Instrukcja ręcznej konfiguracji sieci WiFi dla pracowników oraz studentów Uniwersytetu Medycznego w Łodzi

PARAMETRY POŁĄCZENIA DO SIECI WIFI

Nazwa sieci (SSID): "UMED-Pracownik" w przypadku pracownika / "UMED-Student" w przypadku studenta

Typ zabezpieczeń: WPA2-Enterprise

Typ szyfrowania: AES

Metoda uwierzytelniania sieci: Microsoft: Chroniony protokół EAP (PEAP)

Nazwa użytkownika: adres e-mail w formacie imię.nazwisko@umed.lodz.pl w przypadku

pracownika lub imię.nazwisko@stud.umed.lodz.pl w przypadku studenta.

Hasło: aktualne hasło do poczty Office365 Uniwersytetu Medycznego w Łodzi

UWAGA !!!

Jeżeli użytkownik nie napotyka trudności podczas łączenia się z ww. sieciami bezprzewodowymi za pomocą automatycznych mechanizmów systemowych, sugerujemy pozostanie przy tej metodzie, i zaniechanie ręcznej konfiguracji sieci na podstawie poniższej instrukcji.

PROCEDURA RĘCZNEJ KONFIGURACJI SIECI WIFI

Ze strony http://www.cit.umed.pl/ pobieramy dwa certyfikaty (pliki UMED-RootCA.cer i UMED-IssuingCA1.cer)

http://www.cit.umed.pl/dl.php?file=UMED-RootCA.cer http://www.cit.umed.pl/dl.php?file=UMED-IssuingCA1.cer Zanim zainstalujemy certyfikat musimy skopiować go na pulpit komputera . Jak to zrobić – wykorzystując drugi komputer i pendrive lub w jeszcze inny sposób – to zostawimy w gestii użytkownika.

W tym opisie plik z certyfikatem **UMED-RootCA.cer i UMED-IssuingCA1.cer** jest skopiowany na Pulpit. Najeżdżamy na ikonę pliku i prawym przyciskiem myszki uruchamiamy menu kontekstowe, następnie wybieramy *Zainstaluj certyfikat*.



Pojawi się okno jak poniżej i klikamy na Dalej



Następnie wybieramy opcję *Umieść wszystkie certyfikaty w następującym magazynie* i klikamy w przycisk *Dalej*, pojawi się kolejne okno *Wybieranie magazynu certyfikatów*, gdzie zaznaczamy:

UMED-RootCA.cer >> Zaufane główne urzędy certyfikacji i potwierdzamy OK.

UMED-IssuingCA1.cer >> Pośrednie urzędy certyfikacji i potwierdzamy OK.



W następnym kroku klikamy na Dalej oraz Zakończ

apazyn certyfikatów Magazyny certyfikatów to obszary systemowe, w których przechowywane są certyfikaty.		Kończenie pracy Kreatora importu certyfikatów
System Windows może automatycznie wybrać magazyn certyfikatów; możesz jednak określić inną lokalizocję da certyfikatu.		Certyfikat zostanie zainportowany po kliknięciu przycisku Zalipricz.
Automatycznie wybierz magazyn certyfikatów na podstawie typu certyfikatu	9	Wybrane zostały nasitępujące ustawienia:
Unieść wszystkie certyfikaty = następującym nagazynie		Papazyn certytkatów wybrany pisez użytkownika. Zaufi Zawartość Certy
Magazyn certyfikatów:		
zania e donne grafoù ce rhoark		x []
medz się włęcej o <u>negocymsch certrificatów</u>		

I w tym momencie mamy już zainstalowany certyfikat, co potwierdzi poniższy komunikat:



Dodajemy ręcznie profil sieci bezprzewodowej

Menu start->Panel sterowania->Centrum sieci i udostępniania->Zarządzaj sieciami bezprzewodowymi ->Dodaj- >Ręcznie utwórz profil sieciowy











Podajemy nazwę sieci ("**UMED-Pracownik**" lub "**UMED-Student**"), wybieramy typ zabezpieczeń "**WPA2- Enterprise**" oraz typ szyfrowania "**AES**", a następnie klikamy "Dalej"

🚱 📶 Ręczne nawiązywanie po	vłączenia z siecią bezprzewodową		
Wprowadź informacj	e o sieci bezprzewodowej, którą chcesz dodać.		
Nazwa sieci:	UMED-Pracownik		
Typ zabezpieczeń:	WPA2-Enterprise		
Typ szyfrowania:	AES		
Klucz zabezpieczeń:	🗌 Ukryj znaki		
🔲 Uruchom to połączenie automatycznie			
🔲 Połącz, nawet jeśli sie	🔲 Połącz, nawet jeśli sieć nie wykonuje emisji		
Ostrzeżenie: jeśli wył	Ostrzeżenie: jeśli wybierzesz tę opcję, może to zagrozić prywatności komputera.		
	Dalej Anuluj		

Potwierdzamy opcję "Zmień ustawienia połączenia"



W zakładce "**Zabezpieczenia**" wybieramy z listy metodę zabezpieczenia sieci "**Microsoft: Chroniony protokół EAP (PEAP)**" Klikamy przycisk **Ustawienia.**

ί	JMED-Pracownik — Właściwości sieci bezprzewodowej	×
	Połączenie Zabezpieczenia	
	Typ zabezpieczeń: WPA2-Enterprise Typ szyfrowania: AES	
	Wybierz metodę uwierzytelniania sieci: Microsoft: Chroniony protokół EAP (PEA ▼ Ustawienia Zapamiętaj moje poświadczenia dla tego połączenia przy każdym logowaniu	
	Ustawienia zaawansowane	
	OK An	uluj

Z listy zaufanych głównych urzędów certyfikacji wybieramy opcję UMED-RootCA

Właściwości chronionego protokołu EAP	x
Podczas łaczenia: Weryfikuj certyfikat serwera Połącz tylko z tymi serwerami:	
Zaufane główne urzędy certyfikacji:	,
thawte Primary Root CA - G3 Thawte Timestamping CA UMED-Tossuino CA 1 UMED-Root CA UMED-Root CA UMED-Root CA UN-OSERFIFSt-Object VeriSign Class 3 Public Primary Certification Authority - G5 VeriSign Trust Network Nie monituj użytkownika o autoryzowanie nowych serwerów lub zaufanych urzędów certyfikacji	
Wybierz metodę uwierzytelniania:	
Bezpieczne hasło (EAP-MSCHAP v2) Konfiguruj	
 Włącz szybkie łączenie ponowne Wymuś ochronę dostępu do sieci Rozłącz, jeśli serwer nie przedstawi obiektu TLV powiązania kryptograficznego 	
Włącz prywatność tożsamości OK Anuluj	

W tym samym oknie wybieramy opcję "Konfiguruj..." i ODZNACZAMY opcję "Automatycznie użyj mojej nazwy logowania i hasła systemu Windows" klikamy "OK"

Właściwości protokołu EAP MSCHAPv2	23
Podczas łączenia:	
Automatycznie użyj mojej nazwy logowania (oraz domeny, jeżeli istnieje) systemu Windo	i hasła ows
OK Anuluj	

Następnie wybieramy opcję "**Ustawienia zaawansowane**", i w zakładce "**Ustawienia 802.1X**" AKTYWUJEMY opcję "**Określ tryb uwierzytelniania**" i wybieramy z listy opcję "**Uwierzytelnianie użytkownika**" i zatwierdzamy opcją "OK".

Połączenie Zabezpier	zenia	Ustawienia 202, 1X Ustawienia sieci 802, 11
Typ zabezpieczeń: Typ szyfrowania:	WPA2-Enterprise AES	Vierzytelniania: Uwierzytelnianie użytkownika Usuń poświadczenia dla wszystkich użytkowników
Wybierz metode uwi	rzvtelniania sieci:	Włącz rejestrację jednokrotną dla tej sieci
Microsoft: Chronion	y protokół EAP (PEA * Ustawienia	Wykonaj bezposrednio przed logowaniem uzytkownika Wykonaj bezpośrednio po logowaniem uzytkownika Wykonaj bezpośrednio po logowaniem uzytkownika
Zapamiętaj moje przy każdym logo	poswiadczenia dla tego potączenia waniu	Maksymalne opóźnienie (w sekundach): 10 👘
Ustawienia zaawan	sowane	
	OK A	OK Anuluj

Wybieramy opcję zamknij



Przy próbie połączenia z siecią bezprzewodową jako nazwę użytkownika należy podać adres poczty Office365 w formacie imię.nazwisko@umed.lodz.pl w przypadku pracownika lub imię.nazwisko@stud.umed.lodz.pl w przypadku studenta, natomiast jako hasło należy podać aktualne hasło do poczty Office365.