

# Procédure d'installation du WIFI via Radius

# Table des matières

Équipements utilisés	3
Réinitialisation des paramètres d'usine	3
Configuration de la borne WI-FI	4
Création des différents points d'accès WI-FI	7
Installation du service radius sur le serveur AD	8
Configuration de radius pour une borne WI-FI	9
Installation d'une Autorité de certification	12
Configuration d'une Autorité de certification	13
Sélection du certificat autosigné sur la console NPS	15



## Équipements utilisés

-WAP371 -Cable RJ45 -Ordinateur portable -Un serveur AD, DHCP, DNS préconfigurer -Un switch

#### Réinitialisation des paramètres d'usine

1. Appuyer sur le bouton de réinitialisation situé au fond du périphérique pendant approximativement dix secondes avec une broche.



Les recharges de Point d'accès sont placées en configuration par défaut.

2. Lancez un navigateur Web, tel que Internet Explorer ou Mozilla Firefox. Tapez l'adresse IP statique par défaut 192.168.1.245 dans la barre URL et appuyez sur la touche Entrer. Pour atteindre cette adresse IP, soyez sûr que votre ordinateur est sur le réseau 192.168.1.xxx.

3. Procédure de connexion avec les qualifications par défaut. Le nom d'utilisateur par défaut est Cisco, et le mot de passe par défaut est Cisco.





## Configuration de la borne WI-FI

4. Une fois installée, connectez-vous et cliquez sur Configure LAN Settings

cisco WAP121	Wireless-N Access Point with Single Point	Setup	
Getting Staried Run Setup Wizard Status and Statistics	Getting Started		
Administration     LAN	Use the following links to quickly configure your access point.		
Wireless     System Security     Client QoS     SNMP     Single Point Setup	<ul> <li>Initial Setup</li> <li>Run Setup Wizard</li> <li>Configure Radio Settings</li> <li>Configure Wireless Network</li> <li>ettings</li> <li>Configure LAN Settings</li> <li>Run WPS</li> <li>Configure Single Point Setup</li> <li>Device Status</li> </ul>	Quick Access Change Account Password Upgrade Device Firmware BackupiRestore Configuration	
	System Summary Wireless Status		

5. Configurer l'IPv4 statique de la borne, le masque, la passerelle, le DNS de votre réseau et éventuellement indiqué lui VLAN si votre switch et configuré avec des vlans

cisco WAP121 V	Vireless-N Acce	ss P	oint v	vith S	ingle	(clacco) Log Out About Help
Getting Started						
Run Setup Wizard	VLAN and IPV4 A	adres	SS			
<ul> <li>Status and Statistics</li> </ul>	Global Settings					
Administration     LAN	MAC Address:	04:62:7	'3:36:5A:1	0		
Port Settings VLAN and IPv4 Address	Untagged VLAN:	Er	nable			
IPv6 Addresses	Untagged VLAN ID:	1		(	Range: 1 -	4094, Default 1)
<ul> <li>Wireless</li> </ul>	Management VLAN ID:	1			Range: 1 -	4094 Default 1)
System Security		1.				The second of the second se
Client QoS     SNMP	IPv4 Settings					
Single Point Setup	Connection Type:	O DH	ICP atic IP			
	Static IP Address:	192	. 168	. 1	. 250	
	Subnet Mask	255	. 255	. 255	. 0	
	Default Gateway:	192	. 168	. 1	. 254	
	Domain Name Servers:	O Dyr Ma	namic inual			
		192	. 168	. 1	. 70	
		8	. 8	. 8	. 8	
	Save					

6. Après cela, retournez à l'accueil et cliquez sur Configure Radio Setting. Activez l'option Radio, nous laisserons les paramètres par défaut, mais nous serons amenés à les modifier plus tard pour des questions d'optimisation selon l'environnement de la borne WI-FI.







7. Retournez au menu et cliquez maintenant sur Configure Wireless Network Settings

Netw	Networks									
Select Radio	the radio in () Rad () Rad	nterface fir dio 1 (5 GH dio 2 (2.4 (	rst, and ther Hz) GHz)	n enter the configuration para	meters.					
Virt	Virtual Access Points (SSIDs)									
	VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter			
	0		110	invité-yohan		WPA Personal 🗸	Disabled 🗸			
						Show Details				
	1		103	administration-yohan		None v	Disabled 🗸			
	2		100	administration-marin		None v	Disabled 🗸			
	3		30	invité-marin		WPA Personal 🗸	Disabled 🗸			
						Show Details				
	Add	Edit	De	lete						
Sa	/e									



### Création des différents points d'accès WI-FI

- 11. Cliquez sur le point d'accès par défaut puis sur Edit
- 12. Indiquez le vlan à utiliser si c'est le cas donner un SSID au point d'accès, laissez cocher le SSID Broadcast. Enfin, pour le premier point d'accès on utilise la sécurité WPA Personal. Ensuite nous définissons la clé puis on sauvegarde.

ect	the radio in	nterface fir	st, and the	n enter the configuration	parameters.				
dia	Rad	10 1 (5 GH	(Z)						
	0 1.00	10 2 (2.4 0							
Virt	ual Access	Points (S	SIDs)						
	VAP No.	Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation	Band Steer
~			110	invité-yohan		WPA Personal 🗸	Disabled 🛩		
			-			Hide Details			
						WPA Versions:	WPA-TKIP	WPA2-AES	
						Key:		(Range: 8-63 Characters)	
							Show Key as C	lear Text	
						Key Strength Meter:	1111	Below Minimum	
						Broadcast Key Refresh Rate	86400	Sec (Range: 0-86400, 0 = Dis	sable, Default 8640
						MEP	Not Required	Capable Capable	

13.Votre premier point d'accès WI-FI est fonctionnel. Il vous suffit de vous connecter à l'aide de la clé pour créer celui-ci.

14.Nous allons créer un point d'accès WI-FI d'entreprise

15.On add puis on edit

16. Indiquer le vlan à utiliser si c'est le cas donner un SSID au point d'accès, laissez cocher le SSID Broadcast. Enfin, pour le premier point d'accès on utilise la sécurité WPA Entreprise. Ensuite nous définissons l'adresse IP ou point nos service AD, DHCP ... éventuellement sa réplication et une clé puis on sauvegarde.

-	4 192	102	administration voltan		WPA Enterprise M	Disabled at	
a	<b>M</b>	103	administration-yonan	<u></u>	WPA Enterprise *	Disabled +	
					Hide Details		
					WPA Versions: 🗹 WPA	TKIP 🗾 W	IPA2-AES
					Use global RADIUS s	erver settings	
					Server IP Address Type:	● IPv4 ○ IPv6	
					Server IP Address-1:	172.16.0.1	(1000.1000.1004)
					Server IP Address-2:		(100.305.303.303)
					Server IP Address-3:		(000-000-000()
					Server IP Address-4:		(1001.3001.3001.3001)
					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 Acco	unting	
					Active Server:	Server IP Address-	-1 v
					Broadcast Key Refresh R	ate: 86400	Sec (Range: 0-86400, 0 = Disable, Default: 86400)
					Session Key Refresh Rat	e: 0	ALT Range Vola6490/0= Disable, Default 0)

Le point d'accès sera alors visible, mais il ne sera pas possible de la rejoindre nous devons effectuer une manipulation sur le serveur AD. Il pourra ensuite se connecter avec ses identifiants d'entreprise sur la borne WI-Fi



#### Installation du service radius sur le serveur AD



- 21. Sur le serveur Windows 2019, allez dans le gestionnaire de serveur, cliquez sur « Gérer » puis « Ajouter des rôles et fonctionnalités ».
- 22. Sélectionner le rôle services de stratégie et d'accès réseau et ajouter des fonctionnalités







## Configuration de radius pour une borne WI-FI

	Serveur N	PS (I
Fichier Ac	tion Affichage ?	
● NPS (I J Cli	Importer la configuration Exporter la configuration	7
⊿ Str	Démarrer le service NPS Arrêter le service NPS Inscrire un serveur dans Active Directory	k st
Þ 🍢 Pri	Propriétés	
📲 Ge Þ 🛃 Ge	Anichage	-

24.Lancez le service et faites un clic droit sur NPS

25.Inscrivez le serveur dans l'Active directory sinon il sera impossible de définir les conditions liées aux groupes/utilisateurs dans la stratégie d'accès distant

26.Créez un nouveau client radius sur la console NPS, clic droit nouveau Nom de la borne : wap121 adresse de la borne : 192.168.1.250 secret : Que vous avez défini sur la borne en amont

🚳 NPS (Local)	Clients RADIUS	
Clients et serveurs RADIUS Clients RADIUS	Les clients RADIUS vous permettent de spécifier les serveurs d'accès réseau qui fournissent l'accès à votre rése	cau.
<ul> <li>Stratégies</li> <li>Stratégies de demande de connexion</li> </ul>	Nom convivial Adresse IP Fabricant du périphérique Compatible avec la protection d'accès réseau (NAP) E	Élat
Stratégies réseau Stratégies de contrôle d'intégrité		
Protection d'accès réseau Gestion	Propriétés de wap41e9c0	
Gestion des modèles	Paramètres Avancé	
	Activer ce client RADIUS	
	Sélectionner un modèle existant :	
	APWap307	
	Nom et adresse	
	wap41e9c0	
	Adresse (IP ou DNS) :	
	192.168.90.39 Véntier	
	Secret partagé	
	Sélectionnez un modèle de secrets partagés existant :	
	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 :	
	Confirmer le servet nartané :	
	OK Annuler Appliquer	
27. Configuration de la straté	gie réseau nouvelle stratégie réseau – nom de la stratég	ie : Wifi



Interes et serveurs nabius     Interes et serveurs nabius	Nouvelle stratégie réseau
Stratégies de demande de connexion Stratégies réseau Stratégies de controle d'intégrité Mortection d'accès réseau Stratégies de validation d'intégrité Groupes de serveux de muse à lour	Spécifier le nom de la stratégie réseau et le type de connexion Vous pouvez spécifier le nom de votre stratégie réseau ainsi que le type des connexions auxquelles la stratégie s'applique.
N Gestion	Nom de la stratégie :
4 📕 Gestion des modèles	WH
Cestion des modeles     Sector partagés     Clents RADIUS     Serveurs RADIUS distants     Filmers IP     Statégies de contrôle d'intégrité     Groupes de serveurs de mise à jour	Méthode de connexion réaseu         Sélectionnes le type de serveur d'accès réseau qui envoie la demande de connexion au serveur NPS. Vous pouves sélectionner une vaieur d'ans type de serveur d'accès réseau qui envoir Solicitue au fourniseur, mais ces paremittes ne tont pas obligatione. Si votre serveur d'accès réseau est un commutateur d'authentification ou un point d'accès serveur d'accès réseau :         Image: d'accès réseau est un commutateur d'authentification ou un point d'accès serveur d'accès réseau :         Non spécifié.         Vis spécifique au fournisseur :         Image: de serveur d'accès réseau :
	Pröckdert Suivant Temmer Annuker

28. Nous ajouterons le Groupe utilisateurs du domaine

			Propriétés de Wifi_Cisco
/ue d'ensemble	Conditions	Contraintes	Paramètres
Configurez les c Si la demande d demande de coi stratégies supplé	onditions de le connexion nnexion ne ré émentaires se	cette stratégie répond aux co épond pas aux eraient configu	réseau. onditions, le serveur NPS utilise cette stratégie pour autoriser la demande de connexion. Si la conditions, le serveur NPS ignore cette stratégie et en évalue d'autres, dans l'hypothèse où des rées.
Condition		Valeur	
🚜 Groupes d	l'utilisateurs	AIS\Utili:	sateurs du domaine
Description de la La condition Gro	a condition : pupes d'utilisi	steurs spécifie	que l'utilisateur qui tente d'établir la connexion doit appartenir à l'un des groupes sélectionnés.
			Ajouter Modifier Supprimer

- 29. Sélectionnez MS-CHAP v2 et MS-CHAP pour authentification par mot de passe.
- 30. Montez Le protocole Extended Authentication Protocol. Il sert pour le transport des données nécessaire à l'authentification.



Configurez les ci Si la demande d	ontraintes de	cette stratégie	e réseau. s à toutes les c	intraintes l'accès réseau est	refusé				
Contraintes :									
Contraintes			Autorisez	accès uniquement aux client	s qui s'authentifient à l'aide	des méthodes			
A Méthodes			spécifiées						
📆 Délai d'in	activité		Les types l'ordre dar	le protocoles EAP sont négo s lequel ils sont listés.	ciés entre le serveur NPS et	t le client dans			
Bélai d'es	xpiration de		Types de	rotocoles EAP :					
ID de la s	tation annel	60	Microso	PEAP (Protected EAP)		Monter			
Restriction	ons relatives	aux		54771		Descendre			
Type de port NAS	port NAS           Ajouter         Modfiler         Supprimer								
			Auther	d authentification moins secu ification chiffrée Microsoft w	msees : antion 2 (MS-CHAP v2)				
			✓ L'u	lisateur peut modifier le mot o	le passe après son expiration	n			
			Authentification chiffrée Microsoft (MS-CHAP)						
			✓ L'u	lisateur peut modifier le mot o	le passe après son expiration	n			
			Auther	tification chiffrée (CHAP)					
			Auther	tification non chiffrée (PAP, S	SPAP)				
			Autoris	er les clients à se connecter :	sans négocier une méthode	d'authentification			
			Ventier	uniquement l'integrite de l'ori	dinateur				

31. Type de port NAS - dans rubrique 801.1X , sélectionnez Sans fil – IEEE 802.11 si ce n'est pas un accès sans fil, la demande de connexion est rejetée.

		Nouvelle stratégie réseau X
Configurez les	Configurer Les contraintes so doivent se confor Server) rejette aut configurer de contr contraintes de cette s	des contraintes nt des paramètres supplémentaires de la stratégie réseau, auxquels les demandes de connexion mer. Si une demande de connexion ne répond pas à une contrainte, le serveur NPS (Network Policy omatiquement cette demande. Les contraintes sont facultatives ; si vous ne souhaitez pas raintes, cliquez sur Suivant. tratégie réseau.
Si la demande Contraintes Contraintes Délai d'i Session D de la appelée Restrict aux jour heures Type de	de connexion ne répr : inactivité expiration de station ions relatives s et aux : port NAS	and pas à toutes les contraintes, l'accès réseau est refusé.         Spécifier les types de médias d'accès nécessaires pour correspondre à cette stratégie         Types de tunnels pour connexions d'accès à distance et VPN standard         Asynchrone (Modem)         Synchrone (Modem)         Synchrone (Igne T1)         Virtuel (VPN)         Types de tunnels pour connexions 802.1X standard         Ethemet         FDDI         Sans fit - IEEE 802.11         Token Ring         Autres         ADSL-CAP - Modulation de phase d'amplitude sans porteuse DSL asymétrique         ApsL-DMT - Multi-tonalité discrète DSL asymétrique         ApsL-DMT - Multi-tonalité discrète VSL asymétrique         ApsL-DMT - Multi-tonalité discrète DSL asymétrique
		Précédent Suivant Teminer Annuler



## Installation d'une Autorité de certification

#### 32. Installez les rôles adcs et outil de gestion. Suivant<suivant<installer

Sélectionner des	rôles de serveurs	SERVEUR DE DESTINATION SRV-AD.guilet.fr
Avant de commencer Type d'installation	Sélectionnez un ou plusieurs rôles à installer sur le serveur sélec Rôles	tionné. Description
Sélection du serveur Rôles de serveurs Fonctionnalités Confirmation Résultats	Accès à distance Attestation d'intégrité de l'appareil Contrôleur de réseau Hyper-V Serveur de télécopie Serveur DHCP (Installé) Serveur DNS (Installé) Service Guardian hôte Services AD DS (Installé) Services AD DS (Installé) Services AD DS (Installé) Services AD DS (Installé) Services AD RMS (Active Directory Lightweight Dire Services d'activation en volume Services d'activation en volume Services de fédération Active Directory (1 sur 6 inst Services de fichiers et de stockage (2 sur 12 installé) Services de stratégie et d'accès réseau (Installé)	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 réceau



### Configuration d'une Autorité de certification



33.Démarrez le gestionnaire de serveur, et cliquez sur l'icône drapeau en haut à droite pour démarrer la configuration.

34. Sur la page Services de rôle, sélectionnez Autorité de certification et cliquez sur Suivant.

• Sur la page Type d'installation, sélectionnez Autorité de certification d'entreprise et cliquez sur Suivant.

• Sur la page Type d'autorité de certification, sélectionnez Autorité de certification racine Sur la page Clé privée, sélectionnez Créer une nouvelle clé privée et cliquez sur Suivant.

• Sur la page Chiffrement, entrez les informations comme suit. (Recommandation NIST et globalsign : longueur de clé minimal 2048 et algorithme SHA256)

Chiffrement pour	l'autorité de certification	SRV2012.ais.loc	
Informations d'identificati	Spécifier les options de chiffrement		
Services de rôle		<b>C</b>	
Type d'installation	Sélectionnez un fournisseur de chiffrement :	Longueur de la clé :	
Type d'AC	RSA#Microsoft Software Key Storage Provider	* 2048 (1)	
Cié privée	Sélectionnez l'algorithme de hachage pour signer les certifi	cats émis par cette AC :	
Chiffrement	SHA256	^	
Nom de l'AC	SHA384	=	
Période de validité	SHA512	100	
Base de données de certi	SHA1	~	
Confirmation Progression Résultats	Autorisez l'interaction de l'administrateur lorsque l'autorité de certification accède à la clé privée.		
	En savoir plus sur le chiffrement		

- 35. Sur la page Nom de l'autorité de certification, acceptez les valeurs par défaut et cliquez sur Suivant.
- 36. Donnez un nom au certificat



Nom de l'autorité	de certification	SRV2012.ais.loci
Informations d'Identificati	Spécifier le nom de l'AC	
Services de rôle		
Type d'installation	Tapez un nom commun pour identifier cette autorité de cert	tification. Ce nom est ajouté à tous les
Type d'AC	certificats émis par l'autorité de certification. Les valeurs des automatiquement mais elles sont modifiables.	suffixes du nom unique sont générée
Clé privée	Construction of the second	
Chiffrement	Nom commun de cette AC :	
Nom de l'AC	ais-SRV2012-CA	
Période de validité	Suffixe du nom unique :	
Base de données de certi	DC=ais,DC=local	
Confirmation	Aperçu du nom unique :	
	CN=ais-SRV2012-CA,DC=ais,DC=local	
	En savoir plus sur le nom de l'autorité de certification	

- 37. Sur la page Période de validité, par défaut la valeur est de 5 années, cliquez sur Suivant.
- 38.
- Sur la page Base de données de certificats, cliquez sur Suivant.
- 39. Sur la page Confirmation, passez en revue les informations fournies et cliquez sur Configurer.



## Sélection du certificat autosigné sur la console NPS

- 40. Console NPS stratégie d'accès réseau propriétés de la stratégie wifi onglet contraintes
- 41. Sélectionnez Microsoft PEAP, puis Modifier afin de sélectionner le certificat serveur autosigné.
- 42. Cliquez sur OK pour valider

Vue d'ensemble Conditions Contrarites Paramètres	<u></u>	[ficats délivrés]	-
Configurez les contraintes de cette stratégie réseau. à la demande de connexion ne répond pas à toutes les contraintes, l'accès réseau est refusé. Contraintes Contraintes Méthodes d'authentification Delsis dinactivité Delsis dinactivité Delsis dinactivité Delsis dinactivité Delsis dinactivité Delsis dinactivité Descrictions relatives aux jours et aux heures Type de port NAS Monter Mader 2 Supprimer Méthodes d'authentification Mader 2 Supprimer Méthodes d'authentification Méthodes d'authentification monts sécurisées i Autorisées in autheures Autorisées montéries Monsoft version 2 (MS CHAP v2) Cutilisateur peut modifier le mot de passe après son expiration Authentification chiffrée (DrAP)	5 t	Ificats délivinés]         Modifier les propriétés EAP Protégé         Sélectionnez le certificat que le serveur doit utiliser comme preuve de son identité auprès du clent. Un certificat configuré pour EAP Protégé dans la stratégie de demande de comexion resplacers oc control.         Certificat déliviné à :       [SRV2012.ais.local         Mon convivial :       SRV2012.ais.local         Émetteur :       ais-SRV2012.cA         Date d'expiration :       15/01/2021 15:57:56         Activer la reconnexion rapde Déconnecter les clents sens chiffrement forcé Types EAP       Monifer         Modifier       Suprimer       OK         Ajouter       Modifier       Suprimer	

