Wifi ENSA-Grenoble et eduroam Windows

×

Faites un clic droit sur l'icône du wifi et dans le menu contextuel qui s'affiche cliquez sur **Ouvrir le Centre Réseau et partage**.

Cliquez sur **Configurer** une nouvelle connexion ou un nouveau réseau.



Sélectionnez

Se connecter manuellement à un réseau sans fil puis cliquez sur le bouton Suivant.

Renseignez les informations suivantes :

(les captures d'écran ont été réalisées avec le réseau ENSA-Grenoble mais le principe est exactement le même pour le réseau eduroam)

Résoudre les problèmes

へ 💷 * 腐 🕬

Ouvrir le Centre Réseau et partage

14:43

12/01/2017

Nom réseau : ENSA-Grenoble ou eduroam Type de sécurité : WPA2 - Entreprise Type de chiffrement : AES

Cliquez sur le bouton Suivant.

← 👰 Se connecter manueller	nent à un réseau sans fil
Entrer les informatio	ns relatives au réseau sans fil à ajouter
<u>N</u> om réseau :	ENSA-Grenoble
Type <u>d</u> e sécurité :	WPA2 - Entreprise 🗸 🗸
Type de chiffrement :	AES ~
Clé de sé <u>c</u> urité :	<u>M</u> asquer les caractères
✓ Lancer automatique	ment cette connexion
☐ Me c <u>o</u> nnecter mêm Attention : si vous s risque.	: si le réseau ne diffuse pas son nom électionnez cette option, la sécurité de votre ordinateur peut courir un
	Suivant Annuler

			-	×	
inexion.	~	👻 Se connecter manuellement à un réseau sans fil			
		ENSA-Grenoble a été correctement ajouté.			
		[
		→ Modifier les paramètres de connexion Ouvre les propriétés de connexion pour me permettre de modifier certains paramètres.			

Configurer une connexion ou un réseau
 Choisir une option de connexion
 Connexion à Internet
 Configurer un nouveau roite d'accès à distance à Internet.
 Configurer un nouveau réseau
 Configurer un nouveau roiteur ou un nouveau point d'accès.
 Se connecter manuellement à un réseau sans fil
 Connexion à votre espace de travail
 Configurer une connexion d'accès à distance ou VPN à votre espace de travail.

Cliquez ensuite sur Modifier les paramètres de connexion. Dans l'onglet Sécurité cliquez sur le bouton Paramètres (1).

Propriétés du réseau sans	; fil ENSA-Grenoble	×
Connexion Sécurité		
<u>T</u> ype de sécurité : Type de chi <u>f</u> frement :	WPA2 - Entreprise \checkmark AES \checkmark	
Choisissez une méthode	d'authentification réseau :	
Microsoft: PEAP (Protect	ted EAP)	
✓ Mémoriser mes inforr cette connexion à ch Paramètres ayancés	nations d'îdentification pour paque fois que je suis connecté	
	OK Annu	er

Décochez la case Vérifier l'identité du serveur en validant le certificat (2).

Cliquez sur le bouton **Configurer** (3) à droite de *Mot de passe sécurisé (EAP-MSCHAP version 2)*.

Lors de la connexion : Vérifier l'identité du serveur en validant le certificat 2 Connexion à ces serveurs (exemples : srv1; srv2; * .*\srv3\.com) :	Propriétés EAP protégées		
Autorités de certification racine de confiance : AddTrust External CA Root Baltimore CyberTrust Root Class 3 Public Primary Certification Authority COMODO RSA Certification Authority DigiCert Assured ID Root CA DigiCert Global Root CA DigiCert High Assurance EV Root CA C Notifications avant la connexion : Informer l'utilisateur si l'identité du serveur ne peut pas être vérif Sélectionner la méthode d'authentification : Mot de passe sécurisé (EAP-MSCHAP version 2) Configurer Sélectionnect. si le serveur ne présente pas <u>I</u> LV de liaison de chiffr. Activer la protection <u>de la</u> confidentialité	Lors de la connexion : Vérifier l'identité du serveur en validant le certificat 2 Connexion à ces serveurs (exemples : srv1 ; srv2 ; .*srv3\.com) :		
 Notifications avant la connexion : Informer l'utilisateur si l'identité du serveur ne peut pas être vérif Sélectionner la méthode d'authentification : Mot de passe sécurisé (EAP-MSCHAP version 2) Configurer Activer la reconnexion rapide 3 Déconnect. si le serveur ne présente pas <u>I</u>LV de liaison de chiffr. Activer la protection <u>d</u>e la confidentialité 	Autorités de certification racine de confiance : AddTrust External CA Root AddTrust External CA Root Baltimore CyberTrust Root Class 3 Public Primary Certification Authority COMODO RSA Certification Authority DigiCert Assured ID Root CA DigiCert Global Root CA DigiCert High Assurance EV Root CA		
Sélectionner la méthode d'authentification : Mot de passe sécurisé (EAP-MSCHAP version 2) Activer la reconnexion rapide Déconnect. si le serveur ne présente pas <u>I</u> LV de liaison de chiffr. Activer la protection <u>d</u> e la confidentialité	Notifications avant la connexion :		
	Informer l'utilisateur si l'identité du serveur ne peut pas être verif Sélectionner la méthode d'authentification : Mot de passe sécurisé (EAP-MSCHAP version 2) Activer la reconnexion rapide Déconnect. si le serveur ne présente pas <u>T</u> LV de liaison de chiffr. Activer la protection <u>d</u> e la confidentialité	3	

Décochez la case Utiliser automatiquement mon nom et mon mot de passe Windows d'ouverture de session (et éventuellement le domaine).

Refermez cette fenêtre et la précédente en cliquant sur le bouton **OK**.

EAP MSCHAPv2 Properties	х			
When connecting:				
Automatically use my Windows logon name and password (and domain if any).				
OK Cancel				

Cliquez ensuite sur le bouton **Paramètres avancés** (4) de l'onglet **Sécurité**.

Dans l'onglet **Paramètres 802.1X** cochez la case **Spécifier le mode d'authentification**, choisissez le mode **Authentification utilisateur** puis cliquez sur le bouton **Enregistrer ident.** pour enregistrer votre nom d'utilisateur et votre mot de passe.

(pour le réseau eduroam le nom d'utilisateur doit être sous la forme login@domaine ;

ex : enseignant.t@grenoble.archi.fr)

Paramètres avancés	Х
Paramètres 802.1X Paramètres 802.11	
Spécifier le mode d'authentification :	
Authentification utilisateur \vee 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 aprè <u>s</u> l'ouverture de session de l'utilisateur	
Délai maximal (secondes) :	
Autoriser l'affichage de <u>b</u> oîtes de dialogue supplémentaires pendant l'authentification unique	
Ce réseau utilise des réseaux locaux <u>vi</u> rtuels distincts pour l'authentification de l'ordinateur et de l'utilisateur	
OK Annule	er

Fermez toutes les fenêtres ouvertes (en cliquant sur le bouton **OK**).

Dès que le signal wifi sera à portée, vous serez automatiquement connecté.