

WLAN Verbindung mit eduroam unter Windows 10

Am DHBW CAS und an den Standorten der DHBW können Sie über eduroam eine Internetverbindung herstellen.

- Wählen Sie auf dem Startbildschirm die Desktop-App und klicken Sie mit der rechten Maustaste auf das WLAN-Symbol (unten rechts). Wählen Sie "Netzwerk- und Interneteinstellungen öffnen".
- 2. Wählen Sie "Netzwerk- und Freigabecenter".
- Wählen Sie "Neue Verbindung oder neues Netzwerk einrichten" und dann "Manuell mit einem Drahtlosnetzwerk verbinden".
 Hier tragen Sie als Netzwerkname die SSID eduroam ein und wählen als Sicherheitstyp

WPA2-Enterprise und als Verschlüsselungstyp AES.

÷	🔮 Manuell mit einem Funkr	netzwerk verbinden	
	Geben Sie Informatior möchten.	nen für das Drahtlosnetzwerk e	in, das Sie hinzufügen
	Netzwerkname:	eduroam	
	Sicherheitstyp:	WPA2-Enterprise \checkmark	
	Verschlüsselungstyp:	AES 🗸	
	Sicherheitsschlüssel:		Zeichen ausblenden
	Diese Verbindung auto Verbinden, selbst wen Warnung: Bei Auswał	omatisch starten n das Netzwerk keine Kennung aussende nl dieser Option ist der Datenschutz diese	et es Computers ggf. gefährdet.

Mit "Weiter" richten Sie die Verbindung ein.

Ist die eigentliche Verbindung eingerichtet, müssen noch das T-TeleSec Global Root Class 2 Zertifikat (falls noch nicht vorhanden – siehe unten) sowie Ihre DHBW CAS Benutzerdaten hinterlegt werden. Die nötigen Menüpunkte finden Sie unter "Verbindungseinstellungen ändern".



~	Manuell mit einem Funknetzwerk verbinden
	eduroam wurde erfolgreich hinzugefügt
	→ Verbindungseinstellungen ändern
	Öffnet die Verbindungseigenschaften, um die Einstellungen ändern zu können.

Unter Einstellungen wählen Sie bitte das T-TeleSec GlobalRoot Class 2 Zertifikat aus.

Eigenschaften für Draht	losnetzwerk eduroam	×
Verbindung Sicherheit		
Sicherheitstyp:	WPA2-Enterprise ~	
Verschlüsselungstyp:	AES ~	
Wählen Sie eine Metho	de für die Netzwerkauthentifizierung aus:	
Microsoft: Geschützte	Einstellungen	
Für diese Verbindu jede Anmeldung sp	ng eigene Anmeldeinformationen für eichern	
Erweiterte Einstellur	ngen	
	OK Abbrech	en



	>
Beim Herstellen der Verbindung:	
Identität des Servers mittels Zertifikatprüfung überpr	üfen
Verbindung mit folgenden Servern herstellen (Beispi "srv2", ".*\.srv3\.com"):	iele: "srv1",
Vertrauenswürdige Stammzertifizierungsstellen:	
Thawte Premium Server CA	^
thawte Primary Root CA	
thawte Primary Root CA - G3	
Thawte Timestamping CA	
T-TeleSec GlobalRoot Class 2	
UTN-USERFirst-Object	
VeriSign Class 3 Public Primary Certification Authori	ity - G5 🗸
<	>
Benachrichtigungen vor der Verbindungsherstellung:	
Benachrichtigungen vor der Verbindungsherstellung:	t Obarn and
Benachrichtigungen vor der Verbindungsherstellung: Benutzer benachrichtigen, wenn die Serveridentität nich	nt überp $\!$
Benachrichtigungen vor der Verbindungsherstellung: Benutzer benachrichtigen, wenn die Serveridentität nich	nt überp 🗸
Benachrichtigungen vor der Verbindungsherstellung: Benutzer benachrichtigen, wenn die Serveridentität nich Authentifizierungsmethode auswählen: Gesichertes Kennwort (EAP-MSCHAP v2) V	nt überp
Benachrichtigungen vor der Verbindungsherstellung: Benutzer benachrichtigen, wenn die Serveridentität nich Authentifizierungsmethode auswählen: Gesichertes Kennwort (EAP-MSCHAP v2) VK	nt überp
Benachrichtigungen vor der Verbindungsherstellung: Benutzer benachrichtigen, wenn die Serveridentität nich Authentifizierungsmethode auswählen: Gesichertes Kennwort (EAP-MSCHAP v2) V K Schnelle Wiederherstellung der Verbindung aktivieren Verbindung trennen, wenn Server kein Kryptografiebin vorweist	nt überp ∨ onfigurieren dungs-TLV
Benachrichtigungen vor der Verbindungsherstellung: Benutzer benachrichtigen, wenn die Serveridentität nich Authentifizierungsmethode auswählen: Gesichertes Kennwort (EAP-MSCHAP v2) V K Schnelle Wiederherstellung der Verbindung aktivieren Verbindung trennen, wenn Server kein Kryptografiebin vorweist	nt überp v onfigurieren dungs-TLV
Benachrichtigungen vor der Verbindungsherstellung: Benutzer benachrichtigen, wenn die Serveridentität nich Authentifizierungsmethode auswählen: Gesichertes Kennwort (EAP-MSCHAP v2) V K Schnelle Wiederherstellung der Verbindung aktivieren Verbindung trennen, wenn Server kein Kryptografiebin vorweist Identitätsschutz aktivieren	nt überp v onfigurieren dungs-TLV

Anschließend können noch Benutzername und Passwort hinterlegt werden, damit der Rechner die WLAN-Verbindung zu eduroam automatisch aufbauen kann. Dafür klicken Sie bitte auf "Erweiterte Einstellungen".



Eigenschaften für Draht	losnetzwerk eduroam	×
Verbindung Sicherheit		
Sicherheitstyp:	WPA2-Enterprise ~	
Verschlüsselungstyp:	AES 🗸	
Wählen Sie eine Metho	de für die Netzwerkauthentifizierung aus:	
Microsoft: Geschützte	es EAP (PEAP) 🗸 Einstellungen	
Für diese Verbindu jede Anmeldung sp	ng eigene Anmeldeinformationen für eichern	
Erweiterte Einstellu	ngen	
	OK Abbrech	en

Im folgenden Dialog stellen Sie bitte den Authentifizierungsmodus auf "Benutzerauthentifizierung". Um Ihre Daten zu hinterlegen, klicken Sie bitte auf "Anmeldeinformationen speichern".

Benutzerauth	entifizierung		\sim
Anmeldein Anmeldeinf	formationen speichern ormationen für alle Benutz	er löschen	
Einmaliges Anm	nelden für dieses Netzwerk	aktivieren	
Unmittelbar	r vor der Benutzeranmeldu	ıng ausführe	n
 Unmittelbar 	r nach der Benutzeranmelo	lung ausführ	en
Maximale Verz	ögerung (Sekunden):	10	*
Anzeige zu: Anmeldens	sätzlicher Dialoge während zulassen	des einmali	gen
In diesem M Benutzerau verwendet	letzwerk werden für die C Ithentifizierung separate v	omputer- un irtuelle LANs	d die



Als Anmeldedaten geben Sie bitte Ihre DHBW CAS Benutzerkennung <Benutzerkennung>@cas.dhbw.de und Ihr Passwort ein. Bestätigen Sie mit "OK" und die Verbindung wird aufgebaut.

Root Zertifikat nachinstallieren

Das Root-Zertifikat der Telekom müssen Sie nur nachinstallieren, wenn es auf Ihrem Computer noch nicht vorhanden ist - siehe oben.

Das Prüfen der Identität der Authentifizierungsserver wird dringend empfohlen. Dazu muss das Stammzertifikat der Telekom auf dem lokalen System installiert sein. Ist das nicht der Fall, kann der Client nicht testen, ob er bei der Authentifizierung mit einem offiziellen Server kommuniziert. Ist die Prüfung deaktiviert, so kann das eigene Password gestohlen und der eigene Account missbraucht werden.

Das Stammzertifikat der Telekom finden Sie über den Link: https://www.pki.dfn.de/wurzelzertifikate/globalroot2/

Markieren Sie unter der Überschrift Formate mit der rechten Maustaste die Dateierweiterung .crt und wählen Sie aus dem Menü den Punkt "Speichern unter". Speichern Sie das crt-File an einem beliebigen Ort, z. B. auf dem Desktop. Führen Sie anschließend einen Doppelklick auf das gespeicherte File aus und folgen Sie dem Dialog. Sie können alle Voreinstellungen der Zertifikatsimport-Assistenten übernehmen.