

Schritt für Schritt zur mobilen Nutzung

Für private Handys

Vorwort

Liebe Kolleginnen und Kollegen,

myDUS, das neue Intranet, ist da.

Die Idee: Alles Wesentliche an einem Ort. Nicht mehr überlegen, was ich in welchem System finde, sondern ein zentraler Ort für Informationen, Austausch und Zusammenarbeit inklusive der News und Fachbereichsseiten des Mitarbeiterportals.

Damit alle Kolleginnen und Kollegen – unabhängig von ihrem Arbeitsplatz oder ihrem Endgerät – jederzeit auf myDUS zugreifen können, begleiten wir Euch in diesem Booklet unseres IT-Dienstleisters Avendis Schritt für Schritt bei der Einrichtung auf privaten Endgeräten (Bring Your Own Device – BYOD).

Ihr findet hier Informationen zur Registrierung, Anmeldung sowie zur Installation der SharePoint-App.

Die Inhalte richten sich an unterschiedliche Zielgruppen innerhalb unseres Unternehmens: Die Anleitung iOS-User beginnt auf Seite 2, für Android-Nutzer auf Seite 17.

Neben Mitarbeitenden, die über einen dienstlichen Computer verfügen, erhalten auch Kolleginnen und Kollegen ohne regelmäßigen Zugang zu einem eigenen Rechner wichtige Hinweise und Erläuterungen. An den entsprechenden Stellen sind diese Informationen gekennzeichnet.

Sollten während der Einrichtung oder Nutzung Fragen auftreten, wendet Euch an:

Avendis

Telefon: +49 (0) 211 421 25555
E-Mail: itsm@dus.com

Wir wünschen Euch einen erfolgreichen Start.

Euer Team von myDUS

Inhaltsverzeichnis

1 iOS 2

1.1 MFA-Registrierung (**M**ulti-**F**aktor-**A**uthentifizierung)..... 2

1.2 Anbindung an die IT-Infrastruktur..... 8

1.3 Erstellung eines Apple Accounts..... 16

2 Android 17

2.1 MFA-Registrierung (**M**ulti-**F**aktor-**A**uthentifizierung)..... 17

2.2 Anbindung an die IT-Infrastruktur..... 21

1 iOS

1.1 MFA-Registrierung (Nur für Mitarbeiterinnen und Mitarbeiter ohne Firmen-PC)

Zur Absicherung der Anmeldung an die IT-Infrastruktur muss Ihr Account zwangsläufig mit einem 2. Faktor für die Anmeldung abgesichert werden (Multi-Faktor-Authentifizierung => MFA).

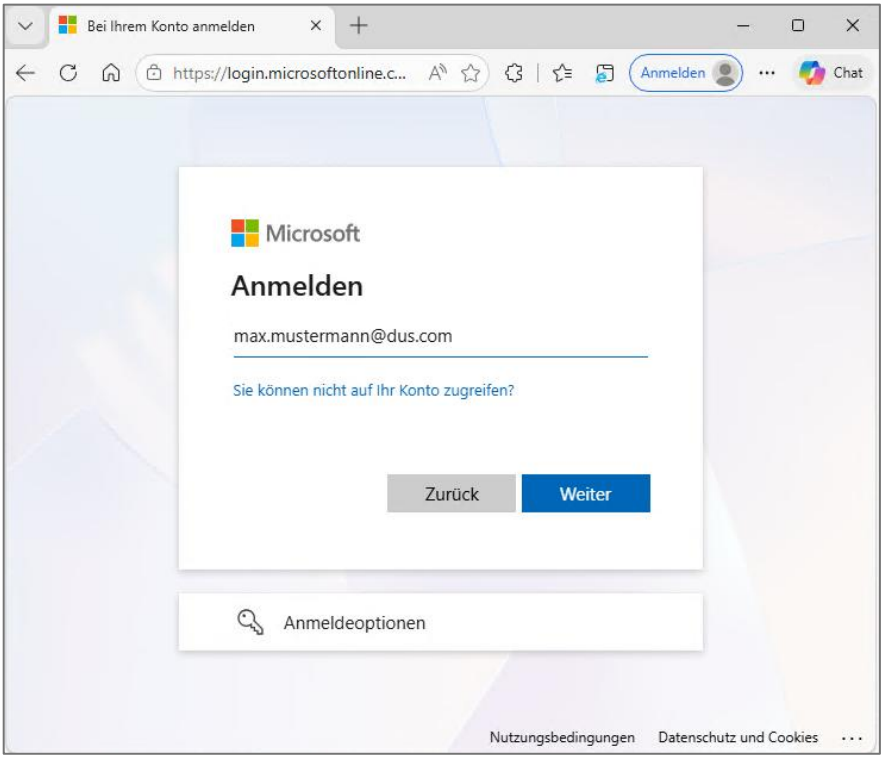
Befolgen Sie für die Einrichtung von der MFA bitte folgende Vorgehensweise:

Melden Sie sich an einem Firmen-PC an und öffnen Sie einen Browser (Edge). Es ist zwingend notwendig, dass Sie diese Einrichtung an einem Firmen-PC durchführen, da sonst die Registrierung technisch nicht möglich ist!

Rufen Sie im Browser folgende Webseite auf oder klicken Sie auf den nachfolgenden Link:

https://aka.ms/mysecurityinfo

Melden Sie sich mit Ihrem bekannten Benutzernamen und Passwort an.



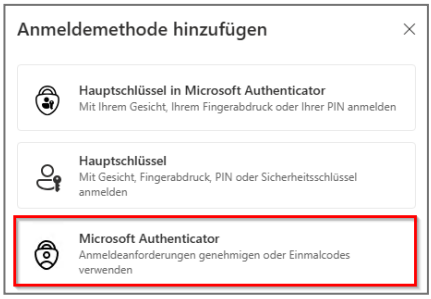
Nach der Anmeldung erhalten Sie eine Aufforderung für die Registrierung Ihrer MFA.



Bestätigen Sie die Meldung mit Klick auf „Weiter“.

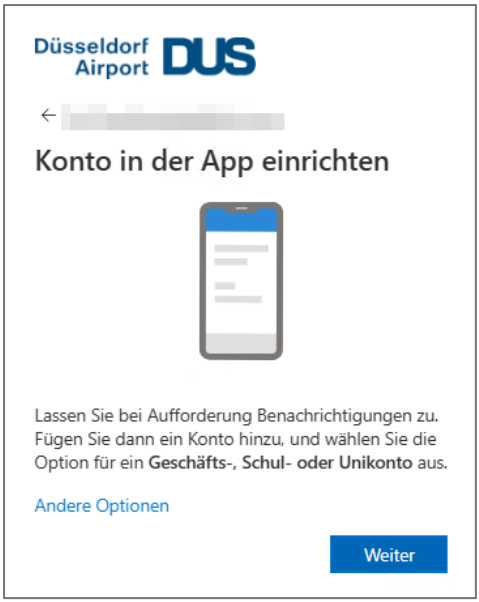
Sollten Sie die Aufforderung nicht erhalten, sondern direkt in der Übersicht der Sicherheitsinformationen landen, klicken Sie bitte auf „Anmeldemethode hinzufügen“ und dann auf „Microsoft Authenticator“.



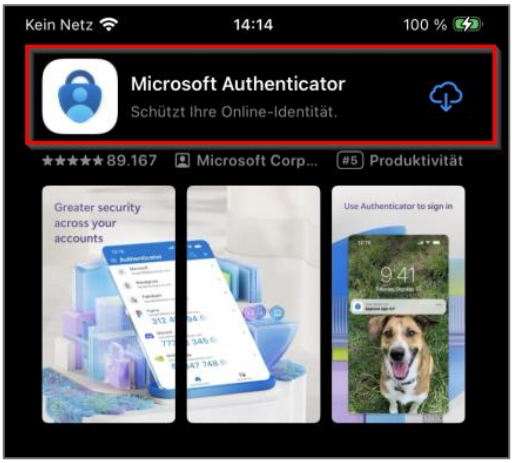


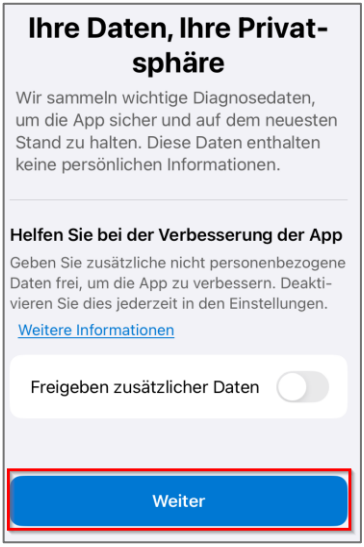
Befolgen Sie nun die Anweisungen für die Einrichtung von der MFA aus dem Smartphone:





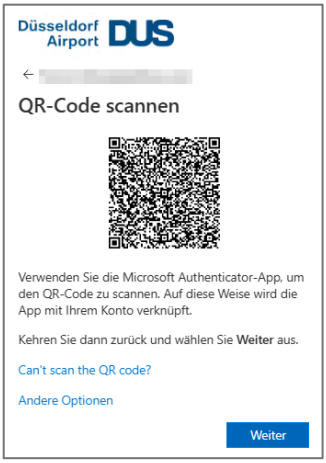
Laden Sie sich die App Microsoft Authenticator im App Store herunter, öffnen Sie diese und bestätigen Sie die Privatsphäre-Einstellungen.

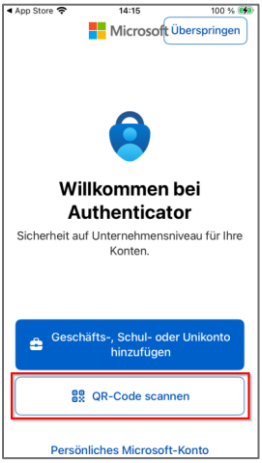




Achtung: Sollten Sie keinen Apple-Account haben und beim Öffnen darauf hingewiesen werden, führen Sie bitte die Schritte unter Anleitung „1.3 Erstellung eines Apple Accounts“ durch.

Achtung: Sollten Sie keinen Apple-Account haben und beim Öffnen darauf hingewiesen werden, führen Sie bitte die Schritte unter Anleitung „1.3 Erstellung eines Apple Accounts“ durch.







Das Konto wird jetzt in Ihrer Authenticator App hinterlegt und die MFA ist registriert. Bestätigen Sie auf dem PC die Meldung mit Klick auf „Weiter“ und testen Sie die MFA.

Sie werden aufgefordert zwei Zahlen einzugeben und erhalten gleichzeitig eine Push-Benachrichtigung auf dem Smartphone.





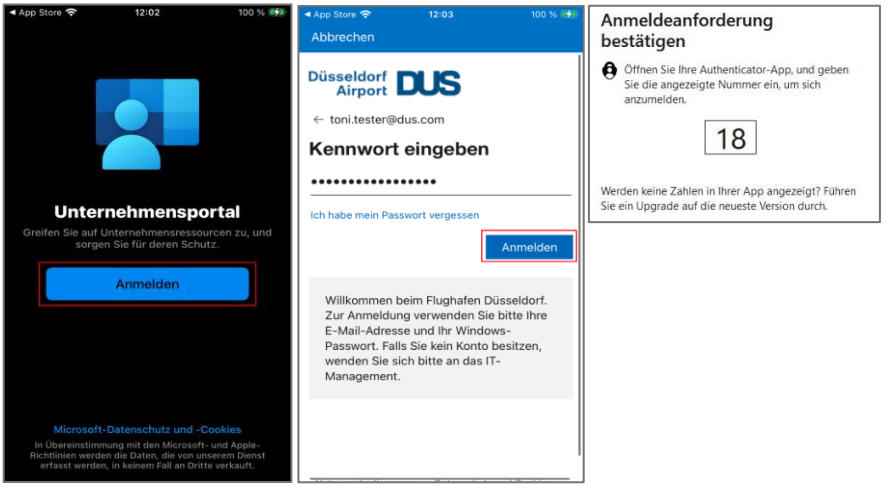
Sobald Sie diese auf dem Smartphone bestätigt haben, zeigt Ihnen der PC eine entsprechende Meldung und Sie sind bereit für die Anbindung des Smartphones an die IT-Infrastruktur im nächsten Kapitel der Anleitung.

1.2 Anbindung an die IT-Infrastruktur

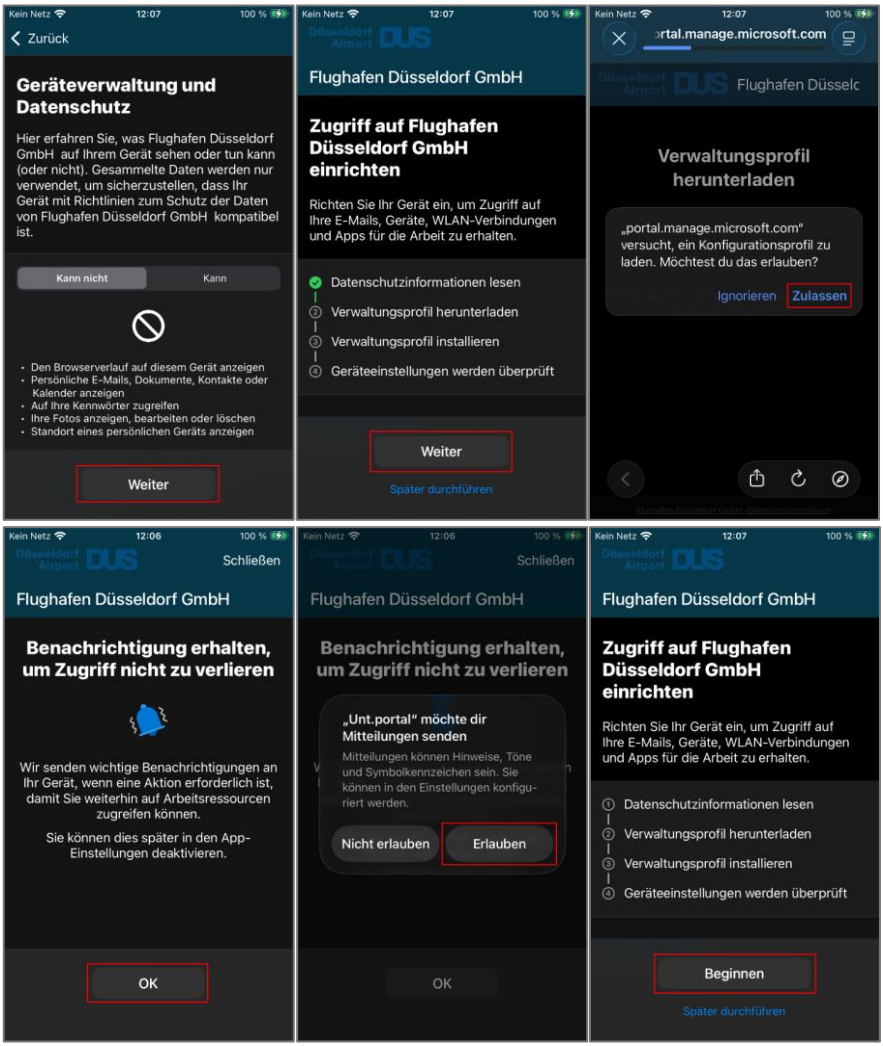
Öffnen Sie den App Store, suchen Sie nach “Unternehmensportal” und installieren Sie die App “Intune-Unternehmensportal”. Öffnen Sie diese im Anschluss.



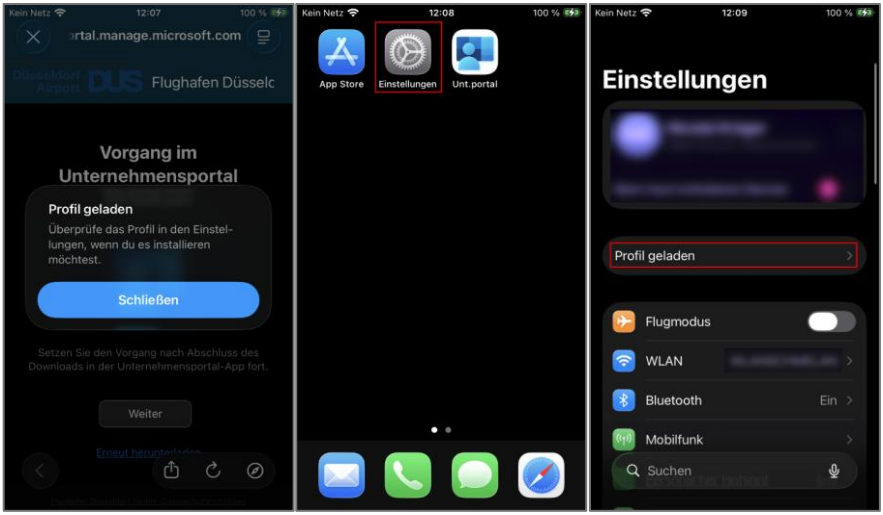
Tippen Sie anschließend auf “Anmelden” und melden sich mit Ihren Benutzerdaten an. Wenn Sie die Anmeldeanforderung bestätigen sollen, wechseln Sie in die Authenticator App und bestätigen Sie die angezeigten Ziffern.



Lassen Sie sich nun durch den Installationsdialog leiten und bestätigen Sie jeweils die Anfragen.

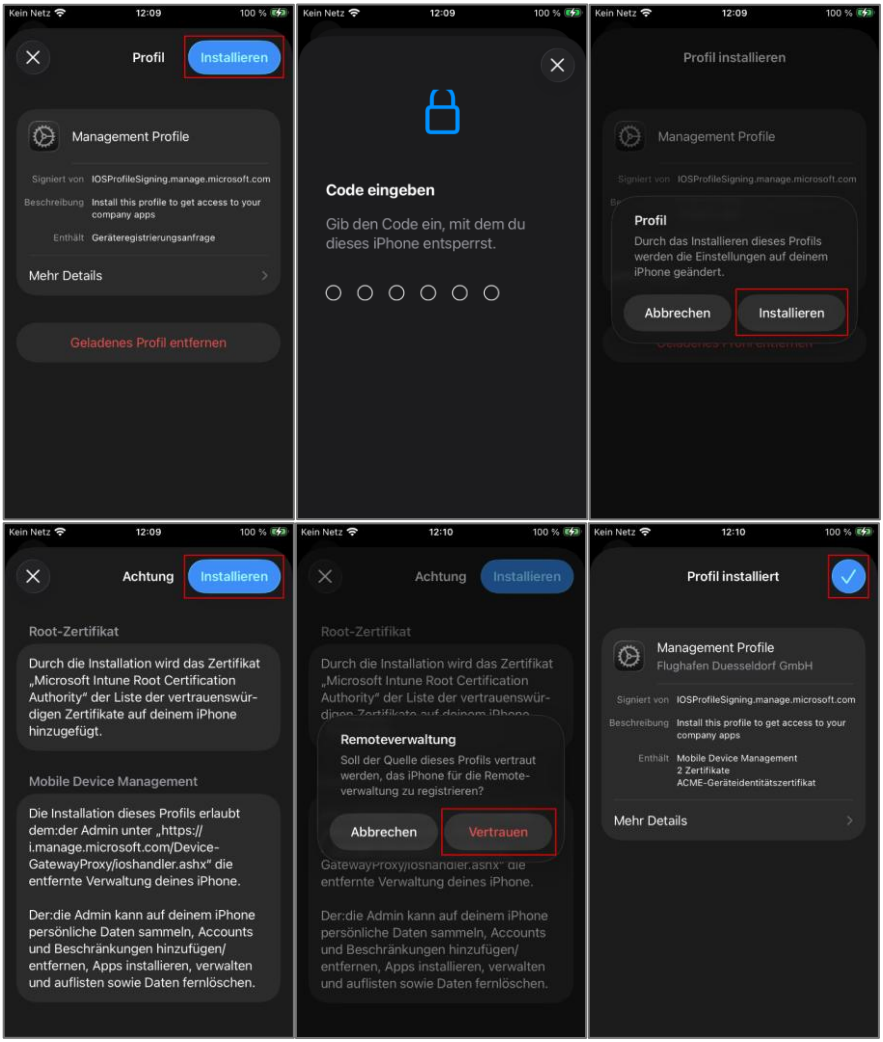


Wechseln Sie in die System-Einstellungen des Endgeräts (über den Homescreen), wenn Sie dazu ausgefordert werden und installieren Sie das Verwaltungsprofil. Sie sollten beim Aufruf der Einstellungen bereits angezeigt bekommen, dass ein neues Profil geladen wurde und installiert werden kann

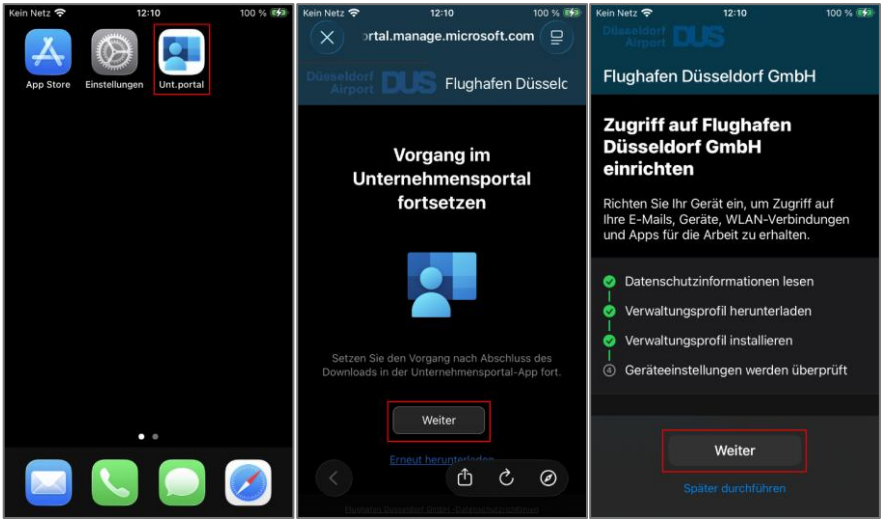


Sollte diese Meldung (Screen „Profil geladen“) bei Ihnen nicht sichtbar sein, können Sie alternativ über “Einstellungen → Allgemein → VPN und Geräteverwaltung” manuell zu der Stelle navigieren.

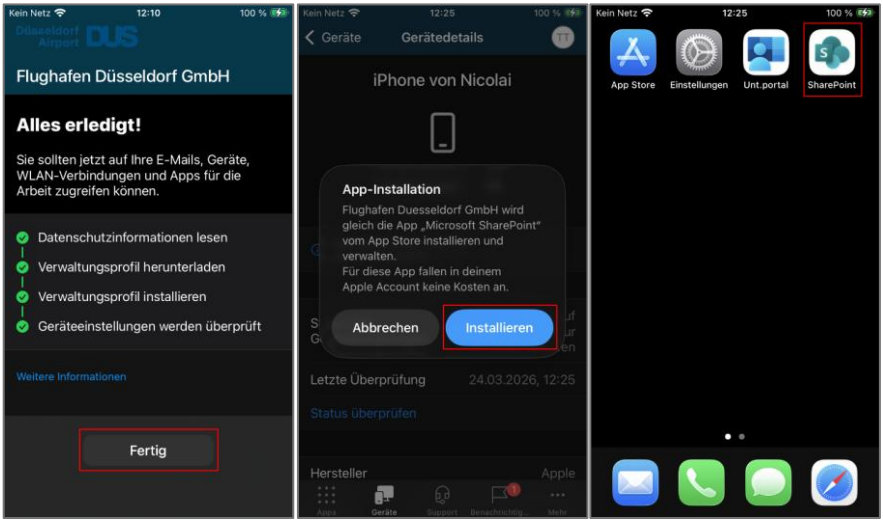
Bestätigen Sie die Anweisungen für die Profilinstallation und geben Sie Ihre Oberflächensperre (der Code, mit dem Sie Ihr Handy entsperren) für die Autorisierung ein



Wechseln Sie nach der erfolgreich Profilinstallation wieder in das Unternehmensportal und schließen Sie die Anbindung ab.



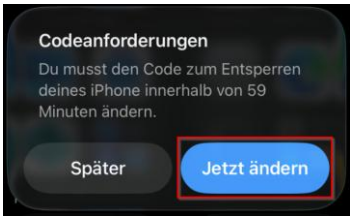
Die Anbindung ist nun abgeschlossen und nach einer kurzen Zeit wird die SharePoint-App automatisch installiert.



Je nachdem, welche Art und Sicherheitsebene der Oberflächensperre Sie derzeit für die Entsperrung Ihres Endgerätes verwenden, kann es während der Anbindung des Smartphones vorkommen, dass Sie für die Vergabe einer sicherer PIN (mindestens 6 Stellen) aufgefordert werden.

Diese Aufforderung ist entweder direkt in der Unternehmensportal App sichtbar oder wir Ihnen als kleines Info-Fenster angezeigt:



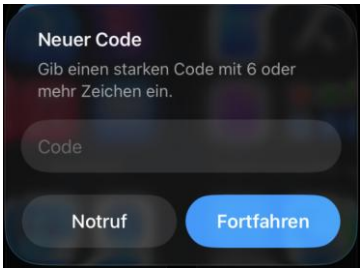


Tippen Sie auf „Jetzt ändern" in dem angezeigten Info-Fenster oder wechseln Sie in den Einstellungen des iPhones auf „Touch ID & Code“.

Sie müssen nun einmalig Ihre bekannte Oberflächensperre eingeben, damit Sie die Daten verändern dürfen.

Vergeben Sie anschließend einen sechsstelligen PIN, welcher zukünftig zur Entsperrung Ihres Smartphones dient.

Wechseln Sie anschließend in die Unternehmensportal-App, um die Geräteeinstellungen erneut zu prüfen und die Anbindung abzuschließen.



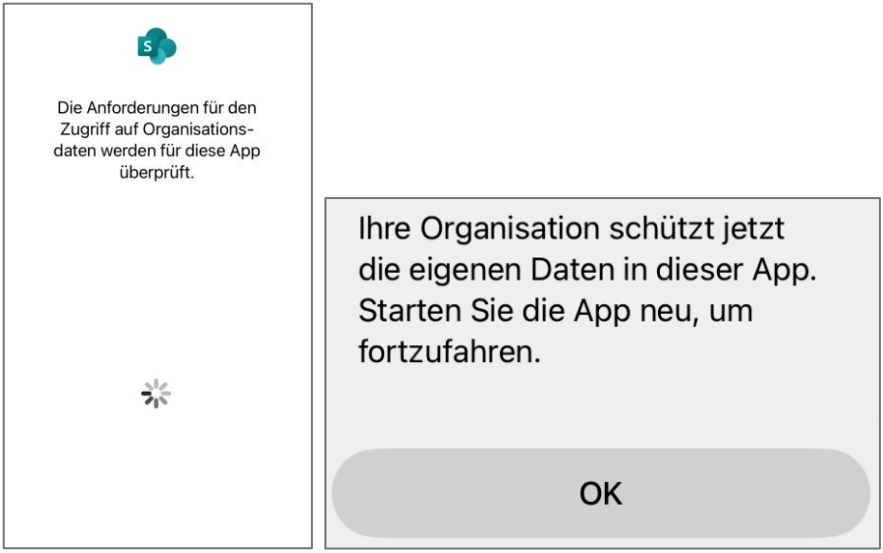




Nach dem Öffnen der SharePoint-App wählen Sie „Anmeldung bei SharePoint Online“ aus und geben Ihre Benutzerdaten für die Anmeldung ein (@dus.com-Adresse). Gegebenenfalls werden Sie nach dem Code für Ihre Multifaktor-Authentifizierung (MFA) gefragt. (Es öffnet sich hierfür eine entsprechende Benachrichtigung, über die Sie den Authenticator öffnen können oder Sie wechseln über den Homescreen manuell dorthin).

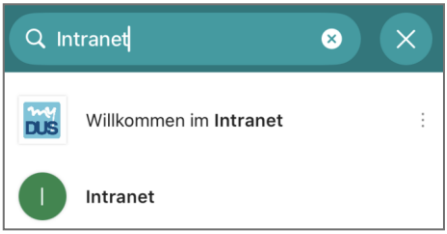


Nach der Anmeldung kann es ein wenig dauern, bis die nächste Meldung angezeigt wird, da die Anforderungen für den Zugriff auf Organisationsdaten für die App überprüft werden



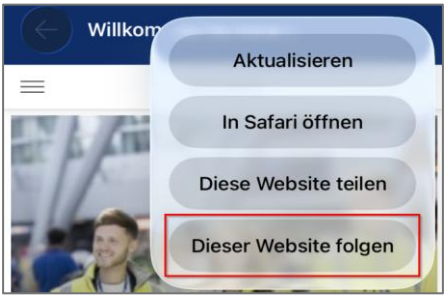
Wenn Sie aufgefordert werden, die App neu zu starten, kommen Sie dem nach und starten Sie die SharePoint-App erneut.

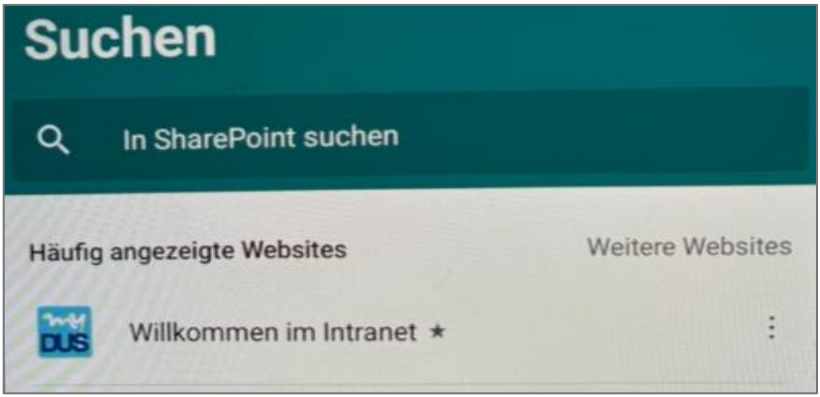
Sie sind nun innerhalb der SharePoint-App angemeldet.
Innerhalb der SharePoint-App haben Sie die Möglichkeit über die Suchleiste am oberen Bildschirmrand das Intranet zu suchen und aufzurufen.



Um das Intranet zukünftig einfacher zu finden, können Sie in der geöffneten Seite über die drei Punkte „dieser Webseite folgen“, so dass diese direkt auf der Startseite beim Öffnen von SharePoint angezeigt wird.







Bitte beachten Sie, dass Links in dem neuen Intranet teilweise auf das alte MA-Portal führen, der Zugriff auf dieses für Ihr Smartphone allerdings nicht freigeschaltet ist und diese Links weiterhin über einen FDG-PC aufgerufen werden müssen.

1.3 Erstellung eines Apple Accounts

Für die Installation der Authenticator App und des Unternehmensportals ist es zwingend notwendig, dass Sie einen Apple Account besitzen, welcher als Authentifizierung für den Download dieser Apps aus dem App Store von Apple verlangt wird.

Sollten Sie noch keinen eigenen Apple Account besitzen, führen Sie bitte folgende Schritte auf Ihrem iOS-Gerät aus, um diesen zu erstellen:

Öffnen Sie den App Store, und tippen Sie auf die Taste „Mein Account“. (Gegebenenfalls werden Sie auch direkt darauf hingewiesen, dass kein Apple Account angemeldet ist und Sie können direkt mit dem nächsten Schritt fortfahren).



Tippen Sie auf „Neuen Apple Account erstellen“.



Befolgen Sie die Anweisungen auf dem Bildschirm, um eine E-Mail-Adresse einzugeben, ein sicheres Passwort zu erstellen und das Land oder die Region festzulegen. Die E-Mail-Adresse, die Sie hier eingeben, wird verwendet, um Sie bei Ihrem neuen Apple Account anzumelden.

Geben Sie „Keine“ als Zahlungsmethode und Zahlungsinformationen ein und tippen Sie auf „Weiter“.

Sie können Ihre Telefonnummer bestätigen. Dies kann dabei helfen, Ihre Identität zu bestätigen und Ihren Account wiederherzustellen, falls erforderlich.

Dieser Schritt ist optional und muss nicht durchgeführt werden. Tippen Sie auf „Weiter“.

Überprüfen Sie, ob Sie eine Bestätigungs-E-Mail von Apple erhalten haben und bestätigen Sie Ihre E-Mail-Adresse über den Link in der E-Mail.

Nachdem Sie Ihre E-Mail-Adresse bestätigen haben, können Sie sich mit dem neuen Apple Account im App Store anmelden und die erforderlichen Apps herunterladen.

2 Android

2.1 MFA-Registrierung (Nur für Mitarbeiterinnen und Mitarbeiter ohne Firmen-PC)

Zur Absicherung der Anmeldung an die IT-Infrastruktur muss Ihr Account zwangsläufig mit einem 2. Faktor für die Anmeldung abgesichert werden (Multi-Faktor-Authentifizierung => MFA).

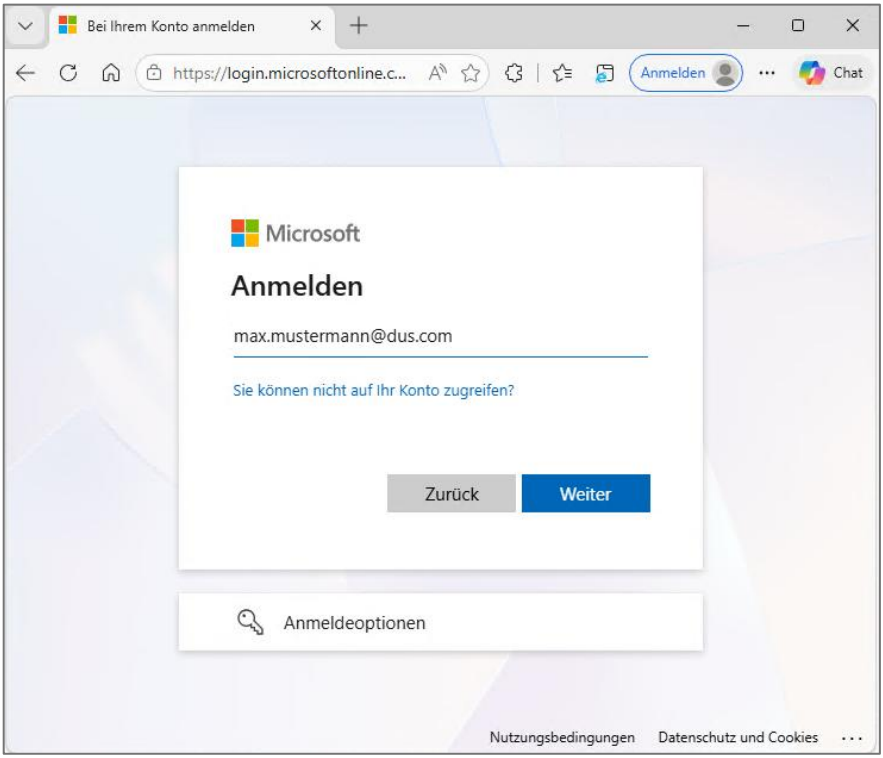
Befolgen Sie für die Einrichtung von der MFA bitte folgende Vorgehensweise:

Melden Sie sich an einem Firmen-PC an und öffnen Sie einen Browser (Edge). Es ist zwingend notwendig, dass Sie diese Einrichtung an einem Firmen-PC durchführen, da sonst die Registrierung technisch nicht möglich ist!

Rufen Sie im Browser folgende Webseite auf oder klicken Sie auf den nachfolgenden Link:

https://aka.ms/mysecurityinfo

Melden Sie sich mit Ihrem bekannten Benutzernamen und Passwort an.



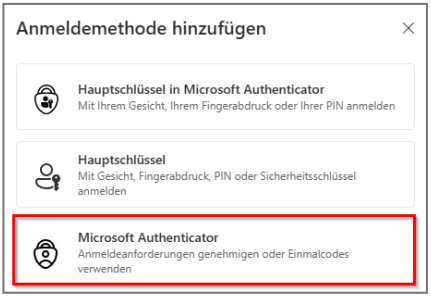
Nach der Anmeldung erhalten Sie eine Aufforderung für die Registrierung Ihrer MFA.



Bestätigen Sie die Meldung mit Klick auf „Weiter“.

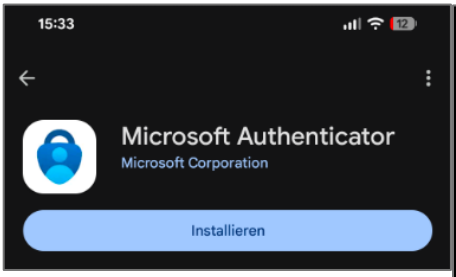
Sollten Sie die Aufforderung nicht erhalten, sondern direkt in der Übersicht der Sicherheitsinformationen landen, klicken Sie bitte auf „Anmeldemethode hinzufügen“ und dann auf „Microsoft Authenticator“.

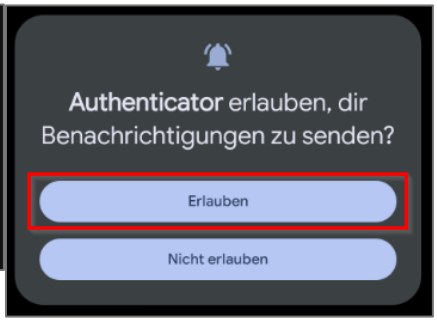




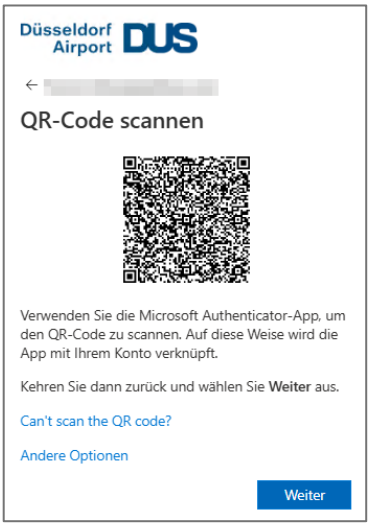
Befolgen Sie nun die Anweisungen für die Einrichtung der MFA auf dem Smartphone:

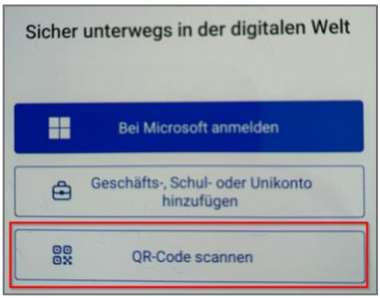
Laden Sie sich die App Microsoft Authenticator in dem App Store herunter, öffnen Sie diese und bestätigen Sie die die Privatsphäre- und Benachrichtigungseinstellungen.





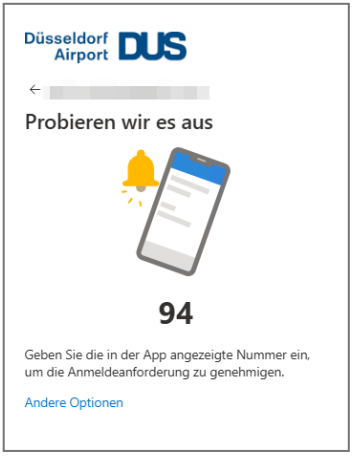
Klicken Sie anschließend auf dem PC auf „Weiter“ und scannen Sie auf dem Smartphone den angezeigten QR-Code.





Das Konto wird jetzt in Ihrer Authenticator App hinterlegt und die MFA ist registriert. Bestätigen Sie auf dem PC die Meldung mit Klick auf „Weiter“ und testen Sie die MFA.

Sie werden aufgefordert zwei Zahlen einzugeben und erhalten gleichzeitig eine Push-Benachrichtigung auf dem Smartphone.

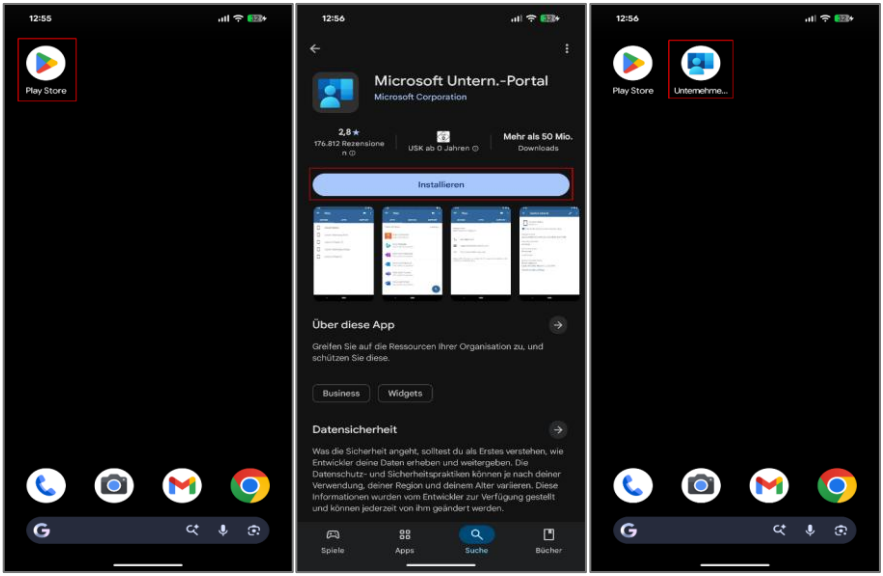




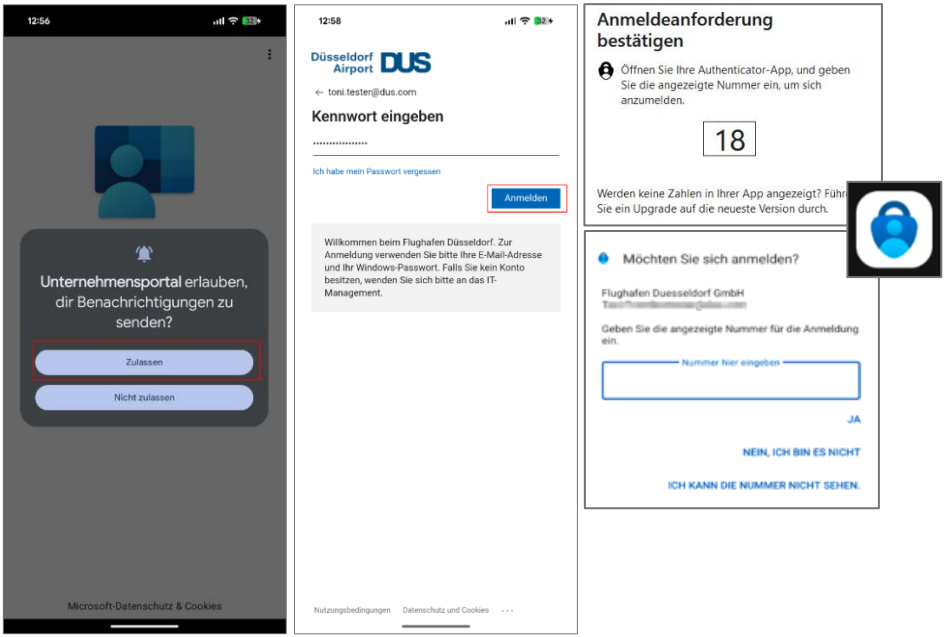
Sobald Sie diese auf dem Smartphone bestätigt haben, zeigt Ihnen der PC eine entsprechende Meldung und Sie sind bereit für die Anbindung des Smartphones an die IT-Infrastruktur im nächsten Kapitel der Anleitung.

2.2 Anbindung an die IT-Infrastruktur

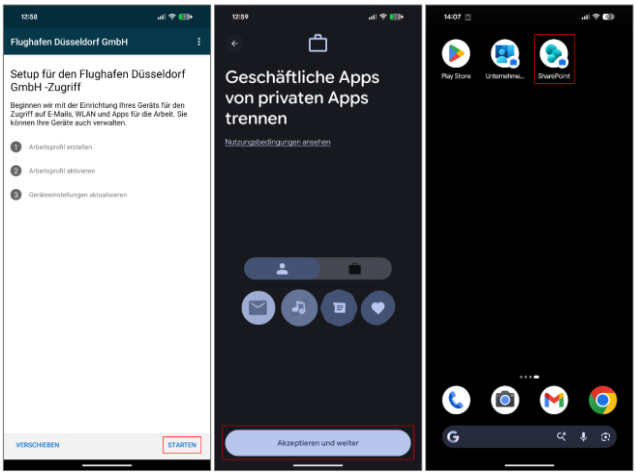
Öffnen Sie den Google Play Store, suchen Sie nach “Unternehmensportal” und installieren Sie die App “Microsoft Unternehmensportal”. Öffnen Sie diese im Anschluss.



Bestätigen Sie die Anfrage für die Benachrichtigungen und melden Sie sich mit Ihren bekannten Anmeldedaten an. Geben Sie die Ziffern in der Authenticator App ein, wenn Sie dazu aufgefordert werden. (Sie erhalten diese per Push-Benachrichtigung und können über diese in den Authenticator wechseln oder Sie navigieren über den Homescreen und öffnen die Authenticator App manuell).

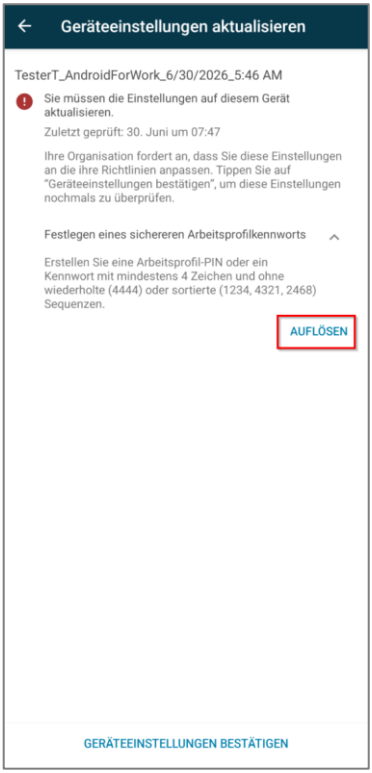


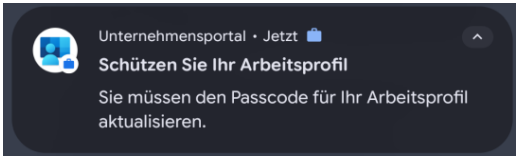
Lassen Sie sich nun durch die Profilinstallation leiten. Der Vorgang kann je nach Modell ein wenig unterschiedlich aussehen, ähnelt aber dem hier angezeigten. Anschließend ist das Gerät angebunden und die SharePoint-App wird nach einer kurzen Zeit automatisch installiert.



Je nachdem, welche Art und Sicherheitsebene der Oberflächensperre Sie derzeit für die Entsperrung Ihres Endgerätes verwenden, kann es während der Anbindung des Smartphones vorkommen, dass Sie für die Vergabe einer sicherer PIN (mindestens 6 Stellen) aufgefordert werden.

Diese Aufforderung ist entweder direkt in der Unternehmensportal App sichtbar oder wir Ihnen als Banner in den Benachrichtigungen angezeigt:

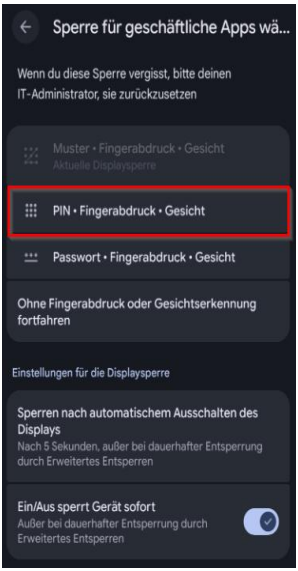




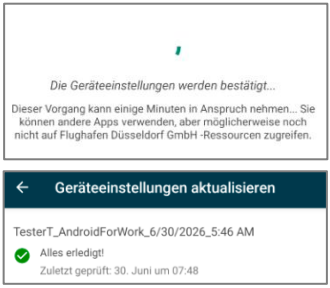
Tippen Sie auf "Auflösen" in dem Unternehmensportal oder auf den entsprechenden Banner, welcher Sie in die Einstellungen leitet.

Sie müssen nun einmalig Ihre bekannte Oberflächensperre eingeben, damit Sie die Daten verändern dürfen.

Vergeben Sie anschließend einen sechsstelligen PIN, welcher zukünftig für den Zugriff auf die Unternehmens-Apps verwendet wird. Ihre derzeit konfigurierte Oberflächensperre für Ihr Smartphone bleibt unverändert.



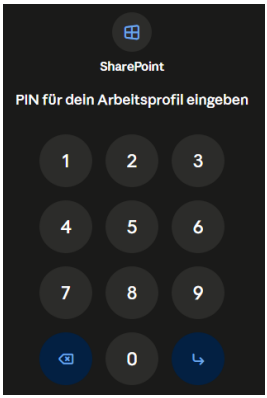




Wechseln Sie anschließend wieder in das Unternehmensportal und tippen auf "Geräteeinstellungen prüfen".

Nach Aktualisierung der Geräteeinstellung ist die Anbindung abgeschlossen.

Wenn Sie nun zukünftig auf Unternehmens-Apps zugreifen (SharePoint-App) werden Sie aufgefordert, den vergebenen PIN einzugeben:



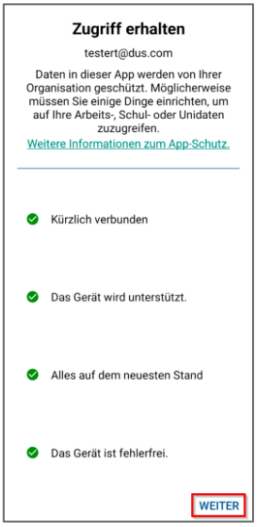
Nach dem Öffnen der SharePoint-App werden Sie aufgefordert Ihre Benutzerdaten für die Anmeldung einzugeben (@dus.com-Adresse). Gegebenenfalls werden Sie nach dem Code für Ihre Multifaktor-Authentifizierung (MFA) gefragt (es öffnet sich hierfür eine entsprechende Benachrichtigung).





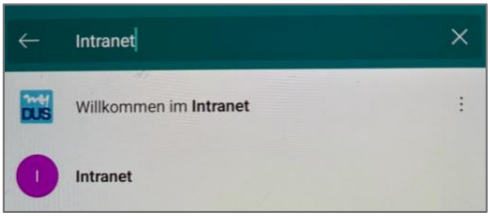
Nach der Anmeldung kann es ein wenig dauern, bis die nächste Meldung angezeigt wird, da die Anforderungen für den Zugriff überprüft werden.

Nach Abschluss erhalten Sie die angezeigte Meldung, welche Sie mit „Weiter“ bestätigen können.



Sie sind nun innerhalb der SharePoint-App angemeldet.

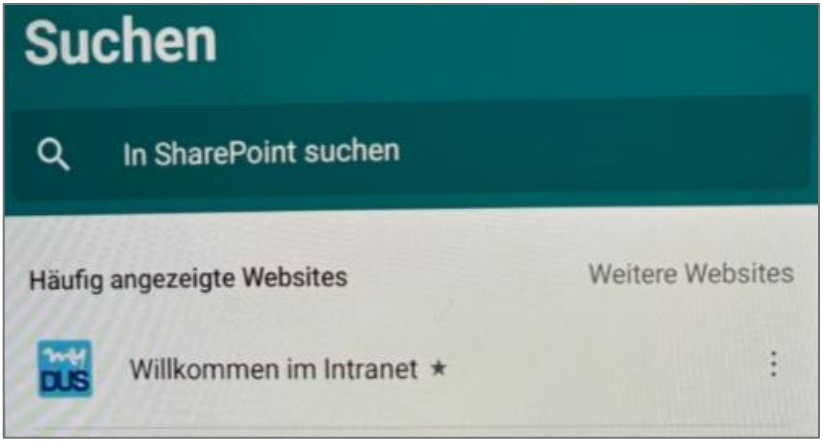
Innerhalb der SharePoint-App haben Sie die Möglichkeit über die Suchleiste am oberen Bildschirmrand das Intranet zu suchen und aufzurufen.



Um das Intranet zukünftig einfacher zu finden, können Sie in der geöffneten Seite über die drei Punkte der Seite „folgen“, so dass diese direkt auf der Startseite beim Öffnen von SharePoint angezeigt wird.







Bitte beachten Sie, dass Links in dem neuen Intranet teilweise auf das alte MA-Portal führen, der Zugriff auf dieses für Ihr Smartphone allerdings nicht freigeschaltet ist und diese Links weiterhin über einen FDG-PC aufgerufen werden müssen.