WLAN

Wir bieten WLAN im Rahmen des eduroam-Verbundes an.

Der Name *eduroam* steht für "education roaming" und ist ein internationales, sicheres und verschlüsseltes WLAN-Netzwerk, das speziell für Bildungseinrichtungen wie Universitäten, Forschungseinrichtungen und Schulen entwickelt wurde. Durch eduroam können Angehörige dieser Einrichtungen weltweit kostenlos und einfach auf das Internet zugreifen, indem sie sich mit ihren eigenen Anmeldeinformationen bei einem eduroam-fähigen WLAN-Netzwerk anmelden. Dadurch sind sie nicht mehr auf lokale Hotspots oder teure Datenverbindungen angewiesen, wenn sie sich innerhalb oder außerhalb ihrer Heimatinstitution befinden.

Zum einrichten der Verbindung zum eduroam bieten wir an: geteduroam-App

- JoinNow! - Abgekündigt zum August 2027
- eduroam mit der geteduroam-App einrichten
- Set up eduroam with the geteduroam app
- WLAN-Paramter
    - Parameter
- Konferenz- und Gast-Netz tubs-guest
- Instituts-WLAN
    - Was ist Instituts-WLAN? (Für DV-Koordinatoren)
    - Instituts-WLAN beantragen & nutzen (für DV-Koordinatoren)
    - Instituts-WLAN nutzen (Benutzer)
    - FAQ
- FAQ
- Zertifikatswechsel im eduroam 2027
- eduroam Certificate Change 2027

JoinNow! - Abgekündigt zum August 2027

Hinweis:

eduroam kann ab sofort auch mit der **geteduroam-App** sicher eingerichtet werden. Die App lädt das passende Profil für die TU Braunschweig herunter und richtet die Verbindung automatisch korrekt ein.

Der Support für den SecureW2-JoinNow-Client wird letztmalig um ein Jahr verlängert und endet am **9. August 2027**.

eduroam can now also be securely configured using the **geteduroam app**. The app downloads the appropriate profile for TU Braunschweig and automatically configures the connection with the correct settings.

Support for the SecureW2 JoinNow client has been extended for one final year and will end on August 9, 2027.

eduroam mit der geteduroam-App einrichten

Die **geteduroam-App** hilft dabei, eduroam auf Smartphone, Tablet oder Laptop **schnell und sicher** einzurichten. Die App übernimmt die passenden WLAN-Einstellungen für die TU Braunschweig und sorgt dafür, dass Sie sich mit einem korrekt konfigurierten eduroam verbindet. Dadurch wird auch die sichere Prüfung des Server-Zertifikats unterstützt.

Wenn es zu Problemen mit eduroam kommt, kann es helfen das Profil und die WLAN-Einstellungen zu löschen und eduroam erneut einzurichten.

> **Hinweis:** Wenn es zu Problemen mit eduroam unter iOS kommt, kann es helfen das Profil und die WLAN-Einstellungen zu löschen und eduroam erneut einzurichten.

> Das WLAN-Profil wurde am 03.08.2026 akualisiert.
> Seit dem 3. August 2026 enthält das über geteduroam bereitgestellte eduroam-Profil zusätzlich zur bisherigen Telekom-Zertifikatskette auch die neue DFN eduroam CA, um die Endgeräte frühzeitig auf den anstehenden Zertifikatswechsel der eduroam-Authentifizierung vorzubereiten und einen möglichst unterbrechungsfreien Übergang zu ermöglichen.
> Halten Sie die Konfiguration von ihrem Gerät auf dem neusten Stand, damit es in Zukunft zu keinen Problemen kommt.
> Installieren Sie das Profil erneut um die neusten Einstellungen zu bekommen.

Bevor Sie starten

Für die Einrichtung benötigt man:

- eine **Internetverbindung während der Ersteinrichtung**,
  - Sie können eduroam auch bequem von zu Hause oder von einem anderen Standort aus einrichten.
  - Ihr Gerät wird sich dann automatisch mit dem eduroam verbinden, sobald es in der Nähe ist
- Falls Sie noch den SecureW2-Client installiert haben, deinstallieren Sie diesen, dabei verlieren Sie die Verbindung zum eduroam
- > benutzen Sie **NICHT** den CAT-Installer von https://cat.eduroam.org/ da dieser keine Unterstützung von uns bekommt

Schritt-für-Schritt-Einrichtung

1. **Laden Sie die geteduroam-App herunter.**
   Die App gibt es für **Android**, **MacOS, iPhone/iPad**, **Windows** und **Linux**.
   Unter Linux ist die App unter anderem über **Flathub** verfügbar.

Die App kann per **Google Play Store, Apple Store** und **F-Droid** bezogen werden.
Hier finden Sie eine Übersicht der Apps

- Für Linux: Flathub oder Github für Paket-Installationen
- Für Microsoft Windows stehen zwei Versionen der geteduroam-App zur Verfügung. Wählen Sie die passende Version für ihr Gerät aus:
  - Windows(Intel/AMD):Für die meisten PCs und Laptops mit Intel- oder AMD-Prozessor
  - Windows(ARM): Für Geräte mit ARM-Prozessor, beispielsweise bestimmte Microsoft-Surface-Modelle

2. **Öffnen Sie die App und suchen nach "Technische Universität Braunschweig"**
3. **Melden Sie sich an mit ihrer TUBS-ID und ihrem Passwort**
4. **Bestätigen Sie die Einrichtung.**
   Die App richtet das WLAN-Profil für Sie ein. Danach sollte sich Ihr Gerät automatisch mit **eduroam** verbinden, sobald das Netz in Reichweite ist.
5. **Lassen Sie die App installiert.**
   Das ist sehr wichtig: Wenn Sie die geteduroam-App wieder deinstallieren, wird auch die von ihr eingerichtete **eduroam-Konfiguration entfernt**. Die App sollte also installiert bleiben, solange Sie eduroam nutzen.

Beispielhaftes Video zur Einrichtung auf Windows - die Einrichtung kann auf anderen Plattformen leicht abweichen:

FAQ

- Es kommt die Fehlermeldung *Verbindung fehlgeschlagen cannot modify system configuration* unter iOS
  - Lösung: Gehen Sie in die iOS-Einstellungen ? Allgemein ? VPN & Geräteverwaltung. Dort können Sie Eduroam-Profile löschen und anschließend mit geteduroam neueinrichten.

Set up eduroam with the geteduroam app

The **geteduroam app** helps you set up eduroam on your smartphone, tablet or laptop **quickly and securely**. The app automatically applies the correct Wi-Fi settings for TU Braunschweig and ensures that your device connects to eduroam using a properly configured profile. It also enables secure validation of the authentication server’s certificate.

> **Note:** If you experience problems with eduroam on iOS, it may help to remove the profile and Wi-Fi settings and then set up eduroam again.

> **Current information: The Wi-Fi profile was updated on 3 August 2026.**
> **Since 3 August 2026, the eduroam profile provided through geteduroam has included the new DFN eduroam CA in addition to the existing Deutsche Telekom certificate chain. This prepares devices in advance for the upcoming change to the certificate used for eduroam authentication and helps ensure a smooth transition without interruptions.**

K**eep the configuration on your device up to date to prevent connection problems in the future.**

R**einstall the profile to obtain the latest settings.**

Before you start

You will need:

- an **internet connection during the initial setup**
  - You can also easily set up eduroam from home or any other location
  - Your device will automatically connect to eduroam as soon as the network is within range
- > **DO NOT** use the CAT installer from https://cat.eduroam.org/, as we do not provide support for it

Step-by-step instructions

1. **Download the geteduroam app.**
   The app is available for **Android**, **iPhone/iPad**, **Windows** and **Linux**.
   On Linux, the app is available from sources including **Flathub**. The app can also be downloaded from the Google Play Store and F-Droid.

   You can find an overview of the available apps here.

   - For Linux: Flathub or Github for package releases
   - Two versions of the geteduroam app are available for Microsofrt Windows. Please select the version that matches your device:
     - Windows (Intel/AMD): For most PCs and laptops with Intel or AMD processors
     - Windows (ARM): For devices with ARM processors, such as certain Microsoft Surface Models
2. **Open the app and search for “Technische Universität Braunschweig”.**
3. **Sign in.**
   - Enter your **TUBS ID and password** as provided by your institution.
     Use the following format for your username: `TUBS-ID@tu-braunschweig.de`
4. **Confirm the setup.**
   The app will install the Wi-Fi profile for you. Your device should then automatically connect to **eduroam** whenever the network is within range.
5. **Keep the app installed.**
   This is very important: If you uninstall the geteduroam app, the **eduroam configuration installed by the app will also be removed**. You should therefore keep the app installed for as long as you use eduroam.

E**xample video showing the setup process on Windows—the process may differ slightly on other platforms:**

FAQ

- Error message: Connection failed – cannot modify system configuration with iOS
  - Solution*:* Go to iOS **Settings → General → VPN & Device Management**. There you can remove existing eduroam profiles and then set up eduroam again using geteduroam.

WLAN-Paramter

Parameter

Verwenden Sie bitte ausschließlich unsere Anleitung zum WLAN einrichten. Mit unseren Anleitungen stellen Sie sicher, dass Ihr Gerät auch ohne Expertenwissen sicher und roaming-konform eingerichtet ist.

> Bei einer manuellen Einrichtung kann das GITZ nur eingeschränkten Support leisten. Aufgrund der Vielzahl unterschiedlicher Betriebssysteme, Netzwerkmanager, Treiber und Softwareversionen können nicht alle möglichen Gerätekonfigurationen unterstützt werden.

> **Konfigurieren Sie Zertifikatsinformationen** und **deaktivieren Sie niemals die Zertifikatsprüfung** bei der WLAN-Anmeldung! Wenn Sie einen Zertifikatsfehler durch Ihr Gerät beim Anmelden an das WLAN bekommen, loggen Sie sich bitte unter keinen Umständen im WLAN ein bzw. ignorieren Sie solche Meldungen niemals! Verwenden Sie zu keinem Zeitpunkt nur TUBS-ID und Passwort, um sich mit eduroam zu verbinden, sondern achten Sie auf die Zertifikate und konfigurieren Sie Ihre Geräte richtig und mit Bedacht.

Für alle diejenigen, die doch lieber selbst Hand an die WLAN-Konfiguration legen wollen, sind hier die notwendigen Konfigurationsparameter angegeben:

Parameter	Einstellung
Funkbänder	2,4Ghz, 5Ghz und an einzelnen Standorten 6Ghz
Verschlüsselung	WPA2/WPA3-Transition Mode-Enterprise mit AES
Authentifizierung	Protokoll 802.1X
Verschlüsselung des Authentifizierungstunnels	EAP-TTLS Geräte die kein EAP-TTLS können steht EAP-PEAP zur Verfügung
TLS Version	TLS1.2
Äußerer Tunnel/Anonyme Identität	anonymous@tu-braunschweig.de
Server/Domain	netauth.rz.tu-bs.de

Parameter	Einstellung
Zertifikate	> Am 18. Januar 2027 wird ein Wechsel der CA durchgeführt für das Zertifikat vom AAA-Server, der die Authentifizierung im eduroam durchführt. Danach werden Zertifikate der eduroam CA bezogen. Zukünftige CA: https://pki.pca.dfn.de/eduroam-ca/pub/cacert/chain.txt Alte CA: T-TeleSec Global Root 2 oder https://pki.pca.dfn.de/dfn-ca-global-g2/pub/cacert/chain.txt Es wird das TeleSec Global Root 2 als Server Zertifikat verwendet. Das Zertifikat TeleSec Global Root 2 ist meist in aktuellen Browser und Betriebsystemen bereits installiert. Bitte stellen Sie sicher, dass das CA-/Root-Zertifikat im **korrekten Dateiformat** angegeben wird. Andernfalls kann die Zertifikatsprüfung fehlschlagen und es kann zu Problemen kommen.
Authentifizierung im inneren verschlüsselten Tunnel	EAP-TTLS:PAP (laufe 2027 wird die Anmeldung über MSCHAPv2 angeschaltet) EAP-PEAP:MSCHAPv2
Authentifizierung/Identitä (innerer Tunnel)	TUBS-ID und Passwort sowie Domainangabe „tu-braunschweig.de“ (<TUBS-ID>@tu-braunschweig.de). Ohne die Angabe <TUBS-ID>@tu-braunschweig.de erfolgt kein Roaming an anderen Einrichtungen!

Konferenz- und Gast-Netz tubs-guest

Das Gauß-IT-Zentrum bietet den Instituten und Einrichtungen mit dem Dienst 1109 „Konferenz- und Gast-Netz für Institute und Einrichtungen“ die Möglichkeit, für deren Gäste einen Zugang zum Internet zur Verfügung zu stellen. Bestandteil des Dienstes ist eine Selbstbedienungsschnittstelle für DV-Koordinatoren zur Einrichtung und Verwaltung von zeitlich befristeten und personenbezogenen Gast-Benutzerkennungen. Sie erhalten mit diesem Dienst eine komfortable und zeitgemäße Nutzungsmöglichkeit, um Ihren Gästen Internetzugang über WLAN so anbieten zu können, wie es auch in anderen Bereichen (Hotels, HotSpots) üblich ist. Das Gauß-IT-Zentrum stellt Ihnen über die Selbstbedienungsschnittstelle die nötigen Mittel zur Verfügung, den einschlägigen Vorgaben gerecht werden zu können. Dieses Dokument beschreibt die Nutzung der Selbstbedienungsschnittstelle.

> Als **Gast** oder **Konferenzteilnehmer** wenden Sie sich bitte an Ihre **Ansprechpartner** in Ihrem gastgebenden **Institut**.

DV-Koordinatoren beantragen WLAN Gast-Kennungen über folgendes Sponsoren-Portal:

- https://tubs-guest.tu-braunschweig.de

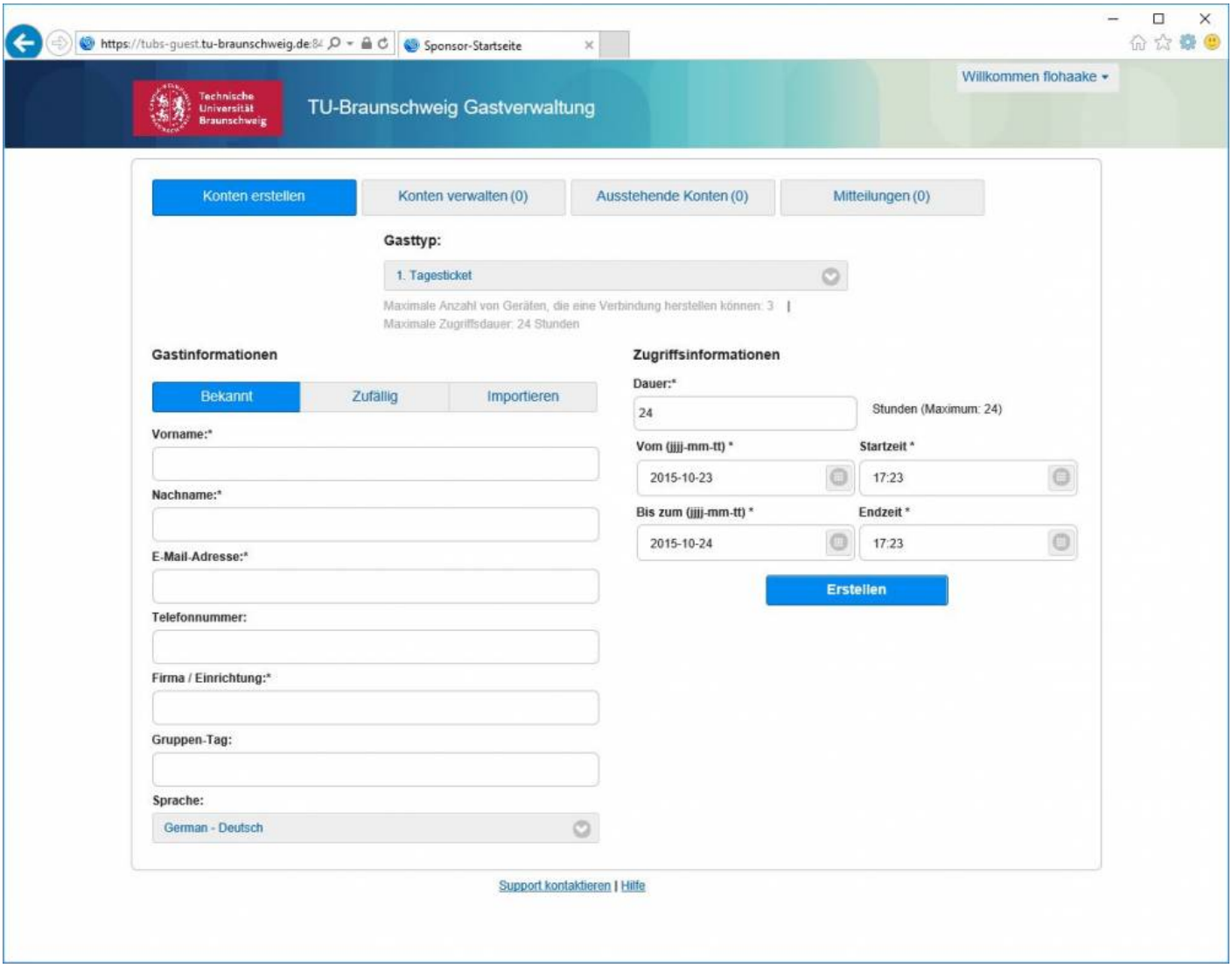
Darüber hinaus weisen wir darauf hin, dass bei Veranstaltungen mit mehr als 100 Teilnehmern eine Mitteilung über das Ihnen bekannte Kontaktformular zwingend benötigt wird. Das Formular erreichen Sie unter unserem Kontakt-Formular. Wir benötigen diese Information, damit u.a. ausreichend IP-Adressen zur Verfügung stehen.

> **Die maximale Verbindungsgeschwindigkeit für Mitarbeiter und Studierende der TU Braunschweig, die sich mit ihrer TUBS-ID im Gast-WLAN anmelden, wird begrenzt.**

> **Es wird empfohlen die Verbindung zum eduroam einzurichten.**

Nutzung durch DV-Koordinatoren

Die Selbstbedienungsschnittstelle zum Erstellen von Gast-Kennungen erreichen Sie unter der URL http://tubs-guest.tu-braunschweig.de aus dem Netz der TU Braunschweig (ggf. bitte per VPN einloggen). Hier loggen Sie sich mit Ihrer TUBS-ID ein. Nur bei uns im Gauß-IT-Zentrum eingetragene DV-Koordinatoren können diese Schnittstelle benutzen. Nach erfolgreichem Login wird die Übersichtsseite der Selbstbedienungsschnittstelle angezeigt.



Erstellen von Gast-Kennungen für tubs-guest

Ihnen als DV-Koordinator stehen zwei Optionen für die Erstellung von Gast-Kennungen zur Verfügung:

- Personalisierte Gast-Kennung erstellen (Reiter „Bekannt“)

- Mehrere Gast-Kennungen erstellen (Reiter „Zufällig“)
- Mehrere Gast-Kennungen via CSV-Datei importieren (Reiter „Importieren“)

Zeitprofile

Beim Anlegen von Gast-Benutzerkennungen kann bei jeder der vorgenannten Möglichkeiten ein Zeitprofil ausgewählt werden. Es stehen drei Zeitprofile zur Auswahl:

- Tagesticket
- Wochenticket
- Monatsticket
- Quartalsticket

Wenn Sie das Zeitprofil „Tagesticket“ auswählen, werden Gast-Kennungen mit einem Gültigkeitszeitraum von 24 Stunden ab dem ersten Login generiert. Dieses Zeitprofil empfehlen wir für Tagesgäste. Analog hierzu gelten Wochen-, Monats- bzw. Quartalstickets maximal sieben, 31 bzw. 180 Tage. Wir behalten uns vor abgelaufene Gast-Benutzerkennungen **nach 31 Tagen** zu löschen.

Der Gültigkeitszeitraum darf maximal 180 Tage umfassen. Das Erstellen von Gast-Kennungen mit diesem Zeitprofil soll nicht **mehr als drei Monate** im Voraus erfolgen.

In der Regel werden die personalisierten Zugangsdaten mit Benutzeranleitung durch Sie als DV-Koordinator ausgedruckt und Ihren Gästen ausgehändigt. Sofern eine E-Mail-Adresse hinterlegt wurde, besteht darüber hinaus die Möglichkeit, die Zugangsdaten mit Benutzeranleitung direkt über das System dem Gast zuzusenden. Bei Angabe einer Mobilfunknummer haben Sie weiterhin die Möglichkeit dem Gast eine SMS mit den Zugangsdaten zu schicken. Bitte beachten Sie auch die Ausführungen im Abschnitt „Aufzeichnungspflichten“.

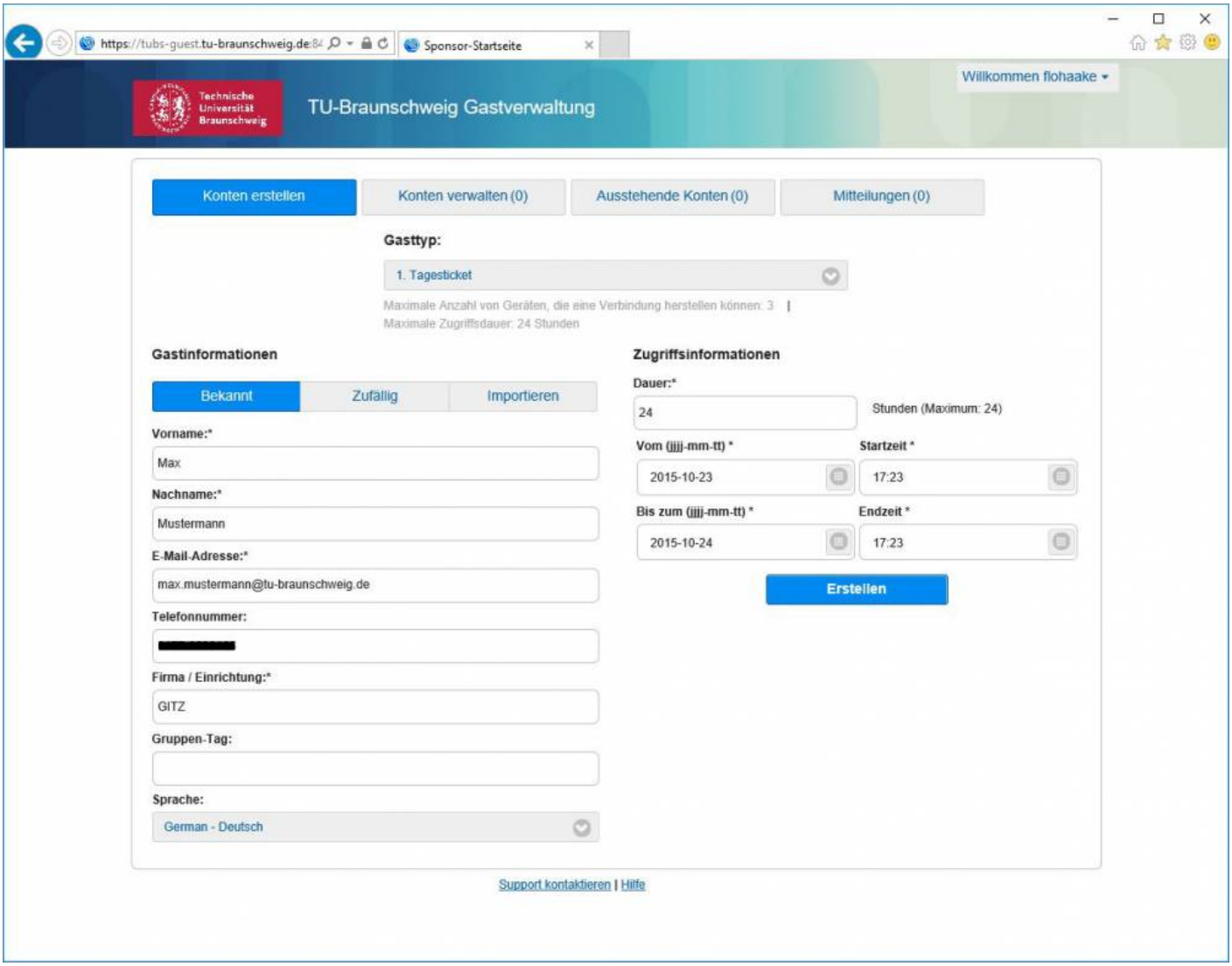
Bei Wochentickets erhält der „Ticketbesitzer“ einen Tag vor Ablauf eine E-Mail mit einem entsprechenden Hinweis. Bei Monatstickets erfolgt ein entsprechender Hinweis per E-Mail eine Woche und bei Quartalstickets 14 Tage vor Ablauf des Zugangs.

Maximale Anzahl von Geräten mit einer Gastkennung

Es können **maximal fünf** unterschiedliche Geräte zeitgleich mit einem Login verwendet werden. Dies ermöglicht z.B. die gleichzeitige Nutzung eines Notebooks, eines Tablets und drei weiteren Geräten.

Personalisierte Gast-Kennung erstellen (Reiter „Bekannt“)

Nach erfolgreichem Login wählen Sie in der Startansicht den Menüpunkt „Konto erstellen“ und „Bekannt“.



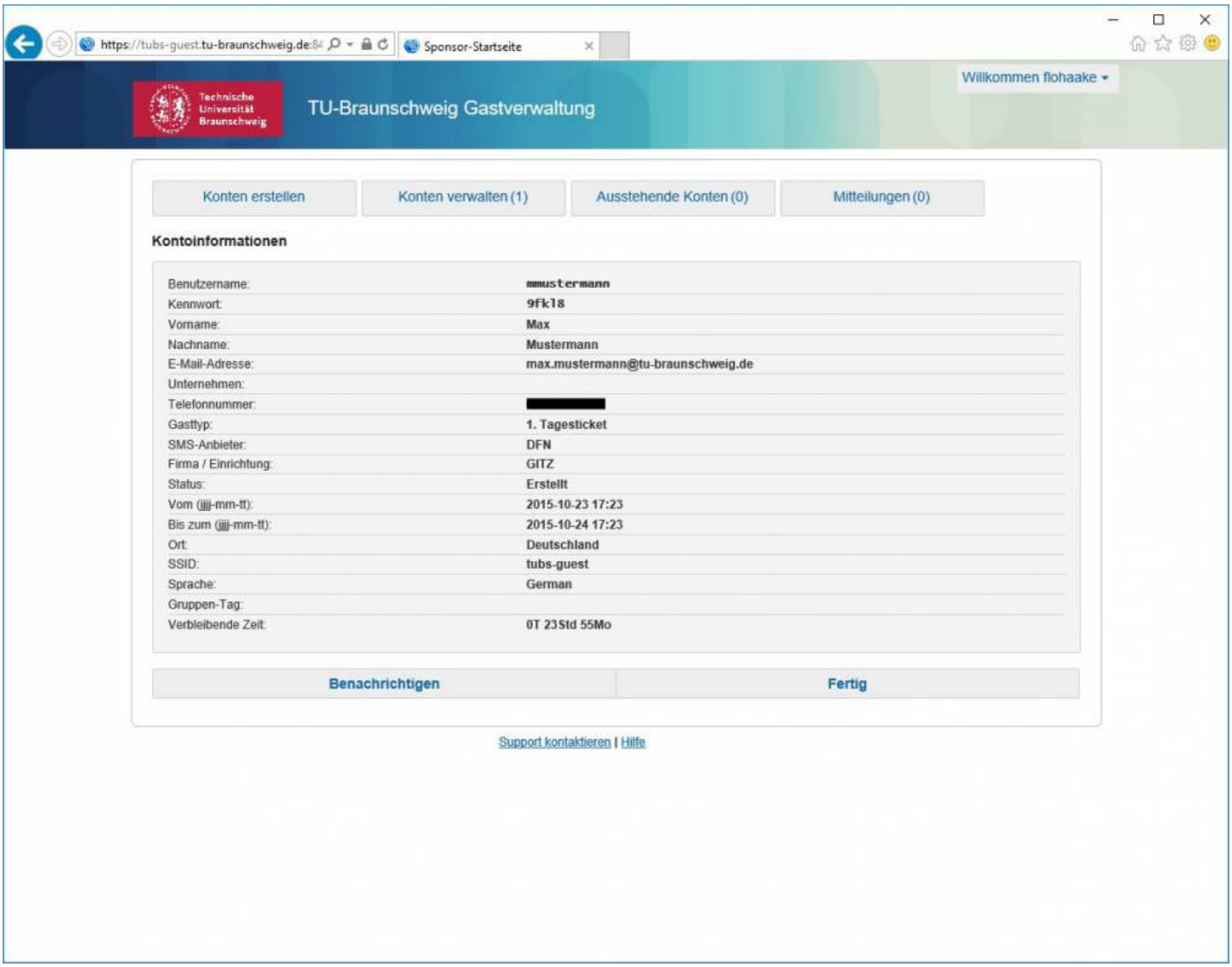
Es erscheint das abgebildete Fenster. Dort wird Vorname, Nachname, E-Mail-Adresse, Telefonnummer sowie Firma/Einrichtung angegeben. Der Gruppen-Tag dient der internen

Zuordnung bzw. Organisation von Kennungen bei Ihnen. Diesen können Sie frei vergeben.

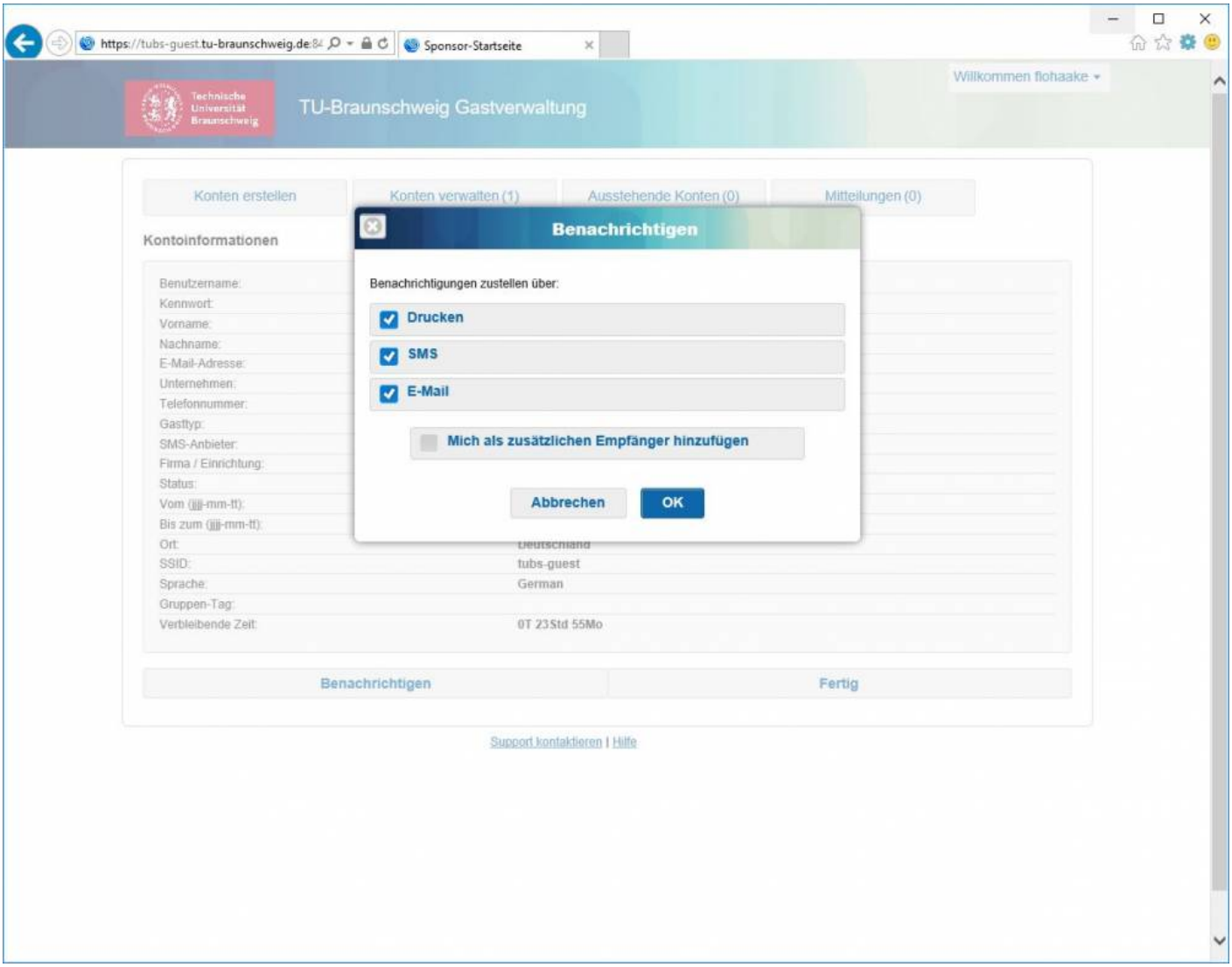
Es existieren zeitliche Beschränkungen für das Anlegen einer Gast-Kennung. Sowohl das Anlegen im Vorfeld als auch die maximale Nutzungsdauer sind befristet, siehe Abschnitt Zeitprofile. Sie können den Zeitraum flexibel per Hand eintragen oder die vordefinierten Zeitprofile verwenden.

Die mit (*) gekennzeichneten Attribute sind verpflichtend anzugeben.

Nach Erstellen der Gast-Kennung über [**Erstellen**] werden in der Übersicht die Details der Gast-Kennung angezeigt.

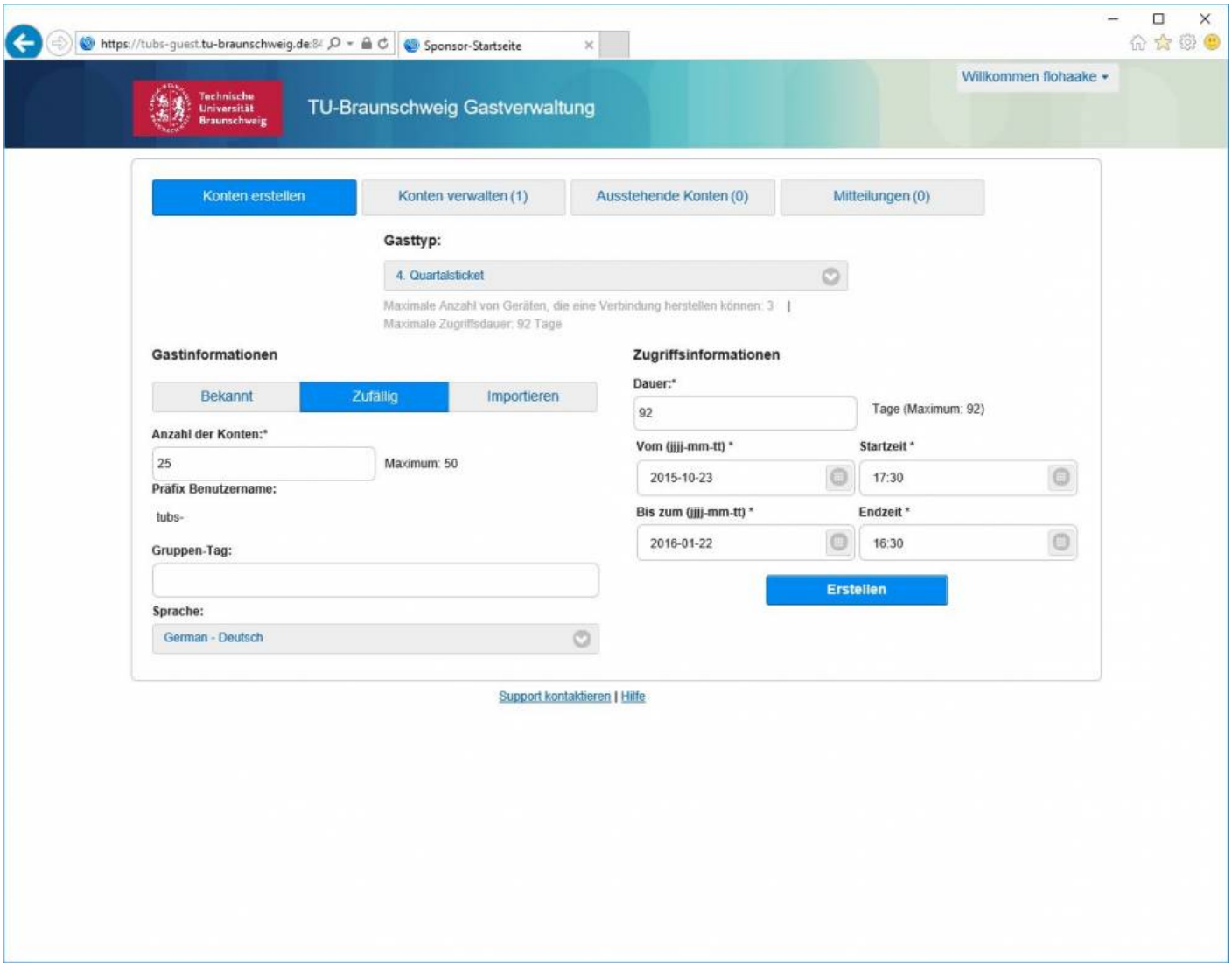


Es ist möglich die mit der Kennung verbundenen Zugangsdaten mit Benutzeranleitung auszudrucken oder/und an die angegebene E-Mail-Adresse zu versenden.



Mehrere Gast-Kennungen erstellen (Reiter „Zufällig“)

Nach erfolgreichem Login wählen Sie in der Startansicht den Menüpunkt „Konto erstellen“ und „Zufällig“ aus.



Sie können maximal bis zu 50 Benutzerkonten auf einmal anlegen. Nach einem Klick auf [**Erstellen**] haben Sie über die Funktion „Drucken“ die Möglichkeit sich eine PDF mit allen Kennungen (eine Seite pro Kennung) anzeigen zu lassen.

Bitte beachten Sie dass Systembedingt maximal 50 Gastaccounts in einem Vorgang erzeugt werden können, dieser Vorgang kann aber beliebig oft wiederholt werden. Wenn Sie für eine Veranstaltung mehr als 100 Accounts erzeugt haben oder benötigen, wenden Sie sich bitte mit dem Kontaktformular an die Abteilung Netze, damit eine ausreichende Versorgung mit W-LAN bereitgestellt werden kann für ihre Veranstaltung.

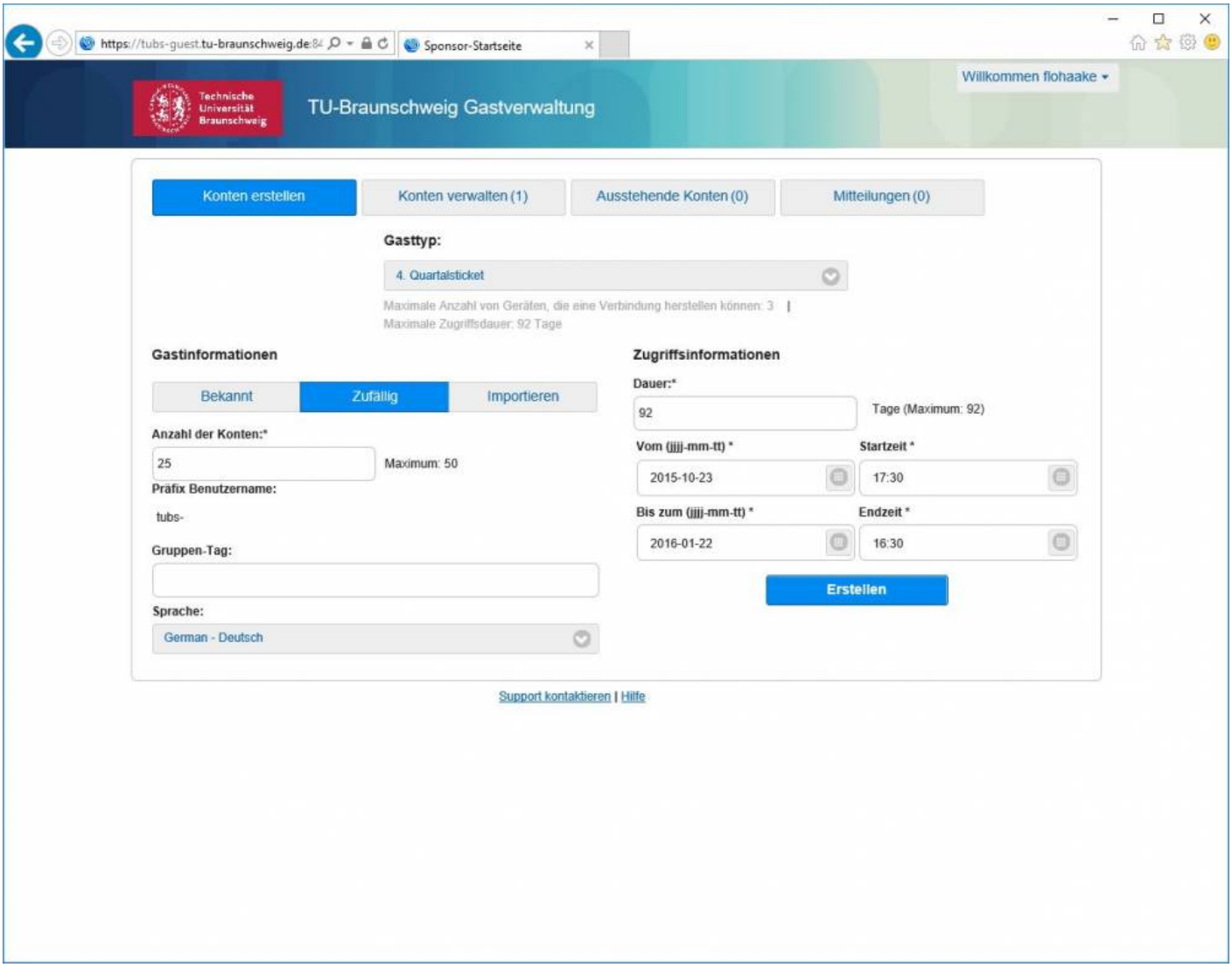
Die mit (*) gekennzeichneten Attribute sind verpflichtend anzugeben. Der Gruppen-Tag dient der internen Zuordnung bzw. Organisation von Kennungen bei Ihnen. Diesen können Sie frei vergeben.

Es existieren zeitliche Beschränkungen für das Anlegen einer Gast-Kennung. Sowohl das Anlegen im Vorfeld als auch die maximale Nutzungsdauer sind befristet, siehe Abschnitt Zeitprofile.

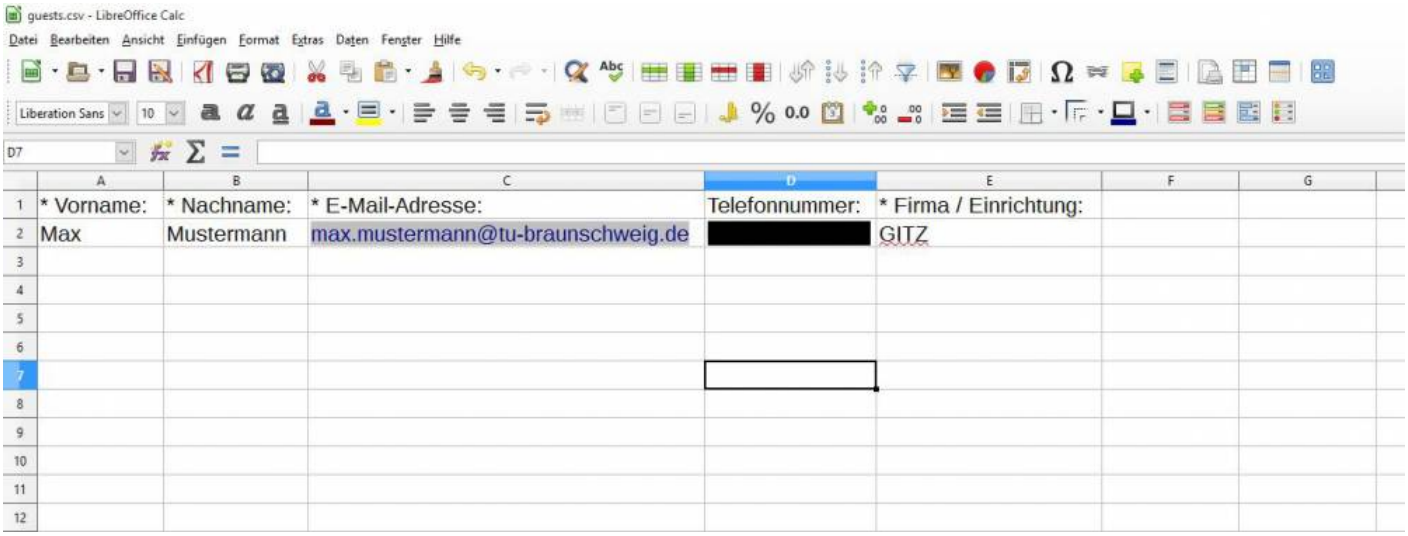
Bei der Ausgabe von nicht personalisierten Gast-Kennungen ist darauf zu achten, dass diese bei der Ausgabe personalisiert werden. Auf dem Ausdruck finden Sie einen Abschnitt, den Ihre Gäste vollständig ausfüllen müssen. Die Hinweise aus dem Abschnitt Aufzeichnungspflichten müssen Sie beachten.

Mehrere Gast-Kennungen via CSV-Datei importieren (Reiter „Importieren“)

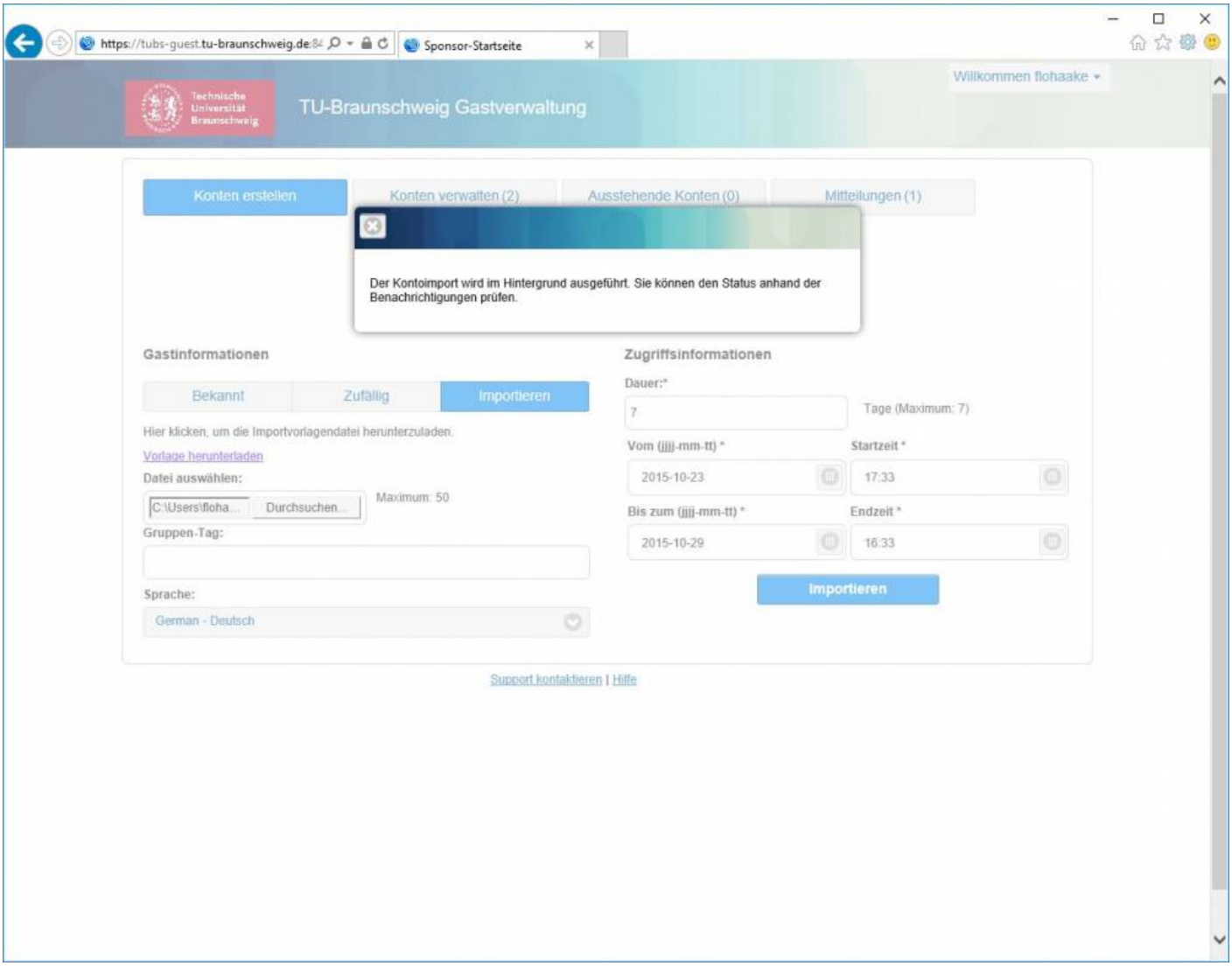
Über diese Funktion haben Sie die Möglichkeit eine CSV-Datei mit bis zu 50 Gast-Benutzern zu importieren und entsprechend Kennungen generieren zu lassen. Ein Beispiel für die Formatierung der CSV-Datei können Sie über „Vorlage herunterladen“ direkt auf Ihrem Computer speichern. Wir empfehlen die Nutzung dieser Vorlage.



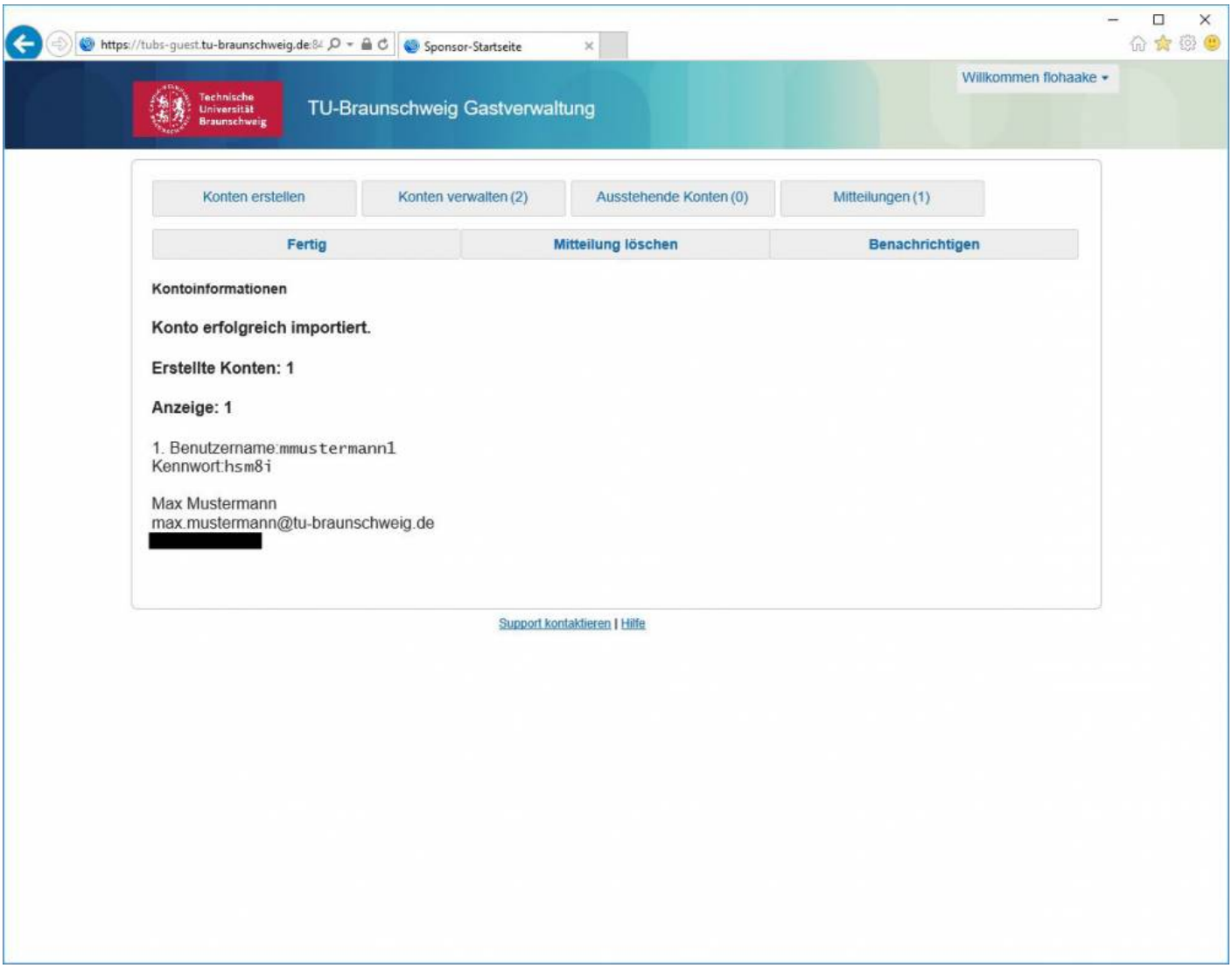
Die mit (*) gekennzeichneten Attribute in der CSV-Datei sind verpflichtend anzugeben. Als Trennzeichen wir das Komma benutzt um die Felder in der CSV-Datei zu trennen. Ein anderes Zeichen als Trennzeichen zu benutzen führt zu einem Fehler. Der Gruppen-Tag dient der internen Zuordnung bzw. Organisation von Kennungen bei Ihnen. Diesen können Sie frei vergeben.



Nach Auswahl und Upload der CSV-Datei werden die angeforderten Gast-Kennungen im Hintergrund generiert.

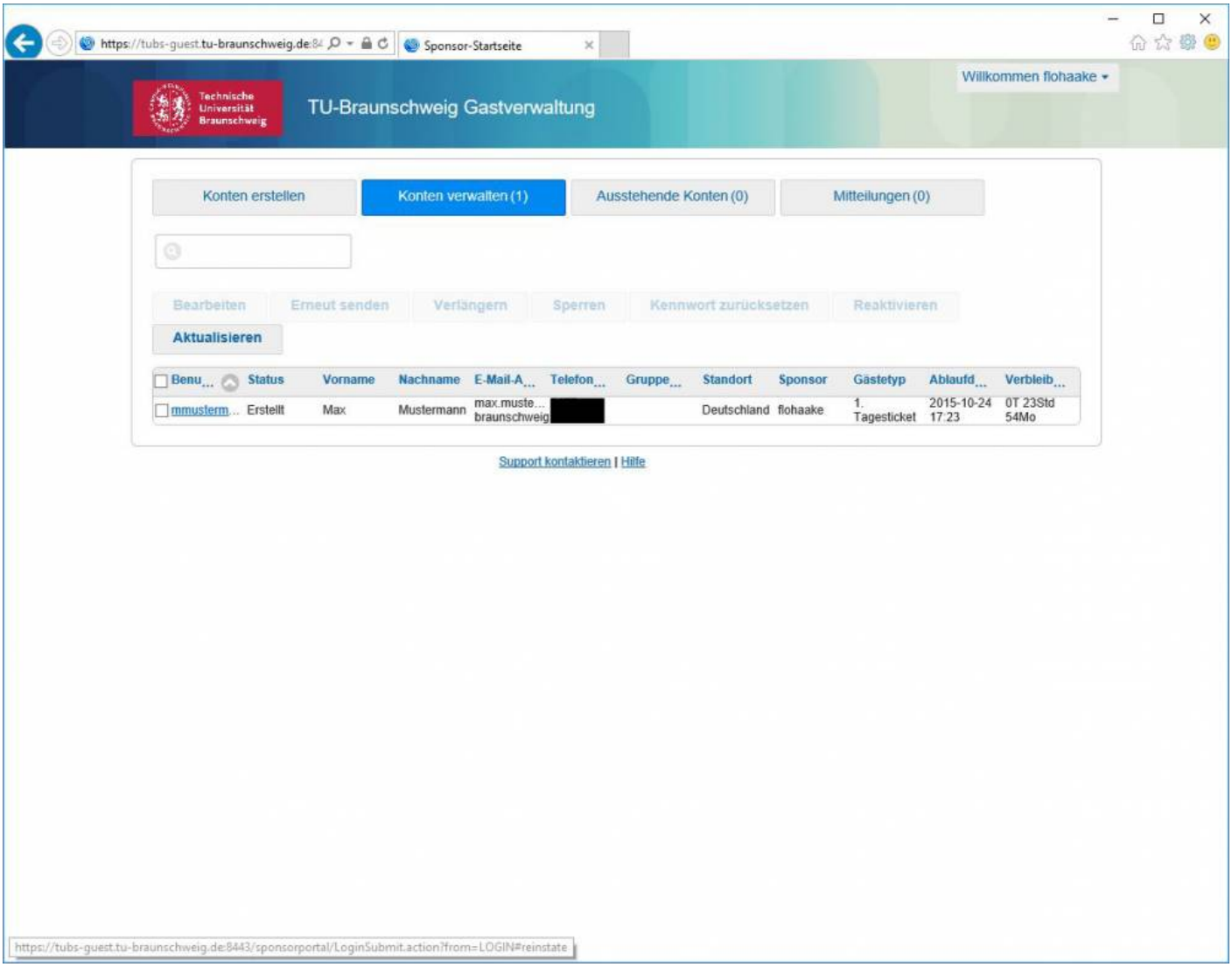


In dem Menüpunkt „Mitteilungen“ finden Sie nach Fertigstellung eine neue Nachricht mit den erzeugten Kennungen. Über „Benachrichtigen“ können Sie hier wie gewohnt eine PDF-Datei mit allen Gast-Kennungen inkl. Anleitungen generieren sowie die Nutzer per E-Mail.



Verwalten von Gast-Kennungen

Über den Menüpunkt „Konten verwalten“ haben Sie die Möglichkeit bestehende Gast-Kennungen zu verwalten bzw. zu editieren.



- [**Bearbeiten**]: Nachträgliches Editieren der Kontaktdaten des Gastes
- [**Erneut senden**]: Zugangsdaten erneut versenden/ausdrucken
- [**Verlängern**]: Gast-Kennung um maximal 24 Stunden verlängern
- [**Sperren**]: Gast-Kennung mit sofortiger Wirkung sperren
- [**Kennwort zurücksetzen**]: Passwort neu setzen und per E-Mail versenden / ausdrucken
- [**Reaktivieren**]: Konto wieder freischalten (nach Sperrung)

Aufzeichnungspflichten

Die Verwaltung der Gast-Kennungen obliegt der Verantwortung Ihres Instituts oder Einrichtung. Diese werden ausschließlich über Sie als DV-Koordinatoren eingerichtet.

Grundsätzlich sind alle Gast-Kennungen spätestens bei deren Ausgabe zu personalisieren (einer Person zuzuordnen). Nicht personalisierte Gast-Kennungen sind nicht zulässig. Auch die Weitergabe an Dritte oder das Einrichten von Sammelkennungen ist nicht zulässig.

Auf Anfragen des GITZ oder von Ermittlungsbehörden müssen Sie als DV-Koordinator die Zuordnung vorlegen können. Daher enthält das Blatt mit den Zugangsdaten und Benutzeranleitung einen Abschnitt, der die Personalisierung und persönliche Identifizierung von Benutzern der Gast-Kennungen erlaubt und vom Gast unterschrieben werden muss. Dieser Abschnitt wird von Ihnen als DV-Koordinator abgetrennt und aufbewahrt, da es sich bei diesen Daten um Bestandsdaten nach dem Telekommunikationsgesetz (TKG) handelt, die Sie mit Ablauf des auf die Nutzung folgenden Kalenderjahres löschen/vernichten müssen.

Siehe hierzu auch TKG §95 Abs. 3. Bezüglich der Einhaltung der gesetzlichen Vorgaben zur Löschung von Gast-Benutzerkennungen und verknüpften Datensätzen aus den Systemen des Gast- und Konferenz-WLAN kümmert sich das Gauß-IT-Zentrum.

Ausgabepraxis von Gast-Benutzerkennungen

Seitens des DFN existieren keine expliziten Empfehlungen zur Ausgabepraxis von personalisierten Gast-Benutzerkennungen. Auf Anfrage wurde mitgeteilt, dass eine Übergabe von personalisierten Gast-Benutzerkennungen gegen Empfangsquittung und persönlicher Identifizierung der empfangenden Person anhand eines gültigen amtlichen Lichtbildausweises die haftungsrechtlich unbedenklichste Lösung ist. Abstriche an diesen hohen Anforderungen lassen das Haftungsrisiko aufgrund möglicher missbräuchlicher Nutzung steigen.

Welchen Grad erhöhter Haftungsrisiken Institute oder Einrichtungen bereit sind zu tragen, obliegt ihnen selbst. Eine Risikoabschätzung muss individuell erfolgen. Seitens des DFN können daher keine verbindlichen Empfehlungen gegeben werden. Als Hinweis zur Abschätzung wird jedoch wie folgt erläutert: Tritt ein Fall von missbräuchlicher Nutzung einer Gast-Benutzerkennung ein und wird dieser Missbrauch durch Polizei und Staatsanwaltschaft geahndet, so ist das Institut/die Einrichtung, die den Zugang durch Erstellen und Ausgabe der Gast-Benutzerkennung gewährt hat, in der Nachweispflicht an wen konkret die Gast-Benutzerkennung ausgegeben worden ist.

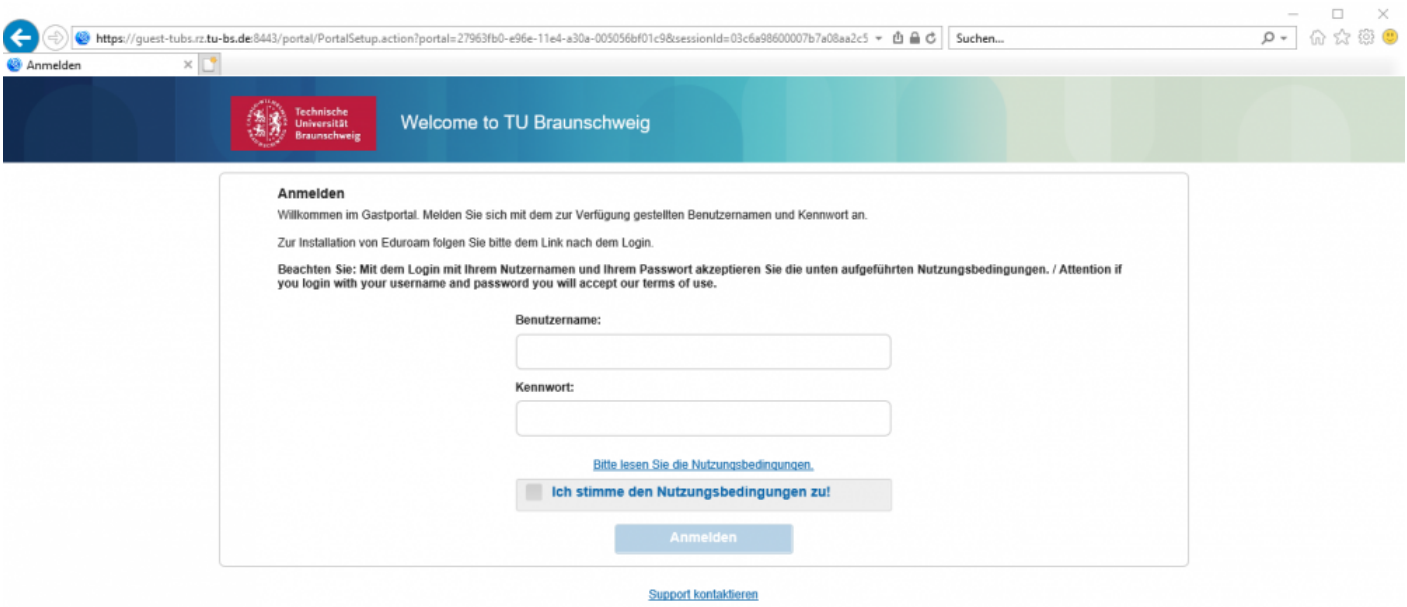
In einem Ermittlungsverfahren werden Polizei und Staatsanwaltschaft dann gegen die genannte Person ermitteln. Kann das Institut/die Einrichtung diesen Nachweis nicht erbringen oder werden die vorgelegten Nachweise im Strafverfahren vom Gericht als nicht ausreichend angesehen, so kann dann der Fall einer Mitstörerhaftung eintreten. Handreichung für eine praktikable Umsetzung passend zu Risikoabschätzung in Ihrer Einrichtung: Von Aushändigung gegen Vorlage der persönlichen Konferenzeinladung am Konferenzdesk - so wie es auch an anderen Einrichtungen üblich ist - bis Versand an die bei der Konferenzanmeldung und Zahlung der Konferenzgebühr übermittelten Post- oder E-Mail-Adresse sind verschiedene Optionen denkbar, die Sie ggf. mit der Leitung Ihres Instituts oder Einrichtung abstimmen.

Als Information für Ihren Abwägungsprozess sei angemerkt, dass die Mehrzahl der Meldungen durch das DFN-CERT erfolgen und lediglich auf kompromittierte Rechner hinweisen (einige Hundert). Gelegentlich finden allerdings auch Ermittlungsanfragen von Polizei und Staatsanwaltschaft statt.

Nutzung durch Gäste

Nachdem Sie über die Selbstbedienungsschnittstelle Gast-Benutzerkennungen generiert haben, erhalten die Nutzer ihre Zugangsdaten mit Benutzeranleitung per E-Mail oder entsprechend durch Sie ausgehändigt. Die Nutzung durch Ihre Gäste ist weitgehend selbsterklärend und intuitiv. Gäste können ihre Geräte über das WLAN-Netz (SSID) tubs-guest verbinden. Der Einsatz verschlüsselter Protokolle wie HTTPS, IMAPS, VPN, usw. oder/und VPN werden empfohlen. Nach erfolgreicher Verbindung mit tubs-guest werden alle (http-)Aufrufe im Internetbrowser automatisch auf eine SSL-gesicherte Login-Seite umgeleitet. Um das Internet nutzen zu können, müssen die Gäste die erhaltenen Zugangsdaten eingeben und die Nutzungsbedingungen akzeptieren.

Sollte kein automatischer Redirect auf die Login-Seite erfolgen „surfen“ Sie einfach https://wlan.tu-braunschweig.de an.



Instituts-WLAN

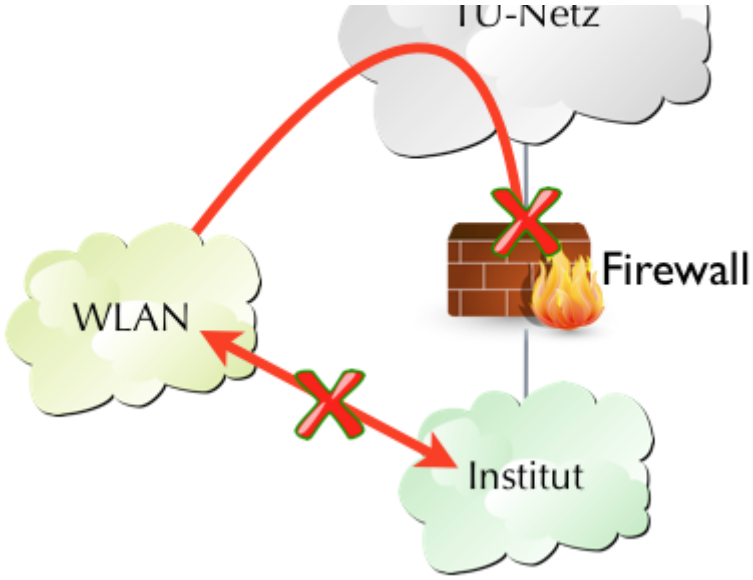
Was ist Instituts-WLAN? Wie wird es vom DV-Koordinator beantragt/eingerichtet? Wie nutzt man es?

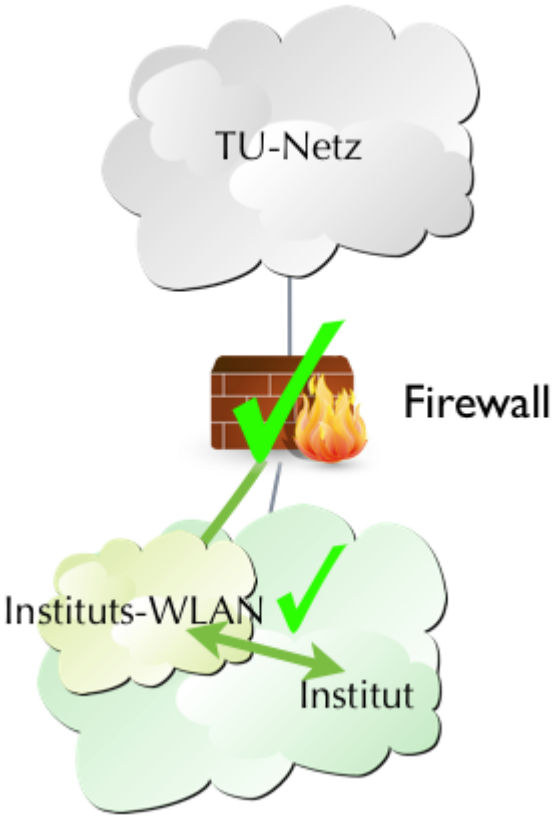
Was ist Instituts-WLAN? (Für DV-Koordinatoren)

Wir betreiben für die TU Braunschweig eine Wireless LAN Infrastruktur mit vielen hundert Access-Points, die weiterhin ständig ausgebaut wird. Mit der SSID eduroam werden moderne Verschlüsselungsverfahren eingesetzt, und über den Protokollstandard 802.1X werden auf Basis von TUBS-ID und Passwort die Zugriffsberechtigten authentifiziert und autorisiert. Einmal richtig konfiguriert, können Sie und Ihre Anwender über das etablierte eduroam-Projekt weltweit an allen teilnehmenden Forschungseinrichtungen das Internet benutzen ohne weitere Konfigurationsänderungen an Ihrem Rechner vornehmen zu müssen.

Als DV-Koordinator Ihrer Einrichtung suchen Sie nach Möglichkeiten, wie Sie Ihren Benutzern das Arbeiten im Instituts-Netz möglichst komfortabel gestalten können. Mobiles Arbeiten mit Unterstützung durch Wireless LAN im Institutsnetz ist dabei eine der am häufigsten angefragten Lösungen im Bereich Wireless LAN.

Seit August 2008 haben wir dazu ein Angebot für Sie. Ob am Arbeitsplatz, in der Bibliothek oder im Hörsaal: Die IP-Adressen Ihres Institutes können auch im Wireless LAN auf dem gesamten Campus der TU Braunschweig und bestimmten Außenstellen genutzt werden. Netzwerk-Ressourcen in Ihrem Institutsnetz werden mobil (z.B. auch im Hörsaal) verfügbar. Mitglieder eines Instituts erhalten die Möglichkeit mit ihrem Laptop so zu arbeiten, als wäre ihr Gerät über ein LAN-Kabel mit einer Netzwerkbuchse im Büro verbunden. Die Nutzung von institutsspezifischen Diensten (Fileserver, etc.) ist mit diesem Angebot flexibel an allen Standorten der TU Braunschweig möglich. Als Teil des Instituts-Netzes gilt für die mobilen Geräte die gleiche Firewall, die das Institut von außen schützt.


TU-Netz
Firewall
WLAN
Institut


TU-Netz
Firewall
Instituts-WLAN
Institut

Instituts-WLAN beantragen & nutzen (für DV-Koordinatoren)

Als DV-Koordinator beantragen Sie die Nutzung von Instituts-WLAN einfach im KDD unter "Datennetz". Sollte der Dienst noch nicht für Ihr Institut konfiguriert sein, können Sie dazu in der entsprechenden Spalte hinter Ihrem Netz/einem Ihrer Netze auf "Beantragen" klicken. Dadurch wird eine Mail ausgelöst, die alle entsprechenden Daten enthält und im Ticket-System bearbeitet wird. Nach Einrichtung des Dienstes erhalten Sie eine entsprechende E-Mail zurück. Weitere Details dazu finden Sie auch in der Dokumentation zum KDD-Datennetzmodul.

Als Vorraussetzung um den Dienst Instituts-WLAN zu nutzen, muss der zentrale DHCP-Dienst vom GITZ benutzt werden.

In Einzelfällen (z.B. wenn Sie noch nicht den Dienst "DHCP" bei uns nutzen) haben wir vor der Einrichtung Rückfragen.

Haben Sie Bedenken, dass die Funkabdeckung durch unsere Access-Points nicht ausreicht? Sprechen Sie uns an, wir möchten gerne mit Ihnen gemeinsam Lösungen zur Verbesserung der Funknetzabdeckung finden. Sollte dafür die Einrichtung weiterer Netzdosen notwendig sein, arbeiten wir dazu eng mit Abteilung 34 der Verwaltung zusammen.

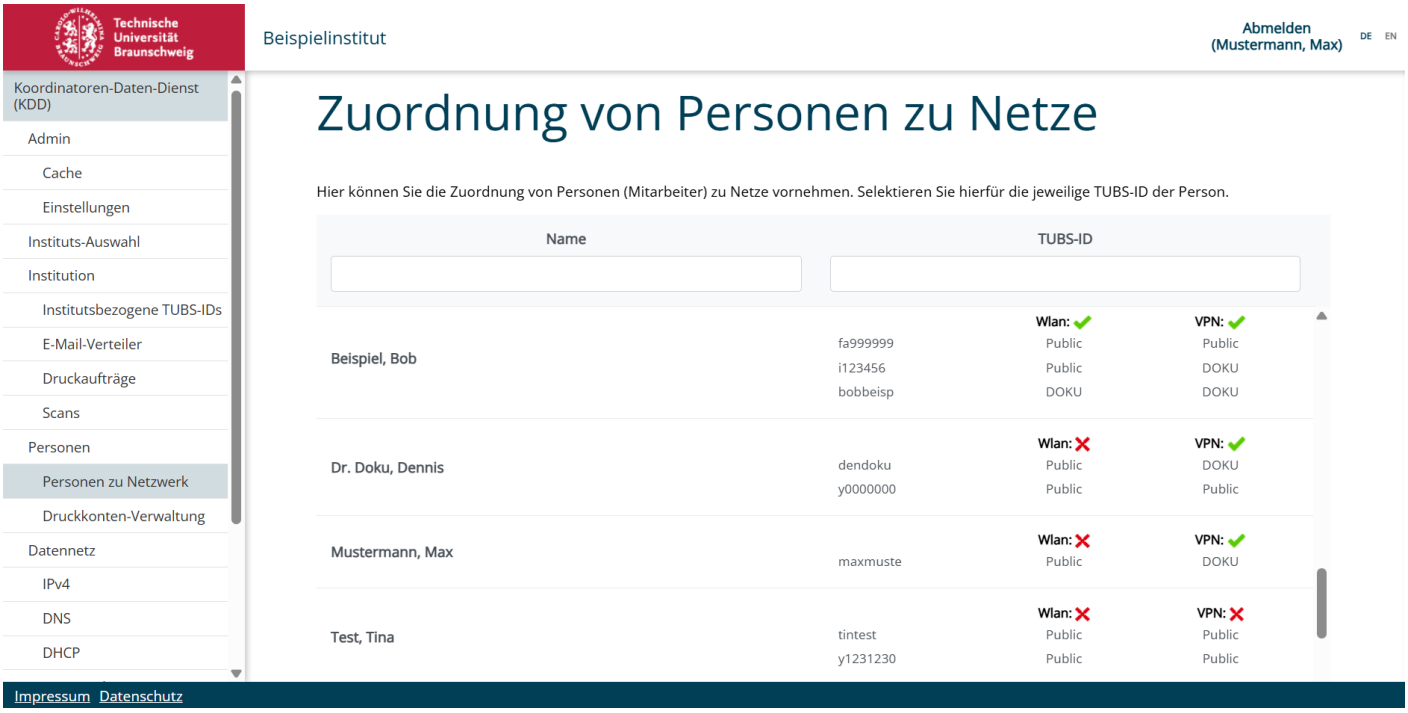
Freischaltung von Mitarbeitenden für Inst-WLAN (oder Inst-VPN)

Als DV-Koordinator schalten Sie Ihre Kollegen/Kolleginnen im KDD für diese Nutzung frei. Sie können hierbei auf Basis der einzelnen TUBS-ID entscheiden, welche Personen mit welcher TUBS-ID diesen Dienst nutzen dürfen und welche Personen in Ihrer Einrichtung weiterhin per WLAN in allgemeine Netze geschaltet werden.

Um die Netzzugehörigkeit festzulegen, gehen Sie bitte wie folgt vor:

Nach der Anmeldung im KDD gehen Sie bitte zum Modul "Personen zu Netzwerk". Sie finden dies in der linken Seitenleiste.
Im Folgenden sollten Sie eine Tabelle mit den Personen sehen, die Ihrem Institut/ Ihrer Einrichtung angehören. Ist dies nicht der Fall, ist weder Instituts-WLAN noch Instituts-VPN in Ihrer Einrichtung

aktiv. Beantragen Sie den Dienst unter "Datennetz" (s.o.).

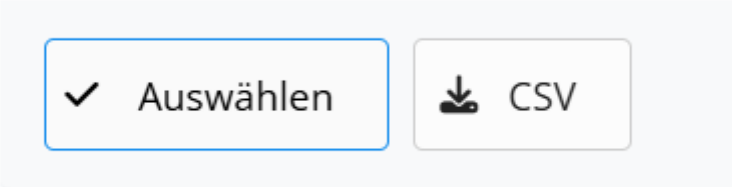


Für jeden Benutzer sehen Sie in den Spalten WLAN und VPN jeweils die für diesen Bereich hinterlegte Konfiguration. Wenn ein rotes Kreuz vorhanden ist, bedeutet dies, dass alle bei dieser Person hinterlegten Benutzernamen nur auf das öffentliche Netz zugreifen können. Sollte ein grüner Haken vorhanden sein, heißt dies, dass für mindestens eine TUBS-ID der Person ein anderes Netzwerk, als das öffentliche Netzwerk, eingerichtet worden ist. Die Details entnehmen Sie der Auflistung der einzelnen TUBS-IDs darunter.

Möchten Sie nun für eine TUBS-ID eine Änderung vornehmen, wählen Sie einfach die Zeile mit der TUBS-ID an - die ausgewählte Zeile wird hellblau hinterlegt.

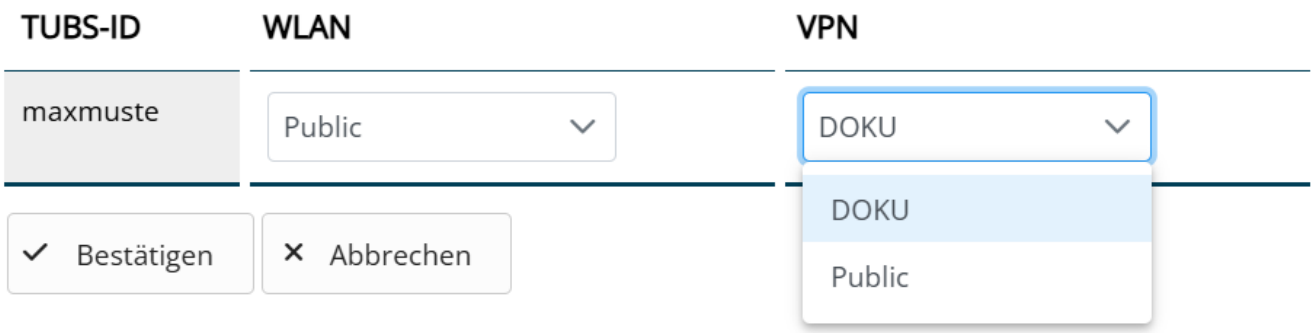


Klicken Sie anschließend unterhalb der Tabelle auf den Button [**Auswählen**].



Es öffnet sich eine neue Seite zu den Einstellungen für die einzelnen TUBS-IDs der ausgewählten Person. Wählen Sie für die zu bearbeitende TUBS-ID nun den jeweiligen Dienst aus und klicken Sie

auf den aktuellen Netzwerknamen. Es öffnet sich daraufhin ein Dropdown-Menü. Dort gibt es die Auswahl zwischen Public (keine Freischaltung) und dem oder den Netzwerken Ihres Institutes/ Ihrer Einrichtung. Wählen Sie das jeweilige Netz aus und bestätigen die Auswahl dann mit einem Klick auf "Bestätigen".



Änderungen, die Sie hier im KDD eintragen, werden spätestens 30 Minuten später aktiv, sofern sich der entsprechende Benutzer dann neu am WLAN bzw. VPN anmeldet.

Instituts-WLAN nutzen (Benutzer)

Das so genannte Instituts-WLAN ist eine auf die Bedürfnisse von Einrichtungen und Instituten der TU Braunschweig angepasste Ausprägung von eduroam auf dem Campus der TU Braunschweig. Es ist so möglich, Geräte im eduroam WLAN auf dem Campus der TU Braunschweig in das Netzwerk der jeweiligen Einrichtung/des jeweiligen Instituts zu schalten. Dies zielt insbesondere darauf ab, dass auf bestimmte, nur im jeweiligen Netz von Einrichtungen und Instituten angebotene Ressourcen (u.a. Fileserver, interne Webdienste, Windows-Domänen-Funktionen) auch über das eduroam WLAN (auf dem Campus der TU Braunschweig) zugegriffen werden können.

Die Freischaltung einzelner Mitarbeitenden für das Instituts-WLAN einer Einrichtung/eines Instituts wird durch die jeweiligen DV-Koordinatoren konfiguriert und bezieht sich auf die TUBS-ID des Benutzers. Es müssen anschließend die verwendeten Geräte eduroam-konform mit der entsprechend für Instituts-WLAN freigeschalteten TUBS-ID und dem Parameter "**#intern**" konfiguriert sein. Weiter unten finden Sie einige Hinweise, wie Sie eine ggf. bestehende WLAN-Konfiguration entsprechend anpassen können.

In vielen Instituten und Einrichtungen der TU Braunschweig ist die Nutzung privater Kommunikationsgeräte im Instituts-WLAN prinzipiell untersagt, und es dürfen dort nur die dienstlich bereitgestellten mobilen Kommunikationsgeräte im Instituts-WLAN genutzt werden. Dies gilt dann natürlich insbesondere für die Anmeldung am Instituts-WLAN. Bitte sprechen Sie mit ihrem DV-Koordinator, welche Geräte Sie im Institutsnetz betreiben und entsprechen im Instituts-WLAN anmelden dürfen. Ohne die ergänzende Konfiguration der Eduroam-Anmeldung (mit "#intern") werden Geräte als Standard weiter im allgemeinen WLAN-Bereich terminiert.

Festlegung für die Verwaltung

In der Verwaltung sind ausschließlich die dienstlich bereitgestellten Notebooks mit dem Flag „#intern“ (vor-)konfiguriert. Benutzer müssen hier bezüglich der mobilen (dienstlich bereitgestellten!) Kommunikationsgeräte (z.B. iPhone und auch iPad) selbst aktiv werden, um die Konfiguration - ggf. mit Unterstützung der Client Betreuung für die Verwaltung - anzupassen.

WLAN Opt-in einrichten mit geteduroam

FAQ

Hier finden Sie gelegentlich gestellte Fragen und die dazugehörigen Antworten zu unserem Angebot Instituts-WLAN:

- **F:** Wenn wir das Instituts-WLAN nutzen wollen, benötigen wir dann noch geteduroam?
- **A**: Ja, Sie benötigen weiterhin einen 802.1X-Supplikanten wie beispielsweise geteduroam auf Ihrem Rechner. Dieser wird benötigt, um den Benutzer an der Infrastruktur zu authentifizieren. Der Benutzer bekommt in diesem Fall jedoch nicht eine Adresse aus dem „allgemeinen Pool von Adressen“, sondern eine IP aus Seinem/Ihrem Institut.

- **F**: Mein DV-Koordinator hat mir gesagt, dass mein Institut jetzt diesen Instituts-WLAN Dienst nutzt. Aber was muss ich jetzt an meinem Notebook einstellen? Ich nutze bisher die über das Gauß- IT-Zentrum bereitgestellte Software und eduroam.
- **A**: Wenn Ihr DV-Koordinator den Dienst Instituts-WLAN für Sie konfiguriert hat müssen Sie zur Nutzung des Dienstes an ihre TUBS-ID den String „#intern“ anhängen, wenn Sie ihr Gerät über JoinNow konfigurieren.

- **F**: Ich war an einer anderen Universität. Zwar konnte ich das Internet nutzen, jedoch konnte ich nicht auf das Institutsnetz zugreifen. Das müsste doch möglich sein?
- **A**: Nein. Wenn Sie sich außerhalb des Campus der TU Braunschweig an einer Partnereinrichtung mit der SSID eduroam verbinden, nutzen Sie das Netz der gastgebenden Einrichtung und eben die IP-Adressen die dort genutzt werden können. Der Dienst Instituts-WLAN steht lediglich an den Standorten der TU Braunschweig zur Verfügung.

- **F**: Mein DV-Koordinator hat mir gesagt, ich darf nur das Notebook im Instituts-WLAN benutzen. Nun habe ich aber – dienstlich notwendig – ein Smartphone. Klar, ich kann auch über LTE auf E-Mail und Groupware zugreifen, um meine Termine zu managen. Aber wir haben doch fast überall eduroam. Darf ich das nun nicht mehr nutzen?
- **A**: Wenn Ihr DV-Koordinator Ihre TUBS-ID für das Instituts-WLAN freischaltet und Ihnen gleichzeitig aufgibt, nur bestimmte Geräte in das Instituts-WLAN zu bringen, hat das seinen Grund. Neben Sicherheitsüberlegungen spielt sicher auch eine Rolle, dass sich Ihr DV-Koordinator/Admin im Institut in einem heterogenen Umfeld mit schier unendlich vielen verschiedenen Geräten nicht um alle Geräte kümmern kann, wenn er seine Arbeit ordentlich machen möchte. Daher helfen Sie ihm/ihr bitte und nutzen Sie die „opt-in“-Lösung (Stichwort „#intern“) nur auf den Geräten, bei denen Sie das Instituts-WLAN zwingend benötigen.

FAQ

Geräte ohne Support:

Das **GITZ** kann nur Unterstützung für **Geräte, Anwendungen und Betriebssysteme** anbieten, die von den jeweiligen Herstellern oder Herausgebenden **aktiv unterstützt** werden (d. h. für die noch Sicherheits- und Funktionsupdates bereitgestellt werden).

Sobald der Hersteller den **Support einstellt** (z. B. bei älteren Windows-, macOS- oder Android-Versionen), kann das GITZ aus **Sicherheitsgründen** keine Hilfe mehr leisten.
Dies betrifft sowohl die **Beratung und den Support über den IT-Service-Desk** als auch die **Nutzung der zentralen IT-Dienste** wie z. B. WLAN oder das TU-Netz.

mögliche Probleme beim Einrichten und Anmelden am WLAN:

- Nach mehreren Fehlversuchen wird der Zugriff automatisch für eine bestimmte Zeit blockiert. Bitte warte etwa **15–30 Minuten**, bevor du es erneut versuchst
- Lösche auf deinem Gerät das gespeicherte eduroam-Netzwerk bzw. das WLAN-Profil.
- Nach Ablauf der Wartezeit und ggf. Passwortänderung kannst du eduroam erneut einrichten

Zertifikatswechsel im eduroam 2027

Kurzfassung – Was muss ich tun?

Bei **eduroam** wird am **18. Januar 2027** das Zertifikat für die Authentifizierung umgestellt. Damit sich Ihr Smartphone, Tablet oder Laptop auch danach weiterhin sicher mit eduroam verbinden kann, muss auf dem Gerät eine aktuelle eduroam-Konfiguration vorhanden sein.

Haben Sie eduroam mit geteduroam am oder nach dem 3. August 2026 neu eingerichtet?

Dann müssen Sie nichts weiter tun. Das seit dem **3. August 2026** bereitgestellte Profil enthält bereits die notwendigen Einstellungen für die bevorstehende Umstellung.

Haben Sie eduroam bereits vor dem 3. August 2026 eingerichtet oder sind Sie sich nicht sicher?

Dann empfehlen wir, eduroam **vor dem 18. Januar 2027 erneut mit geteduroam einzurichten**. Dadurch erhält Ihr Gerät die aktuelle Konfiguration und ist auf den Zertifikatswechsel vorbereitet.

Die Aktualisierung kann bereits jetzt durchgeführt werden. Sie müssen damit nicht bis Januar warten.

Eine Anleitung zur Einrichtung finden Sie auf unseren Dokumentationsseite fürs WLAN.

Wichtig: Sollten nach dem 18. Januar Probleme bei der Verbindung mit eduroam auftreten, deaktivieren Sie bitte nicht die Überprüfung des Serverzertifikats und bestätigen Sie keine unbekannten Zertifikate. Installieren Sie stattdessen die aktuelle eduroam-Konfiguration.

Empfehlung für Nutzerinnen und Nutzer

Wenn Sie eduroam **vor dem 3. August 2026** eingerichtet haben oder nicht wissen, wie aktuell Ihre Konfiguration ist, richten Sie eduroam bitte **vor dem 18. Januar 2027 erneut mit geteduroam ein**.

Wenn Sie eduroam **am oder nach dem 3. August 2026** mit dem aktuellen geteduroam-Profil eingerichtet haben, müssen Sie nichts weiter unternehmen.

Für manuell konfigurierte Geräte sollten die jeweils zuständigen Administratorinnen und Administratoren prüfen, ob die neue Zertifizierungsstelle bereits in der eduroam-Konfiguration hinterlegt ist.

Für Geräte die vom GITZ betreut werden, wird die Umstellung fürhzeitig begonnen.

Warum ist die Umstellung notwendig?

Für die Anmeldung bei eduroam verwenden unsere RADIUS-Server ein Serverzertifikat. Mit diesem Zertifikat können Endgeräte überprüfen, ob sie bei der Anmeldung tatsächlich mit der vorgesehenen eduroam-Infrastruktur kommunizieren.

Das derzeit verwendete Serverzertifikat läuft im **Februar 2027** aus.

Die bisher verwendeten Zertifikate basieren auf der **T-TeleSec GlobalRoot Class 2** der Deutschen Telekom. Unter dieser Root-Zertifizierungsstelle werden jedoch keine neuen Serverzertifikate mehr ausgestellt. Wir können das vorhandene Zertifikat daher nicht wie bisher durch ein neues Zertifikat mit derselben Vertrauenskette ersetzen.

Aus diesem Grund stellen wir unsere eduroam-Infrastruktur auf eine neue Zertifizierungsstelle um.

Warum betrifft das die eduroam-Konfiguration auf meinem Gerät?

Bei eduroam spielt die Überprüfung des Serverzertifikats eine wichtige Rolle für die Sicherheit.

Eine korrekt eingerichtete eduroam-Konfiguration legt fest, welchen Zertifizierungsstellen beim Aufbau der Verbindung vertraut werden darf. Dadurch kann das Endgerät überprüfen, ob es bei der Anmeldung tatsächlich mit einem vertrauenswürdigen Authentifizierungsserver kommuniziert.

Anders als beispielsweise bei vielen Webseiten reicht es deshalb nicht in jedem Fall aus, dass eine neue Zertifizierungsstelle bereits im allgemeinen Zertifikatsspeicher des Betriebssystems enthalten ist. Die für eduroam verwendete Konfiguration muss die entsprechende Zertifizierungsstelle ebenfalls kennen.

Vorbereitung läuft bereits seit dem 3. August 2026

Um den Wechsel möglichst reibungslos durchführen zu können, haben wir die über **geteduroam** bereitgestellte Konfiguration bereits am **3. August 2026** angepasst.

Seit diesem Zeitpunkt enthält das Profil **sowohl die bisher verwendete Telekom-Zertifikatskette als auch die neue DFN eduroam CA**.

Damit können Geräte mit der aktuellen Konfiguration während der Übergangszeit sowohl dem bisherigen als auch dem neuen Serverzertifikat vertrauen.

Die Umstellung erfolgt dadurch in zwei Schritten:

1. **Seit dem 3. August 2026:** Verteilung der aktualisierten eduroam-Konfiguration mit alter und neuer Zertifizierungsstelle.
2. **Am 18. Januar 2027:** Geplante Umstellung des Serverzertifikats auf der eduroam-Infrastruktur.

Wer sein eduroam-Profil seit dem **3. August 2026** über geteduroam neu installiert hat, ist damit bereits auf den zweiten Schritt vorbereitet.

Was passiert am 18. Januar 2027?

Am **18. Januar 2027** soll das Serverzertifikat auf unserer eduroam-Infrastruktur umgestellt werden.

Für Geräte mit der aktuellen eduroam-Konfiguration sollte dieser Wechsel unbemerkt erfolgen. Das Gerät kennt bereits beide Zertifizierungsstellen und kann dem neuen Serverzertifikat vertrauen.

Bei Geräten mit einer älteren Konfiguration kann es dagegen vorkommen, dass nach der Umstellung keine Verbindung mehr zu eduroam hergestellt werden kann oder eine Warnung bezüglich des Serverzertifikats erscheint.

In diesem Fall sollte die Zertifikatsprüfung **nicht deaktiviert** und ein unbekanntes Zertifikat **nicht einfach akzeptiert** werden. Stattdessen sollte eduroam mit der aktuellen, von uns bereitgestellten Konfiguration neu eingerichtet werden.

eduroam Certificate Change 2027

Summary – What do I need to do?

The certificate used for authentication with eduroam will be changed on **18 January 2027**. To ensure that your smartphone, tablet, or laptop can continue to connect securely to eduroam afterwards, your device must have an up-to-date eduroam configuration.

Did you set up eduroam again using geteduroam on or after 3 August 2026?

Then you do not need to take any further action. The profile provided since 3 August 2026 already contains the settings required for the upcoming change.

Did you set up eduroam before 3 August 2026, or are you unsure?

Then we recommend setting up eduroam again with geteduroam before **18 January 2027**. This will provide your device with the current configuration and prepare it for the certificate change.

You can update your configuration now. There is no need to wait until January.

Setup instructions are available on our WLAN documentation pages.

Important: If you experience problems connecting to eduroam after 18 January, please do not disable server certificate validation and do not accept any unknown certificates. Instead, install the current eduroam configuration.

Recommendation for users

If you configured eduroam before 3 August 2026 or are unsure whether your configuration is up to date, please set up eduroam again with geteduroam before **18 January 2027**.

If you set up eduroam on or after 3 August 2026 using the current geteduroam profile, you do not need to take any further action.

For manually configured devices, the responsible administrators should check whether the new certification authority is already included in the eduroam configuration.

For devices managed by the GITZ, preparations for the change will begin in advance.

Why is this change necessary?

For authentication with eduroam, our RADIUS servers use a server certificate. This certificate allows end devices to verify that they are actually communicating with the intended eduroam infrastructure during authentication.

The server certificate currently in use expires in February 2027.

The certificates used until now are based on Deutsche Telekom's **T-TeleSec GlobalRoot Class 2**. However, no new server certificates are being issued under this root certification authority. We can therefore no longer replace the current certificate with a new certificate using the same chain of trust.

For this reason, we are migrating our eduroam infrastructure to a new certification authority.

Why does this affect the eduroam configuration on my device?

Server certificate validation plays an important role in eduroam security.

A correctly configured eduroam profile defines which certification authorities may be trusted when establishing a connection. This allows the device to verify that it is actually communicating with a trusted authentication server during login.

Unlike with many websites, it is therefore not always sufficient for a new certification authority to already be included in the operating system's general certificate store. The configuration used for eduroam must also include the corresponding certification authority.

Preparations have been under way since 3 August 2026

To make the transition as smooth as possible, we updated the configuration provided via geteduroam on **3 August 2026**.

Since then, the profile has included both the previously used Telekom certificate chain and the new **DFN eduroam CA**.

This allows devices with the current configuration to trust both the existing and the new server certificate during the transition period.

The change is therefore being carried out in two steps:

1. **Since 3 August 2026:** Distribution of the updated eduroam configuration containing both the old and the new certification authority.
2. **18 January 2027:** Planned change of the server certificate on the eduroam infrastructure.

Anyone who has reinstalled their eduroam profile using geteduroam since 3 August 2026 is already prepared for the second step.

What will happen on 18 January 2027?

On **18 January 2027**, the server certificate on our eduroam infrastructure is scheduled to be changed.

For devices with the current eduroam configuration, this change should happen without the user noticing. The device already knows both certification authorities and can therefore trust the new server certificate.

Devices with an older configuration, however, may no longer be able to connect to eduroam after the change, or they may display a warning regarding the server certificate.

In this case, certificate validation should **not** be disabled and an unknown certificate should **not** simply be accepted. Instead, eduroam should be set up again using the current configuration provided by us.