzg+2aBI02
BcQ3nqrdpj3RywKCAQEA5SMaj6KhTaamd1E6hchnnEenkcPO8Lp+V+9EZ98gtWFk
isTe/i1ptZOK48NcSISyzZ3HAF1QASjNZCUWbXbe7GfcRyAA5bnOyAexkrBs5wso
Mx1w1v7OIytF1c0IqbQ26EeCLhYxoEg6ws+X6Q1viUH3IiS/ovFQDq2bncuuChsd
5xHAnF5Hsxb1pO6fZVpmq2nAM/xzO/IsYqrwwoyq16h+ep5DWopKS+n8d+ZVZXer
dO/pAKSvMrYNJoo8NFR2k2LSGqBLp92PaKO1fH6tdOfEDK5MTiR/AOwSSq8qKMcp
```

c. Copy your Private key and SSL certificate file content to “Certificate” and “Private key” field.

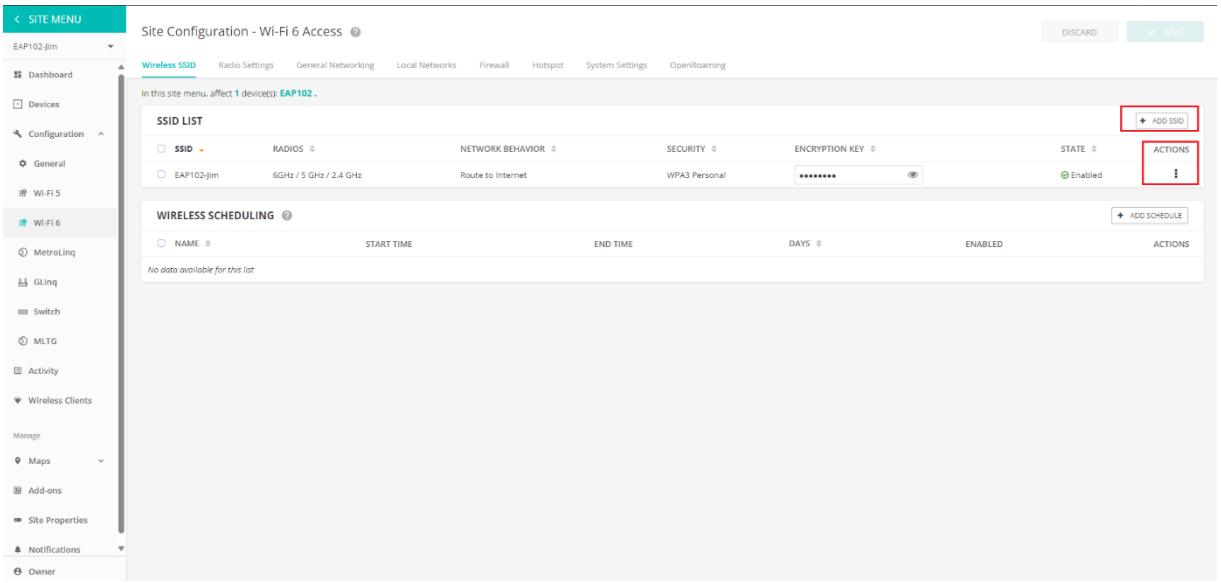


d. The “**DNS**” field does not need to be filled and will be automatically filled by the system with the certificate’s common name once the “**Certificate**” field has been filled.

6. Enable AuthPort in SSID Configuration Settings

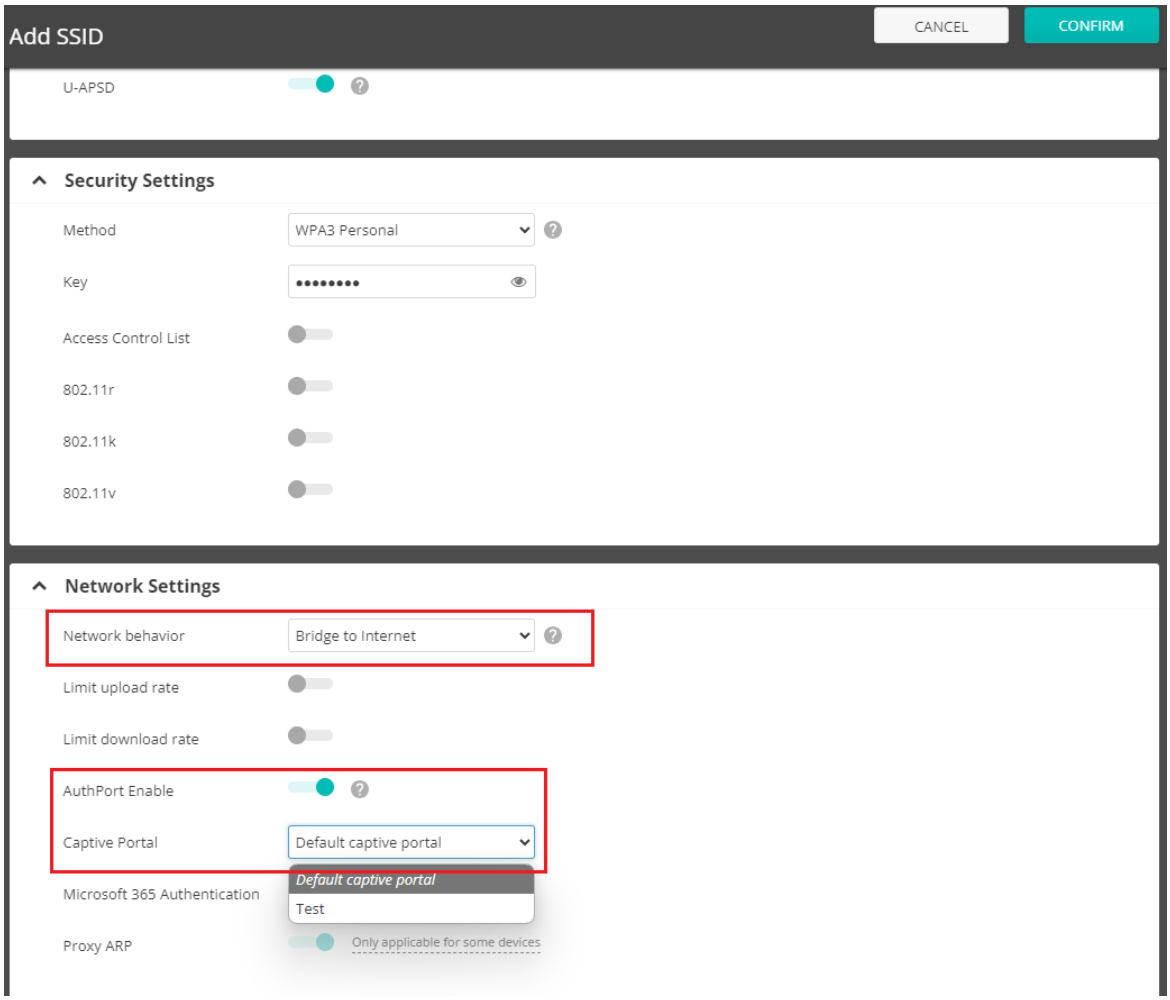
In configuration settings of each SSID, AuthPort can be enabled under "**Network Settings**". Once enabled, the "**Captive Portal**" option will appear for the desired captive portal to be selected. Thus, each SSID can have its independent AuthPort setting and captive portal.

a. On the Site Menu, go to "**Configuration > WiFi 5/ WiFi 6 > Wireless SSID**" and click on "**Add SSID**" to create a new SSID. To modify an existing SSID, click on "**Edit**" under Actions.

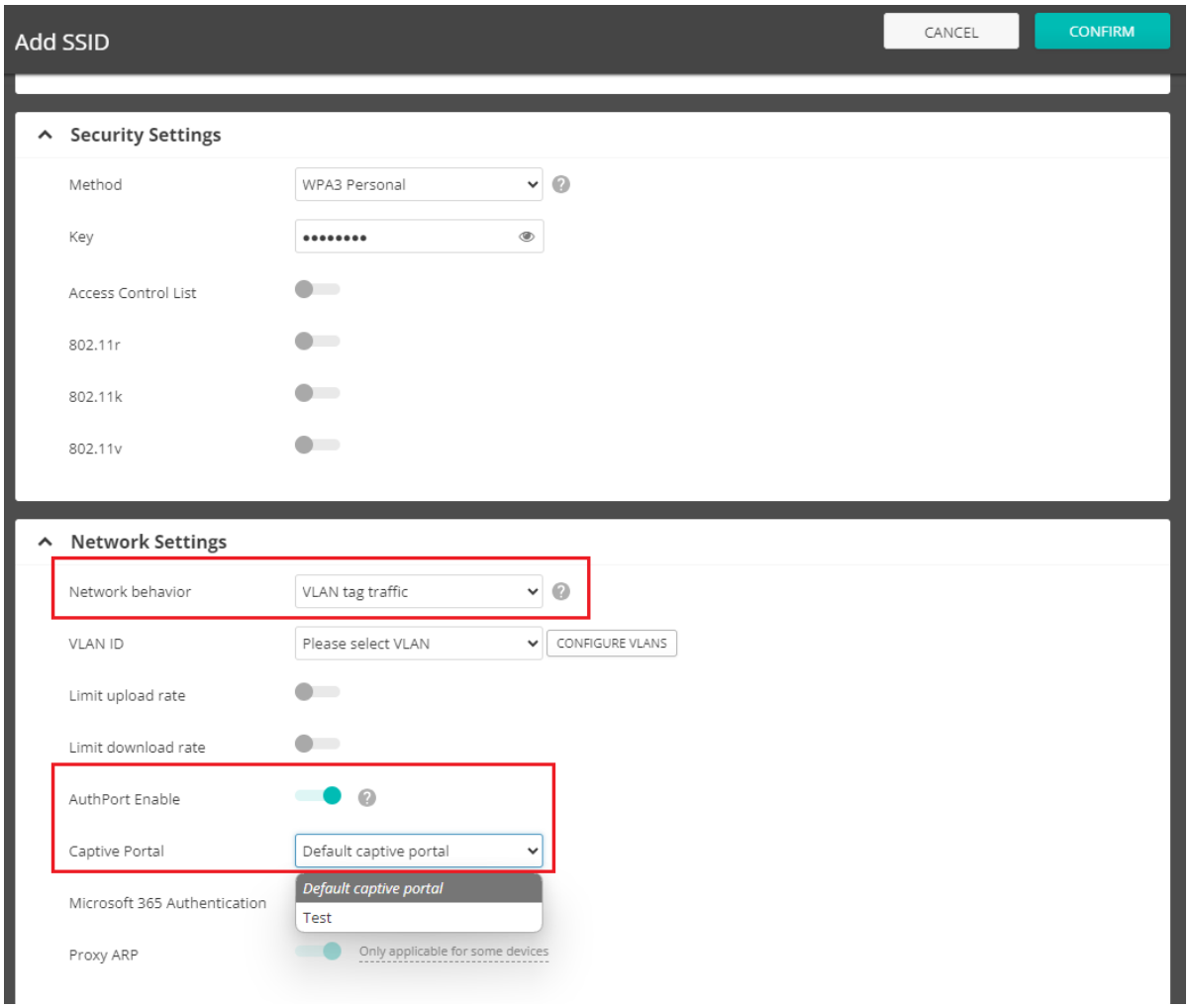


b. Scroll down to “**Network Settings**”, Select Network behaviour: “**Bridge to Internet**” or “**VLAN tag traffic**” and enable “**AuthPort**”. Once enabled, the "**Captive Portal**” setting will be displayed below. If no captive portals have been added previously in “**AuthPort > Captive Portal**” at the cloud level, only the default captive portal will be available. However, you can also add captive portals from this page by clicking on “**ADD NEW PORTAL**”. Captive portals added from this page will appear under “**AuthPort > Captive Portal**” at the cloud level.

- Network behaviour: “**Bridge to Internet**”



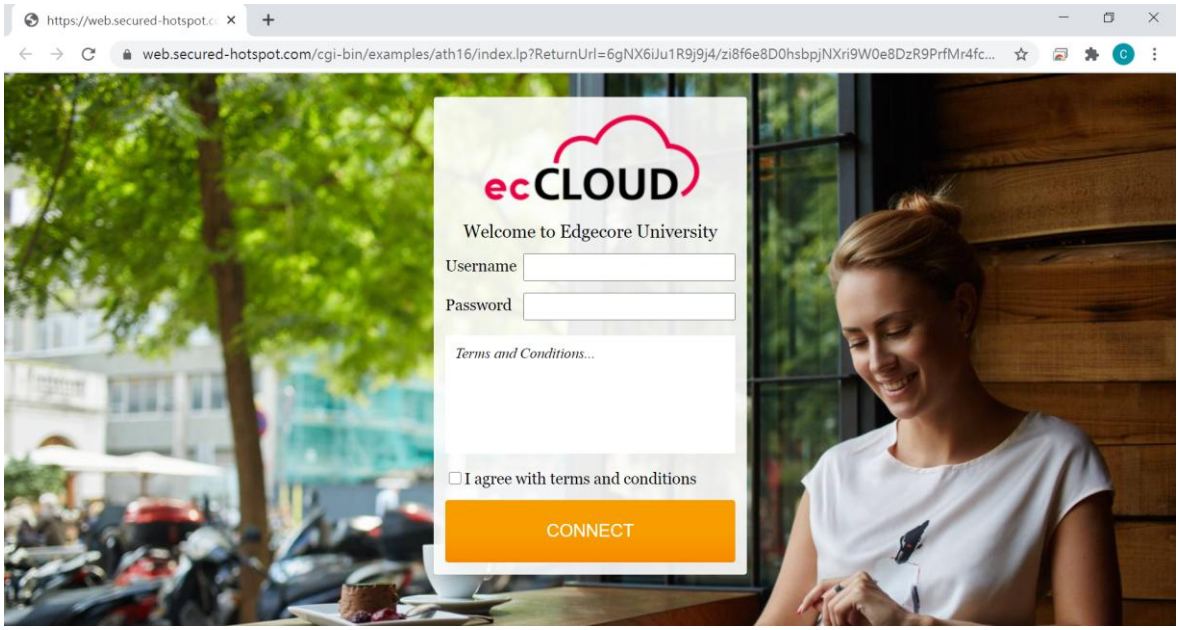
- Network behaviour: “**VLAN tag traffic**”



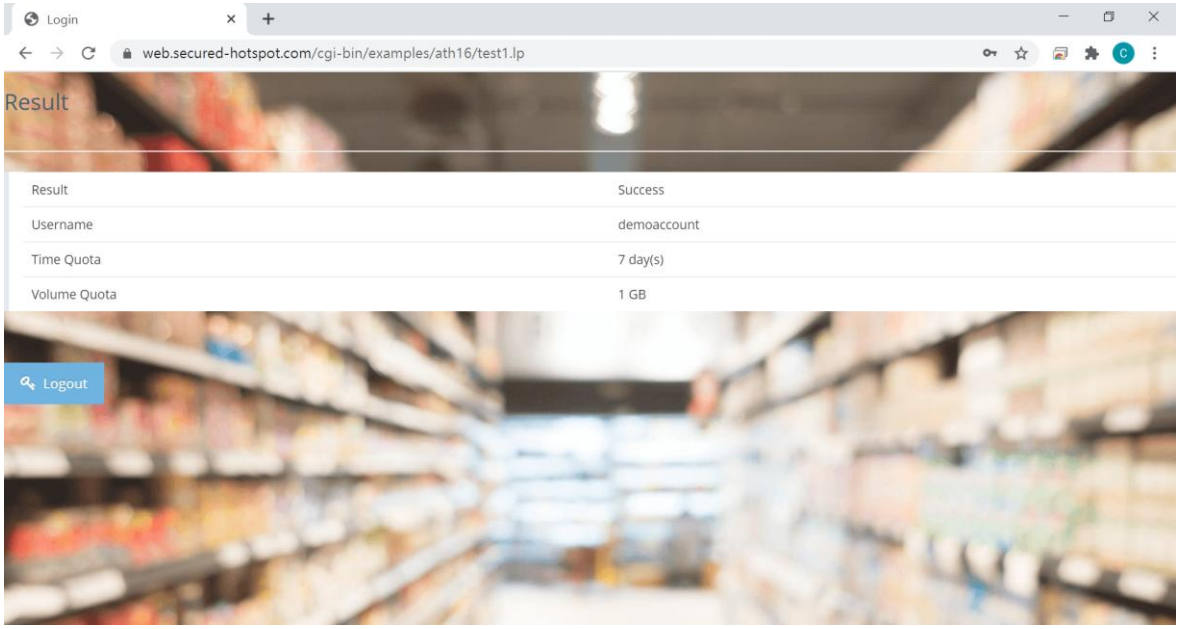
7. Wireless Client Login Test & Account Monitoring

7.1 Wireless Client Login Test

a. On your Wi-Fi device, connect to an SSID that has AuthPort enabled.
b. On the login screen, enter a set of pre-generated username and password (and tick the box for “I agree with terms and conditions” if necessary) to login.



c. The following screen will be shown upon successful login.



7.2 Account Monitoring

a. Go to “**Accounts**” from the “**AuthPort**” submenu. Here you will be able to monitor account status in real-time.