Anleitung für neue Mitarbeiter

Login (Kennwort ändern, Anmeldung an CFAED Rechnern)

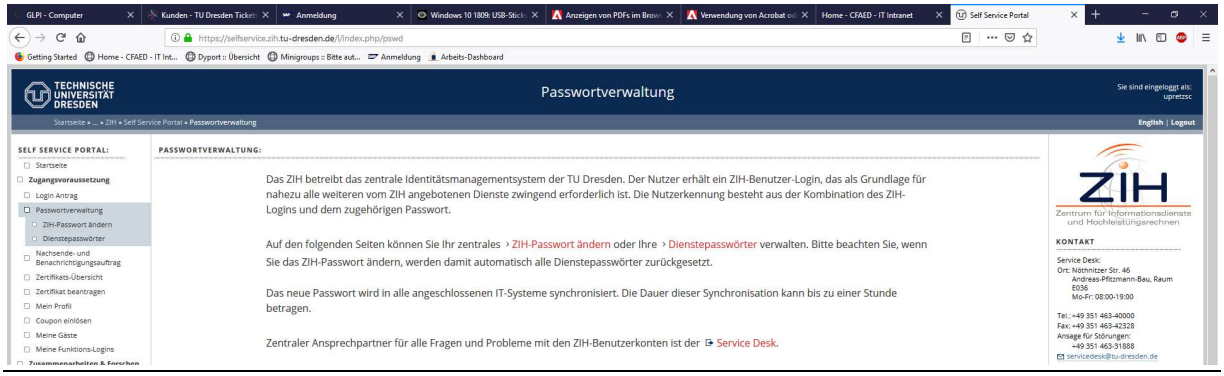
Das Login an CFAED PCs und Laptops erfolgt mit Domäne\zih-login und dem ZIH-Passwort, Bsp.:

- User = DOM\mmuster
- Passwort =ZIH Passwort von mmuster

Ist ein anderer Nutzer angezeigt muss vorher im Anmeldebildschirm auf „Other User“ gewechselt werden.

Eine Passwortänderung des ZIH-Logins ist nur über das Selfservice Portal der TUD (hier muss sich ebenfalls vorher mit dem ZIH-Login angemeldet werden) möglich:

https://selfservice.zih.tu-dresden.de/



E-Mail (Outlook, OWA)

Jeder CFAED und TUD Mitarbeiter erhält eine Mailbox auf dem TUD Exchangeserver. Unter Windows wird die Nutzung des E-Mailclients ***Outlook*** und unter Linux der E-Mailclient ***Evolution*** empfohlen. Nur mit diesen Mailclients ist eine direkte Exchange-Anbindung (zur Nutzung von gemeinsamen Kalendern und gemeinsamen Postfächern möglich).

Die Nutzung weiterer E-Mailclients, z.B. Thunderbird ist aber über das Protokoll IMAP ebenfalls möglich. Nur die Kalender müssen dann über Plugins eingebunden werden.

Mobile Geräte können die Exchange-Postfächer über ***Active Sync*** einrichten. ***Die Nutzung der Outlook-Apps bei Androids und iPhones ist verboten und gesperrt, hier bitte andere Apps wie z.B. Gmail nutzen.***

ZIH Anleitungen:

https://tu-dresden.de/zih/dienste/service-katalog/zusammenarbeiten-und-forschen/groupware/exchange/Anleitungen

ggf. einzugebende Nutzerdaten:

- server = msx.tu-dresden.de
- user / email = zih-login@msx.tu-dresden.de (nicht die vorname.nachname@tu-dresden.de Mail verwenden, sonst funktioniert das Auto-Discovery nicht)
- passwort = zih-passwort
- domäne = USER

WLAN (eduroam, CAT)

Zur Nutzung von eduroam ist ein gültiges ZIH-Login notwendig. Bei Windows PCs ab Windows 8.1. sind lediglich die Zugangsdaten anzugeben:

- User = zih-login@tu-dresden.de
- Passwort = zih-passwort

Anleitungen für andere Clients:

https://tu-dresden.de/zih/dienste/service-katalog/arbeitsumgebung/zugang_datennetz

Bei mobilen Geräten empfiehlt sich die Einrichtung über die Eduroam CAT App. Hierfür muss zuerst die nötige App installiert und die jeweilige Konfiguratiosndatei heruntergeladen werden.

https://tu-dresden.de/zih/dienste/service-katalog/arbeitsumgebung/zugang_datennetz/#section-1-1-2

Gast WLAN und VPN

Für Gäste ist die Nutzung des unverschlüsselten WLANs VPN-Web mit webbasierter VPN Lösung möglich.

https://tu-dresden.de/zih/dienste/service-katalog/arbeitsumgebung/zugang_datennetz/wlan_gast
https://tu-dresden.de/zih/dienste/service-katalog/arbeitsumgebung/zugang_datennetz/vpn/webvpn

---

Anmeldung:

- User = zih-login@tu-dresden.de
- Passwort = zih-passwort

Hierüber können zahlreiche TUD Dienste genutzt werden.

VPN (allgemein, cfaed VPN)

Um von außerhalb auf die CFAED Netze und Ressourcen zu kommen muss eine VPN Verbindung hergestellt werden. Empfohlen wird hier CISCO AnyConnect.

1. ZIH Anleitungen und Downloads:
   https://tu-dresden.de/zih/dienste/service-katalog/arbeitsumgebung/zugang_datennetz/vpn
2. Für manche Dienste (SLUB) kann es nötig sein, den C-Tunnel als Group zu verwenden, Erklärungen zu den Tunneln, siehe folgender Link:
   https://tu-dresden.de/zih/dienste/service-katalog/arbeitsumgebung/authentifizierungsdienst/2_faktor_auth#section-4

Anmeldedaten für das CFAED VPN:

- Server = vpn2.zih.tu-dresden.de
- Group = A-Tunnel-TU-Networks
- User = zih-login@vpn-cfaed-ma
- Passwort = zih-passwort

Aus dem CFAED VPN heraus ist folgende Nutzung möglich:

- Cfaed Drucker
- Cfaed Dateiserver
- Cfaed sonstige Server
- RDP und SSH Verbindung in die Labornetze
- Nutzung der cfaed Netzlizenzen (Origin, Matlab, Mathematica, Autodesk)

Benutzer-Profile

Auf den CFAED Rechner werden zwei Profilarten unterschieden:

- Laptops => lokale Benutzerprofile (außer Leihgeräte)
- PCs => Roaming Profils von Microsoft

Bei Nutzung der ***lokalen Benutzerprofile*** wird zusätzlich die Nutzung des UrBackup Clients, ***siehe Client-Backup***, empfohlen um Benutzer Profildaten zu sichern. Die Anmeldung bei lokalen Profilen erfolgt schneller, es wird aber nichts auf einem zentralen Server gesichert. Bei Verlust der lokalen Daten sind diese, bis auf im Backup vorhandene Sicherungen, verloren.
Diese Nutzung wird an Rechnern mit Einzelnutzern bevorzugt.

Bei Nutzung der ***Roaming Profiles*** wird das Nutzerprofil bis zu max. 1 GB Größe auf einem zentralen Server gespiegelt. Die Nutzerordner Downloads, Dokumente, Videos, Musik, Bilder werden mit dem Microsoft Sync-Center auf einen zentralen Speicher synchronisiert. Dadurch dauert die Anmeldung etwas länger, aber ein Nutzer bekommt auf allen PCs mit dieser Profilart seine Arbeitsumgebung identisch bereitgestellt.
Diese Nutzung wird hauptsächlich an PCs mit Mehrbenutzerbetrieb (Studenten etc.) angewendet.

Netz-Laufwerke

Batchdateien für manuelle Verbindungen:

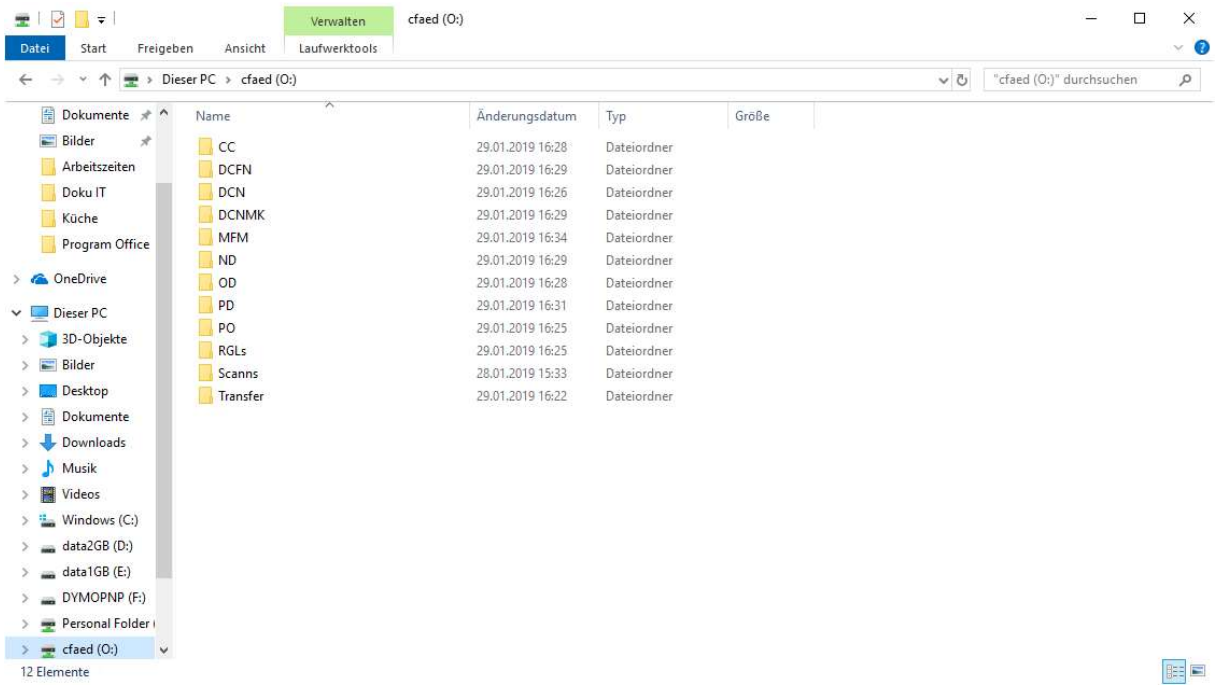
https://intranet.cfaed.tu-dresden.de/it/index.php/Downloads?dir=vFiler%20Batch%20Dateien/

Bei Problemen mit der vfiler.cmd die vfiler-Homeoffice.cmd verwenden!

Das cfaed betreibt einen eigenen vFiler auf der NetApp des ZIH. Die Berechtigungen hierfür werden von den cfaed Administratoren über ZIH IDM Gruppen vergeben.

Nach Anmeldung an den Windows-Rechnern wird automatisch das cfaed DFS Laufwerk O:\ eingebunden. Unter diesem sind die Ordner aller Gruppen und Professuren zu finden. Zugriff bekommt der Nutzer aber nur auf für Ihn freigegebene Ordner.

Außerdem wird das ZIH Nutzer Homelaufwerk als Laufwerk H:\ eingebunden.



Zusätzlich liegt auf dem Desktop der Rechner unter c:\temp eine cfaed-vFiler.cmd (Verknüpfung auf dem Desktop cfaed-Netzlaufwerke-Script). Diese wird benötigt zum Laufwerke verbinden von außerhalb der TUD über VPN. Diese mountet die Laufwerke identisch wie oben im Screenshot zu sehen.

Unter Linux und Mac OS X müssen die Laufwerke manuell über smb eingebunden werden. Es gibt zwei Laufwerke die gemountet werden müssen:
Gesonderte Anleitung für Linux (für automatische Verbindung mit Gigolo, gibt's in allen Distributionen):
https://intranet.cfaed.tu-dresden.de/it/data/_uploaded/downloads/Manuals/SMB%20automatisch%20mit%20Linux%20mounten%20mit%20Gigolo.pdf

- Smb://vf-home.zih.tu-dresden.de/zih-login = Nutzer-Home-Laufwerk
- Smb://cfaed.ing.dom.tu-dresden.de/cfaed = cfaed Laufwerk (DFS)

Unter Windows können die Laufwerke ebenso gemountet werden. In Windows aber Backslash anstatt Slash und kein Kürzel Smb: verwenden. Bsp.: \\vf-home.zih.tu-dresden.de\<zih-login>

Netzwerk-Drucker

Alle cfaed Drucker können als Netzwerkdrucker eingerichtet werden. Es gibt insgesamt drei Netzwerkdrucker:

- \\141.76.69.4 = automatische Druckereinrichtung über die Domainanmeldung
- \\141.76.18.120 = manueller Druckserver für Nicht-Domain-Rechner (vorne URL öffnen, Drucker suchen -> rechte Maustaste -> connect (dauert etwas bis die Druckertreiber geladen und eingerichtet sind))
    - Anleitung: https://cfaed-intranet.et.tu-dresden.de/data/_uploaded/file/Druckereinrichtung%20mit%20Authentifizierung.pdf
    - für Linux und Mac OSX mit LDP nutzbar, z.B. ldp://141.76.18.120/BAR-E82-MP_C307-A4COLOR (Druckername steht auf dem Drucker)
- Linux CUPS Printserver (Anleitung folgt noch)

Standardmäßig sind alle Drucker auf SW eingestellt. Um Farbe zu drucken muss im Druckermenü unter Einstellungen auf COLOR umgestellt werden.

Software Installation

Folgt noch

Software Netzwerklizenzen

Das cfaed hat Zentral folgende Netzwerklizenzen:

- 20 x Matlab alle Module
- 5 x Mathematica
- 1 x Institutslizenz Origin Pro (100)
- 5 x Autodesk (Inventor, AutoCAD Architecture, AutoCAD Electrical, AutoCAD Mechanical, Nastran In-CAD)

Die Nutzung dieser Lizenzen ist innerhalb der cfaed Netze ohne VPN möglich und von außerhalb der TUD über das cfaed VPN.

AntiVir

Die Nutzung einer Anti-Virensoftware ist zwingend erforderlich. Auf Mac OSX und Windows wird daher die an der TUD für alle Nutzer kostenlose Software ***Sophos Endpoint Protection*** empfohlen. ***Eine Deinstallation dieser Software durch den Nutzer ist nicht gestattet. Bei Problemen hiermit ist die IT zu informieren.***

Linux Nutzer sollten sich ebenfalls eine Anti-Virensoftware installieren. Nicht weil Sie selbst gefährdet sein könnten, sondern weil Sie ggf. verseuchte Dateien mit anderen Nutzern über Netzwerk austauschen können.

Empfehlung:

Verschlüsselung

Bei dienstliche Notebooks sind die Festplatten komplett zu verschlüsseln um den Diebstahl von Daten bei Verlust zu verhindern. Bei Linux und Mac OSX kann die systemeigene Verschlüsselung verwendet werden.

Unter Windows wird hier das Produkt Bitlocker von Microsoft verwendet:

Anmerkungen:

- Vor jeglicher Hardwareänderung (BIOS Updates, Treiberupdates etc.) sollte der Bitlocker in der Windows Systemsteuerung auf ***Suspend*** gesetzt werden. Ansonsten kann das System ggf. nicht booten und verlangt den Bitlocker-Recovery-Key beim Start.
- Eingesteckte USB Sticks oder Festplatten können beim Start ebenfalls als Hardwareänderung angesehen werden und das System bleibt beim Bitlocker-Recovery-Key hängen (das Notebook einfach hart ausschalten, die USB-Geräte entfernen und nochmal starten)
- Der Bitlocker-Recovery-Key wird bei den Domain-Rechnern automatisch im Active-Directory gesichert. Wird dieser benötigt, dann am besten an die IT wenden.

Client-Backup (Laptops, Labor, PCs, Gruppenlaufwerke)

Auf allen Notebooks und Laborgeräten ist der UrBackup Client installiert. Auf den Notebooks findet eine Dateisicherung statt und auf den Laborgeräten eine Festplatten-Image-Sicherung.

Standard-Backupeinstellungen:

- Backup der Nutzerprofile c:\User\... (darin enthalten die Benutzerordner Documents, Desktop etc.)
- Zusätzlich im Backup c:\temp (wird empfohlen für eigene (auch Portable Programme) Programme, besonders bei den PCs mit Roaming Profiles)

Weiteres folgt! Noch nicht fertig!