



Eli Banque

Paris, 2 Rue du Pont Neuf,
75001 Paris.
04 44 44 44 44
contact@elibanque.fr
elibanque.fr

Documentation WIFI

Table des matières

Documentation WIFI	1
Configuration initiale	3
Docker compose	4
Remote Management	5
Adoption des AP	6
Adoption terminée	7
Test de connexion	8
Portail Captif.....	9
Serveur RADIUS	10
Création client RADIUS.....	11
Configuration Policies	13
Active Directory Certificate Services	14
Autorisation d'accès.....	15
Test et vérification :	15
Redirection HTTPS	17

Configuration initiale

Configuration d'un réseau Docker nommé `vlan-server`, utilisant le pilote `macvlan`. Ce type de réseau permet de connecter directement des conteneurs au réseau physique, leur attribuant des adresses IP uniques comme s'ils étaient des machines physiques. Le réseau est configuré avec le sous-réseau `172.18.100.0/24` et une passerelle `172.18.100.254`. Deux conteneurs sont connectés : `user-controller-1` `172.18.100.6` et `user-mongo-1` `172.18.100.7`, chacun ayant une adresse MAC unique, ce qui facilite leur identification et leur communication sur le réseau. Ce réseau repose sur l'interface physique `ens192`, permettant aux conteneurs d'accéder directement à un VLAN spécifique.

```
[
  {
    "Name": "vlan-server",
    "Id": "ee94558d3074e88fbb3e404899504c02cfd6edc94060e9ccad4a3fdef22742a3",
    "Created": "2024-11-26T13:58:18.457133166Z",
    "Scope": "local",
    "Driver": "macvlan",
    "EnableIPv6": false,
    "IPAM": {
      "Driver": "default",
      "Options": {},
      "Config": [
        {
          "Subnet": "172.18.100.0/24",
          "Gateway": "172.18.100.254"
        }
      ]
    },
    "Internal": false,
    "Attachable": false,
    "Ingress": false,
    "ConfigFrom": {
      "Network": ""
    },
    "ConfigOnly": false,
    "Containers": {
      "9327e7f7b1ad925e17c3a027ebca281ddc0e8e13407f469e516fafa9c049d413": {
        "Name": "user-controller-1",
        "EndpointID": "ec06ad10a7f99067a4efdc0eddd16d8ee6ccd7562e45effcc07f34ba14bad8",
        "MacAddress": "02:42:ac:12:64:06",
        "IPv4Address": "172.18.100.6/24",
        "IPv6Address": ""
      },
      "a0e124420b8862ae061e457087e6713a6c24604dec093033e3966466fccfaed8": {
        "Name": "user-mongo-1",
        "EndpointID": "d9f2616fc765345b7cde9b13ba924be5dc4b328b44347e73598ed35e1fa6fb7c",
        "MacAddress": "02:42:ac:12:64:07",
        "IPv4Address": "172.18.100.7/24",
        "IPv6Address": ""
      }
    },
    "Options": {
      "parent": "ens192"
    },
    "Labels": {}
  }
]
```

Docker compose

Création de notre Docker Compose qui va permettre d'avoir notre BDD Mongo et notre Controller Unifi.

```
[User@localhost ~]$ cat docker-compose.yml
services:
  mongo:
    image: mongo:3.6
    networks:
      out:
        ipv4_address: 172.18.100.7
    restart: always
    volumes:
      - db:/data/db
      - dbcfg:/data/configdb

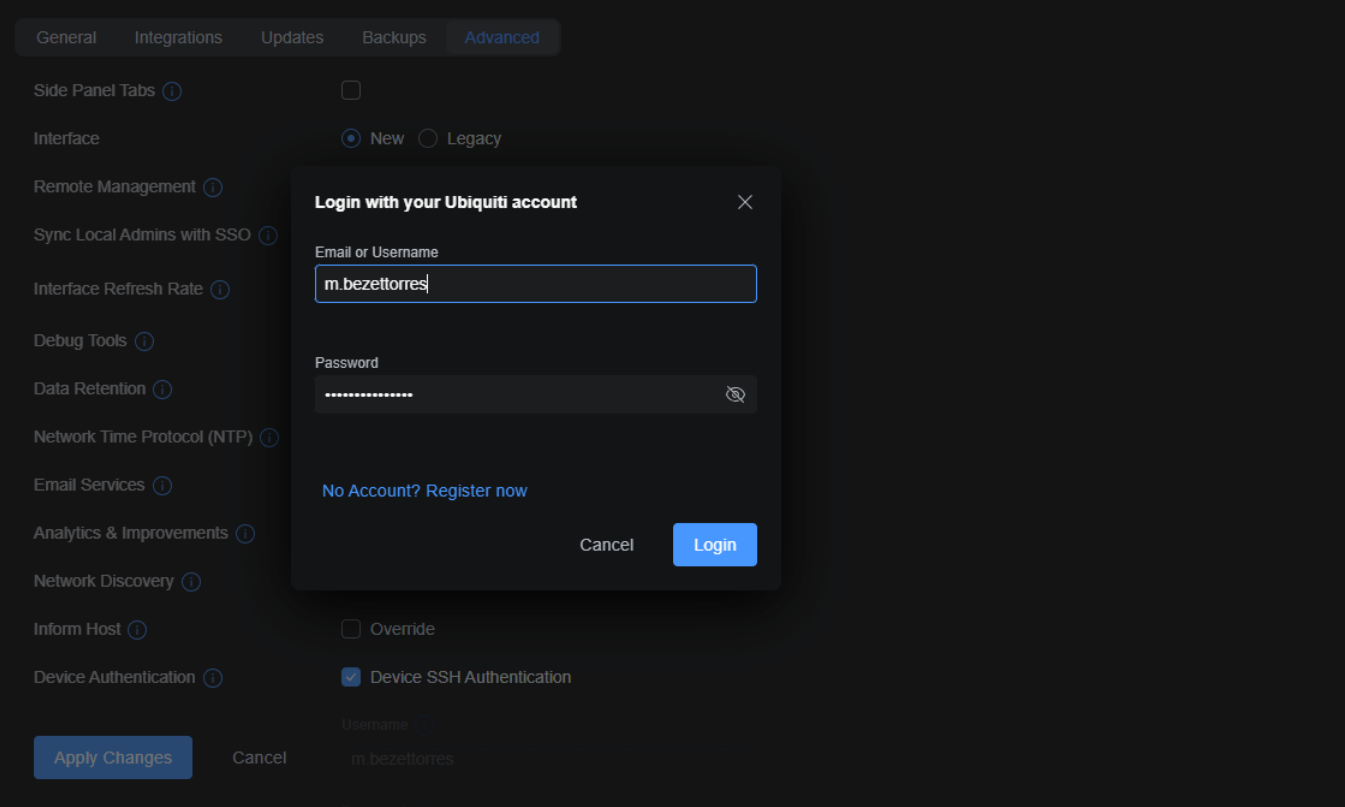
  controller:
    image: "jacobalberty/unifi:${TAG:-latest}"
    depends_on:
      - mongo
    networks:
      out:
        ipv4_address: 172.18.100.6
    restart: always
    volumes:
      - dir:/unifi
      - data:/unifi/data
      - log:/unifi/log
      - cert:/unifi/cert
      - init:/unifi/init.d
      - run:/var/run/unifi
      - ./backup:/unifi/data/backup
    environment:
      DB_URI: mongodbd://mongo/unifi
      STATDB_URI: mongodbd://mongo/unifi_stat
      DB_NAME: unifi
    ports:
      - "3478:3478/udp"
      - "6789:6789/tcp"
      - "8080:8080/tcp"
      - "443:8443/tcp"
      - "8880:8880/tcp"
      - "8843:8843/tcp"
      - "10001:10001/udp"

networks:
  out:
    name: vlan-server
    external: true

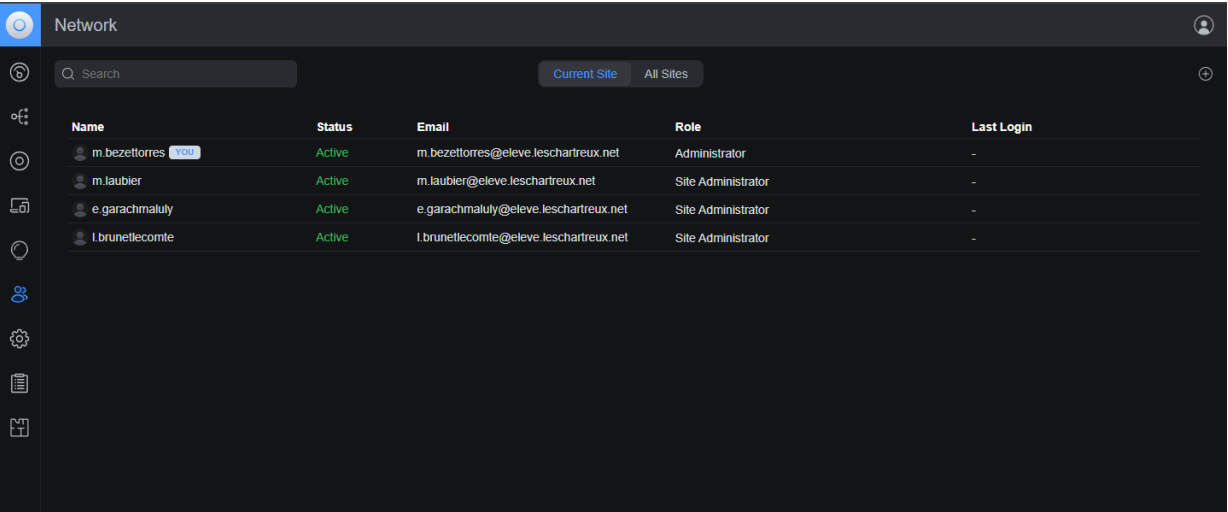
volumes:
  db:
  dbcfg:
  data:
  log:
  cert:
  init:
```

Remote Management

Nous devons activer le Remote Management afin de pouvoir se connecter sur notre interface et gérer nos AP par la suite sans cette option nous ne pouvons administrer nos AP.

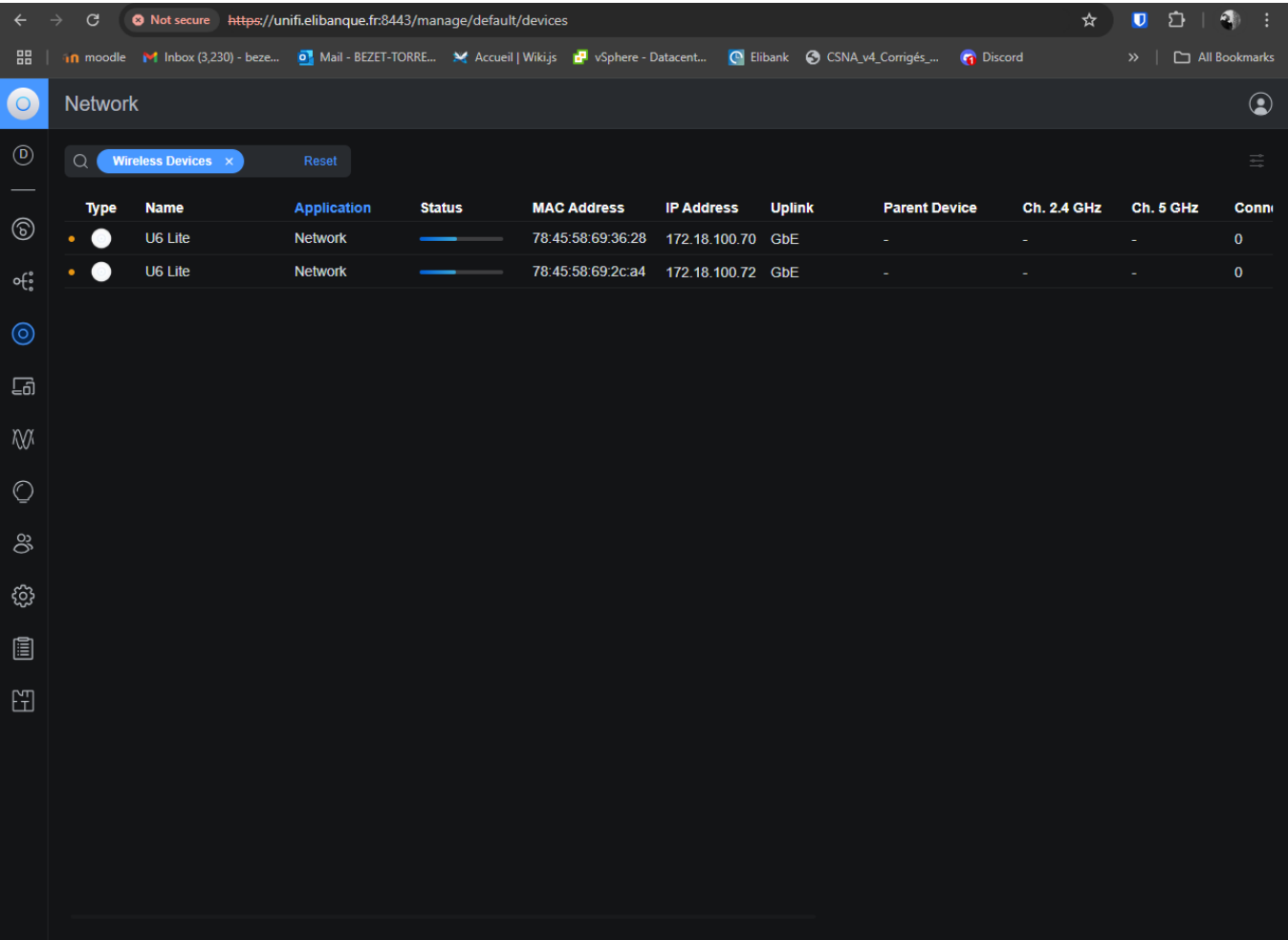


Création des comptes de management pour les membres de l'organisation afin que tout le monde ai accès à l'administration.



Adoption des AP

Nos AP on récupérer deux adresses IP via notre DHCP et nous pouvons ainsi les adopter sous Unifi.



Adoption terminée

← → ↻

Not secure https://unifi.elibanque.fr:8443/manage/default/devices

☆ ⓘ 🔒 🌐

moodle

Inbox (3,230) - beze...

Mail - BEZET-TORRE...

Accueil | Wiki.js

vSphere - Datacent...

Elibank

CSNA_v4_Corrigés...

Discord

»

All Bookmarks

Network

Wireless Devices

Reset

Type	Name	Application	Status	MAC Address	IP Address	Uplink
• ●	U6 Lite	Network	Getting Ready	78:45:58:69:36:28	172.18.100.70	GbE
• ●	U6 Lite	Network	Getting Ready	78:45:58:69:2c:a4	172.18.100.72	GbE

U6 Lite

🔗 📊 ⚙️

U6 Lite

Connected to -

Radio Manager

TX Retries

Low (0%)

16:35 04:35 Now

↓ 538 bps ↑ 5.42 Kbps 16m 14s

Ch. 6 (2.4 GHz, 20 MHz) 2x2 WiFi 4 0 Clients

Ch. 48 (5 GHz, 40 MHz) 2x2 WiFi 6 0 Clients

Model U6 Lite

IP Address 172.18.100.72

MAC Address 78:45:58:69:2c:a4

Device Version 6.6.78

WiFi Name G2-WIFI-PPE

Uptime 16m 14s

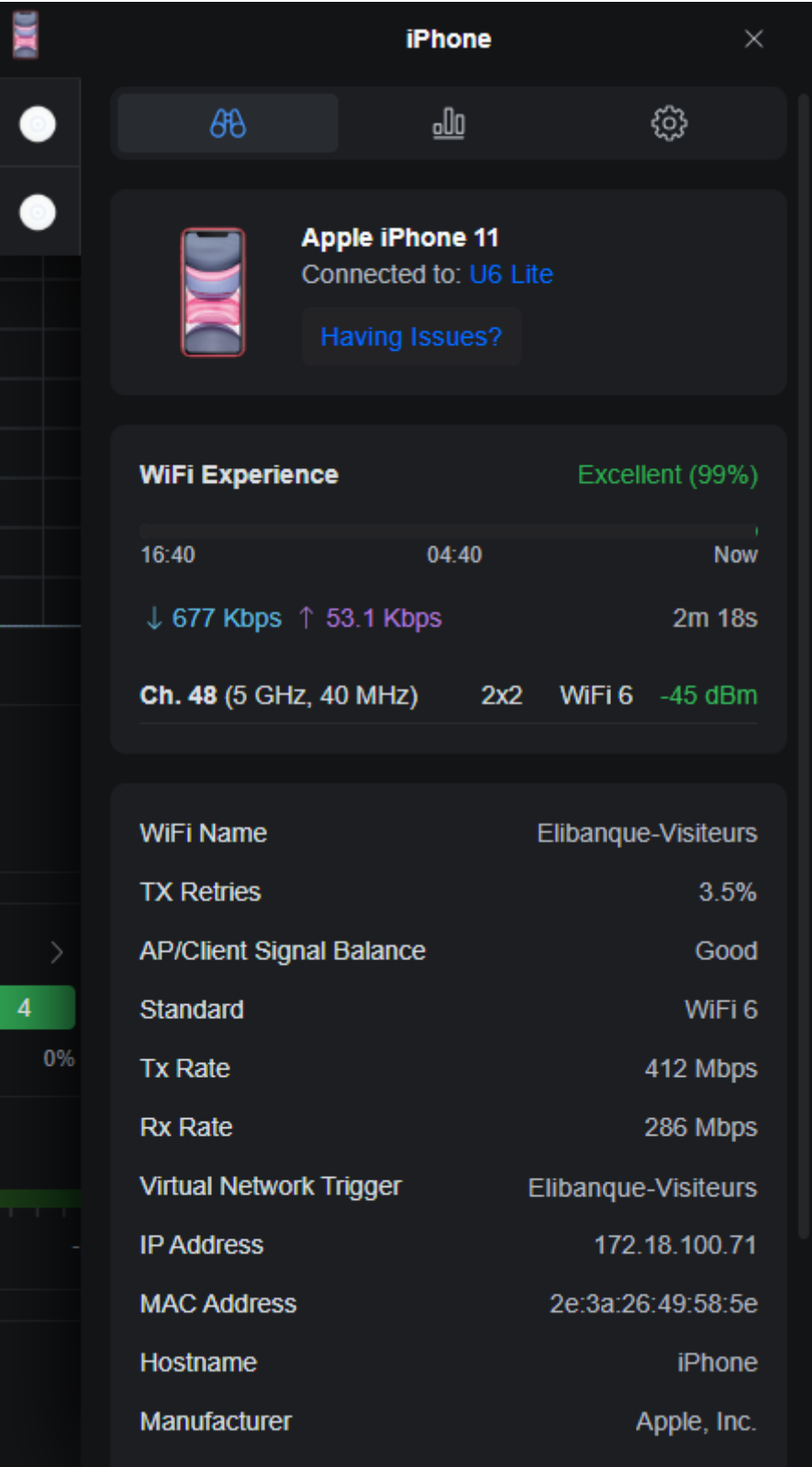
Memory Usage 31.2%

Load Average 0.54 / 0.63 / 0.47

AP Groups All APs

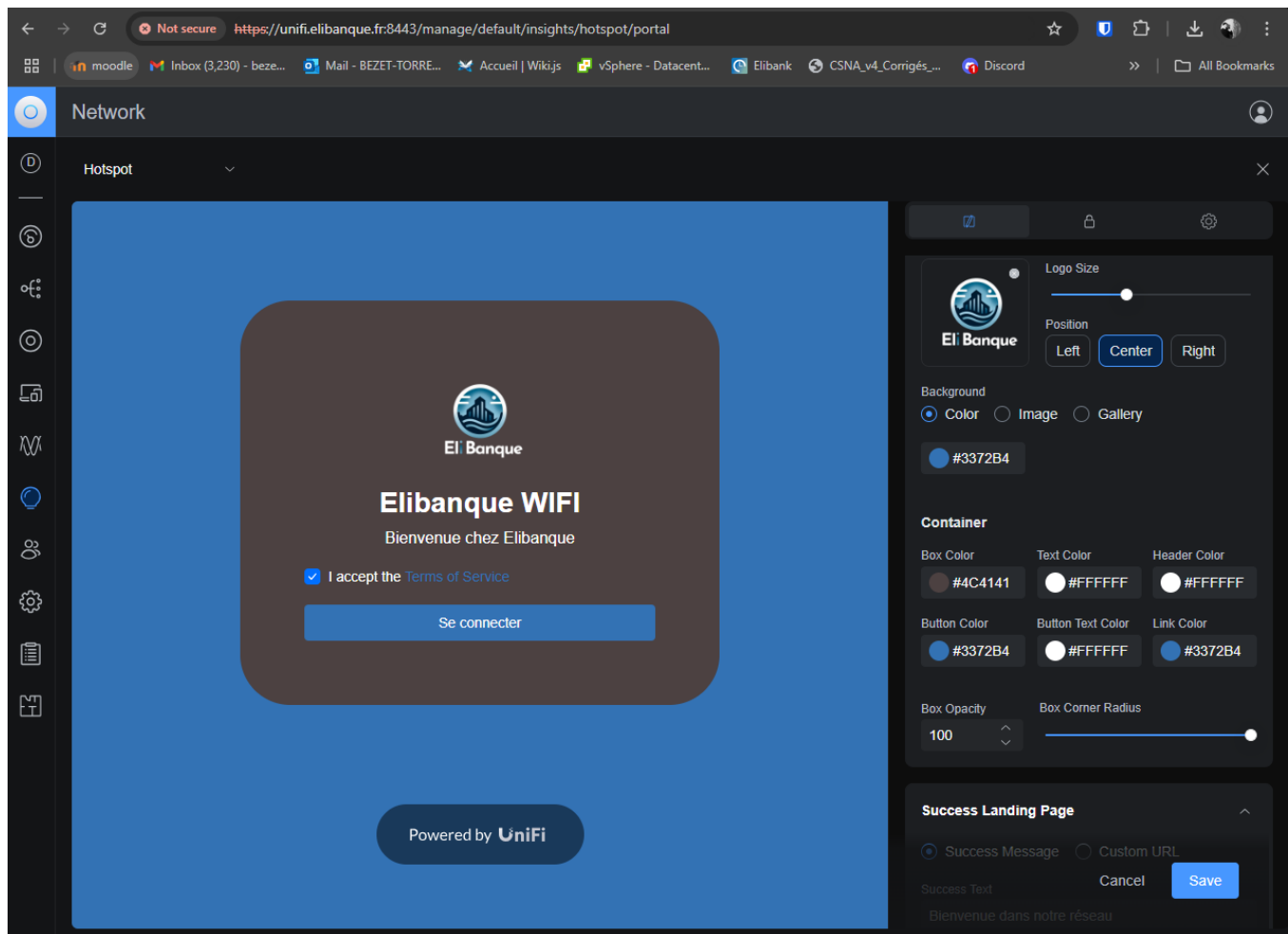
7

Test de connexion



Portail Captif

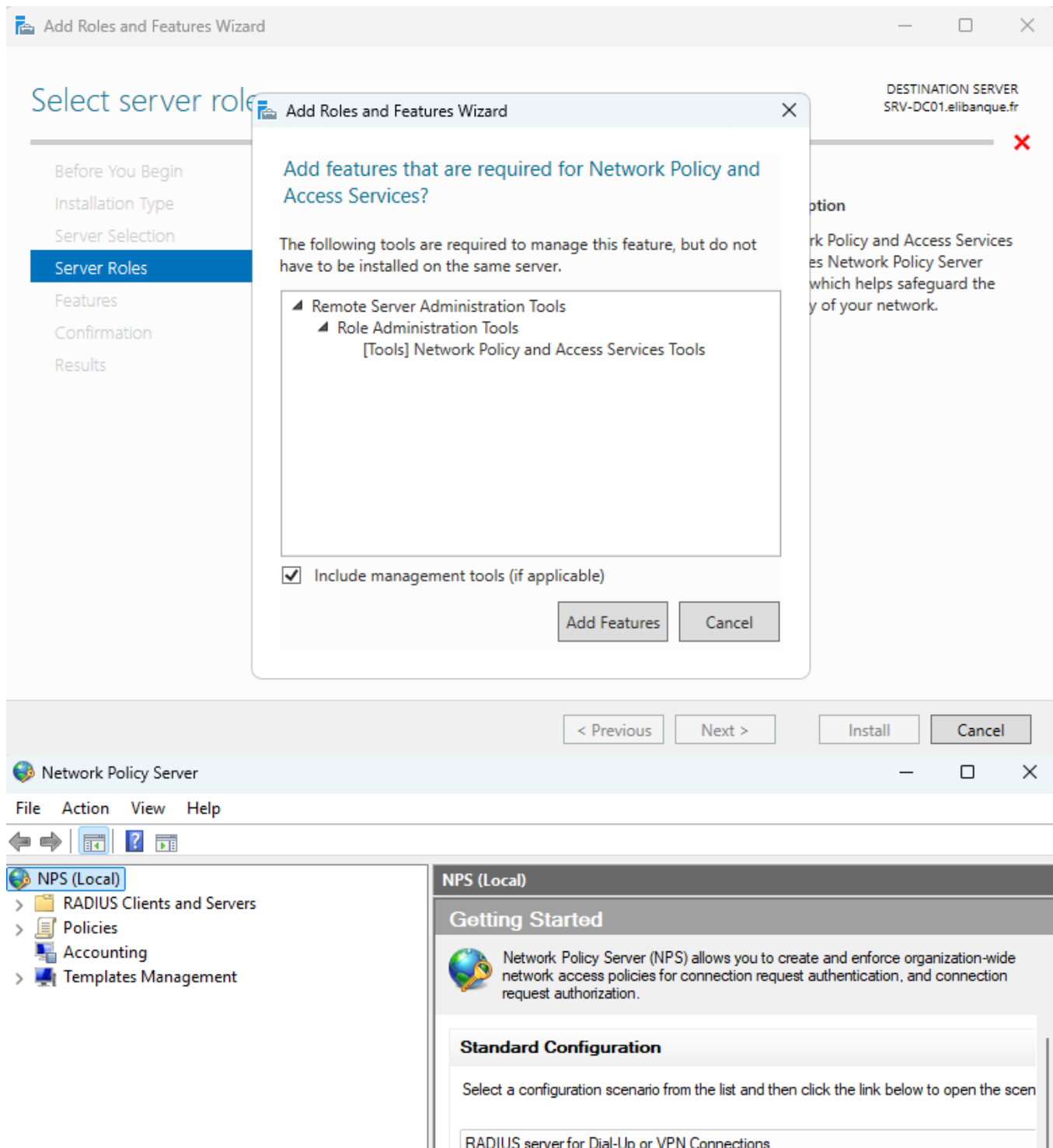
Création de notre **Portail Captif** d'accès au WIFI avec image personnalisée et relié à notre **Serveur Radius**.



Serveur RADIUS

Ajout du rôle NPS à notre Serveur Membre :

Le serveur NPS effectue de façon centralisée les processus d'authentification, d'autorisation et de gestion des comptes pour les connexions sans fil, par commutateur d'authentification, par accès à distance et VPN.



Création client RADIUS

Création d'un client RADIUS avec l'adresse IP de notre contrôleur Unifi 172.18.100.6
 Nous avons donc généré un Shared Secret que l'on rentrera dans notre contrôleur Unifi
 Shared Secret : « SuNs\$LqxKJFor#thn0AhBSIAIwDJhy2IOqBFIDuFEzkITi97\$4Er8i8 »

New RADIUS Client

Settings

Advanced

☒ Enable this RADIUS client

☐ Select an existing template:

Name and Address

Friendly name:

UniFi Controller

Address (IP or DNS):

172.18.100.6

Verify...

Shared Secret

Select an existing Shared Secrets template:

None

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

☐ Manual
 ☒ Generate

Shared secret:

SuNs\$LqxKJFor#thn0AhBSIAIwDJhy2IOqBFIDuFEzkITi97\$4Er8i8

⚠

Generate

Clear

Création de notre Authentication Server sous UNIFI avec 172.18.100.3 l'adresse IP de notre serveur NPS avec la Shared Secret précédente :

<

Name

RADIUS-WIFI

RADIUS Assigned VLAN Support

Wired Networks ⓘ

☐

Wireless Networks ⓘ

☐

RADIUS Settings

TLS ⓘ

☐

Authentication Servers

IP Address

1812

Shared Secret ⓘ

Add

IP Address	Port	Shared Secret	Edit
172.18.100.3	1812	

Accounting

☐

Interim Update Interval


☐

Configuration Policies

Nous devons ajouter le **Secured Password EAP-MSCHAP v2** :

Méthode **EAP** définie par **Microsoft** qui encapsule le protocole d'authentification **MSCHAP v2**, utilisant le nom d'utilisateur et un mot de passe pour l'authentification.

New Network Policy



Configure Authentication Methods

Configure one or more authentication methods required for the connection request to match this policy. For EAP authentication, you must configure an EAP type.

EAP types are negotiated between NPS and the client in the order in which they are listed.

EAP Types:

Microsoft: Secured password (EAP-MSCHAP v2)

Move Up
Move Down

Add...
Edit...
Remove

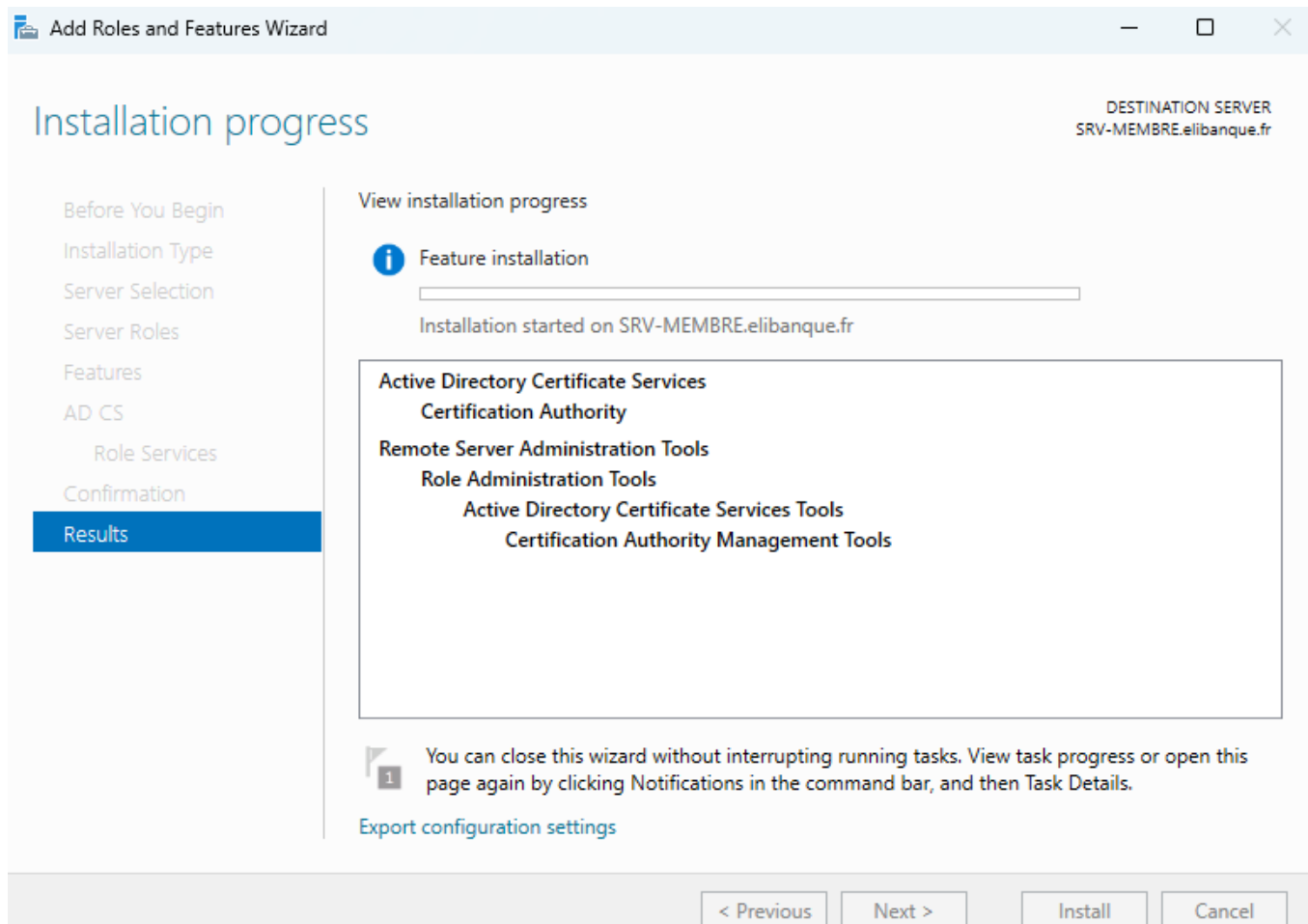
Less secure authentication methods:

- ☒ Microsoft Encrypted Authentication version 2 (MS-CHAP-v2)
 - ☒ User can change password after it has expired
- ☒ Microsoft Encrypted Authentication (MS-CHAP)
 - ☒ User can change password after it has expired
- ☐ Encrypted authentication (CHAP)
- ☐ Unencrypted authentication (PAP, SPAP)
- ☐ Allow clients to connect without negotiating an authentication method.

Previous
Next
Finish
Cancel

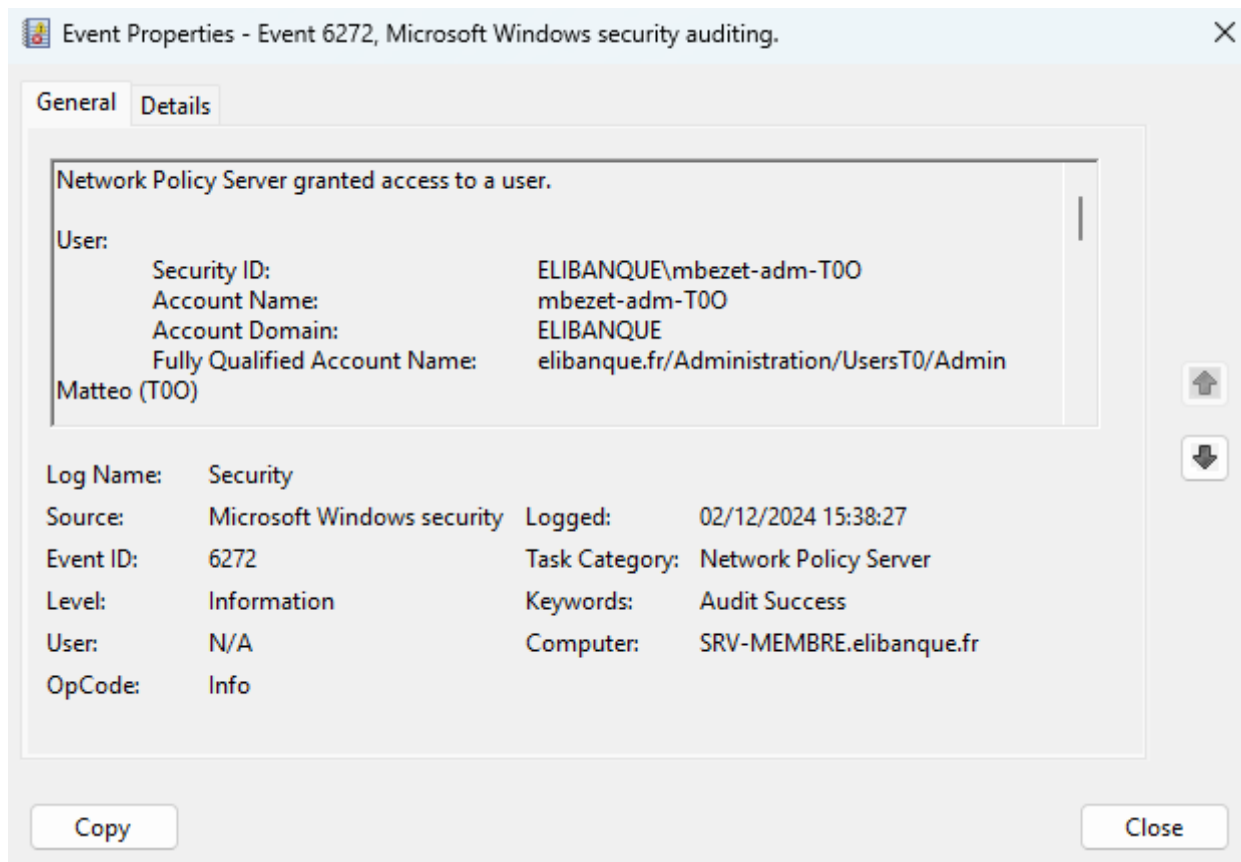
Active Directory Certificate Services

Services de certificats Active Directory est un rôle Windows Server pour l'émission et la gestion des certificats d'infrastructure à **clé publique** (PKI) utilisés dans les protocoles de communication et d'authentification sécurisés.



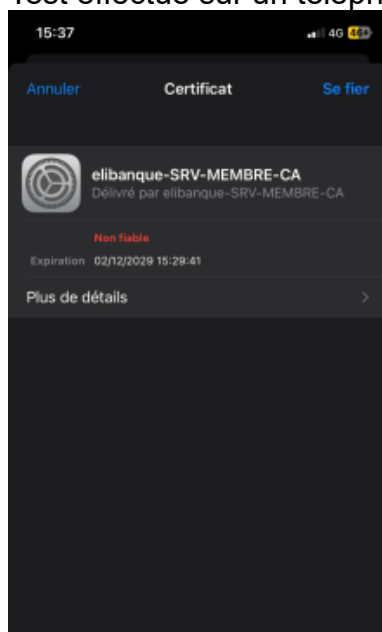
Autorisation d'accès

Nous pouvons voir via l'Event Viewer que le serveur NPS à autoriser l'accès à mon compte m.bezet-adm-T00 sur notre WIFI Elibanque.



Test et vérification :

Test effectué sur un téléphone se connectant au WIFI :



Notre téléphone est donc rentré en tant que Client dans nos Pannels.

Network

🔍 Clients ✕ Reset

Name ↑	Vendor	Connection	Network	WiFi	Experie...	Technol...	Channel
📱 Apple iPhone 11	Apple, Inc.	U6 Lite	-	Elibanque...	Excellent	1x1, WiFi 6	48 (5 GHz, 40 MHz)

Apple iPhone 11 ✕

🔗 📊 ⚙️

WiFi Experience Excellent (99%)

15:4503:45Now

↓ 38.2 Kbps ↑ 8.33 Kbps1m 57s

Ch. 48 (5 GHz, 40 MHz)1x1WiFi 6-40 dBm

WiFi NameElibanque-Visiteurs

TX Retries0.0%

AP/Client Signal BalanceGood

StandardWiFi 6

Tx Rate286 Mbps

Rx Rate286 Mbps

Virtual Network TriggerElibanque-Visiteurs

IP Address172.18.100.75

MAC Address86:ba:86:98:ab:76

ManufacturerApple, Inc.

ModelApple iPhone 11

OSApple iOS

Down Pkts/Bytes235 / 97.1 KB

Up Pkts/Bytes134 / 22.2 KB

16

Redirection HTTPS

The screenshot shows a configuration interface for a Captive Portal. At the top, there are three icons: a notepad, a lock, and a gear. The main settings are organized into three sections:

- Default Expiration:** A dropdown menu set to "8 Hours" and a language selector set to "English". Below these is an "Edit (1)" link.
- Landing Page Settings:** A section with four checkboxes:
 - ☒ Show Landing Page
 - ☒ HTTPS Redirection Support (with an info icon)
 - ☒ Encrypted URL (with an info icon) and ☒ Secure Portal (with an info icon)
 - ☐ Domain (with an info icon)
- Authorization Access:** A section with a "Pre-Authorization Allowances" header (with an info icon) and a "+ Add Hostname, IP or Subnet" button. Below this is a "Post-Authorization Restrictions" header (with an info icon) followed by a list of IP ranges:
 - 192.168.0.0/16 (with a delete icon)
 - 172.16.0.0/12 (with a delete icon)

La redirection automatique en **HTTPS** pour notre Portail Captif doit se faire via HTTPS :

L'utilisation de HTTPS garantit que ces données sont chiffrées lors de leur transmission

Si le portail captif utilise uniquement HTTP, un attaquant peut intercepter la requête et rediriger l'utilisateur vers une fausse page, lui volant ses informations.

Les connexions HTTP non sécurisées permettent à des attaquants d'injecter du contenu malveillant dans la page du portail captif, ce qui peut compromettre la sécurité des utilisateurs.