Cloudi-Fi integration with Commscope Ruckus

vSZ controller 5.2.1.0.515

Table of Contents

1 Value Proposition

Cloudi-Fi is 100% cloud-based Guest Wifi Saas solution that transforms Wifi access into a new communication channel with the guarantee to be secured and compliant with local regulation laws.
Our solution helps you drive both entreprises and hotspots digital transformation through innovative digital services.

Cloudi-Fi Value proposition
Bring innovative services with WiFi

From Commodity → To Utility

FREE WIFI
- Opportunity-based deployment
- Basic Access
- Industrialized Captive portals
- No added-value nor services

- **Monetizable**
- **Customized** user experience
- **Secured** and **Compliant**
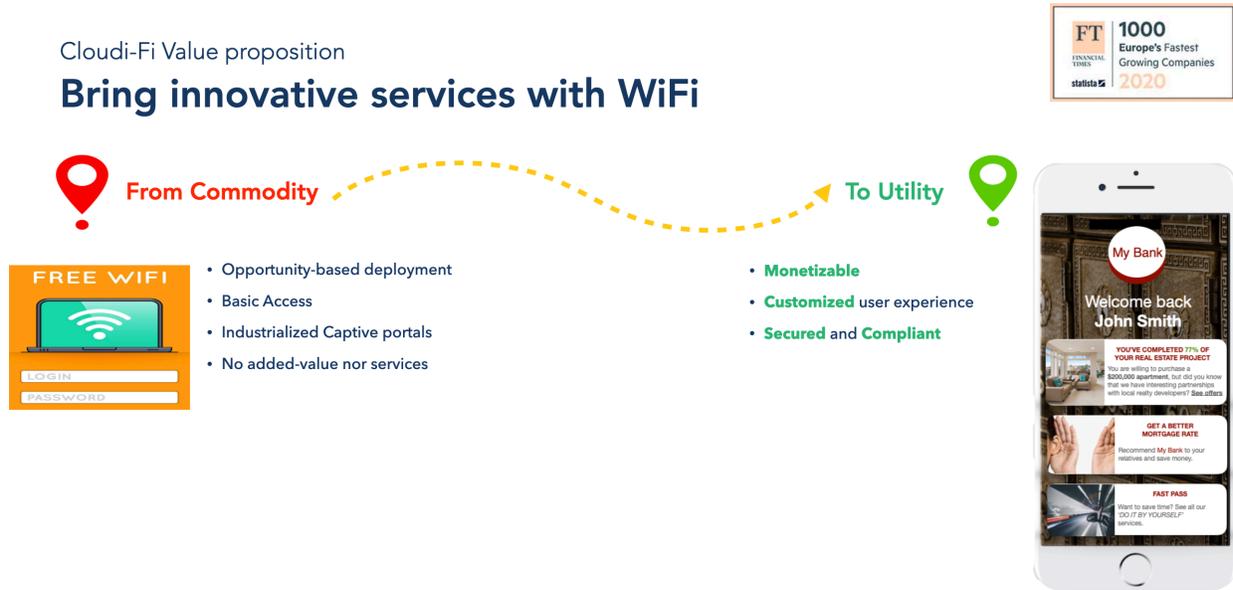
We address 3 main concerns in our solution
1/ User experience

- Provide the best user experience
- Collect digital identity and track user behaviour with his consent
- Tailored and automated communication based on user recognition Monetizable

2/ Compliance

- Provide compliance based on each country has specific regulations.
- On one hand, data have to be kept and guest to be identified (EU & APAC).
- On the other hand, data privacy should be enforced. Some countries such as China, Russia and Middle East have specific concerns.

3/ Security

- Brands are sensitive to their image. They require to have a minimum of security on their guest network.
- We are able to package Extreme Networks security offer.

2 Use Cases

The partnership with Cloudi-Fi addresses both **Corporate and Hotspots market segments**.
In **Corporate market,** Cloudi-FI solution transforms the WiFi into **a new way to connect and access enterprises resources**.
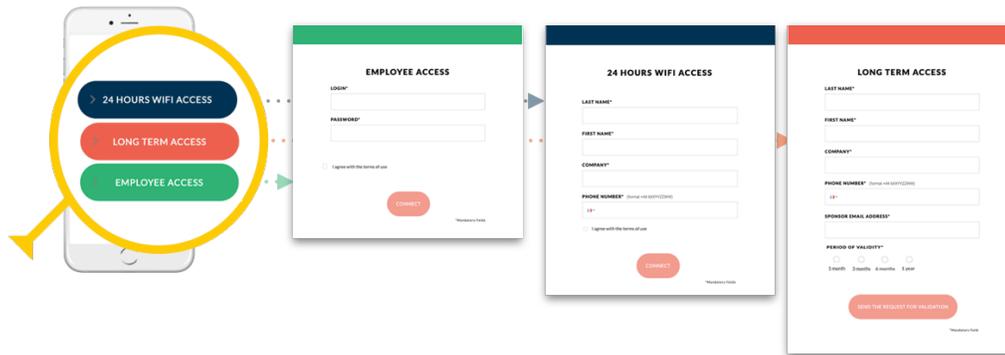
The different types of users are **profiled** to propose and adapt a **personalized and secured WiFi experience**

1st visit   **Returning visitor**
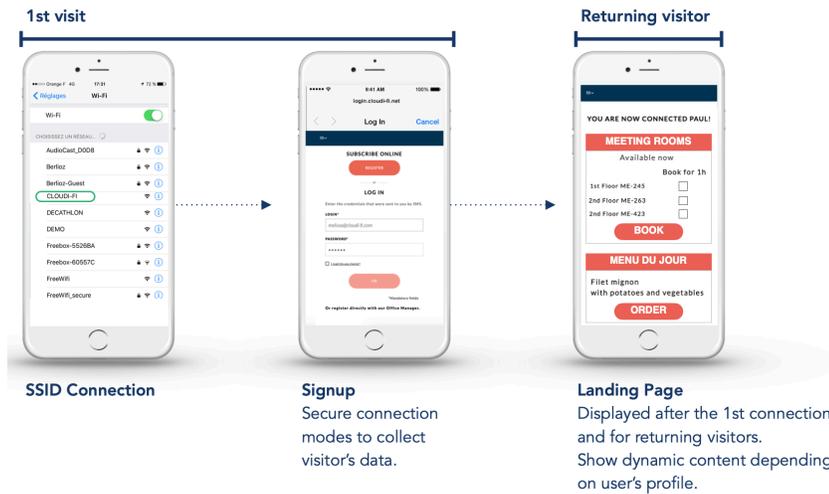
In addition to dedicated access, Cloudi-Fi creates **phygital services**

SSID Connection

Signup
Secure connection modes to collect visitor's data.

Landing Page
Displayed after the 1st connection and for returning visitors.
Show dynamic content depending on user's profile.

Cloudi-Fi enriched Commscope solution in **Hotspots market** to deliver **a unique user digital experience**

Signup

Collect data and demographics of your visitors

Landing Page

Marketing page displayed with coupons, video, contests, ads, survey…

Phygital Communication

Personalized retargeting campaigns (email, SMS, Facebook ads…).
Additional off-site interactions to improve user profiling.

Individualized Landing Page

Recognize the visitor at the door and display a dynamic marketing page with the best offers / campaigns matching visitors' profile.

Thanks to an efficient **phygital omni-channel communication**, the **digital** user experience is reconciled with the **physical** presence onsite.

3 Integration Configuration steps
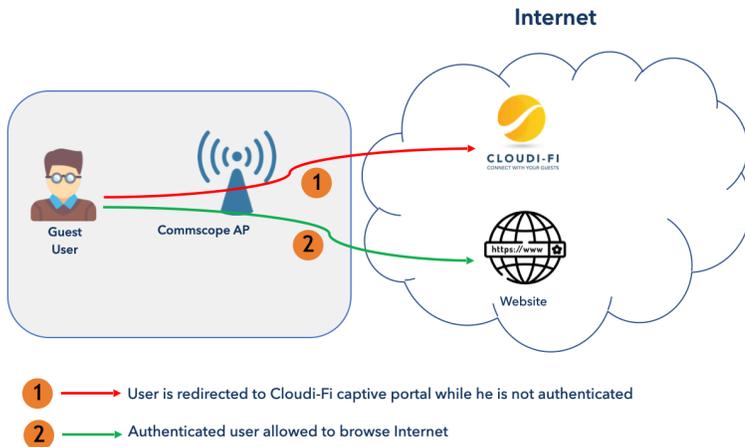
Internet

The above diagram shows the Cloudi-Fi integration.
- First (1) the Guest connects to Internet through an open SSID configured on the Extreme Networks AP.
- A splash page or captive portal pops up immediately on its device and is directly redirected to Cloudi-Fi portal while he is not authenticated.
- Cloudi-Fi hosts the captive portal, handles guest authentication and manages the access logs.
- The guest is invited to authenticate with his preferred method.
- Once authenticated (2), the user is allowed to browse Internet.

1 → User is redirected to Cloudi-Fi captive portal while he is not authenticated

2 → Authenticated user allowed to browse Internet

3.1   Get Cloudi-Fi required URL and RADIUS secret

Go to your Cloudi-Fi administration interface and get the URL for external authentication
- Go to Locations Menu
    - o Click on the menu button of the location and select "Copy Splash page URI"
    - o Copy the URL
- Then Go to Settings :
    - o Copy your Cloudi-Fi Company Key
- Go to the chat interface and ask for your Radius secret
    - o Copy the secret as well

3.2   Create Hotspot WISPr Service

Go to Services > Profiles > Hotspots & Portals > Hotspot (WISPr) > Create
- Portal Name : Cloudi-FI Captive Portal
- Logon URL : External
- Redirect unauthenticated user, Primary : <Cloudi-FI Redirect URL>
- Start Page : Redirect to the following URL : <Cloudi-Fi Success page>
- HTTPS Redirect : ON
- Session Timeout : Same valueas CLoudi-Fi Session lifetime
- Grace Period : Same value as Cloudi-Fi Session Lifetime
- Walled Garden : Add only below URL (Additional URL may be added in case of Social Media connector on your caprive portal)

```
*.cloudi-fi.net
*.cloudi-fi.com
```

- Save

3.3 Create Authentication Service

Go to Services & Profiles > Authentication > Proxy (SZ Authenticator)
- Name : Cloudi-FI Radius
- Service Protocol : Radius
- IP Address, Port and Secret will be provided by Cloudi-FI Support team
- Save

3.4 Create the Guest WLAN

Go to Wireless LANs > Select the correct Zone/WirelessGroup > Create
- Name : Your Guest SSID Name
- SSID : Your Guest SSID Name
- Authentication Type : Hotspot (WISPr)
- Method : Open
- Encryption Options : None
- Hotspot WISPr Portal : Cloudi-Fi Captive Portal
- Bypass CNA : OFF
- Authentication Service : Use the controller as proxy and Select Cloudi-FI Radius
- Radius Option NAS-ID : Select Custom : <Cloudi-Fi Company Key>
- Called Station ID : AP MAC

3.5 Disable MAC-Address Encryption

By default, Ruckus vSZ controller will encrypt the device's mac-address.
Cloudi-Fi needs to see the actual mac-address of the client's device.
To disable this feature, connect in CLI to your vSZ controller and run the following command in **config mode** :

```
no encrypt-mac-ip
```

Save the configuration.

3.6 Configure the Northbound Interface (NBI) credentials

To allow Cloudi-Fi to communicate with your vSZ controller, we use the NBI.
It allow us to avoid redirection issues (Security Warning to due HTTP Redirection or Certifcate warning with HTTPS redirection).
Go to System > General Settings > WISPr Northbound Interface
- Enable Northbound Portal Interface Support : ON
- Then configure you Username and password

3.7 Provide NBI credentials to Cloudi-Fi

Go to Cloudi-Fi Admin interface > Settings > Advanced Settings > Ruckus NBI
And fill out the username and password fields

4 ADMINISTRATION GUI

The Administration GUI offers a centralized point of management to manage every parameter of your WiFi.
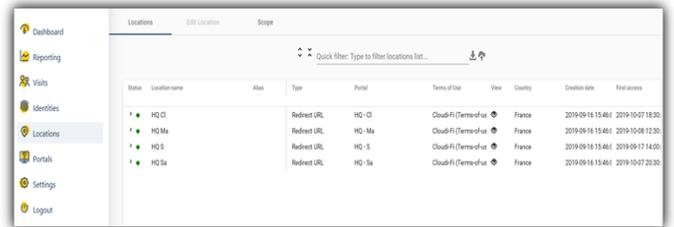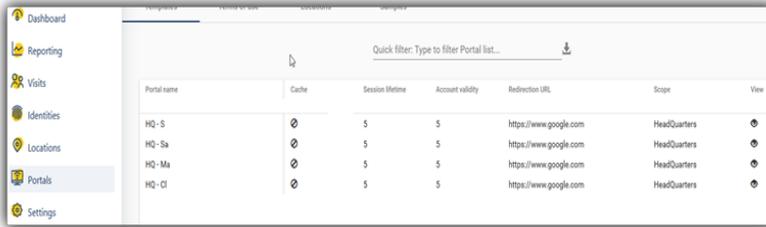
Available portals with the session lifetime

Locations with sites overview, associated portals, MAC AP address and Terms of Use
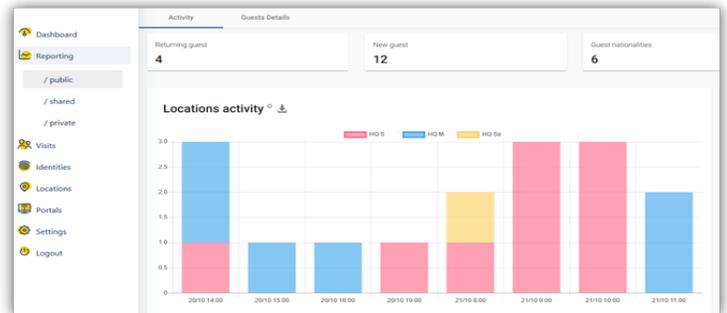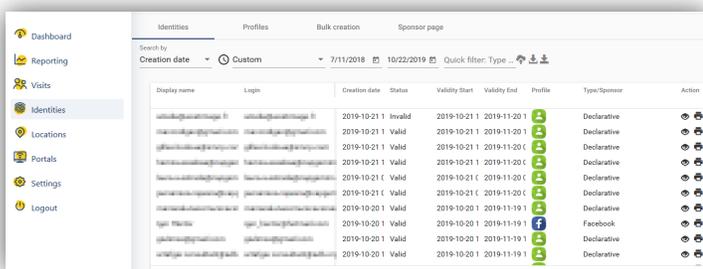
Collected identities overview and management

Personalized Reporting
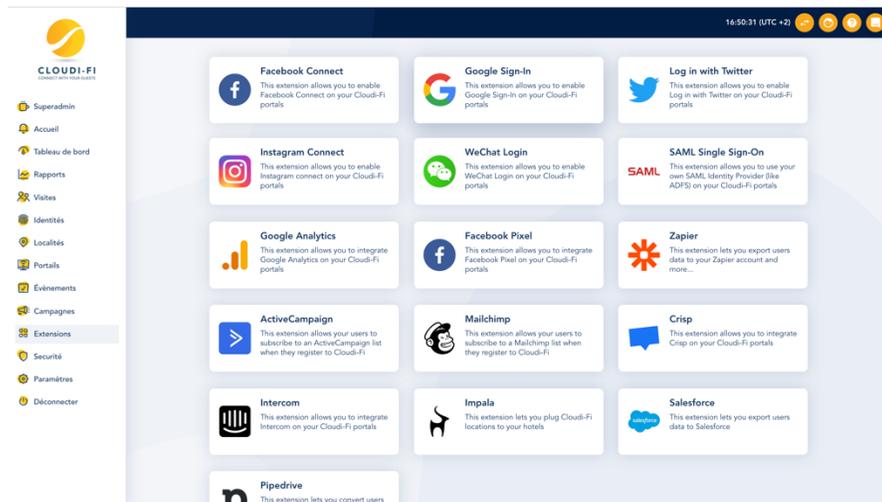
Cloudi-Fi GUI also enables **extensions** to allow **customers third-party services** to connect to the service and provide a seamless

5 Contact information

Information is also available here: http://help.cloudi-fi.net/en/articles/4776589-ruckus-vsz-integration
Our support mail is: support@cloudi-fi.com