	HUYNH Michael
Procédure Configuration WIFI + RADIUS	SAKO Bah
	FRANCAIS
	Benjamin
ASSURMER	28 SISP
	2D-01013
Procédure configuration	
Wifi & Radius	

ASSURMER

Version	Auteur	Date	Nombre de pages	À l'attention	Mode de diffusio n	Validateur
1.0	FRANCAIS Benjamin ; SAKO BAH ;HUYNH Michael	31/01/2025	29	Assurmer-IT	.pdf	FRANÇAIS Benjamin

Sommaire

PREREQUIS :	2
INSTALLATION « NETWORK POLICY SERVER » :	3
Liaison NPS et AD :	6
CONFIGURATION RADIUS :	8
Liaison Borne WiFi et AD :	8
CONFIGURATION « AD CERTIFICATE SERVICES »	15
CONFIGURATION 802.1X :	23
CONFIGURATION BORNE WIFI POUR RADIUS :	27

Prérequis :

- 1 serveur AD; 1 Borne Wifi
- Compte Administrateur

Installation « Network Policy Server » :

• Cliquer sur « Add Roles and Features Wizard » dans le « Server Manager » puis sélectionner « Role-based or feature-based installation »

		- 0	
Select installation	type	DESTINATION SER SRV-ADDC01.assurme	VEF er.IT
Before You Begin	Select the installation type. You can install roles and features on a running physica machine, or on an offline virtual hard disk (VHD).	I computer or virt	ua
Server Selection	Role-based or feature-based installation Configure a single server by adding roles, role services, and features.	1 .	
Features Confirmation Results	 Remote Desktop Services installation Install required role services for Virtual Desktop Infrastructure (VDI) to create a or session-based desktop deployment. 	virtual machine-b	ase
	2. < Previous Next > Inst	tall Cance	el
Sélectionner le	e serveur concerné		
Add Roles and Features Wizard		- 0	
Add Roles and Features Wizard	server	DESTINATION SER	VE er.l
Add Roles and Features Wizard Select destination Before You Begin	Server Select a server or a virtual hard disk on which to install roles and features.	DESTINATION SER	VE er.l
Add Roles and Features Wizard Select destination Before You Begin Installation Type Server Selection	Select a server or a virtual hard disk on which to install roles and features. Select a server from the server pool Select a virtual hard disk	DESTINATION SER	IVE er.l
Add Roles and Features Wizard Select destination Before You Begin Installation Type Server Selection Server Roles	Server Select a server or a virtual hard disk on which to install roles and features. Select a server from the server pool Select a virtual hard disk Server Pool	DESTINATION SER	IVE er.l
Add Roles and Features Wizard Select destination Before You Begin Installation Type Server Selection Server Roles Features	Server Select a server or a virtual hard disk on which to install roles and features. Select a server from the server pool Select a virtual hard disk Server Pool Filter:	DESTINATION SER SRV-ADDC01.assurm	(VE)
Add Roles and Features Wizard Select destination Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	Select a server or a virtual hard disk on which to install roles and features. Select a server from the server pool Select a virtual hard disk Server Pool Filter: Name IP Address Operating System	DESTINATION SER SRV-ADDC01.assurm	(VE)
Add Roles and Features Wizard Select destination Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	Select a server or a virtual hard disk on which to install roles and features. Select a server from the server pool Select a virtual hard disk Server Pool Filter: Name IP Address Operating System SRV-ADDC01.assurmer.IT 172.16.0.1 Microsoft Windows Server 2022 S	DESTINATION SER SRV-ADDC01.assurm	er.l
Add Roles and Features Wizard Select destination Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	Select a server or a virtual hard disk on which to install roles and features. Select a server from the server pool Select a virtual hard disk Server Pool Filter: Name IP Address Operating System SRV-ADDC01.assurmer.IT 172.16.0.1 Microsoft Windows Server 2022 S	DESTINATION SER SRV-ADDC01.assurm	tver.i
Add Roles and Features Wizard Select destination Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	Select a server or a virtual hard disk on which to install roles and features. Select a server from the server pool Select a virtual hard disk Server Pool Filter: Name IP Address Operating System SRV-ADDC01.assurmer.IT 172.16.0.1 Microsoft Windows Server 2022 S 1 Computer(s) found	DESTINATION SER SRV-ADDC01.assurm Standard Evaluatio	on
Add Roles and Features Wizard Select destination Before You Begin Installation Type Server Selection Server Roles Features Confirmation Results	Select a server or a virtual hard disk on which to install roles and features. Select a server from the server pool Select a virtual hard disk Server Pool Filter: Name IP Address Operating System SRV-ADDC01.assurmer.IT 172.16.0.1 Microsoft Windows Server 2022 Server 2022 Server 2022 Server 2012 or a newer release and that have been added by using the Add Servers command in Server Manager newly-added servers from which data collection is still incomplete are not shown.	DESTINATION SER SRV-ADDC01.assurm Standard Evaluatio standard Evaluatio of Windows Serv . Offline servers an	on ver,

Sélectionner « Network Policy and Access Services »



< Previous

Next >

Install

Cancel

Cliquer sur « Next »



Liaison NPS et AD :

• Sur le « Server Manager », aller dans « NPAS » et faire un clic-droit sur le serveur. Puis sélectionner « Network Policy Server »

Dashboard	SERVERS All servers 1 t	otal				TASKS
Local Server All Servers	Filter	• (ii) • (ii)				۲
AD DS	Server Name IPv4 /	Address Manageability	Last Update	Windows Activation		
DNS File and Storage Services IS NPAS Remote Desktop Services	SRV-ADDC01 172.1	601 Ohlines Performance counters and Add Roles and Features Shut Down Local Server Computer Management Remote Desktop Connection Windows PowerShell Configure MC Teaming	started 28/01/2025 16:42	203 00454-40000-00001-AA15	(Activated)	
	· · · · ·	Network Policy Server	2.			
	EVENTS All events 1 total	Manage As Start Performance Counters Refresh				TASKS
	Filter	Сору	•			۲
	Server Name ID SRV-ADDC01 4421	Severity Source Log Date and Time Warning NPS System 28/01/2025 16	-40:46			



• Cliquer sur « OK »

Network Policy Server		×
To enable NPS to authenticate computers running NPS must properties from the domain.	e users in the Active Dir be authorized to read	ectory, the users' dial-in
Do you wish to authorize this properties from the assurmer.	computer to read user IT domain?	s' dial-in
	N OK	Cancel

Configuration RADIUS :

Liaison Borne WiFi et AD :

• Récupérer le « Host name » de la borne sur l'interface en ligne de la borne :

← → C 😣 Non se	→ C Non sécurisé https://172.16.0.10/admin.cgi?action=main							
UIUU WAP371 Wireless-AC/N Dual Radio Access Point with Single Point Setup								
Getting Started Run Setup Wizard	System Settings							
Status and Statistics Administration	Host Name: wap255450 (Range: 1-63 Characters)							
System Settings User Accounts	System Contact : (Range: 0-255 Characters)							
Time Settings Log Settings Email Alert LED Display	System Location: (Range: 0-255 Characters)							

• Retourner sur NPS et clic-droit sur « RADIUS CLIENTS » et « New »



• Rentrer les informations relatives à la borne Wifi

Self Fuel	Advanced		
1.7	Advanced		
Enab	le this RADIUS	client	
Sele	ct an existing te	emplate:	
Name	and Address		
Friend	y name:		
wap2	55450		
Addres	(IP or DNS)		
172 1	6.0.10		Verify
	0.0.10		(Comp
Shared	Secret		
Select	an existing Sha	ared Secrets template:	
None			
None To ma secret secret	nually type a sh , click Generate entered here. S nual d secret;	ared secret, click Manual. To - You must configure the RAD Shared secrets are case-sensiti O Generate	automatically generate a sha NUS client with the same sha ive.
None To ma secret secret Shared	nually type a sh , dick Generate entered here. S nual d secret:	ared secret, click Manual. To 2. You must configure the RAD Shared secrets are case-sensiti O Generate	automatically generate a sha NUS client with the same sha ive.
None To ma secret secret Shared Confirm	nually type a sh click Generate entered here. S nual d secret:	ared secret, click Manual. To . You must configure the RAD Shared secrets are case-sensiti Generate	automatically generate a sha IUS client with the same sha ive.
None To ma secret secret Shared	nually type a sh click Generate entered here. S nual d secret: n shared secret	ared secret, click Manual. To . You must configure the RAD Shared secrets are case-sensiti Generate :	automatically generate a sha IUS client with the same sha ive.

• Développer Policies puis clic-droit sur « Network Policies » et « New »

Network	Policy Server				5 .	- 🗆	×
File Action	View Help						
🗢 🔿 🖄							
🛞 NPS (Loca	sl)	Network Policies					
RADIU	IS Clients and Servers DIUS Clients mote RADIUS Server	Network pol under which	icies allow you to designate who is authorized they can or cannot connect.	to connect	to the network and t	he circumstanc	es
	nnection Request Po	Policy Name		Status	Processing Order	Access Type	S
	New.	Connections to M	icrosoft Routing and Remote Access server	Enabled	999998	Deny Access	U
Acc	Expolt	Connections to other access servers Enabled 999999			999999	Deny Access	U
	View	>					
	Refresh						
	Help	Conditions - If the f	ollowing conditions are met:				
		Condition	Value				
		Settings - Then the	following settings are applied: Value				
<	>	<					>
New		,					

• Nommer la politique en « SSID »

You can	ty Network Policy		
You can		Name and Connection Type	
	specify a name for your netwo	rk policy and the type of connections to which the policy is app	plied.
olicy name:			
SSID			
etwork connection meth	hord		
elect the type of networ	k access server that sends the c	connection request to NPS. You can select either the network acce	ess server
elect Unspecified.	ut neitner is required. If your net	work access server is an 802. IX authenticating switch or wireless a	access point,
Type of network acce	ss server		
Unspecified		~	
Vendor specific:			
10			
		Previous Next. Finish	Cancel
Cliquer su	ur « Add »		
Spacif	fy Conditions		
Specify the	ne conditions that determine w	whether this network policy is evaluated for a connection rec	quest. A mini
Specify th of one co	e conditions that determine ndition is required.	whether this network policy is evaluated for a connection rec	quest. A mini
Specify th of one co	e conditions that determine ndition is required.	whether this network policy is evaluated for a connection rec	quest. A mini
Additions:	e conditions that determine of ndition is required.	whether this network policy is evaluated for a connection rec	quest. A mini
nditions:	e conditions that determine of a second seco	whether this network policy is evaluated for a connection rec	quest. A mini
Additions:	ve conditions that determine of a second sec	whether this network policy is evaluated for a connection rec	quest. A mini
Additions:	value	whether this network policy is evaluated for a connection rec	quest. A mini
Additions:	value	whether this network policy is evaluated for a connection rec	quest. A mini
Additions:	value	whether this network policy is evaluated for a connection rec	quest. A mini
Additions:	Value	whether this network policy is evaluated for a connection rec	quest. A mini
Additions:	Value	whether this network policy is evaluated for a connection rec	quest. A mini
Additions:	Value	whether this network policy is evaluated for a connection rec	quest. A mini
Additions: Condition	ve conditions that determine of a second sec	whether this network policy is evaluated for a connection rec	quest. A mini
Additions: Condition	ve conditions that determine of a second sec	whether this network policy is evaluated for a connection rec	quest. A mini
dition description:	ve conditions that determine of ndition is required.	whether this network policy is evaluated for a connection rec	quest. A mini
Addition description:	value	whether this network policy is evaluated for a connection rec	quest. A mini
Addition description:	value	whether this network policy is evaluated for a connection rec	quest. A mini
Addition description:	Value	whether this network policy is evaluated for a connection rec	quest. A mini
Addition description:	Value	whether this network policy is evaluated for a connection rec	quest. A mini
dition description:	Value	whether this network policy is evaluated for a connection rec	quest. A mini
dition description:	Value	whether this network policy is evaluated for a connection rec	quest. A mini
dition description:	ve conditions that determine of ndition is required.	whether this network policy is evaluated for a connection rec	quest. A mini

• Choisir « User Groups »

Select condition				×		
Select a condition, and then click Add.						
Groups				^		
Windows Groups The Windows Groups condition specifies that the connect groups.	ing user or compu	iter must belong t	o one of the sele	cted		
Machine Groups The Machine Groups condition specifies that the connecting computer must belong to one of the selected groups.						
User Groups The User Groups condition specifies that the connecting us	User Groups The User Groups condition specifies that the connecting user must belong to one of the selected groups.					
Day and time restrictions						
Day and Time Restrictions Day and Time Restrictions specify the days and times wh restrictions are based on the time zone where the NPS set	en connection atte rver is located.	empts are and are	not allowed. Th	ese		
Connection Properties				~		
			Add	Cancel		
		Add	Edit	Remove		
	\square					
	Previous	Next	Finish	Cancel		

• On rajoute le groupe de sécurité « Domain User »

Select Group	×
Select this object type:	
Group	Object Types
From this location:	
assumer.IT	Locations
Enter the object name to select (example	es):
20main Osers	Check Names
Advanced	OH Cancel

• Cliquer sur « OK »

 ain Users	

• Cliquer sur « Next »

New	Network	Policy						×
		Specify of one condit	Conditions onditions that deta ion is required.	ermine whether th	is network pol	cy is evaluated for a	connection re	quest. A minimum
Con	ditions: Condition	1	Value					
2	User Gro	ups	ASSURMER	Iomain Users				
Conc	dition desc User Grou	ription: ps condition spe	acifies that the conn	necting user must b	elong to one of	the selected groups.	Edit	Remove
					Previous	Next	Rnish	Cancel

• Sélectionner « Access granted » puis « Next »

New Network	Policy	×
	Specify Access Permission	
R	Configure whether you want to grant network access or deny network access if the policy.	connection request matches this
Access gra Grant acce	anted	
O Access de	enied	
Deny acce	ess if client connection attempts match the conditions of this policy.	
Grant or de	eny access according to user dial-in properties if client connection attempts match the condit	ions of this policy.
	Previous Next	Finish Cancel

• Cliquer « Next »

ew Network Policy

	_			
41			Δ.	
		_		_

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.

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

	Move Up	
	Move Down	
Add Edit. Remove		
ess secure authentication methods:		
/ Microsoft Encounted Authentication Version / (MSJ HAP-V/)		
User can change password after it has expired		
User can change password after it has expired Microsoft Encrypted Authentication (MS-CHAP) User can change password after it has expired Encrypted authentication (CHAP)		
Inclusion Encrypted Automatication Version 2 (indication Version 2 (indication Version Versio Version Version Version Ver	G	
Indecision Electric devices relation relation version 2 (indication v2) User can change password after it has expired Incrosoft Encrypted Authentication (MS-CHAP) User can change password after it has expired Encrypted authentication (CHAP) Unencrypted authentication (CHAP) Unencrypted authentication (PAP, SPAP) Allow clients to connect without negotiating an authentication	method.	

×

• Cliquer « Finish »

ten network roney	×
Complet	ing New Network Policy
You have successfully created SSID	the following network policy:
Policy conditions:	
User Groups ASSURMER\D	Iomain Users
Condition	Value
Authentication Method	MS-CHAP v1 OR MS-CHAP v1 (User can change password after it has expired) OR MS-CHAP v2
Access Permission	Grant Access
Framed-Protocol Service-Type	PPP Framed

Configuration « AD Certificate Services »

• Sélectionner « Active Directory Certificate Services » puis « Add Features »



• Cliquer « Install »

ᡖ Add Roles and Features Wizi	ard	-		×
Confirm installa	tion selections	DESTIN SRV-ADDC	ATION SER	VER Br.IT
Before You Begin Installation Type Server Selection Server Roles	To install the following roles, role services, or features on selected server, click li Restart the destination server automatically if required Optional features (such as administration tools) might be displayed on this pag been selected automatically. If you do not want to install these optional feature their check boxes.	nstall. e because t is, click Prev	hey have vious to cl	lear
Features AD CS Role Services Confirmation Results	Active Directory Certificate Services Certification Authority Remote Server Administration Tools Role Administration Tools Active Directory Certificate Services Tools Certification Authority Management Tools			
	Export configuration settings Specify an alternate source path < Previous	Install	Cance	el

• A la fin de l'installation cliquer sur « Close »



• Configurer le service précédemment installer



• Cliquer « Next »

AD CS Configuration		6 <u>920</u>		×
Credentials	SR	DESTINAT	ION SER	VER er.IT
Credentials Role Services Confirmation Progress Results	Specify credentials to configure role services To install the following role services you must belong to the local Administra • Standalone certification authority • Certification Authority Web Enrollment • Online Responder To install the following role services you must belong to the Enterprise Admin • Enterprise certification authority • Certificate Enrollment Policy Web Service • Certificate Enrollment Web Service • Network Device Enrollment Service	ators grouț ins group:	D:	
	Credentials: ASSURMER\Administrator Change]		
	More about AD C5 Server Koles			
	< Previous Next > Con	figure	Cance	el 🗌

Sélectionner « Certification Authority »



• Sélectionner « Enterprise CA » puis « Next »



Sélectionner « Root CA » puis « Next »



• Sélectionner « Create a new private key » puis « Next »



• Cliquer « Next »

AD CS Configuration			1.000		×
Cryptography fo	or CA		DESTINA SRV-ADDCC	TION SEF)1.assurm	VER Ner.IT
Credentials Role Services Setup Type	Specify the cryptographic options Select a cryptographic provider:		Key length:		
CA Type	RSA#Microsoft Software Key Storage Provider	×	2048		¥
Private Key	Select the hash algorithm for signing certificates issued by	y this CA:			
Cryptography	SHA256	^	1		
CA Name	SHA384				
Validity Period	SHA512				
Certificate Database	SHA1				
Confirmation	MD5		1		
	Allow administrator interaction when the private key is	s accessed	by the CA.		
	More about Cryptography				
	< Previous Next	1 202	Configure	Canc	el

Cliquer « Next »



• Choisir la durée du certificat puis cliquer « Next »

🚵 AD CS Configuration								-		×
Validity Period							DE SRV-	ADDC0	ION SER	VER er.IT
Credentials Role Services Setup Type	Speci Select th	fy the validi	ty perio	od rtificate g	enerated fo	r this certifi	cation auth	iority (C	А):	
CA Type	5	Years		* 1						
Private Key	CA expir	ration Date: 28/0	1/2030 17	06:00						
Cryptography CA Name	The valid certificat	dity period config tes it will issue.	gured for t	his CA cer	tificate sho	uld exceed	the validity	period	for the	
Validity Period										
Certificate Database										
Confirmation										
Results										
	More ab	out Validity Perio	od							
			[< Previou	us Ne	×?	Config	lure	Cance	el

• Laisser les chemins par défauts et cliquer « Next »

AD CS Configuration			-		×
CA Database			DESTINAT SRV-ADDC0	ION SER I.assurm	VER er.IT
Credentials Role Services	Specify the database locations				
Setup Type	Certificate database location:				
CA Type	C:\Windows\system32\CertLog				
Private Key	Certificate database log location:				
Cryptography	C:\Windows\system32\CertLog				
CA Name					
Validity Period					
Certificate Database					
Confirmation					
	More about CA Database				
	< Previous Next :	>	Configure	Cance	el l

• Cliquer sur « Configure »



< Previous Next >

Close

Cancel

Results

Configuration 802.1X :

 Dans NPS sélectionner « RADIUS server for 802.1X … » puis « Configure 802.1X »



 Sélectionner « Secure Wireless Connections » puis choisir un nom Configure 802.1X

Type of 802 1X connections	
 Secure Wireless Connections When you deploy 802.1X wireless a connection requests made by wirele 	access points on your network, NPS can authenticate and authorize ess clients connecting through the access points.
 Secure Wired (Ethemet) Connection When you deploy 802.1X authentic connection requests made by Ether 	ns ating switches on your network, NPS can authenticate and authorize met clients connecting through the switches.
Name: This default text is used as part of the r default text or modify it .	name for each of the policies created with this wizard. You can use the
WIELBADIUS	
MI HADIOS	

Select 802 1X Connections Type

• Ensuite la borne sera identifiée et cliquer « Next »

Configure 8	302.1X	×
	Specify 802.1X Switches	
5	Please specify 802.1X switches or Wireless Access Points (RADIUS	Clients)
RADIUS cli	ents are network access servers, such as authenticating switches and w	vireless access point.
To specify	a RADIUS client, click Add.	
RADIUS c	lients:	
wap255450	2011 (Y	Add
		Edit
		Remove
1		
	Previous New Finis	h Cancel

 Sélectionner « Microsoft Smart … » dans le menu déroulant puis cliquer sur « Configure »



• Choisir le groupe de sécurité qui doit avoir accès au WiFi

Select Group	×
Select this object type:	
Group	Object Types
From this location:	
assumer.IT	Locations
Enter the object name to select (examples):	
User-WIFI	Check Names
I	
Advanced	GOK Cancel

• Cliquer « Next »

Configure 802	2.1X						×
	Specify Us	er Gro	ups				
A	Users that are m based on the net	embers of work polic	the selected cy Access Per	l group or rmission s	groups wi etting.	ll <mark>be all</mark> ower	d or denied access
To select User	Groups, click Add. I	f no group:	s are selected	I, this policy	applies to	all users.	
Groups							Add
ASSURMER	\User-WIFI						Remove
		[Previous	Ne	15	Finish	Cancel

• Cliquer « Finish »

1	Configure 802.1X	×	
e	Completing New IEEE 802.1X Secure Wired and Wireless Connections and RADIUS clients		
9 N	You have successfully created the following policies and configured the following RADIUS clients. To view the configuration details in your default browser, click Configuration Details. To change the configuration, click Previous. To save the configuration and close this wizard, click Finish. 		
	Connection Request Policy: WIFI-RADIUS Network Policies: WIFI-RADIUS		
	Configuration Details		
	Previous Next Finish Cancel		

Configuration borne WiFi pour RADIUS :

• Sur l'interface Web, sélectionner « Edit »

cisco WAP371 V	Vireless-AC/N Dual Radio Access Point with Single Point Setup							
Getting Started	Networks							
Run Setup Wizard								
 Status and Statistics 	Select the radio interface first, and then enter the configuration parameters.							
 Administration 	Radio: Radio 1 (5 GHz)							
► LAN	Radio 2 (2.4 GHz)							
▼ Wireless	Virtual Access Points (SSIDs)							
Radio Roque AP Detection	VAP No. Enable VLAN ID SSID Name SSID Broadcast Security MAC Filter Channel Isolation Band Steer							
Networks	n 🖉 n Assumer-bbm 🖉 None 🗸 Disabled 🗸 🗖							
Wireless Multicast Forward Scheduler	Add Edit Delete							
Scheduler Association								
Bandwidth Utilization	Save							
MAC Filtering								
WorkGroup Bridge								
QoS								
 System Security 								
Client QoS								
SNMP								
Single Point Setup								
 Captive Portal 								

Cocher « Use global RADIUS server settings »

rtual Acc	ess Points (SSIDs)						
VAP N	o. Enable	VLAN ID	SSID Name	SSID Broadcast	Security	MAC Filter	Channel Isolation	Band Steer
	0 🔽	1	Assurmer-bbm		WPA Enterprise 🗸	Disabled 🗸		
					Hide Details			
					WPA Versions: WPA	-TKIP 🛛 WPA2	AES	
					Enat	ble pre-authentication	Required	
					🔽 Use global RADIUS s	erver settings		
					Server IP Address Type:	IPv4 OIPv6		
					Server IP Address-1:	0.0.0.0	(XXX.XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	
					Server IP Address-2:		(XXX.XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX	
					Server IP Address-3:		(XXX.XXX.XXXX)	
					Server IP Address-4:		(XXX.XXX.XXXX	
					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	ounting		
					Active Server:	Server IP Address-1 🗸		
					Broadcast Key Refresh Ra	ate: 86400	Sec (Range: 0-86400, 0 = Di	sable, Default: 86400)
					Session Key Refresh Rate	e: O	Sec (Range: 30-86400, 0 = D	isable, Default: 0)

 Retourner sur NPS puis « Network Polities » puis clic-droit sur la politique RADIUS

Network Policy Server				-	- 🗆	×				
File Action View Help										
🗢 🔿 🖄 📆 🖬 🖬										
🚯 NPS (Local)	Network Policies									
RADIUS Clients and Servers Policies Connection Request Po Network Policies	Network policies allow you under which they can or ca	to designate who is authorize annot connect.	itized to connect to the network and the circumstances							
Accounting	Policy Name		Status	Processing Order	Access Type	S				
> 🙀 Templates Management	Connections to Microsoft Ro Connections to other access Connections to other access WIFI-RADIUS Conditions - If the following cc Condition Value NAS Port Type Wireless Windows Groups ASSUR	Move Up Enabled 1 Gamma Finabled 2 Gamma Finabled 1000000 D Finable Finabled 1000000 D Finable Fi				rant Access U rant Access U eny Access U eny Access U				
>	Settings - Then the following setti	ings are applied: Value				^ ,				

• Sélectionner « Wireless – IEEE 802.11 » puis « Apply » et « OK »

all constraints are not matched by the	policy. connection request, network access is denied.	
Constraints: Authentication Methods	Specify the access media types required to match this policy Common dial-up and VPN tunnel types	
Session Timeout Called Station ID	Async (Modem) ISDN Sync Sync (T1 Line) Virtual (VPN) Common 802.1X connection tunnel types	
1 NAS Port Type	Ethemet FDDI Token Ring Wireless - IEEE 802.11 Othered	
	Conteres ADSL-CAP - Asymmetric DSL Carrierless Amplitude Phase Modulation ADSL-OMT - Asymmetric DSL Discrete Multi-Tone Async (Modem) Cable Y	

• Sur NPS et « Network Policies », supprimer les politiques par défaut

2							
Vetwork Policy Server					-	- 🗆	×
File Action View Help							
🗢 🔿 🙋 📅							
NPS (Local)	Network Policies						
ADJUS Clients and Servers Policies Connection Request Policier	Network policies allo under which they ca	w you to designate wh n or cannot connect.	o is authorized to	connect t	o the network and t	he circumstanc	85
Accounting	Policy Name WIFI-RADIUS SSID Connections to Microsoft Connections to other acc Conditions - If the following Condition Day and time restrictions	Routing and Remote Ad ress servers conditions are met Value Sunday 00:00-24:0	Move Up Move Dow Disable Delete Rename Duplicate P	Status Enabled Enabled Enabled	Processing Order 1 2 999999	Access Type Grant Access Grant Access Deny Access Deny Access	S U U U U
			Properties				
			Help				
	Settings - Then the followin	a settings are applied:					
	Jeanga - men are rollowi	ng acturinga uro uppricu.					_
	Setting	/alue					~
‹ >	<						>
Delete							
Network Policy Server File Action View Help File Provide the server of the server	Network Policies				-	- 🗆	×
Policies Connection Request Po Network Policies	Network policies all under which they ca	ow you to designate wh an or cannot connect.	o is authorized to	o connect t	o the network and t	he circumstanc	es
Accounting	Policy Name			Status	Processing Order	Access Type	S
Iemplates Management	SSID			Enabled	2	Grant Access	U
	Connections to Microsoft	R				Deny Access	U
		Undo					-
	Connections to Microso	ft Cut					
	Conditions - If the following	Copy					^
		Paste			_		_
	Condition Val	ue Delete					
	MS-RAS Vendor ID "31	1: Select All					
		Right to left	Reading order				
		Show Unico	de control char	acters			
	Cottingo Theo the full	Insert Unico	de control char	acter	>		
	Sewings - Then the following	Open IME					_
	Setting	Reconversio	n				^ ~
< >	<						>
	52.						