



LEITFADEN

Praxisguide: Einführung und Betrieb von MDM im Enterprise- Bereich

Inhalt

Einleitung	3
1. Zieldefinition und Rahmenbedingungen	4
2. Anforderungen definieren	6
3. Marktanalyse und Produktauswahl	7
4. Projektplanung und Team aufsetzen	10
5. Infrastruktur vorbereiten	12
6. Richtlinien und Konfigurationen definieren	15
7. Pilotphase durchführen	18
8. Schulung und Dokumentation	21
9. Rollout planen und durchführen	24
10. Betrieb und Monitoring etablieren	27
11. Review & Optimierung	30
Fazit	32

Einleitung

In Unternehmen mit tausenden oder gar zehntausenden mobilen Geräten ist die Einführung eines Mobile Device Managements (MDM) unerlässlich, um Sicherheit, Effizienz und Produktivität in Einklang zu bringen. Die Einrichtung eines MDM-Systems ist jedoch komplex: Es gilt, technische Rahmenbedingungen, organisatorische Abläufe und unternehmensspezifische Anforderungen sauber aufeinander abzustimmen.

Dieser Leitfaden begleitet IT-Verantwortliche und Entscheider chronologisch durch alle Phasen eines MDM-Projekts – von der Zieldefinition über die Einführung bis hin zum laufenden Betrieb. Wir zeigen bewährte Vorgehensweisen und geben konkrete Handlungsempfehlungen – praxisnah anhand des Beispiels von Cortado MDM. Darüber hinaus werden typische Stolperfallen aufgezeigt, die bei Planung und Umsetzung zu vermeiden sind. So gelingt eine strukturierte, wirtschaftliche und nachhaltige Einführung von Mobile Device Management im Unternehmen.

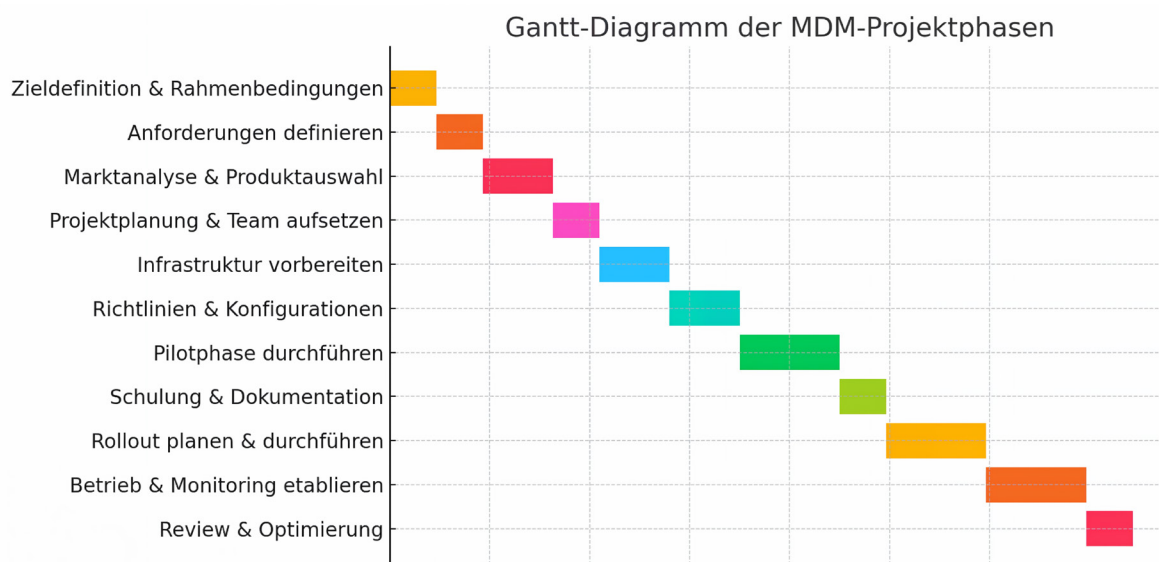


Abbildung 1 Überblick über die Phasen eines MDM-Projekts von der Planung bis zum laufenden Betrieb (Zeitachse)

1. Zieldefinition und Rahmenbedingungen

Zielsetzung definieren

Zu Beginn jedes MDM-Projekts steht die klare Zielsetzung. Definieren Sie, warum Ihr Unternehmen eine MDM-Lösung einführen will und welche übergeordneten Geschäftsziele damit unterstützt werden sollen.

Häufige Ziele sind z. B.:

- **IT-Sicherheit und Compliance erhöhen:** Schutz sensibler Unternehmensdaten auf mobilen Geräten und Einhaltung von Vorschriften (z. B. DSGVO, NIS2).
- **Effizientere Geräteverwaltung:** Zentrale Steuerung von Einstellungen, Updates und Apps auf allen Geräten, um den Verwaltungsaufwand zu reduzieren.

- **Produktivität und Flexibilität steigern:** Unterstützung von BYOD (Bring Your Own Device) ohne Sicherheit einzubüßen, sowie bessere Unterstützung für mobile Mitarbeiter im Vertrieb oder Service.
- **Kostenkontrolle:** Senkung von Supportkosten und Vermeidung von Sicherheitsvorfällen, die hohe Kosten verursachen können (Datenlecks, Geräteverlust etc.).

Stakeholder einbinden

Binden Sie die relevanten Interessengruppen von Anfang an ein. Dazu zählen neben der IT-Abteilung auch Fachabteilungen, Geschäftsführung sowie HR/Personal, Rechtsabteilung/Compliance und ggf. die Datenschutzbeauftragten.

Insbesondere **in Deutschland ist die frühzeitige Einbindung des Betriebsrats zwingend** erforderlich, damit er bereits zu Projektbeginn über die klaren Trennmechanismen und Datenschutzvorkehrungen des MDM-Systems Bescheid weiß. So können spätere Blockaden aufgrund befürchteter Mitarbeiterüberwachung verhindert werden.

Klären Sie gemeinsam die Rahmenbedingungen: Welche Nutzungsrichtlinien sollen gelten? Wie wird der Schutz der Mitarbeiterdaten und der Privatsphäre garantiert? (Etwa, indem private Daten auf BYOD-Geräten vom MDM nicht erfasst werden.)

Ein Konsens zwischen IT, Personal, Recht und Betriebsrat über Work-Life-Balance, Datenschutz und Nutzungsregeln bildet die Grundlage für die weitere Planung.



Bestandsaufnahme durchführen

Noch vor Auswahl einer Lösung sollten Sie den Status quo erfassen. Erstellen Sie eine **vollständige Bestandsaufnahme der mobilen Gerätelandschaft** im Unternehmen. Dokumentieren Sie:

- Wie viele Geräte, welche Geräte-Typen (Smartphone/Tablet) und welche Betriebssysteme (iOS, iPadOS, Android, eOS) und Versionen sind im Einsatz?
- Wo befinden sich die Geräte, und wie werden sie genutzt (z. B. reine Bürogeräte vs. Außendienst)?
- Auch der Geräteeigentümer ist wichtig: Sind es ausschließlich Firmengeräte oder nutzen Mitarbeiter bereits private Geräte (BYOD) für Unternehmensdaten?

Diese Inventur deckt oft vergessene Endgeräte oder Schatten-IT auf und schafft eine Datenbasis für alle weiteren Schritte (z.B. für die Budget Planung).

Identifizieren Sie außerdem technische Rahmenbedingungen – insbesondere die vorhandene IT-Infrastruktur wie E-Mail-Systeme, Verzeichnisdienste (z.B. Microsoft Entra), Zertifikatsstellen, Netzwerkanbindung (VPN, WLAN), die in das MDM-Konzept integriert werden müssen.

Ziele messbar machen

Legen Sie fest, welche **Kennzahlen** oder Kriterien den Erfolg der MDM-Einführung messen. Beispielsweise könnte ein Ziel sein, dass binnen 6 Monaten **100% der Unternehmensgeräte im MDM registriert** sind, oder dass **Sicherheitsrichtlinien (Passwort, Verschlüsselung etc.) zu 100% durchgesetzt** werden.

Auch die Reduktion von Zwischenfällen (z. B. verlorene Geräte ohne Fernlöschung) oder Zeitersparnis im Onboarding neuer Geräte können Erfolgsindikatoren sein. Solche Metriken helfen später bei der Bewertung – und dienen als Grundlage, um den Zielerreichungsgrad sowie den Nutzen des MDM-Projekts systematisch zu erfassen (siehe Phase 11).



2. Anforderungen definieren

Steht das “Warum” fest, folgt das “Was”: Sammeln und dokumentieren Sie **detaillierte Anforderungen** an die MDM-Lösung. Orientieren Sie sich dabei an den zuvor definierten Zielen und der Bestandsaufnahme. Wichtige Aspekte sind:

- **Unterstützte Gerätetypen und Plattformen:** Stellen Sie sicher, dass alle relevanten Betriebssysteme abgedeckt werden (typisch: **iOS, Android**). Gerade bei großen Umgebungen ist Vielfalt üblich. Notieren Sie spezielle Anforderungen, z. B. die Unterstützung von Geräten ohne Google-Dienste, falls erforderlich.



Tipp: Nicht alle Geräte sind für den Einsatz in Unternehmen gedacht und geeignet. Gerade bei Android-Geräten sollten Sie einen Blick auf die [Liste Android Enterprise Recommended](#) von Google werfen. Dort finden Sie außerdem wichtige Infos wie z.B. zur Update-Spanne der Geräte.

- **Nutzungs- und Ownership-Modelle:** Definieren Sie, welche Nutzungsszenarien unterstützt werden müssen – reine **Firmengeräte (COBO) vs. BYOD**. Wenn BYOD erlaubt ist, muss die MDM-Lösung Funktionen zur Trennung von geschäftlichen und privaten Daten bieten (Containerization, Dual-Profile, etc.) und Datenschutz gewährleisten. Gegebenenfalls soll die Lösung **COPE (Corporate-owned, Personally enabled)** Geräte unterstützen – also Firmengeräte, die privat mitbenutzt werden, was ähnliche Anforderungen wie BYOD stellt.



- **Kernfunktionen des MDM:** Legen Sie fest, welche Kernfeatures Priorität haben. Typische MDM-Funktionen sind u. a. **Geräte-Inventarisierung**, **Remote-Konfiguration** von Einstellungen/Profilen, **Durchsetzung von Sicherheitsrichtlinien** (Passwortvorgaben, Verschlüsselung etc.), **App-Verteilung und -Management** und **Gerätesperrung/Löschung aus der Ferne**. Entscheiden Sie, ob Sie z. B. *Kiosk-Modus* (für Geräte mit speziellem Anwendungsfall) benötigen. Notieren Sie auch Anforderungen an **Berichtswesen und Dashboards**, um den Gerätestatus und Verstöße gegen Richtlinien auszuwerten.
- **Integration in bestehende Systeme:** Ein MDM-System steht selten isoliert. Erstellen Sie Anforderungen an Schnittstellen: **Anbindung an Verzeichnisdienste** (zur Nutzersynchronisation z.B. Entra-ID), **E-Mail-Server** (für Gerätezugriff auf Firmenmails, z.B. Exchange Online), **Zertifikat-Infrastruktur** (für WLAN, VPN), **Auch API-Schnittstellen** für Automatisierung oder Spezialanwendungen sollten berücksichtigt werden.
- **Sicherheits- und Compliance-Vorgaben:** Leiten Sie aus Konzernrichtlinien oder gesetzlichen Vorgaben konkrete MDM-Anforderungen ab. Zum Beispiel: Unterstützung von **Geräteverschlüsselung**, **starken Passcodes** (Komplexitätsregeln), Mehr-Faktor-Authentifizierung für kritische Apps, **VPN-Nutzung erzwingen**, **Business App-Erlaubnisliste** bzw. Sperrliste etc. Falls relevant, muss die MDM-Lösung bestimmte **Zertifizierungen** (z. B. ISO 27001, BSI-Grundschutz) erfüllen.
- **Supportanforderungen:** Überlegen Sie, welche Support-Levels benötigt werden. Bei mehr als 1.000 Geräten ist ein direkter Support vom Hersteller nötig. Definieren Sie, ob es zeitkritische Funktionen gibt (z. B. Gerät sperren bei Diebstahl innerhalb von Minuten) und ob das System entsprechende **Alarmierungsmechanismen** bieten muss. Planen Sie auch Anforderungen an **Skalierbarkeit** (muss die Lösung in Zukunft 10.000 Geräte verwalten?) und **Mandantenfähigkeit** falls Sie mehrere Unternehmenseinheiten getrennt verwalten wollen.

Erarbeiten Sie die Anforderungen **gemeinsam mit den Stakeholdern**. Beziehen Sie Vertreter der Fachabteilungen ein, um spezielle Needs zu entdecken – etwa braucht der Vertrieb vielleicht eine Möglichkeit, unterwegs unkompliziert auf Verkaufsunterlagen zuzugreifen (Content-Management-Funktionen), während die Entwicklung Wert auf Entwickler-freundliche Richtlinien legt. **Dokumentieren** Sie alle Anforderungen schriftlich, z. B. in einem **Lastenheft** oder einer Kriterienliste. Diese Liste bildet die Bewertungsgrundlage in der nächsten Phase.

3. Marktanalyse und Produktauswahl

Der MDM-Markt ist vielfältig: Von komplexen Enterprise-Suiten bis hin zu spezialisierten Tools ist alles vertreten. Doch nicht immer ist die größte Lösung auch die beste: Entscheidend ist, dass das System zur IT-Landschaft, den Sicherheitsanforderungen und den organisatorischen Abläufen des Unternehmens passt.

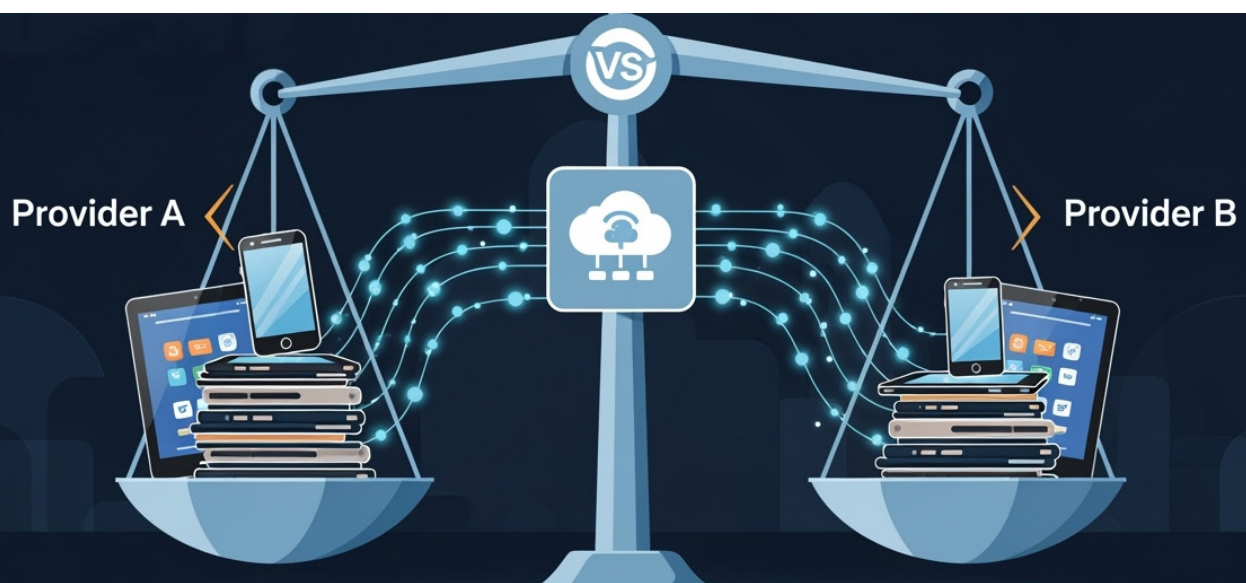
Nutzen Sie die definierten Anforderungen, um eine **Longlist** potenzieller Lösungen zu erstellen. Quellen für die Marktanalyse sind z. B. **Trusted.de** oder **OMR**, Fachartikel, Erfahrungsberichte anderer Unternehmen sowie Beratungen durch Systemintegratoren.

Wichtig ist, eine Lösung zu finden, die technisch passt und vom Hersteller die benötigte Unterstützung bietet. Insbesondere bei großen Projekten mit mehr als 1.000 Geräten sind die Hersteller-Expertise und die Qualität des Supports kritische Erfolgsfaktoren. Idealerweise erfolgt die Betreuung auch auf Deutsch.

Bewertungsfaktoren

Vergleichen Sie die Lösungen anhand **objektiver Kriterien**. Dazu zählen u. a.:

- **Funktionale Abdeckung:** Decken die Tools alle „Must-have“ Anforderungen ab (vgl. Funktionsliste aus Phase 2)? Wo gibt es Abweichungen?
- **Benutzerfreundlichkeit:** Ist die Admin-Oberfläche intuitiv? Gibt es automatisierte Workflows wie etwa **Zero-Touch-Bereitstellung** für neue Geräte? Ist die Lösung auch in deutscher Sprache verfügbar? Ein hoher Einarbeitungsaufwand und eine komplexe Bedienung können den laufenden Betrieb erschweren.
- **Plattform-Unterstützung:** Unterstützt die Lösung zuverlässig alle gewünschten Gerätetypen und Betriebssystem-Versionen? Nicht alle MDM-Systeme verwalten beispielsweise BYOD und COPE-Geräte gleich gut.
- **Sicherheit und Compliance:** Welche **Sicherheitsfeatures** sind eingebaut? Bietet diese Lösung etwa eine **Remote-Wipe-Funktion** oder spezielle Compliance-Vorlagen zur Einhaltung der DSGVO? Werden **Verschlüsselung** und **Container** unterstützt? Wichtig ist auch, ob das System **Reports und Audits** liefert, die den Anforderungen von Datenschutzbeauftragten oder Wirtschaftsprüfern entsprechen.
- **Integration:** Lässt sich das MDM in Ihre IT-Landschaft integrieren? Essenziell ist hier oft die Authentifizierung gegen Entra-ID, APIs für Automatisierungen und Single-Sign-On.
- **Skalierbarkeit und Performance:** Achten Sie auf Referenzen oder Reviews für Installationen in ähnlicher Größenordnung. Die Lösung sollte auch 10.000 oder mehr Geräte verwalten können, falls Wachstum absehbar ist – und zwar ohne Performanceeinbußen.
- **Betriebsmodell Cloud:** Entscheiden Sie, ob eine **Cloud-Lösung** in Frage kommt. Cloud-MDM (Software as a Service) bietet oft Vorteile wie eine skalierbare Infrastruktur und geringere interne Betriebsaufwände, da keine Updates notwendig sind und keine eigene Infrastruktur gepflegt werden muss. Sie sollten hier besonders darauf achten, dass der Hosting-Standort der Lösung in Deutschland liegt, so erfüllen Sie deutlich einfacher die Anforderungen an die DSGVO und NIS2.
- **Kostenmodell:** Vergleichen Sie die **Total Cost of Ownership (TCO)** der Lösungen. Berücksichtigen Sie Lizenzkosten – typischerweise pro Gerät und oft gestaffelt nach Funktionsumfang –, als auch laufende Kosten für Support und Updates. Achten Sie außerdem auf versteckte Kosten, z. B. für zusätzliche Module oder **Add-ons**. **Einige Anbieter verlangen Aufpreise für wichtige Supportleistungen** oder Sicherheitsfeatures, was eine vermeintlich günstige Lösung schnell teuer machen kann.



Produkttest und PoC

Engen Sie die Auswahl auf eine **Shortlist** (z. B. 2–3 Lösungen) ein und führen Sie – falls möglich – **Teststellungen** durch. Viele Hersteller bieten kostenlose Testversionen oder Pilotprogramme an. Nutzen Sie diese, um die Lösungen mit *echten Geräten* in Ihrer Umgebung zu erproben.

Überprüfen Sie dabei insbesondere:

- Erfüllt das Produkt die Kernanforderungen?
- Wie einfach ist die Bedienung wirklich? Müssen Admins viele manuelle Schritte tun?
- Treten unerwartete Probleme auf?

Ein kurzer Pilot mit einer kleinen Nutzergruppe **vor** endgültiger Kaufentscheidung kann Aufschluss über die Praxistauglichkeit geben.

Ebenso empfiehlt es sich, *Referenzkunden* der Hersteller zu kontaktieren oder Erfolgsgeschichten zu studieren, idealerweise in Ihrer Branche oder vergleichbarer Größe.

Bereits während der Testphase sollten Sie Reaktionszeiten und Lösungsqualität des Supports genau beobachten, denn ein schnell erreichbares und fachkundiges Support-Team ist im späteren Betrieb der Schlüssel, um Störungen zügig zu beheben und eine hohe Systemverfügbarkeit sicherzustellen.

Auch die Kommunikation und der generelle Austausch mit dem Anbieter sollte in die Bewertung einfließen, denn Sie streben eine langfristige Partnerschaft mit diesem Unternehmen an. Eine einfache und schnelle Kommunikation kann hier auf Dauer viel Aufwand ersparen.

Anhand aller Informationen bewerten Sie die Optionen und treffen schließlich eine **Produktauswahl**. Oft kristallisiert sich ein Favorit heraus, der die Anforderungen am besten erfüllt, der Preis der Lösung sollte nicht das entscheidende Kriterium sein.

Stellen Sie sicher, dass auch langfristige Überlegungen einbezogen werden: Die gewählte Lösung sollte eine *Roadmap* haben, die mit Ihrer Mobilstrategie mitwachsen kann.

Wenn die Entscheidung gefallen ist, sichern Sie sich, wenn nötig, die Budget-Freigabe und gehen in Vertragsverhandlungen.

Wichtig ist, die Lösung zu finden, die **am besten zu Ihren Geschäftsanforderungen und Ihrer IT-Landschaft passt**. Nehmen Sie sich für die Marktanalyse und Auswahl ausreichend Zeit – Fehlentscheidungen in dieser Phase führen später zu kostspieligen Problemen.

4. Projektplanung und Team aufsetzen

Ist die Entscheidung für Ihre MDM-Lösung gefallen, beginnt die eigentliche **Projektplanung**. Gerade bei umfangreichen Rollouts mit tausenden Geräten, zahlreichen Nutzergruppen und möglicherweise globalen Standorten ist ein strukturiertes Projektmanagement entscheidend. Im Folgenden erläutern wir die hierfür erforderlichen Schritte praxisnah am Beispiel von [Cortado MDM](#).

Projektplan erstellen

Definieren Sie einen detaillierten **Projektplan mit Meilensteinen** für alle folgenden Phasen. Typische Meilensteine sind z. B.: *Kickoff*, *Abchluss der Infrastrukturvorbereitung*, *Policies definiert*, *Pilot erfolgreich*, *Rollout Start*, *Rollout Ende*, *Projekt-Review*.

Schätzen Sie realistisch, wie lange jede Phase des Projekts dauern wird, und planen Sie Pufferzeiten für unerwartete Verzögerungen ein. Unsere Erfahrungen zeigen: Ein MDM-Projekt für 1.000 oder mehr Geräte erstreckt sich – je nach Komplexität – über einen Zeitraum von 6 bis 12 Monaten.

Visualisieren Sie den Zeitplan in Form eines Projektphasen-Gantt oder einer Timeline (siehe Abb. 1 oben) und stimmen Sie ihn frühzeitig mit den relevanten Stakeholdern ab.

Ressourcen planen

Stellen Sie sicher, dass genügend personelle und finanzielle Ressourcen für das Projekt vorhanden sind. Legen Sie ein Projektbudget fest, das neben den Lizenzkosten auch Aufwände für Schulungen, externe Berater (z.B. vom Hersteller), Hardware (z. B. neue Endgeräte) und Puffer für Unvorhergesehenes umfasst.

Identifizieren Sie Abhängigkeiten und Vorleistungen: Müssen vor dem Rollout z. B. alle Geräte auf eine bestimmte OS-Version gebracht werden? Müssen Accounts für Apple Business Manager oder Google-Workspace-Integrationen eingerichtet sein? Solche Aufgaben gehören früh in den Plan.



Projektteam und Rollen

Benennen Sie ein kompetentes Team, welches das MDM-Projekt trägt. Ein Projektteam für die Einführung eines MDM-Systems besteht typischerweise aus folgenden Rollen:

Rolle im Projekt	Aufgaben und Verantwortlichkeiten
<i>Projekt-Initiator</i> (Auftraggeber, z. B. CEO, CTO, IT-Leiter)	Setzt das Mandat und die Ziele des Projekts fest, stellt Budget bereit und unterstützt bei Eskalationen. Vertritt das Projekt gegenüber der Geschäftsführung.
<i>Projektleiter</i>	Steuert das Projekt im Tagesgeschäft: Plant und koordiniert Phasen und Aufgaben, überwacht den Zeitplan und das Budget, stimmt sich mit allen Beteiligten ab, managt Risiken und Kommunikation. Ist zentrale Ansprechperson.
<i>MDM-Architekt / Technischer Lead</i>	Übersetzt Anforderungen in technische Umsetzung. Verantwortet Architektur der MDM-Lösung, Integration in IT-Landschaft, Schnittstellen. Plant die Infrastruktur (Netzwerk, Cloud-Setups) und leitet die technische Implementierung an.
<i>MDM-Administrator / Engineer</i>	Führt die konkrete Konfiguration der MDM-Plattform durch (Einrichtung der Policies, Profile, Apps etc.). Testet die Funktionen in Pilotphase, behebt technische Probleme. Wird später oft hauptverantwortlicher Betreiber der Lösung.
<i>IT-Sicherheitsbeauftragter (InfoSec/Compliance)</i>	Definiert inhaltlich die Sicherheitsrichtlinien und Compliance-Vorgaben, die im MDM umgesetzt werden (Passwort Policy, Verschlüsselung, App-Freigaben etc.). Prüft laufend die Einhaltung und bewertet Risiken.
<i>Datenschutzbeauftragter (optional)</i>	Berät das Team bzgl. Datenschutz-Themen, insbesondere bei BYOD & COPE. Stellt sicher, dass die Lösung DSGVO-konform eingesetzt wird (z. B. keine unzulässige Mitarbeiterüberwachung).
<i>Netzwerk-/Infrastruktur-Experten</i>	Bereiten die benötigte Infrastruktur vor: Netzwerkzugänge, Firewall-Freischaltungen (z. B. für APNs/FCM), Verzeichnisdienst-anbindung. Sorgen dafür, dass die technische Basis reibungslos funktioniert.
<i>Support-/Helpdesk-Leiter</i>	Plant die Support-Strategie für den Rollout und den Betrieb: definiert Prozesse für Störungsmeldungen der User während und nach dem Rollout. Koordiniert Kommunikation an Endanwender.
<i>Pilotanwender-Vertreter (Key User)</i>	Vertreter der Endbenutzer (z. B. aus Abteilungen), die in der Pilotphase teilnehmen. Geben Feedback zur Nutzersicht, helfen Akzeptanzprobleme früh zu erkennen. Können später als „Multiplikatoren“ Kollegen unterstützen.

Je nach Unternehmensgröße können Rollen auch mehrfach durch eine Person abgedeckt werden (in kleineren Firmen übernimmt z. B. der IT-Leiter oft Sponsor und Projektleiter in Personalunion).

Wichtig ist, **klare Verantwortlichkeiten** festzulegen, damit jeder weiß, wer welche Entscheidungen treffen darf und wer für welche Aufgaben zuständig ist. Kommunizieren Sie diese Rollenverteilung an alle Projektbeteiligten und Stakeholder, um Erwartungshaltungen zu klären.

Kommunikation und Change-Management

Planen Sie von Anfang an, wie die **interne Kommunikation** rund um das Projekt ablaufen soll. Gerade wenn viele Mitarbeiter betroffen sind, ist Change-Management essenziell: Stellen Sie früh die Vorteile der MDM-Einführung heraus – etwa erhöhte Sicherheit, effizienteren Support sowie die Möglichkeit zur gleichzeitigen Nutzung der Geräte für private und berufliche Zwecke (BYOD, COPE).

Gehen Sie außerdem offen auf mögliche Bedenken ein, zum Beispiel das Thema "Überwachung". Erklären Sie klar und verständlich, welche Daten **nicht** erfasst werden. Dieser Punkt ist wichtiger als häufig angenommen. Cortado ist sich dessen bewusst und stellt daher umfangreiche Informationsmaterialien zur Verfügung.

Ein durchdachter Kommunikationsplan kann die Veröffentlichung und regelmäßige Updates im Intranet, Präsentationen auf Betriebsversammlungen, verständliche FAQ-Dokumente und weitere Formate beinhalten. So schaffen Sie Transparenz, fördern die Akzeptanz und minimieren mögliche Widerstände.

Zusammengefasst wird in dieser Phase das Fundament gelegt: Ein realistischer Zeitplan, ein kompetentes Team und alle erforderlichen Ressourcen – damit ist das Projekt bereit für die Umsetzung.

5. Infrastruktur vorbereiten

Bevor die eigentliche MDM-Einrichtung startet, muss die technische Infrastruktur geschaffen werden. In dieser Phase bringen Sie alle nötigen Systeme und Verbindungen an den Start, damit das MDM-System reibungslos funktionieren kann.

Systemarchitektur aufbauen

Für eine **Cloud-Lösung** wie die von Cortado, müssen Sie ein Admin-Konten im Cloud-Portal einrichten. Es sollte möglichst früh die **Verzeichnisdienst-Anbindung** (z. B. Entra) eingerichtet werden, damit Benutzer und Gruppen aus Ihrem Firmenverzeichnis im MDM-System verfügbar sind. Alternativ bietet sich ein Import via CSV-Datei an.

Netzwerkconfiguration

Stellen Sie sicher, dass alle nötigen **Firewall-Freigaben** und Netzwerkpfader eingerichtet sind, damit mobile Geräte mit dem MDM-Server kommunizieren können.

Außerdem benötigen **Apple-Geräte** Zugriff auf die Apple Push Notification Service (APNs) Server, damit Push-Benachrichtigungen vom MDM an die iPhones/iPads gelangen.

Android-Geräte nutzen Google Firebase Cloud Messaging (FCM) und benötigen ebenfalls spezielle Ports für die Benachrichtigung. Diese Ports und Adressen müssen ins Internet offen sein, sonst können Sie Geräte nicht wecken/ansprechen.

Wir empfehlen, die Kommunikationswege in einem Architekturdiagramm – bestehend aus Geräten, Push-Dienst, MDM-Server und interne Systemen – zu skizzieren, um nichts zu übersehen.¹

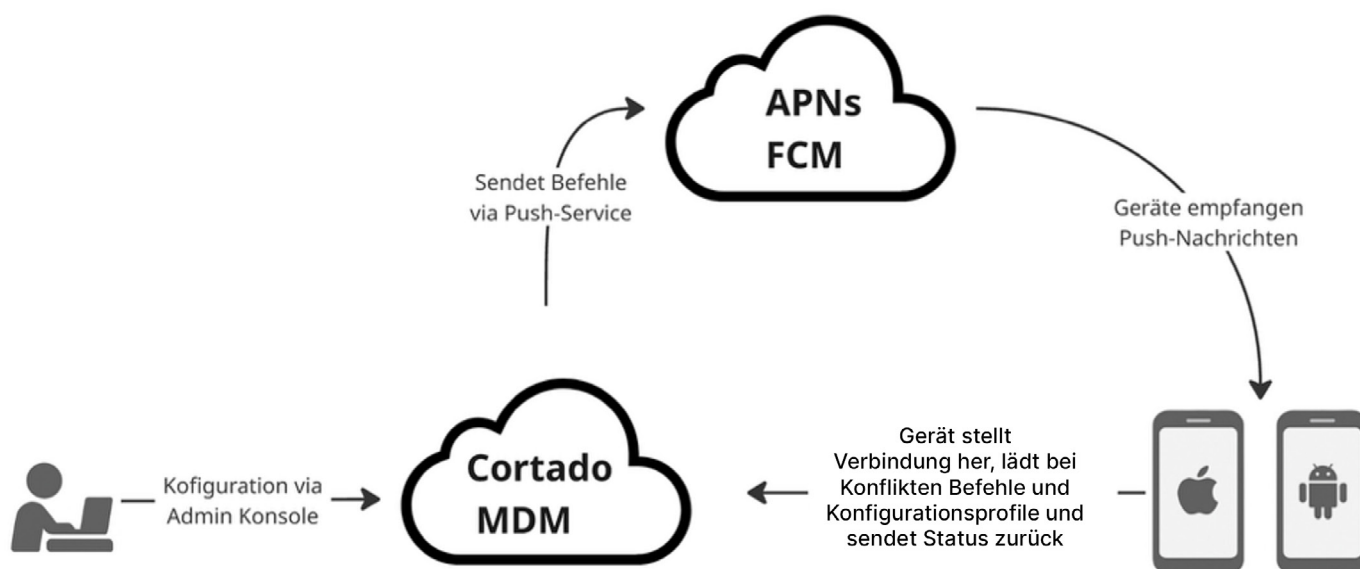


Abbildung 3 Beispiel der Cortado-MDM-Systemarchitektur (vereinfacht)

Vendor Accounts und Zertifikate

Richten Sie erforderliche **Herstellerkonten** ein, die nötig sind. Beispielsweise erfordert die Verwaltung von Apple-Geräten, dass Sie ein **Apple Business Manager (ABM)** Konto haben und ein **APNs-Zertifikat** erstellen, das in der MDM-Konsole hinterlegt wird (dies erlaubt Ihrem Cortado MDM-Server, APNs-Mitteilungen zu signieren und Geräte zu verwalten).

Für Android-Geräte muss Android Enterprise eingerichtet werden – entweder über ein kostenloses Geschäftskonto (rein für die diesen Zweck oder durch die Integration in einen bestehenden Google Workspace des Unternehmens).

Stellen Sie außerdem sicher, dass alle erforderlichen **Zertifikate** und **Token** vorliegen, beispielsweise der Apple DEP/ABM Token oder ein VPP-Token zur App-Verteilung, falls genutzt.

Cortado stellen für diesen Prozess eine ausführliche Schritt-für-Schritt-Anleitung zur Verfügung.

¹ Allg. Apple Ports: <https://support.apple.com/de-de/103229>
 Apple Geräte direkt in Unternehmensnetzwerken: <https://support.apple.com/de-de/101555>
 Android: <https://support.google.com/work/android/answer/10513641?hl=de>

Integrationen vorbereiten

Falls Ihre MDM-Lösung externe Systeme integrieren soll, stellen Sie die **Schnittstellenverbindungen** her, wie zum Beispiel:

- Integrieren Sie das **E-Mail-System** (Exchange/Office 365) mittels OAuth, wenn Cortado den mobilen E-Mail-Zugriff steuern soll.
- Richten Sie **PKI-Integrationen** ein, wenn Zertifikatsprofile automatisch verteilt werden sollen, etwa Gerätezertifikate für die WLAN-Nutzung.
- Binden Sie **Identity-Provider** an, falls das MDM SSO-Profil ausrollen soll, wie zum Beispiel SAML/OAuth mit Entra.

Je nach Tool können hier einige technische Schritte nötig sein – führen Sie diese sorgfältig durch und testen Sie jeden Baustein.

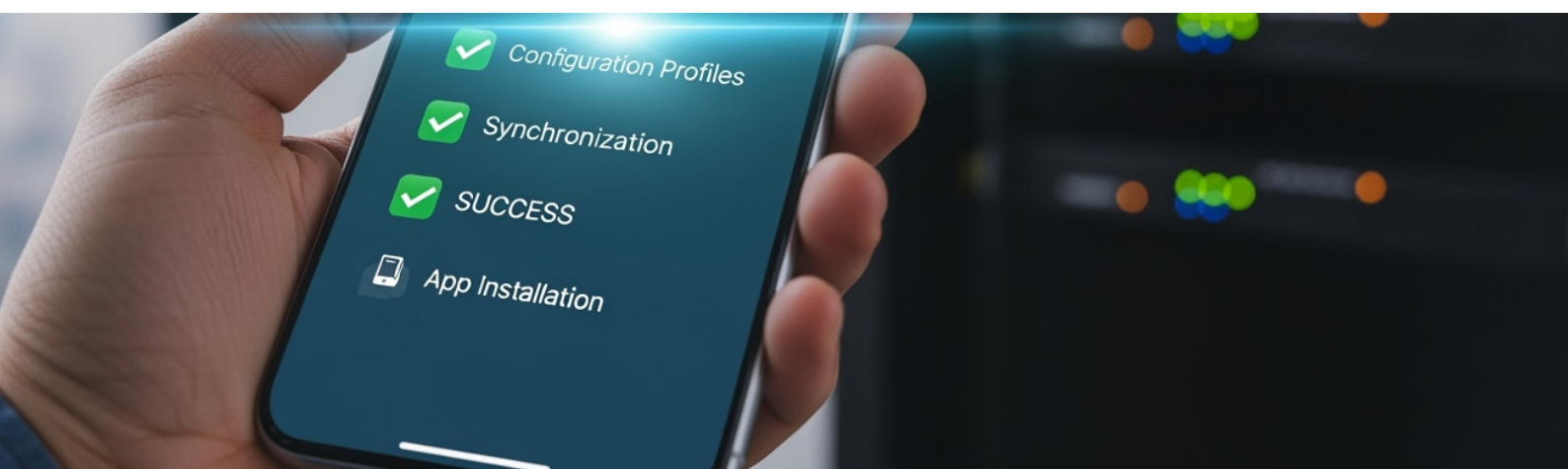
Test der Infrastruktur

Zum Abschluss dieser Phase sollten Sie sicherstellen, dass die grundlegende Infrastruktur funktionsfähig ist. Ein einfacher Smoke-Test kann dabei helfen: Nehmen Sie ein Testgerät manuell ins MDM auf und prüfen Sie, ob es eine Verbindung zum Server herstellen, Konfigurationsprofile empfangen, eine Test-E-Mail synchronisieren und Apps installieren kann.

So erkennen Sie frühzeitig, ob Netzwerk, Zertifikate und grundlegende Einstellungen korrekt konfiguriert sind – bevor Sie mit dem großflächigen Rollout beginnen. Diese Vorbereitungen sind unsichtbar für Endnutzer, aber absolut kritisch: Sie bilden das technische Rückgrat des gesamten MDM-Projekts. Nehmen Sie sich Zeit, alles richtig zu konfigurieren und dokumentieren Sie die Einstellungen für den späteren Betrieb.



Tipp: Fragen Sie Ihren MDM-Anbieter nach Best-Practices aus vergleichbaren Projekten, dies kann Ihnen viel Zeit und Mühe sparen. [Cortado](#) bietet neben einem sehr detaillierten Handbuch (DE/EN mit Videoanleitungen) auch passende Einrichtungspakete an, um Sie in dieser Phase direkt aus erster Hand zu unterstützen. Um ein besseres Gefühl für die benötigte Zeit zu bekommen: Die Grundkonfiguration der Cortado Lösung ist in weniger als 2h möglich



6. Richtlinien und Konfigurationen definieren

Mit einer vorbereiteten Plattform können Sie nun die konkreten Richtlinien, Profile und Konfigurationen entwerfen, die später auf die Geräte ausgerollt werden. Diese Phase ist der inhaltliche Kern des MDM-Projekts: Hier entscheiden Sie, wie die Geräte gemanagt werden und welche Regeln gelten.



Tipp: Premium-Lösungen wie Cortado bieten hier bereits Vorlagen, die Sie als Grundlage für die Erstellungen von Richtlinien nutzen können. So müssen Sie, nicht bei null beginnen, was den Prozess stark beschleunigen kann.

MDM-Policies entwickeln

Basierend auf Ihren Sicherheits- und Nutzungsanforderungen (siehe Phase 2) erstellen Sie einen Satz von **MDM-Richtlinien**. Dabei handelt es sich um Regeln und Einstellungen, die das MDM-System auf den Geräten durchsetzt. Wichtige Policie-Bereiche sind beispielsweise:

- **Sicherheitsrichtlinien:** Hierzu zählen unter anderem Passwortvorgaben wie eine Mindestlänge, Komplexitätsanforderungen oder das Erzwingen einer Geräte-PIN. Weitere Elemente sind die *automatischen Sperren nach Inaktivität*, *Gerätezeitüberschreitungen*, individuell anpassbare *Bildschirmsperrtexte* (z.B: mit Kontaktinformationen für den Verlustfall) sowie eine maximal zulässige Anzahl an Entsperrversuchen vor einer automatischen Datenlöschung.
- **Gerätefunktionen einschränken:** Je nach Einsatzszenario können kritische Funktionen deaktiviert werden. Beispiele: *Kamera sperren* (etwa in sensiblen Bereichen), Deaktivierung von *Bluetooth* oder *USB-Schnittstellen*, Unterbinden von *Cloud-Backups* (zum Schutz vor Datenabfluss in private Clouds), oder die Beschränkung der *Screenshot-* und *Copy-Paste-Funktion* auf den Arbeitsbereich in BYOD- und CO-PE-Modellen.
- **App-Richtlinien:** Auch Anwendungen lassen sich zentral über das MDM verwalten. Legen Sie fest, welche Apps erlaubt sind (Positivliste) und blockieren Sie alle anderen (Negativliste). Alternativ kann ein unternehmenseigener App Store bereitgestellt werden. Bei Cortado erfolgt dies über die gleichnamige App auf dem Gerät. So stellen Sie sicher, dass nur geprüfte und erwünschte Anwendungen installiert werden. Für bestimmte Nutzergruppen kann auch ein Kiosk-Modus sinnvoll sein, in dem nur eine oder ausgewählte Apps genutzt werden dürfen.



Tipp: Mit Cortado MDM lassen sich Apps zudem vorkonfigurieren und unternehmenseigene Apps im APK- oder IPA-Format verteilen.

- **Netzwerk- und Kommunikationsrichtlinien:** Falls Geräte auf das Unternehmensnetzwerk zugreifen, können Sie den Zugriff über VPN vorschreiben und bei Bedarf die automatische VPN-Nutzung erzwingen. WLAN-Profile lassen sich vorkonfigurieren – etwa mit Zertifikatsauthentifizierung oder Zugang über Benutzername und Passwort. Auch E-Mail-Profile (z. B. für Exchange oder Microsoft 365) können so eingerichtet werden, dass der Nutzer nur noch sein Passwort oder den zweiten Authentifizierungsfaktor eingeben muss.
- **BYOD/COPE-spezifische Einstellungen:** Für private Geräte (BYOD) oder Firmengeräte mit privater Nutzung (COPE) sollten besondere Datenschutzrichtlinien gelten. Das MDM darf in diesem Fall keine privaten Daten erfassen. Achten Sie darauf, dass ein Arbeitsprofil bzw. Arbeitsbereich eingerichtet wird, um geschäftliche und private Daten strikt zu trennen. Kommunizieren Sie diese Trennung klar an die Nutzer, um Vertrauen zu schaffen.

Wichtig ist, die Richtlinien so zu gestalten, dass **Sicherheit und Benutzerfreundlichkeit** die Balance halten. Zu restriktive Policies können die Produktivität behindern oder auf Ablehnung bei den Mitarbeitern stoßen. Als Entscheider wissen Sie: **Eine Einheitslösung passt nicht für alle.** Daher sollten Policies **differenziert nach Nutzergruppen** konfiguriert und ausgerollt werden.

Nutzergruppen und Rollen berücksichtigen

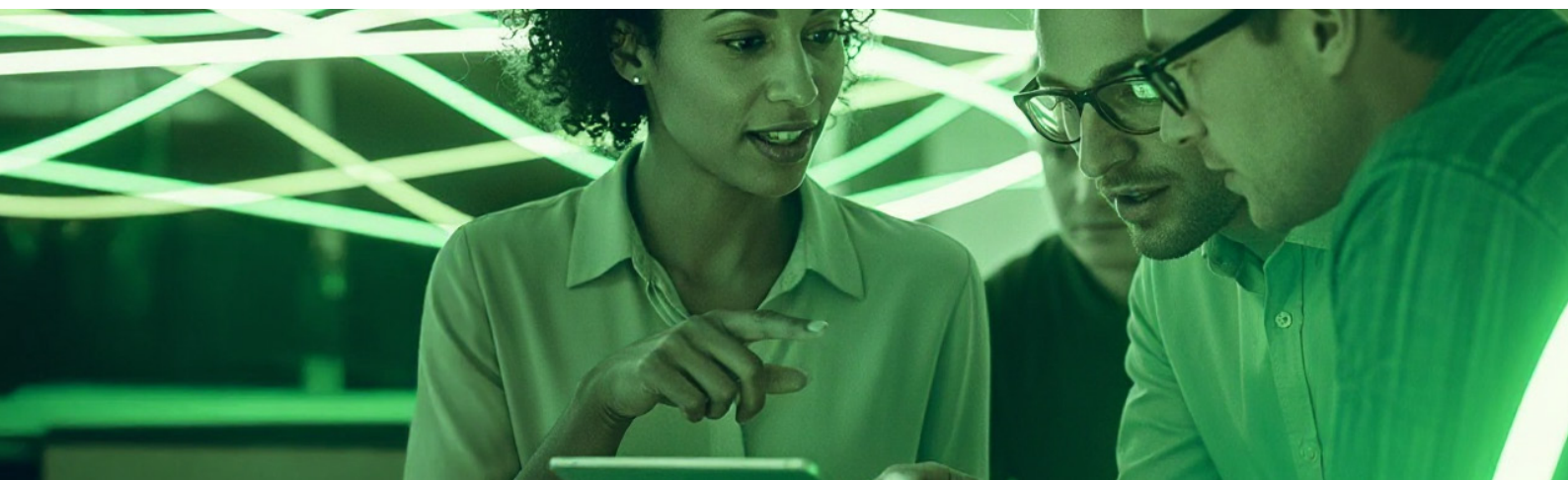
Definieren Sie im Cortado MDM-System verschiedene **Geräte- oder Nutzergruppen** (– etwa nach Abteilung, Standort, Funktionsebene) –, um unterschiedliche Richtlinien zuweisen zu können.

Beispiel: Führungskräfte benötigen möglicherweise einen offeneren App-Store, um flexibel arbeiten zu können – oder besonders strikte Sicherheitsprofile, da sie auf hochsensible Daten zugreifen. Außendienstmitarbeiter wiederum benötigen evtl. spezielle Dokumente direkt auf ihren Geräten, um unterwegs effizient arbeiten zu können

Weisen Sie die Geräte/Nutzer beim Enrollment entsprechenden Gruppen zu, damit automatisch die korrekten Richtlinien greifen. In der Praxis bedeutet das, dass Sie allgemeine Einstellungen idealerweise immer auf Gruppen-Ebene zuweisen, während individuellere Einstellungen auf Nutzer- oder sogar Geräteebene getroffen werden.



Tipp: Bei [Cortado](#) können Nutzer und Geräte auch mehreren Gruppen zugewiesen werden, das MDM kombiniert dann intelligent die einzelnen Richtlinien der einzelnen Gruppen zu einer übergreifenden.



Zur Orientierung dient folgende Tabelle mit *Beispiel-Richtlinien* für verschiedene Nutzergruppen:

Nutzergruppe	Gerätetyp / Nutzung	Beispiel-Richtlinien
<i>Geschäftsführung</i>	Firmengeräte (Corporate-Owned)	Volle Geräteverwaltung mit höchsten Sicherheitsstandards. Durchsetzung starker Passwörter und Verschlüsselung; Kamera und Cloud-Backups erlaubt, aber regelmäßige Compliance-Reports ans IT-Security-Team. Möglichkeit für VIP-Ausnahmen bei App-Installationen nach Freigabe.
<i>Mitarbeiter (Standard-Nutzer)</i>	Firmengeräte – teilweise privat genutzt (COPE)	Standard-Policy: Gerät muss Passcode haben, Auto-Lock nach 3 Min. Unternehmens-Apps werden vom MDM vorinstalliert; Installation weiterer Apps nur aus freigegebenem App-Store. Cloud-Backup der Firmenapps deaktiviert; persönliche Nutzung in definiertem Rahmen erlaubt (COPE).
<i>Außendienst/Vertrieb</i>	Firmengeräte – oft mit spezialisierten Apps	Kiosk-Modus oder eingeschränkter Modus für bestimmte Business-Apps (z. B. CRM). Zugriff auf Firmendaten nur über VPN.
<i>BYOD-Nutzer (alle Ebenen)</i>	Private Geräte, geschäftlich genutzt	Leichtgewichtiges Management: Einsatz eines Work-Profils/Container für Unternehmensdaten. Klare Trennung: MDM kann nur auf Firmenbereich zugreifen. Bei Compliance-Verstoß wird nur der Firmencontainer gelöscht (private Daten bleiben unberührt). Keine Standortdienste.

Diese *Beispiele* zeigen, wie *Richtlinien* je nach Gruppe variieren können. Führungskräfte erhalten vollen Zugriff auf benötigte Apps, während Außendienst-Geräte stärker eingeschränkt sein können (z. B. Kiosk-Modus für ein einzelnes Tool). BYOD-Geräte wiederum werden mit minimal-invasiven Mitteln verwaltet, um die Privatsphäre zu schützen und dennoch Unternehmensdaten abzusichern.

Cortado erlaubt das Anlegen solcher Nutzerrollen mit individuellen Zugriffsrechten und Restriktionen. Diese Granularität sollten Sie nutzen, um bedarfsgerechte Policies zu gestalten, statt pauschal alle über einen Kamm zu scheren.

Konfigurationsprofile einrichten

Neben den Richtlinien, die allgemeine Regeln und Einschränkungen definieren, legen Sie im MDM-System auch konkrete Konfigurationsprofile für die Geräteeinstellungen fest. Dazu gehören zum Beispiel WLAN-Profile für den sicheren Zugang zum Firmennetz (etwa über Zertifikatsauthentifizierung), E-Mail-/Exchange-Profile, VPN-Einstellungen und vieles mehr.

Richten Sie diese Profile gezielt nach den Anforderungen Ihrer IT-Infrastruktur und Nutzergruppen ein. Durch vorkonfigurierte Einstellungen sparen Sie Aufwand im Support, minimieren Bedienfehler und stellen sicher, dass alle Geräte einheitlich und sicher eingebunden sind.

Testen im kleinen Rahmen

Bevor es in die breite Pilotphase geht, testen Sie die konfigurierten Richtlinien und Profile **intern im IT-Team**. Melden Sie ein paar Geräte der Projektmitglieder an und weisen Sie verschiedene Rollen zu, um sicherzustellen, dass die Einstellungen wie gewünscht greifen.

Prüfen Sie beispielsweise, ob sich ein gesperrter Gerätetyp tatsächlich nicht mehr benutzen lässt - durch einen sogenannten Kiosk-Test. Solche Trockenübungen helfen dabei, Schwachstellen oder Inkonsistenzen in den Richtlinien frühzeitig zu erkennen, **bevor** sie den Endnutzern auffallen.

Passen Sie die Policies bei Bedarf an. Ziel ist ein konsistentes, klares Regelwerk, das die notwendige Sicherheit gewährleistet und Gleichzeitig im Arbeitsalltag praktikabel bleibt.

Wenn alle Richtlinien und Konfigurationsprofile abgestimmt und technisch umgesetzt sind, ist die Grundkonfiguration Ihres MDM-Systems abgeschlossen. Die nächste Herausforderung besteht darin, diese in der Praxis zu erproben.

7. Pilotphase durchführen

Die Einführung einer MDM-Lösung sollte nie im „Big Bang“ ohne vorherige Tests erfolgen. Stattdessen bewährt sich eine **Pilotphase**, um das Setup unter realen Bedingungen zu erproben und Feedback zu sammeln. In dieser Phase rollen Sie das MDM in kontrolliertem Umfang an eine kleine Gruppe aus.

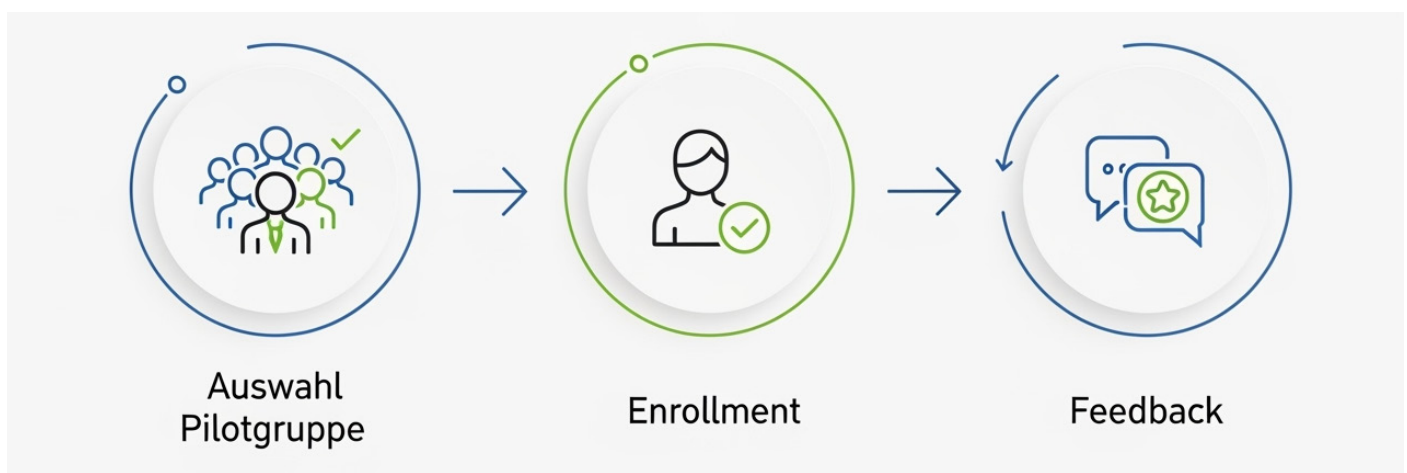


Abbildung 4 Pilotphase

Pilotgruppe definieren

Wählen Sie eine repräsentative Pilotgruppe aus. Diese sollte genügend Benutzer umfassen, um verschiedene Szenarien abzudecken, aber klein genug sein, damit eventuelle Probleme kontrollierbar bleiben. Oft nimmt man z. B. **eine Abteilung** oder **20–50 Nutzer** als Pilot.

Achten Sie auf **Diversität**: Ideal ist es, wenn verschiedene Gerätetypen und Plattformen für das Pilotprojekt ausgewählt werden – zum Beispiel iPhones und Android-Geräte sowie verschiedene Geschäftsbereiche. Viele Unternehmen starten die Pilotphase im **IT-Bereich selbst**, da dort eine höhere technische Affinität besteht und bei Bedarf schnell und direkt Unterstützung geleistet werden kann. Wichtig ist, dass die Pilotteilnehmer dem Projekt gegenüber aufgeschlossen sind und bereit, Rückmeldungen zu geben.

Kommunikation mit Teilnehmenden

Informieren Sie Mitarbeitende, die am Pilotprojekt teilnehmen, die Pilotnutzer ausführlich über das Vorhaben. Erklären Sie, dass eine neue MDM-Lösung eingeführt wird, welche Änderungen diese mit sich bringt (z. B. eine neue Firmen-App oder bestimmte Einschränkungen), und an wen sie sich bei Fragen oder Problemen wenden können.

Betonen Sie, dass Feedback ausdrücklich erwünscht ist und die Pilotphase dazu dient, das Setup zu optimieren. Bieten Sie bei Bedarf eine kurze Einweisung oder begleitende Unterlagen an, damit die Nutzer wissen, wie sie z. B. ihr Gerät registrieren oder wie sie im Falle eines Verlusts vorgehen sollten.

Cortado bietet hier zur Unterstützung ein Selfservice-Portal sowie spezielle Anleitungen für Endnutzer.

Device Enrollment in der Pilotphase

Melden Sie die Pilotgeräte am MDM-System an. Je nach Gerätesituation stehen verschiedene Enrollment-Methoden zur Verfügung:

- Bei neuen, firmeneigenen Geräten erfolgt die Registrierung i.d.R. automatisiert via Apple DEP/ADE oder Android Zero-Touch. In diesem Fall werden die Geräte bereits vorkonfiguriert an die Endnutzer ausgeliefert.
- Bei vorhandenen oder privat genutzten Geräten (z.B. im BYOD-Modell) erfolgt die Anmeldung meist manuell, typischerweise durch den Erhalt eines Einladungslinks und anschließende Registrierung über das Selfservice-Portal.

Führen Sie die Registrierung durch und stellen Sie sicher, dass alle Geräte in Ihrem MDM-Verwaltungsportal auftauchen.

Cortado bietet eine API-Schnittstelle, die Sie z.B. via Mail über das Hinzufügen neuer Geräte zu Ihrem MDM-System informiert.

Dieses *Onboarding* der Geräte ist ein erster Praxistest. Achten Sie auf Stolpersteine – funktionieren die Push-Nachrichten zuverlässig? Treten Fehlermeldungen auf? Dokumentieren Sie außerdem den Ablauf und die benötigte Zeit – diese Erkenntnisse helfen für den großen Rollout (die durchschnittliche Zeit liegt bei Cortado bei weniger als 3min/User).

Pilotbetrieb und Tests

Lassen Sie die Pilotnutzer nun im realen Alltag mit den verwalteten Geräten arbeiten. Beobachten Sie dabei mehrere Wochen lang die Ergebnisse: Werden alle geplanten Richtlinien wie vorgesehen durchgesetzt? Kontrollieren Sie in der Verwaltungskonsole stichprobenartig, ob Pilotgeräte korrekt als „compliant“ geführt werden – Abweichungen sollten nur auftreten, wenn sie ausdrücklich erwünscht sind.

Achten Sie auch auf die Auswirkungen der Konfiguration auf die Nutzer: Gibt es Beschwerden über Einschränkungen durch Policies? Werden Self-Service-Funktionen wie der Lost Mode aktiv genutzt?

Neben der Nutzerakzeptanz sind technische Aspekte zu bewerten: Beeinträchtigen Konfigurationen die Geräteperformance, etwa durch Ladezeiten, Batterieprobleme oder zu aggressive Sicherheitseinstellungen? Funkzionieren Push-Benachrichtigungen zuverlässig und ohne spürbare Verzögerung?

Support in der Pilotphase

Stellen Sie während des Piloten einen **verstärkten Support** bereit. Das IT-Projektteam sollte für die Pilotteilnehmer leicht erreichbar sein (Hotline, Chatgruppe o. Ä.), um Fragen sofort zu klären.

Alle auftretenden Probleme oder Fragen sollten sorgfältig **erfasst** werden. Beispielsweise könnte sich zeigen, dass die Anleitung zum Enrollment unklar war – dann verbessern Sie die Dokumentation, bevor der Massen-Rollout startet. Oder Nutzer melden, eine geschäftskritische App werde vom MDM blockiert – dann müssen Sie die Policy anpassen.

Cortado begleitet Unternehmen in dieser Phase mit engmaschigem Support. Aus der Erfahrung hunderter erfolgreich abgeschlossener Projekte wissen wir, worauf es im Pilotbetrieb ankommt – und geben dieses Wissen gerne weiter.

Feedback auswerten und optimieren

Am besten sammeln Sie Feedback laufend, spätestens jedoch am Ende der Pilotphase. Nutzen Sie dafür strukturierte Methoden wie kurze Umfragen oder persönliche Gespräche. Fragen Sie: Wie zufrieden sind die Pilotnutzer? Was hat gut funktioniert – was nicht?

Nehmen Sie dieses Feedback ernst. Leiten Sie daraus gezielt Optimierungen ab: Möglicherweise lassen sich zu strengen Richtlinien anpassen, ohne die Sicherheit zu gefährden. Oder es zeigt sich Schulungsbedarf, weil Funktionen missverstanden wurden.

Passen Sie Policies an, beheben Sie erkannte Fehler, und aktualisieren Sie Dokumentationen. Eine erfolgreich durchgeführte Pilotphase gibt allen Beteiligten Vertrauen in den anstehenden Rollout – und reduziert das Risiko unangenehmer Überraschungen, da kritische Probleme bereits im Kleinen identifiziert und gelöst wurden.

8. Schulung und Dokumentation

Noch bevor der große Rollout startet, kümmern Sie sich um **Schulungsmaßnahmen und Dokumentationen** – sowohl für Administratoren/Support-Teams als auch für die Endbenutzer. Ein gut informiertes Team und aufgeklärte Nutzer sind der Schlüssel, um reibungslos in den Betriebsalltag mit MDM überzugehen.

Admin- und IT-Schulungen

Stellen Sie sicher, dass die IT-Mannschaft, die das MDM betreut, umfassend geschult ist. Dazu gehören die *MDM-Administratoren* ebenso wie der *Helpdesk/Support*. Planen Sie Trainings direkt beim Hersteller, um tiefgehendes Know-how aufzubauen. Cortado bietet hier verschiedene Optionen an, die Sie bequem buchen können. Die Teilnehmer erhalten am Ende ein passendes Zertifikat.

Die Administratoren sollten sämtliche Funktionen der neuen Plattform sicher beherrschen – vom Anlegen neuer Policies bis zur Fehleranalyse bei Verbindungsproblemen. Das Erstellen interner **Administrations-Handbücher** oder Knowledge-Base-Artikel, wie typische Aufgaben durchzuführen sind (z. B. *Gerät für neuen Mitarbeiter einrichten*, *Gerät bei Austritt löschen*, *Compliance-Verstöße prüfen*) ist bei Cortado nicht nötig, da die Lösung selbst über eine ausführliche [Dokumentation in Deutsch und Englisch](#) verfügt auf die jeder frei zugreifen kann. Dadurch stellen Sie Einheitlichkeit sicher und erleichtern die Einarbeitung neuer Kollegen.

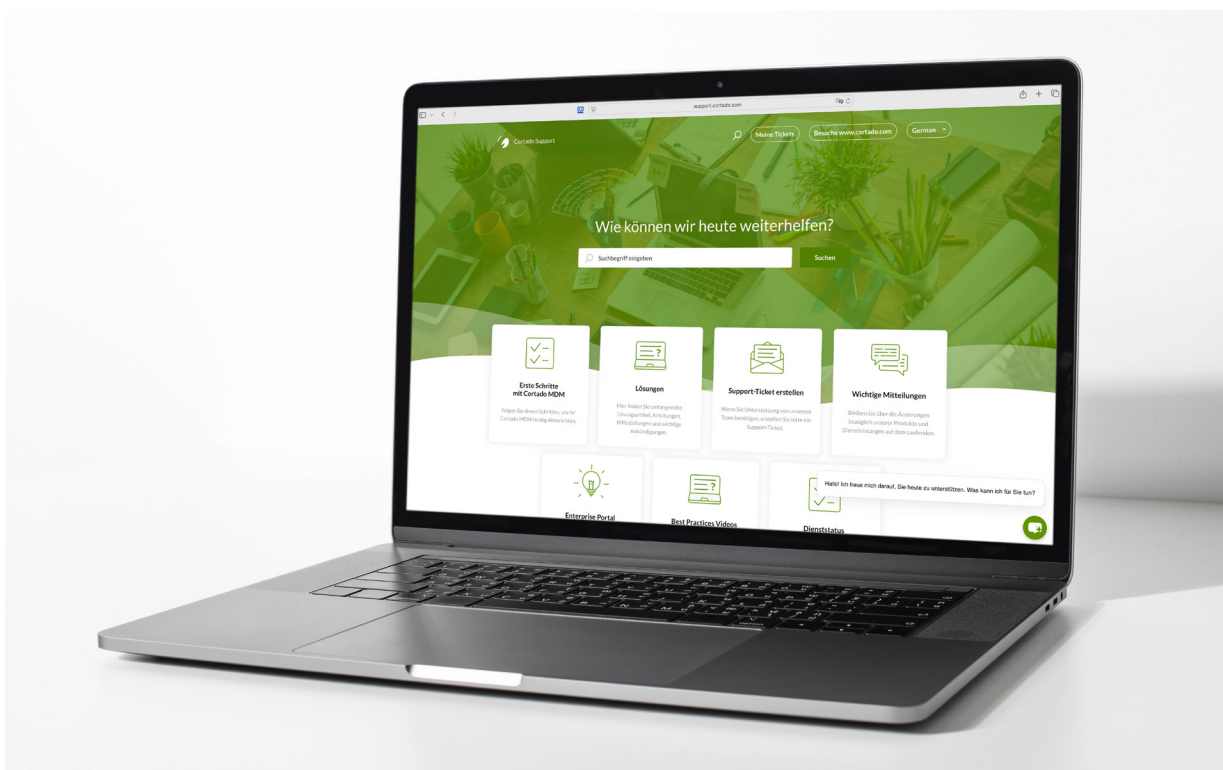


Abbildung 5 Cortado bietet Ihnen eine umfassende Knowledge Base mit hilfreichen Artikeln, Schritt-für-Schritt-Anleitungen und praxisnahen Lösungen für häufige Anwendungsfälle.

Endbenutzer-Schulungen und Kommunikation

Die meisten Mitarbeiter benötigen kein technisches Training im Detail – wohl aber klare, verständliche Informationen darüber, was von ihnen erwartet wird und wie sie ihr gemanagtes Gerät sicher und korrekt nutzen.

Typische Inhalte sollten folgende Fragen beantworten:

- **Wie registriere ich mein Gerät?** Eine Schritt-für-Schritt-Anleitung mit Screenshots hilft, Unsicherheiten beim Enrollment zu vermeiden.
- **Was bedeutet es, dass mein Gerät verwaltet wird?** Erläutern Sie, welche Zugriffe die IT hat und was privat bleibt – das schafft Vertrauen und nimmt mögliche Ängste.
- **An wen wende ich mich bei Problemen?** Geben Sie klare Support-Kontakte an, zum Beispiel eine Hotline oder eine zentrale E-Mail-Adresse.
- **Welche Regeln muss ich beachten?** Machen Sie verständlich, was erlaubt ist und was nicht – etwa, dass Geräte nicht gerootet werden dürfen und Verstöße gegen Richtlinien vermieden werden sollten.

Achten Sie auf eine einfache, klare Sprache und verzichten Sie auf unnötigen Fachjargon.

Je nach Zielgruppe und Umfang der Änderungen können zusätzliche Schulungsformate sinnvoll sein: etwa **kurze Webinare, Live-Demos, eLearning-Module** oder **Kickoff-Sessions im Team**. All dies hilft, die Akzeptanz zu erhöhen und Unsicherheiten abzubauen. **Cortado** stellt hierfür auf Wunsch passende Präsentationsfolien und Materialien als Vorlagensatz zur Verfügung.

IT-Support vorbereiten

Bringen Sie den Helpdesk auf den neuesten Stand: alle Support-Mitarbeiter sollten in der Lage sein, typische Anfragen rund um das MDM zu bearbeiten. Häufig Fälle sind zum Beispiel: „*Ich habe mein Gerät verloren – was soll ich tun?*“, „*Ich kann keine App installieren, weil MDM den Zugriff blockt*“, oder „*Seit der MDM-Einführung funktioniert mein E-Mail nicht mehr*“.

Erstellen Sie für diese und ähnliche Szenarien **Standard Operating Procedures (SOPs)**, damit der 1st-Level-Support schnell helfen kann.

Je nach Umfang des Projekts kann es sinnvoll sein, ein spezielles **Support-Team für den Rollout** einzurichten, das in der Umstellungsphase das erhöhte Anfragevolumen abfängt. Denn nichts sorgt für mehr Frustration, als wenn betroffene Nutzer während der Einführung keinen kompetenten Ansprechpartner finden. Das Support-Team selbst sollte in dieser Phase eng mit dem Hersteller in Kontakt stehen.

Dokumentation des Systems

Parallel gilt es, das technische System zu dokumentieren. Zeichnen Sie die **finale Architektur** auf. Dokumentieren Sie alle **MDM-Einstellungen und Profile**: Welche Richtlinien sind aktiv, und mit welchen Werten? So behalten Sie stets die Übersicht und können Änderungen nachvollziehen. Diese Dokumentation ist Gold wert für den laufenden Betrieb und bei Audits. Auch Zugriffsrechte (z.B. wer MDM-Admin sein darf) und Prozessbeschreibungen (z. B. für den Enrollment-Prozess für neue Geräte) sollten enthalten sein. Cortado liefert hier viele dieser Informationen direkt über die Reporting-Funktion. Cortado stellt passende Musterverträge für die Konzepte COBO, COPE und BYOD bereit.

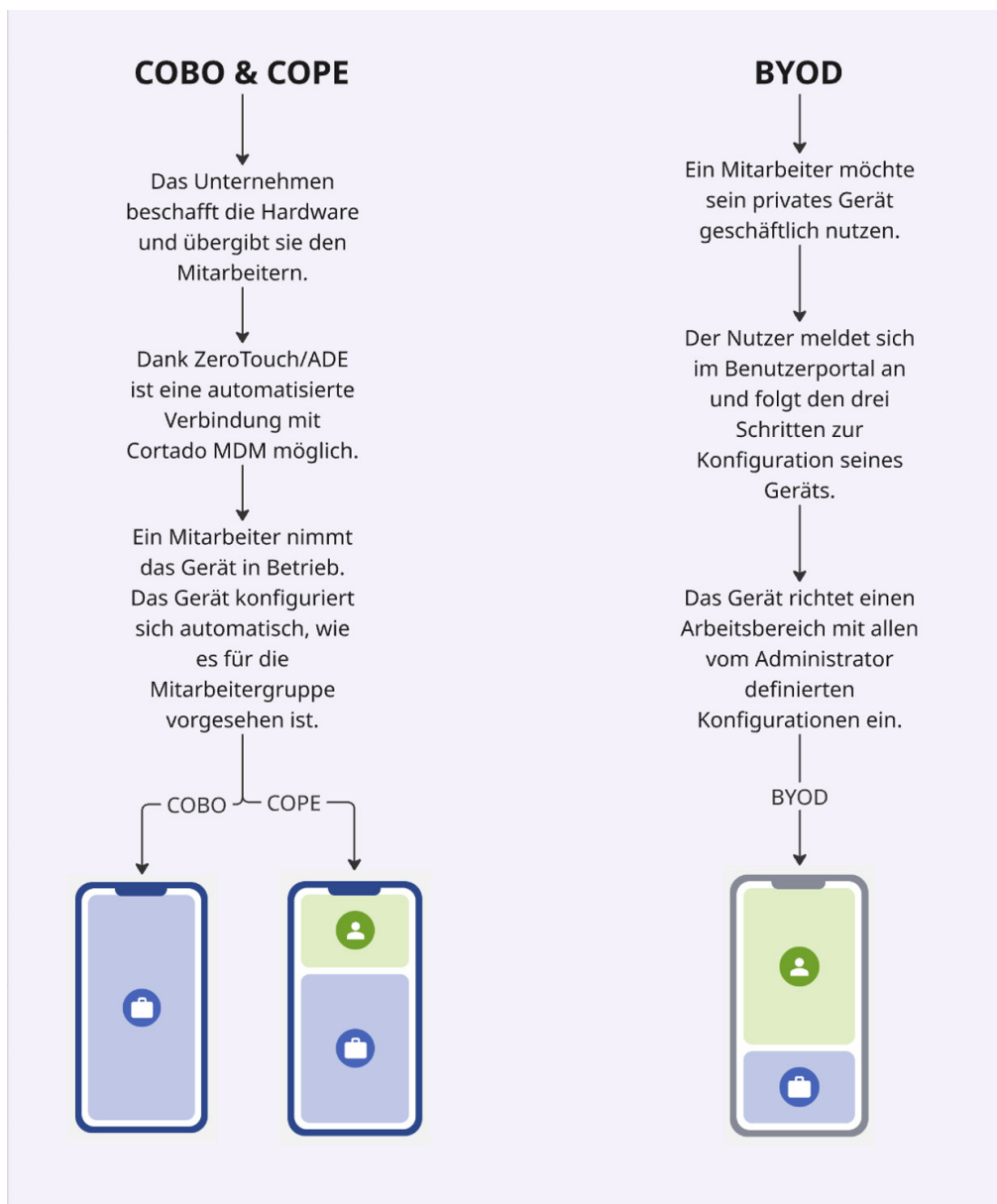


Abbildung 6 Beispiel des Enrollment-Prozesses für neue Geräte mit Cortado

Nutzervereinbarung / Richtliniendokument

Oft sinnvoll – und in vielen Unternehmen obligatorisch – ist eine Nutzungsvereinbarung oder aktualisierte IT-Richtlinie für mobile Geräte. Darin wird geregelt, was Mitarbeiter mit den Geräten tun dürfen und was nicht, welche Maßnahmen zur Einhaltung der Richtlinien ergriffen werden und welche Konsequenzen bei Verstößen drohen.

Diese Vereinbarung sollte idealerweise von allen Mitarbeitern akzeptiert werden – sei es im Intranet oder direkt auf dem Gerät im Rahmen des Enrollment-Prozesses. Arbeiten Sie dabei eng mit der Personalabteilung, dem Betriebsrat sowie der Rechtsabteilung zusammen, um sicherzustellen, dass das Dokument klar formuliert und rechtskonform ist.

Cortado stellt passende Musterverträge für die Konzepte COBO, COPE und BYOD bereit. Diese Vorlagen ersparen Ihnen viel Zeit und Kosten in der Rechtsabteilung oder bei externen Beratern und können im Handumdrehen an die spezifischen Rahmenbedingungen Ihres Unternehmens angepasst werden.

In Summe stellen Sie in dieser Phase sicher, dass **alle Beteiligten gut vorbereitet** sind, wenn der eigentliche Rollout startet. Die Investition in Schulung und Dokumentation zahlt sich aus – durch weniger Fehlern, höherer Akzeptanz, schnellere Umsetzung und eine effizientere Nutzung des MDM-Systems. So wird Ihre Organisation befähigt, den Wechsel bzw. die Einführung mit minimalen Reibungsverlusten zu meistern.

9. Rollout planen und durchführen

Nun kommt der entscheidende Schritt: Der **flächendeckende Rollout** der Cortado-MDM-Lösung auf alle vorgesehenen Geräte. Mit den Erkenntnissen aus der Pilot-Phase gilt es, den Übergang für die breite User-Basis möglichst reibungslos zu gestalten.



Rollout-Strategie festlegen

Entscheiden Sie sich für eine geeigneten Rollout-Strategie:

- **Schrittweise in Wellen** – empfohlen bei größeren Umgebungen
- **Flächendeckender Rollout** für alle auf einmal – nur in Ausnahmefälle ratsam

Bei mehreren tausend Geräten empfiehlt sich ein *phasenweiser Rollout*, z. B. nach Abteilungen oder Standorten in mehreren Wellen. So kann das IT-Team größere Mengen schrittweise bewältigen, aus jeder Welle lernen und Optimierungen direkt umsetzen. Legen Sie die Kriterien für einen Ablaufplan fest, zum Beispiel:

- 100 Geräte pro Woche
- Start mit der Zentrale, anschließend die Niederlassungen.
- Erst alle iOS-Geräte, dann Android-Geräte (falls separate Betreuung nötig).

Diese Planung sollte im Projektplan detailliert abgebildet sein.

Kommunikation im Vorfeld

Informieren Sie jeden betroffenen Nutzer rechtzeitig über den anstehenden Rollout – am besten *personalisiert* oder zumindest zielgruppenspezifisch. Bereits einige Wochen vor dem Termin sollten die Nutzer wissen, was auf sie zukommt:

„Sehr geehrte/r Herr/Frau X, am TT/MM/JJJJ wird Ihr Dienst-Smartphone in unser neues Mobile Device Management aufgenommen.“

Erläutern Sie nochmals kurz den Nutzen und die wichtigsten Punkte der Nutzeranleitung. Diese Vorabinformation bereitet die Leute mental vor und verhindert Überraschungen. Erinnern Sie kurz vor dem Stichtag erneut – inklusive Hinweisen zum Sichern persönlicher Daten, falls z.B. das Gerät komplett neu aufgesetzt wird (bei BYOD selten nötig, bei Firmengeräten evtl. in Austauschaktionen).

Durchführung des Rollouts

Setzen Sie den ausgearbeiteten Plan konsequent um.

- Bei firmeneigenen Geräten kann der Rollout oft remote erfolgen, indem Sie den Nutzern Einladungslinks schicken.
- Bei neuen Geräten oder Tauschgeräten nutzen Sie idealerweise die automatische Provisionierung, z. B. via Apple ADE oder Android Zero Touch.

Auch Vor-Ort-Unterstützung kann in manchen Fällen sinnvoll sein – etwa bei weniger technikaffinen Nutzern. Hier lohnt es sich, Rollout-Tage zu veranstalten, wo IT-Mitarbeiter beim Einrichten der Geräte helfen. Denkbar ist beispielsweise „MDM-Helpdesk“ in einer Filiale einrichten, an dem Mitarbeiter innerhalb eines Zeitfensters ihre Geräte vorbeibringen, um diese zu registrieren. Passen Sie die Methode Ihrer Unternehmenskultur an.

Controlling während des Rollouts

Überwachen Sie die Fortschritte aktiv: Wie viele Geräte haben sich erfolgreich angemeldet? Wo treten Fehler auf? Seien Sie bereit, bei Abweichungen schnell zu reagieren. Wenn etwa plötzlich für 50 Geräte eines Typs Fehler gemeldet werden, untersuchen Sie das sofort – vielleicht gibt es ein Problem seitens des Geräte-Herstellers.

Halten Sie außerdem engen Kontakt mit dem Support-Team, um Probleme zu lösen. Planen Sie tägliche *Meetings* im Team, um den Rollout-Verlauf zu besprechen und ggf. Optimierungsmaßnahmen abzuleiten. Halten Sie auch hier die enge Zusammenarbeit mit dem MDM-Hersteller aufrecht, um im Bedarfsfall schnell Hilfe zu bekommen.

Flexibilität bewahren

Trotz ausgiebiger Vorbereitung können unvorhergesehene Hindernisse auftreten. Bleiben Sie flexibel und passen Sie den Rollout-Plan bei Bedarf an. Wenn zum Beispiel in der ersten Welle des Rollouts größere Probleme auftauchen, zögern Sie Welle 2 hinaus, bis die Probleme gelöst sind. Kommunizieren Sie Änderungen transparent an alle Stakeholder.

Folgen Sie dem Grundsatz Qualität geht vor Geschwindigkeit, Es ist immer besser, den Rollout-Prozess, um eine Woche zu strecken als hunderte unzufriedene Nutzer mit unlösbaren Problemen und nicht funktionierenden Geräten zu überrollen.

Abschluss und Übergabe

Sobald alle vorgesehenen Geräte eingebunden sind, gilt der Rollout als abgeschlossen. (Feiern Sie diesen Meilenstein ruhig – das Team hat eine große Leistung erbracht!)

Planen Sie – sofern der Rollout von einem separaten Projektteam durchgeführt wurde – die Übergabe an das Betriebsteam. Dabei gilt es, alle offenen Punkte zu dokumentieren, relevante Informationen vollständig zu übergeben und sicherzustellen, dass keine offenen Themen zurückbleiben – etwa bewusst ausgenommene Geräte oder sonstige Sonderfälle.

10. Betrieb und Monitoring etablieren

Sind alle geplanten Geräte in das MDM-System eingebunden, wechselt der Fokus vom Projekt zum **laufenden Betrieb**. Nun heißt es, die Umgebung stabil zu halten, die Sicherheit kontinuierlich zu gewährleisten und Prozesse für den täglichen Umgang mit den Geräten zu etablieren.

Monitoring von Compliance und Sicherheit

Richten Sie im Cortado-System Berichte ein, die den Status aller Geräte übersichtlich darstellen. Wichtige Kennzahlen sind etwa:

- Zeitpunkt der letzten Verbindung der Geräte
- Ausstehende OS-Updates
- Fehlgeschlagene Policy-Pushs

Legen Sie Verantwortlichkeiten fest: Wer kontrolliert die Reports täglich oder wöchentlich? Wer reagiert auf Auffälligkeiten? Das Security-Team sollte bei sicherheitsrelevanten Alerts (z. B. *Gerät XYZ wurde als verloren gemeldet*) immer involviert sein.

Incident-Management

Entwickeln Sie klare **Prozesse für Sicherheitsvorfälle** im mobilen Bereich. Ein typisches Beispiel ist der Geräteverlust oder -Diebstahl. Bei vielen Cortado-Kunden sieht der Ablauf wie folgt aus:



Abbildung 7 Prozess bei Geräteverlust/Diebstahl

Klare Regeln helfen hier:

- Ab wann gilt ein Gerät als verloren oder gestohlen?
- Wer gibt die Freigabe zur Datenlöschung?

Testen Sie diese Abläufe regelmäßig in der Praxis, z.B. durch Simulation eines verlorenen Geräts.

Denken Sie auch an **Notfallpläne**: Da es sich bei Cortado um eine Cloud-Lösung handelt, müssen Sie sich nicht selbst um die Backups der MDM-Datenbanken kümmern – diese werden von Cortado durchgeführt. Sollten die MDM-Server von Cortado einmal nicht erreichbar sein, hat diese keinen unmittelbaren Einfluss auf den Betrieb der Geräte, diese bleiben funktionsfähig. Lediglich das Hinzufügen neuer Geräte oder das Senden von neuen Befehlen an die Geräte wäre in solch einem Ausnahmefall nicht möglich.

Updates und Wartung

Die Cortado-MDM-Lösung ist vollständig cloudbasiert (SaaS). Updates und Patches werden automatisch vom Anbieter eingespielt – Sie müssen keine Infrastruktur selbst pflegen.

Auf den mobilen Geräten sollten Betriebssystem-Updates ebenfalls zügig verteilt werden. Cortado unterstützt hier die automatisierte Verteilung, inklusive zeitgesteuerter Rollouts. Nutzen Sie diese Funktion, um Sicherheitsupdates schnell bereitzustellen.

Bei größeren OS-Upgrades (z. B. iOS 18 auf iOS 19) empfiehlt es sich, kontrolliert in Wellen zu aktualisieren – insbesondere, wenn Kompatibilitätstests erforderlich sind. Automatisieren Sie den Update-Prozess so weit wie möglich (z. B. nächtliche Updates), um eine hohe Patch-Compliance zu erreichen.

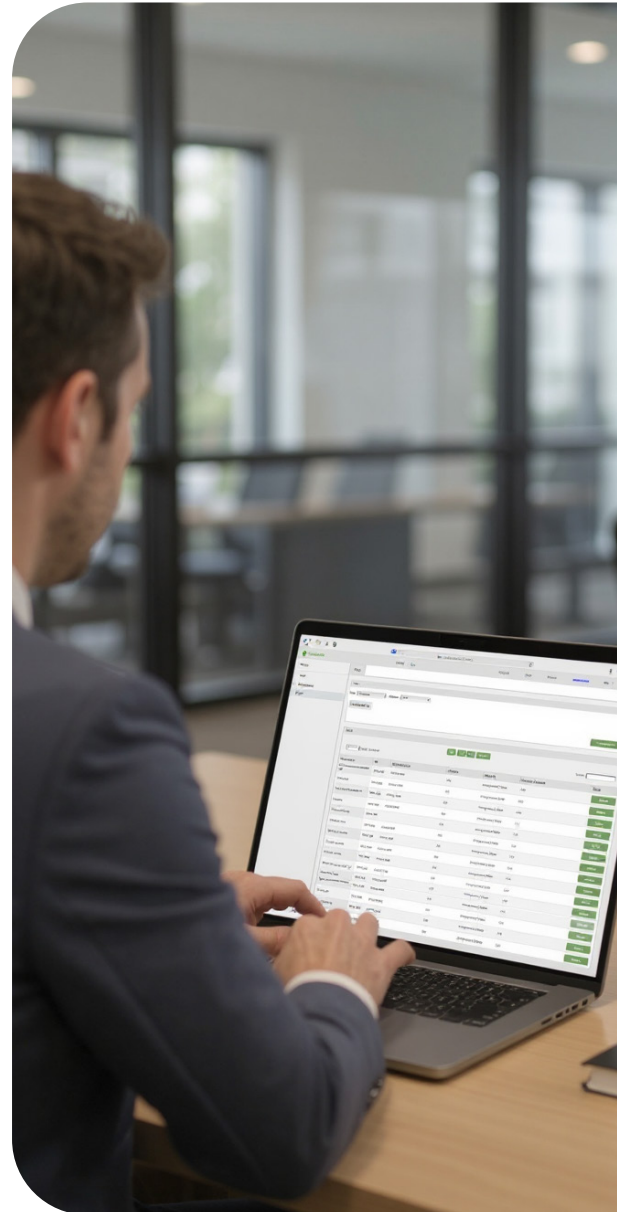
Erfahrungswerte zeigen: Automatisierte, regelmäßige Updates können die Update-Quote von rund 67 % auf über 95 % steigern.

Regelmäßige Audits

Führen Sie in festen Intervallen (z. B. quartalsweise) **Überprüfungen der MDM-Einstellungen** und der Geräte durch.

- Stimmen die Policies noch mit den Unternehmensvorgaben überein?
- Sind alle neuen Mitarbeitergeräte bereits eingebunden – oder gibt es „blinde Flecken“?

Gerade in regulierten Branchen und KRITIS-Umgebungen können MDM-Audits ein Pflichtbestandteil von IT-Sicherheitsprüfungen sein. Dokumentieren Sie die Ergebnisse und leiten Sie Korrekturmaßnahmen ein.



KPIs und Reporting

Etablieren Sie Key Performance Indicators für Ihr Mobile Device Management. Beispiele:

- Anteil verwalteter Geräte im Verhältnis zur Gesamtzahl
- Durchschnittliche Bereitstellungszeit für neue Geräte
- Anzahl sicherheitsrelevanter Vorfälle pro Quartal,
- Benutzerzufriedenheit mit dem Support (z.B. anhand von Ticket-Bewertungen)

Berichten Sie diese KPIs regelmäßig an das Management, um den **Wert der MDM-Lösung** zu belegen. Beispiele:

- „Seit Einführung von Cortado gab es keine Datenverluste mehr bei Geräteverlust.“
- „Das Onboarding eines neuen Mitarbeiters dauert seit der Einführung von Cortado nur noch Minuten statt Tage.“

Stetige Verbesserung im laufenden Betrieb

Der Betrieb eines MDM-Systems ist kein statischer Zustand. **Passen Sie Richtlinien und Prozesse kontinuierlich an**, wenn sich Anforderungen ändern. Zum Beispiel können neue Bedrohungen strengere Sicherheitsvorgaben erfordern), oder das Benutzerfeedback Anlass für pragmatische Lockerungen bieten.

Denken Sie immer daran, dass MDM-Teil einer *übergeordneten Sicherheitsstrategie* ist – und kein Selbstzweck. Es sollte mit Maßnahmen Zero-Trust-Architekturen oder Multifaktor-Authentifizierung (MFA) verzahnt sein. Auch diese Weiterentwicklungen sollten sich in der Mobile-Policy widerspiegeln.

Durch ein wachsames Monitoring und eine vorausschauende Wartung stellen Sie sicher, dass das MDM-System seinen Zweck erfüllt: **Geräte und Daten dauerhaft zu schützen**, ohne den Geschäftsbetrieb einzuschränken. Gleichzeitig geben Sie dem Unternehmen die Möglichkeit, mobil und agil zu arbeiten.



Tipp: Cortado bietet [regelmäßige Webinare](#) an, um neue Funktionen und Anwendungsfälle zu demonstrieren. Nutzen Sie diese als Inspirationsquelle, um Ihre Umgebung weiter zu optimieren und Ihren eigenen Anwendungsfall abzustimmen.

11. Review & Optimierung

Nach Abschluss des Projekts und einer gewissen Laufzeit im produktiven Betrieb ist es Zeit für ein **Resümee** und die kontinuierliche Weiterentwicklung der Lösung. Denn: In der IT ist kein Projekt je wirklich „abgeschlossen“ – Anforderungen und Technologien verändern sich ständig. Als vorausschauende IT-Leitung sollten Sie daher regelmäßige Reviews und Optimierungszyklen einplanen.

Projekt-Nachbetrachtung

Führen Sie ca. 1 – 2 Monate nach dem Rollout ein **Lessons-Learned-Meeting** mit dem Projektteam und dem MDM-Anbieter durch. Reflektieren Sie offen: Was lief gut in der Einführung, was hätte besser laufen können?

Dokumentieren Sie Ihre Erkenntnisse für zukünftige Projekte. Vielleicht war die Pilotphase zu kurz angesetzt, oder die frühzeitige Einbindung der Fachabteilungen und des Betriebsrats hat sich als besonders wertvoll erwiesen.

Und: Feiern Sie auch Ihre Erfolge! Etwa, dass die ersten 1.000 Geräte innerhalb weniger Wochen erfolgreich eingebunden wurden – und die Unternehmensdaten nun deutlich besser geschützt sind.

Zielabgleich

Vergleichen Sie die aktuellen Ergebnisse mit den Zielen aus Phase 1 – idealerweise anhand messbarer Kennzahlen. Beispielsweise:

- „100% der Geräte sind verschlüsselt und mit Passcode geschützt.“
- „Das Geräte-Inventar ist stets aktuell und vollständig.“

Wenn Ziele nicht erreicht wurden, analysieren Sie die Ursachen, ob es sinnvoll ist, Maßnahmen nachzuziehen oder Ziele nachzujustieren.

Weiche Ziele wie „höhere Mitarbeiterzufriedenheit“ lassen sich ggf. mit gezielten Umfragen erfassen.

Endbenutzer-Feedback und Akzeptanz

- Nach einigen Monaten Betrieb lohnt sich eine **Mitarbeiterbefragung** gezielt zum Thema MDM.
- Wie bewerten die Nutzer die Lösung?
- Gibt es Verständnisprobleme oder Verbesserungsvorschläge?



Solches Feedback zeigt Optimierungsbedarf – etwa in der Kommunikation, in den Schulungsunterlagen oder bei gesperrten Funktionen. Vielleicht fehlt vielen Nutzern eine bestimmte App, die blockiert war – sofern vertretbar, kann diese nachträglich freigegeben werden.

Positives Feedback wiederum kann helfen, den Nutzen intern zu belegen – etwa durch Zitate in Management-Reports oder Success Storys im Intranet.

Technische Optimierung

Überprüfen Sie regelmäßig Ihre MDM-Konfiguration:

- Gibt es neue Funktionen oder Module von Cortado, die zusätzlichen Nutzen bieten?
- Gibt es neue Schnittstellen oder Integrationen, die Effizienzgewinne ermöglichen?

Bleiben Sie technisch am Ball – Cortado entwickelt sich kontinuierlich weiter, und oft lassen sich neue Potenziale schnell erschließen.

Policies anpassen

Nutzen Sie die im Betrieb gewonnenen Daten, um **Ihre Richtlinien gezielt zu verfeinern**. Beispiele:

- **Wird die Gerätekamera kaum noch benötigt?** Ziehen Sie in Erwägung, diese standardmäßig zu sperren, um das Risiko von Foto-Lecks zu minimieren
- **Ist die Pflege einer Blacklist sehr aufwendig?** Ziehen Sie einen Wechsel zu einer Positivliste (Allowlist) in Betracht.

Wichtig: Stimmen Sie größere Policy-Änderungen stets mit Datenschutz, Betriebsrat und ggf. der Rechtsabteilung ab. Führen Sie Neuerungen zunächst in einer Testgruppe ein, bevor Sie sie breit ausrollen.

Regelmäßiger Audit & Optimierungszyklus

Etablieren Sie letztlich einen **kontinuierlichen Verbesserungsprozess** für die Weiterentwicklung Ihres Mobile Device Management. Planen Sie:



- *Jährliche Strategie-Reviews mit dem Management*
- *Quartalsweise Technik-Reviews gemeinsam mit dem Admin-Team und Cortado zur Feinjustierung der Systemkonfiguration*
- *Laufendes Monitoring – wie in Phase 10 beschrieben.*

So stellen Sie sicher, dass Ihre MDM-Strategie mit der dynamischen Mobile-Landschaft Schritt hält – und dass Ihre Organisation das volle Potenzial der Lösung ausschöpft.

Fazit

Ein erfolgreich eingeführtes MDM-System ist ein echter **Enabler** für moderne, mobile Arbeitsweisen. Wenn Sie den in diesem Leitfaden beschriebenen Weg gehen – von der klaren Zieldefinition über die saubere technische Basis bis hin zu Schulung, Betrieb und kontinuierlicher Optimierung – positionieren Sie sich als **Thought Leader in Ihrem Unternehmen** und Praktiker zugleich.

Sie zeigen, dass hohe Sicherheit und Benutzerfreundlichkeit kein Widerspruch sein müssen –, sondern bei planvollem Vorgehen Hand in Hand gehen. So wird Ihr MDM-Projekt nicht nur ein IT-Erfolg, sondern ein Gewinn für das gesamte Unternehmen!

Und das Beste: Sie sind nicht allein!

Wir bei Cortado begleiten seit vielen Jahren Unternehmen aller Größenordnungen und Branchen erfolgreich bei der Einführung ihrer MDM-Lösungen – von der Planung bis zum Rollout und darüber hinaus.

Gern teilen wir unsere Erfahrung mit Ihnen! Sprechen Sie uns einfach an – gemeinsam finden wir die effizienteste Lösung für Ihr Vorhaben und bringen Ihr Projekt sicher und schnell ans Ziel.



Lassen Sie uns gemeinsam den nächsten Schritt gehen.

Buchen Sie jetzt ein unverbindliches Gespräch mit unseren Cortado-Experten – ob zur Optimierung Ihrer bestehenden MDM-Umgebung, zur strategischen Planung eines Rollouts oder zur Klärung technischer Detailfragen.

Profitieren Sie von unserer Erfahrung aus zahlreichen Projekten und finden Sie gemeinsam mit uns die effizienteste Lösung für Ihr Unternehmen.

Headquarters
Cortado Mobile Solutions GmbH
Alt-Moabit 91 a
10559 Berlin, Germany
Tel.: +49 (0)30 408 198 500
Fax: +49 (0)30 408 198 501
E-Mail: info@cortado.de
www.cortado.de



Alle Namen und Warenzeichen sind Namen und Warenzeichen der jeweiligen Hersteller.

Folgen Sie Cortado auf:



facebook



twitter



youtube



linkedin