Quick Start Guide for using the SSL Network Extender (Checkpoint)

(platform independent clientless network access)

Which resources and services can be used via SSL VPN access?

By using the SSL tunnel you have a secure (encrypted) access to the local resources of the Institute of Computer Science like:

- Internal mail and fax server
- File systems (HOME, projects etc.)
- Web services (internal)
- FTP, RSH, Rlogin, R-Desktop

1. Introduction

SSL Network Extender (SNX) is a solution for remote access, the user requires a web browser only. It is a browser plugin that provides clientless access to resources of the Institute of Computer Science and provides at the same time full network connectivity for IP-based applications.
2. Establish a connection

Open the following link in your browser:

https://vpn.informatik.uni-rostock.de

Please consider:
- Access requires a user account at the Institute of Computer Science.
- Pop-up Windows must be allowed for https://vpn.informatik.uni-rostock.de.
- A current version of Java with the appropriate settings is required.
- The security certificate must be confirmed.

![SSL Network Extender](image)

*Figure 1 SSL Network Extender - login*

Now enter your login and password (account at the Institute of Computer Science). Thereafter a pop-up window will open with the connection details and the option to disconnect.
3. Further information

- **Establishing a Remote desktop connection**
  
  → Start => Run: `mstsc /v: Servername`
  
  Connects to „servername“.

- **Mounting a network drive**
  
  → Start => Run: e.g. `\ordo.informatik.uni-rostock.de\<username>`
  
  → Username: `informatik\username`
  
  Password: (password)

- **Contact**

  In case you have any questions, please send an email to:

  `stg-cs@uni-rostock.de`