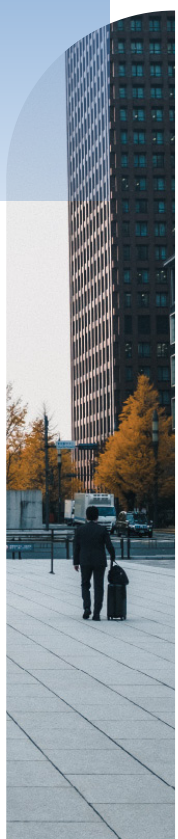
DEPLOYMENT GUIDE

FortiGate Integration—Enable Cloudi-Fi Captive Portal in FortiOS

How To Enable Cloudi-Fi Captive Portal Natively With FortiOS



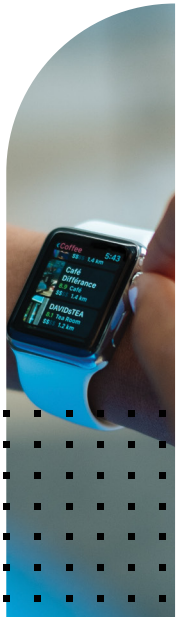


Table of Content

Overview

This information applies if you use any WiFi infrastructure connected as a Layer 2 to your FortiGate without Fortinet Access Points. If you are routing your WiFi, you should use our WAN deployment on the FortiGate.

Configuration steps

1. Get Cloudi-Fi required URL and RADIUS secret
2. Create the Cloudi-Fi RADIUS Server
3. Configure Captive Portal settings

   3a. WiFi deployment

   3b. Interface deployment
4. Configure the security policy

```
Validated with FortiOS 6.2.5 build 1142
```

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.
- Click on the menu button of the location and select “Copy Splash page URI”.
  - Copy the URI.
  - Transform the URI as shown in the following screenshot.

SPLASH PAGE URL TRANSFORMATION

Original URL Format	https://login.cloudi-fi.net/auth/saml2/idp/SSOService.php? spentityid=spsomething.com&ch=**27014ceebb1dcf42a788cd0a8f000b81**&lh=**221bd9676101dd83bf1c4ef85a03f4cc**&
Fortinet URL Format	https://login.cloudi-fi.net/start/**27014ceebb1dcf42a788cd0a8f000b81**/**221bd9676101dd83bf1c4ef85a03f4cc**? spentityid=spforti.com

- Go to the chat interface and ask for your RADIUS secret.
  - Copy the secret as well.

2. Create the Cloudi-Fi RADIUS Server

- **Go to your FortiGate administration interface.**
- Go to User & Device → RADIUS Servers → Create New :
  - **Name:** Cloudi-Fi_Radius_Srv
  - **Authentication Method:** Default
  - **IP/Name:** radius.cloudi-fi.net

- **Secret:** Provided by Cloudi-Fi Support team
- **Save**

- Go to **User & Device** → **User Groups** → **Create New:**
  - **Name:** Cloudi-Fi_Radius_group
  - **Type:** Firewall
  - **Remote Groups:** Add Cloudi-Fi_Radius_Srv
  - **Save**

3. Configure Captive Portal settings

Note: The Captive Portal feature can be enabled in two different ways with FortiGate, depending on your infrastructure:

- In the **FortiGate WiFi controller** if you have FortiAP (FortiGate WiFi Access Points).
- In a **FortiGate interface** (physical or VLAN interface) if you have other WiFi vendor or if you want to enable Captive Portal for wired users.

3a. Enable Captive Portal in FortiGate WiFi controller

If you have FortiAP and want to enable Cloudi-Fi in the Fortinet WiFi controller:

- Go to **WiFi & Switch Controller** → **SSID** → **Create New:**
  - Provide a name, the mode (tunnel or bridge) and fill the network information
  - **WiFi Settings:**
  - **Security Mode:** Captive Portal
  - **Portal type:** External Authentication
  - **URL:** https://login.cloudi-fi.net/start/***CompanyKey/Location-ID***?spentityid=spforti.com
  - **User Groups:** Cloudi-Fi_Radius_Group
  - **Redirect After Captive Portal:** Specific URL: https://login.cloudi-fi.net/success.php
  - **Save**

3b. Enable Captive Portal in FortiGate interface

If you want to enable the Captive Portal for your wireless and/or wired users and you don't have FortiAP.

```
Note: Because the captive portal feature is enabled for all the traffic of a
specific interface, we recommend to have a dedicated interface (physical or
VLAN) for the Guest network.
```

- Go to **Networks** → **Interfaces** → **Edit the Guest interface**. Then go to the **Network Section** of the interface and enable **Security Mode:**
  - **Security Mode:** Captive Portal
  - **Authentication Portal:** External
  - **URL:** https://login.cloudi-fi.net/start/***CompanyKey/Location-ID***?spentityid=spforti.com
  - **User Access:** Restricted to Groups: Cloudi-Fi_Radius_group
  - **Exempt Destinations:** Create a FQDN Object for *.cloudi-fi.net
  - **Redirect After Captive Portal:** https://login.cloudi-fi.net/success.php
  - **Save**

4. Configure the security policy

To finalize the configuration, you have to create security rules to allow unauthenticated users to access the Captive Portal.

- Go to **Policy & Objects** → **IPv4 Policy** and create below rules in the same order:
  - Rules for unauthenticated users:

Name	Source	Destination	Service	NAT	Action
DNS	Guest interface	DNS Servers	DNS	TBD	Accept
Walled Garden	Guest interface	FQDN_CloudiFi	HTTPS	Yes	Accept

- Once these rules are created, right click **on each rule** and select "**Edit in CLI**" and copy/paste this command in order to bypass the Captive Portal authentication for above rules.

```
set captive-portal-exempt enable
end
```

  - Rules for authenticated users:

Name	Source	Destination	Service	NAT	Action
Allow-Guest	Guest interface	Outside interface	ALL	Yes	Accept
Guest-Deny-All (Optional*)	Guest interface	RFC1918: 10.0.0.0/8 172.16.0.0/12 192.168.0.0/16	ALL	No	Deny

*The explicit deny rule is optional if your FortiGate Implicit Rule is already configured to deny all the traffic.

August 24, 2021 2:20 AM
1238660-0-0-EN