Centrum Informatyki



Uniwersytet Ekonomiczny w Poznaniu

Eduroam

Windows Vista / Windows 7

Konfiguracja przyłączenia do sieci **eduroam** komputera pracującego pod nadzorem systemu operacyjnego MS Windows Vista lub MS Windows 7.

1. Za pomocą Panelu sterowania uruchamiamy Centrum sieci i udostępniania:



lub



2. Wybieramy opcję Skonfiguruj nowe połączenie lub sieć:



3. Wybieramy opcje ręcznej konfiguracji połączenia:

ybierz	opcję połączenia.
0	Połącz z Internetem Skonfiguruj połączenie bezprzewodowe, szerokopasmowe lub telefoniczne z Internetem.
2	Skonfiguruj nową sieć Konfiguruj nowy router lub punkt dostępu.
ł	Ręczne nawiązywanie połączenia z siecią bezprzewodową Połącz się z siecią ukrytą lub utwórz nowy profil sieci bezprzewodowej,
b	Połącz z miejscem pracy Skonfiguruj połączenie telefoniczne lub połączenie VPN z miejscem pracy.
4	Skonfiguruj połączenie telefoniczne Połącz z Internetem przy użyciu połączenia telefonicznego.

4. Zaznaczone pola wypełniamy jak na rysunku i potem klikamy na przycisk Dalej:

<u>N</u> azwa sieci:	eduroam	
Typ z <u>a</u> bezpieczeń:	WPA2-Enterprise	
<u>T</u> yp szyfrowania:	AES	
<u>K</u> lucz zabezpieczeń:	🗖 🗆 🗖 🖄	
🔽 Uruch <u>o</u> m to połąc	zenie automatycznie	
🗖 Połącz, nawet jeśl	i sieć nie wykonuje emisji	
Ostrzeżenie: jeśli v	vybierzesz tę opcję, może to zagrozić prywatności komp	utera.

5. Klikamy na zaznaczone pole:

ęczne nawiązywanie połączenia z siecią bezprzewodową			
Ręczne nawiązywanie połączenia z siecią bezprzewodową			
nmvšlnje dodano: UF. Hotsnot. SFC			
A Zmień ustawienia połaczenia	1		
Otwórz właściwości połączenia, aby można było zmienić ustawienia.			
	-		
	7		
	Zam		

 W okienku *eduroam – Właściwości sieci bezprzewodowej* sprawdzamy, czy w pierwszej zakładce *Połączenie* zaznaczono opcję jak na rysunku i klikamy na drugą zakładkę *Zabezpieczenia:*

duroam — Właściw	ości sieci bezprzewodowej	
Połączenie Zabezpie	eczenia	
Nazwa:	eduroam	
SSID:	eduroam	
Typ sieci:	Punkt dostępu	
Dostępność sieci:	Wszyscy użytkownicy	

 Upewniamy się że wybrano odpowiednią metodę uwierzytelniania (protokół EAP) i klikamy przycisk Ustawienia

yp zabezpieczeń:	WPA2-Enterprise	
yp <u>s</u> zyfrowania:	AES	-
/y <u>b</u> ierz metodę uwie	rzytelniania sieci:	1
Microsoft: Chroniony	v protokół EAP (PEAI	<u>U</u> stawienia
	7010	
Ustawienia zaawan	sowane	

8. Usuwamy zaznaczenie opcji *Weryfikuj certyfikat serwera*, upewniamy się co do metody uwierzytelniania (EAP-MSCHAP v2) i klikamy przycisk *Konfiguruj*. W kolejnym okienku pozostawiamy niezaznaczoną opcję (jak na rys. poniżej), a następnie dwa razy klikamy przycisk *OK*.

Właściwości chronionego protokołu EAP 🔀	
Podczas łączenia: Weryfikuj certyfikat serwera Połącz tylko z tymi serwerami: Zaufane główne urzędy certyfikacji: AddTrust External CA Root Certum CA Class 3 Public Primary Certification Authority	
Entrust.net Secure Server Certification Authority Equifax Secure Certificate Authority GeoTrust Global CA GlobalSign Root CA	
Wybierz <u>m</u> etodę uwierzytelniania: Bezpieczne hasło (EAP-MSCHAP v2)	Właściwości protokołu EAP MSCHAPv2
 ✓ Włącz szy<u>b</u>kie łączenie ponowne Wymuś ochronę dostępu do gieci Rozłącz, jeśli serwer nie przedstawi obiektu <u>T</u>LV powiązania kryptograficznego Włącz prywatność tożsamości OK Anuluj 	Podczas łączenia: Automatycznie użyj mojej nazwy logowania i nasła (oraz domeny, jeżeli istnieje) systemu Windows OK Anuluj

9. Wracamy do zakładki *Zabezpieczenia* w okienku *eduroam – Właściwości sieci bezprzewodowej* i klikamy na przycisk *Ustawienia zaawansowane:*

Połączenie Zabezpieczenia Iyp zabezpieczeń: WPA2-Enterprise Typ szyfrowania: AES Wybierz metodę uwierzytelniania sieci: Microsoft: Chroniony protokół EAP (PEAI V Ustawienia Zapamiętaj moje poświadczenia dla tego połączenia przy każdym logowaniu Ustawienia zaawansowane OK Anuluj	duroam — V	Vłaściwo	sści sieci bezprzev	vodowej		5
Iyp zabezpieczeń: WPA2-Enterprise Typ gzyfrowania: AES Wybierz metodę uwierzytelniania sieci: Microsoft: Chroniony protokół EAP (PEAI) Ustawienia Zapamiętaj moje poświadczenia dla tego połączenia przy każdym logowaniu Ustawienia zaawansowane OK Anuly	Połączenie	Zabezpie	czenia			
Iyp zabezpieczeń: WPA2-Enterprise Typ gzyfrowania: AES Wybierz metodę uwierzytelniania sieci: Microsoft: Chroniony protokół EAP (PEAI) Ustawienia Zapamiętaj moje poświadczenia dla tego połączenia przy każdym logowaniu Ustawienia zaawansowane OK Anuluj						
Typ szyfrowania: AES Wybierz metodę uwierzytelniania sieci: Microsoft: Chroniony protokół EAP (PEAI) Ustawienia Image: Zapamiętaj moje poświadczenia dla tego połączenia przy każdym logowaniu Image: Sapamietel Statemark Ustawienia zaawansowane Ustawienia zaawansowane	<u>⊺</u> yp zabez	abezpieczeń: WPA2-Enterprise			_	
Wybierz metodę uwierzytelniania sieci: Microsoft: Chroniony protokół EAP (PEAI V Ustawienia) Zapamiętaj moje poświadczenia dla tego połączenia przy każdym logowaniu Ustawienia zaawansowane	Typ <u>s</u> zyfro	wania:	AES		-	
Wybierz metodę uwierzytełniania sieci: Microsoft: Chroniony protokół EAP (PEAI ▼ Ustawienia) ✓ Zapamiętaj moje poświadczenia dla tego połączenia przy każdym logowaniu Ustawienia zaawansowane OK						
Wybierz metodę uwierzytelniania sieci: Microsoft: Chroniony protokół EAP (PEAI) Ustawienia Zapamiętaj moje poświadczenia dla tego połączenia przy każdym logowaniu Ustawienia zaawansowane OK						
Microsoft: Chroniony protokół EAP (PEAI ▼ Ustawienia I Zapamiętaj moje poświadczenia dla tego połączenia przy każdym logowaniu Ustawienia zaawansowane OK Anuluj	Wybierz m	atoda uwi	ierzyteľniania cieci:			
Zapamiętaj moje poświadczenia dla tego połączenia przy każdym logowaniu Ustawienia zaawansowane OK	Microsoft	: Chronior	v protokół FAP (PFA		wienia	
Zapamiętaj moje poświadczenia dla tego połączenia przy każdym logowaniu Ustawienia zaawansowane OK Anuluj	I. see erer te		.,			
Ustawienia <u>z</u> aawansowane OK Anuluj						
OK Anuluj	Ustawier	ia zaawai	osowape			
OK Anuluj			bornance			
OK Anuluj						
OK Anuluj						
OK Anuluj						
OK Anuluj						
				OK	Anuluj	

10. Zaznaczamy opcję **Określ tryb uwierzytelniania**, z udostępnionej listy wybieramy tryb "*Uwierzytelnianie użytkownika*", następnie klikamy na przycisk **Zapisz poświadczenia**.

2	Określ tryb uwierzytelniania:
	Uwierzytelnianie użytkownika 💌 Zapisz poświadczenia
	📰 geen permaterant die naar, einen uzytkownikow
Г	Włącz <u>r</u> ejestrację jednokrotną dla tej sieci
	Wykonaj bezpośrednio przed logowaniem użytkownika
	C Wykona) bezpośrednio po logowaniu użytkownika
	Maksymalne opóźnienie (w sekundach):
	Zegwalaj na wyświetlanie dodatkowych okien dialogowych podczas rejestracji jednokrotnej
	Ta sieć używa oddzielnych wirbualnych sieci LAN do uwierzytelnienia komputera i użytkownika

11. W poniższym okienku podajemy nasze NIU, po którym wpisujemy "@ue.poznan.pl" i hasło (uwaga - hasło, a nie numer PESEL) tak, jak przy logowaniu do e-dziekanatu.

والمستحد القريشي و			cupice positi
γ μεγικόψηικ	połączenie komputera z siecią, gd w celu pobrania aktualizacji).	ooświadczeń umożliwia ogowany (na przykłac	Zapisanie pośw nie jest zalogo
	ownīka	Nazwa użyt	SIR
		Hasło	
	WYTERO	Hasło	

12. Klikamy dwa razy **OK** i raz guzik **Zamknij**. Konfiguracja jest jednorazowa i nie wymaga ponownego wprowadzania NIU i hasła przy kolejnych połączeniach – powinny być nawiązywane automatycznie.

Zgodnie z przyjętą na UEP procedurą wszyscy nasi pracownicy i studenci (również doktoranci oraz osoby studiujące w ramach programu wymiany Erasmus) mają dostęp do systemu e-dziekanat/e-kadry <u>https://e-dziekanat.ue.poznan.pl</u>. Dane uwierzytelniające do tego systemu składają się z **NIU** (numer identyfikujący użytkownika) **oraz hasła.** Te dane służą również do uwierzytelnienia (zalogowania) się do sieci WiFi.

Studenci i pracownicy, którzy logują się do e-dziekanatu/e-kard wpisując w polu "NIU użytkownika" swój numer PESEL mogą odczytać przydzielony im identyfikator NIU na ekranie systemu e-dziekanat/e-kadry w linijce informacji o zalogowanej osobie.

Studenci i pracownicy nie znający swojego NIU mogą skorzystać z wyszukiwarki udostępnionej na stronie <u>http://sso.ue.poznan.pl/Niu.php</u> (w przypadku pracownika UEP) lub na stronie <u>http://sso.ue.poznan.pl/StudentNiu.php</u> (w przypadku studenta UEP), podając swoje nazwisko.

Procedura odzyskania hasła dostępna jest pod adresem

<u>https://e-dziekanat.ue.poznan.pl/register_pracownik.php</u> (w przypadku pracownika UEP) oraz pod adresem <u>https://e-dziekanat.ue.poznan.pl/register.php</u> (w przypadku studenta UEP).

Uwaga !

Jeśli czytasz ten dokument to znaczy, że nie jesteś zalogowany i w tej sytuacji odsyłacze do stron internetowych niestety nie zadziałają. Sugerujemy, więc zachować ten dokument do późniejszego wykorzystania.