802.1x Authentifizierung am kabelgebundenen Netz

Dieser Bereich wird in Kürze überarbeitet.

In dieser Anleitung wird beschrieben wie Sie sich mit 802.1x am kabelgebundenen Netz authorisieren können.

802.1x - Was ist das?

Der IEEE 802.1X Standard stellt Ihnen eine alternative Methode zur Verfügung sich über einen entsprechend gekennzeichneten „öffentlichen“ Netzwerkanschluss im Netzwerk der TU-Clausthal zu authentisieren (ähnlich wie Sie unter Umständen schon im WLAN eduroam/WiTuc kennen gelernt haben).

Voraussetzung für die Nutzung ist eine entsprechende Konfiguration ihrer Netzwerkeinstellungen!

Installation/Konfiguration

1. Schritt: Laden Sie das Konfigurationspaket herunter (Download)[1)] und entpacken Sie dieses mit Hilfe der Funktin **Alle Extrahieren...** an einen Ort Ihrer Wahl.

Exp. Script Download

2. Schritt: Makieren Sie die drei Sicherheitszertifikate und machen Sie einen Rechtsklick darauf. Danach wählen Sie Zertifikat installieren aus.

3. Schritt: Es öffnet sich der Installationsassistent und klicken Sie auf Weiter.

4. Schritt: Auf der nächsten Seite klicken Sie auf Durchsuchen. Wählen Sie dann den Punkt Alle Zertifikate in folgendem Speicher speichern. Wählen Sie in dem sich geöffneten Fenster

Dieses Dokument stammt aus der Dokuwiki-Instanz mit dem Titel RZ-Dokumentationen, die vom Rechenzentrum der Technischen Universität Clausthal bereitgestellt wird.

Vertrauenswürdige Stammezertifizierung aus und bestätigen Sie mit OK.



5. Schritt: Danach muss man auf der nächsten Seite nur noch mit Fertig stellen bestätigen. Danach öffnet sich ein Fenster das der Importvorgang erfolgreich war.

6. Schritt: Öffnen Sie als nächstes Die Systemsteuerung und wählen Sie Verwaltung aus.



7. Schritt: Wählen Sie in dem Fenster, welches sich geöffnet hat, Dienste aus und öffnen Sie diese.



8. Schritt: Suchen Sie den Punkt Automatische Konfiguration (verkabelt) heraus und öffnen Sie über einen Rechtsklick die Eigenschaften.



9. Schritt: Ändern Sie in den Eigenschaften den Starttyp auf Automatisch und starten Sie den Dienst.



10. Schritt: Als nächstes gehen Sie zurück in die Systemsteuerung und öffnen das Netzwerk- und Freigabecenter.



11. Schritt: Im nächsten Schritt öffnen Sie die Adaptereinstellungen indem Sie auf Adaptereinstellungen ändern klicken.



12. Schritt: Danach wählen Sie die Verbindung aus und machen einen Rechtsklick darauf. Dann wählen Sie die Eigenschaften aus und öffnen diese.



13. Schritt: Es öffnet sich ein Fenster, wählen Sie in diesem den Reiter Authentifizierung aus und klicken Sie auf die Zusätzlichen Einstellungen.



Dieses Dokument stammt aus der Dokuwiki-Instanz mit dem Titel RZ-Dokumentationen, die vom Rechenzentrum der Technischen Universität Clausthal bereitgestellt wird.

14. Schritt: Setzen Sie den Harken bei Authentifizierung angeben. Anschließend wählen im Dropdown Menü Benutzerauthentifizierung aus und klicken auf OK.

15. Schritt: Sie gelangen zurück, dort gehen Sie nun auf die Einstellungen.

16. Schritt: Setzen den Harken bei Serverzertifikat überprüfen. Setzen Sie bei Vertrauenswürdige Stammzertifizierungsstellen die Harken bei Deutsche Telekom Root CA 2. DFN-Verein PCA Global – G01 und TU Clausthal CA – G02. Weiterhin müssen Sie den Haken bei Schnelle Wiederherstellung der Verbindung aktivieren und Identitätsdatenschutz aktivieren. Tragen Sie hinter dem letzten Punkt guest ein.

17. Schritt: Klicken Sie anschließend unter Authentifizierungsmethode auswählen auf Konfigurieren.

18. Schritt: Es öffnet sich ein Fenster, wo der Harken nicht gesetzt sein darf. Bestätigen Sie dies mit OK.

19. Schritt: Bei dem Verbinden mit dem Netzwerk müssen Sie nun noch ihre User ID un das Passwort eingeben.

1)

Veröffentlicht unter der Apache-2.0-Lizenz

Direkt-Link:
https://doku.tu-clausthal.de/doku.php?id=netzwerknutzung:802.1x_kabelgebundene_authentifizierung&rev=1391164297

Letzte Aktualisierung: **10:31 31. January 2014**

Dieses Dokument stammt aus der Dokuwiki-Instanz mit dem Titel RZ-Dokumentationen, die vom Rechenzentrum der Technischen Universität Clausthal bereitgestellt wird.