1 Anleitung RDS-(VPN-) Zugang

1.1 Einleitung

Die in der Folge beschriebene RDS-(VPN-)Lösung ist für den Zugriff auf Business-Anwendungen gedacht, welche am KBZ oder der Akademie im Einsatz sind. Die Nutzung soll aus Performance-Gründen nur dann erfolgen, wenn unbedingt notwendig.

Es steht lediglich eine bestimmte Anzahl Zugriffe zur Verfügung, welche nach dem First Come - first serve Prinzip vergeben werden. Ist die Anzahl Zugriff ausgeschöpft, erscheint einer Meldung, dass keine weiteren Benutzer zugelassen werden. Aus diesem Grund sollte der Zugriff nur wenn notwendig verwendet und nach der Nutzung raschmöglichst wieder freigegeben werden (siehe Kap. 4 Abmeldung). Es ist davon auszugehen, dass mit jedem Teilnehmenden die Performance abnimmt.

Machen Sie sich mit dem Dokument vertraut, bevor Sie den Zugang in Betrieb nehmen. Neben Installations- und Funktionshinweisen sind die aufgeführten Sicherheitshinweise verbindlich zu berücksichtigen.

1.2 Leistungsumfang

Mit Hilfe des RDS-Zugangs erhalten die berechtigten Personen Zugriff auf die IT-Umgebung am KBZ und der Akademie. Der Zugriff umfasst dabei die folgenden Bereiche:

- Business Anwendungen, inbesondere der speziellen Anwendungen wie Displaysoftware, PerformX oder PowerBI
- Netzwerkdrucker von KBZ und der Akademie
- Persönliche und lokal installierte Geräte / Drucker
- Zwischenablage
- Sämtliche Netzlaufwerke
- Persönliches OneDrive-Laufwerk

1.3 Verantwortung der Benutzer

Die Nutzer tragen in Bezug auf Verwendung der Infrastruktur (PC, Mac) die volle Verantwortung, insbesondere für:

- Den eigentlichen Zugriff, welcher ausschliesslich über persönliche oder vertraute Hardware zu erfolgen hat (und nicht über fremde Hardware, wie z.B. öffentliche WLAN in Internet-Cafes, frei zugängliche Geräte in Hotels, Verkehrsmitteln, Messen sowie öffentlichen Räumen)
- Softwareversionen von Betriebssystem sowie Office und Browser auf der persönlichen Hardware sind aktuell und die Sicherheitsupdates werden regelmässig gemacht

Bei der Nutzung des RDS-Zugriffs sind die folgenden Regeln zu beachten:

Verbot	Lösung
Nutzung offener Netzwerke z.B. in Restaurants oder öffentlichen Räumen	Hotspot auf dem eigenen Mobile einrichten
Keine grafikintensiven Anwendungen wie z.B. Adobe Premiere, nanoo.tv o.ä. verwenden	Grafikintensive Anwendungen lokal installieren und nutzen
Surfen im Internet / Filme streamen	Lokal zugreifen, ausserhalb von RDS surfen

2 Registrierung Multifaktor-Authentifizierung

2.1 Einleitung

Unter Multifaktorauthentifizierung (MFA) versteht man die Absicherung der Zugriffsberechtigung auf dem RDS-Zugang. Mit diesem wird der Benutzer neben dem Username / Passwort zusätzlich in Kombination mit dem Mobile authentifiziert.

2.2 App-Installation

Der MFA-Zugriff erfordert die Installation des „Microsoft Authenticator“-Apps auf dem persönlichen Handy. Dieses kann aus den gängigen Stores heruntergeladen werden:

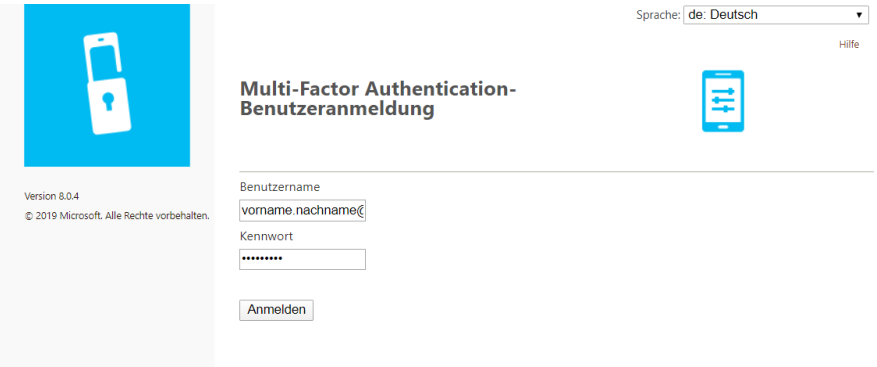
Apple-Store	Google-Play-Store

2.3 Einmalige Einrichtung der Authentifizierung

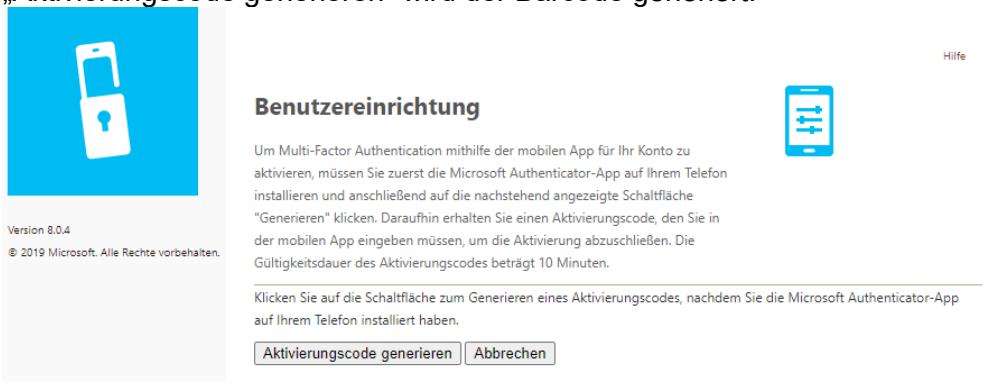
Der Zugriff für den Benutzer geschieht im ersten Schritt über den Arbeitsplatz (nicht Mobile) des User-Portals in einem Browser unter: **https://mfa.cl03.ch**

Unter Benutzername ist die folgenden Zeichenkette einzugeben:
vorname.nachname@kbzsg.ch bzw. **vorname.nachname@akademie.ch**

Unter Passwort ist das bekannte User-Passwort vom Arbeitsplatz zu erfassen

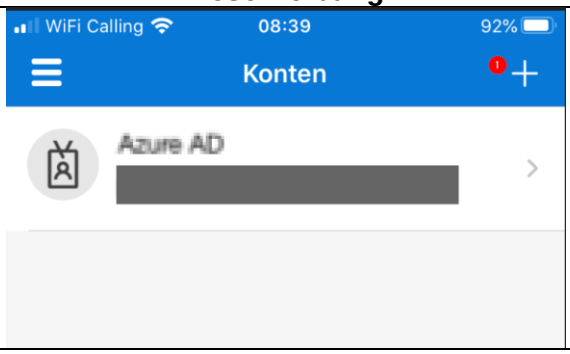


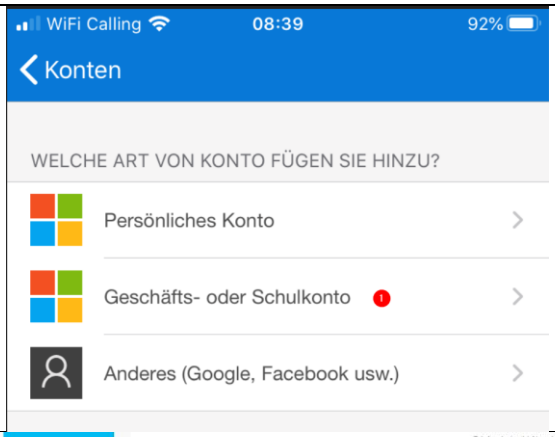
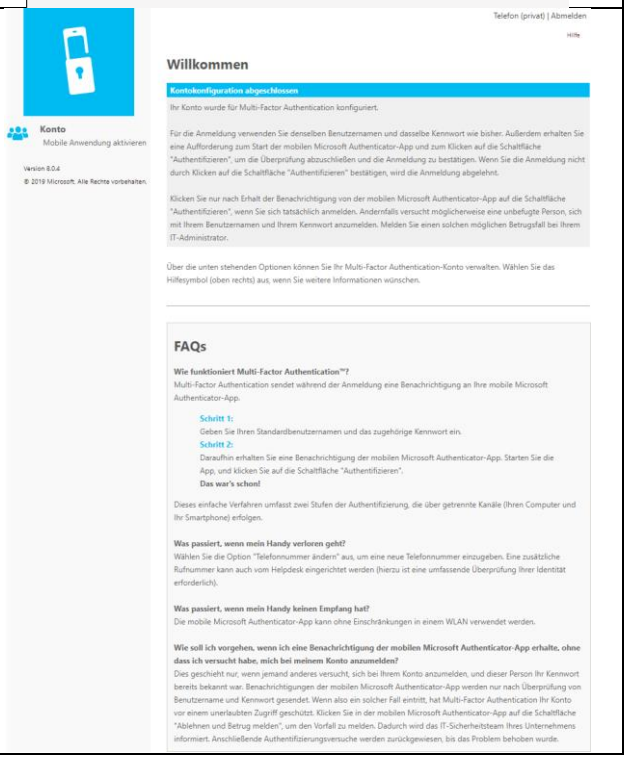
Nach der Anmeldung erscheint die Benutzereinrichtung. Durch Drücken des Buttons „Aktivierungscode generieren“ wird der Barcode generiert.



Der generierte Barcode wird auf dem Bildschirm angezeigt.

Nun kann auf dem Mobile das App „Authenticator“ gestartet und die Authentifizierung eingerichtet werden.

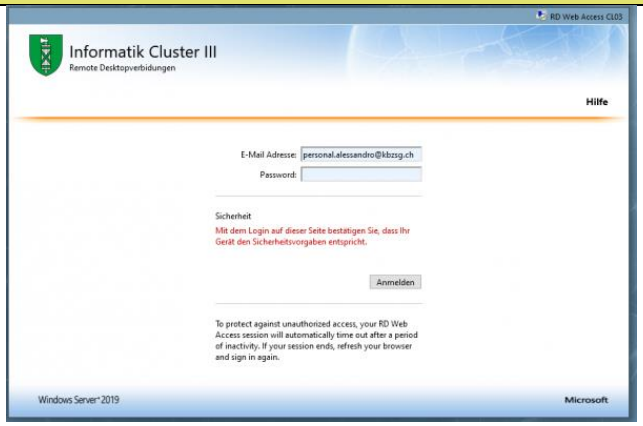
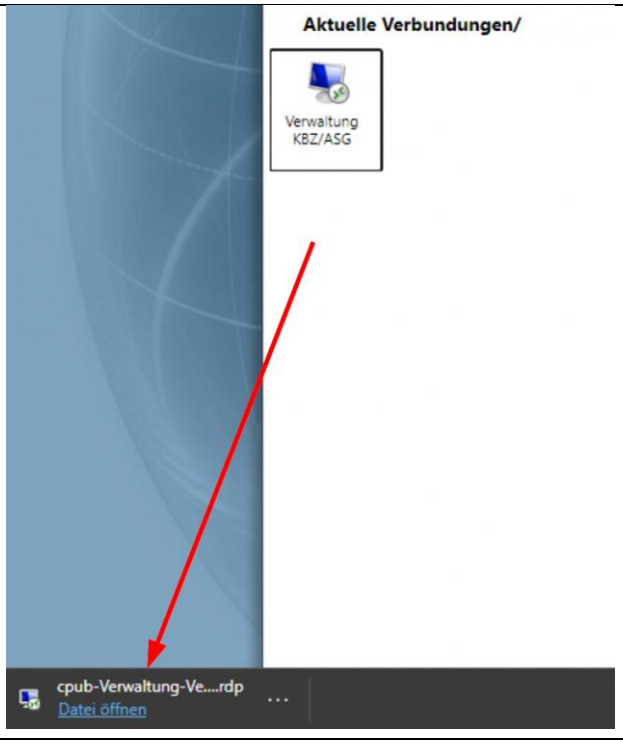
Schritt	Beschreibung
Über das Symbol + kann ein neues Konto hinzugefügt werden.	

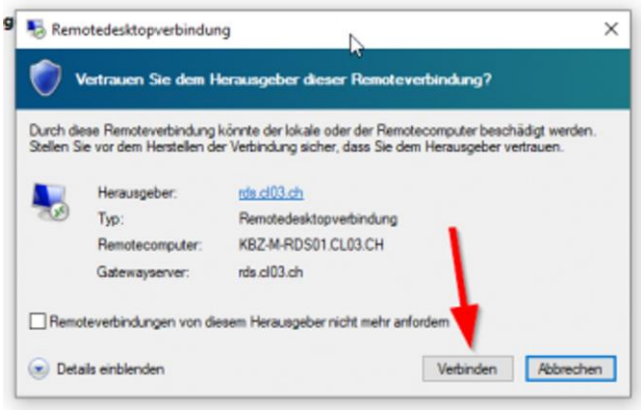
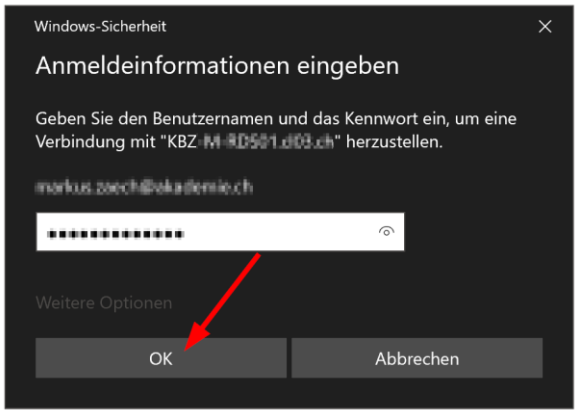
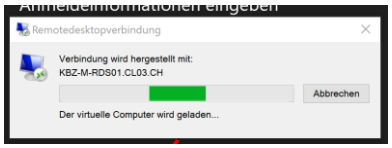
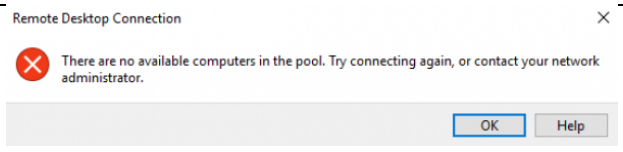
Durch die Selektion des „Geschäfts- oder Schulkonto“ kann nun im nächsten Schritt der Code gescannt werden.	
Wurde der Code erfolgreich gescannt, so bestätigt der Browser die erfolgreiche Einrichtung	

Hinweise:
Die Einrichtung ist nun abgeschlossen und die Anmeldung am RDS kann nun erfolgen.
Für die Anmeldung und Authentifizierung ist nun immer das Mobile erforderlich!

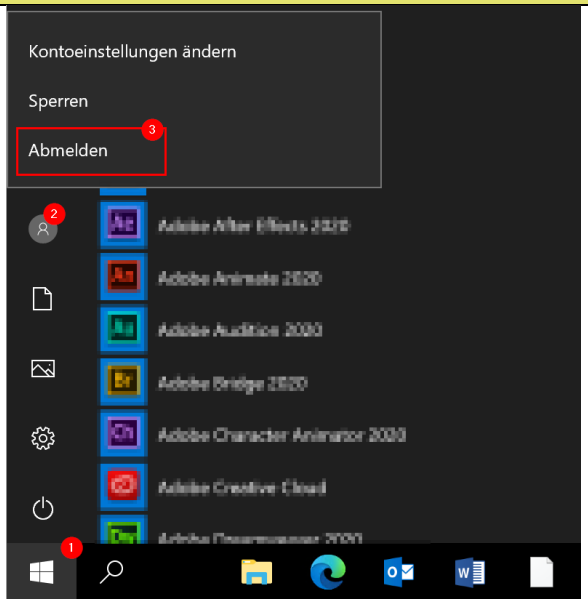
3 Anmeldung

Hinweis: Bitte Mobile für die Authentifizierung bereithalten

Schritt	Abbildung
Remote Desktop Verbindungen Web Access aufbauen https://rds.cl03.ch Anmelden mit eigener E-Mail Adresse und Kennwort (normales Kennwort vom KBZ/ASG Konto) wichtig: inkl. @ !!	
Die gewünschte Verbindung auswählen Hinweis: mit dem Selektieren der Verbindung wird das RDP-File heruntergeladen, welches in der Fusszeile des Browsers erscheint	
Das heruntergeladene RDP-File kann mittels anklicken von „**Datei öffnen**“ ausgeführt werden. Das System startet nun den Desktop.	

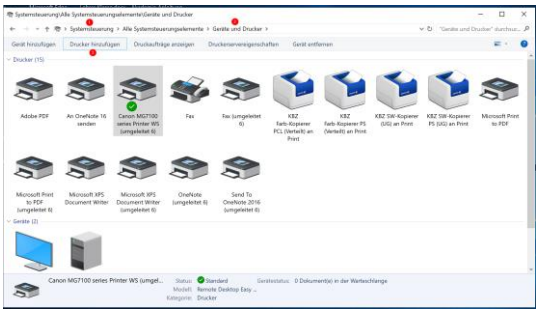
Bestätigen der Verbindung: Beim ersten Start der Verbindung erfolgt eine Rückfrage nach der Vertrauenswürdigkeit der Verbindung. Dies kann durch Selektion des Buttons „Verbinden“ bestätigt werden.	
Starten des Desktops: Anmeldeinformationen wie gewohnt eingeben: Username und Passwort eingeben und mit „OK“ bestätigen.	
Multifaktor-Authentifizierung in der App auf dem Mobile: Auf dem Handy / Mobile erscheint nun die rechtsstehende Meldung. Diese kann mittels „Genehmigen“ bestätigt werden.	
Der Desktop startet nun auf. Die Startgeschwindigkeit hängt von mehreren Faktoren ab und kann zwischen 30 und 90 Sekunden dauern	Meldung 1 → Verbindungsaufbau  Meldung 2 → Desktop und Profil laden 
Sind alle Lizenzen vergeben, erscheint nebenstehende Meldung. Lösung: Bei den Arbeitskollegen (z.B. im Chat) nachfragen, wer den Account freigeben kann und wieder versuchen	

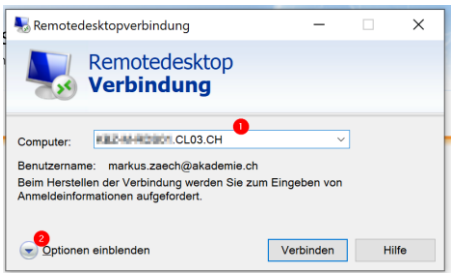
4 Abmeldung

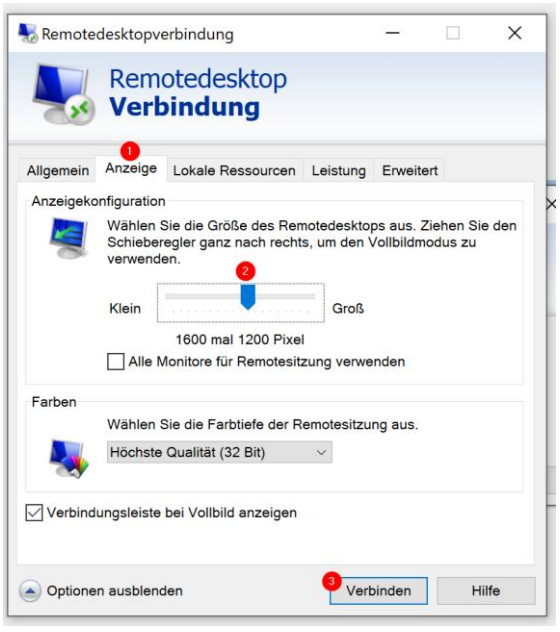
Schritt	Abbildung
Am Ende der Arbeiten ist die Verbindung sauber zu trennen. Nur dann werden die Lizenzen wieder freigegeben. Die Abmeldung erfolgt aus diesem Grund nicht über das gewohnte „Herunterfahren“, sondern über „Windows“ und „Abmelden“ Hinweis: Die Abmeldung dauert bis 45 Sekunden. Auf keinen Fall das Fenster schliessen, weil dann die Linzenz nicht freigegeben wird.	

5 Wissenswertes und Tipps zu RDS

<table>
<tr><th>Thema</th><th>Abbildung</th></tr>
<tr><td>Drucken
1. Installieren Sie private Drucker über die Systemsteuerung und den Button „Drucker hinzufügen“
2. Selektieren Sie den gewünschten Drucker
3. Der Druckertreiber wird nun installiert und steht zum Drucken zur Verfügung

Hinweis: installierte, private Drucker können nicht mehr entfernt werden. Dazu mit der IT Kontakt aufnehmen.</td><td>Drucker hinzufügen:
  </td></tr>
<tr><td>Auflösung Bildschirm (Diese Option steht nicht allen Benutzern zur Verfügung)

Standardmässig wird RDS im Vollbild gestartet. Bei grossen Bildschirmen kann es sich lohnen, das Fenster zu verkleinern, damit RDS als Task gewechselt werden kann.
Zu diesem Zweck muss das App „Remotedesktopverbindung“ gestartet werden:
1. Server selektieren
2. Optionen einblenden
3. Unter „Anzeige“ kann nun die Auflösung eingestellt und gespeichert werden.
4. Mittels „Verbinden“ werden die neuen Einstellungen übernommen und angewandt
Tipp: Die richtige Auflösung muss in den meisten Fällen ausgetestet und mehrfach adaptiert werden. Ebenfalls hängt diese Auflösung von der Qualität des Bildschirms ab. Die Auflösung kann beliebig viele Male angepasst werden.</td><td>App starten
 

Auflösung anpassen
 
</td></tr>
<tr><td colspan="2">Kopieren von Files und Inhalten
Für das Kopieren von Files und Inhalten müssen keine Mails an die eigene Mailadresse versandt werden.
1. Zwischenablage
Mittels Kopieren (CRTL+C und CRTL+V, resp. Kontexmenu) können Files und Inhalte (z.B. Texte) vom lokalen Gerät auf RDS kopiert werden.</td></tr>
</table>

2. **OneDrive**
   Auf dem RDS steht das Laufwerk B: zur Verfügung. Über dieses können die Files einfach nach OneDrive und auf andere Geräte übertragen werden.

Sicherheitshinweis:
Es dürfen nur Dateien kopiert werden, bei welchen sich der Benutzer sicher ist, dass diese nicht durch Malware oder Viren verseucht sind. Im Zweifelsfalle ist auf diese Funktion zu verzichten.

Systemabstürze auf dem lokalen Gerät

Einer der Vorteile von RDS ist, dass die Session auch nach einem lokalen PC-Absturz im Hintergrund weiterläuft und wieder verbunden werden kann.
Dabei ist zu beachten, dass die Session spätestens eine Stunde ohne „Traffic“=Nutzung vom System getrennt wird. In diesem Fall werden die Anwendungen beendet und die Session muss neu gestartet werden.

Versionsdatum: Version 2.1
Autor: Zäch Markus AKADEMIE