

# Mise en place d'une infrastructure radius

## Table des matières

Mise en place d'une infrastructure radius .....	1
Installation du serveur NPS (radius) .....	1
Pare-feu du serveur NPS .....	10
Configuration du client Windows.....	11
Configuration du switch .....	15
Configuration de la borne wifi.....	15

Installation du serveur NPS (radius)

Installer le serveur nps

## Sélectionner des rôles de serveurs

SERVEUR DE DESTINATION  
WIN-SRV-CD1.tierslieux.pod1

Avant de commencer  
Type d'installation  
Sélection du serveur  
Rôles de serveurs  
Fonctionnalités  
Confirmation  
Résultats

Sélectionnez un ou plusieurs rôles à installer sur le serveur sélectionné.

## Rôles

- Attestation d'intégrité de l'appareil
- Hyper-V
- Serveur de télécopie
- Serveur DHCP (Installé)
- Serveur DNS (Installé)
- Serveur Web (IIS)
- Service Guardian hôte
- Services AD DS (Installé)
- Services AD LDS (Active Directory Lightweight Dire
- Services AD RMS (Active Directory Rights Manage
- Services Bureau à distance
- Services d'activation en volume
- Services d'impression et de numérisation de docu
- Services de certificats Active Directory (1 sur 6 inst
- Services de déploiement Windows
- Services de fédération Active Directory (AD FS)
- Services de fichiers et de stockage (2 sur 12 install
- Services de stratégie et d'accès réseau (Installé)
- Services WSUS (Windows Server Update Services)

## Description

L'accès à distance fournit une connectivité transparente via DirectAccess, les réseaux VPN et le proxy d'application Web. DirectAccess fournit une expérience de connectivité permanente et gérée en continu. Le service d'accès à distance (RAS) fournit des services VPN classiques, notamment une connectivité de site à site (filiale ou nuage). Le proxy d'application Web permet la publication de certaines applications HTTP et HTTPS spécifiques de votre réseau d'entreprise à destination d'appareils clients situés hors du réseau d'entreprise. Le routage fournit des fonctionnalités de routage classiques, notamment la traduction d'adresses réseau.

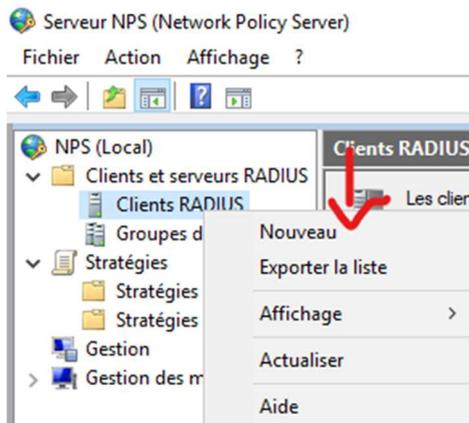
&lt; Précédent

Suivant &gt;

Installer

Annuler

## Ajouter un nouveau client



Propriétés de Borne wifi



Paramètres Avancé

Activer ce client RADIUS

Sélectionner un modèle existant :

▼

Nom et adresse

Nom convivial :

Borne wifi

Adresse (IP ou DNS) :

172.17.1.240 Vérifier...

Secret partagé

Sélectionnez un modèle de secrets partagés existant :

Aucun ▼

Pour taper manuellement un secret partagé, cliquez sur Manuel. Pour générer automatiquement un secret partagé, cliquez sur Générer. Vous devez configurer le client RADIUS avec le même secret partagé entré ici. Les secrets partagés respectent la casse.

Manuel  Générer

Secret partagé :

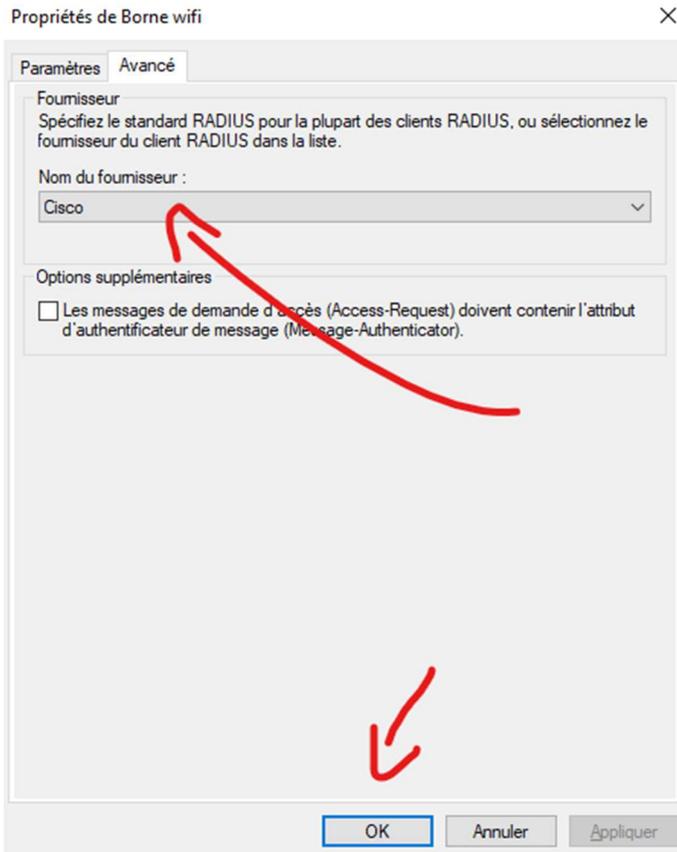
●●●●●●●●

Confirmez le secret partagé :

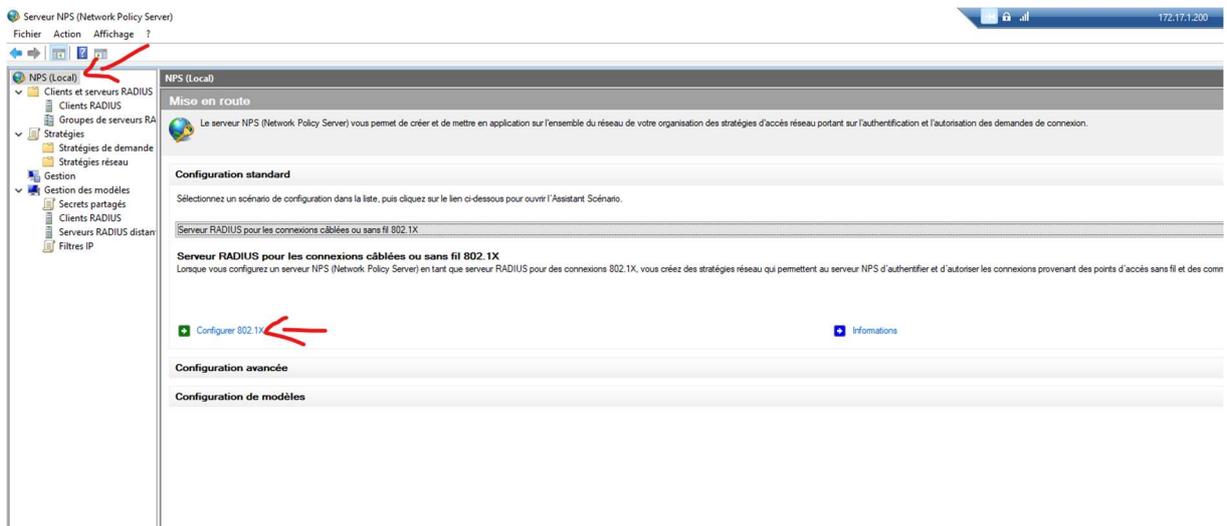
●●●●●●●●

OK Annuler Appliquer

Ajouter le fournisseur Cisco si le client est de la marque Cisco



## Ajouter la règle des autorisations





## Sélectionner le type de connexions 802.1X

### Type de connexions 802.1X :

- Connexions sans fil sécurisées

Lorsque vous déployez des points d'accès sans fil 802.1X sur votre réseau, le serveur NPS (Network Policy Server) peut authentifier et autoriser les demandes de connexion effectuées par les clients sans fil qui se connectent via ces points d'accès.

- Connexions câblées (Ethernet) sécurisées

Lorsque vous déployez des commutateurs d'authentification 802.1X sur votre réseau, le serveur NPS (Network Policy Server) peut authentifier et autoriser les demandes de connexion effectuées par les clients Ethernet qui se connectent via ces commutateurs.

### Nom :

Ce texte par défaut est utilisé pour composer le nom de chacune des stratégies créées à l'aide de cet Assistant. Vous pouvez vous servir du texte par défaut ou le modifier.



Précédent

Suivant

Terminer

Annuler



## Spécifier les commutateurs 802.1X

Spécifiez les commutateurs ou points d'accès sans fil 802.1X (clients RADIUS)

Les clients RADIUS sont des serveurs d'accès réseau, à l'image des commutateurs d'authentification et des points d'accès sans fil. Les clients RADIUS ne sont pas des ordinateurs clients.

Pour spécifier un client RADIUS, cliquez sur Ajouter.

### Clients RADIUS :

Bome wifi

Ajouter...

Modifier...

Supprimer

Précédent

Suivant

Terminer

Annuler



## Configurer une méthode d'authentification

Sélectionnez le type de protocole EAP pour cette stratégie.

**Type (basé sur la méthode d'accès et la configuration réseau) :**

Microsoft: PEAP (Protected EAP) ▾

Configurer...

Précédent

Suivant

Terminer

Annuler

Ajouter le groupe d'utilisateur ou d'ordinateur pouvant se connecter au réseau



## Spécifier des groupes d'utilisateurs

L'accès des utilisateurs membres du ou des groupes sélectionnés sera autorisé ou non en fonction du paramètre d'autorisation d'accès de la stratégie réseau.

Pour sélectionner des groupes d'utilisateurs, cliquez sur Ajouter. Si aucun groupe n'est sélectionné, cette stratégie s'applique à tous les utilisateurs.

Groupes

TIERSLIEUX\GG\_Pod1

Ajouter...

Supprimer

Précédent

Suivant

Terminer

Annuler

Configuration Optionnel



## Configurer les contrôles du trafic

Utilisez des réseaux locaux virtuels (VLAN) et des listes de contrôle d'accès (ACL) pour contrôler le trafic réseau.

Si vos clients RADIUS (commutateurs d'authentification et points d'accès sans fil) prennent en charge l'affectation de contrôles de trafic à l'aide d'attributs de tunnel RADIUS, vous pouvez configurer ces attributs ici. Si vous configurez ces attributs, le serveur NPS invite les clients RADIUS à appliquer ces paramètres pour les demandes de connexion authentifiées et autorisées.

Si vous n'utilisez pas de contrôles du trafic ou si vous souhaitez les configurer ultérieurement, cliquez sur Suivant.

### Configuration du contrôle du trafic

Pour configurer les attributs de contrôle du trafic, cliquez sur Configurer.

Configurer...

Précédent

Suivant

Terminer

Annuler

Puis cliquer sur terminer

Voici le résultat attendu

Connexions sans fil sécurisées	Activé	1	Accorder l'accès	Non spécifié
Connexions au serveur Microsoft de Routage et Accès distants	Activé	2	Refuser l'accès	Non spécifié
Connexions à d'autres serveurs d'accès	Activé	3	Refuser l'accès	Non spécifié

Connexions sans fil sécurisées

Conditions - Si les conditions suivantes sont réunies :

Condition	Valeur
Type de port NAS	Sans fil - Autre OU Sans fil - IEEE 802.11
Groupes Windows	TIERSLIEUXGG_Pod1

Paramètres - Les paramètres suivants sont appliqués :

Paramètre	Valeur
Ignorer les propriétés de numérotation des utilisateurs	Vrai
Autorisation d'accès	Accorder l'accès
Méthode EAP (Extensible Authentication Protocol)	Microsoft: PEAP (Protected EAP)
Méthode d'authentification	Protocole: EAP OU Authentification avec chiffrement (CHAP) OU MS-CHAP v1 OU MS-CHAP v2 (Utilisateur peut modifier le mot de passe après son expiration) OU MS-CHAP v2 OU MS-CHAP v2 (Utilisateur peut modifier le mot de passe après son expiration)
Framed-Protocol	PPP
Service-Type	Framed

Pour faire l'association user vlan il faut rajouter ces trois paramètres

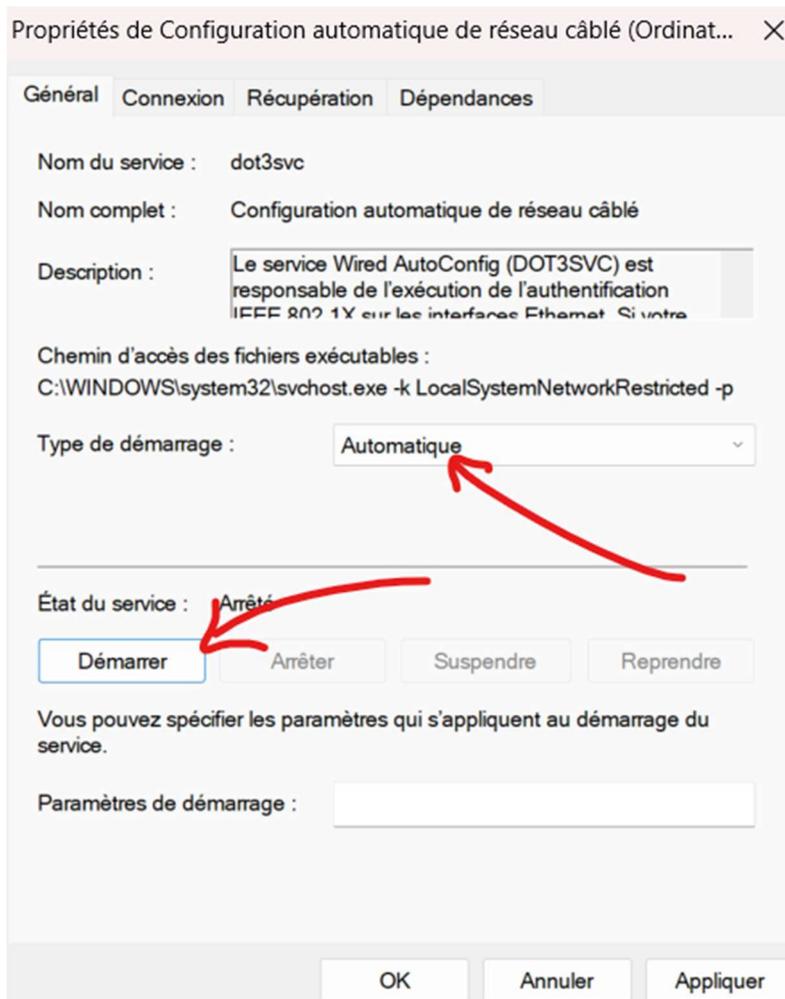
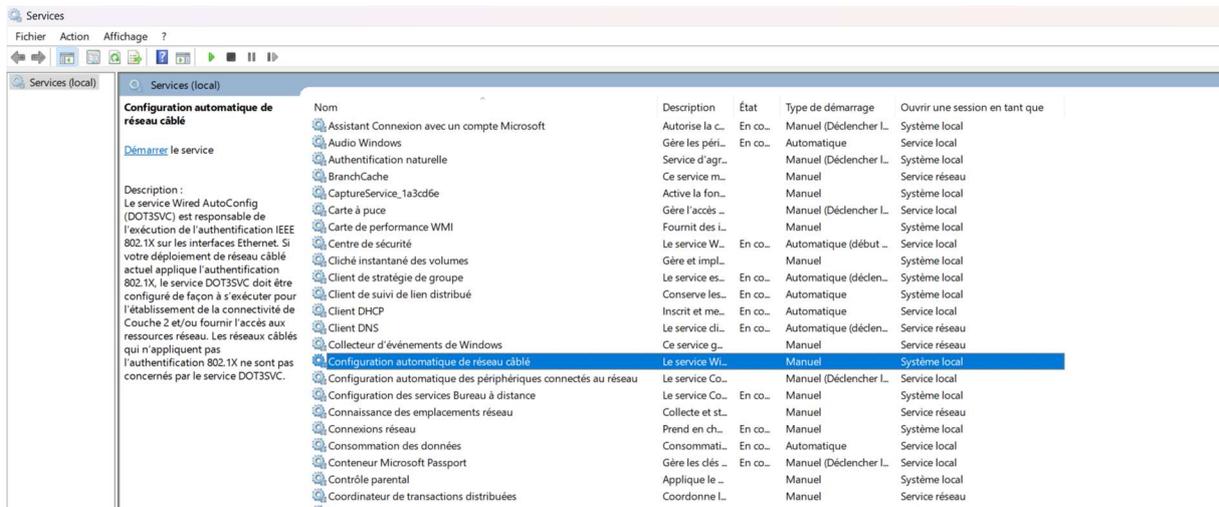
**Tunnel-Type**                      **Virtual LANs (VLAN)**  
**Tunnel-Pvt-Group-ID**            **101**  
**Tunnel-Medium-Type**            **802 (includes all 802 media plus Ethernet canonical for...**

### Pare-feu du serveur NPS

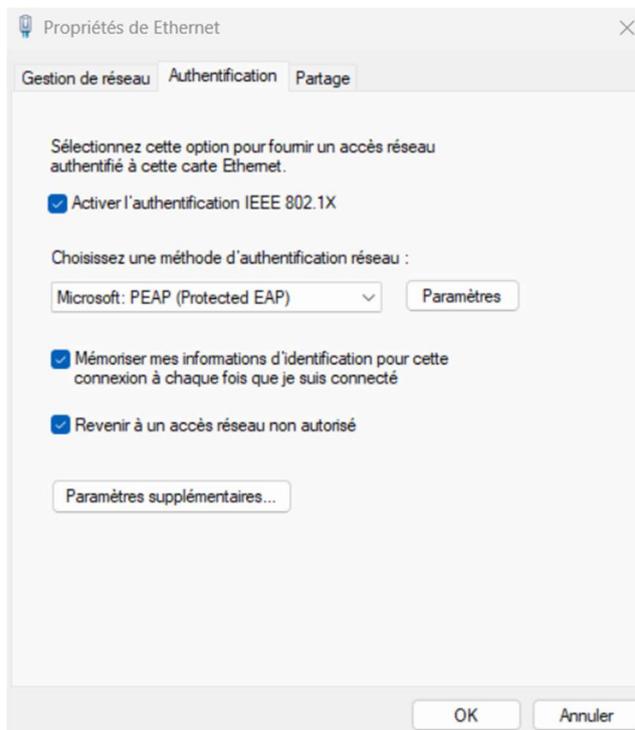
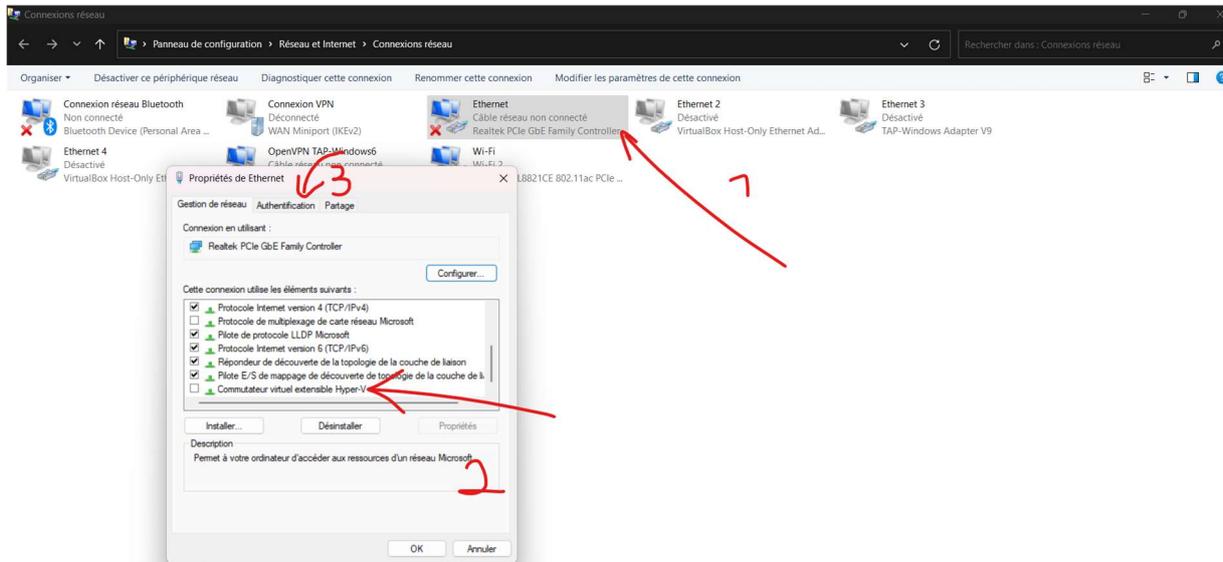
Rajouter 2 règles de pare-feu en trafics entrant

<input checked="" type="checkbox"/> RADIUS		Doma...	Oui	Autoriser	Non	Tout	Tout	Tout	UDP	1812	Tout	Tout	Tout
<input checked="" type="checkbox"/> RADIUS		Doma...	Oui	Autoriser	Non	Tout	Tout	Tout	UDP	1813	Tout	Tout	Tout

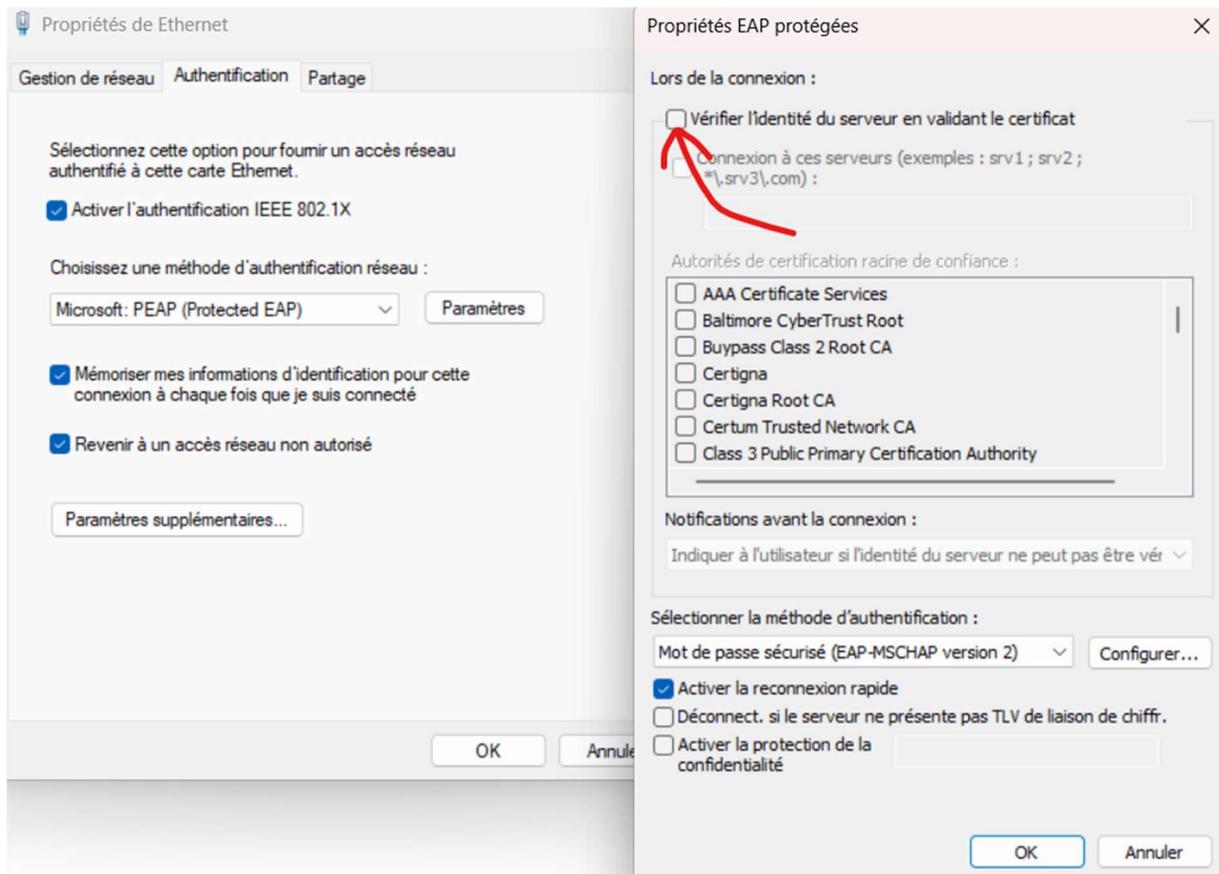
## Configuration du client Windows



Dans les propriétés de la carte réseau désactivé « le commutateur virtuel extensible hyper-v »



Désactivé la vérification de certificat



Et l'authentification avant l'ouverture de session

Paramètres avancés



Paramètres 802.1X

Spécifier le mode d'authentification

Authentification de l'utilisateur ▾

Enregistrer ident.

Supprimer les informations d'identification pour tous les utilisateurs

Activer l'authentification unique pour ce réseau

Immédiatement avant l'ouverture de session de l'utilisateur

Immédiatement après l'ouverture de session de l'utilisateur

Délai maximal (secondes) :

10



Autoriser l'affichage de boîtes de dialogue supplémentaires pendant l'authentification unique

Ce réseau utilise des réseaux locaux virtuels distincts pour l'authentification de l'ordinateur et de l'utilisateur

OK

Annuler

## Configuration du switch

```
(config)#aaa new-model
```

```
(config)#aaa authentication dot1x default group RADIUS
```

```
(config)#aaa authorization network default group RADIUS
```

```
(config)#dot1x system-auth-control
```

```
(config)# RADIUS-server host 172.16.0.1 auth-port 1812 acct-port 1813 key toto
```

```
(config)# interface f0/1
```

```
(config-if)#switchport mode access
```

```
(config-if)#authentication port-control auto
```

```
(config-if)#dot1x pae authenticator
```

```
(config-if)#authentication event no-response action authorize vlan 99
```

```
(config-if)#authentication event fail action authorize vlan 100
```

## Configuration de la borne wifi

Il faut passer en mode expert

The screenshot displays the Cisco Business Wireless 150AX Access Point management interface. The top navigation bar includes a search icon, a help icon, a warning icon, a refresh icon, a save icon, a settings icon (highlighted with a red arrow), and a mail icon. The main content area is divided into several sections:

- Network Summary:** A dashboard showing various network metrics with status indicators (green checkmarks or red dots).

Metric	Status	Value
Wireless Networks	✓	3
Access Points	✓	1
Active Clients	✓	1
APs	✓	1
Rogues	✓	0
Interferers	✓	0
802.11a/n/ac/ax Radios	✓	1
802.11b/g/n/ax Radios	✓	1
LAN	●	
Internet	●	
- ACCESS POINTS BY USAGE:** A section showing a large blue donut chart representing usage data for AP1484.7364.19E8.
- CLIENTS:** A table listing active clients with columns for Client Identity, Device Type, Usage, and Throughput.

Client Identity	Device Type	Usage	Throughput
1 → 4e:eb:3a:ea:bc:b8	Unclassified	244.1 MB	
2 → ismael.fahdi	Unclassified	4.6 MB	

Ajouter l'ip du radius

Cisco Business Wireless 150AX Access Point

- Monitoring
- Wireless Settings
- Management
  - Access
  - Admin Accounts
  - Time
  - Software Update
- Services
- Advanced

Admin Accounts

Users 1

Management User Priority Order Local Admin Accounts TACACS+ **RADIUS** Auth Cached Users

Authentication Call Station ID Type AP MAC Address:SSID

Authentication MAC Delimiter Hyphen

Accounting Call Station ID Type IP Address

Accounting MAC Delimiter Hyphen

Fallback Mode Active

Username cisco-probe

Add RADIUS Authentication Server

Action	Server Index	Network User	Management	State	Server IP Address	Shared Key	Port
	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	172.17.1.200	*****	1812

Add RADIUS Accounting Server

Action	Server Index	Network User	Management	State	Server IP Address	Shared Key	Port
	2	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	172.17.1.200	*****	1813

Add/Edit RADIUS Authentication Server

Server Index 2

Network User Enabled

Management Enabled

State Enabled

CoA

Server IP Address 172.17.1.200

Shared Secret \*\*\*\*\*

Confirm Shared Secret \*\*\*\*\*

Show Password

Port Number 1812

Server Timeout 5 Seconds

Relier le wifi avec le radius

Monitoring  
Wireless Settings  
WLANs  
Access Points  
Access Points Groups  
WLAN Users  
Guest WLANs  
Mesh  
Management  
Services  
Advanced

CISCO Cisco Business Wireless 150AX Access Point

WLANs

Active WLANs 3

Add new WLAN

Action	Active	Type	Name	SSID	Security Policy
<input checked="" type="checkbox"/>	Enabled	WLAN	POD1-perso	POD1-perso	Personal(WPA2+WPA3)
<input checked="" type="checkbox"/>	Enabled	WLAN	POD1-tierslieux	POD1-tierslieux	WPA2Enterprise
<input checked="" type="checkbox"/>	Enabled	WLAN	POD1-Invité	POD1-Invité	Guest

General WLAN Security VLAN & Firewall Traffic Shaping Advanced Scheduling

Guest Network

Captive Network Assistant

MAC Filtering

RADIUS Compatibility Cisco ACS

Security Type WPA2 Enterprise

Authentication Server External Radius

Radius Profiling

BYOD

RADIUS Server

Authentication Caching

Add RADIUS Authentication Server

Ac...	State	Server IP Address	Port
<input checked="" type="checkbox"/>	Enabled	172.17.1.200	1812

Add RADIUS Accounting Server

Ac...	State	Server IP Address	Port
<input checked="" type="checkbox"/>	Enabled	172.17.1.200	1813