

---

# Handbuch zur Benutzung von Citrix Private Geräte – iOS

---



Herausgeber:

Zentrum für Informationstechnologie und  
Medienmanagement (ZIM)

# Inhaltsverzeichnis

<b>1</b>	<b>CITRIX ALLGEMEIN</b> .....	<b>2</b>
1.1	INTERNES- UND EXTERNES-NETZWERK.....	2
1.2	PRIVATE GERÄTE .....	2
	<b>Smartphone und Tablet</b> .....	2
<b>2</b>	<b>EINRICHTEN VON CITRIX - PRIVATE GERÄTE</b> .....	<b>3</b>
2.1	CITRIX-SYSTEMANFORDERUNGEN – BETRIEBSSYSTEM IOS.....	3
2.2	EXTERNER ZUGANG – ZWEI-FAKTOR-AUTHENTIFIZIERUNG (2FA) .....	3
	<b>Android</b> .....	4
	<b>iOS</b> .....	6
2.3	REGISTRIERUNG DES GERÄTS .....	8
	<b>Android</b> .....	8
	<b>iOS</b> .....	11
2.4	EINRICHTUNG DER CITRIX WORKSPACE APP.....	14
	<b>iOS</b> .....	14
2.5	AUDIO- UND VIDEOKONFERENZEN.....	16
<b>3</b>	<b>CITRIX OBERFLÄCHE</b> .....	<b>17</b>
	<b>Abmelden</b> .....	17

# 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.

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

## 1.2 Private Geräte

### Smartphone und Tablet

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

## 2

## Einrichten von Citrix - Private Geräte

---

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 iOS

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**.

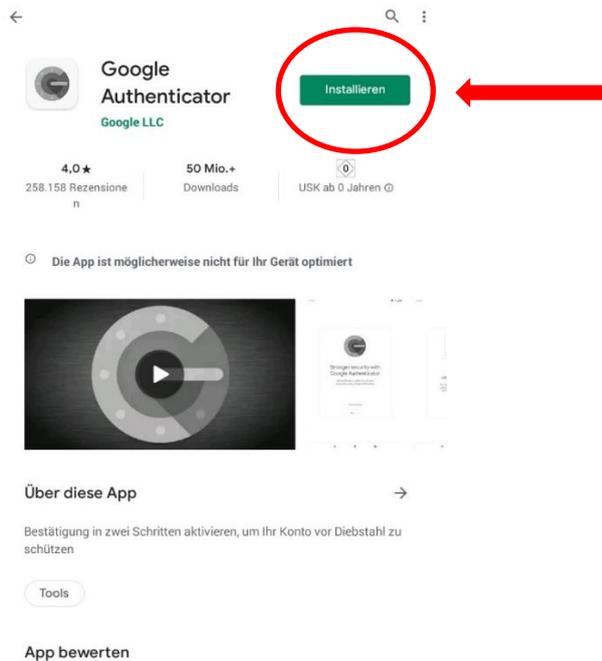


## Android

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

### Schritt 1:

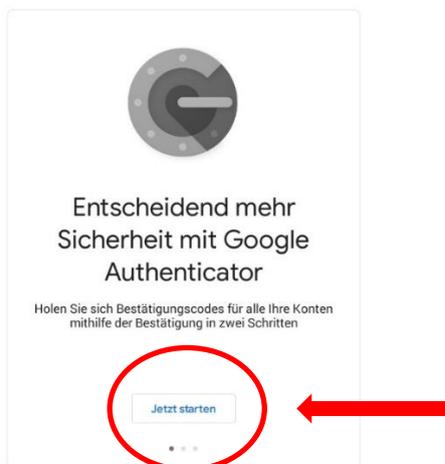
Bitte suchen Sie in Ihrem Google Play Store die App „Google Authenticator“.



### Schritt 2:

Bitte installieren Sie die App.

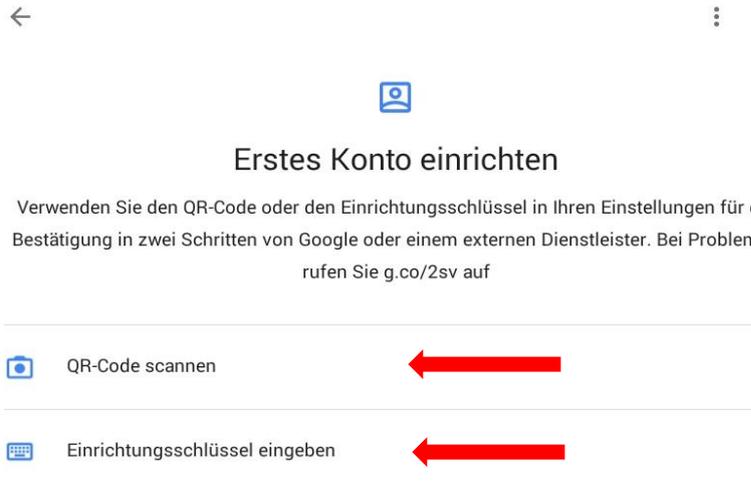
Nach erfolgreicher Installation der App auf einem Android-Gerät erscheint diese nun in der Übersicht aller installierten Apps auf ihrem Smartphone oder Tablet. Wenn die App nun geöffnet wird, sollte der folgende Bildschirm erscheinen:



Wenn Sie danach gefragt werden, ob ein Google-Konto hinzugefügt werden soll, so 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](https://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.

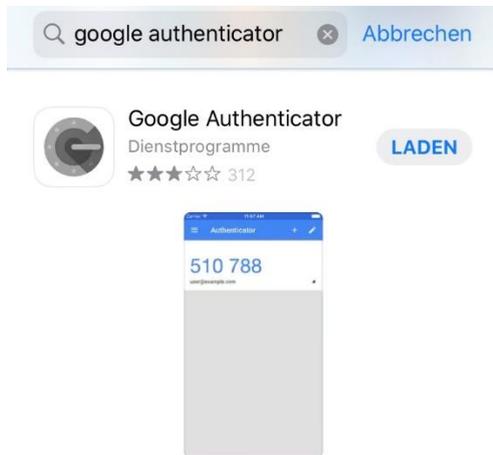


## ios

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](https://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](#).

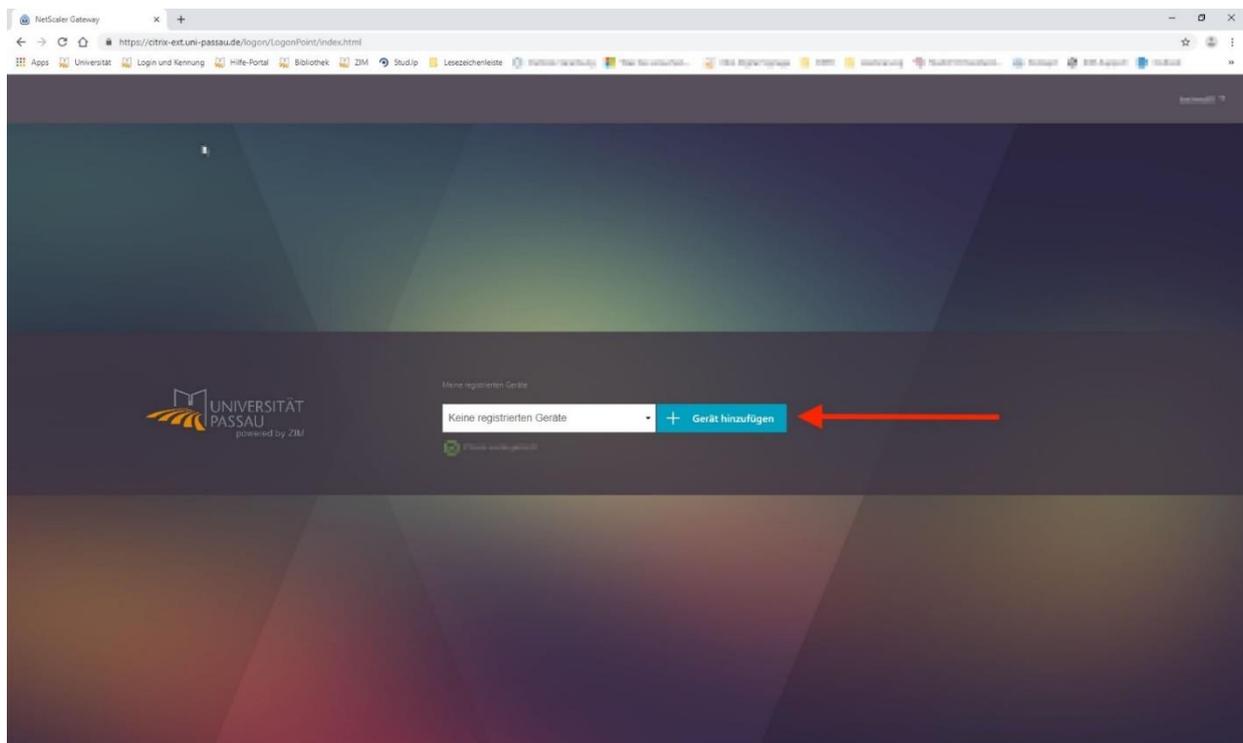


### Android

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:



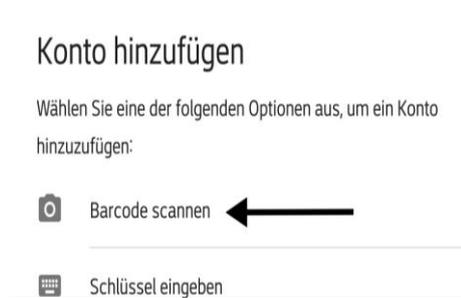
Nachdem auf „Gerät hinzufügen“ geklickt wurde, kann ein beliebiger Name für das Smartphone oder Tablet vergeben werden. Nach Eingabe des Namens wird eine Zeichenkette und ein QR-Code bereitgestellt.

*Hinweis: Die Einrichtung der 2FA 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](https://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.

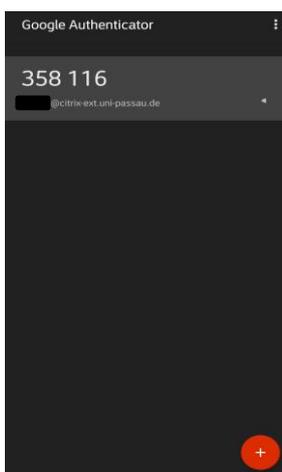
*Hinweis: Es ist zwingend erforderlich den Barcode-Scanner der App „Google Authenticator“ zu nutzen! Bitte scannen Sie den Code nicht mit einer anderen beliebigen App.*

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



### Schritt 3:

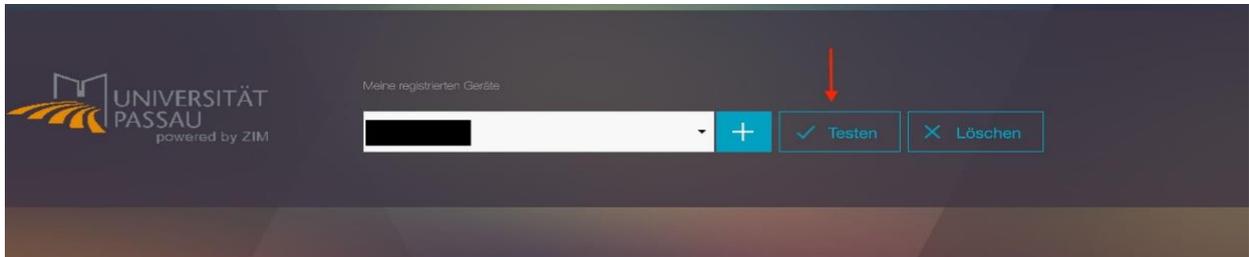
Nachdem das Konto hinzugefügt wurde, sollte die App folgendermaßen aussehen:



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.

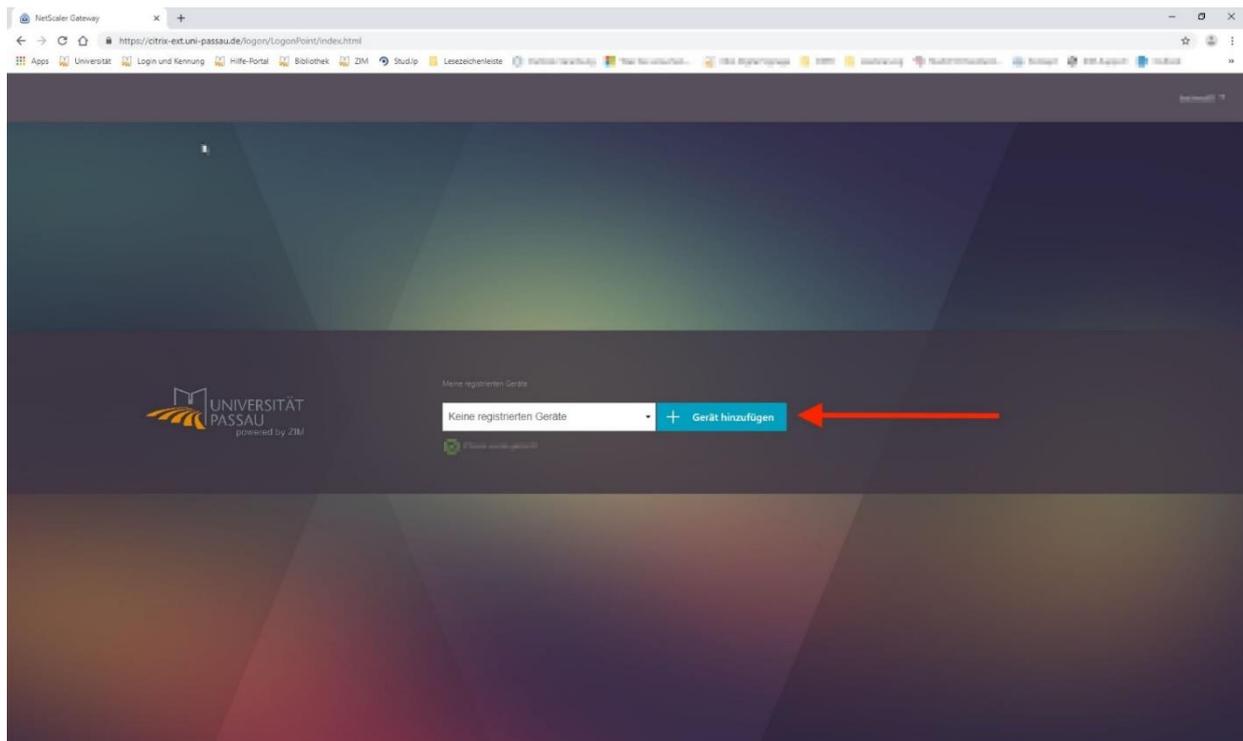


## iOS

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](https://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:



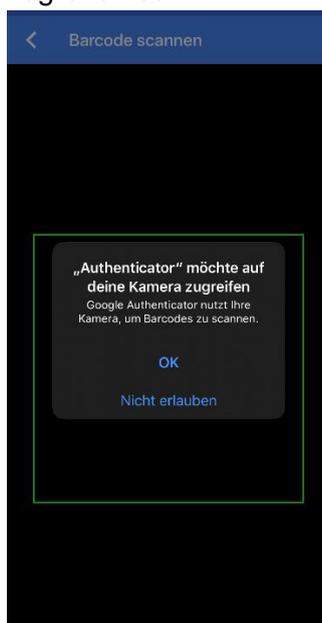
### Schritt 2:

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:

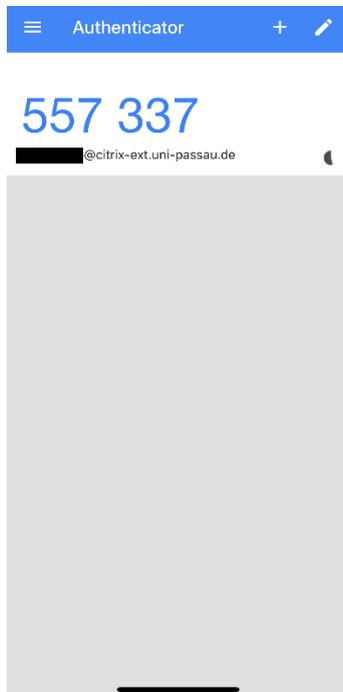


Der Dialog muss mit dem Klicken auf „OK“ bestätigt werden.

#### Schritt 4:

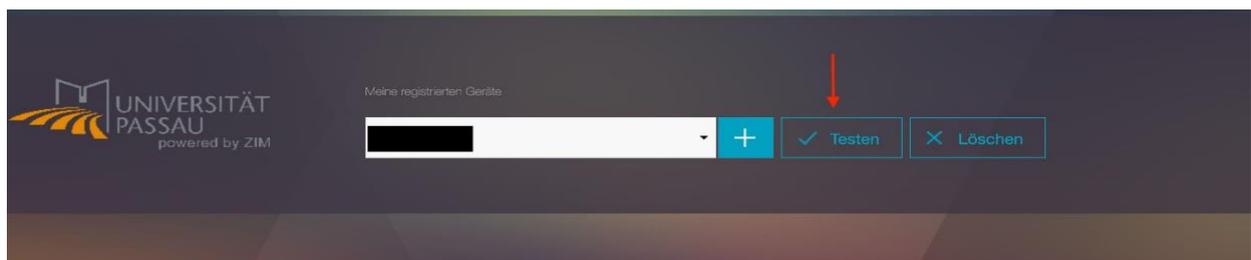
Anschließend wird der QR-Code gescannt.

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.

## 2.4 Einrichtung der Citrix Workspace App

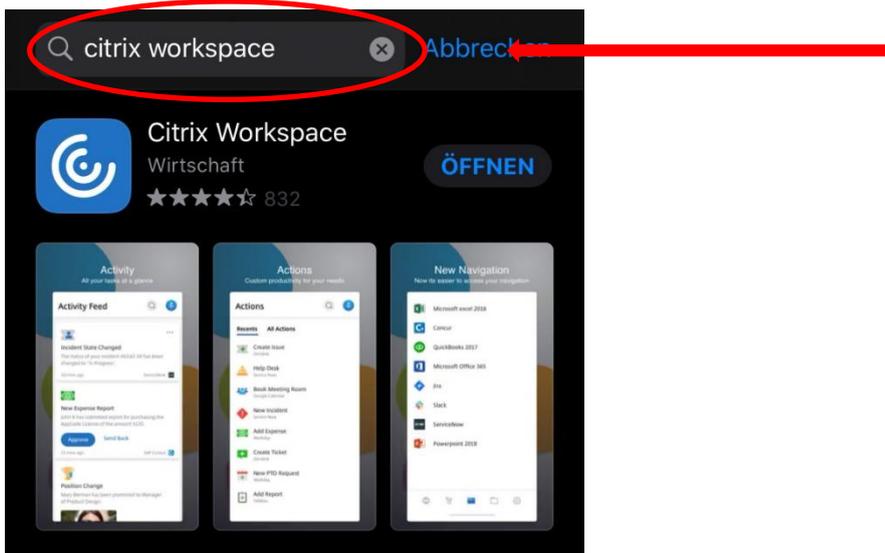
In diesem Abschnitt wird beschrieben, wie Citrix auf einem privaten iOS-Gerät installiert wird.



### iOS

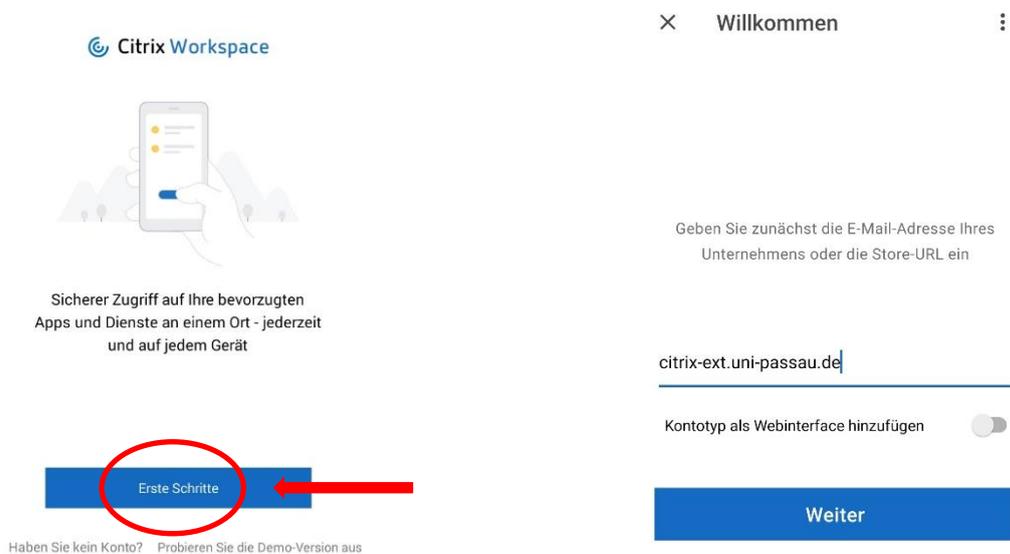
#### Schritt 1:

Zuerst öffnen Sie den „App Store“ auf dem iOS-Gerät und suchen dort nach der „Citrix Workspace“- App.



#### Schritt 2:

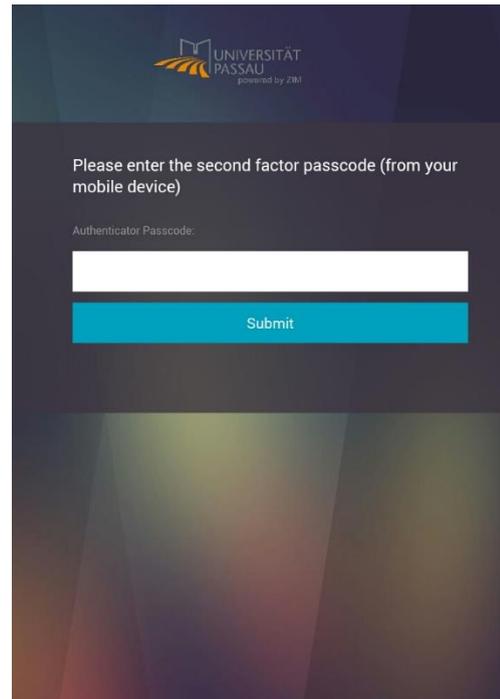
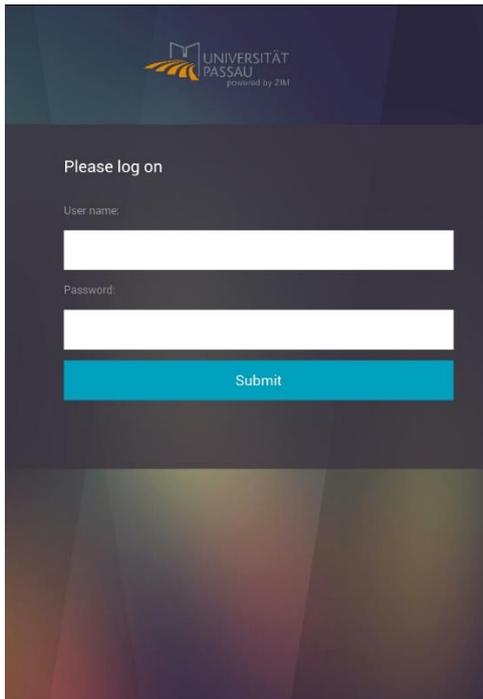
Nachdem die App auf Ihrem Gerät installiert ist, können Sie diese öffnen und sehen nachfolgende Bildschirme. Klicken Sie auf „Erste Schritte“. Anschließend werden Sie aufgefordert das Konto ihrer Firma anzugeben. Dieses ist **citrix-ext.uni-passau.de**.



### Schritt 3:

Nach Eingabe und Bestätigung des Kontos, werden Sie auf den Bildschirm weitergeleitet, an dem Sie sich selbst einloggen können.

Zunächst geben Sie ihre ZIM-Kennung und Ihr Passwort ein. Daraufhin werden Sie aufgefordert das aktuell generierte Einmalpasswort aus der Google Authenticator App einzugeben. Nun haben Sie Zugriff über Citrix auf Ihrem iOS-Gerät.



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

## 2.5 Audio- und Videokonferenzen

Aktuell ist es nicht möglich die Tools Zoom und Skype for Business für Audio- und Videokonferenzen unter Citrix für iOS zu nutzen.

Sie haben die Option, den offiziellen Skype for Business und Zoom Client für iOS-Geräte über den offiziellen System-App-Stores zu beziehen. Mehr Informationen zur Registrierung von [Skype for Business](#) und [Zoom](#), sowie viele weitere Themen und Inhalte finden Sie in unserem [Hilfeportal](#).

Wenn Sie diese Dienste also auf Ihrem Tablet oder Smartphone nutzen möchten, installieren Sie bitte die App lokal.

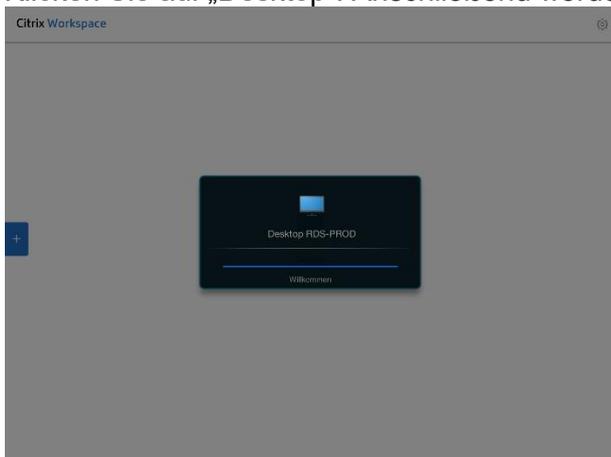
*Hinweis: Die Installation von Plugins ist an dieser Stelle also nicht notwendig.*

## 3 Citrix Oberfläche

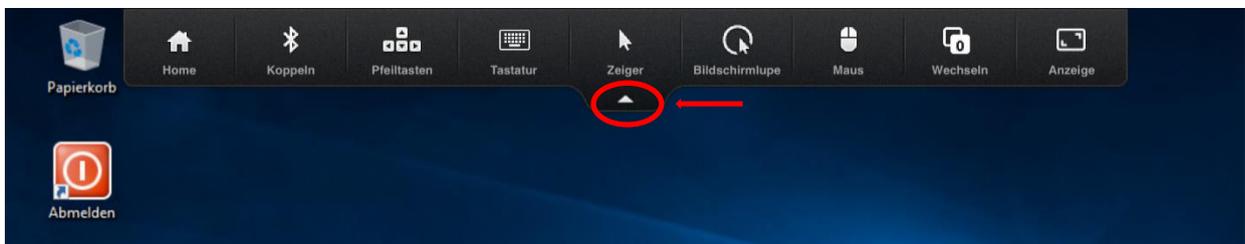
Im Folgenden wird die Benutzeroberfläche von Citrix gezeigt, auf welche man nach dem Login gelangt. Dabei ist beim Start eine Übersicht mit dem Symbol „Desktop“ zu finden:



Klicken Sie auf „Desktop“. Anschließend werden Sie weitergeleitet:



Home-Desktop in Citrix:



### Abmelden

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

App schließen: trennt die aktuelle Sitzung, diese wird jedoch noch 4 Stunden erhalten, sprich diese Funktion ist dazu gedacht, wenn man das Gerät wechselt.