MacOS Tips & Tricks

- How to Disable SIP
- MacOS - Flush DNS Cache
- MacOS - Privacy hint / OCSP patch
- Map a shared drive on MacOS

How to Disable SIP

Introduction

System Integrity Protection (SIP)

SIP protects MacOS from cyber attacks. However, it also prevents the installation of certain software. So it can become necessary to disable SIP temporarily.

Boot into recovery mode

Silicon M1, M2, M3

Shut down your Mac and wait for 20 seconds. Then, hold the power button until you see the "Loading startup options" message under the Apple logo. Then, select Options and click Continue to enter the macOS Recovery screen.

Intel based

Restart your Mac and wait for 30 seconds. Press the power button and immediately hold Command + R keys on the keyboard until you see the Apple logo. Your Mac will boot into macOS Recovery after a while.

Open a terminal

Under utilities, you will find "Terminal". Open it.Type the following command:

```
csrutil disable
```

After that reboot the Mac, make all the necessary changes and enable SIP after that by entering the command:

```
csrutil enable
```

MacOS - Flush DNS Cache

Introduction

For some reasons Apple nurses a bug in the DNS resolver. This leads to the problem, that some FQDNs cannot be resolved correctly. The workaround is quite simple.

Resolution

```
sudo dscacheutil -flushcache
sudo killall -HUP mDNSResponder
```

MacOS - Privacy hint / OCSP patch

Introduction

The **Online Certificate Status Protocol** (**OCSP**) is an Internet protocol used for obtaining the revocation status of an X.509 digital certificate.It is described in RFC 6960 and is on the Internet standards track. It was created as an alternative to certificate revocation lists (CRL), specifically addressing certain problems associated with using CRLs in a public key infrastructure (PKI). Messages communicated via OCSP are encoded in ASN.1 and are usually communicated over HTTP. The "request/response" nature of these messages leads to OCSP servers being termed *OCSP responders*.

Wikipedia OCSP Protocol

The OCSP protocol is used to check whether or not a certificate has been revoked. In this context, it is used to give Apple the opportunity to revoke the “blessing” it has given to a specific piece of software. Whenever you start an application, MacOS checks back with the OCSP server.

Resolution

There are two ways to prevent MacOS from checking back to Apple.

Local patch

```
echo 0.0.0.0 ocsp.apple.com | sudo tee -a /etc/hosts
```

Router patch

Discussion

In fact, Apple does not associate the information coming with this request to any person or any IP address. Apple does also not track, when you start an application. Apple could figure out, which software vendor an application is coming from (thinking about Microsoft, that leaves a lot of possibilities).

In the end, it is a simple check whether a certificate is valid or not.

Security professional criticized that a man in the middle attack is possible and you might start an application of which the certificate is revoked. The data itself is also transferred over HTTP without encryption. So a 3rd party could get an idea than somebody runs software from a specific software vendor.

Keeping aside the security concerns, it could be a little bit slower to start an application with a low bandwidth internet connection. In that case, it could make sense to block the request.

Useful links

https://www.sentinelone.com/blog/what-happened-to-my-mac-apples-ocsp-apocalypse/

https://www.theverge.com/2020/11/16/21569316/apple-mac-ocsp-server-developer-id-authentication-privacy-concerns-encryption-promises-fix

Map a shared drive on MacOS

Introduction

Mapping of network drive seems to be a big issue. Hopefully this manual brings a little light into the fog.

Requirements

Any kind of network resource, that offers any kind of network share. A network resource can be:

- Windows Server
- Linux Server
- NAS (Network attaches storage)

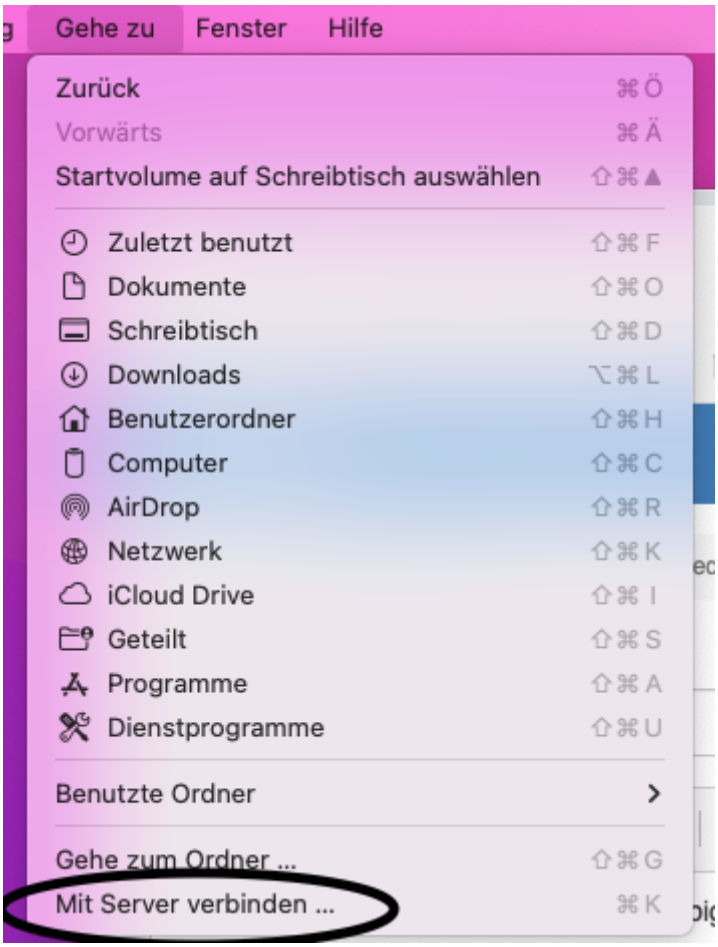
A network share can be provided by one of the following protocols:

- SMB or SAMBA
- CIFS
- NFS
- (FTP (SFTP))
- AFP (Apple File Protocol)

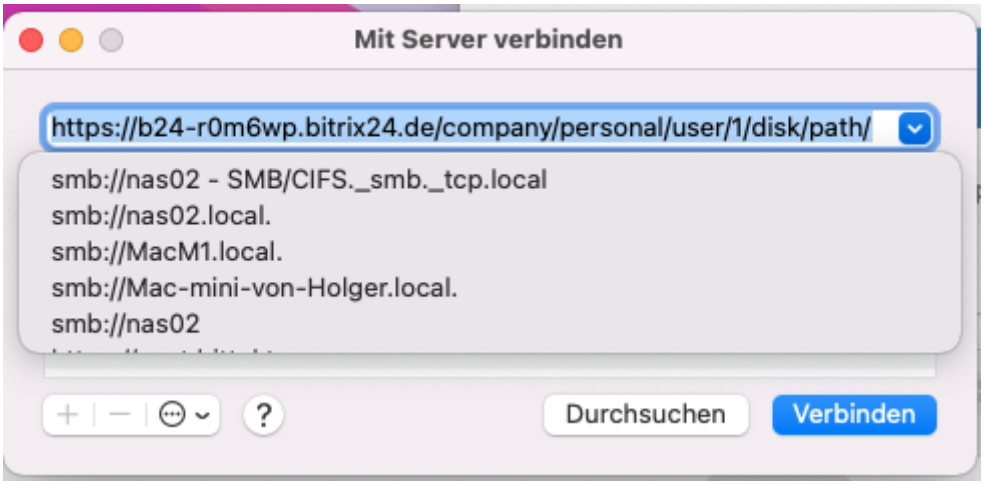
This manual will focus on SMB

Map a drive with MacOS and Finder

Open Finder and go to this menu or simply press cmd-k



Finder will provide you with a list of network resources it already found:



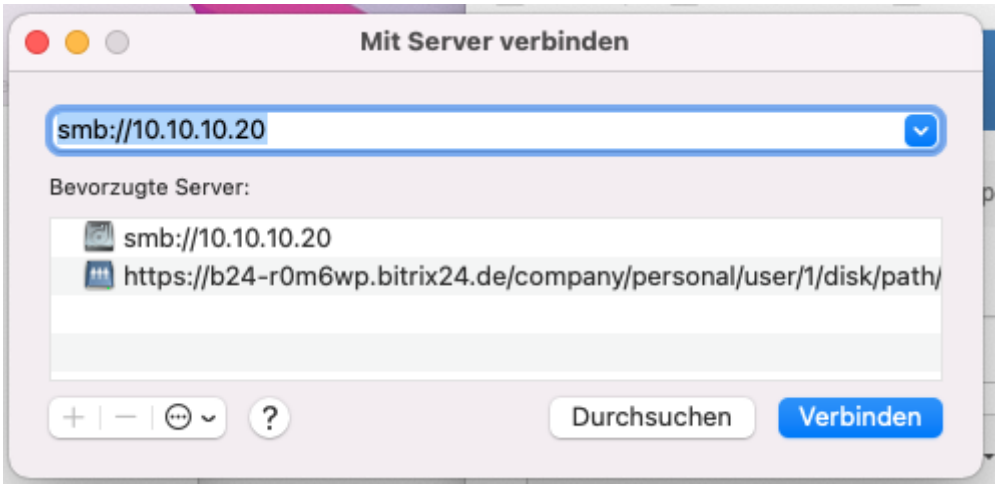
If you can already see your resource, you can click on it. If not, you will need to input the resource manually. You will need the protocol and ether the IP Address or an DNS name.

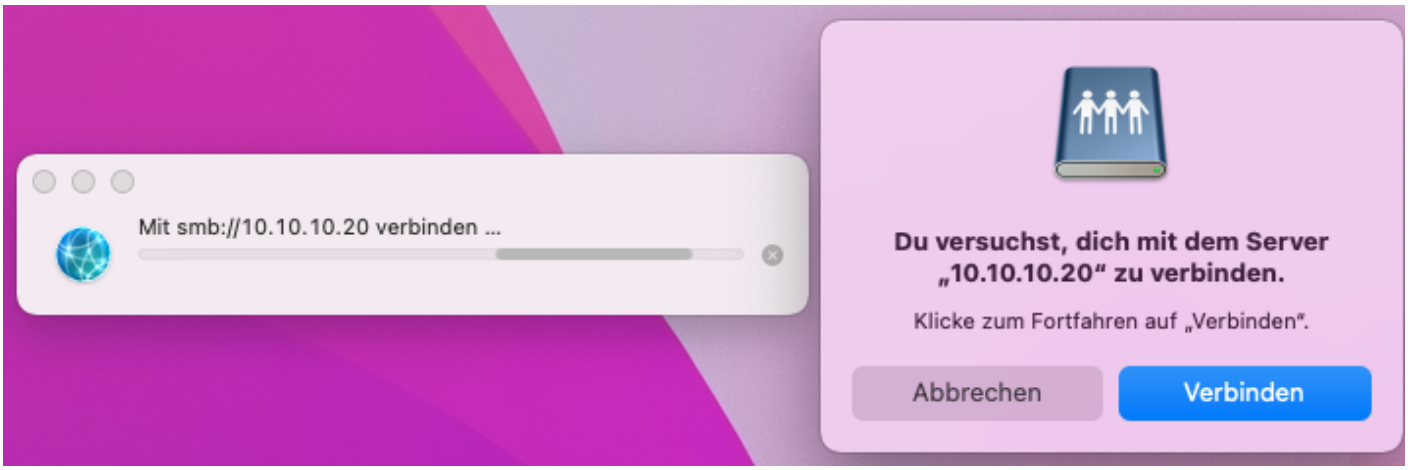
Finder understands these protocols:

- smb
- cifs (http, https)
- ftp
- afp

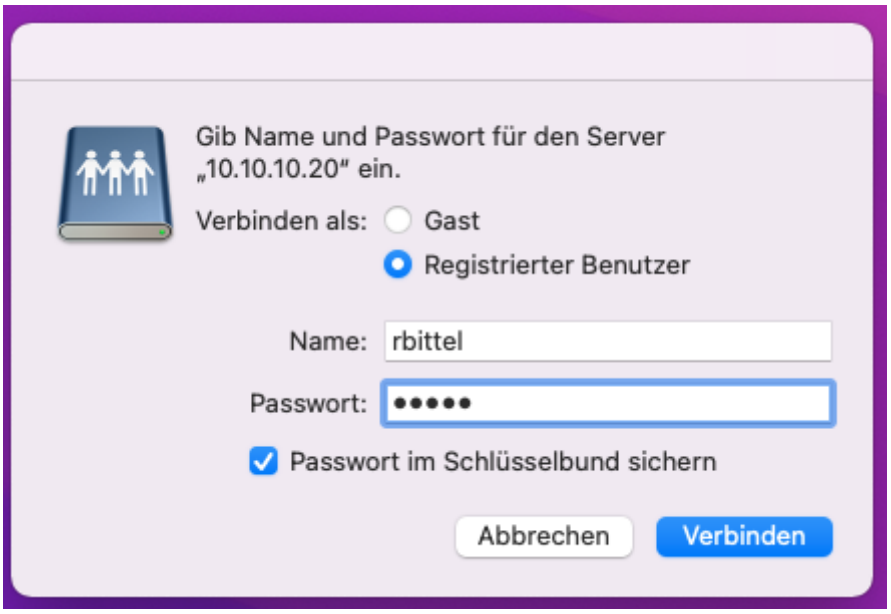
If our resource is located on nas01.simmy.ch and the protocol is smb, you will have to type in:

smb://nas01.simmy.ch

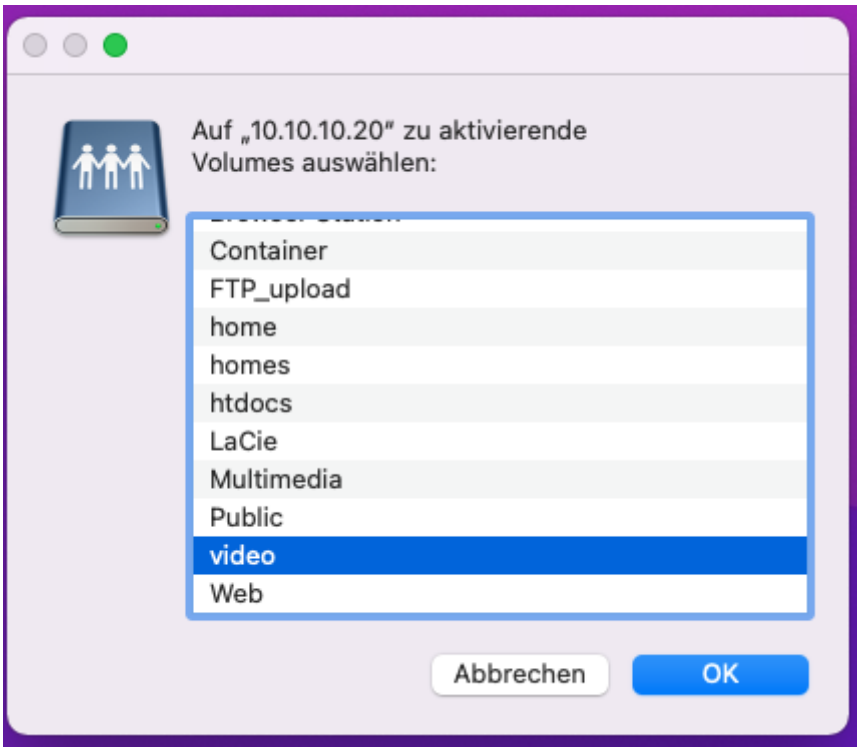




Most resources are protected with username and password:



If you manage to enter your username and password correct, please select the resource, you want to access:



Next thing you will see is the data, that is located on the network share:

