LAN

- LAN in Hörsälen
  - Einrichtung von 802.1X unter Windows
  - Einrichten von 802.1X unter MacOS
- MAC-Adress-Management an Dockingstationen
- Netze für IT-Systeme ohne Support

LAN in Hörsälen

Zur Unterstützung der Lehre, gerade auch in hybriden Veranstaltungen, werden sukzessive die Netzwerkanschlüsse in den Redner- bzw. Bühnenbereichen der Hörsäle mit sicherem kabelgebundenen Netzwerk versorgt.

An diesen Anschlüssen ist die Netzwerkanmeldung - vergleichbar mit dem eduroam - mittels Authentifizierung nach 802.1x erforderlich.

Die hierfür erforderlichen Konfigurationen finden Sie auf den folgenden Seiten.

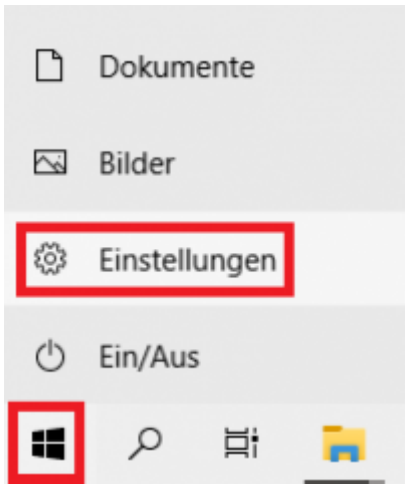
Einrichtung von 802.1X unter Windows

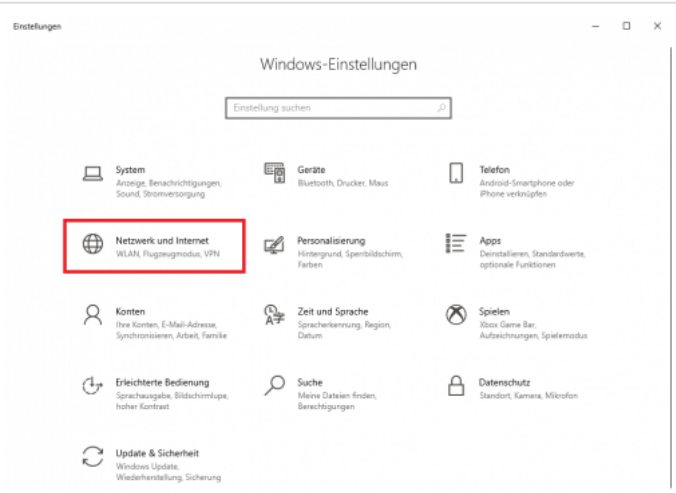
Für den Betrieb von Windows-Geräten an Netzwerkanschlüssen mit 802.1x Authentifizierung müssen zwei Vorbereitungen getroffen werden:

1. Aktivierung des Windows-Dienstes für kabelgebundene Netzwerkadapter.
2. Einrichtung der Authentifizierung für diesen Anschluss an der TU Braunschweig.
3. (Eingabe der Zugangsdaten).

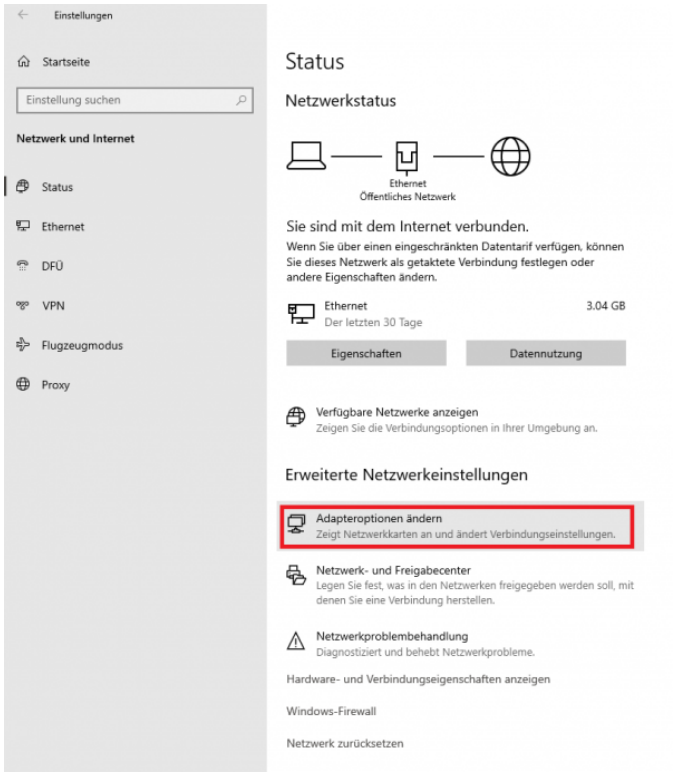
1. Aktivierung des Windows-Dienstes

In den Standardinstallationen von Windows ist der notwendige Dienst „Automatische Konfiguration (verkabelt)“ in der Regel deaktiviert. Dieser muss gestartet und sinnvollerweise als automatisch startender Dienst konfiguriert werden.

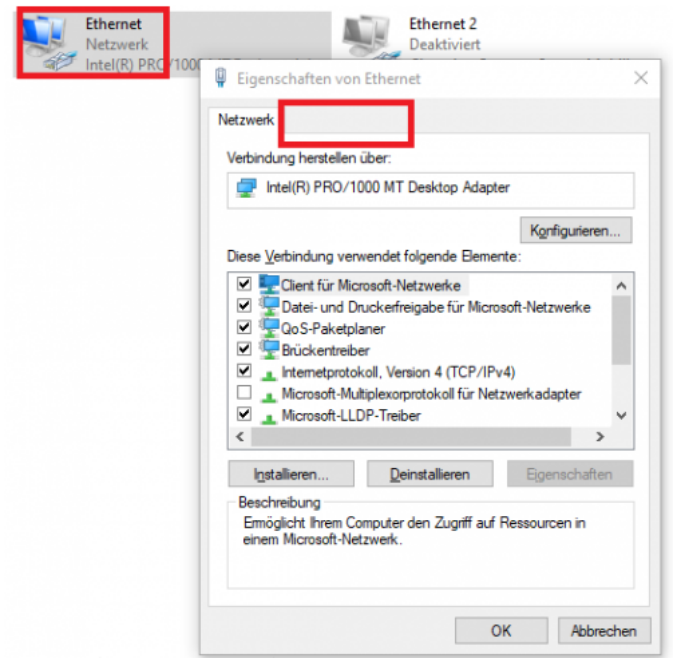
	Im Startmenü die **Einstellungen** öffnen.



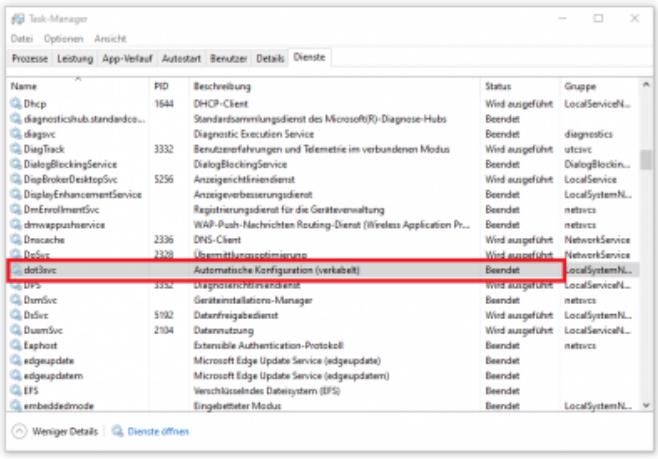
Anschließend in den Einstellungen den Punkt **[Netzwerk und Internet]** auswählen.



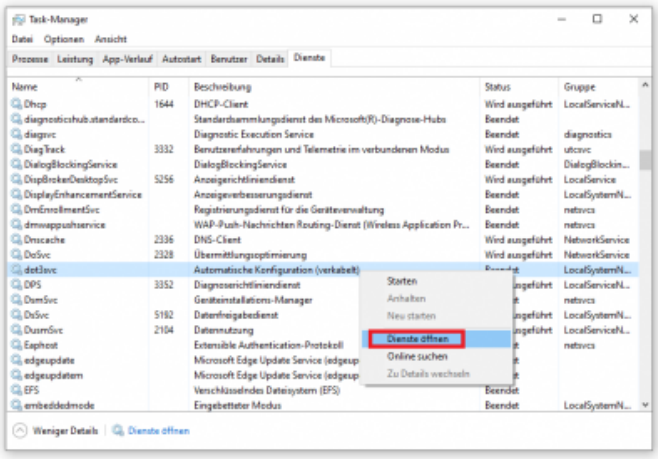
Hier in der linken Spalte entweder unter „Status“ oder unter „Ethernet“(auch LAN-Verbindung) die **[Adapteroptionen ändern]**.



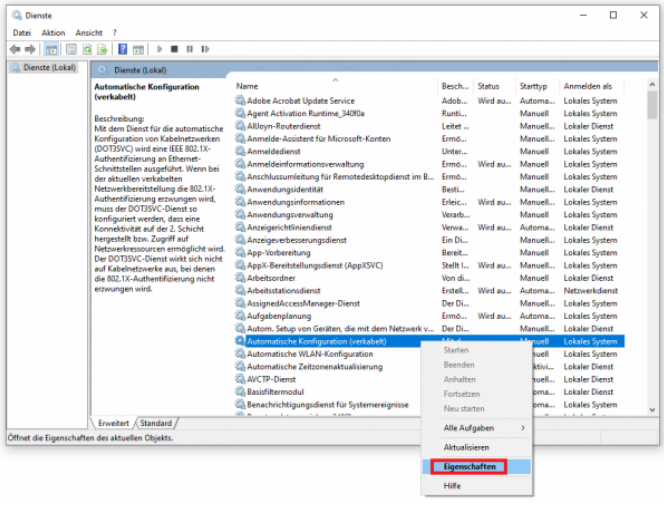
Hier mit Rechtsklick auf dem Kabel-Netzwerkadapter die Eigenschaften auswählen.
Fehlt hier im roten Kästchen der Punkt „Authentifizierung“, so muss der Diest aktiviert werden.
(**Hinweis** diese Verbindung kann durchaus andere Namen haben, sollte aber mit einem Steckersymbol gekennzeichnet sein.)



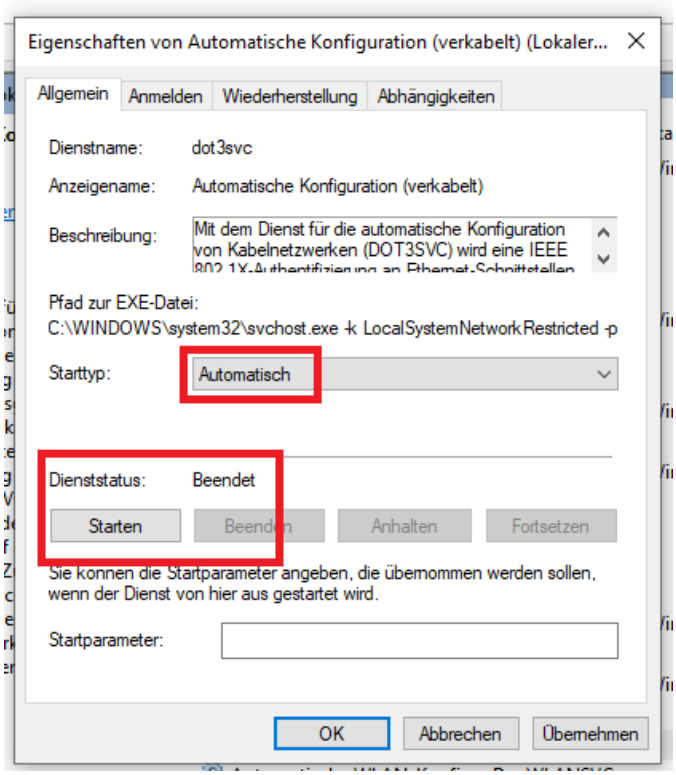
Sollten Sie Administratorrechte haben, können Sie den Status direkt im Taskmanager verifizieren.



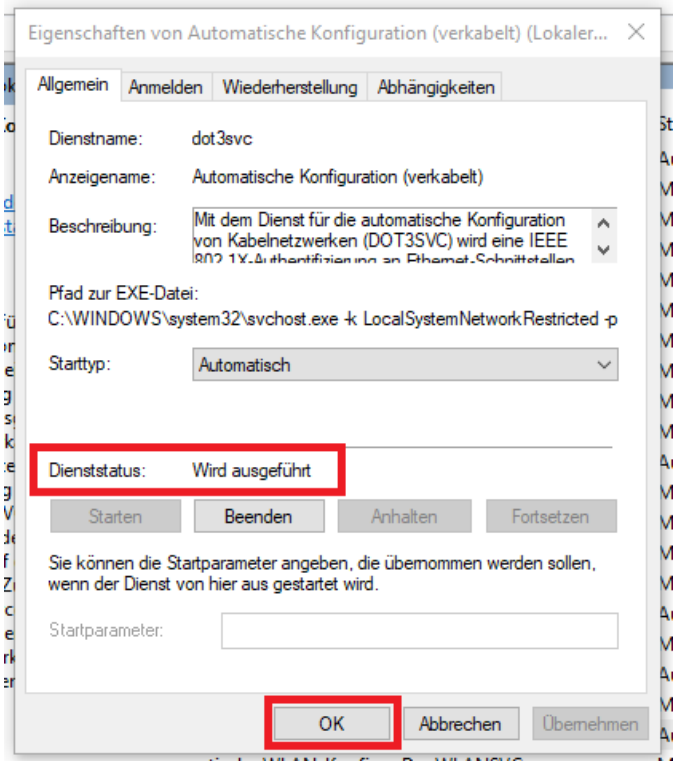
Hier ist es möglich zur Diensteverwaltung zu wechseln.



Hier werden zwingend Adminstratorrechte auf dem Gerät benötigt. Kontaktieren Sie ggf. bitte den Admin/Koordinator Ihrer Organisationseineit.
Auswahl des Dienstes **[Automatische Konfiguration (verkabelt)] → [Eigenschaften]**

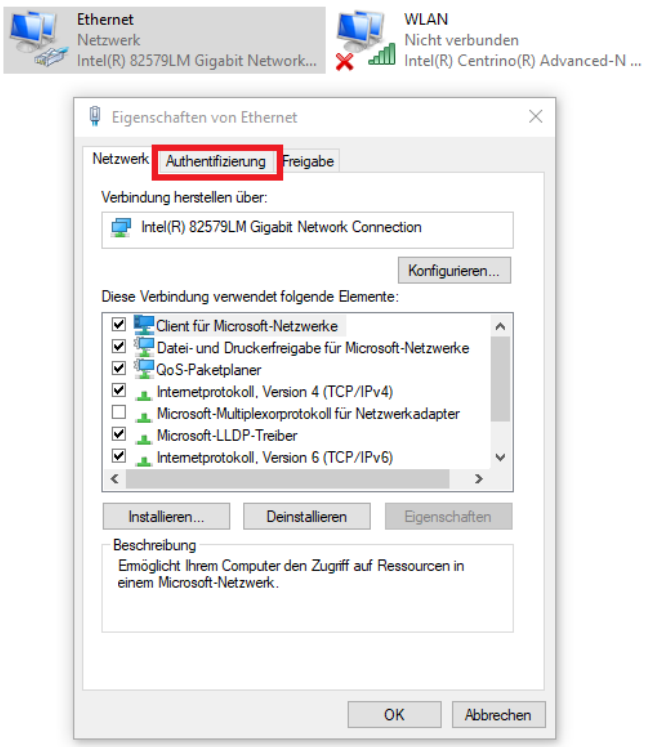


Wechsel auf Automatischen Start in der Auswahlliste und Start.



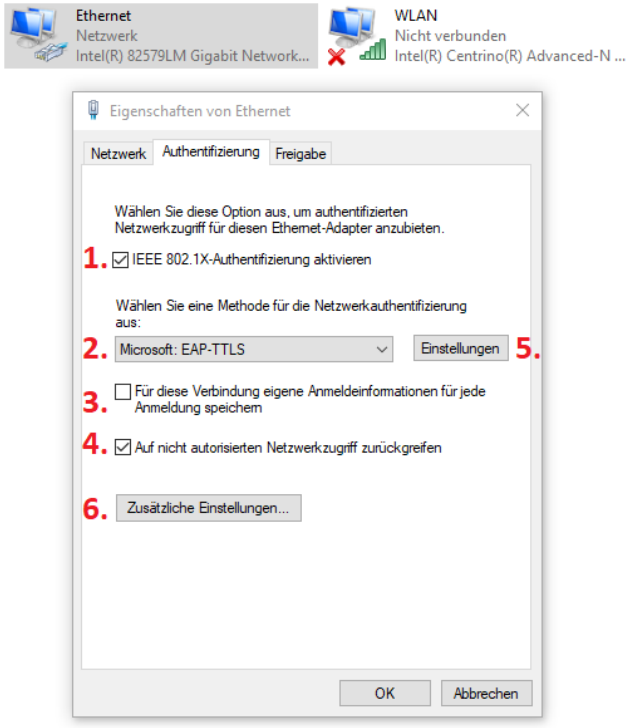
Verifizierung des Status des Dienstes und Bestätigen der Einstellungen mit **[OK]**.

2. Einrichtung der Authentifizierung



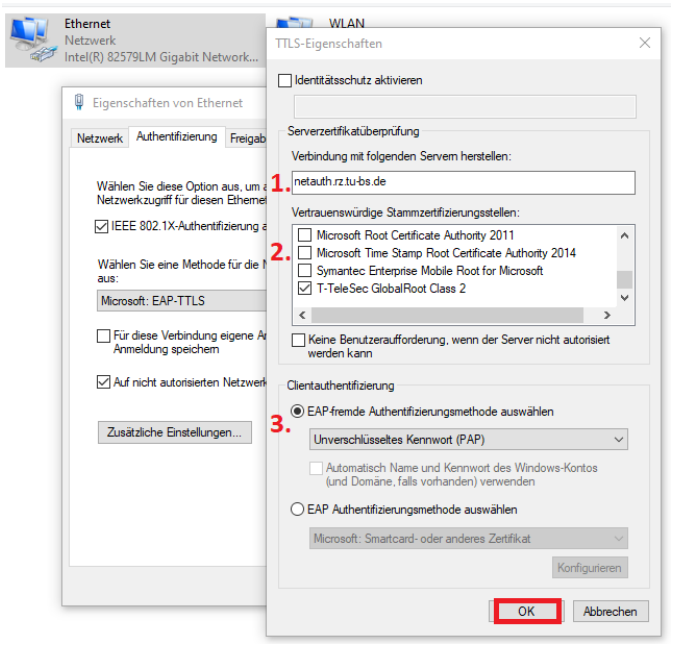
Ist der o.g. Dienst aktiv können Sie in den Adaptereinstellungen die Konfiguration starten.
Zur Erinnerung: **[Startmenü]** → **[Einstellungen]** → **[Netzwerk und Internet]** → **[Status]** → **[Adapteroptionen ändern]** → Rechtsklick auf **[LAN-Adapter]**.

Auch hier werden für die erste Einrichtung Admin-Rechte benötigt. Die Zugangsdaten werden dann vom Benutzer bei Verbindung mit dem Netzwerk eingegeben.



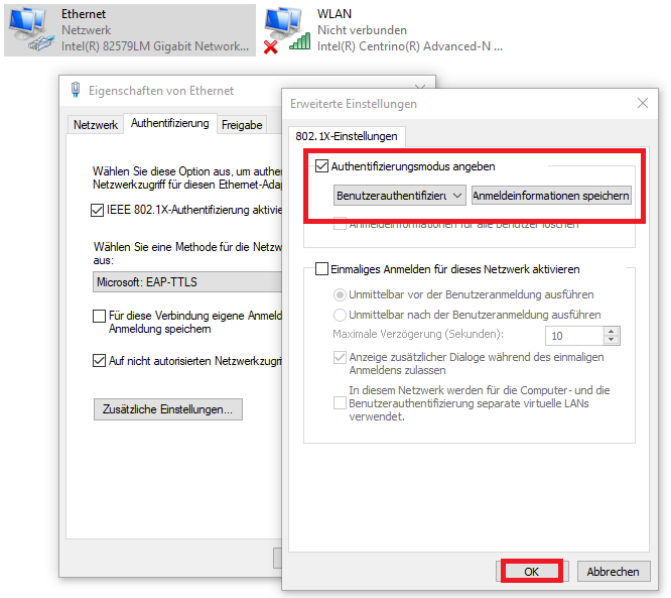
Die Einstellungen in den Punkten 1-4 bitte übernehmen und anschließend in Punkten 5 und 6 anschließend die folgenden Einstellungen vornehmen.

Sollen die Anmeldeinformationen für alle Verbindungen hinterlegt werden, bitte in Punkt 3 aktivieren.



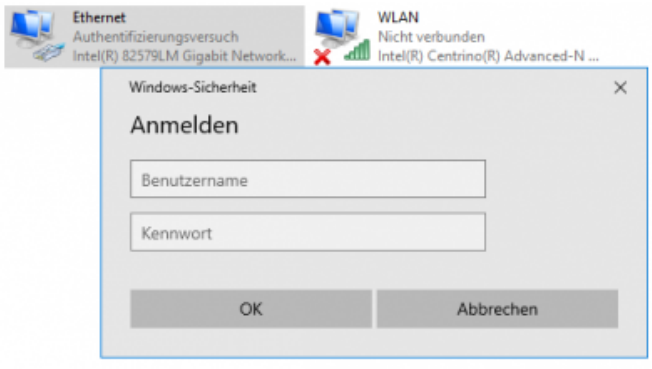
Zu Punkt 5:

Identitätsschutz möglich aber zwingend nicht notwendig.
1. Server netauth.rz.tu-bs.de
2. Stammzertifikatsstellen „T-Telesec GlobalRoot Class 2“ und „AAA Certificate Services“
3. PAP Kennwort



Zu Punkt 6:

Benutzerauthentifizierung auswählen, Hier können direkt Zugangsdaten hinterlegt werden.



In der Regel werden diese aber auch bei der ersten Verbindung mit dem Netzwerk abgefragt.

Hier bitte analog zur eduroam Konfiguration bei Benutzername ihre TUBS-ID gefolgt von "@tu-braunschweig.de" (z.B. "maxmuste@tu-braunschweig.de") oder nur die TUBS-ID mit dem normalen Passwort der TU Braunschweig eintragen.

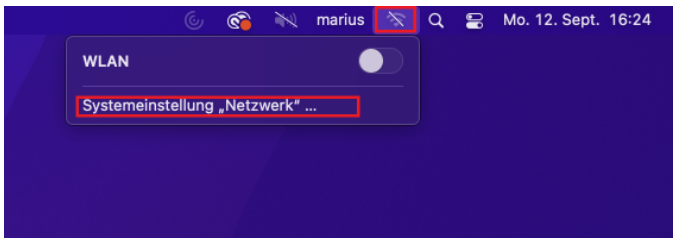
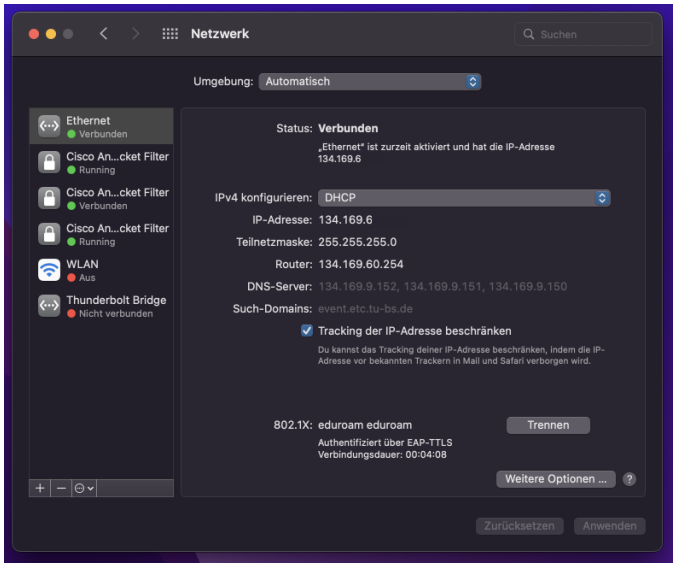
tl;dr Parameter

- 802.1x Dienst für LAN aktivieren: WiredAutoConf dot3svc
- EAP-TTLS mit PAP
- Server netauth.rz.tu-bs.de
- Stammzertifikatsstellen „T-Telesec GlobalRoot Class 2“ und „AAA Certificate Services“
- Benutzerauthentifizierung
- Identitätsschutz und Speichern der Zugangsdaten optional

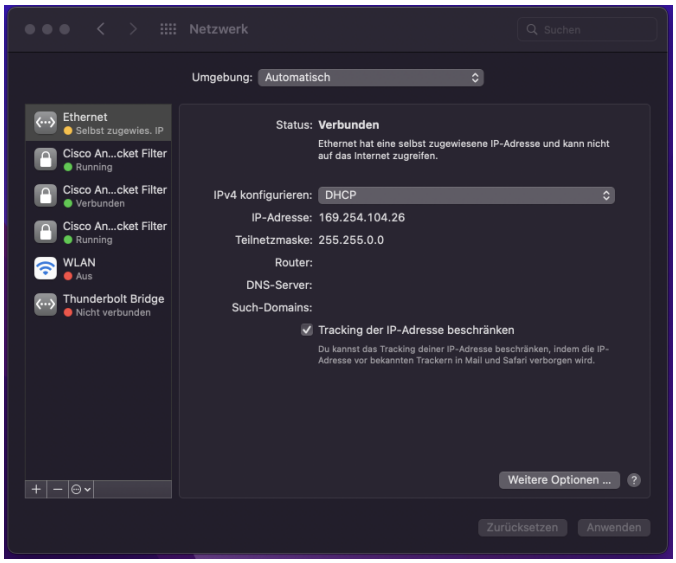
Einrichten von 802.1X unter MacOS

Einrichtung durch Übernahme der Parameter vom eduroam-Profil

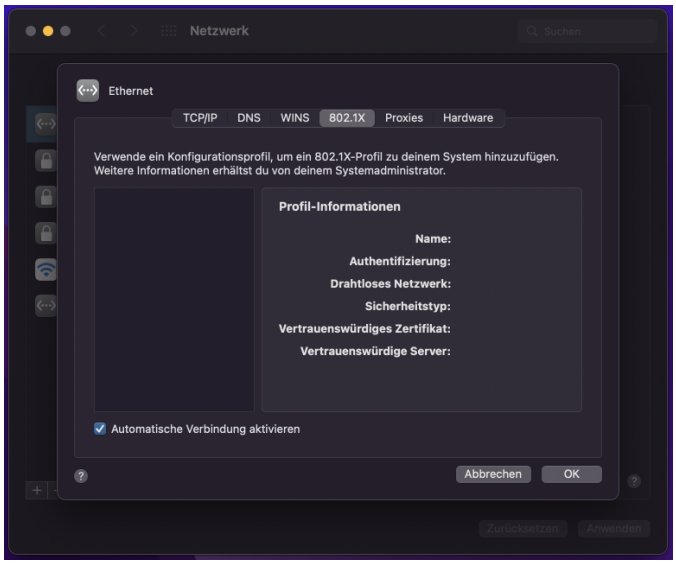
Die Netzwerkverwaltung von macOS Geräten kann grundsätzlich die 802.1x Parameter des eduroam-Konfigurationsprofil übernehmen und sich direkt mit dem kabelgebundenen Netz authentifizieren.
Dies können Sie in den Systemeinstellungen Netzwerk nachvollziehen:

	**[Systemeinstellungen Netzwerk]** öffnen.
	Unten erkennen Sie das verwendete Profil.

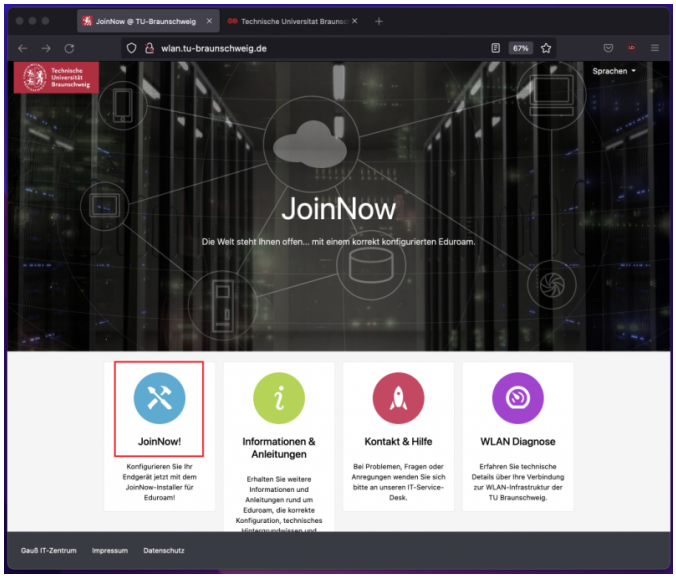
Konfigurationsprofil hinzufügen



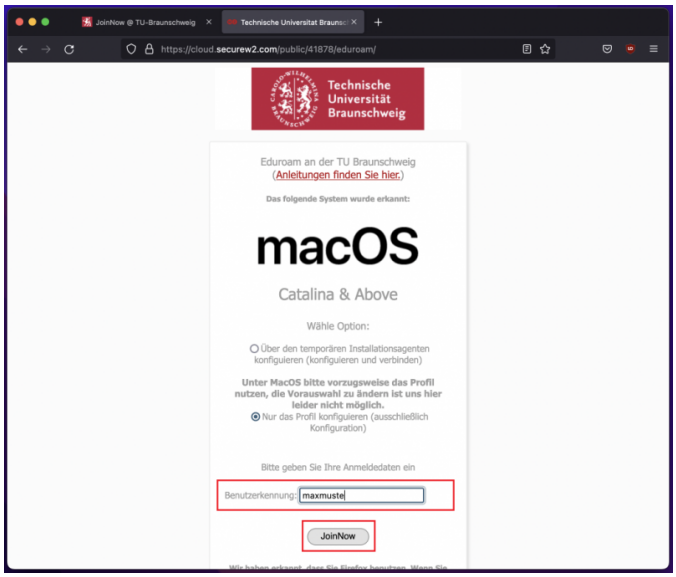
Sollten Sie noch keine solche Konfiguration haben, wird der Status entsprechend so aussehen: Ethernet ist zwar als verbunden markiert wird aber nicht akzeptiert und hat eine ungültige lokale IP-Adresse.



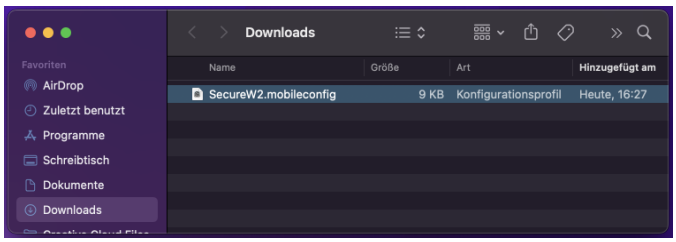
Die 802.1x Einstellungen sind leer, es wird auf ein Konfigurationsprofil verwiesen.



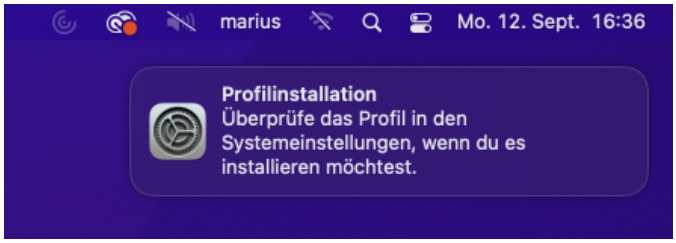
Dieses Profil können Sie z.B. von der Website JoinNow oder dem Administrator/ Koordinator Ihrer Organisationseinheit erhalten.
Sollten Sie zu diesem Zeitpunkt keine weitere Netzwerkverbindung haben, können Sie sich auch vorübergehend im unverschlüsseltem Netzwerk tubs-guest anmelden.



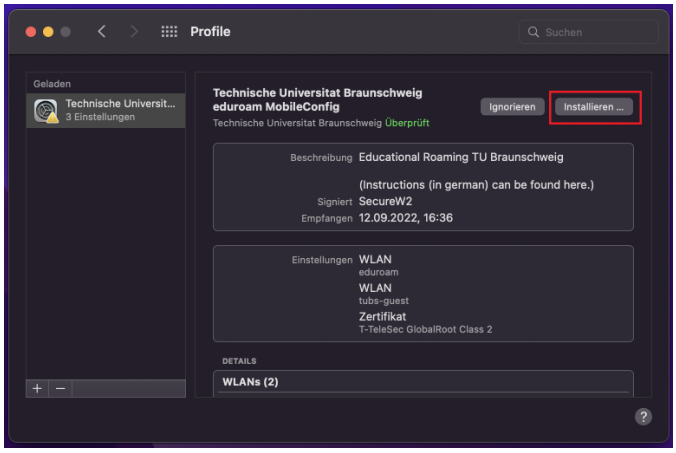
Auswahl des Konfigurationsprofils und Eingabe der Benutzerkennung → JoinNow



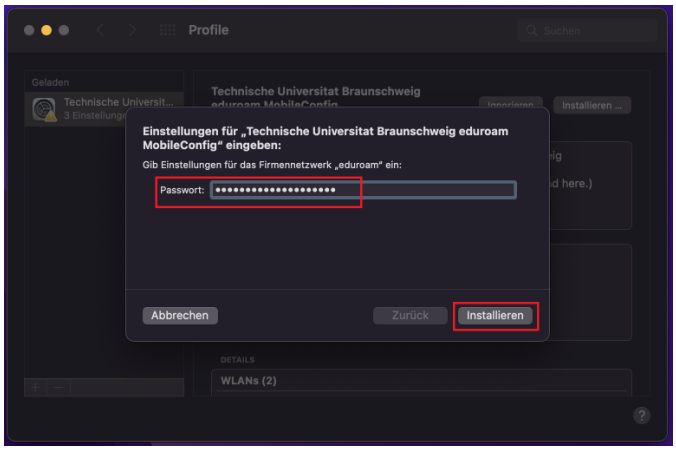
Konfigurationsprofil im Downloadverzeichnis ausführen.



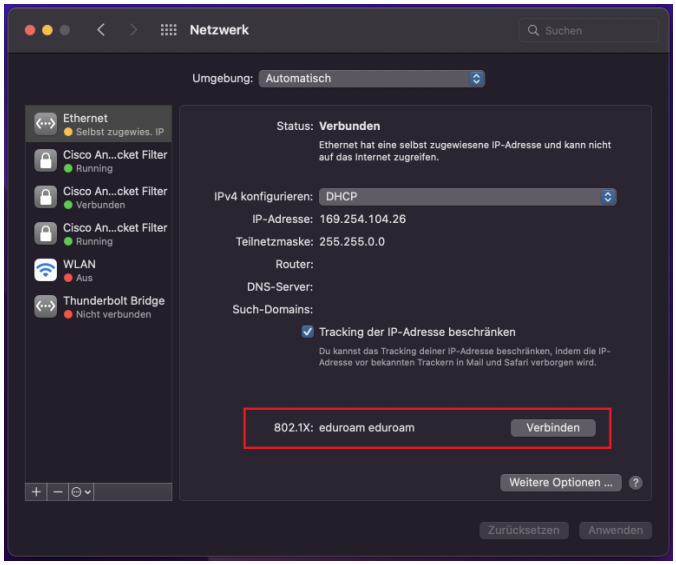
Dialog zum Profil-Hinzufügen.



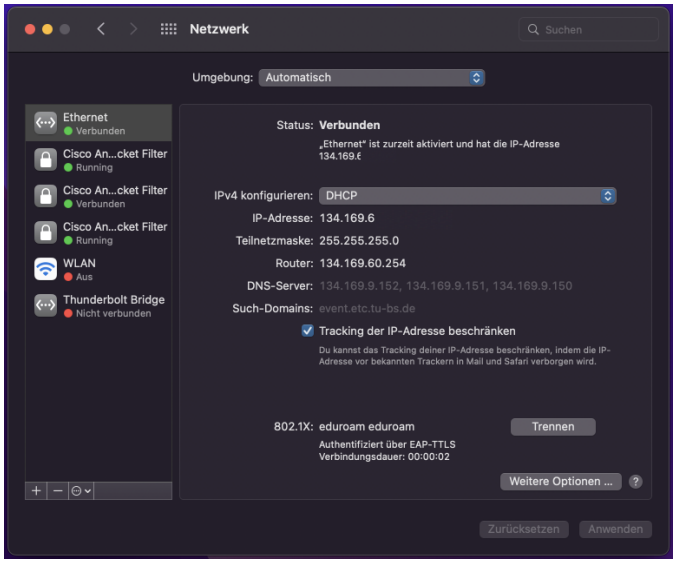
[Systemeinstellungen] → [Profile]
Dort das Konfigurationsprofil installieren.



Das Passwort für die TUBS-ID angeben und eine Administratorabfrage im darauffolgenden Dialog bestätigen.



[Systemeinstellungen] → [Netzwerk]
Hier kann nun die Verbindung mit dem Konfigurationsprofil mit Klick auf **[Verbinden]** bestätigt werden.


Netzwerk
Suchen
Umgebung: Automatisch
Ethernet
Verbunden
Cisco An...cket Filter
Running
Cisco An...cket Filter
Verbunden
Cisco An...cket Filter
Running
WLAN
Aus
Thunderbolt Bridge
Nicht verbunden
Status: Verbunden
„Ethernet" ist zurzeit aktiviert und hat die IP-Adresse 134.169.6
IPv4 konfigurieren: DHCP
IP-Adresse: 134.169.6
Teilnetzmaske: 255.255.255.0
Router: 134.169.60.254
DNS-Server: 134.169.9.152, 134.169.9.151, 134.169.9.150
Such-Domains: event.etc.tu-bs.de
Tracking der IP-Adresse beschränken
Du kannst das Tracking deiner IP-Adresse beschränken, indem die IP-Adresse vor bekannten Trackern in Mail und Safari verborgen wird.
802.1X: eduroam eduroam
Trennen
Authentifiziert über EAP-TTLS
Verbindungsdauer: 00:00:02
Weitere Optionen ...
Zurücksetzen
Anwenden

Erfolg!

MAC-Adress-Management an Dockingstationen

Werden Laptops an Dockingstationen mit dem kabelgebundenen Campusnetzwerk verbunden, so muss in der Regel darauf geachtet werden, dass die korrekten Hardware-Adressen ("MAC-Adressen") der Netzwerkadapter an das Campusnetzwerk durchgereicht werden.

Nur wenn die identische MAC-Adresse des mobilen Geräts - und nicht die der verwendeten Dockingstation - übermittelt wird, funktioniert z.B. die Zuweisung von IP-Adressen des Netzbereichs der Einrichtung per statischem DHCP.

Dies ist insbesondere bei aktuellen Ein-Kabel-Lösungen per USB-C / Thunderbolt der Fall.

Hintergrund

Je nach verwendeter Baureihe von z.B. Dell-Dockingstationen sind dort interne Netzwerkadapter mit eigenen MAC-Adressen verbaut, die eine Zuweisung von IP-Adressen bei wechselnden Geräten/Nutzern am gleichen Dock oder wechselnden Arbeitsplätzen eines Nutzers verhindern würden.

MAC-Adress-Passthrough

Die Lösung für dieses Problem ist das sog. „MAC-Address-Passthrough“ bei dem das Netzwerkgerät in der Dockingstation die z.B. im DHCP-Bereich des KDD hinterlegte MAC-Adresse des Laptops an das Campusnetzwerk weiterreicht.

Dell liefert hierzu einen kleinen Artikel in der Knowledgebase: Dell-KB

Voraussetzung für den erfolgreichen Einsatz dieses Features ist:

1. Aktueller Patch-Stand des Systems und Dock-Firmware, z.B. per Dell-Command-Update während Dock und Laptop verbunden sind.
2. Aktivierung dieses Feature im UEFI/BIOS des Laptops. Diese Option ist je nach Gerät und Patchlevel unter „Pre-Boot Behaviour“ oder „System-Configuration“ → „MAC Address Pass-through“ zu finden.

3. Korrekte Erfassung der LAN-MAC-Adresse des Laptops im KDD oder lokalem DHCP der Einrichtung.

Netze für IT-Systeme ohne Support

Systeme, die vom Hersteller nicht länger mit Sicherheits-Updates etc. versorgt werden, dürfen an der TU Braunschweig laut der "Richtlinie zum Umgang mit IT-Systemen ohne Support" nur noch im Rahmen eines Ausnahmeverfahrens und ggf. unter Auflagen (nach Genehmigung des IT-Security-Boards) betrieben werden. Eine Möglichkeit zum Weiterbetrieb besteht in der Ausgliederung dieser Systeme in ein privates, vom Rest der IT an der TU-Braunschweig gekapseltes lokales Netzwerk (... siehe Handreichung der Stabsstelle CISO zur oben genannten Richtlinie). Dies wird von der Abteilung Netze am Gauß-IT-Zentrum wie folgt unterstützt, wobei die vorliegende Handreichung lediglich ein (mit der Stabsstelle CISO abgestimmtes) Konzept beschreibt, das von den Einrichtungen jedoch in Eigenverantwortung umgesetzt werden muss.

Wie sieht ein solcher Aufbau aus?

Ganz einfach gesagt wird für die alten Systeme ein separates Netz gebaut. Dies kann, je nach lokalen Gegebenheiten wie folgt geschehen:

- Systeme stehen physisch nah beieinander: Die Systeme werden über einen separaten, lokalen Switch vor Ort miteinander verbunden. Eine Datenschleuse (s.u.) erhält ggf. einen Anschluss an diesen Switch und einen Anschluss an eine normale Netzwerkdose (oder wird direkt an ein betroffenes einzelnes System angeschlossen).
- Systeme sind über die Etage/Gebäude verteilt, aber über **einen** Switch an die Infrastruktur der TU-Braunschweig angebunden: Es wird ein lokales Vlan auf diesem Switch angelegt, in dem nur diese Geräte miteinander verbunden werden. Eine Datenschleuse (s.u.) wird mit je zwei Datendosen verbunden, von denen eine in das lokalen Vlan, die andere in ein reguläres Vlan geschaltet ist.
- Systeme sind über mehrere Etagen/Gebäude verteilt (und über mehrere Switche an die Infrastruktur der TU-Braunschweig angebunden): Die Geräte können zur Zeit nicht gemeinsam in einem Netz gekapselt werden. Es müssen ggf. mehrere lokale Netze (s.o.) angelegt werden.

Wie kann man den Austausch von Daten zwischen den IT-Systemen ohne Support und der restlichen Welt lösen? (Stichwort "Datenschleuse")

Der Austausch von Daten zwischen den nicht mehr supporteten System und dem Rest der IT ist als kritisch zu bewerten und muss über eine "Datenschleuse" erfolgen, die Kompromittierungen in beide Richtungen ausschließt. D.h. Daten, die von den nicht supporteten Systemen auf regulär betriebene Systeme übertragen werden sollen, müssen vorher zunächst auf dieses System übertragen und nach aktuellem Stand der Technik auf Viren etc. untersucht werden. Gleiches gilt in die andere Richtung.

Solche Datenschleusen können in der Praxis auch Rechner sein, die über zwei Netwerkkarten verfügen, und jeweils mit "einem Bein" im privaten/lokalen Netz mit den nicht supporteten Systemen stehen und mit dem anderen Bein in einem regulären Netz. Dabei muss es sich bei diesem Rechner in jedem Fall um ein vom Hersteller des Betriebssystems noch unterstütztes (jederzeit vollständig gepatchtes) System handeln, dass ebenso über Virenscanner mit jederzeit aktuellen Virensignaturen etc. verfügt und die Daten vor Weiterübertragung in beide Richtungen überprüft. Dieses System darf zudem nicht von außerhalb des Netzes zugreifbar sein (FW-Regeln auf Instituts-Firewall) und muss auch über die lokale Firewall so weit wie möglich geschützt werden.

> Was ausdrücklich **nicht** passieren darf, ist der **Austausch von Daten über Wechselmedien** (USB-Sticks und co.) ohne Überprüfung auf Kompromittierung mit aktuellen Virenscannern etc.

Kann ich dann aus dem "Alt-Netzwerk" z.B auf Netzlaufwerke zugreifen (Isilon)?

Nein. Das darf so nicht umgesetzt werden, weil das den ganzen Aufwand zur Kapselung wieder in Frage stellt. Die Daten sollten immer nur auf einer Datenschleuse (s.o.) abgelegt werden, die z.B. in beiden Welten steht und auf der ein Virenscanner läuft, der die Transferdaten in beide Richtungen prüft.

Habe ich von dort aus Zugang zum Internet?

Nein. Ziel der Kapselung ist die beidseitige Trennung der nicht supporteten Systeme vom Rest der IT.

Kann man mittels Fernwartprogrammen wie Rustdesk (ähnlich Teamviewer, aber Open Source) auf die Altgeräte zugreifen?

Jein. Sinnvoll ist dies eigentlich nur über den Weg der Datenschleuse (s.o.), die dann in jedem Fall mit beiden Netzen verbunden sein muss. Als Software-Lösung können hier z.B. die OpenSource Software https://guacamole.apache.org/ (Linux) in Frage kommen.