Evaluierung und Migration eines non Managed Devices in eine EMM Umgebung

Dokumentation der betrieblichen IHK-Projektarbeit

Durchführungszeitraum:
05.03.2020 – 15.04.2020

Auszubildender

Martin Goltschewski
Nadorsterstraße 129-131
26123 Oldenburg

Ausbildungsberuf:

Fachinformatiker*in Systemintegration

Ausbildungsbetrieb:
BTC IT Services GmbH
Escherweg 5
26121 Oldenburg
0441 – 3612 0
ausbildung@btc-ag.com

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

In dieser Dokumentation beschreibe ich den Ablauf meines IHK-Projektes, welches ich zum Abschluss meiner Ausbildung durchgeführt habe. Das Projekt wurde innerhalb der BTC IT Services GmbH (nachfolgend BITS 🕮 genannt) im Team Agile Projekte – Mobility durchgeführt. Aus Datenschutzgründen habe ich alle Kundendaten, Passwörter sowie E-Mail-Adressen unkenntlich gemacht.

1.1 Projektbeschreibung

Der Kunde ist ein mittelständiger Fernleitungsnetzbetreiber für Erdgas, welcher eine Umstrukturierung plant. Zurzeit gibt es beim Kunden noch keine Enterprise Mobile Management (nachfolgend EMM 🕮 genannt) Lösung. Die Mitarbeiter empfangen ihre betrieblichen E-Mails lediglich über den betrieblichen Exchange-Server. Aus diesem Grund unterliegen die Geräte keiner Security-Compliance 🕮 und können nicht auf ihre compliance überwacht werden.

1.2 Projektziele

Das Ziel meines Projektes ist es eine geeignete EMM-Lösung sowie geeignete Endgeräte zu evaluieren und anschließend zu migrieren. Dabei sollten alle Anforderungen des Kunden abgedeckt sein. Die dienstlichen mobilen Endgeräte sollten daher, nach der Umsetzung des Projektes, verwaltet werden können und einer Security-Compliance unterliegen. Die genauen Einschränkungen und Compliance Policies werden hierbei im Rahmen des Projektes mit dem Kunden abgestimmt.

1.3 Projektumfeld

Das Projekt wird bei der BTC IT Services GmbH mit Hauptsitz in Oldenburg durchgeführt. Die BITS ist eine Tochterfirma der Business Technology Consulting AG (im folgenden BTC AG genannt) und eine Enkelgesellschaft der EWE AG. Die BITS beschäftigt derzeit ca. 300 Mitarbeiter und wurde im Jahre 2009 durch die Ausgliederung des Systemmanagements der BTC AG gegründet. Das Portfolio der BITS beinhaltet IT-Services wie z.B. Outsourcing-, Outtasking, Applikation (Betreuung und Monitoring) und projektorientierte Dienstleistungen.

Ich führe das Projekt im Team Agile Projekte – Mobility (auch Team – MDM 🕮 genannt) durch. Das Team kümmert sich um die Verwaltung von mobilen Endgeräten im eigenen Haus und beim Kunden. Das Team begleitet Projekte und erarbeitet permanent neue Methoden zur Verbesserung der Effizienz. Des Weiteren gibt es im Team auch einen Tagesdienst, welcher als Third-Level agiert.

2 Projektplanung

Im Projektmanagement ist die Projektplanung von großer Bedeutung. Ohne eine ausreichende Planung ist ein Projekt schon von Beginn an zum Scheitern verurteilt. Daher möchte ich zu Beginn den Ist-Zustand beschreiben und anschließend die Anforderungen, welche ich mit dem Kunden abstimmen werde, erläutern.

2.1 Zeitplanung

Mein Projekt habe ich in drei Projektphasen aufgeteilt, welche ich in einem Gantt-Diagramm

dargestellt habe.[1] Die einzelnen Projektphasen haben mehrere Teilschritte, welche ich in der detaillierten Zeitplanung aufgeführt habe. Die detaillierte Zeitplanung befindet sich im Anhang.[2]

2.2 Ist-Analyse

Zurzeit befindet sich bei dem Kunden keine EMM - Lösung im Einsatz. Alle dienstlichen mobilen Endgeräte werden manuell per Exchange Active Sync (EAS) 🕮 an das Postfach des Mitarbeiters angebunden und obliegen daher nur sehr begrenzten Einschränkungen. Aus diesem Grund unterliegen die Geräte keiner Security-Compliance und können nicht überwacht werden. Der derzeitige Endgerätebestand setzt sich aus einem nicht homogenen Pool zusammen **(siehe Abbildung 1: Ist-Zustand).**

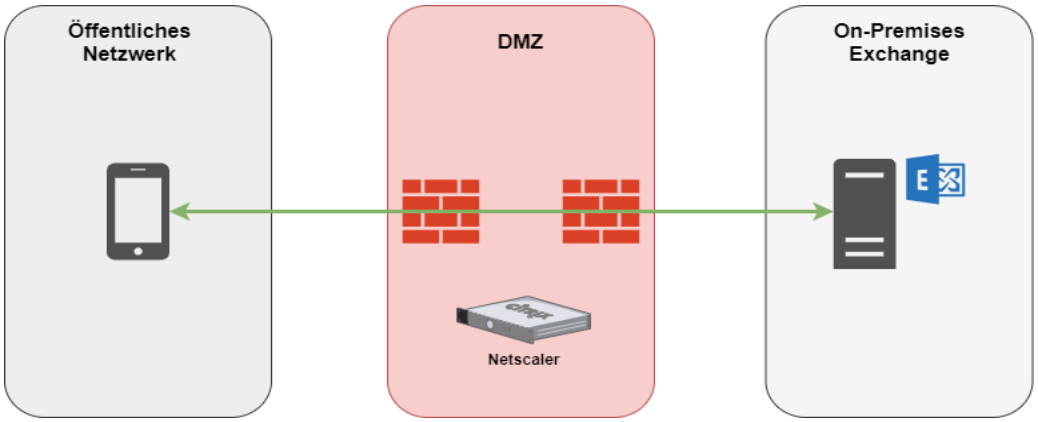


Abbildung 1: Ist-Zustand

2.3 Soll-Konzeption

In der Analysephase meines Projekts werde ich eine geeignete EMM-Lösung anhand einer Nutzwertanalyse 🕮 sowie die dazugehörigen Endgeräte evaluieren. Für die Evaluierung werde ich mich mit dem Kunden zusammensetzen und abstimmen, welche Anforderungen erfüllt sein müssen. Für die Nutzwertanalyse werde ich mir von unserem Einkauf mehrere Angebote für Endgeräte sowie für die EMM-Lösungen einholen. Anschließend werde ich die EMM-Lösung aufbauen, eine Standard-Konfiguration konfigurieren, Compliance Richtlinien festlegen, Gerätebeschränkungen sowie Applikationsrichtlinien konfigurieren und mich um die Bereitstellung der Unternehmens-Apps kümmern. Zum Abschluss werde ich noch eine Qualitätskontrolle durchführen.

2.4 Auflistung meiner Tätigkeiten innerhalb des Projekts

- Evaluierung der Endgeräte
- Evaluierung einer geeigneten EMM-Lösung
- Beschaffung der EMM-Lösung sowie der Endgeräte
- Einrichtung und Konfiguration der EMM-Lösung
- Erstellung einer Standard Konfiguration der Endgeräte
- Erstellung von Compliance Richtlinien
- Erstellung der Geräteeinschränkungen
- Bereitstellung von Apps (Benutzerspezifisch)

[1] Siehe Anhang, Abbildung 4: Soll-Zustand Gantt-Diagramm

[2] Siehe Anhang, Tabelle 7: Detaillierter Zeitplan

- Erstellung von Applikationsrichtlinien
- Qualitätskontrolle – Systemtest

Die Planung sowie die Durchführung des Rollouts und der HyperCare Phase 🕮 ist aus zeitlichen Gründen kein Bestandteil meines Projektes. Diese Tätigkeiten werden daher von meinem Arbeitskollegen übernommen, welche ich nur begleiten werde.

2.5 Terminabstimmung

Da kurzfristige Termine, der Erfahrung nach nicht möglich sind, habe ich zu Beginn des Projektes schon einige Termine definiert. Aufgrund der aktuellen Corona-Pandemie musste ich einige vor Ort-Termine absagen. Ich habe mich mit dem Kunden und meinen Kollegen darauf geeinigt, unseren Termin virtuell stattfinden zu lassen. Ich habe uns daher eine Microsoft Teams-Besprechung 🕮 eingestellt. Zur Veranschaulichung habe ich den AirServer Connect 🕮 von Legamaster benutzt.

2.6 Evaluierung der Endgeräte

Der Kunde hat in unserem Abstimmungstermin den Wunsch geäußert, dass Produkte aus dem Apple Portfolio eingesetzt werden sollen. Bei der Auswahl der Endgeräte, soll vor allem der Patchzyklus beachtet werden. Die Endgeräte sollen so lange wie möglich, im Idealfall noch drei Jahre, mit Sicherheitsupdates versorgt werden und sich im mittleren Preissegment bewegen. Nach einer Umfrage der Mitarbeiter, sollte das Display im Idealfall ca. 6,5“ groß sein. Eine gute Performance sowie eine lange Akkulaufzeit sollten die Endgeräte ebenfalls aufweisen. Die Speicherkapazität sollte mindestens 64GB betragen. Eine Erweiterung des internen Speichers ist nicht zwingend erforderlich. Unser Kunde bevorzugt ein Endgerät, welches wir ggf. bereits bei anderen Kunden im Einsatz haben, um auf ein zuverlässiges Gerät mit guten Erfahrungswerten zu setzen. Eine Fingerprint oder Face-ID 🕮 Authentifizierung 🕮 ist gleichgültig.

Dazu habe ich vier Endgeräte rausgesucht[3] und diese anhand der bereits im Vorfeld definierten Anforderungen, mit Hilfe einer Nutzwertanalyse verglichen.[4] Die Kriterien der Nutzwertanalyse konnte ich anhand der Anforderungen des Kunden ableiten. Die Gewichtung der einzelnen Kriterien habe ich dann gemeinschaftlich mit dem Kunden proportioniert.

2.7 Evaluierung der EMM-Lösungen

In der heutigen Zeit ist es sinnvoll über eine EMM-Lösung nachzudenken, da mobile Endgeräte immer mehr an Bedeutung gewinnen. Ein konventioneller Rechner bietet in der Regel mehr Leistung, jedoch lassen sich viele Aufgaben auch problemlos und angenehmer mit mobilen Endgeräten verrichten. Eine EMM Lösung beinhaltet das MIM (Mobile Information Management), das MDM (Mobile Device Management) und das MAM (Mobile Application Management). Mit einer EMM-Lösung wird daher nicht nur die Managebarkeit von Endgeräten, sondern auch das Managen des Betriebssystems, der APPs und des Datenflusses gewährleistet.

2.7.1 Anforderung der EMM-Lösung

Unser Kunde hat folgende Funktionalitäten als Anforderung gesetzt:

- Endgeräte sollen mit der gleichen Konfiguration ausgerollt werden

[3] Siehe Anhang, Tabelle 8: Vergleich-Endgeräte

[4] Siehe Anhang, Tabelle 9: Nutzwertanalyse-Endgeräte

- Festlegung von Compliance Richtlinien
- Definition von Applikationsrichtlinien
- Konfiguration von Geräteeinschränkungen
- Guter Support (Hersteller)

Des Weiteren hat der Kunde noch vorgegeben, dass bei Verlust oder Diebstahl es möglich sein muss, alle Daten vom Endgerät zu löschen. Diese Anforderungen wird mit der Funktion, dem Full-Wipe 🕮 abgedeckt. Neben den Anforderungen, die der Kunde gestellt hat, gibt es für das MDM noch einen Mindeststandard, welcher vom BSI 🕮 veröffentlicht wurde.[5] Dort sind funktionale Sicherheitsanforderungen definiert, wie z.B:

MDM.01: Nutzdaten = Anfallende Nutzdaten (Konfigurationsprofile, PINs, persönliche Identitätsmerkmale) müssen innerhalb der IT-Infrastruktur des Betreibers verbleiben.

MDM.02: Cloud-Dienste = Wird das MDM ganz oder nur teilweise von einem externen Cloud-Anbieter bezogen, sind zusätzlich die Anforderungen aus dem Mindeststandard des BSI zur „Nutzung externer „Cloud-Dienste“[6] einzuhalten (wie z.B. das Recht auf Prüfungen und Kontrollen vertraglich zusichern, Lokation vertraglich zusichern, Leistungsfähigkeit prüfen [...]).

MDM.03: Mandantentrennung = Sobald mehrere Mandanten auf einem MDM verwaltet werden, muss eine wirksame Trennung der Mandanten sichergestellt sein.

MDM.04: Kompromittierte mobile Endgeräte = Zum Schutz des MDM müssen kompromittierte verwaltete Endgeräte (z.B. durch ein Jailbreak) zeitnah erkannt und ausgeschlossen werden.

MDM.05: Berechtigungsmanagement = Das MDM muss über eine Rechteverwaltung verfügen. Über die Rechteverwaltung müssen Zugriffsrechte zugeordnet werden können.

[…]

Der Mindeststandard stellt Sicherheitsanforderungen an ein MDM, wodurch ein Mindestsicherheitsniveau erreicht wird, welches nicht unterschritten werden sollte.

Mit Hilfe des Magic Quadrant habe ich eine Übersicht der aktuellen Unternehmen im Bereich EMM erhalten.[7] Magic Quadrant ist eine Reihe von Marktforschungsberichten des IT-Beratungsunternehmen „Gartner“. Die Unternehmen werden in vier Quadranten (Nische Players, Visionäre, Challengers, Leader) eingeteilt. Der Magic Quadrant dient zur genauen Analyse der Position eines Unternehmens in einem speziellen Markt. Ich habe mich dazu entschlossen, zwei On-Premises 🕮 Lösungen sowie zwei Cloud 🕮 Lösungen zu evaluieren. Dazu habe ich die Funktionalitäten gegenübergestellt und mit Hilfe einer Nutzwertanalyse verglichen.[8] Die Gewichtung der einzelnen Kriterien habe ich ebenfalls gemeinschaftlich mit dem Kunden proportioniert.

Bei Citrix XenMobile und MobileIron handelt es um On-Premises-Lösungen, wobei Microsoft Intune und VMWare Air-Watch Cloud-Lösungen sind. Daher muss bei den On-Premises-Lösungen noch die Anschaffung der Server berücksichtigt werden. Bezüglich der Anschaffung der Server habe ich mich an unseren Windows Support gewandt und anschließend beim Einkauf ein Kostenvorschlag angefragt. Bei den Cloud-Lösungen fallen diese Kosten natürlich weg. Die Hersteller empfehlen folgende Hardware Anforderungen:

[5].https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_Mobile-Device-Management.pdf?__blob=publicationFile&v=7

[6].https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindeststandards/Mindeststandard_Nutzung_externer_Cloud-Dienste.pdf?__blob=publicationFile&v=9

[7] Siehe Anhang, Abbildung 5: Magic Quadrant-EMM

[8] Siehe Anhang, Tabelle 10: Vergleich-EMM

	Prozessor (vCPU)	Arbeitsspeicher (RAM)	Festplattenkapazität (GB)
MobileIron			
MobileIron Server Appliance	2	4	80
Citrix XenMobile			
Citrix XenMobile Server Appliance	4	8	50

Tabelle 1: Server Hardware Requirements

2.7.2 Kosten-Analyse

Ich habe mir für alle EMM-Lösungen ein Angebot erstellen lassen und mit diesen Werten kalkuliert. Die Kalkulation der jährlichen Lizenzkosten befindet sich im Anhang.[9] Die Microsoft Intune Lizenz ist in der Microsoft Office 365 E3 Lizenz 🕮 enthalten. Da der Kunde uns ebenfalls beauftragt hat, Microsoft Office 365 im Unternehmen einzuführen, habe ich mit den anteiligen Lizenzkosten in Höhe von 4,43 Euro gerechnet.

Kalkulation der Betriebskosten

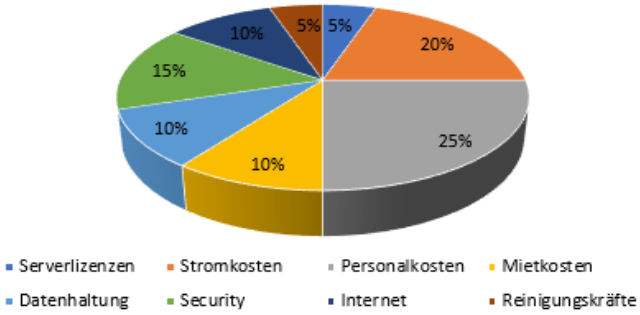


Abbildung 2: Betriebskosten

Die EMM-Lösung soll länger eingesetzt werden, daher habe ich ebenfalls eine Kostenanalyse nach drei und fünf Jahren durchgeführt.

	User (Anzahl)	Citrix XenMobile €	MobileIron €	VmWare Air-Watch €	Microsoft Azure Intune €
Lizenzkosten (Einmalig)	200	8.976,00	19.940,00	33.672,00	10.632,00
Wartungskosten (Jährlich)	200	2.516,52	2.120,00	⊗	⊗
Anschaffungskosten		75.000,00	75.000,00	⊗	⊗
Betriebskosten		8.649,25	9.706,00	⊗	⊗
1-Jahr (Gesamtkosten)	200	95.141,77	106.766,00	33.672,00	10.632,00
3-Jahre (Gesamtkosten)	200	135.425,31	170.298	101.016,00	31.896,00
5-Jahre (Gesamtkosten)	200	175.708,85	233.830,00	168.360,00	53.160,00

Tabelle 2: Lizenzkosten – Jahresübersicht

[9] Siehe Anhang, Tabelle: 12: Citrix XenMobile Jahreskosten – Tabelle 15: Microsoft Intune Jahreskosten

2.7.3 Fazit

Im Anschluss habe ich eine Nutzwertanalyse durchgeführt.[10] Die meisten EMM-Lösungen besitzen nur wenige Unterschiede. Unser Kunde benötigt ebenfalls eine MS365 Lizenz. In der MS365 Lizenz ist eine Microsoft Intune Lizenz enthalten. Microsoft Intune ist für den Kunden im Vergleich zu den anderen Anbietern am günstigen und bietet alle Funktionalitäten, die vom Kunden gefordert waren. Ein weiterer Vorteil ist, dass der Kunde keinen weiteren Support bezahlen muss, da der Intune Support im normalen Microsoft 365 Support enthalten ist. Nach Rücksprache mit dem Kunden, haben wir uns daher aus wirtschaftlichen Gründen für Microsoft Intune entschieden, um die Kosten so gering wie möglich zu halten.

2.8 Rollout – Struktur

Bei der Abstimmung mit dem Kunden sind einige Fragen zum Thema: „Rollout Struktur“ und die „Privatnutzung der mobilen Endgeräte“ aufgekommen. Nach Absprache mit dem Kunden, werde ich eine Übersicht mit den wichtigsten Informationen erstellen, welche ich ihm dann im Nachgang aufzeigen kann. [11]

BYOD = Bring-Your-Own-Device

Bei dieser Strategie werden die mobilen Endgeräte von den Mitarbeitern selbst gekauft und ins Unternehmen eingeführt. Das Unternehmen kann diese Strategie z.B. durch eine Bezuschussung bestärken.

CYOD = Choose-You-Own-Device

Bei dieser Strategie beschafft das Unternehmen die Endgeräte (Corporate Owned) welche dann als Arbeitsmittel an die Mitarbeiter ausgegeben werden. Die Endgeräte gehören vollständig dem Unternehmen. CYOD lässt sich noch in Corporate Owned Business Only (COBO) und Corporate Owned Personally Enabled (COPE) unterteilen:

Corporate Owned Business Only (COBO)	Corporate Owned Personally Enabled (COPE)
Endgerät soll nur beruflich und nicht privat genutzt werden.	Endgerät soll beruflich genutzt werden und ist ebenfalls für die private Nutzung freigegeben.

Tabelle 3: COBO-COPE

2.9 Betrachtung der Privatnutzung

Die Erlaubnis der privaten Nutzung bringt einige Vorteile, aber auch einige Nachteile mit sich. Wenn die private Nutzung des Endgerätes erlaubt ist, gibt es bei den Mitarbeitern eine größere Nutzerakzeptanz. Dadurch, dass die Mitarbeiter nicht noch zusätzlich ein weiteres Endgerät mitnehmen müssen, gestaltet sich der Alltag wesentlich angenehmer. Bei einer privaten Nutzung ist ebenfalls von keiner Einschränkung der Produktivität auszugehen. Privat installierte Applikationen stellen jedoch ein großes Sicherheitsrisiko dar. Das wären z.B. datenschutzrechtliche Gründe oder potenzielle Sicherheitslücken / Schadsoftwaren bei Applikationen oder Updates. Bei Endgeräten wo die private Nutzung verboten und mit Hilfe von Richtlinien eingeschränkt worden ist (COBO), werden nur bekannte und geprüfte Applikationen oder Updates freigegeben. Bei der COPE Struktur kann alles personalisiert werden und jeder Mitarbeiter kann selbst entscheiden, welche Applikationen oder Updates er auf seinem Endgerät installiert. Dadurch kann ein erhöhter Supportaufwand entstehen, wenn

[10] Siehe Anhang, Tabelle 16: Nutzwertanalyse-EMM

[11] Siehe Anhang, Tabelle 17: Rollout-Struktur

durch ein Update oder eine Applikation das Endgerät nicht mehr ordnungsgemäß funktioniert.

Um dem Kunden die bereitgestellten Informationen aufzuzeigen und zu erklären, habe ich mich wenige Tage später mit dem Kunden zusammengesetzt, um mit ihm die weitere Vorgehensweise zu besprechen. Der Kunde und ich sind dann zu dem Ergebnis gekommen, dass der Kunde die Endgeräte bereitstellt (CO) und die private Nutzung der Endgeräte untersagt ist.

3 Durchführungsphase

3.1 Erstellung eines Microsoft Azure Mandanten (Tenant)

Im weiteren Verlauf des Projektes wurde mit dem Kunden abgestimmt, dass die Erstellung des Mandanten (nachfolgend auch „Tenant“ 🕮 genannt) mit Hilfe einer von mir bereitgestellten Anleitung, durch den Kunden eigenständig durchgeführt wird.

3.2 Beschaffung der E3 Lizenz

Nach Rücksprache mit dem Kunden ist die Muttergesellschaft für die Beschaffung der Lizenzen verantwortlich. Ich habe mit dem Kunden vereinbart, dass sobald die Bestellung der Lizenzen ausgelöst worden ist, ich benachrichtigt werde. Nachdem einige Tage vergangen waren und ich keine Rückmeldung erhalten habe, habe ich den Kunden angerufen, mit der bitte um den aktuellen Status. Daraufhin hat er mir mitgeteilt, dass der Antrag bei der Muttergesellschaft liegt und die Lizenzen demnächst vorliegen. Nach wenigen Tagen habe ich dann die Rückmeldung erhalten, dass die Lizenzen bestellt worden sind und auch nun dem Tenant zur Verfügung stehen.

3.3 Azure Active Directory Connect

3.3.1 Abstimmung AD Attribute für Azure AD-Connect

Nachdem die Lizenzen nun verfügbar sind, habe ich mich mit dem AD befasst. Mit dem Kunden wurde abgestimmt, dass die Pflege der Objekte führend im On-Premises AD erfolgen soll und mit Hilfe von Microsoft Azure Active Directory-Connect (nachfolgend Azure AD-Connect 🕮 genannt) in einem vorher definierten Synchronisationsintervall synchronisiert werden. Der Kunde und ich haben uns dann nochmal zusammengesetzt und ich habe ihm meine Empfehlung mitgeteilt, welche Attribute synchronisiert werden sollten und welche nicht. Microsoft bietet eine Empfehlung der zu synchronisierenden Attribute für Intune an, an welche ich mich gehalten habe.[12]

3.4 Einrichtung des Azure Active Directory Connect

3.4.1 Vorbereitung – Azure AD Connect

Damit die Synchronisation 🕮 der benötigten Attribute klappt, muss zu Beginn der Microsoft AD-Connect auf dem Windows Server (On-Premises) installiert werden. Ein Arbeitskollege vom Windows Support, hat mir die benötigten Login Daten für die remote Desktop Verbindung (nachfolgend auch RDP 🕮 genannt) bereitgestellt. Anschließend konnte ich mich mit RDP auf den Server verbinden. Nun habe ich im Azure den Azure Active Directory Dienst aufgerufen und anschließend „Azure AD-Connect“ ausgewählt. Dort erhalte ich einen Überblick über den

[12] https://docs.microsoft.com/de-de/azure/active-directory/hybrid/reference-connect-sync-attributes-synchronized (aufgerufen am 20.03.2020)

Synchronisationsstatus. Da jedoch noch keine Verbindung zwischen dem Azure AD und dem On-Premises AD vorhanden ist, erhalte ich die Rückmeldung, dass noch keine Synchronisation stattgefunden hat. Im Reiter „Namen der benutzerdefinierten Domänen“ habe ich dann die Domäne 🕮 ausgewählt und habe nun die Möglichkeit, die Setup Datei für den AD-Connect herunterzuladen.

3.4.2 Installation vom Azure AD-Connect

Nachdem das Setup nun erfolgreich heruntergeladen worden ist, habe ich die Installation vom Azure AD-Connect gestartet. Dort kann ich zwischen den Express und den benutzerdefinierten Einstellungen wählen. Dort wähle ich die benutzerdefinierten Einstellungen aus, da der Kunde will, dass nur die Intune Attribute und nicht alle Attribute der Domäne synchronisiert werden sollen. Die Auswahl der Attribute erfolgt zu einem späteren Zeitpunkt. Nachdem ich nun die benutzerdefinierte Variante ausgewählt habe, erhalte ich die Rückmeldung, dass kein Synchronisierungsdienst gefunden wurde und der Azure AD Connect-Synchronisierungsdienst installiert wird. Nun muss ich eine Anmeldemethode zur Benutzeranmeldung auswählen, wo ich wie bereits standardmäßig hinterlegt, die Kennworthashsynchronisierung auswähle. Anschließend muss ich mich mit den Azure AD Zugangsdaten authentisieren 🕮. Nach einer erfolgreichen Authentifizierung wird mir dann die erforderliche Gesamtstruktur und die bereits konfigurierten lokalen Verzeichnisse angezeigt. Daraufhin muss ich anschließend überprüfen, ob die Azure AD Domain mit der lokalen Domain übereinstimmt. Eine übereinstimmende User Principal Name (auch UPN 🕮 genannt) wie z.B. die E-Mail-Adresse ist essenziell, um sich später auch mit denselben Anmeldeinformationen, wie bei der lokalen Domain anmelden zu können.

Daraufhin lege ich fest, welche Organisationseinheiten 🕮 in der Domain synchronisiert werden sollen. Hätte ich mich zu Beginn für die Express-Einstellungen entschieden, würden jetzt alle Organisationseinheiten automatisch synchronisiert werden.

Im Anschluss besteht noch die Möglichkeit festzulegen, ob nur bestimmte Benutzer oder Endgeräte synchronisiert werden sollen. Da jedoch mit dem Kunden abgestimmt worden ist, dass alle Endgeräte und Benutzer der Domain synchronisiert werden sollen, habe ich mich für die Auswahl „Alle Benutzer und Geräte synchronisieren“ entschieden.

Im nächsten Schritt besteht die Möglichkeit, Optionale Features zu installieren. Ich habe mich entschieden, die Funktion „Azure AD-App- und Attributfilterung“ sowie die Funktion „Kennwortrückschreiben“ zu aktivieren. Bei der Azure AD-Attributfilterung habe ich die Möglichkeit zu entscheiden, welche Attribute synchronisiert werden sollen und welche nicht.

Wie auch schon unter 3.3.1 Abstimmung AD-Attribute für Azure AD Connect beschrieben, hat Microsoft eine Empfehlung über die erforderlichen Attribute verfasst. Diese Empfehlung hat Microsoft in sogenannte „App-Sets“ 🕮 zusammengefasst. Bei der Kennwortrückschreibung werden Passwörter, die in der Cloud geändert worden sind, in Echtzeit, in das lokale Verzeichnis zurückgeschrieben.

Sobald die Funktion aktiviert ist, kann ich nun zwischen den App-Sets (Intune, Exchange Online, SharePoint, Lync Online, etc.) auswählen. Daraufhin erhalte ich eine Übersicht mit den Attributen, die nun synchronisiert werden. Es besteht die Option, erneut zu Filtern. Da dort jedoch keine Anpassung mehr nötig ist, klicke ich auf „Weiter“. Nach wenigen Sekunden ist die Konfiguration abgeschlossen und der AD-Connect ist erfolgreich eingerichtet.

3.5 Microsoft E3 Lizenz – Überprüfung

Nachdem der AD-Connect installiert und konfiguriert worden ist, muss ich überprüfen, ob die Lizenzen nun im Azure Tenant hinterlegt sind. Unter dem Reiter „Lizenzen“ gibt es eine Übersicht über alle Lizenzen, die erworben und dem Tenant zugewiesen wurden. Dort sind nun auch die von der Muttergesellschaft bestellten Lizenzen vorhanden. Über die Option

„Serviceplandetails“ erhalte ich die Übersicht über alle Lizenzen, die in der Microsoft E3 Lizenz enthalten sind.

3.6 Erstellung einer Gruppe und Zuweisung der Microsofts E3 Lizenz

Da die E3 Lizenz dem Tenant nun zugewiesen ist, kann ich mit der Erstellung der Gruppe fortfahren. Um sich alle Gruppen im Azure anzeigen zu lassen, muss „Gruppen“ im linken Reiter ausgewählt werden. Dort habe ich die Möglichkeit, eine neue Gruppe anzulegen. Beim Anlegen einer neuen Gruppe, muss ich nun einen Gruppentyp, Gruppennamen, eine Gruppenbeschreibung(optional) und einen Mitgliedschaftstyp festlegen. Beim Gruppentyp habe ich die Auswahl zwischen folgenden Typen:

- **Sicherheit** = dient zur Verwaltung von Mitgliedern und des Computerzugriffs auf freigegebene Ressourcen für eine Gruppe von Benutzern. Es kann daher zum Beispiel eine Sicherheitsgruppe für eine bestimmte Sicherheitsrichtline erstellt werden.
- **Office 365** = bietet die Möglichkeit zur Zusammenarbeit, indem Mitgliedern Zugriff auf freigegebene Postfächer, Kalender, Dateien, SharePoint gewährt wird. Des Weiteren können auch Personen außerhalb der Organisation Zugriff auf die Gruppe erhalten.

Bei dem Gruppentyp entscheide ich mich bewusst für „Sicherheit“, da ich dieser Gruppe die E3 Lizenz zuweisen möchte. Alle Mitglieder dieser Gruppe erhalten dann eine Microsoft E3 Lizenz. Ich kann somit ohne großen Aufwand festlegen, welcher Mitarbeiter eine Microsoft E3 Lizenz erhalten soll. Alternativ muss ich jedem Benutzer eine Lizenz zuweisen, was jedoch mit einem sehr hohen Arbeitsaufwand verbunden ist. Ein weiterer Vorteil ist, dass die Lizenzzuweisung natürlich auch für Mitarbeiter gilt, die in der Zukunft der Gruppe zugewiesen werden. Nachdem ich die aufgelisteten Parameter nun ausgefüllt habe, habe ich die Gruppe angelegt. In den Gruppeneinstellungen kann ich unter dem Reiter „Lizenzen“, der Gruppe eine Lizenz zuweisen.

3.7 Einrichtung: Apple Business Manager

Nachdem nun die Gruppe mit der Microsoft E3 Lizenz im Azure angelegt worden ist, habe ich mich mit dem Apple Business Manager beschäftigt. Der Apple Business Manager (nachfolgend ABM 🕮 genannt) ist ein webbasiertes Portal für die IT-Administration, um iPhone, iPad, iPod touch- und Apple TV-Geräte sowie Mac-Computer von einem Ort aus bereitzustellen. Mithilfe einer MDM-Lösung lassen sich Geräteeinstellungen konfigurieren sowie Apps und Bücher kaufen und verteilen.

Die Erstellung des ABM Kontos obliegt der Mitwirkungspflicht des Kunden. Die BITS ist lediglich für die Bereitstellung einer Anleitung verpflichtet. Da wir mehrere Kunden betreuen haben wir bereits ein Quick Start Guide für die Erstellung eines ABM Kontos. Bei der Anleitung handelt es sich um eine standardisierte Anleitung, welche nicht von mir verfasst worden ist. Daher kann die Anbindung an das MDM System erst nach der Aktivierung und Verifizierung des Accounts durch Apple erfolgen. Mit dem Kunden wurde abgestimmt, dass dieser mir mitteilt, sobald der Account erstellt und die Apple Verifizierung abgeschlossen worden ist. Nachdem der ABM Account erstellt und verifiziert worden ist, kann der Kunde anhand der Organisations-ID 🕮 die mobilen Endgeräte beschaffen.

3.8 Einrichtung: Apple Push Notification Service (APNS)

Nachdem nun der Kunde beauftragt wurde einen ABM Konto anzulegen, habe ich mich mit dem Apple Push Notification Service (nachfolgend auch APNS 🕮 genannt) befasst. APNS ist ein Dienst von Apple, der es einem Drittanbieter (wie z.B. Intune) erlaubt, Nachrichten oder

Befehle an ein iOS 🕮 Endgerät zu senden (siehe Abbildung 2: APNS-Aufbau). Aus diesem Grund wird der APNS auch oft als Herzstück der Remote-Benachrichtigungsfunktion bezeichnet. APNS verwendet dabei die Push-Technologie über eine stets geöffnete IP-Verbindung.

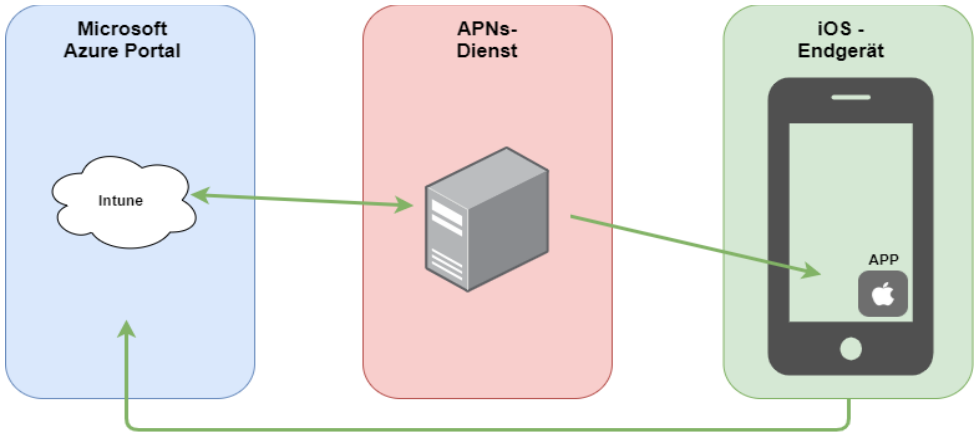


Abbildung 3: APNS-Aufbau

3.8.1 Erstellung des Apple MDM-Push-Zertifikats

Das gewünschte MDM-Push-Zertifikat 🕮 lässt sich mit Hilfe von Microsoft Intune und dem Apple Push Certificate Portal[13] 🕮 erstellen. Um jetzt das gewünschte MDM-Push-Zertifikat zu erstellen, muss ich zuerst die Geräteregistrierung aufrufen. Dort kann ich zwischen einer Apple, Android 🕮, sowie einer Windows-Registrierung 🕮 unterscheiden. Dort muss ich die Apple-Registrierung auswählen. Unter dem Punkt „Apple-MDM-Push-Zertifikat“ habe ich nun die Möglichkeit, dass gewünschte Zertifikat anzufordern. Dort muss ich zuerst Microsoft die Erlaubnis erteilen, sowohl Benutzer als auch Geräteinformationen an Apple zu senden. Im Anschluss kann ich dann die Intune-Zertifikatsanforderung herunterladen. Diese Zertifikatsanforderung wird nachher bei der Erstellung des MDM-Push-Zertifikats benötigt. Um jetzt ein MDM-Push-Zertifikat zu erstellen, muss ich auf den Link „Eigenes MDM-Push-Zertifikat erstellen“ klicken. Dieser Link ist eine Weiterleitung zum Apple Push Certificate Portal. Dort werde ich aufgefordert, mich mit dem Apple Account anzumelden. In diesem Portal kann nun das gewünschte Zertifikat mit Hilfe der Intune-Zertifikatsanforderung erstellt werden. Um jetzt das Zertifikat zu erstellen, klicke ich auf „Create a Certificate“. Daraufhin werden mir die „MDM Certificate Agreements“ angezeigt, welche ich erst bestätigen muss. Nun werde ich aufgefordert, die Intune-Zertifikatsanforderung auszuwählen. Im Anschluss wird die Zertifikatsanforderung überprüft und ich erhalte mein MDM-Push-Zertifikat.

3.9 Apple Business Manager: MDM-Server hinzufügen

Mittlerweile habe ich vom Kunden die Rückmeldung erhalten, dass die Endgeräte geliefert worden sind. Nun kann ich im ABM einen neuen „MDM-Server“ hinzufügen. Der gewünschte Server wird erst durch die erfolgreiche zweistufige Autorisierung im ABM hinzugefügt. Dazu habe ich mich an die von Microsoft zur Verfügung gestellte Anleitung gehalten[14]. Bevor ich im ABM einen MDM-Server hinzufügen kann, muss beim MDM-Provider ein Zertifikat angefordert werden. Bei der Geräteregistrierung im Microsoft Intune kann ich unter dem Reiter „Token für

[13] https://idmsa.apple.com/ (aufgerufen am 24.03.2020)

[14] https://support.apple.com/de-de/guide/apple-business-manager/asm1c1be359d/web (aufgerufen am 26.03.2020)

Registrierungsprogramm“ einen Token 🕮 hinzufügen. Dort wird mir eine Übersicht angezeigt, welche Token bereits hinzugefügt worden sind. Da jedoch noch kein Token für ein MDM-Server vorhanden ist, muss ich erst einen hinzufügen. Dazu muss ich Microsoft erneut die Genehmigung erteilen, sowohl Benutzer- als auch Geräteinformationen an Apple zu senden. Im Anschluss kann ich das Intune-Zertifikat herunterladen. Dieses Zertifikat dient als öffentlicher Schlüssel. Diesen Schlüssel kann man sich anzeigen lassen, indem man das Zertifikat (die „.pem“ Datei 🕮) mit einem Texteditor (z.B. Notepad++) öffnet. Nachdem ich nun das Intune Zertifikat heruntergeladen habe, habe ich mich im ABM angemeldet. Da es sich bei meinem Account um einen Admin-Account mit vollen Zugriffsrechten handelt, habe ich die Möglichkeit, in den Einstellungen einen neuen MDM-Server einzurichten. Dazu muss ich einen MDM-Servernamen auswählen, dem MDM-Server das Entfernen von Geräten erlauben und das vorhin heruntergeladene Zertifikat (Öffentlicher Schlüssel) einbinden. Mit „Sichern“ kann ich diesen MDM-Server erstmal sichern. Der MDM-Server im ABM ist jedoch noch nicht funktionsfähig, da dieser noch nicht beim MDM-Server Provider installiert worden ist. Um diesen Server auch beim MDM-Provider zu installieren, muss ich einen Token vom MDM-Server im ABM generieren. Dieser Token lässt sich generieren, indem ich den vorhin erstellten MDM-Server auswähle und über den Button „Token laden“ einen Token generiere. Daraufhin erhalte ich einen Token im „.p7m“ Dateiformat 🕮. Diesen Token muss ich im Microsoft Intune einbinden, genau dort wo ich den Intune Token für den ABM MDM-Server heruntergeladen habe. Zum Abschluss erhalte ich eine Zusammenfassung der Einstellungen und mit dem Button „Erstellen“ ist die Registrierung und Erstellung des MDM-Servers im ABM abgeschlossen. Die Autorisierung war erfolgreich. Abschließend muss ich diesen MDM-Server jedoch noch als Default-Server festlegen. Unter dem Punkt „Einstellungen für die Geräteverwaltung“ habe ich die Möglichkeit, sowohl für iPhones, iPads. iPods, Macs, und Apple TVs einen Default MDM-Server festzulegen. Jedes Endgerät, welches dann im ABM eingebunden wird, wird dann anschließend dem standardmäßig hinterlegten MDM-Server zugewiesen.

3.10 VPP Token im Microsoft Intune einrichten

3.10.1 Was ist VPP?

VPP 🕮 ist die Abkürzung für Volume Purchase Program. VPP bietet Unternehmen die Möglichkeit, verschiedene APPs (Volumelizenzen) zentral im VPP-Store zu kaufen und über die MDM-Lösung an die Anwender zu verteilen. Dieses funktioniert für Kostenpflichtige und kostenlose Apps. Daher wird VPP genutzt um Apps ohne eine Apple-ID auf iOS und macOS Geräten bereitzustellen.

3.10.2 Einrichtung

Nachdem der MDM-Server im ABM und im Intune erfolgreich installiert worden ist, habe ich mich mit der Erstellung und Einbindung des VPP Token im Intune beschäftigt. Dort muss ich mir im ABM in den „Apps und Bücher“ Einstellungen ein VPP Token generieren und herunterladen. Im Intune, in den Client Apps Einstellungen, habe ich die Option einen Apple-VPP-Token hinzuzufügen. In den Grundeinstellungen muss ich einen Tokennamen angeben, die Apple-ID festlegen und anschließend die VPP-Tokendatei hochladen. Bei der Tokendatei handelt es sich um die Datei, welche ich zuvor aus dem ABM heruntergeladen habe. Anschließend muss ich ein Land /eine Region sowie den Typ des VPP-Kontos auswählen. Bei der Art des VPP-Kontos habe ich Business ausgewählt, da es sich um ein Unternehmens-VPP Konto handelt. Des Weiteren muss ich Microsoft erneut die Erlaubnis erteilen, sowohl Benutzer- als auch Geräteinformationen an Apple zu senden. Im weiteren Schritt gekennzeichnet mit dem Namen „Bereichstags“, habe ich keinen Tag ausgewählt. Mit einem Bereichstag, auch Bereichsmarkierungen genannt, wird sichergestellt, dass die richtigen

Administratoren über die korrekten Zugriffsrechte für die entsprechenden Intune-Objekte verfügen[15]. Wenn dieser den erforderlichen Bereichstag nicht besitzt, hat er keine Zugriffsrechte, welche daher für ihn auch nicht sichtbar sind. Abschließend erhalte ich noch eine Zusammenfassung und kann anschließend den VPP Token erstellen.

3.11 Erstellung eines DEP – Profil

Ich habe mich dazu entschieden, erst ein VPP Token zu erstellen damit ich anschließend bei der Erstellung des DEP 🕮 Profil einen VPP Token einbinden kann. Dadurch wird bei dem Enrollment gleich der VPP Token mit eingebunden und es ist später im Apple Store kein Account mehr nötig. Das gewünschte DEP-Profil lässt sich ebenfalls im Microsoft Intune erstellen. Dort muss ich den zu Beginn erstellten Token für das Registrierungsprogramm auswählen. Nun kann ich zwischen der Geräte-Verwaltung und der Profil-Verwaltung wählen. Da ich ein DEP-Profil erstellen möchte, wähle ich die Profil-Verwaltung aus. Dort kann ich dann noch beim Anlegen eines neuen Profils, zwischen einem iOS und einem macOS 🕮 Profil unterscheiden. Da es sich dabei um iOS-Endgeräte handelt, habe ich das iOS-Profil ausgewählt. Nun muss ich einen Profilnamen sowie eine Beschreibung angeben. Nach den Grundlegenden Einstellungen folgen die Geräteverwaltungseinstellungen. Dort besteht die Option mit oder ohne Benutzeraffinität zu registrieren. Ich habe mich mit dem Kunden abgestimmt, dass mit Benutzeraffinität registriert werden soll. Durch die Benutzeraffinität erfolgt eine Zuordnung zwischen dem Benutzer und einem Endgerät, weswegen dort dann auch eine Authentisierung erforderlich ist. Des Weiteren lassen sich noch Verwaltungseinstellungen wie z.B. das Verhindern einer Synchronisation mit einem Computer oder das dynamische Festlegen eines Gerätenamen, tätigen. Vor dem Erstellen des Profils, erhalte ich noch eine Zusammenfassung der Einstellungen, welche ich bestätigen muss.

3.12 Abstimmung der Benutzerrichtlinien und Konformitätsrichtlinien

Nachdem das DEP Profil erstellt worden ist, habe ich mich nun um die Benutzerrichtlinien 🕮 sowie die Konformitätsrichtlinien 🕮 gekümmert. Dazu habe ich mit dem Kunden einen Termin vereinbart, indem wir uns bezüglich der Richtlinien abgestimmt haben. Da wir Intune bereits bei mehreren Kunden vertreiben, habe ich von meinem Kollegen eine Policy-Vorlage erhalten, wo schon einige Device-Features enthalten waren, die ich dann erweitert und anschließend für die Kundenabstimmung vorbereitet habe[16]. Ich habe daher schonmal meine Empfehlungen vorgegeben und diese dann mit dem Kunden besprochen. Die Benutzerrichtlinien habe ich in folgende Unterkategorien unterteilt: Gerätefunktionen, Geräteeinschränkungen und E-Mail-Verkehr.

3.12.1 Einrichtung der Konformitätsrichtlinien

Die Compliance-Richtlinien, auch Konformitätsrichtlinie genannt, lassen sich im Intune unter der Gerätekompatibilität, in den Richtlinien-Einstellungen verwalten. Die Konformitätsrichtlinie gibt an, welchen Anforderungen ein Endgerät entsprechen muss, um als konform zu gelten. Nur Endgeräte die Konform sind erhalten Unternehmenszugang. Die Erstellung von Richtlinien ist im Microsoft Intune sehr benutzerfreundlich, da jede Richtlinie eine genaue Beschreibung enthält und sich die Richtlinien einfach über ein „Slider-Button“ anpassen lassen. Die iOS-Richtlinien sind in 4 Kategorien unterteilt:

[15] https://docs.microsoft.com/de-de/mem/intune/fundamentals/scope-tags (aufgerufen am 27.03.2020)

[16] Siehe Anhang, Abbildung 7: Richtlinien-Gerätefunktion – Abbildung9: Richtlinien-Geräteeinschränkungen_III

E-Mail

Bei der E-Mail Richtline hat der Administrator die Möglichkeit, festzulegen, ob ein installiertes verwaltetes E-Mail Profil erforderlich ist.

Geräteintegritätsdienst

Bei dem Geräteintegritätsdienst lassen sich Einstellungen tätigen, welche verhindern, dass Geräte z.B. mit einem Jailbreak 🕮 Unternehmenszugriff erhalten. Des Weiteren lässt sich noch festlegen, welche Gerätebedrohungsstufe ein Endgerät max. oder mind. enthalten darf/muss. Diese Funktion benötigt jedoch die Anbindung an eine Threat-Defense-Lösung 🕮.

Geräteeigenschaften

Unter den Geräteeigenschaften lässt sich festlegen, welche Mindestversion oder maximale Version vom iOS vorhanden sein muss.

Systemsicherheit

Unter diesem Punkt kann der Administrator die Gerätesicherheit konfigurieren. Dort besteht die Möglichkeit, einfache Passwörter wie z.B. „123“ oder „000“ zu blockieren, eine Mindestlänge sowie den Typ eines Kennwortes festzulegen. Ebenso lässt sich noch der Zeitintervall für eine Kennwortänderung festlegen sowie unerwünschte APPs einschränken. Sobald mindestens eine App auf einem Endgerät installiert ist, welche sich ebenfalls auf der Liste der Einschränkungen befindet, wird das Gerät als nicht konform markiert und der Unternehmenszugang wird verweigert.

Ebenfalls lässt sich noch einstellen, welche Aktion ausgeführt werden sollen, sobald eine Inkompatibilität vorliegt.

- E-Mail an Endbenutzer senden
- Nicht konformes Gerät zurückziehen
- Nicht konformes Gerät remote sperren

3.12.2 Zuweisung der Konformitätsrichtlinien

Nachdem die Compliance-Richtlinie erfolgreich erstellt worden ist muss ich die Geräterichtlinie noch einer Gruppe oder Benutzern zuweisen. Sobald in einem Unternehmen verschiedene Endgeräte zum Einsatz kommen, empfiehlt es sich für jeden Gerätetyp/ jedes OS eine eigene Gruppe zu erstellen. Da bei meinem Kunden nur Endgeräte aus dem Apple Portfolio zum Einsatz kommen, welche nur auf iOS basieren, habe ich die Richtlinie nur einer Gruppe mit allen Mitarbeitern zugewiesen.

3.12.3 Einrichtung der Benutzerrichtlinien

Die Benutzerrichtlinien dienen zur Geräteeinschränkung, da nicht jeder Benutzer die gleichen Berechtigungen hat. Die Einrichtung der Benutzerrichtlinien basiert auf dem gleichen Konzept wie bei den Konformitätsrichtlinien. Dort muss ich zu Beginn ein Profil erstellen und anschließend die benötigte Plattform auswählen. Danach habe ich nun die Auswahl zwischen verschiedenen Kategorien wie z.B. E-Mail, Geräteeinschränkungen, Gerätefunktionen, Benutzerdefiniert, VPN, WLAN 🕮 etc. Dadurch, dass ich mich mit dem Kunden bereits abgestimmt habe, musste ich lediglich die Liste abarbeiten und die richtigen Einstellungen tätigen.

3.12.4 Zuweisung der Benutzerrichtlinien

Die Zuweisung der Benutzerrichtlinien erfolgt genauso wie bei den Konformitätsrichtlinien.

3.13 Abstimmung der Unternehmens-App

Da ich mit dem Kunden einen Termin zur Abstimmung der Benutzerrichtlinien hatte, habe ich in dem gleichen Termin auch die Abstimmung der Unternehmens-Apps durchgeführt. Der

Kunde hatte mir vorab eine Liste geschickt, in welcher die benötigten Apps aufgelistet waren. Da mehrere Apps gleiche Funktionalitäten beinhalteten, habe ich eine Vorauswahl getroffen und diese dann im Anschluss mit dem Kunden abgestimmt.[17]

3.13.1 Einführung der Unternehmens Apps ins Intune

Da ich bereits den VPP Token im Intune eingebunden habe, befinden sich nun alle gekauften Apps im Intune. Nachdem nun die VPP Apps im Intune eingebunden sind und die Abstimmung mit dem Kunden erfolgte, kann ich mich der Erstellung der App-Schutzrichtlinien widmen.

3.13.2 Erstellung der App-Schutzrichtlinien

Die Schutzrichtlinien lassen sich im Microsoft Intune unter den Client-Apps Einstellungen einrichten. Bei der Erstellung kann ich zwischen einer iOS/iPadOS 🕮, Android oder Windows 10 Richtlinie präferenzieren. Standardmäßig muss ich zu Beginn einen Namen für die Richtlinie festlegen und kann ggf. eine Beschreibung hinzufügen. Es besteht noch die Möglichkeit, die Apps auf allen Gerätetypen oder auf nur einen vorher definierten Gerätetypen festzulegen. Da ich jedoch will, dass die Schutzrichtlinie auf allen Endgeräten wirkt, habe ich die Apps auf allen Gerätetypen festgelegt. Damit eine Schutzrichtlinie auch Sinn macht, muss auch definiert werden, bei welchen Apps die Richtlinien wirken sollen. In den Einstellungen kann ich daher zwischen öffentlichen und benutzerdefinierten Apps auswählen. Nachdem die Apps nun ausgewählt worden sind, besteht die Option, Einstellungen in den nachfolgenden Kategorien zu tätigen.

- **Datenschutz =** In dieser Kategorie lassen sich Einstellungen in Bezug auf die Verhinderung von Datenverlust (Data Loss Prävention 🕮) tätigen.
- **Zugriffsanforderungen =** Bei den Zugriffsanforderungen besteht die Option festzulegen, welche Anmeldeinformationsanforderungen erfüllt sein müssen, um auf die App zuzugreifen.
- **Bedingter Start =** Dort habe ich die Möglichkeit, Sicherheitsanforderungen für meine Zugriffsschutzrichtlinie festzulegen.
- **Zuweisung =** In dieser Kategorie lässt sich nun die erstellte Sicherheitsrichtline einer Gruppe zuweisen und einigen Gruppen ausschließen.

3.13.3 Zuweisung der Unternehmens- App

Die Apps befinden sich nun im Intune und eine Schutzrichtlinie ist auch erstellt. Das System kann jedoch noch keine Zuordnung zwischen Applikation und dem Anwender herstellen. Dazu muss ich einem Anwender die gewünschten Applikationen zuweisen. Dazu habe ich die Gruppe „XXX_Mitarbeiter“ erstellt und alle „normalen“ Mitarbeiter hinzugefügt. Bei der Erstellung der Gruppe ist zu beachten, dass der Mitgliedschaftstyp ebenfalls auf „Dynamischer Benutzer“ gesetzt wird. Dadurch werden nun alle neuen Mitarbeiter automatisch in die Gruppe eingepflegt. Für die Führungskräfte, sowie die VIPs 🕮 habe ich eine separate Gruppe erstellt. Somit muss ich die ausgewählten Apps nicht jedem Anwender zuweisen, sondern kann die Zuweisung der Apps mit Hilfe der Gruppe tätigen. Im Intune gibt es folgende verschiedene Zuweisungsarten:

Erforderlich: Bei dieser Zuweisungsart werden die Applikationen automatisch auf die registrierten mobilen Endgeräte gepusht und installiert.

Für registrierte Geräte verfügbar: Bei dieser Zuweisungsart werden die Applikationen der Gruppe zugewiesen. Die Anwender können sich die Applikationen im Nachhinein aus dem Unternehmensportal herunterladen.

Deinstallieren: Bei dieser Zuweisungsart wird die Applikation automatisch auf den mobilen Endgeräten gelöscht.

[17] Siehe Anhang, Tabelle 18: Unternehmens-Apps-1 – Tabelle 19: Unternehmens-Apps-2

Bei der Zuweisung habe ich ebenfalls die Möglichkeit, zwischen einer Benutzerlizensierung und einer Gerätelizensierung zu unterscheiden. Es besteht ebenfalls die Option, die Lizenz nach der Deinstallation der App zu entfernen. Bei der Benutzerlizensierung wird die Lizenz (gekaufte Apps) an die Apple-ID des Nutzers verknüpft. Bei der Gerätelizensierung wird die Lizenz mit dem Endgerät verknüpft. Ich habe mich daher bewusst für die Gerätelizensierung entschieden, da jeder Mitarbeiter nur ein Endgerät besitzt und somit auch keine Abfrage bezüglich der Apple-ID erhält.

4 Abschluss und Abnahme

In der Abschlussphase habe ich mein Projekt rückwirkend bewertet, indem ich meinen zu Beginn erstellten Zeitplan überprüft habe. Abschließend habe ich eine Kostenkalkulation meines Projektes erstellt.

4.1 Soll- / Ist-Vergleich

Im Vergleich zu dem Projekt Antrag gab es kleinere Abweichungen im Zeitplan. Die Abweichungen habe ich in der folgenden Tabelle gekennzeichnet. Der detaillierte Zeitplan ist dem Anhang angefügt.[18]

Projektphase	Dauer (Soll) in h	Dauer (Ist) in h	Abweichungen (h)
Planungsphase	8	11	+3
Durchführungsphase	19	18	-1
Abschlussphase	8	6	-2

Tabelle 4: Soll-/ Ist-Vergleich - Grobe Übersicht

4.2 Projektkosten

Während der Durchführung meines Projektes sind verschiedene Kosten innerhalb der BITS entstanden. Die entstandenen Kosten lassen sich in Personal- und Materialkosten aufteilen.

4.2.1 Projektkostenanalyse

Kostenart	Person / Abteilung	Aufwand (h)	Einzelkosten €/h	Gesamtkosten (€)
Personalkosten	Martin Goltschewski	35	75,00	2.625,00
	Windows Support	1	97,00	97,00
	MDM Betrieb	2	97,00	194,00
	Einkauf	3	97,00	291,00
Materialkosten	iPhone 11 (Testgerät)	1.Monat	49,00	49,00
	Kundentermin (Bewirtung)		25,00	25,00
	Gemeinkosten (Strom, Miete etc.)	5 % der Projektkosten		164,05
Gesamtkosten		**3.445,05**		

Tabelle 5: Projektkostenanalyse

[18] Siehe Anhang, Tabelle 7: Detaillierter Zeitplan

Gemeinkosten: Die BITS berechnet bei Projekten in diesem Umfang, für die Gemeinkosten, eine Pauschale in Höhe von 5%.

4.3 Fazit

Aufgrund der Ist-Analyse sowie der Soll-Konzeption konnte ich relativ schnell geeignete Endgeräte sowie eine EMM-Lösung evaluieren. Bei der Planung des Projektes habe ich jedoch die Rollout-Struktur sowie die private Nutzung der Endgeräte nicht von Anfang an bedacht. Daher hat die Ausarbeitung der Informationen, die Erstellung der Dokumente sowie die Bereitstellung zusätzlich Zeit beansprucht. Insgesamt habe ich in der Planungsphase drei Stunden mehr benötigt, als zu Beginn geplant. Diese zusätzlichen Stunden konnte ich jedoch in der Durchführungsphase sowie in der Abschlussphase wieder einsparen. Das Projekt wurde daher trotz der kleinen Abweichungen im Zeitplan, erfolgreich innerhalb der 35 Stunden umgesetzt. Jedes Endgerät, welches mit der Organisations-ID beschafft wird und sich im ABM befindet, befindet sich nun in der Geräteverwaltung und wird daher automatisch mit einer Standard-Konfiguration ausgeliefert. Es wurden alle angeforderten Compliance Richtlinien festgelegt, Applikationsrichtlinien sowie Gerätebeschränkungen konfiguriert. Des Weiteren erfolgt eine benutzerspezifische Bereitstellung von APPs. Während der Umsetzung kamen jedoch noch einige neue Anforderungen vom Kunden bezüglich einer VPN-Verbindung 🕮 und einem PKCS 🕮. Diese Anforderungen werden jedoch innerhalb eines anderen Projektes realisiert.

5 Anwenderdokumentation

Die Anwenderdokumentation ist dem Anhang beigefügt. Nach Rücksprache mit dem Kunden, wird dem Kunden eine PowerPoint bereitgestellt. Das PowerPoint Design wurde nicht von mir, sondern von einem Arbeitskollegen erstellt. Aufgrund des PowerPoint Designs, lassen sich jedoch Rückschlüsse auf die Identität des Kunden schließen. Daher wurde die PowerPoint in Word importiert.

6 Betriebsdokumentation

Die Betriebsdokumentation ist dem Anhang beigefügt.

7 Quellenverzeichnis

www.bsi.bund.de
www.docs.microsoft.com
www.microsoft.com
www.apple.com
www.mobileiron.com
www.citrix.com
www.air-watch.com
www.portal.azure.com

8 Anhang

Anhangsverzeichnis

8.1 Glossar

ABM	Apple Business Manager.
AirServer	Mit AirServer ist es möglich, Inhalte vom mobilen Endgerät auf einen Desktop Rechner zu streamen.
Android	Android ist ein Betriebssystem sowie eine Software Plattform für mobile Endgeräte.
APNS	Apple Push Notification Service - Plattformbenachrichtigungsdienst mit dem Drittanbieter Benachrichtigungsdaten an ein Apple Endgerät senden können.
Apple Push Certificates Portal	Portal, um ein MDM-Push-Zertifikat zu erstellen und zu verwalten.
Appliance	Funktionelle Kombination von Hard- und Software welche für eine bestimmte Aufgabe erstellt worden ist.
App-Sets	Von Microsoft veröffentlichte Liste von AD Attributen, welche für einen bestimmten Dienst benötigt werden wie z.B. Microsoft Intune.
Authentifizierung	Prüfung der Authentisierung.
Authentisierung	Nutzer legt mit einer Authentisierung einen Nachweis einer bestimmten Identität vor.
Azure AD-Connect (AAD-Connect)	Ermöglicht die Synchronisation zwischen On-Prem AD und Azure-AD.
Benutzerrichtlinien	Richtlinie für die Geräteeinschränkung.
BITS	BTC IT Services.
BSI	Bundesamt für Sicherheit in der Informationstechnik.
BTC	Business Technology Consulting.
Cloud	Kurzform für Cloud Computing; Nutzung von IT-Infrastrukturen und Dienstleistungen, die sich nicht auf einem lokalen Rechner, sondern von einem virtuellen Rechenzentrum bereitgestellt wird. Das virtuelle Rechenzentrum besteht aus mehreren

	zusammengeschalteten Computern.
Data Loss Prävention (DLP)	Eine Reihe von Tools und Prozessen mit der sichergestellt wird, das vertrauliche Daten nicht durch unautorisierte Personen verloren gehen.
DEP	Device Enrollment Program – Automatische Registrierung, Konfiguration sowie Überwachung von Apple Endgeräten während des MDM-Setups.
Domäne	Teilbereich aus einem DNS.
E3	Microsoft 365 Enterprise 3 Lizenz (umfasst Windows 10 Enterprise E3, Office 365 E3 sowie Mobility + Security E3).
EAS	Exchange Active Sync; Protokoll welches das Synchronisieren von E-Mails, Kontakte, Kalendereinträge, Aufgaben etc. von einem Nachrichten Server mit einem mobilen Endgerät ermöglicht.
EMM	Enterprise Mobile Management – umfasst MDM+MAM+MIM.
Exchange	E-Mail Server aus dem Hause Microsoft.
Face-ID	Gesichtserkennungstechnologie welche bei Apple zum Einsatz kommt.
Fingerprint (Touch-ID)	Finderabdruckscanner welcher bei Apple bis zum iPhone X zum Einsatz kommt.
Full-Wipe	Komplette Formatierung eines mobilen Endgerätes.
HyperCare-Phase	Zusätzliche und intensive Unterstützung nach dem Produktivstart.
iOS	von Apple entwickeltes Betriebssystem
iPadOS	Betriebssystem für iPads aus dem Hause Apple.
Jailbreak	Jailbreak bezeichnet das nicht autorisierte deaktivieren oder entfernen der Nutzungsbeschränkungen.
Konformitätsrichtlinien	Richtlinie, die ein Endgerät erfüllen muss, um Unternehmenszugang zu erhalten.
Lizenz	Lizenznehmer erhält Berechtigung zur Nutzung einer Software oder einem Dienst.
macOS	Betriebssystem von Apple für Notebooks und Macs.
MAM	Mobile Application Management – Administration der Anwendungen auf einem Gerät.
MDM	Mobile Device Management – Verwaltung mobiler Endgeräte.
MDM-Push-Zertifikat	Zertifikat welches die sichere Kommunikation zwischen dem Kommunikationsserver und den Apple APNS Servern sicherstellt.
Microsoft Active Directory (AD)	Microsoft Active Directory (nachfolgend AD genannt) ist ein zentraler Verzeichnisdienst. Im Grunde ist das Active Directory nur eine Datenbank, in der die Ressourcen innerhalb eines Netzwerkes gespeichert sind. Ressourcen sind z.B. Benutzer, Computer, Gruppen, Drucker etc.
Microsoft Endpoint Manager	System Center Configuration + Microsoft Intune.

Microsoft Teams	Bei MS-Teams handelt es sich um eine Plattform die Chats, Besprechungen, Notizen und Anhänge kombiniert. MS-Teams ist ein zentraler Ort für Teamarbeit, dass von Microsoft vertrieben wird.
MIM	Mobile Information Management – Verwaltung des Datenflusses
MobileIron App-Connect	Containerisiert Apps, um gespeicherte App-Daten zu schützen.
Netscaler	Application Delivery Controller aus dem Hause Citrix. Der Citrix Netscaler bietet ebenfalls Funktionen wie SSL-VPN, Load-Balancing und Firewall.
Nutzwertanalyse	Analysemethode; Methodik die die Entscheidungsfindung rational unterstützen soll.
On-Premises	auch mit On-Prem abgekürzt, beschreibt ein Lizenzmodell, bei dem die Software lokal auf einem Server betrieben wird.
Organisationseinheiten	Containerobjekt; Benutzer, Gruppen, Computer können in einem logischen Container hinzugefügt werden.
Organisations-ID	Eindeutige Identifikationsnummer welche die Zuordnung zu einem ABM gewährleistet.
PKCS	PKCS ist eine Ansammlung von Standards für die asymmetrische Kryptographie.
RDP	Remote Desktop Protocol; Netzwerkprotokoll für Fernzugriff auf einem anderen Computersystem (Windows) aus dem Hause Microsoft.
Security-Compliance	Beschreibt die Einhaltung der gesetzlichen, internen und vertraglichen IT Regelungen.
SQL	Structured Query Language; Datenbanksprache für relationale Datenbanken.
Synchronisation	Zeitgleiche Abgleichen von Daten.
Team MDM	Agile Projekte – Team Mobility.
Tenant	Speicherplatz in einem der Microsoft Rechenzentren.
Threat-Defense	Dient zum Schutz und zur Erkennung von Bedrohungen auf dem Endgerät. Aktuelle MTD Lösungen benutzen mittlerweile die KI (Künstliche Intelligenz) Technologie.
Token	Folge von zusammengehörigen Zeichen von Bits.
UPN	User Principal Name – Alias für den Benutzernamen.
VIP	Very Important Person.
VPN	Virtuelles privates Netzwerk; VPN stellt eine gesicherte Verbindung zwischen zwei oder mehreren Kommunikationspartnern über eine potenziell gefährdete Internetverbindung dar.
VPP	Volume Purchase Program.
Windows	Betriebssystem aus dem Hause Microsoft.
WLAN	Wireless Local Area Network; Lokales Funknetzwerk.
„.p7m“-Datei	Verschlüsselte und signiertes Push-Zertifikat.
„.pem“-Datei	Format für die Speicherung von Zertifikaten.

Tabelle 6: Glossar

8.2 Soll-Zustand (Gantt-Diagramm)

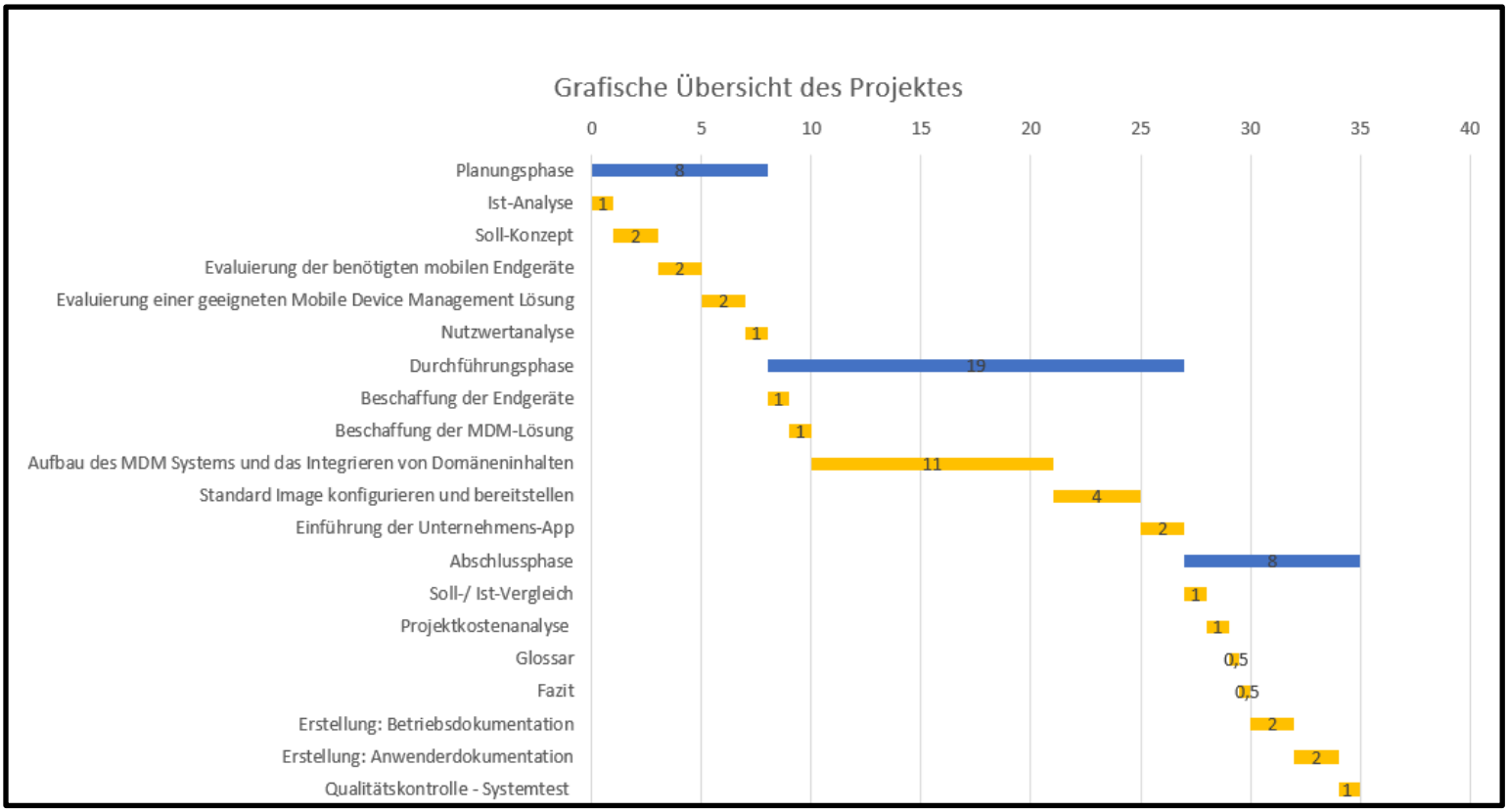


Abbildung 4: Soll-Zustand Gantt-Diagramm

8.3 Detaillierter Zeitplan

	Dauer (geplant) gesamt in h	Dauer in h	Abweichungen in h
1. Planungsphase	8	11	+3
Ist-Analyse	1	1	
Termin: Soll-Konzeption	2	2	
Evaluierung der Endgeräte	2	3	+1
Evaluierung der EMM-Lösung	2	3	+1
Erstellung: Nutzwertanalyse	1	1	
Rollout-Struktur	0	0,5	+0,5
Betrachtung der Privatnutzung	0	0,5	+0,5
2. Durchführungsphase	19	18	-1
Erstellung eines Azure Mandanten	1	0	-1
Termin: Abstimmung AD Attribute für Azure Active Directory Connect	1	1	

Azure AD-Connect: Installation, Konfiguration	3	3	
Microsoft E3 Lizenz – Überprüfung	0,5	0,5	
Erstellung: Azure Gruppe + Zuweisung der E3 Lizenz	0,5	0,5	
Einrichtung: Apple Business Manager	1	0	-1
Einrichtung: Apple Push Notification Service (APNs) - Erstellung: Apple MDM-Push-Zertifikat	2	2	
Anlegen eines MDM Server im ABM	1	2	+1
VPP – Volume Purchase Program	1	2	+1
DEP – Device Enrollment Program	2	1,5	-0,5
Termin: Abstimmung der Konformitätsrichtlinien / Geräterichtlinien	1	1,5	+0,5
Einrichtung & Zuweisung: Konformitätsrichtlinien / Geräterichtlinien	3	1,5	-1,5
Termin: Abstimmung der Unternehmens-App	1	1	
Erstellung: APP-Schutzrichtlinien	1	1,5	+0.5
3. Abschluss und Abnahme	8	6	-2
Soll- / Ist-Vergleich	1	1	
Projektkostenanalyse	1	0,5	-0,5
Fazit	0,5	0,5	
Glossar	0,5	0,5	
Erstellung: Betriebshandbuch	2	1,5	-0,5
Erstellung: Anwenderdokumentation	2	1	-1
Qualitätskontrolle - Systemtest	1	1	

Tabelle 7: Detaillierter Zeitplan

8.4 Vergleich der Endgeräte

Merkmale	Apple iPhone XR	Apple iPhone 11	Apple iPhone 11 Pro	Apple iPhone 11 Pro Max
Betriebssystem	iOS	iOS	iOS	iOS
Displaygröße	6,1“	6,1“	5,8“	6,5“
Display	Liquid Retina HD Display	Liquid Retina HD Display	Super Retina XDR Display	Super Retina XDR Display
Auflösung	1792 x 828 Pixel bei 326ppi	1792 x 828 Pixel bei 326ppi	2436 x 1125 Pixel bei 458ppi	2688 x 1242 Pixel bei 458 ppi
Kontrastverhältnis	1400:1	1400:1	2.000.000:1	2.000.000:1
Prozessor	A12 Bionic Chip 2.Gen	A13 Bionic Chip 3.Gen	A13 Bionic Chip 3.Gen	A13 Bionic Chip 3.Gen
Typische max. Helligkeit	625 Nits	625 Nits	800 Nits	800 Nits
Kamera (Back)	12 Megapixel mit Weitwinkelobjektiv	12 Megapixel Zweifach-Kamera mit Ultraweitwinkel und Weitwinkelobjektiv sowie Nachtmodus	12 Megapixel Dreifach-Kamera mit Ultraweitwinkel und Weitwinkelobjektiv sowie Nachtmodus und Teleobjektiv	12 Megapixel Dreifach-Kamera mit Ultraweitwinkel und Weitwinkelobjektiv sowie Nachtmodus und Teleobjektiv
Kamera (Front)	7 Megapixel 1080p – 60fps	12 Megapixel Kamera mit 4K Videoaufnahme – bis zu 60fps	12 Megapixel mit 4K Videoaufnahme – bis zu 60fps	12 Megapixel mit 4K Videoaufnahme – bis zu 60fps
Speicherkapazitäten	64GB, 128GB	64GB, 128GB, 256GB	64GB, 256GB, 512GB	64GB, 256GB, 512GB
Akku Kapazität	2.942 mAh	3.110 mAh	3.174 mAh	3.969 mAh
Patchzyklus	4 Jahre	5 Jahre	5 Jahre	5 Jahre

Tabelle 8: Vergleich - Endgeräte

8.5 Nutzwertanalyse für mobile Endgeräte

		Apple iPhone XR		Apple iPhone 11		Apple iPhone 11 Pro		Apple iPhone 11 Pro Max	
Kriterium	**Gewichtung**	**Wertung**	**Gesamt**	**Wertung**	**Gesamt**	**Wertung**	**Gesamt**	**Wertung**	**Gesamt**
Haptik	5%	4	20	4	20	5	25	3	15
Patchzyklus	20%	4	80	5	100	5	100	5	100
Display	5%	4	20	4	20	5	25	5	25
Displaygröße	10%	5	50	5	75	5	50	3	30
Akku Kapazität	10%	3	30	4	60	5	50	5	50
Speicherkapazität	5%	5	25	5	25	5	25	5	25
Performance (Prozessor)	10%	4	40	5	75	5	50	5	50
Erfahrung	10%	4	40	4	60	4	40	4	40
Design	5%	5	25	5	25	5	25	5	25
Wirtschaftlichkeit (P/L)	20%	4	80	5	100	4	80	4	80
Gesamt	**100%**		**410**		**560**		**470**		**440**

Tabelle 9: Nutzwertanalyse - Endgeräte

8.6 Vergleich der EMM-Lösungen

Eigenschaften	Citrix XenMobile	Mobile Iron	VMWare Air Watch	Microsoft Azure Intune
Attachment Control (E-Mail)	-	+	-	-
Richtlinienkonfiguration	+	+	+	+
Device Management	+	+	+	+
Monitoring	+	+	+	+
Full-Wipe	+	+	+	+
Beschränkung (App)	+	+	+	+
Beschränkung (Endgerät – Nutzung)	+	+	+	+
Applikationsliste (Übersicht)	+	+	+	+
Phone Management (Ortung)	+	+	+	-
Phone Management (Factory Reset)	+	+	+	+
Verschlüsselung der Daten (Datenintegrität)	+	+	+	+
Self-Service	+	+	+	+

Tabelle 10: Vergleich - EMM

8.7 Gartner Magic Quadrant

Abbildung 5: Magic Quadrant - EMM

8.8 Detaillierte Kostenanalyse – Lizenzkosten (1 Jahr)

Citrix XenMobile

	Art	Menge	Monatskosten €	Jahreskosten €
Lizenzkosten (pro User)	Lizenz 🕮	200	748,00	8.976,00
Wartungskosten (1-Jahr)	Lizenz	200	209,71	2.516,52
Anschaffungskosten	Server	3	6.250	75.000,00
Betriebskosten	Betrieb	10%	720,77	8.649,25
Gesamtkosten			7.928,48	95.141,77

Tabelle 11: Citrix XenMobile Jahreskosten

MobileIron

	Art	Menge	Monatskosten €	Jahreskosten €
Lizenzkosten (pro User)	Lizenz	200	1.661,67	19.940,00
Wartungskosten (1-Jahr)	Lizenz	200	176,67	2.120,00
Anschaffungskosten	Server	3	6.250	75.000
Betriebskosten	Betrieb	10%	808,83	9.706,00
Gesamtkosten			8.088,34	106.766,00

Tabelle 12: MobileIron Jahreskosten

VMWare Air-Watch

	Art	Menge	Monatskosten €	Jahreskosten €
Lizenzkosten	Lizenz	200	2.806	33.672
Wartungskosten (1-Jahr)	Lizenz	200	0	0
Anschaffungskosten	⊗	⊗	⊗	⊗
Betriebskosten	Betrieb		⊗	⊗
Gesamtkosten			2.806	33.672

Tabelle 13: VMWare Air-Watch Jahreskosten

Microsoft Office 365 E3 (inkl. Intune)

	Art	Menge	Monatskosten €	Jahreskosten €
Lizenzkosten (per User)	Lizenz	200	6.300	75.600
Wartungskosten	Lizenz	200	0	0
Anschaffungskosten	⊗	⊗	⊗	⊗
Betriebskosten	Betrieb	⊗	⊗	⊗
Gesamtkosten			6.300	75.600

Tabelle 14: Microsoft Office 365 E3 Jahreskosten

Microsoft Azure Intune

	Art	Menge	Monatskosten €	Jahreskosten €
Lizenzkosten (pro User)	Lizenz	200	886	10.632
Wartungskosten	Lizenz	200	0	0
Anschaffungskosten	⊗	⊗	⊗	⊗
Betriebskosten	Betrieb		⊗	⊗
Gesamtkosten			886	10.632

Tabelle 15: Microsoft Intune Jahreskosten

8.9 Nutzwertanalyse für EMM-Lösung

		Citrix XenMobile		Mobile Iron		VMWare Air Watch		Microsoft Azure Intune	
Kriterium	**Gewichtung**	**Wertung**	**Gesamt**	**Wertung**	**Gesamt**	**Wertung**	**Gesamt**	**Wertung**	**Gesamt**
Kompatibilität	5%	5	25	5	25	5	25	5	25
Anwenderfreundlichkeit / Bedienbarkeit	10%	5	50	4	40	5	50	5	50
Device Management	25%	4	100	4	100	5	125	4	100
Monitoring	10%	5	50	5	50	5	50	5	50
Support	15%	4	60	4	60	4	60	5	65
Ressourcenbedarf	10%	4	40	4	40	5	50	5	50
Wirtschaftlichkeit (P/L)	25%	3	75	3	75	4	100	5	125
Gesamt	**100%**		**400**		**390**		**460**		**465**

Tabelle 16: Nutzwertanalyse - EMM

8.10 Rollout-Struktur

	BYOD	COBO	COPE
Wem gehört das Gerät?	Mitarbeiter	Unternehmen	Unternehmen
Wie kommt das Gerät ins Management	Mitarbeiter führt Enrollment selbst durch.	Per Device Enrollment Programm werden Geräte als Unternehmensgerät beschafft und ausgerollt.	Per Device Enrollment Programm werden Geräte als Unternehmensgerät beschafft und ausgerollt.
Ist Private Nutzung erlaubt?	Ja	Nein	Ja
Wer übernimmt Geräte-Support?	Fürsorgepflicht liegt beim Mitarbeiter. Unternehmen unterstützt bei Unternehmens-Apps.	Unternehmen	Unternehmen verwaltet das Gerät. Mitarbeiter hat Fürsorgepflicht für private Apps und Daten.
Was passiert beim Geräteverlust?	Nur der Unternehmensbereich kann gelöscht werden (partieller Wipe).	Gerät wird vollständig auf Werkseinstellungen zurückgesetzt.	Gerät wird vollständig auf Werkseinstellungen zurückgesetzt. Dabei gehen auch private Daten, die nicht gesichert sind, verloren.
Gibt es eine Apple-ID auf dem Gerät?	Ja – private Apple-ID.	Nein	Optional – private Apple-ID.
Gibt es einen AppStore auf dem Gerät?	Ja –private Apple-ID.	Nein	Optional – private Apple-ID.
Dürfen zusätzliche, private Accounts aufs Gerät gelangen?	Ja, da nicht Teil des Managements.	Nein	Im Ermessen des Unternehmens.
Wie gelangen Applikationen auf das Gerät?	MDM Client muss durch eine Apple-ID (privat) heruntergeladen werden. Alle Unternehmens-Applikationen werden per VPP verteilt.	Keine Apple-ID und kein AppStore auf dem Gerät. Alle Applikationen werden per Volume Purchase Program verteilt.	Alle Unternehmens-Applikationen werden per Volume Purchase Program verteilt. Private Applikationen werden durch private Apple-ID verwaltet.
Wie wird Datensicherheit gewährleistet	2 Bereiche auf dem Gerät, ein überwachter Unternehmensbereich und ein freier Privatbereich.	Gesamtes Gerät wird verwaltet, es gibt keine privaten Daten.	Gesamtes Gerät wird verwaltet, private Daten werden durch MDM von Unternehmensdaten getrennt gehalten.

Tabelle 17: Rollout-Struktur

8.11 Abstimmung der Benutzerrichtlinien

Einstellung	Beschreibung	Intune Standard	Empfehlung	Kunde
Gerätefunktionen				
AirPrint				
AirPrint	Stellt die Verbindung zu AirPrint kompatiblen Druckern im Netzwerk her. Benötigt wird hierbei die IP-Adresse und der Ressourcenpfad des Druckers.	-	-	-
Layout der Startseite				
Andocken	Definiert die Applikationen, die im iOS Dock am unteren Bildschirmrand zu sehen sein sollen	-	-	-
Seiten	Definiert die Reihenfolge, in der die Apps auf dem Startbildschirm und allen weiteren Seiten angeordnet werden.	-	Wird nichts eingestellt, wird standardmäßig die zweite Seite befüllt.	-
App Benachrichtigung				
App Benachrichtigungen	Erlaubt das Management der Push-Notifications für einzelne Applikationen.	-	App Notifications sollten wenn dann direkt über die Applikation gesteuert werden.	-
Nachrichten auf Sperrbildschirm				
Nachricht "Bei Verlust zurück an.."	Definiert die Nachricht, die im Verlustfall (Lost-Mode) angezeigt werden soll	-	Ergänzung der Message um den Firmennamen.	
Kennzeicheninformation	Inventarnummer, die im Sperrbild bei Verlustfall (Lost-Mode) angezeigt wird.	-	Hier kann mit Variablen gearbeitet werden, z.B. [Username].	-
Einmaliges Anmelden				
Benutzernamenattribut aus AAD	Welches AD-Attribut soll zur Anmeldung verwendet werden.	-	-	-
Bereich	Domänenbereich zur Kerberos-Anmeldung	-	-	-
URL; einmaliges Anmelden	Definiert die URLs, für die SSO verwendet werden soll.	-	-	-
Apps; einmaliges Anmelden	Definiert die Apps anhand Bundle-ID, die SSO verwenden dürfen.	-	-	-
Webinhaltsfilter				
Filtertyp	Wahl zwischen URL Blacklist/Whitelist oder Webseiten-Angabe.	-	-	-
Hintergrundbild				
Hintergrundbild	Bild im Start/Sperrbildschirm/beiden anzeigen	-	Falls ein Firmenwallpaper vorhanden ist, kann dieses eingbunden werden. Bei Bedarf kann ein Wallpaper erstellt werden.	Wallpaper, welches identisch zum Client ist, soll beim Start ausgerollt werden. Der User darf

Abbildung 6:Richtlinien - Gerätefunktionen

Einstellung	Beschreibung	Intune Stand	Empfehlu	Kund
Geräteeinschränkung				
Allgemein				
Nutzungsdaten freigeben	Nutzungsinformationen zu Apple übermitteln	ON	OFF	OFF
Bildschirmaufnahme		ON	ON	ON
Nicht vertrauenswürdiges TLS-Zertifikat		ON	OFF	OFF
Drahtlose PKI-Updates blockieren		OFF	ON	ON
Anzeigennachverfolgung	Deaktiviert die Geräteanzeigen-ID	OFF	ON	ON
Änderung der Einstellungen zur Diagnoseübermittlung	Einstellungen für Diagnosedaten zu Apple ändern	ON	OFF	OFF
Beobachtung von Remotebildschirmen durch Classroom-App	Beobachtung von Remotebildschirmen durch die Classroom-App	ON	OFF	OFF
Unangekündigte Bildschirmüberwachung durch Classroom-App	Unangekündigte Beobachtung von Remotebildschirmen durch die Classroom-App	OFF	OFF	OFF
App-Sicherheit	Installation von Drittanbieterapps ermöglichen	ON	OFF	OFF
Kontoänderung		ON	OFF	ON
Bildschirmzeit		ON	ON	ON
Verwendung der Option zum Löschen aller Inhalte und Einstellung		ON	ON	ON
Bearbeitung des Gerätenamens		ON	OFF	OFF
Bearbeitung der Benachrichtigungseinstellungen		ON	ON	ON
Hintergrundbild ändern		ON	Wenn ein Wallpaper	ON
Konfigurationsprofiländerungen	Änderungen am MDM Profil durch Nutzer	ON	ON	OFF
Aktivierungssperre	Erschwert die erneute Aktivierung verlorener oder gestohlener Geräte	OFF	OFF	OFF
Entfernen von Appls blockieren	Benutzer darf Apps nicht mehr deinstallieren	OFF	OFF	OFF
USB-Zubehör bei gesperrtem Gerät zulassen	USB nur auf vertrauten Geräten erlauben	OFF	Falls es dem	OFF
Automatische Datums- und Uhrzeiteinstellung erzwingen		OFF	OFF	OFF
Erlaubnis für Kursteilnehmer vor dem Verlassen des Classrooms erforderlich		OFF	OFF	OFF
Das Beschränken von Classroom auf eine App und das Sperren von Geräten		OFF	OFF	OFF
VPN-Erstellung blockieren		OFF	OFF	OFF
eSIM-Einstellungen ändern		ON	Ist die	ON
Softwareupdates zurückstellen		OFF	ON	OFF
Sichtbarkeit von Softwareupdates verzögern		-	Empfehlung von 30	0
Kennwort				
Kennwort		OFF	ON	ON
Einfache Kennwörter blockieren		OFF	ON	ON
Erforderlicher Kennworttyp	Numerisch/Alphanumerisch	Gerätestandard	Numerisch	Numerisch
Kennwortlänge (Minimum)		4	6	6
Anzahl von Anmeldefehlern, bevor das Gerät zurückgesetzt wird		4	10	10
Maximaler Zeitraum der Bildschirmsperre (Minuten) bis zur Kennwortanforderung		Not configured	0	0
Maximaler Zeitraum der Inaktivität (Minuten) bis zur Bildschirmsperrung		Not configured	10	2
Kennwortablauf (Tage)		41	Der	0
Wiederverwendung vorheriger Kennwörter verhindern		-	Beim Anwender	6
Touch-ID (Fingerprint)		ON	ON	ON
Passcodeänderung		ON	ON	ON
Touch-ID Änderung		ON	ON	ON
AutoAusfüllen für Kennwörter blockieren		OFF	OFF	OFF
Kennwortfreigabe blockieren		OFF	OFF	OFF
Authentifizierung über Touch-ID oder Face-ID für AutoAusfüllen		OFF	ON	ON
Gesperrter Bildschirm				
Kontrollcenterzugriff bei gesperrtem Gerät		ON	ON	ON
Zugriff auf Mitteilungszentrale bei gesperrtem Gerät		ON	ON	ON

Abbildung 7: Richtlinien - Geräteeinschränkungen

Apps anzeigen oder ausblenden				
Type of apps list	Hidden/Visible list of Apps	Not configured	Hidden Apps	Hidden A
App list	,com.apple.AppStore,App Store,			
	,com.apple.Music,Music,			
	,com.apple.MobileStore,iTunes Store,			
	,com.apple.iBooks,Books,			
	,com.apple.store.Jolly,Apple Store,			
	,com.apple.mobilegarageband,GarageBand,			
	,com.apple.Bridge,Watch,			
	,com.apple.tv,TV,			
	,com.apple.stocks,Stocks,			
	,com.apple.itunesu,iTunes U,			
	,com.apple.Keynote,Keynote,			
	,com.apple.Home,Home,			
	,com.apple.podcasts,Podcasts,			
Drahtlosnetzwerke				
Datenroaming		ON	ON	ON
Globales Abrufen im Hintergrund beim Roaming		ON	ON	ON
Sprachwahlverfahren		ON	ON	ON
Sprachroaming		ON	ON	ON
Privater Hotspot		ON	OFF	ON
Verbundene Geräte				
Handgelenkerkennung für gekoppelte Apple Watch		ON	ON	ON
Kopplungskennwort für ausgehende AirPlay-Anforderungen anfordern		OFF	ON	ON
AirDrop		ON	ON	ON
Apple Watch-Kopplung		ON	ON	ON
Bluetooth-Änderung		ON	ON	ON
Hostkopplung zum Steuern der Geräte, mit denen ein iOS-Gerät gekoppelt werden kann		ON	OFF	ON
AirPrint blockieren		OFF	OFF	OFF
Speicherung von AirPrint-Anmeldeinformationen im Schlüsselbund blockieren		OFF	OFF	OFF
Vertrauenswürdiges TLS-Zertifikat für AirPrint erforderlich		OFF	OFF	OFF
iBeacon-Ermittlung durch AirPrint-Drucker blockieren		OFF	ON	ON
Einrichten neuer Geräte in der Nähe blockieren		OFF	ON	ON
Zugriff auf Dateien in USB-Laufwerk		ON	OFF	OFF
Tastatur und Wörterbuch				
Suche nach Wortdefinition		ON	ON	ON
Tastaturwortvorschläge		ON	ON	ON
Autokorrektur		ON	ON	ON
Rechtschreibprüfung über Tastatur		ON	ON	ON
Tastenkombinationen		ON	ON	ON
Diktat		ON	ON	ON
QuickPath		ON	ON	ON
Cloud und Speicher				
Verschlüsselte Sicherung		OFF	OFF	OFF
Synchronisierung verwalteter Apps mit der Cloud		ON	OFF	OFF
Enterprise Book-Sicherung blockieren		ON	OFF	OFF
Synchronisierung von Enterprise Book-Metadaten blockieren (Notizen und Highlights)		ON	OFF	OFF
Synchronisierung von Fotostreams in iCloud		ON	OFF	OFF
iCloud-Fotomediathek		ON	OFF	OFF
Streaming freigegebener Fotos		ON	OFF	OFF
Handoff		ON	OFF	OFF
In iCloud sichern		ON	OFF	OFF
iCloud-Dokumentsynchronisierung blockieren		ON	OFF	OFF
Synchronisierung zwischen iCloud und Keychain blockieren		ON	OFF	OFF

Abbildung 8: Richtlinien - Geräteeinschränkungen_II

Autonomer Einzelanwendungsmodus				
App List	Liste der Apps die Geräte in KIOSK Modus versetzen können		OFF	OFF
Kiosk				
App zur Ausführung im Kioskmodus	Store App, Verwaltete App, Integrierte App	Nicht konfiguriert	OFF	OFF
Touch-Unterstützung		OFF	OFF	OFF
Farben umkehren		OFF	OFF	OFF
Mono-Audio		OFF	OFF	OFF
VoiceOver		OFF	OFF	OFF
Zoom		OFF	OFF	OFF
Automatische Sperre		OFF	OFF	OFF
Ruftonschalter		OFF	OFF	OFF
Automatische Ausrichtung		OFF	OFF	OFF
Standbytaste		OFF	OFF	OFF
Touch		ON	OFF	OFF
Lautstärkeregler		OFF	OFF	OFF
AssistiveTouch - Steuerung		OFF	OFF	OFF
Steuerelement zum Umkehren von Farben		OFF	OFF	OFF
Ausgewählten Text sprechen		OFF	OFF	OFF
VoiceOver Steuerelement		OFF	OFF	OFF
Zoomsteuerelement		OFF	OFF	OFF

Abbildung 9: Richtlinien - Geräteeinschränkungen_III

8.12 Abstimmung der Unternehmens-Apps

Unternehmens-App	Vorauswahl	Abstimmung mit dem Kunden
LikedIn: Business-Netzwerk	x	
Yammer	x	
XING - Ihr berufliches Netzwerk	x	
Lufthansa	x	x
Monal - XMPP chat		
HRS Hotel Suche - Top Hotels		
DB Navigator	x	
Keynote		
Numbers		
Pages		
TimeboxApp		x
Booking.com: Hotel Angebote		x
mehr-tanken		
MeinVodafone	x	x
MeinMagenta		
Microsoft OneNote		
Skyscanner - günstig reisen		
DB Navigator für iPad		
Citrix Secure Hub		
RegenRadar		
Adobe Acrobat Reader für PDF		
FahrPlaner		
Ryanair		
Mobile Authenticator ES.	x	x
ALE OpenTouch Conversation for iPad		
Google Maps - Transit & Essen		
Microsoft Word	x	x
Microsoft PowerPoint	x	
Microsoft Excel	x	
OpenVPN Connect		
Skype for Business	x	x
Slack		
Yahoo Wetter		
ADAC Pannenhilfe	x	x
CamCard -Business Card Scanner		x
CamScanner: PDF Scanner		x
Cisco Webex Meetings		x
Citrix SSO		x
Das Telefonbuch: mobile Guide	x	x
DB Streckenagent		x
DKV		x
Doodle: Termine finden	x	x
energate		x
MOIA in Hamburg & Hannover		x

Tabelle 18: Unternehmens-Apps - 1

Unternehmens-App	Vorauswahl	Abstimmung mit dem Kunden
OpenTouch Conversation		
F24 Alert!		x
Azure Information Protection		
Intune-Unternehmensportal	x	x
Teamwire		
Mobility foor Jira - Team		
Post-it		
Microsoft Power BI		
Intune Managed Browser		
Kaspersky QR Scanner		
NINA		x
Citrix VPN		
Microsoft Outlook		
Microsoft Office Lens|PDF Scan		x
Microsoft Authenticator		x
Power Apps		
Adobe Acrobat Reader Intune		
Eurowings		
Power Automate		
Microsoft Teams		
Notate for Microsoft Intune		
Microsoft Vidio Viewer		
MAGI		
Microsoft To Do	x	
Microsoft Planner	x	
OpenTouch Conversation Plus		
ELO 11 for Mobilde Devices		
Workforcemanagement		
FREE NOW (mytaxi)		x
Garmin Smartphone Link		x
Google Authenticator	x	x
Google Chrome	x	x
GoToMeeting		x
GVH		x
KATWARN		x
LEO Wörterbuch	x	x
NormenBibliothek		x
Scout GPS Navigation & Karten		x
ScrumCards		x
TripSource		x
WarnWetter		x
Zeno Connect		x
smARt Haufe		x
Tagesschau	x	x

Tabelle 19: Unternehmens-Apps - 2

Anwenderdokumentation:

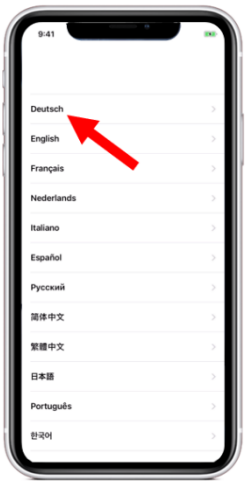
Grundeinrichtung eines iPhones mit Microsoft Intune

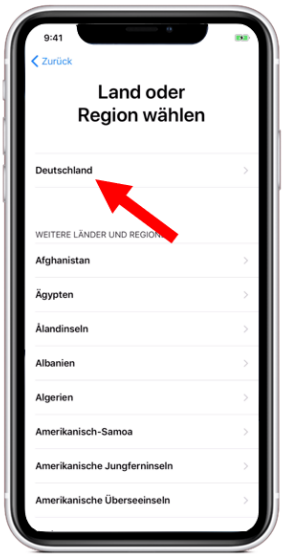
1.

Nach dem Einschalten Ihres iPhones, werden Sie aufgefordert, die PIN Ihrer SIM-Karte einzugeben. Geben Sie dort bitte die PIN Ihrer SIM-Karte ein. Sollten Sie keine SIM-Karte eingelegt haben, können Sie diesen Schritt ignorieren.

2.

Wählen Sie hier Ihre Sprache aus. Wir empfehlen „Deutsch“.



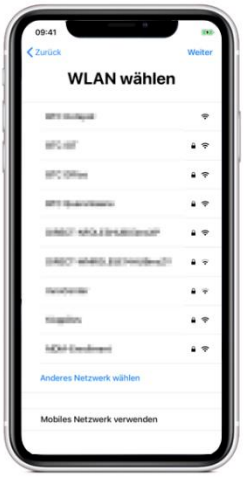


3.

Wählen Sie „Deutschland“ als Land aus.

4.

Wählen Sie „Manuell konfigurieren“ zum Fortfahren.



5.

Wir empfehlen Ihnen die Inbetriebnahme mit dem Mobilfunk-Netzwerk durchzuführen. Alternativ wählen Sie bitte eine WLAN Verbindung aus und geben Sie den dazugehörigen Schlüssel ein.

6.

Nun wird Ihr iPhone bei Apple registriert. Es handelt sich bei diesem iPhone um ein Unternehmensgerät, daher wird nun die Konfiguration abgerufen.

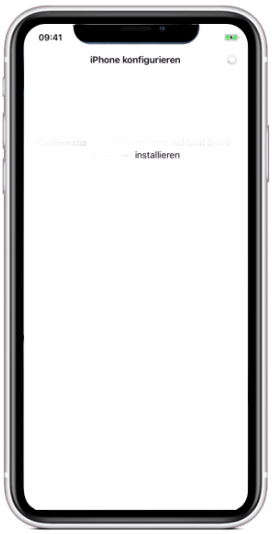
7.

Ihr Gerät wurde bei Apple registriert. Nun erhalten Sie unter Punkt 1 weitere Informationen über die Entfernte Verwaltung.

Anschließend tippen Sie auf „Weiter".

8.

Die Konfiguration für Ihr iPhone wird abgerufen.



9.

Sie haben nun die Möglichkeit Face ID einzurichten. Face ID ermöglicht es Ihnen, ihr Endgerät mit Ihrem Gesicht zu entsperren.

10.

Unabhängig davon ob Sie Face ID nutzen wollen oder nicht, müssen Sie ein 6-stelligen Code hinterlegen.

11.

In diesem Schritt werden Sie aufgefordert, die Ortungsdienste zu aktivieren oder zu deaktivieren. Aktivieren Sie bitte die Ortungsdienste.

12.

Anschließend haben Sie die Möglichkeit, einen Anzeigezoom zu konfigurieren.

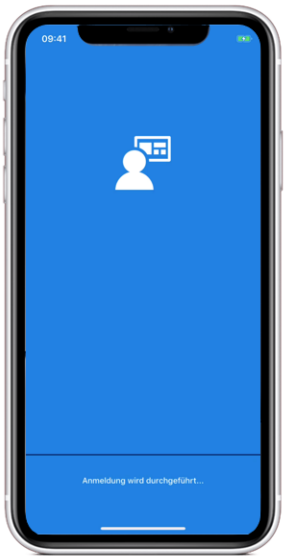
Wählen Sie hier zwischen den beiden Optionen, eine Option aus.

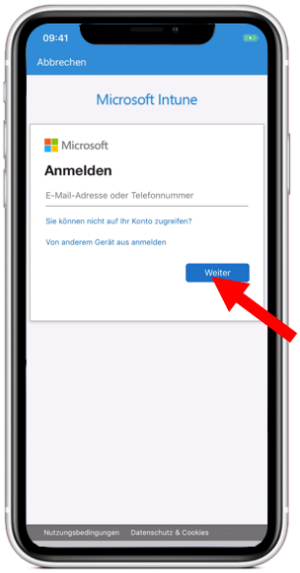
13.

Die Einrichtung Ihres iPhones ist abgeschlossen. Wischen Sie nun von unten nach oben.

14.

Nachdem Ihr iPhone eingerichtet ist, installiert sich die Applikation „Unternehmensportal“ automatisch. Warten Sie einen Moment und rufen Sie anschließend die App auf.



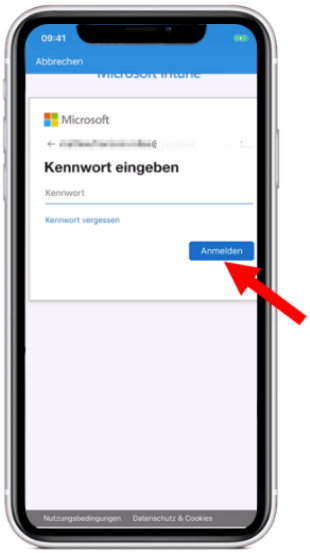


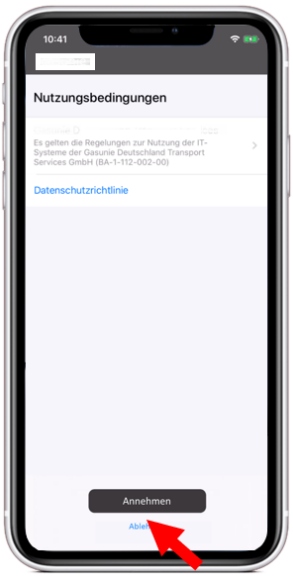
15.

Geben Sie nun Ihre betriebliche E-Mail-Adresse ein und bestätigen Sie mit „Weiter“.

16.

Geben Sie anschließend Ihr Kennwort ein und bestätigen Sie mit „Anmelden“.



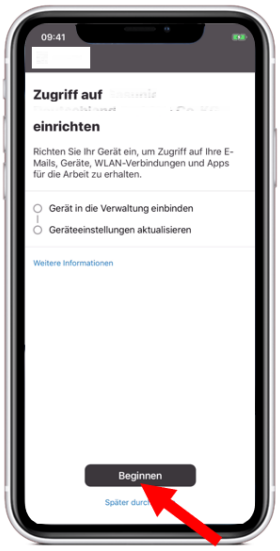


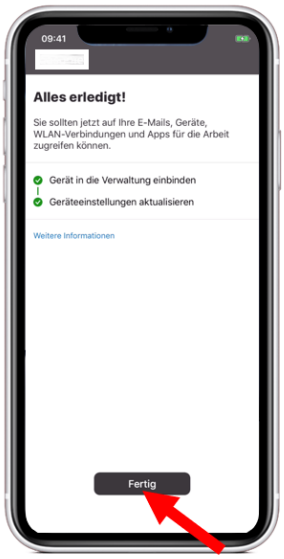
17.

Nun erhalten Sie die Nutzungsbedingungen. Lese Sie sich diese durch und Bestätigen Sie diese mit „Annehmen“.

18.

In diesem Schritt wird ihr iPhone in Microsoft Intune eingebunden. Wählen Sie dazu „Beginnen“.



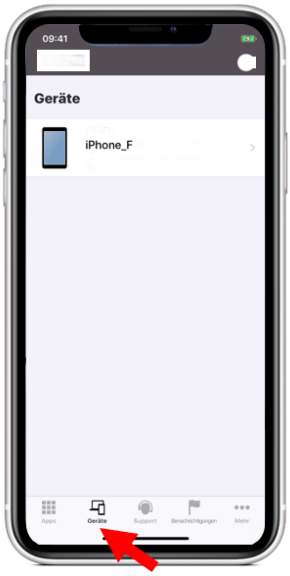


19.

Wenn die Einbindung erfolgreich war, erhalten Sie die folgende Übersicht mit dem Titel „Alles erledigt!“. Sollte die Einbindung in die Geräteverwaltung nicht funktioniert haben, wenden Sie sich bitte an Ihren Vorgesetzten.

20.

Im Reiter „Geräte“ können Sie sich nun die Informationen über Ihr Gerät anzeigen lassen.



Betriebsdokumentation

Ansprechpartner:

Projektverantwortlicher:	Martin Goltschewski
Team Windows Support:	XXXXXXX XXXXXXX
Team Agile Projekte Mobility:	XXXXXXX XXXXXXX
Einkauf:	XXXXXXX

Änderungshistorie:

Version	Abschnitt	Änderung	Autor / Bearbeiter	Datum
0.1	alle	Erstellung der Betriebsdokumentation	Martin Goltschewski	XXXXXXX

In den folgenden Seiten möchte ich näher auf den Ist-Zustand und die Administration eingehen.

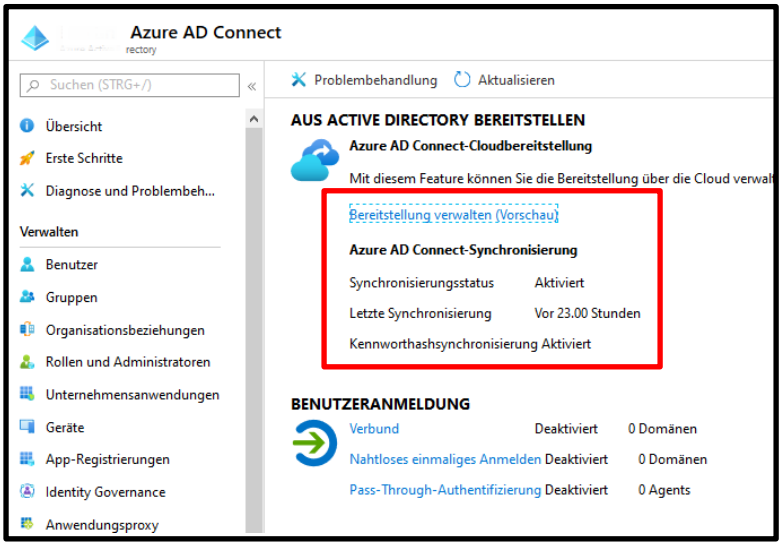
OnPremises Server Anmeldeinformation:

Hostname:	GUXXXXXX
Benutzer:	xxxxxxxx
Kennwort:	xxxxxxxxxx

Azure Portal Zugang:

Benutzer (E-Mail-Adresse):	xxxxxxxx
Kennwort:	xxxxxxxxxx

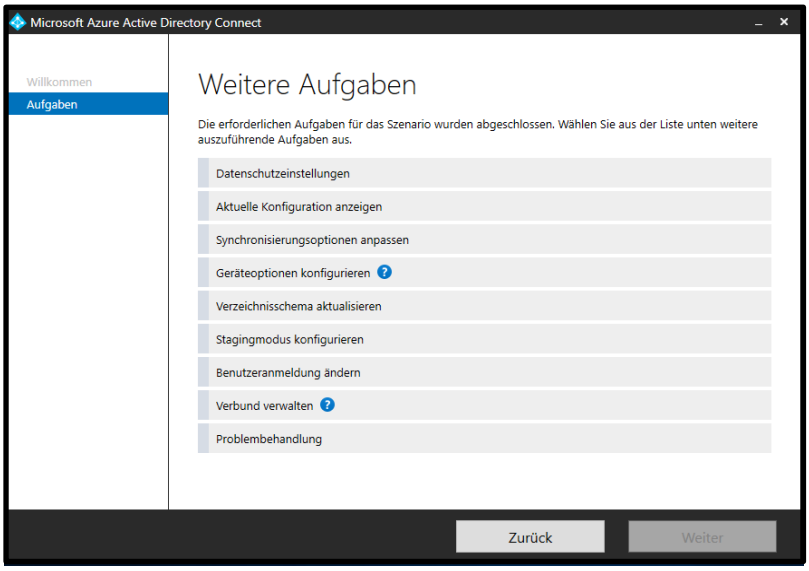
Die angelegten User in der On-Premises Domäne werden mit Hilfe von Microsoft Azure AD-Connect synchronisiert. Im Azure Portal unter den Active Directory Einstellungen ist der Synchronisationsstatus sowie die letzte Synchronisierung ersichtlich.



Anpassung des AAD-Connect

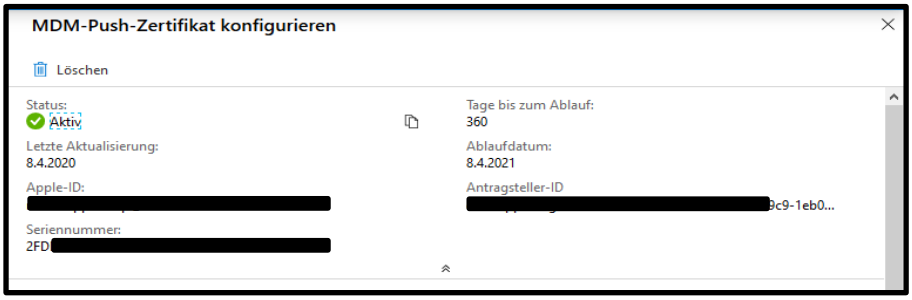
Zu Beginn muss eine RDP-Verbindung mit dem On-Premises Server hergestellt werden. Im Anschluss muss Microsoft Azure Active Directory Connect aufgerufen werden, wo die Möglichkeit besteht, die in der Grafik erkenntlichen Aufgaben auszuführen. Jede Änderung ist mit dem Projektverantwortlichen und im Anschluss mit dem Kunden abzustimmen.

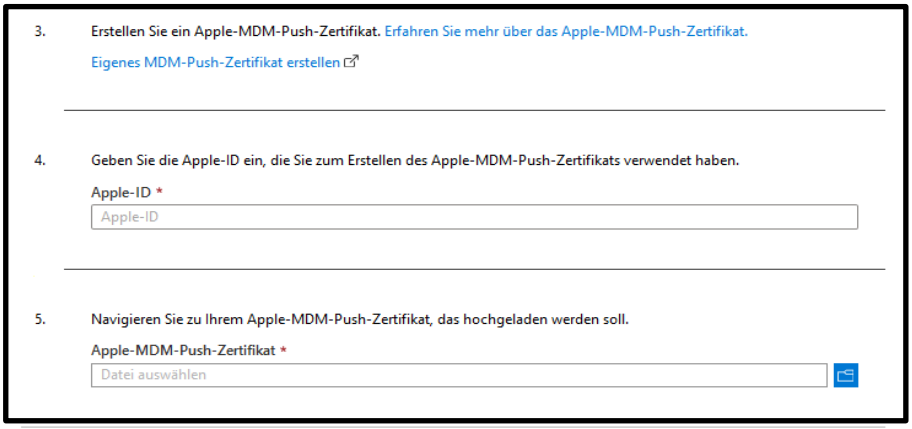
Alle weiteren administrativen Einstellungen können im Microsoft Azure Portal, im Microsoft Endpoint Manager Admin Center oder im Apple Business Manager getätigt werden.



Erneuerung des MDM-Push-Zertifikats

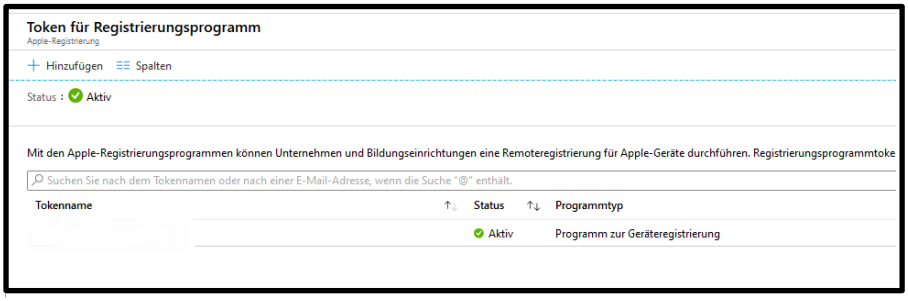
Das MDM-Push-Zertifikat muss alle 360 Tage erneuert werden. Die Erneuerung kann im Azure Portal unter der Geräteregistrierung getätigt werden. Dort muss die aktuelle „IntuneCSR.csr“ Zertifikatsanforderung heruntergeladen werden, welche im Anschluss im Apple Push Certificates Portal hochgeladen werden muss. Im Apple Push Certificates Portal wird dann das MDM-Push-Zertifikat erstellt. Dieses Zertifikat muss nun zusammen mit der Apple-ID (4. Schritt) im Intune (5. Schritt) hochgeladen werden.



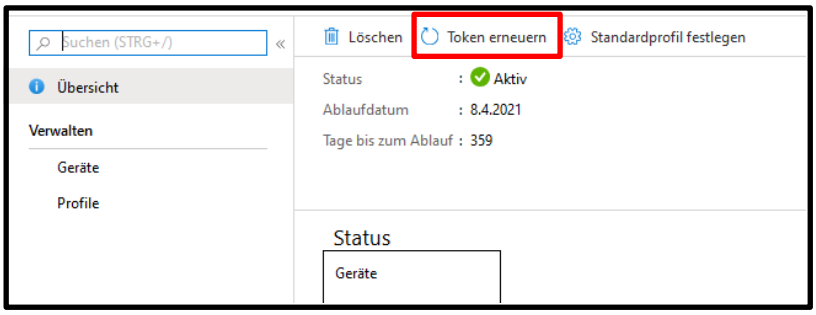


Erneuerung des Registrierungsprogramm – Token

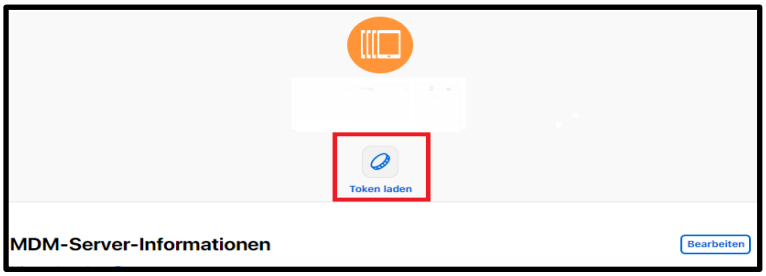
Die Erneuerung des Tokens kann ebenfalls in den Geräteregistrierungs-Einstellungen durchgeführt werden. In den Einstellungen gibt es eine Übersicht über alle Tokens. Zurzeit ist jedoch nur ein Token hinterlegt.

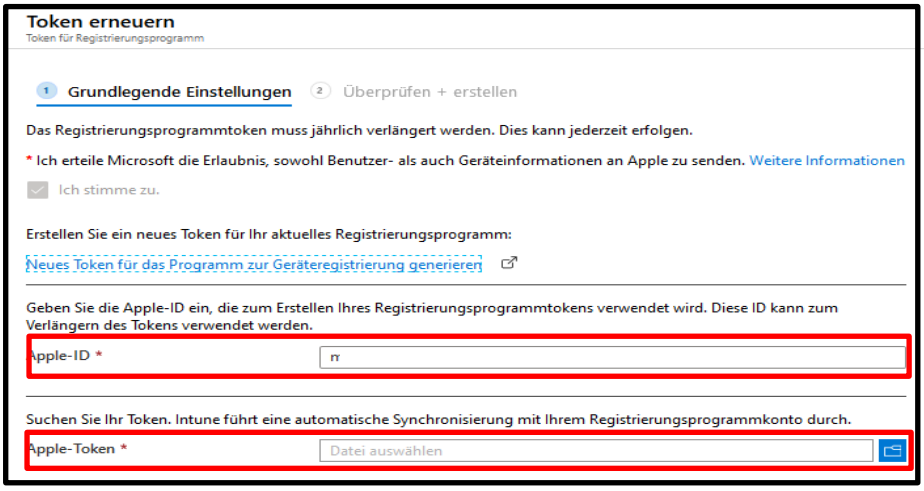


Dieser Token muss anschließend aufgerufen werden. In der Menüleiste, besteht nun die Option, den Token zu erneuern.



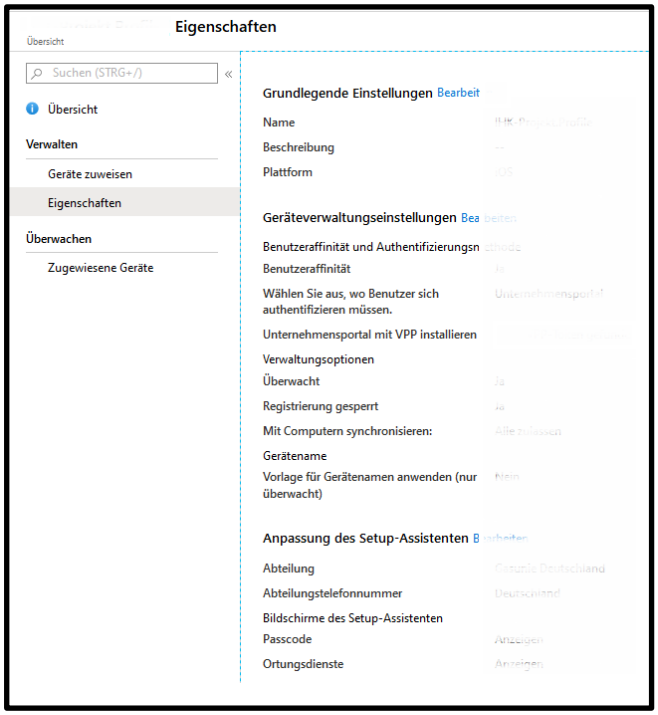
Im Apple Business Manager muss daher im erstellen XXX_MDM-Server, ein neuer Token heruntergeladen werden, welcher im Anschluss im Intune hochgeladen werden muss (siehe 2). Ebenfalls muss erneut, die Apple-ID angegeben werden, was jedoch i.d.R. automatisch passiert (siehe 1). Nachdem bestätigen wird der Token erneuert.





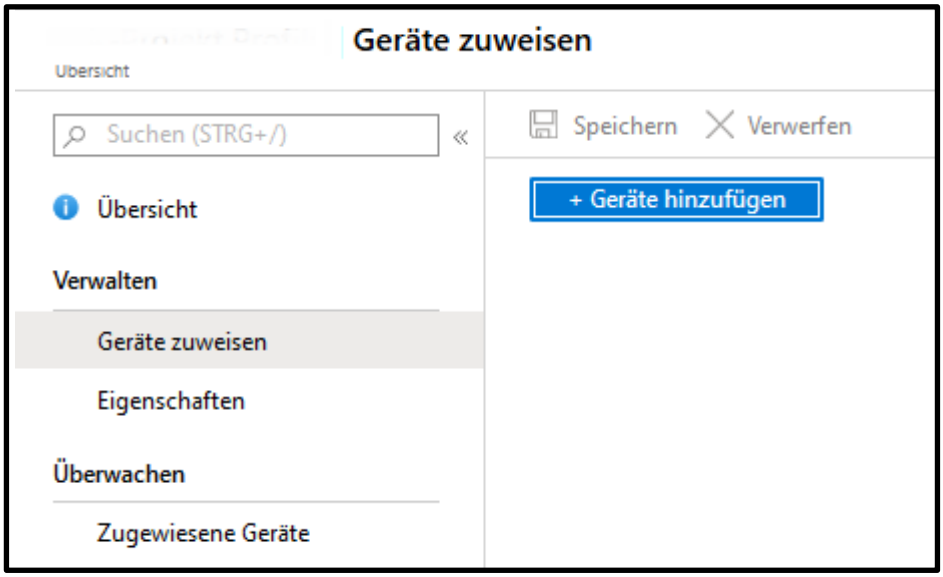
Änderung des Enrollment Prozess

Um Änderung im Enrollment Prozess vorzunehmen, muss das DEP-Profil verändert werden. Das derzeitige DEP-Profil lässt sich im Registrierungsprogramm unter dem Reiter „Profile“ anpassen.



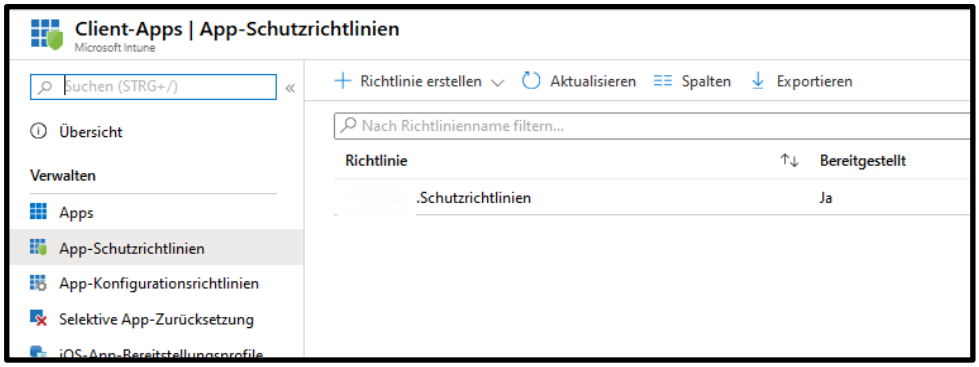
Beschaffung neuer mobilen Endgeräte

Sobald ein neues Endgerät mit der Organisations-ID vom Kunden beschafft worden ist, wird dieser automatisch dem Apple Business Manager zugewiesen. Die Zuweisung zwischen Endgerät und dem MDM-Server (XXX_MDM-Server) erfolgt automatisch, da der MDM-Server als „default“ Server gesetzt worden ist. Nach der nächsten Synchronisation wird das Endgerät im Intune angezeigt. Diesem Gerät muss anschließend keinem DEP-Profil zugewiesen werden, da ein Standardprofil erstellt worden ist, welches den neuen Endgeräten automatisch zugewiesen wird.



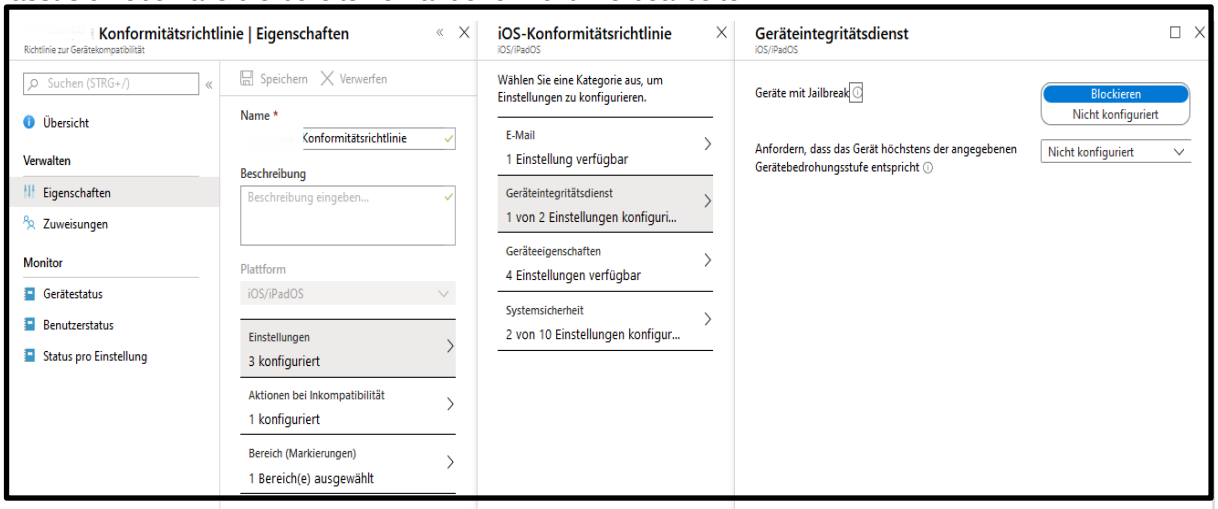
Anpassung der APP-Schutzrichtlinien

Anpassung der Schutzrichtlinien lassen sich im Intune unter den Client-Apps tätigen. Dort lassen sich neue Richtlinien anlegen und bereits vorhandene Richtlinien bearbeiten.



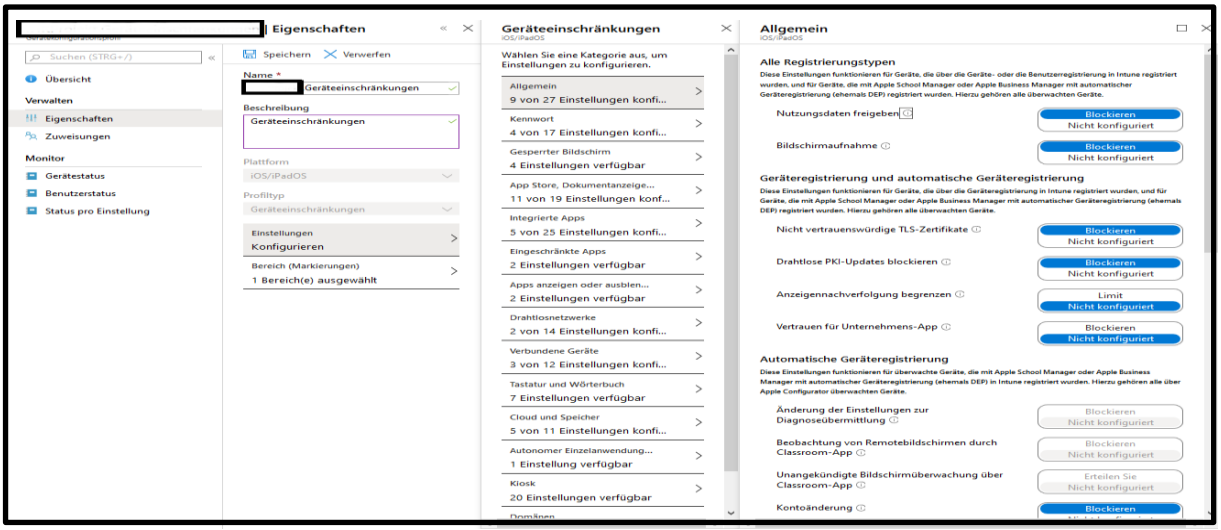
Anpassung der Konformitätsrichtlinien

Anpassung der Konformitätsrichtlinien lassen sich im Intune unter Gerätekompatibilität tätigen. Dort lässt sich ebenfalls die bereits vorhandene Richtlinie bearbeiten.



Anpassung der Richtlinien zur Geräteeinschränkung und Gerätefunktionen

Anpassungen der Geräteeinschränkungen/Gerätefunktionen lassen sich im Intune unter den Gerätekonfigurationen tätigen.

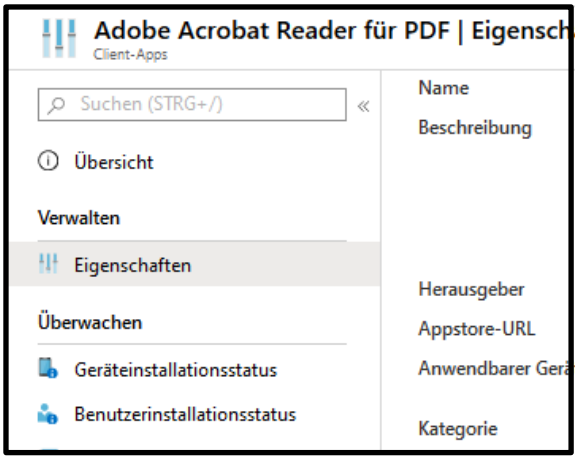


Unternehmens-App

Um die Zuweisung der Unternehmens-App zu vereinfachen, wurden zwei Gruppen erstellt. Diesen beiden Gruppen wurden dann, die entsprechen Applikationen zugewiesen.

XXX_Mitarbeiter → Applikationen für alle Mitarbeiter

XXX_GF → Applikationen für Geschäftsführung



Anpassungen der Apps lassen sich im Intune unter den Client Apps tätigen. Dort muss die gewünschte Applikation ausgewählt werden und in den Eigenschaften unter Zuweisung kann eine Zuweisung getätigt werden.