ZIM Zentrum für Informationstechnologie und Medienmanagement

UNIVERSITÄT PASSAU

Handbuch zur Benutzung von Citrix
Private Geräte – Linux

Herausgeber: Zentrum für Informationstechnologie und Medienmanagement (ZIM)

Inhaltsverzeichnis

1 CITRIX ALLGEMEIN

1.1 Internes- und Externes-Netzwerk

Die Verbindung zum digitalen Arbeitsplatz (Digital Workspace) kann sowohl aus dem internen Netz der Universität als auch von einem externen Netzwerk aufgebaut werden.

Intern	in einem Universitätsbüro per Kabel mit dem Netzwerk verbunden
Extern	WLAN an der Universität, Netzwerk zuhause oder weltweit

1.2 Private Geräte

Rechner und Laptops

Sollten Sie ein privates Gerät verwenden auf dem das Betriebssystem **Linux** eingerichtet ist, beachten Sie bitte die **Mindestanforderungen,** welche von **Citrix Systems, Inc.** in offiziellen Dokumenten vorgesehen sind.

2 Einrichten von Citrix

Zum Einrichten von Citrix auf Privatgeräten müssen mehrere Faktoren beachtet werden. Hierbei gibt es mehrere Möglichkeiten Citrix zu nutzen, welche in diesem Kapitel dargestellt werden.

Aus Sicherheitsgründen ist für Zugriffe aus externen Netzbereichen (z.B. für Homeoffice, Zugriff aus dem WLAN der Uni etc.) eine sogenannte „**Zwei-Faktor-Authentifizierung**“ (2FA) notwendig. Um von extern auf Citrix zugreifen zu können, müssen Sie daher ein zweites Gerät (z.B. Ihr Smartphone oder Tablet mit dem Sie nicht auf die Citrix-Umgebung zugreifen) **für die 2FA einrichten** um darauf **Einmalpasswörter** generieren zu können.

2.1 Citrix-Systemanforderungen – Betriebssystem Linux

Über den Link finden Sie eine Übersicht der Systemanforderungen an das Gerät, welche von **Citrix Systems, Inc.** in offiziellen Dokumenten vorgeschlagen werden.

Nachdem nun die Systemanforderungen an das Gerät bekannt sind, kann im Anschluss der externe Zugang für Privatgeräte eingerichtet werden.

2.2 Externer Zugang – Zwei-Faktor-Authentifizierung (2FA)

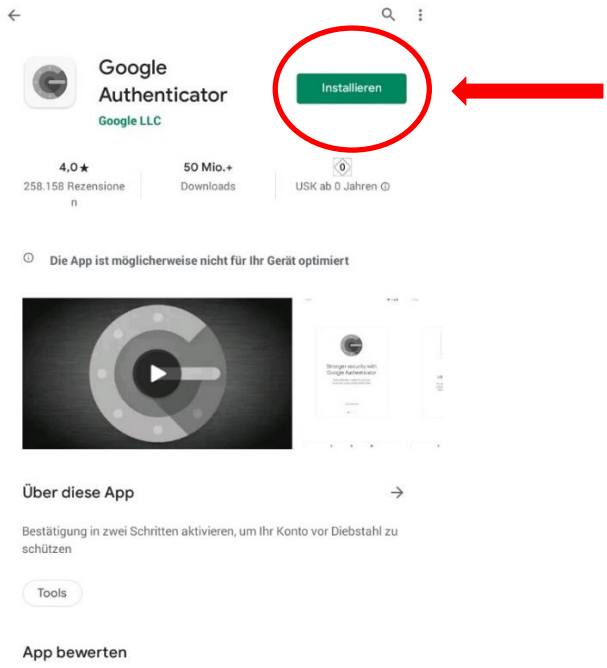
In diesem Abschnitt des Kapitels wird die Einrichtung der Applikation für das Einmalpasswort der Zwei-Faktor-Authentifizierung (2FA) erklärt. Wenn Sie ein iPhone oder iPad verwenden, können Sie direkt zur **iOS-Anleitung** springen, falls sie ein Android-Gerät verwenden, folgen Sie der **Android-Anleitung**.

Android

Hier wird das Einrichten der Applikation (App) auf einem Android-Gerät erklärt.

Schritt 1:

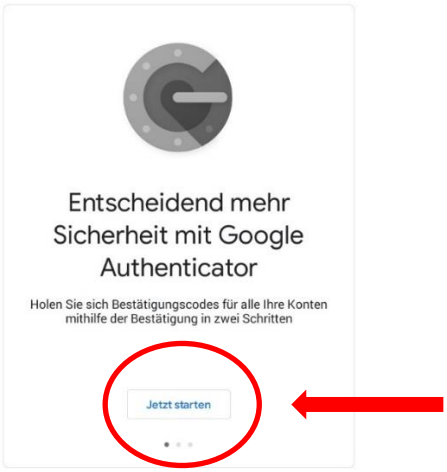
Bitte suchen Sie in Ihrem Google Play Store die App „Google Authenticator“.



Schritt 2:

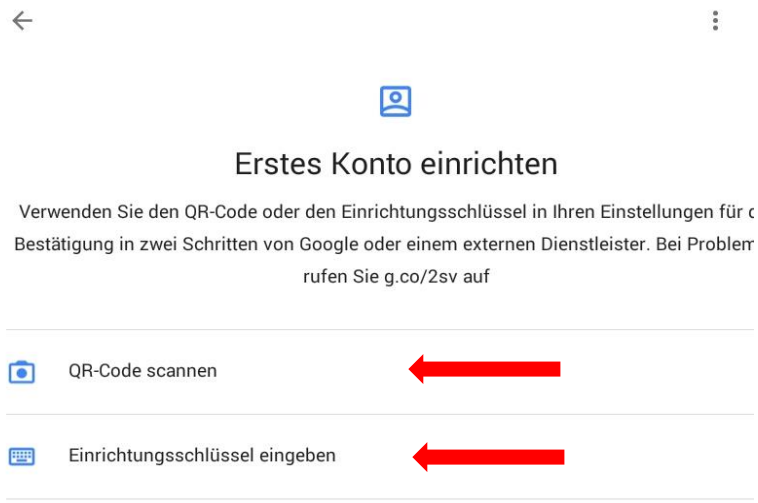
Bitte installieren Sie die App.

Nach erfolgreicher Installation der App auf einem Android-Gerät erscheint diese nun in der Übersicht aller installierten Apps auf ihrem Smartphone oder Tablet. Wenn die App nun geöffnet wird, sollte der folgende Bildschirm erscheinen:



Wenn Sie danach gefragt werden, ob ein Google-Konto hinzugefügt werden soll, können Sie diesen Schritt überspringen.

Schritt 3:
Klicken Sie auf „Start”. Anschließend sehen Sie ein neues Fenster, in welchem Sie ein Konto hinzufügen können.



Dabei haben Sie stets die Auswahl, einen Barcode zu scannen oder alternativ einen Schlüssel einzugeben. Wählen Sie eine der beiden Optionen, um Ihr Smartphone oder Tablet zu registrieren.
Der QR-Code ist auf dem Gerät zu finden, auf dem Sie Citrix nutzen wollen. Gehen Sie dazu auf **citrix-ext.uni-passau.de/manageotp**.

Hinweis: Wie Sie Ihr Gerät für die 2FA registrieren erfahren Sie in Punkt 2.1.3.

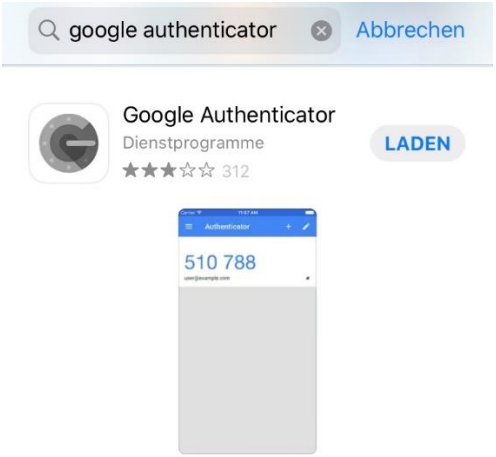
Schritt 4:
Nun ist die App auf Ihrem Android-Gerät verwendbar und kann mit Ihrer ZIM-Kennung verknüpft werden, um dort Einmalpasswörter generieren zu lassen, mit denen ein externer Zugang zu Citrix möglich ist.

iOS

Hier wird das Einrichten der Applikation auf einem iOS-Gerät erklärt.

Schritt 1:

Bitte suchen Sie in Ihrem App Store die App „Google Authenticator“.



Schritt 2:

Bitte installieren Sie die App.

Nach erfolgreicher Installation der App auf einem iOS-Gerät erscheint diese nun in der Übersicht aller installierten Apps auf Ihrem Smartphone oder Tablet. Wenn die App nun geöffnet wird, sollte der folgende Bildschirm erscheinen:

Schritt 3:
Klicken Sie auf „Einrichtung starten”, anschließend sehen Sie ein neues Fenster, bei dem Sie ein Konto hinzufügen können.

Dabei haben Sie stets die Auswahl, einen Barcode zu scannen oder alternativ einen Schlüssel manuell einzugeben. Wählen Sie eine der beiden Optionen, um Ihr Smartphone oder Tablet zu registrieren.
Der QR-Code ist auf dem Gerät zu finden auf dem Sie Citrix nutzen wollen. Gehen Sie dazu auf **citrix-ext.uni-passau.de/manageotp**.

Hinweis: Wie Sie Ihr Gerät für die 2FA registrieren erfahren Sie in Punkt 2.1.3.

Schritt 4:
Nun ist die Applikation auf Ihrem iOS-Gerät verwendbar und kann mit Ihrer ZIM-Kennung verknüpft werden, um dort Einmalpasswörter generieren zu lassen, mit denen man sich beim externen Zugang bei Citrix anmeldet.

2.3 Registrierung des Geräts

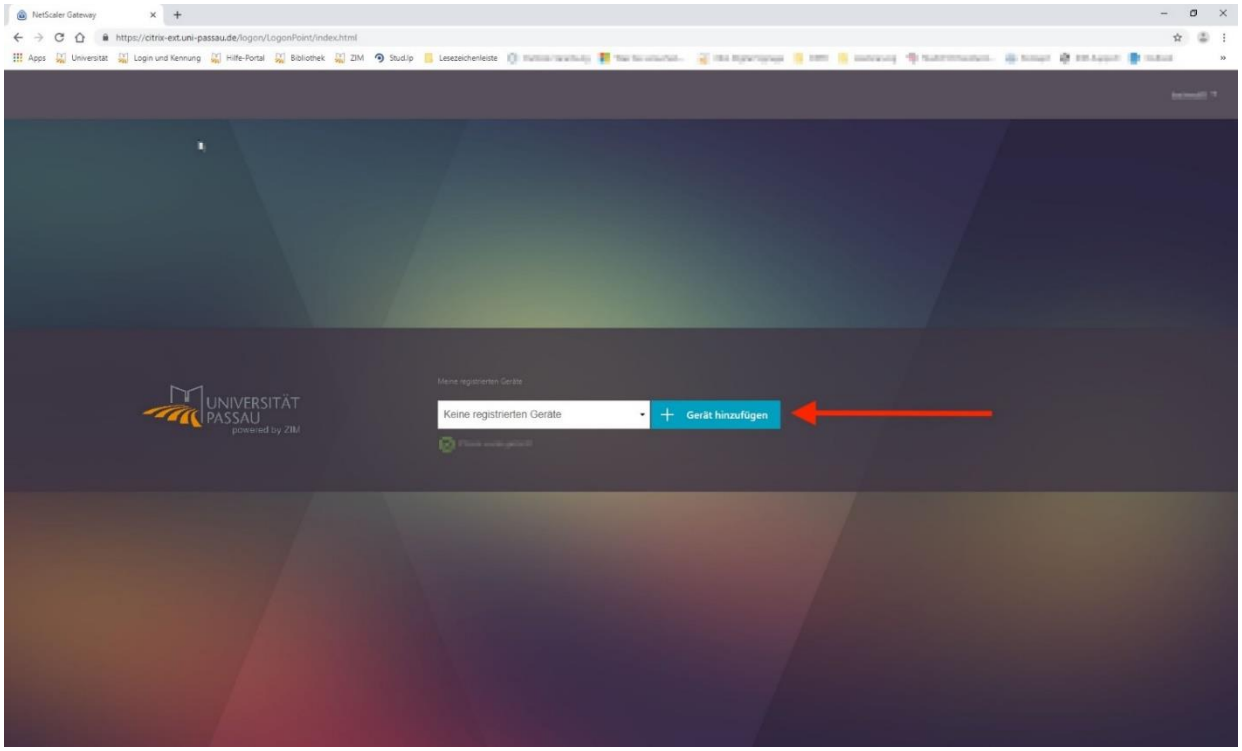
In diesem Abschnitt des Kapitels wird die Registrierung eines Gerätes über die 2FA erklärt. Wenn Sie ein iPhone oder iPad verwenden, können Sie direkt zur **iOS-Anleitung** springen, falls sie ein Android-Gerät verwenden folgen Sie der **Android-Anleitung**.

Android

Da nun die App auf ihrem Smartphone oder Tablet installiert ist, kann das Gerät registriert werden, um valide Einmalpasswörter für den externen Zugang zu generieren.

Erfolgt die Ersteinrichtung nicht im kabelgebundenen Netz der Universität, so können Sie **exakt (!) einmal** Ihr Smartphone oder Tablet für die Zwei-Faktor-Authentifizierung (2FA) auf der Webseite https://citrix-ext.uni-passau.de/manageotp einrichten.

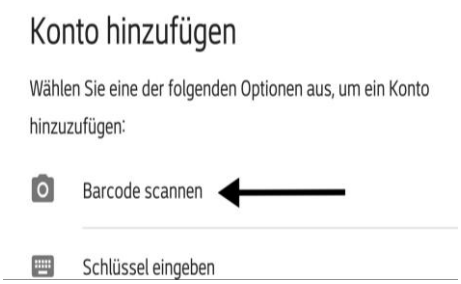
Bitte melden Sie sich auf der o.g. Website mit Ihrer ZIM-Kennung und Ihrem Passwort an:



Nachdem auf „Gerät hinzufügen" geklickt wurde, kann ein beliebiger Name für das Smartphone oder Tablet vergeben werden. Nach Eingabe des Namens wird eine Zeichenkette und ein QR-Code bereitgestellt.

Hinweis: Die Einrichtung der 2FA von Extern können Sie auf diesem Weg exakt einmal selbst für Ihr mobiles Smartphone oder Tablet vornehmen. Wenn Sie also z.B. ein neues Smartphone haben, loggen Sie sich unbedingt mit dem alten Gerät nochmals in Citrix ein, gehen Sie über den Browser VIA Citrix auf citrix-ext.uni-passau.de/manageotp und registrieren Sie dort das neue Gerät.
Sollten Sie diese Möglichkeit nicht mehr haben (z.B. durch Geräteverlust) oder auf weitere Probleme stoßen, so kontaktieren Sie bitte den ZIM-Support.

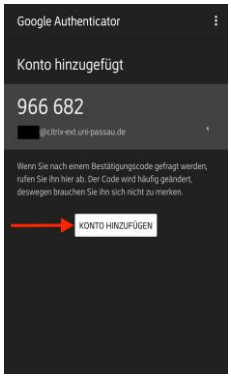
Schritt 1:
Klicken Sie auf „Starten” in der App. Anschließend ist der folgende Bildschirm zu sehen:



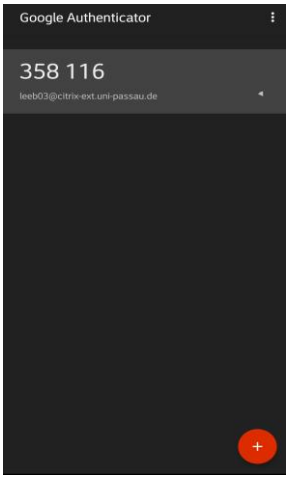
Schritt 2:
Dort wählen Sie dann die Option „Barcode scannen” und scannen den bereitgestellten Barcode.

Hinweis: Es ist zwingend erforderlich den Barcode-Scanner der App „Google Authenticator“ zu nutzen! Bitte scannen Sie den Code nicht mit einer anderen beliebigen App.

Anschließend sollte die App abfragen, ob das Konto wirklich hinzugefügt werden soll:



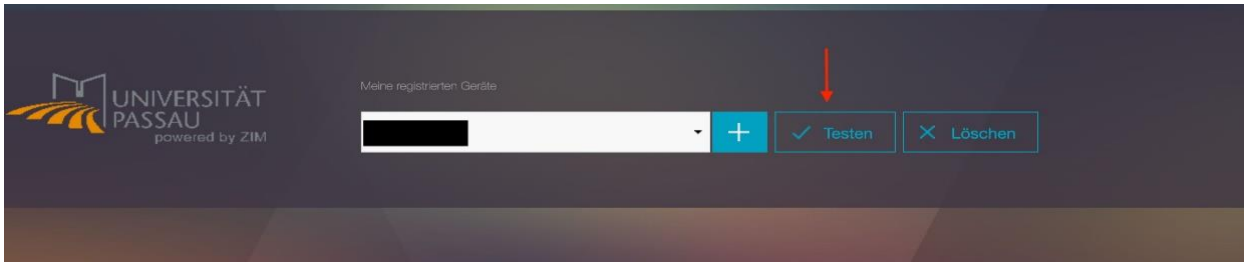
Schritt 3:
Nachdem das Konto hinzugefügt wurde, sollte die App folgendermaßen aussehen:



Nachdem der QR-Code erfolgreich gescannt wurde, sollte die Meldung erscheinen, dass das Gerät hinzugefügt wurde.

Registrierung des Geräts abschließen

Nachdem nun das Konto betriebsbereit eingerichtet wurde, sieht die Webseite zum Registrieren des Smartphones oder Tablets folgendermaßen aus:



Der vorhandene Button „Testen” ermöglicht eine Überprüfung, ob die Einrichtung erfolgreich war. Dazu klicken Sie auf den „Testen”-Button, anschließend kommt die Abfrage eines Einmalpassworts. Dazu in der App das Einmalpasswort ablesen, eingeben und bestätigen. Wenn der Test funktioniert, so ist die Zwei-Faktor-Authentifizierung (2FA) erfolgreich eingerichtet.

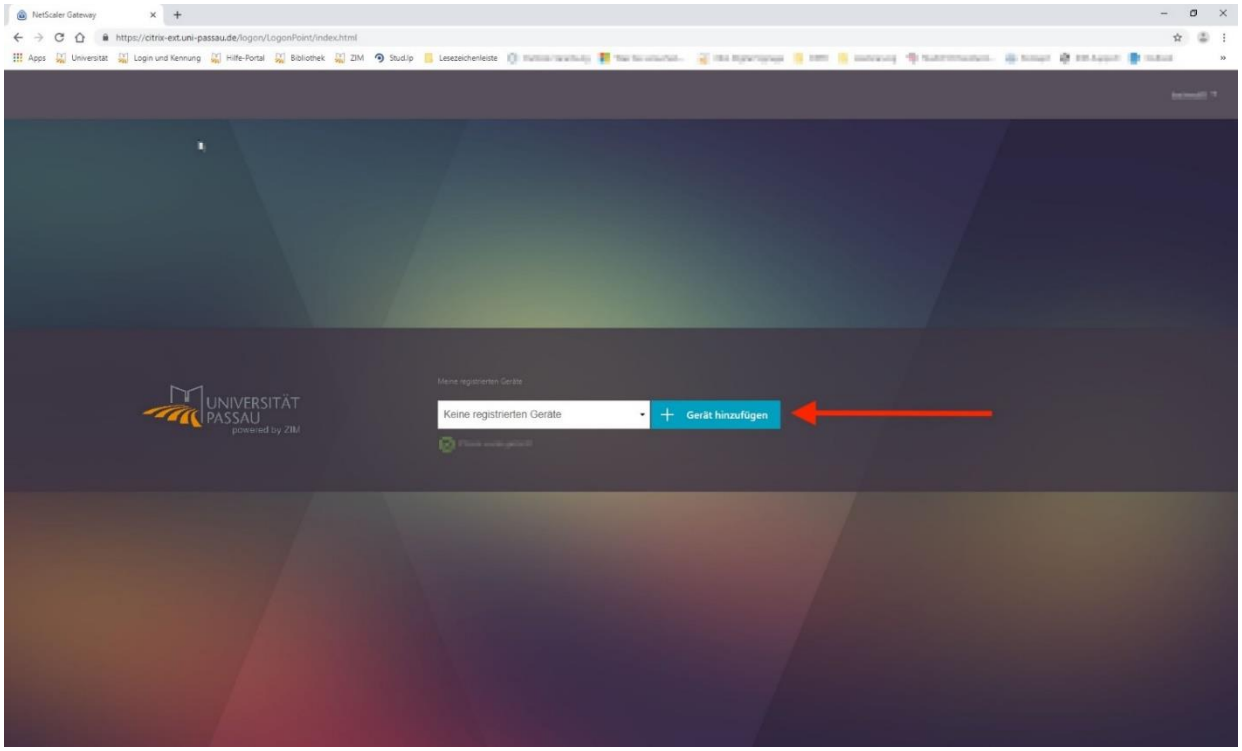
Hinweis: Stellen Sie sicher, dass Ihr Smartphone oder Tablet und Ihr Rechner die gleiche Uhrzeit eingestellt haben. Nur so ist die 2FA valide.

iOS

Da nun die App auf ihrem Smartphone oder Tablet installiert ist, kann das Gerät registriert werden, um valide Einmalpasswörter für den externen Zugang zu generieren.

Erfolgt die Ersteinrichtung nicht im kabelgebundenen Netz der Universität, so können Sie **exakt (!) einmal** Ihr Smartphone oder Tablet für die Zwei-Faktor-Authentifizierung (2FA) auf der Webseite https://citrix-ext.uni-passau.de/manageotp einrichten.

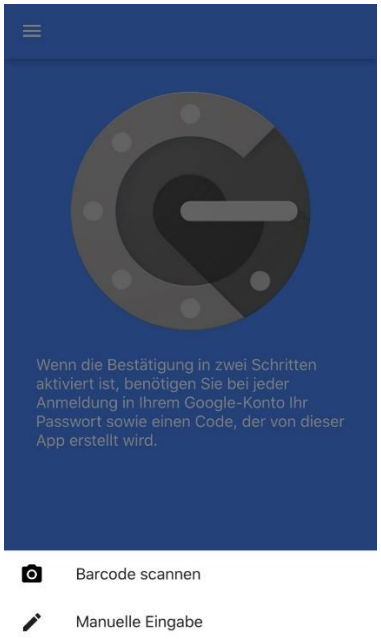
Bitte melden Sie sich auf der o.g. Website mit Ihrer ZIM-Kennung und Ihrem Passwort an:



Nachdem auf „Gerät hinzufügen" geklickt wurde, kann ein beliebiger Name für das Smartphone oder Tablet vergeben werden. Nach Eingabe des Namens wird eine Zeichenkette und ein QR-Code bereitgestellt.

Hinweis: Die Einrichtung der 2FA auf diesem Weg können Sie exakt einmal selbst für Ihr mobiles Smartphone oder Tablet vornehmen. Wenn Sie also z.B. ein neues Smartphone haben, loggen Sie sich unbedingt mit dem alten Gerät nochmals in Citrix ein, gehen Sie über den Browser VIA Citrix auf citrix-ext.uni-passau.de/manageotp und registrieren Sie dort das neue Gerät.
Sollten Sie diese Möglichkeit nicht mehr haben (z.B. durch Geräteverlust) oder auf weitere Probleme stoßen, so kontaktieren Sie bitte den ZIM-Support.

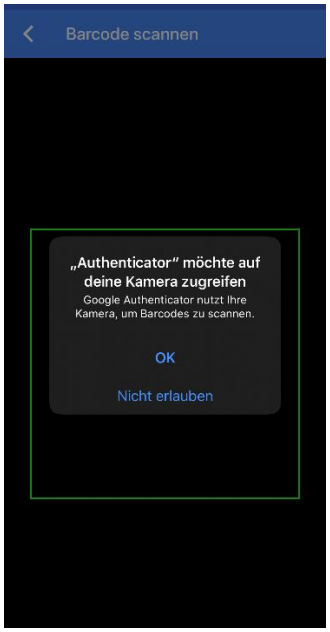
Schritt 1:
Klicken Sie auf „Einrichtung starten” in der App. Anschließend ist der folgende Bildschirm zu sehen:



Schritt 2:
Klicken Sie zum Scannen des QR-Codes auf „Barcode scannen”.

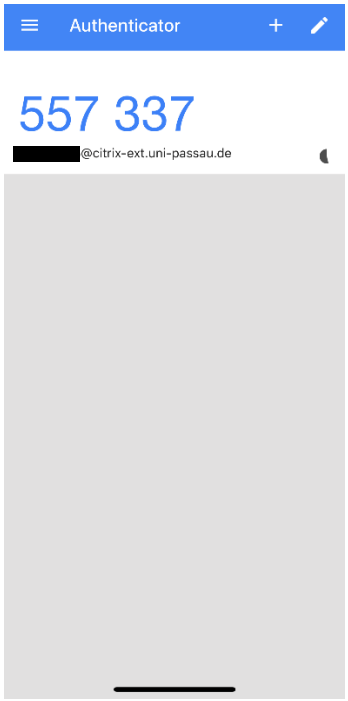
Hinweis: Es ist zwingend erforderlich den Barcode-Scanner der App „Google Authenticator“ zu nutzen! Bitte scannen Sie den Code nicht mit einer anderen beliebigen App.

Schritt 3:
Danach öffnet sich die Kamera mit der Abfrage, ob „Google Authenticator“ auf die Kamera zugreifen darf:



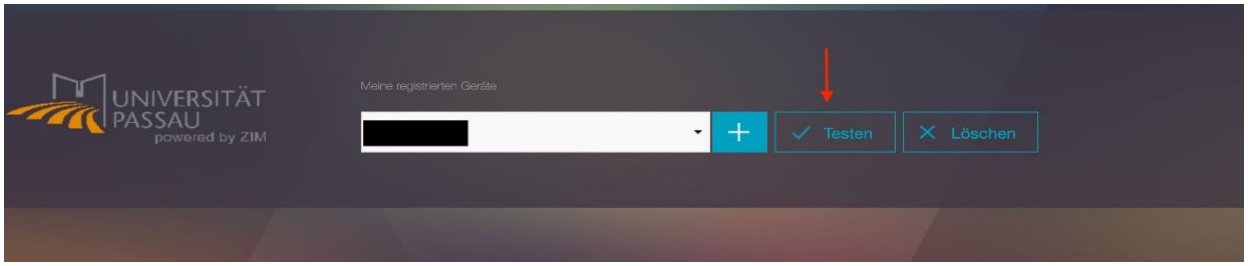
Der Dialog muss mit dem Klicken auf „OK” bestätigt werden.

Schritt 4:
Anschließend wird der QR-Code gescannt.
Nachdem das Konto hinzugefügt wurde, sollte die App folgendermaßen aussehen:



Registrierung des Geräts abschließen

Nachdem nun das Konto betriebsbereit eingerichtet wurde, sieht die Webseite zum Registrieren des Smartphones oder Tablets folgendermaßen aus:



Der vorhandene Button „Testen" ermöglicht eine Überprüfung, ob die Einrichtung erfolgreich war. Dazu klicken Sie auf den „Testen"-Button, anschließend kommt die Abfrage eines Einmalpassworts. Dazu in der App das Einmalpasswort ablesen, eingeben und bestätigen. Wenn der Test funktioniert, so ist die Zwei-Faktor-Authentifizierung (2FA) erfolgreich eingerichtet.

Hinweis: Stellen Sie sicher, dass Ihr Smartphone oder Tablet und Ihr Rechner die gleiche Uhrzeit eingestellt haben. Nur so ist die 2FA valide.

2.4 Einrichtung der Citrix Workspace App

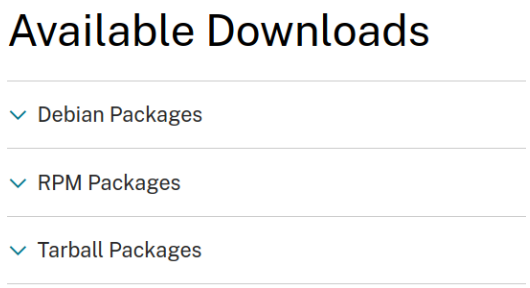
Nun muss noch die Citrix Workspace App für das Betriebssystem auf Ihr privates Gerät heruntergeladen und installiert werden. Auf der Citrix Downloadseite finden Sie die aktuelle Version des Linux Betriebssytems für Rechner und Laptops.

Linux

In diesem Abschnitt wird beschrieben, wie Citrix auf einem privaten Linux-Gerät installiert wird, am Beispiel von **Ubuntu.**

Schritt 1:
Download der notwendigen Programme für Linux

Je nach eingesetzter Distribution werden verschiedene Pakete zum Download angeboten.



Folgen Sie der Installationsanleitung für Ihr Betriebssystem in der Dokumentation des Herstellers.

Bitte beachten Sie, dass mehrere Pakete installiert werden müssen, um den vollständigen Funktionsumfang verwenden zu können.
Die Installationspakete finden sich auf der Downloadseite des Herstellers unter der jeweiligen Paketquelle:

- Citrix Workspace App for Linux
- USB Support Package

Wichtige Plugins – Initiale Installation wichtiger Software

Damit Sie reibungslos Audio- und Videokonferenzen über Skype for Business und Zoom unter Citrix durchführen können, ist es zwingend erforderlich, dass Sie nach Installation von Citrix selbst auch Plugins für die jeweilige Konferenzsoftware auf Ihrem Privatrechner hinzufügen.

Beachten Sie bitte:

- Sie müssen die Plugins auf dem **Basisbetriebssystem** installieren, nicht in Citrix selbst.
- **Citrix darf** während der Installation der Plugins **nicht laufen**.

Essentielle Citrix Plugins für Zoom und Skype for Business finden Sie hier.

Schritt 2:

Installation (dieses Skript funktioniert nur unter Ubuntu 20.04 LTS 64 Bit. Ein Debian System liefert bei der Verwendung des Skripts Fehler)

Workspace App:

```
ubuntu@ubuntu:~/Downloads$ sudo dpkg -i icaclient_20.9.0.15_amd64.deb
```

Web client:

```
ubuntu@ubuntu:~/Downloads$ sudo dpkg -i icaclientWeb_20.9.0.15_amd64.deb
```

USB Support Package:

```
ubuntu@ubuntu:~/Downloads$ sudo dpkg -i ctxusb_20.9.0.15_amd64.deb
```

Skype for Business Plugin (entpacken, Installationsskript ausführbar machen und dann das Installationsskript install.sh ausführen):

```
ubuntu@ubuntu:~/Downloads$ unzip HDX_RealTime_Media_Engine_2.9_for_Linux_x64.zip
```

```
ubuntu@ubuntu:~/Downloads$ chmod 777 HDX_RealTime_Media_Engine_2.9.100_for_Linux
_x64/HDXRTME_install.sh
```

```
ubuntu@ubuntu:~/Downloads$ ./HDX_RealTime_Media_Engine_2.9.100_for_Linux_x64/HDX
RTME_install.sh
```

```
-----------------------------------------------------------------
Willkommen beim Installationsprogramm für Citrix HDX RealTime Media Engine 2.9.1
00.
-----------------------------------------------------------------

Wählen Sie eine Setupoption:

  1. Produkt installieren
  2. Produkt entfernen
  3. Beenden

Setupoption eingeben [1-3]: 1
```

Zoom Plugin:

```
ubuntu@ubuntu:~/Downloads$ sudo dpkg -i zoomcitrixplugin-ubuntu_amd64.deb
```

Bitte kontrollieren Sie die Konfigurationsdatei.
Das Zoom Citrix-Plugin und das HDX RTME Plugin bearbeiten beide die Konfiguration der Workspace App. Leider kann es hier zu Fehlern kommen, insbesondere nach den Aktualisierungen.

Bitte prüfen Sie folgenden Inhalt der Datei mit Administrator-Rechten:

Datei: /opt/Citrix/ICAClient/config/module.ini

Inhalt:

```
; ---------
[ICA 3.0]
VirtualDriver = Thinwire3.0, Clipboard, ClientDrive, ClientPrinterQueue, ClientAudio,
ClientComm, FlashV2, TWI, ZL_FONT, ZLC, ICACTL, SmartCard, UserExperience,
KeyboardSync, MultiMedia, WebPageRedirection, PortForward, VDTUI, HDXRTME,
ZoomMedia
Thinwire3.0 = On
Clipboard = On
TWI = On
ZLC=On
ZL_FONT=On
ICACTL=On
SmartCard=On
ClientDrive=On
ClientPrinterQueue=On
ClientAudio=On
ClientComm=On
UserExperience=On
KeyboardSync=Off
MultiMedia=On
FlashV2=Off
WebPageRedirection=On
PortForward=On
VDTUI=On
HDXRTME=On
ZoomMedia=On

[ZoomMedia]
DriverName=ZoomMedia.so
; ---------
```

Am Ende der Datei findet sich zusätzlich folgender Eintrag:

```
; ---------
[HDXRTME]
DriverName=HDXRTME.so
; ---------
```

Schritt 3:

Zertifikatsfehler

Je nach Konfiguration kann es vorkommen, dass bei der Verbindung zum Workspace Zertifikatsfehler auftreten. Um dies zu vermeiden kann der Zertifikatsstore der Workspace App auf den Zertifikatsstore des Firefox gelinked werden. Dadurch sind die nötigen Root-Zertifikate auch in der Workspace App bekannt.

```
ubuntu@ubuntu:~/Downloads$ sudo ln -s /usr/share/ca-certificates/mozilla/* /opt/
Citrix/ICAClient/keystore/cacerts/
```

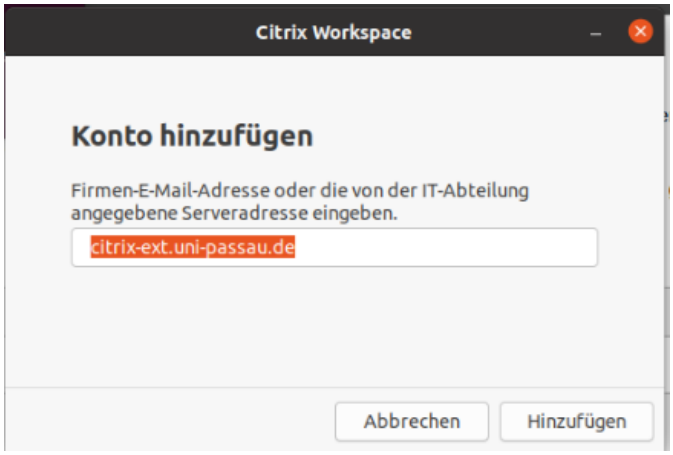
Schritt 4:

Start und Konfiguration der Citrix Workspace App

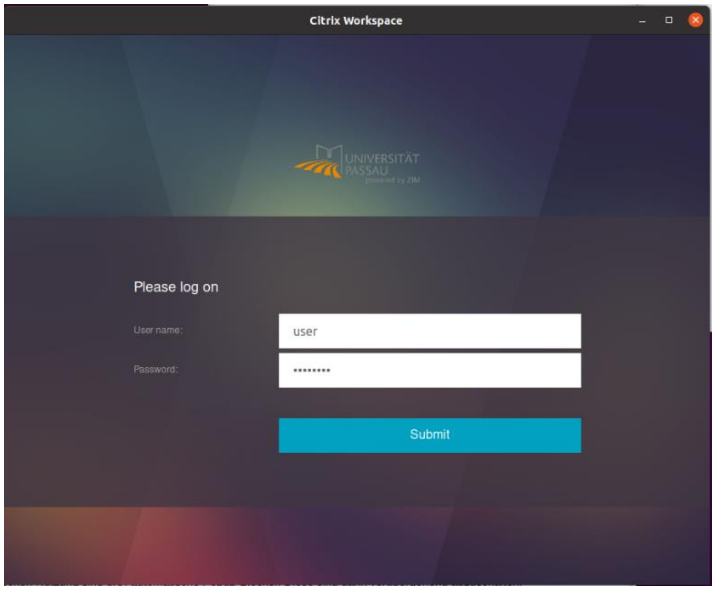
Aufruf über Programmmenü (wahlweise über Kommandozeile)

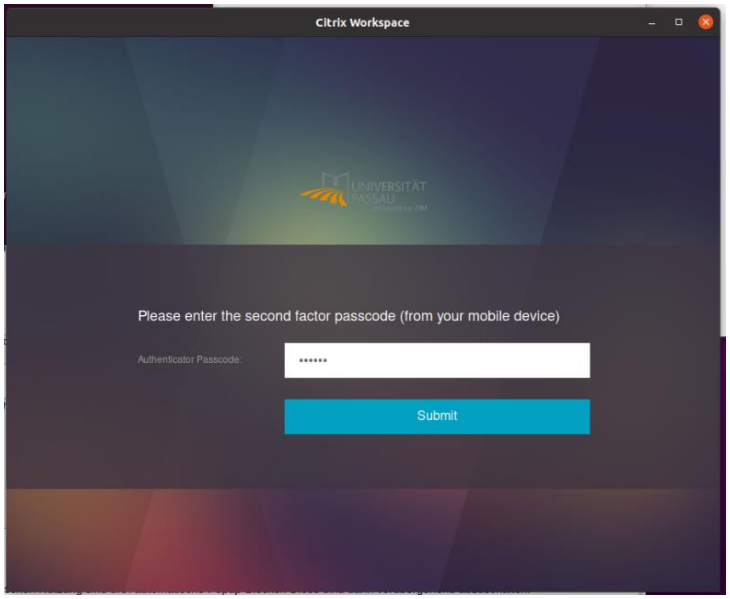
EULA akzeptieren

Führen Sie die Installation bis zum Schluss durch. Geben Sie nun das folgende Konto der Universität Passau für den externen Zugang an: **citrix-ext.uni-passau.de** Klicken Sie hier auf „Hinzufügen".



Nach Angabe des Kontos öffnet sich automatisch „Citrix Workspace“ und bietet an, sich anzumelden.



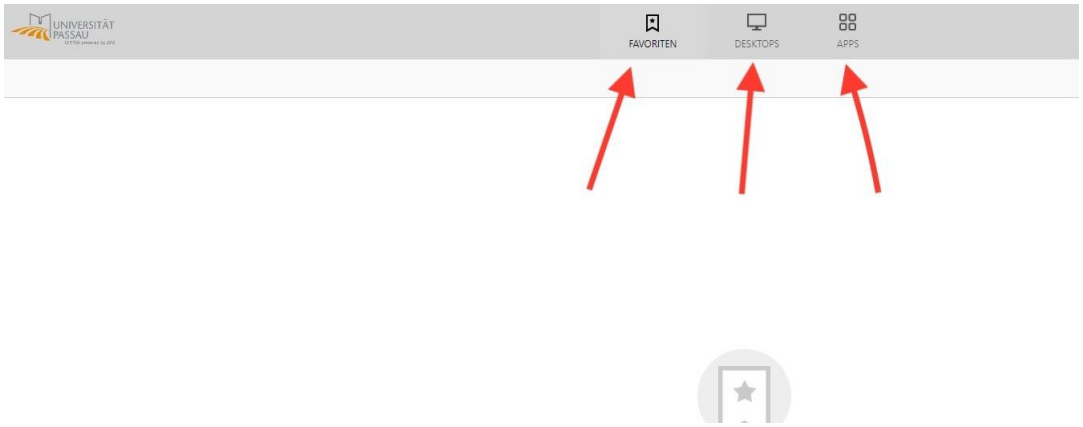


Die hierfür benötigten Anmeldedaten finden Sie in nachfolgender Tabelle aufgelistet:

Feld	**Eingabe**
User Name	Ihre ZIM-Kennung (z.B. muster00)
Password	Das Passwort Ihrer ZIM-Kennung
Passcode	Das aktuell generierte Einmalpasswort

3 Citrix Oberfläche

Im Folgenden wird die Benutzeroberfläche von Citrix erläutert, auf welche man nach dem Login gelangt. Dabei wird beim ersten Start eine leere Übersicht gezeigt:



3.1 Favoriten

Hier befinden sich alle Desktops bzw. Applikationen, welche als Favoriten markiert wurden. Diese können nach Belieben selbst verwaltet werden, also hinzugefügt oder entfernt werden. Dies geschieht über den Button „Details“. Es wird empfohlen, sich den Desktop als Favorit zu setzen, da dieser die eigentliche Desktopanwendung darstellt und somit schneller erreicht werden kann.

3.2 Desktops

Details

Was bewirken „**Details**” bei einem Desktop?

Dieser kann **Geöffnet**, **Neu gestartet** oder **Zu Favoriten hinzugefügt** werden

Standardmäßiger Home-Desktop in Citrix:

Abmelden vs. Trennen

Abmelden: **muss** doppelt geklickt werden und schließt die Sitzung komplett (= Herunterfahren).

Trennen: trennt die aktuelle Sitzung, diese wird jedoch noch 4 Stunden erhalten, sprich diese Funktion ist dazu gedacht, wenn man den Rechner wechselt.