

Configuration du réseau sans fil « UdeM avec cryptage » pour Windows 10

1. Avant de commencer, il est nécessaire de supprimer la configuration d'accès au réseau sans fil qui est déjà existante. Cliquer sur l'icône réseau, située dans la barre des tâches au bas de l'écran. Ensuite, cliquer sur « Paramètres réseau & internet ».



2. Dans la fenêtre des paramètres, choisir « Gérer les réseaux connus » de la rubrique « Wi-Fi ».



3. Ensuite, choisir « UdeM avec cryptage », puis cliquer sur le bouton « Oublier ».



4. Cliquer sur l'icône réseau située dans la barre des tâches au bas de l'écran et choisir « UdeM avec cryptage ». Ensuite, cocher la case « Se connecter automatiquement », puis cliquer sur le bouton « Se connecter ».



5. À la fenêtre d'avertissement, cliquer sur le bouton « Se connecter ».



6. Pour poursuivre, faire un clic droit sur l'icône réseau de sélectionner « Ouvrir le Centre Réseau et partage » du menu contextuel.



7. À cette fenêtre, cliquer sur le lien « Wi-Fi (UdeM avec cryptage) ».

Centre Réseau et partage				-		×
🚽 🕤 🛧 🙀 - Tous les Pann	eaux de conf	iguration > Centre Réseau et partage		~ O	Rechercher	,
Page d'accueil du panneau de configuration	Affiche Afficher v	r les informations de base de vo ros réseaux actifs	otre réseau et cor	nfigurer de	es connexi	ion
Modifier les paramètres de la carte Modifier les paramètres de partage avancés	ads.u Résea	imontreal.ca au avec domaine	Type d'accès : Connexions :	Intern Wi-Fi crypta	et (UdeM avec ge)	
	Modifier	vos paramètres réseau Configurer une nouvelle connexion ou un Configurez une connexion haut débit, d'a un point d'accès. Résoudre les problèmes Diagnostiquez et réparez les problèmes d dépannage.	nouveau réseau ccès à distance ou VPN le réseau ou accédez à	l, ou configur des informati	ez un routeur ions de	ou
Voir aussi						
Groupement résidentiel						
Infrarouge						
Options Internet						
Pare-feu Windows						

8. Dans la fenêtre des détails du réseau Wi-Fi, cliquer sur le bouton « Propriétés sans fil ».

⊿ État de Wi-Fi			×
Général			
Connexion			
Connectivité IF	2v4:		Internet
Connectivité IP	2v6:	Pas d'acc	cès réseau
État du média	:		Activé
SSID :		UdeM ave	c cryptage
Durée :			19:10:03
Vitesse :		144	,0 Mbits/s
Qualité du sign	al :		littee
Détails	Propriétés	sans fil	
Activité			
	Envoyés —	S	Reçus
Octets :	354 470	400	354 086
Propriétés	Désactiver	Diagnostiquer	[
			Fermer

9. Dans l'onglet « Connexion », cocher la case « Me connecter automatiquement lorsque ce réseau est à portée ».

Propriétés du	u réseau sa	ns fil UdeM a	vec cryptage	×
Connexion	Sécurité			
Nom :		UdeM avec o	ryptage	
SSID :		UdeM avec of	ryptage	
Type de ré	seau :	Point d'accès		
Disponibilit réseau :	é du	Tous les utili	sateurs	
Me con	necter auto	matiquement lo	rsque ce réseau	est à portée
Rechere à ce rés	cher d'autre seau	s réseaux sans	fil tout en étant	connecté
Me con	necter mêm	e si le réseau	ne diffuse pas so	n nom (SSID)
			ОК	Annuler

- 10. Toujours dans la même fenêtre, sélectionner l'onglet « Sécurité » et suivre les étapes suivantes :
 - Type de sécurité : « WPA2 Entreprise »;
 - Type de chiffrement : « AES »;
 - À l'option « Choisissez une méthode d'authentification réseau », sélectionner « Microsoft : PEAP (Protected EAP) »;
 - Cocher la case « Mémoriser mes informations d'identification pour cette connexion à chaque fois que je suis connecté »;
 - Ensuite, cliquer sur le bouton « Paramètres ».

Propriétés du réseau sar	ns fil UdeM avec c	ryptage	×	
Connexion Sécurité				
Type de sécurité : Type de chiffrement :	WPA2 - Entreprise AES	9	• 0 •	
Choisissez une méthode d'authentification réseau : Microsoft: PEAP (Protected EAP) Mémoriser mes informations d'identification pour cette connexion à chaque fois que je suis connecté				
Paramètres avancés				
		ОК	Annuler	

- 11. Dans la fenêtre des propriétés EAP, suivre les étapes suivantes :
 - Cocher la case « vérifier l'identité du serveur en validant le certificat »;
 - Cocher la case « Connexion à ces serveurs (exemples srv1;srv2;.*\.srv3\.com) : » et inscrire « accesreseau.umontreal.ca » dans la zone de texte;
 - Dans la section « Autorités de certification racine de confiance : », cocher « Entrust Root Certification Authority – G2 »;
 - Sous la section « Notifications avant la connexion : », sélectionner « Informer l'utilisateur si le nom du serveur ou le certificat racine »;
 - Sous la section « Méthode d'authentification », choisir « Mot de passe sécurisé (EAPMSCHAP version 2) », cocher la case « Activer la reconnexion rapide » et cliquer sur le bouton « Configurer... ».

Propriétés EAP protégées	>
Lors de la connexion :	
Vérifier l'identité du serveur en validant le certificat	
Connexion à ces serveurs (exemples : srv1 ; srv2 ; .*\.srv3\.com) :	
accesreseau.umontreal.ca	
Autorités de certification racine de confiance :	
DigiCert Global Root CA DigiCert High Assurance EV Root CA	^
DST Root CA X3	
Entrust Root Certification Authority - G2 Entrust.net Certification Authority (2048) Equifax Secure Certificate Authority	
GeoTrust Global CA	~
< >	
Notifications avant la connexion :	
Informer l'utilisateur si le nom du serveur ou le certificat racine	~
Sélectionner la méthode d'authentification :	
Mot de passe sécurisé (EAP-MSCHAP version 2) 🛛 🗸 🚺 Configu	irer
Activer la reconnexion rapide	
Déconnect. si le serveur ne présente pas TLV de liaison de chi	iffr.
Activer la protection de la confidentialité	
OK Ann	uler

- 12. Pour la prochaine étape, si vous utilisez un **poste non géré** par les Technologies de l'information (poste personnel) et que votre session de travail est ouverte avec des informations différentes de celles de votre compte UdeM, vous devez :
 - décocher la case « Utiliser automatiquement mon nom et mon mot de passe Windows d'ouverture de session (et éventuellement le domaine) »;
 - cliquer sur le bouton « OK » pour fermer la fenêtre.



Par contre, si vous utilisez un **poste géré** par les Technologies de l'information et que votre session de travail est ouverte avec des informations différentes de celles de votre compte UdeM, vous devez :

- cocher la case « Utiliser automatiquement mon nom et mon mot de passe Windows d'ouverture de session (et éventuellement le domaine) »;
- cliquer sur le bouton « OK » pour fermer la fenêtre.



13. De retour à la fenêtre des propriétés EAP, cliquer sur le bouton « OK ».

Propriétés EAP protégées	×
Lors de la connexion :	
Vérifier l'identité du serveur en validant le certificat	
Connexion à ces serveurs (exemples : srv1 ; srv2 ; .*\.srv3\.com) :	
accesreseau.umontreal.ca	
Autorités de certification racine de confiance :	
DigiCert Global Root CA DigiCert High Assurance EV Root CA DigiCert High Assurance EV Root CA	^
IDST ROOT CA X3 Entrust Root Certification Authority	
Entrust Root Certification Authority - G2 Entrust.net Certification Authority (2048)	
Equifax Secure Certificate Authority	
GeoTrust Global CA	~
Notifications avant la connexion :	
Informer l'utilisateur si le nom du serveur ou le certificat racine	~
Sélectionner la méthode d'authentification :	
Mot de passe sécurisé (EAP-MSCHAP version 2) Configur	er
C Activer la reconnexion rapide	
Déconnect. si le serveur ne présente pas TLV de liaison de chif	fr.
Activer la protection de la confidentialité	
OK Annu	ler

14. À la fenêtre suivante, sélectionner l'onglet « Sécurité » et cliquer sur le bouton « Paramètres avancés ».

Propriétés du réseau sans fil UdeM avec cryptage					
Connexion Sécurité					
Type de sécurité :	WPA2 - Entreprise	~			
Type de chiffrement :	AES	~			
Choisissez une méthode	e d'authentification ré	seau :			
Microsoft: PEAP (Prote	cted EAP) ~	Paramètres			
Mémoriser mes informations d'identification pour cette connexion à chaque fois que je suis connecté					
Paramètres avancés	J				
		OK A	nnuler		

- 15. Dans la fenêtre des paramètres avancés, si vous utilisez un **poste non géré** par les Technologies de l'information (poste personnel), vous devez :
 - sélectionner l'onglet « Paramètres 802.1x »;
 - cocher la case « Spécifier le mode d'authentification »;
 - sélectionner « Authentification utilisateur » et cliquer sur le bouton « OK ».



Par contre, si vous utilisez un **poste géré** par les Technologies de l'information, à cette fenêtre, vous devez :

- cocher la case « Activer l'authentification unique pour ce réseau »;
- cocher la case « Immédiatement avant l'ouverture de session de l'utilisateur » et cliquer sur le bouton « OK ».



16. À cette fenêtre, cliquer sur le bouton « OK ».

Propriétés du réseau san	s fil UdeM avec cry	ptage	×
Connexion Sécurité			
Type de sécurité : Type de	WPA2 - Entreprise	~	
cniffrement :			
Choisissez une méthode	d'authentification ré	seau :	
Microsoft: PEAP (Protect	ted EAP) ~	Paramètres	
Mémoriser mes infor cette connexion à ch	mations d'identificati aque fois que je suis	on pour s connecté	
Paramètres avancés			
		OK A	nuler

17. Fermer la fenêtre « État de Wi-Fi ».

🛋 État de Wi-Fi				×
Général				
Connexion				
Connectivité IPv	4:		Internet	
Connectivité IPv	6 :	Pas d'acc	cès réseau	
État du média :			Activé	
SSID :		UdeM ave	c cryptage	
Durée :			19:19:14	
Vitesse :		130	0,0 Mbits/s	
Qualité du signa	!:		attl	
Détails	Propriétés	sans fil		
Activité				-
	Envoyés —	N –	Reçus	
Octets :	256 157		282 990	
Propriétés	Désactiver	Diagnostiquer		
			Ferme	r

18. Pour vous connecter au réseau sans fil avec cryptage, cliquer sur « UdeM avec cryptage ».



19. Ensuite, cliquer sur le bouton « Se connecter » pour vous connecter au réseau « UdeM avec cryptage ».

