

ASSURMER



ASSURMER

PROCEDURE DE CONFIGURATION DU POINT D'ACCES SANS FIL CISCO WAP371

Bruno LEVESQUE & Ugo BERNARD

BTS SIO SISR 2B

Référence :	ASSURMER Procédure AP 8	Document :	PROCEDURE AP 8
Responsables :	Ugo BERNARD Bruno LEVESQUE	Date :	08/01/2024

PROCEDURE D'INSTALLATION DU POINT D'ACCES SANS FIL CISCO WAP371

ETAT DU DOCUMENT

☐ Validé
 ☒ En cours de validation
 ☐ En projet
 ☐ Périmé

Liste des révisions

Version	Date	Auteur	Description de la révision	Page
1	08/01/2024	Ugo BERNARD	Création du document et détail de la configuration	10

Redacteurs et Approbateurs

	Nom	Fonction	Visa
Rédacteurs	LEVESQUE Bruno Ugo BERNARD	Techniciens Systèmes et Réseaux	OK
Approbateurs Signataires &	Mme MONSIRE Claire Mr DEGEN Loïc	DSI	
Lecteur	LEVESQUE Bruno Ugo BERNARD	Techniciens Systèmes et Réseaux	OK

Référence :	ASSURMER Procédure AP 8	Document :	PROCEDURE AP 8
Responsables :	Ugo BERNARD Bruno LEVESQUE	Date :	08/01/2024

Table des matières

1. Point d'accès sans fil CISCO WAP371 : paramètres par défaut	3
2. Connexion au point d'accès sans fil CISCO WAP371.....	3
3. Configuration du point d'accès sans fil CISCO WAP371	3
4. Configuration du WPA Enterprise	9

Référence :	ASSURMER Procédure AP 8	Document :	PROCEDURE AP 8
Responsables :	Ugo BERNARD Bruno LEVESQUE	Date :	08/01/2024

1. Point d'accès sans fil CISCO WAP371 : paramètres par défaut

Paramètre	Valeur par défaut
Nom d'utilisateur	cisco
Mot de passe	cisco
Adresse IP LAN	192.168.1.245
Masque de sous-réseau	255.255.255.0

2. Connexion au point d'accès sans fil CISCO WAP371

Dans la configuration par défaut de l'appareil, l'accès Wi-Fi est désactivé. Vous devez exécuter la configuration initiale en utilisant une connexion Ethernet filaire. Pour connecter l'appareil au réseau filaire :

- ETAPE 1 : Modifiez les paramètres de la carte réseau de votre machine pour être sur le même réseau que la borne.
- ETAPE 2 : Connectez le câble Ethernet au port Ethernet de votre PC et reliez l'autre extrémité au port Ethernet du point d'accès sans fil CISCO WAP371.
- ETAPE 3 : Sur votre navigateur renseignez l'adresse suivante dans la barre de recherche : <https://192.168.1.245>.
- ETAPE 4 : Dans les champs « Nom d'utilisateur » et « Mot de passe », saisissez le nom d'utilisateur par défaut « cisco » et le mot de passe par défaut « cisco ». Cliquez sur connexion.

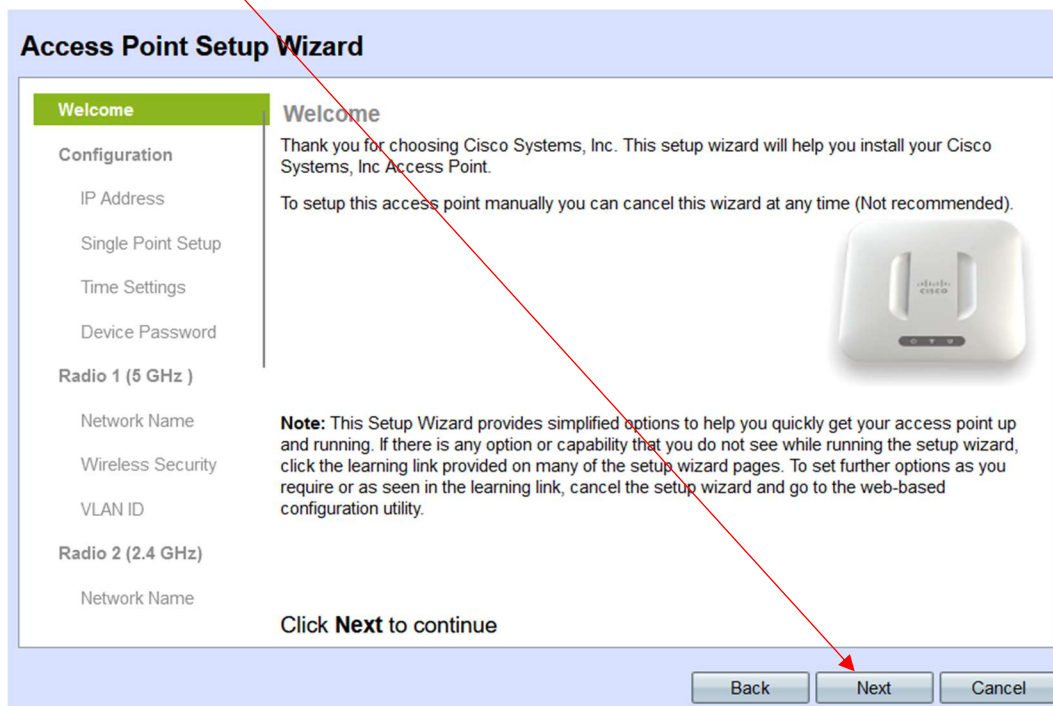


3. Configuration du point d'accès sans fil CISCO WAP371

Pour terminer l'installation du point d'accès, suivez les instructions de l'Assistant Installation. Il est vivement conseillé d'utiliser cet assistant lors de la première installation. En effet, il active le Wi-Fi et permet de vous connecter au réseau sans fil.

Référence :	ASSURMER Procédure AP 8	Document :	PROCEDURE AP 8
Responsables :	Ugo BERNARD Bruno LEVESQUE	Date :	08/01/2024

Une fois sur l'assistant d'installation, vous pouvez commencer à utiliser votre point d'accès sans fil, cliquez sur « Next » :



Access Point Setup Wizard

Welcome

Thank you for choosing Cisco Systems, Inc. This setup wizard will help you install your Cisco Systems, Inc Access Point.

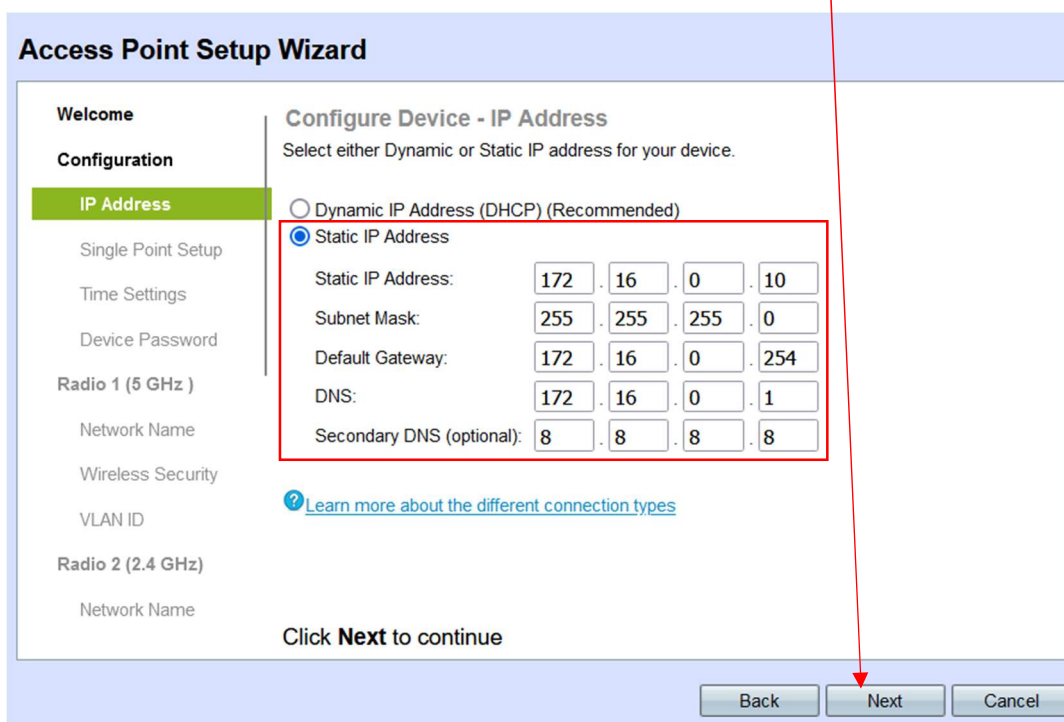
To setup this access point manually you can cancel this wizard at any time (Not recommended).

Note: This Setup Wizard provides simplified options to help you quickly get your access point up and running. If there is any option or capability that you do not see while running the setup wizard, click the learning link provided on many of the setup wizard pages. To set further options as you require or as seen in the learning link, cancel the setup wizard and go to the web-based configuration utility.

Click **Next** to continue

Buttons: Back, Next, Cancel

Renseignez une adresse IP statique pour la borne en 172.16.0.10/24 (passerelle par défaut 172.16.0.254) et l'IP du serveur DNS (172.16.0.1), puis cliquez sur « Next » :



Access Point Setup Wizard

Configure Device - IP Address

Select either Dynamic or Static IP address for your device.

☐ Dynamic IP Address (DHCP) (Recommended)

☒ Static IP Address

Static IP Address: 172 . 16 . 0 . 10

Subnet Mask: 255 . 255 . 255 . 0

Default Gateway: 172 . 16 . 0 . 254

DNS: 172 . 16 . 0 . 1

Secondary DNS (optional): 8 . 8 . 8 . 8

[? Learn more about the different connection types](#)

Click **Next** to continue

Buttons: Back, Next, Cancel

Référence :	ASSURMER Procédure AP 8	Document :	PROCEDURE AP 8
Responsables :	Ugo BERNARD Bruno LEVESQUE	Date :	08/01/2024

Ensuite il vous sera proposé de créer un « Cluster », sélectionnez « Do not Enable Single Point Setup » et cliquez sur « Next » :

Access Point Setup Wizard

Welcome

Configuration

- ✓ IP Address
- Single Point Setup**
- Time Settings
- Device Password

Radio 1 (5 GHz)

- Network Name
- Wireless Security
- VLAN ID

Radio 2 (2.4 GHz)

- Network Name

Single Point Setup -- Set A Cluster

A cluster provides a single point of administration and lets you view, deploy, configure, and secure the wireless network as a single entity, rather than separate wireless devices.

☐ Create a New Cluster
Recommended for a new deployment environment.

New Cluster Name:

AP Location:

Cluster Mgmt Address (optional):

☐ Join an Existing Cluster
Recommended for adding new wireless access points to the existing deployment environment.

Existing Cluster Name:

AP Location:

☒ Do not Enable Single Point Setup
Recommended for single device deployments or for configuring each device individually.

[Learn more about single point setup](#)

Click **Next** to continue

Back Next Cancel

Ensuite, définissez la « Time Zone : France », (vous avez la possibilité de renseigner un autre serveur NTP), cliquez sur « Next » :

Access Point Setup Wizard

Welcome

Configuration

- ✓ IP Address
- ✓ Single Point Setup
- Time Settings**
- Device Password

Radio 1 (5 GHz)

- Network Name
- Wireless Security
- VLAN ID

Radio 2 (2.4 GHz)

- Network Name

Configure Device - Set System Date And Time

Enter the time zone, date and time.

Time Zone:

(Gets The First Country Name from the Time Zone You Belong)

Set System Time: ☒ Network Time Protocol (NTP)
☐ Manually

NTP Server:

[Learn more about time settings](#)

Click **Next** to continue

Back Next Cancel

Référence :	ASSURMER Procédure AP 8	Document :	PROCEDURE AP 8
Responsables :	Ugo BERNARD Bruno LEVESQUE	Date :	08/01/2024

La prochaine étape sera de définir le mot de passe administrateur du point d'accès CISCO WAP371, définissez votre mot de passe et cochez la case « Password Complexity », cliquez sur « Next » :

Access Point Setup Wizard

Welcome

Configuration

- ✓ IP Address
- ✓ Single Point Setup
- ✓ Time Settings
- Device Password**

Radio 1 (5 GHz)

Network Name

Wireless Security

VLAN ID

Radio 2 (2.4 GHz)

Network Name

Configure Device - Set Password

The administrative password protects your access point from unauthorized access. For security reasons, you should change the access point password from its default settings. Please write this password down for future reference.

Enter a new device password:

New password needs at least 8 characters composed of lower and upper case letters as well as numbers/symbols by default.

New Password:

Confirm Password:

Password Strength Meter: Below Minimum

Password Complexity: ☒ Enable

[Learn more about passwords](#)

Click **Next** to continue

Back Next Cancel

Ensuite, vous avez la possibilité de configurer la radio 1 (avec une bande 5 GHz) offrant une portée plus courte permettant une meilleure qualité de connexion dans des environnements où les réseaux Wi-Fi sont nombreux et/ou la radio 2 (avec une bande 2.4 GHz) offrant une plus grande portée mais pouvant être sujette à des interférences provenant d'autres appareils.

Pour la radio 1 les étapes sont les mêmes : saisissez le nom du réseau (SSID) que vous souhaitez créer et cliquez sur « Next » :

Access Point Setup Wizard

Welcome

Configuration

- ✓ IP Address
- ✓ Single Point Setup
- ✓ Time Settings
- ✓ Device Password
- Radio 1 (5 GHz)**
- Network Name**
- Wireless Security
- VLAN ID
- Radio 2 (2.4 GHz)**
- Network Name

Configure Radio 1 - Name Your Wireless Network

The name of your wireless network, known as an SSID, identifies your network so that wireless devices can find it.

Enter a name for your wireless network:

Network Name (SSID):

For example: MyNetwork

[Learn more about network names](#)

Click **Next** to continue

Back Next Cancel

Référence :	ASSURMER Procédure AP 8	Document :	PROCEDURE AP 8
Responsables :	Ugo BERNARD Bruno LEVESQUE	Date :	08/01/2024

Ensuite, cochez la case « **Best Security (WPA2 Personal – AES)** » et renseignez un **mot de passe robuste**. Cliquez sur « **Next** » :

Access Point Setup Wizard

Welcome

Configuration

- ✓ IP Address
- ✓ Single Point Setup
- ✓ Time Settings
- ✓ Device Password

Radio 1 (5 GHz)

- ✓ Network Name

Wireless Security

VLAN ID

Radio 2 (2.4 GHz)

Network Name

Configure Radio 1 - Secure Your Wireless Network

Select your network security strength.

☒ **Best Security (WPA2 Personal - AES)**
Recommended for new wireless computers and devices that support this option. Older wireless devices might not support this option.

☐ Better Security (WPA/WPA2 Personal - TKIP/AES)
Recommended for older wireless computers and devices that might not support WPA2.

☐ No Security (Not recommended)

Enter a security key with 8-63 characters.

|||| Below Minimum

☒ Show Key as Clear Text

[? Learn more about your network security options](#)

Click **Next** to continue

Back Next Cancel

Dans le champ « **VLAN ID** », entrez l'ID correspondant au groupe d'utilisateurs (ex : 10 pour le Comité de Direction, 20 pour le Service Finance). Cela assurera une isolation logique et une gestion optimisée du trafic réseau. Cliquez sur « **Next** » :

Access Point Setup Wizard

Welcome

Configuration

- ✓ IP Address
- ✓ Single Point Setup
- ✓ Time Settings
- ✓ Device Password

Radio 1 (5 GHz)

- ✓ Network Name
- ✓ Wireless Security

VLAN ID

Radio 2 (2.4 GHz)

Network Name

Configure Radio 1 - Assign The VLAN ID For Your Wireless Network

By default, the VLAN ID assigned to the management interface for your access point is 1, which is also the default untagged VLAN ID. If the management VLAN ID is the same as the VLAN ID assigned to your wireless network, then the wireless clients associated with this specific wireless network can administer this device. If needed, an access control list (ACL) can be created to disable administration from wireless clients.

Enter a VLAN ID for your wireless network:

VLAN ID: (Range: 1 - 4094)

[? Learn more about vlan ids](#)

Click **Next** to continue

Back Next Cancel

La configuration de la radio 2 est exactement pareil que la radio 1, vous pouvez recommencer les étapes de la radio 1 pour configurer la radio 2.

Référence :	ASSURMER Procédure AP 8	Document :	PROCEDURE AP 8
Responsables :	Ugo BERNARD Bruno LEVESQUE	Date :	08/01/2024

Lors de la prochaine étape, le **portail captif** n'a pas été activé, car nous configurerons par la suite un **serveur RADIUS** pour l'authentification des utilisateurs. Cochez la case « No, thanks. » et cliquez sur « Next » :

Access Point Setup Wizard

Radio 2 (2.4 GHz)

- ✓ Network Name
- ✓ Wireless Security
- ✓ VLAN ID

Captive Portal

Creation

Do you want to create your guest network now?

☐ Yes

☒ No, thanks.

[? Learn more about captive portal guest networks](#)

Click **Next** to continue

Back Next Cancel

Sur cette dernière étape de l'assistant d'installation, vous pouvez voir un résumé des paramètres que vous avez configurés, cliquez sur « Submit » pour appliquer ces paramètres.

Access Point Setup Wizard

Summary - Confirm Your Settings

Please review the following settings and ensure the data is correct.

Radio 1 (5 GHz)

Network Name (SSID):	ASSUR_MGMT
Network Security Type:	WPA2 Personal - AES
Security Key:	test_1234
VLAN ID:	2

Radio 2 (2.4 GHz)

Network Name (SSID):	ASSUR_MGMT
Network Security Type:	WPA2 Personal - AES
Security Key:	test_1234
VLAN ID:	2

Summary

Click **Submit** to enable settings on your Cisco Systems, Inc Access Point

Back Submit Cancel

Référence :	ASSURMER Procédure AP 8	Document :	PROCEDURE AP 8
Responsables :	Ugo BERNARD Bruno LEVESQUE	Date :	08/01/2024

Un fois que vous aurez cliqué sur « Submit » le point d'accès réseau sans fil CISCO WAP371 va appliquer les paramètres et redémarrer par la suite. Une fois le redémarrage terminé connectez via l'adresse IP que vous lui avez attribué



Ensuite, renseignez dans de le champs nom d'utilisateur « cisco » avec le mot de passe que vous avez défini lors des étapes précédentes :



The image shows the login interface of a Cisco Wireless Access Point. It has a blue header with the Cisco logo and the text 'Wireless Access Point'. Below the header, there are two input fields: 'Username:' with the value 'cisco' and 'Password:'. A 'Log In' button is located below the password field. Red arrows from the text above point to these fields.

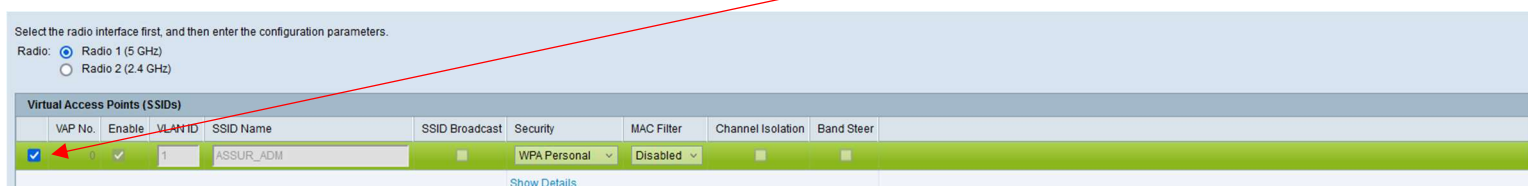
4. Configuration du WPA Enterprise

Le WPA Enterprise (Wi-Fi Protected Access - Enterprise) est un protocole de sécurité avancé qui utilise un serveur RADIUS pour authentifier les utilisateurs. Contrairement au WPA/WPA2 Personnel, qui repose sur un mot de passe partagé, le WPA Enterprise permet une authentification individuelle et sécurisée des utilisateurs via des identifiants uniques.

Une fois connecté à l'interface web du point d'accès sans-fil CISCO WAP371, rendez vous dans la section « Wireless » -> « Networks » :



Sélectionnez le réseau sur lequel vous souhaitez activer le WPA Enterprise (par défaut la page « Networks » vous affiche les réseaux de la « Radio 1 (5 GHz) », pour modifier ceux de la « Radio 2 (2.4 GHz) vous devrez cocher la case « Radio 2 (2.4 GHz) » et répéter les mêmes étapes que pour la « Radio 1 (5 GHz) »). Une fois le réseau sélectionné, cliquez sur « Edit » :



The image shows the 'Virtual Access Points (SSIDs)' configuration page. At the top, there's a section for selecting the radio interface: 'Radio 1 (5 GHz)' (selected) and 'Radio 2 (2.4 GHz)'. Below this is a table with columns: 'VAP No.', 'Enable', 'VLAN ID', 'SSID Name', 'SSID Broadcast', 'Security', 'MAC Filter', 'Channel Isolation', and 'Band Steer'. The first row is highlighted in green and shows '1' in the VAP No. column, 'ASSUR_ADM' in the SSID Name column, and 'WPA Personal' in the Security column. A red arrow points from the text above to the 'WPA Personal' dropdown menu.

Référence :	ASSURMER Procédure AP 8	Document :	PROCEDURE AP 8
Responsables :	Ugo BERNARD Bruno LEVESQUE	Date :	08/01/2024

Sur le réseau sélectionné, cliquez sur [« Show Details »](#) :

Virtual Access Points (SSIDs)									
	VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation	Band Steer
☒	0	☒	1	ASSUR_ADM	☐	WPA Personal	Disabled	☐	☐
Show Details									

Dans la rubrique [« Security »](#), sélectionnez [« WPA Enterprise »](#) :

WPA Enterprise

[Hide Details](#)

WPA Versions: ☐ WPA-TKIP ☒ WPA2-AES
☒ Enable pre-authentication

MFP: ☐ Not Required ☒ Capable ☐ Required

☒ Use global RADIUS server settings

Server IP Address Type: ☒ IPv4 ☐ IPv6

Server IP Address-1: (xxx.xxx.xxx.xxx)
 Server IP Address-2: (xxx.xxx.xxx.xxx)
 Server IP Address-3: (xxx.xxx.xxx.xxx)
 Server IP Address-4: (xxx.xxx.xxx.xxx)

Key-1: (Range: 1-64 Characters)
 Key-2: (Range: 1-64 Characters)
 Key-3: (Range: 1-64 Characters)
 Key-4: (Range: 1-64 Characters)

☐ Enable RADIUS Accounting

Active Server:

Broadcast Key Refresh Rate: Sec (Range: 0-86400, 0 = Disable, Default: 86400)
 Session Key Refresh Rate: Sec (Range: 30-86400, 0 = Disable, Default: 0)

Pour la suite de la configuration, merci de bien vouloir vous référer à la [procédure de configuration de RADIUS](#).