

HowTo zum Remote-Arbeiten am Lehrstuhl für Schaltungstechnik und Simulation



1. Passwort ändern: <https://sus.ziti.uni-heidelberg.de/password/>
Das zugewiesene Passwort muss zuerst geändert werden, bevor der Login funktioniert. Das neue Passwort muss min. 8 Zeichen lang sein und Groß- und Kleinbuchstaben sowie Zahlen und/oder Sonderzeichen enthalten.
2. Der Login kann am Lehrstuhl in Mannheim an den Rechnern in Raum B3.01 verwendet werden oder man kann sich remote einloggen.
3. Für den Remotezugang muss man mit dem Uni-HD Netzwerk verbunden sein:
 - per WLAN: <http://www.urz.uni-heidelberg.de/netz/laptop/>
 - per VPN: <http://www.urz.uni-heidelberg.de/zugang/vpn/>
 - per SSH portforwarding (siehe unten)
 - auf den CIP-Pools
4. Grafischer Remotezugang kann auf diese Arten erfolgen:
 - per SSH X-forwarding: bei schneller Internetverbindung
 - per x2go-Client (empfohlen)
 - per NX-Client
5. Server: `susnx.ziti.uni-heidelberg.de`
 - Key Fingerprint beim ersten Aufbau der SSH Verbindung
ED25519: 28:f2:83:ae:3b:87:7c:bb:13:cd:ee:55:00:e1:bf:26
RSA: a1:1b:45:03:a9:a4:00:e7:7e:79:f1:cf:4e:e9:6c:b3
6. optional: einrichten und login mit SSH public-key: Dann muss man nicht mehr mit dem Uni-HD Netzwerk verbunden sein.

x2go-Client: (empfohlen)

Download des aktuellen x2go-Client: <http://wiki.x2go.org/doku.php/download:start>

NX-Client: (nicht empfohlen)

Download des NX-Client (Version 3.5.x) und des Keys:

<https://sus.ziti.uni-heidelberg.de/SuSinternal/nxclient/>

Es wird ein spezieller Key (SuSNXClientKey.id_rsa.key) benötigt, um die NX-Verbindung zum Server `susnx.ziti.uni-heidelberg.de` aufbauen zu können. Er lässt sich bei den Einstellungen hinzufügen.

Windows: Für Cadence werden auch die zusätzlichen Schriftarten benötigt.

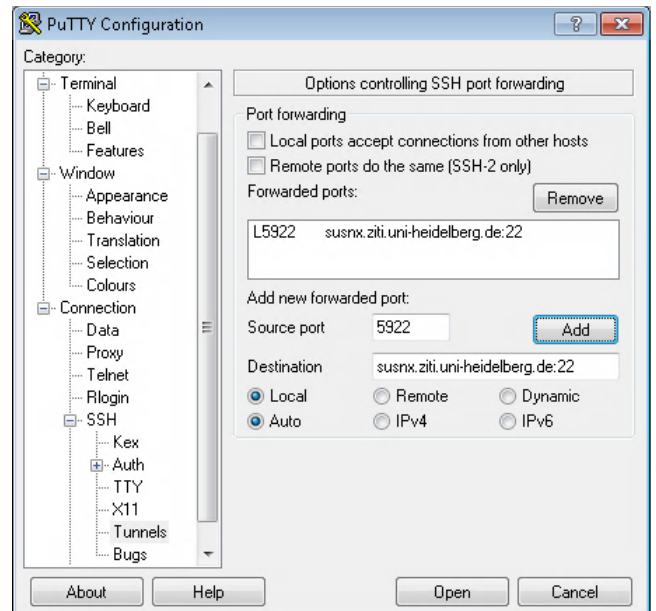
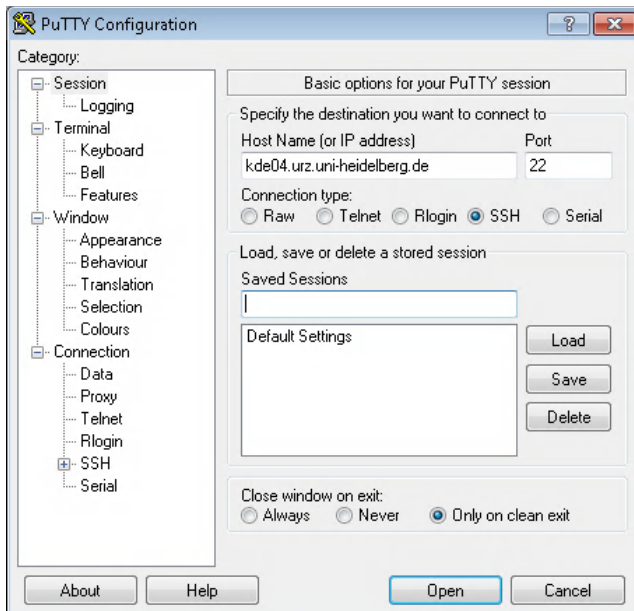
Linux: den offiziellen NX-Client 3.5 oder <http://opennx.net/>

Mac: <http://opennx.net/> ; Mit der offiziellen Version 4.x kann es Probleme geben.

SSH portforwarding

Bei einer SSH Verbindung wird, im Gegensatz zu VPN, der eigene Computer nicht Teil des Uni-Netzes. Jede Verbindung (jeder einzelne Port) muss über den Server `kde04.urz.uni-heidelberg.de` des Rechenzentrums zu unserem Server getunnelt werden.

Mit dem SSH-Client [PuTTY](#) für Windows sieht das so aus:



Linux-Kommandozeile von zu Hause:

```
ssh -N -L 5922:susnx.ziti.uni-heidelberg.de:22 UniID@kde04.urz.uni-heidelberg.de
```

Das bedeutet z.B.: Verwende den lokalen Port (des Computers, auf dem der Befehl ausgeführt wird) 5922, melde Dich beim kde04 als user an, tunnel dann durch den kde04 nach susnx und beende den Tunnel schließlich bei Port 22. Es ist dann also der lokale Port 5922 per ssh mit dem susnx Port 22 verbunden. Das -N verhindert, dass eine bash gestartet wird.

NX-Client / x2go-Client mit ssh-portforwarding

Lokal kann dann (z.B. per NX-Client) auf den Port 5922 verbunden werden: `localhost:5922`