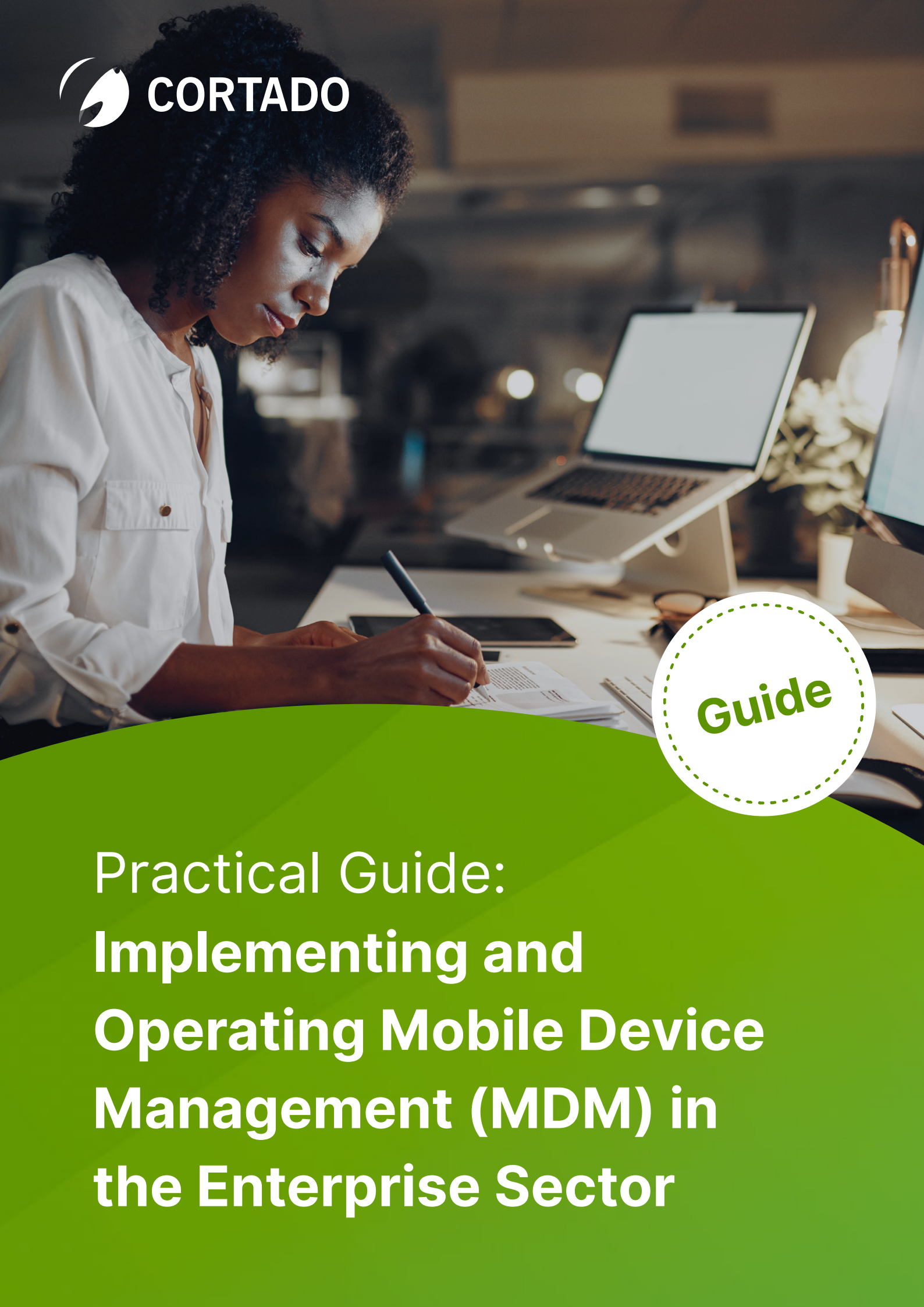




Guide

Practical Guide: Implementing and Operating Mobile Device Management (MDM) in the Enterprise Sector

Contents

Introduction.....	3
1. Defining Objectives and Framework Conditions	3
2. Defining Requirements.....	6
3. Market Analysis and Product Selection	7
4. Project Planning and Setting Up the Team.....	10
5. Preparing the Infrastructure	12
6. Defining Policies and Configurations	15
7. Conducting the Pilot Phase	18
8. Training and Documentation	20
9. Planning and Executing the Rollout.....	23
10. Establishing Operations and Monitoring	25
11. Review & Optimization.....	28
Conclusion.....	30

Introduction

For companies managing thousands or even tens of thousands of mobile devices, implementing a Mobile Device Management (MDM) system is essential to balance security, efficiency, and productivity.

However, setting up an MDM system is complex: technical requirements, organizational processes, and company-specific needs all have to be carefully aligned.

This guide walks IT managers and decision-makers step-by-step through every phase of an MDM project—from defining goals through implementation and on to ongoing operations. We present proven best practices and provide concrete recommendations, illustrated with real-world examples from Cortado MDM. We also highlight common pitfalls to avoid during planning and execution.

Following these steps will help ensure that Mobile Device Management is introduced in your company in a structured, cost-effective, and sustainable way.

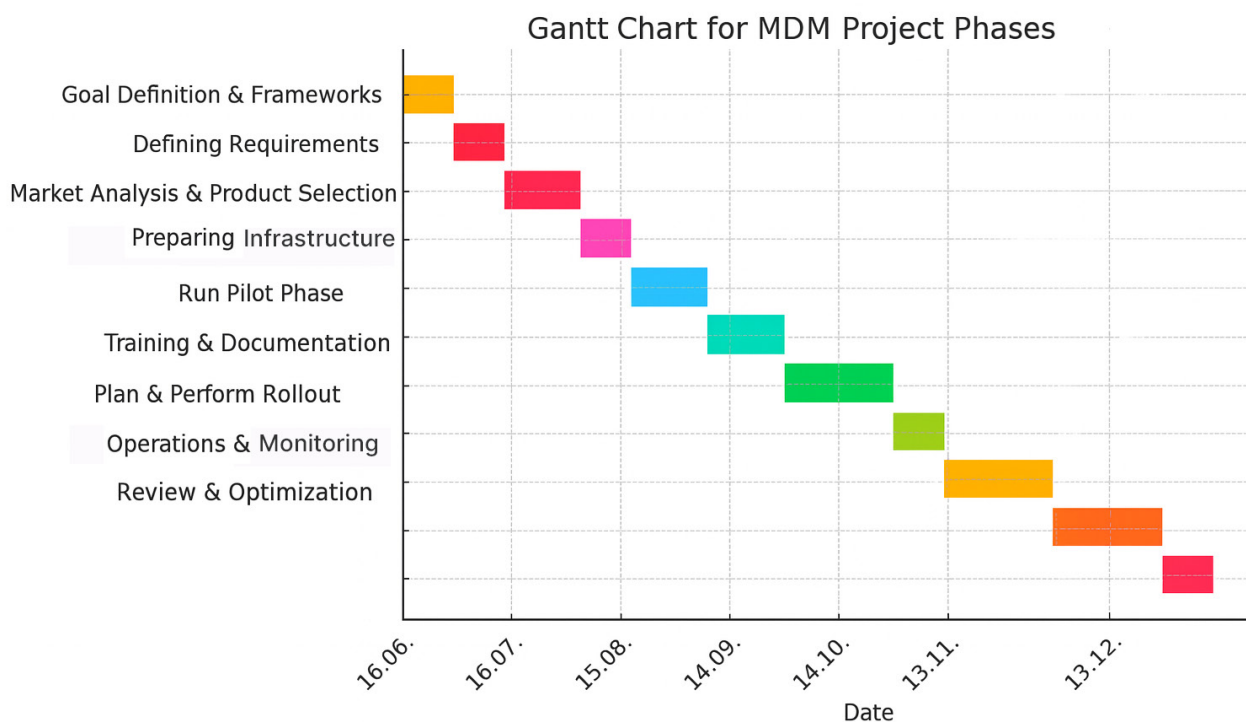


Figure 1 Overview of the phases of an MDM project from planning to ongoing operation (timeline)

1. Defining Objectives and Framework Conditions

Define your objectives

At the start of every MDM project, you need to establish a clear set of goals. Define why your company wants to introduce an MDM solution and what overarching business goals it is meant to support.

Common goals include, for example:

- **Increase IT security and compliance:** Protect sensitive corporate data on mobile devices and ensure adherence to regulations (e.g., GDPR, NIS2).
- **Streamline device management:** Centrally control settings, updates, and apps on all devices to reduce administrative workload.
- **Boost productivity and flexibility:** Support BYOD (Bring Your Own Device) without compromising security, and better support mobile employees in sales or service.
- **Control costs:** Reduce support expenses and avoid costly security incidents such as data breaches or device loss.

Involve stakeholders

Engage all relevant stakeholders from the very beginning. In addition to the IT department, this includes business units, company management, HR, legal/compliance, and, if applicable, data protection officers.

Early involvement of employees is essential so that they are informed from the start about clear separation mechanisms and privacy safeguards within the MDM system. This helps prevent later resistance over concerns about employee surveillance.

Clarify framework conditions together: What usage policies will apply? How will employee data and privacy be protected? (For example, by ensuring that private data on BYOD devices is not captured by the MDM.)

A consensus between IT, HR, legal, and employees about work-life balance, data protection, and usage policies forms the foundation for further planning.



Conduct an inventory

Before selecting a solution, document the current status. Create a **full inventory of the company's mobile device landscape**, noting:

- How many devices are in use, which device types (smartphone/tablet), and which operating systems (iOS, iPadOS, Android, eOS) and versions are being used.
- Where the devices are located and how they are used (e.g., strictly office use vs. field work).
- Ownership of devices: Are they all company-owned, or are employees already using personal devices (BYOD) for company data?

This process often reveals forgotten devices or shadow IT and creates a data foundation for all further steps (including budget planning).

Also identify technical framework conditions—especially existing IT infrastructure such as email systems, directory services (e.g., Microsoft Entra), certificate authorities, and network connections (VPN, WLAN) that need to be integrated into the MDM concept.

Make goals measurable

Decide which KPIs or criteria will measure the success of MDM implementation. For example:

- Within six months, 100% of company devices are registered in the MDM.
- Security policies (password, encryption, etc.) are enforced on 100% of devices.

Other possible success indicators include reducing incidents (e.g., lost devices without remote wipe) or saving time when onboarding new devices. Such metrics help evaluate results later and form the basis for systematically measuring goal achievement and the ROI of the MDM project (see Phase 11).



2. Defining Requirements

Once the “why” is clear, the next step is the “what”: Gather and document **detailed requirements** for the MDM solution. Use your previously defined goals and the device inventory as a reference. Key aspects include:

- **Supported device types and platforms:** Ensure all relevant operating systems are covered (typically iOS, Android). Large environments usually have a mix of platforms. Note any specific requirements, such as support for devices without Google services, if applicable.



Tip: Not all devices are designed or suitable for corporate use. Especially for Android, check Google’s [Android Enterprise Recommended list](#). This provides useful information such as guaranteed update timelines for devices.

- **Usage and ownership models:** Define which scenarios must be supported—company-owned, business-only devices (COBO) vs. BYOD. If BYOD is allowed, the MDM must offer features to separate business and private data (containerization, dual profiles, etc.) and ensure data privacy. You may also need support for COPE (Corporate-Owned, Personally Enabled) devices—company-owned devices used privately, which have similar requirements to BYOD.
- **Core MDM features:** Decide which core functions are a priority. Typical MDM functions include device inventory, remote configuration of settings/profiles, enforcement of security policies (password requirements, encryption, etc.), app distribution and management, and remote device lock/wipe. Consider whether you need kiosk mode (for single-use or specialized devices). Note reporting and dashboard requirements for tracking device status and policy violations.



- **Integration with existing systems:** An MDM rarely runs in isolation. Define integration needs, such as directory services (e.g., Entra ID for user synchronization), email servers (e.g., Exchange Online for corporate email access), certificate infrastructure (for WLAN, VPN), and API connections for automation or specialized applications.
- **Security and compliance requirements:** Derive specific MDM requirements from corporate policies or legal mandates. Examples: device encryption support, strong passcodes (complexity rules), multi-factor authentication for critical apps, enforced VPN usage, business app allow/deny lists. If relevant, the MDM must hold certain certifications (e.g., ISO 27001, BSI baseline protection).
- **Support requirements:** Decide what level of support you need. For more than 1,000 devices, direct support from the vendor is essential. Define if time-critical features are needed (e.g., remote lock within minutes of theft) and whether the system needs alerting mechanisms. Plan for scalability (can the solution handle 10,000+ devices in the future?) and multi-tenancy if you manage multiple business units separately.

Work with stakeholders to develop these requirements. Involve business unit representatives to uncover specific needs—for example, sales teams may require quick mobile access to marketing collateral (content management functions), while engineering teams may value developer-friendly policies. Document all requirements in writing, such as in a requirements specification or checklist. This list will be your evaluation baseline in the next phase.

3. Market Analysis and Product Selection

The MDM market is diverse: ranging from complex enterprise suites to specialized tools. But the biggest solution isn't always the best. What matters is finding a system that fits your IT landscape, security requirements, and organizational processes.

Use your defined requirements to create a thorough list of potential solutions. Sources for market research can include platforms like Capterra or OMR, industry articles, case studies from other companies, and consulting from system integrators.

It's crucial to choose a solution that not only fits technically but also comes with the vendor support you need. Especially for large projects with more than 1,000 devices, vendor expertise and quality of support are critical success factors. Ideally, the vendor should also offer support in German for German-speaking teams.

Evaluation criteria

Compare solutions using **objective criteria**, such as:

- **Feature coverage:** Does the tool meet all your "must-have" requirements (see the function list from Phase 2)? Where are there gaps?
- **Ease of use:** Is the admin interface intuitive? Are there automated workflows like zero-touch provisioning for new devices? Is the solution available in German? A steep learning curve and complicated operation can make ongoing management harder.

- **Platform support:** Does the solution reliably support all desired device types and OS versions? Not all MDMs handle BYOD and COPE equally well.
- **Security and compliance:** What security features are included? Does the solution have remote wipe capabilities, compliance templates for GDPR, encryption, and containerization support? Does it provide reports and audits that meet the needs of data protection officers or auditors?
- **Integration:** Can the MDM integrate with your IT environment? Common needs include Entra ID authentication, APIs for automation, and single sign-on.
- **Scalability and performance:** Look for references or reviews from similarly sized installations. The solution should handle 10,000+ devices if growth is expected—and without performance issues.
- **Cloud operating model:** Decide whether a cloud-based solution is a possibility. Cloud MDM (SaaS) offers advantages like scalable infrastructure and reduced internal operational overhead, as no updates or on-premises infrastructure are needed. Pay special attention to the hosting location; if it's in Germany, meeting GDPR and NIS2 requirements is far simpler.
- **Cost model:** Compare the total cost of ownership (TCO). Consider license costs—typically per device, often tiered by feature set—plus ongoing support and update fees. Watch out for hidden costs, like extra fees for modules or add-ons. Some vendors charge extra for key support services or security features, turning a “cheap” solution into an expensive one.

MDM



Product testing and PoC

Narrow your list to a shortlist (e.g., 2–3 solutions) and, if possible, arrange test deployments. Many vendors offer free trials or pilot programs. Use them to test solutions with real devices in your environment.

Check in particular:

- Does the product meet core requirements?
- How easy is it to operate in practice?
- Do any unexpected issues occur?

A short pilot with a small user group before making a final purchase decision can give valuable insight into practical usability.

It's also wise to contact vendor reference customers or review success stories—ideally from your industry or similar company size.

During testing, observe the support team's response times and solution quality carefully. A knowledgeable, accessible support team is key for resolving issues quickly and maintaining system availability in production. Also assess vendor communication in general. Since you're aiming for a long-term partnership, a smooth, fast communication flow can save you a lot of effort over time.

After gathering all the information, evaluate your options and choose a product. Often a clear favorite emerges that best meets your needs; price alone should not be the deciding factor.

Ensure long-term considerations are included: The chosen solution should have a roadmap that can grow with your mobility strategy.

Once the decision is made, secure budget approval if necessary and move into contract negotiations. Choosing the solution that best matches your business needs and IT environment is essential. Take your time with market analysis and selection—mistakes here can lead to costly problems later.



4. Project Planning and Setting Up the Team

Once you've decided on your MDM solution, the real project planning begins. Especially for large-scale rollouts with thousands of devices, multiple user groups, and potentially global locations, structured project management is essential. The following steps outline how to do this in practice, using [Cortado MDM](#) as an example.

Create a project plan

Define a detailed project plan with milestones for all upcoming phases. Common milestones include project kickoff, completion of infrastructure setup, policy definition, successful pilot, rollout start, rollout end, and project review.

Estimate realistically how long each project phase will take and build in buffer time for unexpected delays. Experience shows that an MDM project for 1,000+ devices can take anywhere from 6 to 12 months, depending on complexity.

Visualize the schedule in a Gantt chart or project timeline (see Fig. 1) and get early approval from relevant stakeholders.

Plan resources

Ensure you have sufficient personnel and budget for the project. Define a project budget that includes license costs, expenses for training, external consultants (e.g., from the vendor), hardware (e.g., new devices), and contingency funds.

Identify dependencies and prerequisites. For example:

- Do all devices need to be updated to a certain OS version before rollout?
- Do you need accounts for Apple Business Manager or Google Workspace integration?

Include these tasks early in your plan.



Project team and roles

Assemble a competent team to lead the MDM project. Typical roles in an MDM implementation project include:

Role	Responsibilities
<i>Project Sponsor (e.g., CEO, CTO, IT Director)</i>	Defines project mandate and goals, provides budget, supports escalations, represents project to executive leadership.
<i>Project Manager</i>	Manages the project day-to-day, plans and coordinates phases and tasks, monitors schedule and budget, liaises with all stakeholders, manages risks and communications, acts as central point of contact.
<i>MDM Architect / Technical Lead</i>	Translates requirements into technical implementation, designs MDM architecture, integrates it with IT systems, plans infrastructure (network, cloud setups), and leads technical deployment.
<i>MDM Administrator / Engineer</i>	Configures the MDM platform (policies, profiles, apps), tests functions in the pilot phase, troubleshoots issues, often becomes the main operator post-rollout.
<i>IT Security Officer (InfoSec/Compliance)</i>	Defines security policies and compliance requirements implemented via MDM (password policy, encryption, app approvals), continuously monitors adherence, evaluates risks.
<i>Data Protection Officer (optional)</i>	Advises on data protection issues, especially for BYOD & COPE, ensures GDPR compliance (e.g., no unauthorized employee monitoring).
<i>Network/Infrastructure Specialists</i>	Prepare necessary infrastructure: network access, firewall rules (e.g., for APNs/FCM), directory service integration. Ensure technical foundations work smoothly.
<i>Support/Helpdesk Lead</i>	Plans rollout and operational support strategy, defines user incident processes during and after rollout, coordinates end-user communications.
<i>Pilot User Representatives (Key Users)</i>	Represent end users in the pilot phase, provide feedback on usability, help identify acceptance issues early, later act as “multipliers” to support colleagues.

In smaller companies, roles may be combined (e.g., the IT director acts as both sponsor and project manager). Clear responsibilities are crucial – everyone should know who makes which decisions and who is accountable for what. Communicate the role assignments to all project members and stakeholders to set expectations.

Communication and change management

Plan internal communication from the outset. When many employees are affected, change management is essential: Highlight the benefits of MDM early—such as increased security, more efficient support, and the ability to use devices for both personal and business purposes (BYOD, COPE).

Address concerns openly, such as the issue of “surveillance.” Explain clearly what data is not collected. This point is more important than many expect, and Cortado provides extensive informational materials for this purpose.

A solid communication plan may include intranet updates, presentations at company meetings, FAQ documents, and other formats. This creates transparency, fosters acceptance, and minimizes resistance.

In summary, this phase lays the foundation: a realistic timeline, a capable team, and all necessary resources – setting the stage for successful implementation.

5. Preparing the Infrastructure

Before actual MDM setup begins, you need to put the technical infrastructure in place. In this phase, you prepare all systems and connections so the MDM platform can run smoothly.

Build the system architecture

For a cloud solution like Cortado, create an admin account in the cloud portal. Set up directory service integration (e.g., Entra) early so users and groups from your company directory are available in the MDM. Alternatively, you can import via CSV file.

Network configuration

Make sure all necessary firewall rules and network paths are configured so mobile devices can communicate with the MDM server.

Apple devices require access to the Apple Push Notification service (APNs) to receive MDM push notifications. Android devices use Google Firebase Cloud Messaging (FCM) and require specific open ports for notifications. If these ports and addresses are blocked, you won't be able to wake or communicate with devices.

We recommend sketching communication paths in an architecture diagram – showing devices, push services, MDM server, and internal systems – to ensure nothing is overlooked.¹

¹ General Apple Ports: <https://support.apple.com/en-us/103229>
Apple devices directly in corporate networks: <https://support.apple.com/en-us/101555>
Android: <https://support.google.com/work/android/answer/10513641?hl=en&sjid=7639552788236774933-EU>

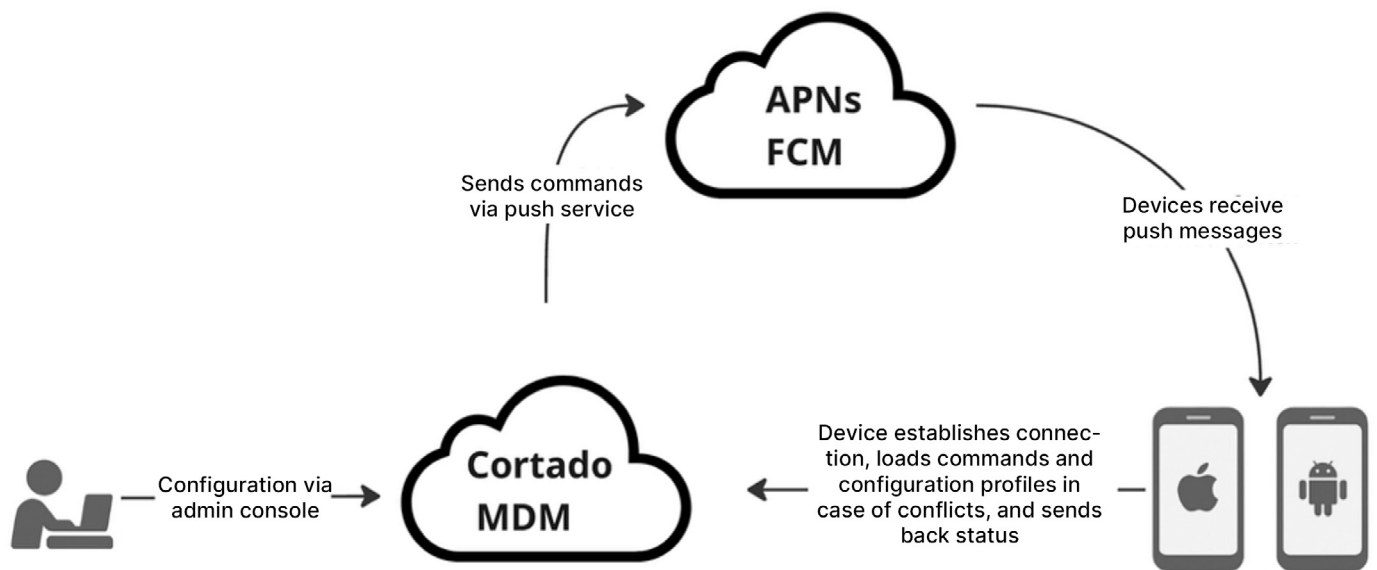


Figure 3 Example of the Cortado MDM system architecture (simplified)

Vendor accounts and certificates

Set up required vendor accounts. For Apple devices, you need an Apple Business Manager (ABM) account and must create an APNs certificate, which you upload to the MDM console. This allows the Cortado MDM server to sign APNs messages and manage devices.

For Android devices, you must set up Android Enterprise – either via a free business account for this purpose or by integrating with an existing company Google Workspace.

Also ensure you have all required certificates and tokens, such as the Apple DEP/ABM token or a VPP token for app distribution if used.

Cortado provides detailed step-by-step instructions for this process.

Prepare integrations

If your MDM will integrate with external systems, set up the connections, such as:

- Email system (Exchange/Office 365) via OAuth if Cortado will manage mobile email access.
- PKI integration for automatic certificate distribution, e.g., device certificates for WLAN access.
- Identity provider integration for SSO profiles, such as SAML/OAuth with Entra.

Depending on the tool, these steps may be technical—perform them carefully and test each integration.

Test the infrastructure

Before large-scale rollout, verify that the basic infrastructure works. A simple smoke test can help: manually enroll a test device into the MDM and check whether it can connect to the server, receive configuration profiles, sync a test email, and install apps.

Catching misconfigurations in network settings, certificates, or integrations at this stage prevents larger rollout issues.



Tip: Ask your MDM provider for best practices from similar projects. [Cortado](#) offers a detailed manual (in German and English, with video tutorials) and setup packages to support this stage. The base configuration for Cortado can be done in under two hours.



6. Defining Policies and Configurations

With the platform prepared, you can now design the specific policies, profiles, and configurations that will later be rolled out to devices. This is the core of the MDM project: here you decide how devices will be managed and what rules will apply.



Tip: Premium solutions like Cortado offer ready-made templates you can use as a basis for creating policies, so you don't have to start from nothing – this can greatly speed up the process.

Develop MDM policies

Based on your security and usage requirements (see Phase 2), create a set of MDM policies – rules and settings that the MDM system enforces on devices. Important policy areas include:

- **Security policies:** Examples include password requirements (minimum length, complexity), enforced device PIN, automatic lock after inactivity, lock screen text (e.g., with contact info in case of loss), maximum failed unlock attempts before data is wiped.
- **Restricting device functions:** Depending on the use case, certain features can be disabled. Examples: block camera use in sensitive areas, disable Bluetooth or USB ports, prevent cloud backups (to stop data from going to private clouds), or limit screenshots and copy-paste to the work profile in BYOD/COPE setups.
- **App policies:** Manage apps centrally. Decide which apps are allowed (whitelist) and block others (blacklist). Alternatively, provide a corporate app store. In Cortado, this is done via the Cortado app on the device. For certain groups, kiosk mode (only one or a few apps available) may be appropriate.



Tip: With Cortado MDM, apps can also be preconfigured and company-specific apps can be distributed in APK or IPA format.

- **Network and communication policies:** Require VPN for access to corporate networks, enforce automatic VPN use if needed, preconfigure WLAN profiles (with certificate authentication or username/password), and set up email profiles so users only need to enter their password or MFA code.
- **BYOD/COPE-specific settings:** For personal devices or company devices with personal use, enforce privacy rules – MDM must not access private data. Use a work profile or container to separate work and personal data. Communicate this clearly to build trust.

Security and usability must be balanced. Overly restrictive policies can harm productivity or face employee pushback. Policies should be tailored to different user groups rather than applied uniformly.

Consider user groups and roles

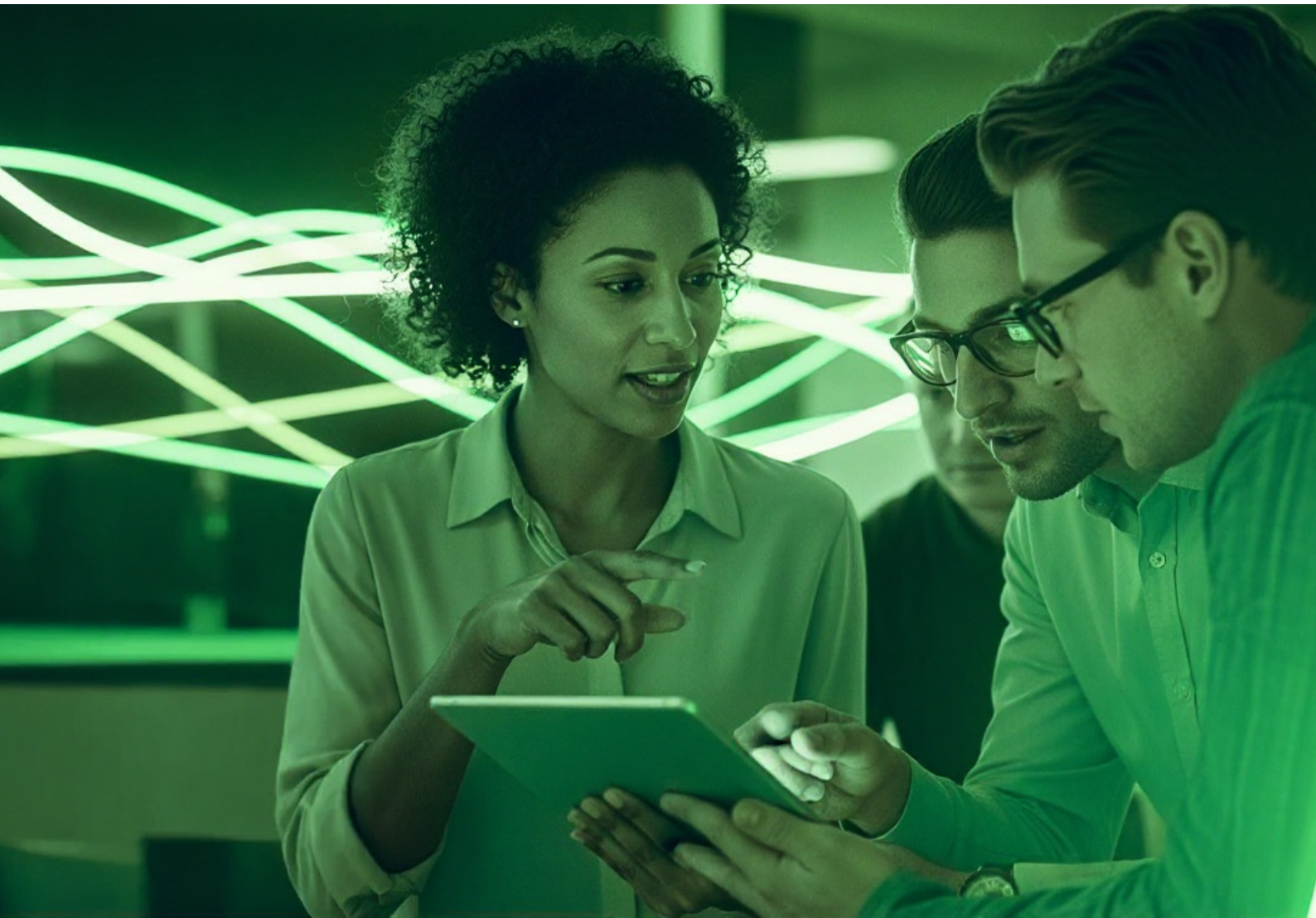
In Cortado MDM, you can create device/user groups (e.g., by department, location, job level) and assign different policies.

Example: Executives might have a broader app store or stricter security profiles due to access to sensitive data. Sales teams may need special documents preloaded for fieldwork.

Assign devices/users to groups during enrollment so the right policies are applied automatically. In Cortado, devices can belong to multiple groups, and the MDM will intelligently combine their policies.



Tip: With [Cortado](#), users and devices can also be assigned to multiple groups. The MDM then intelligently combines the individual policies of each group into one comprehensive one.



Example policy table

User group	Device type/use	Example policies
<i>Executives</i>	Company-owned	Full device management with highest security; strong passwords, encryption; camera and back-ups allowed; compliance reports to IT security; VIP exceptions for app installs with approval.
<i>Standard employees</i>	COPE	Passcode required, auto-lock after 3 mins; corporate apps preinstalled; additional apps only from approved store; cloud backups disabled for corporate apps; limited personal use allowed.
<i>Sales/Field staff</i>	Company-owned, specialized apps	Kiosk mode for business apps (e.g., CRM); corporate data access only via VPN.
<i>BYOD users</i>	Personal devices used for work	Light management: work profile for corporate data only; MDM can only access work container; only corporate container wiped in case of non-compliance; no location tracking.

These examples demonstrate how policies can vary depending on the group. Managers receive full access to required apps, while field staff devices may be more restricted (e.g., kiosk mode for a single tool). BYOD devices, on the other hand, are managed using minimally invasive means to protect privacy while still securing company data.

Cortado allows you to create such user roles with individual access rights and restrictions. You should use this granularity to design policies tailored to needs, rather than applying a one-size-fits-all approach.

Set up configuration profiles

Alongside policies, define configuration profiles in the MDM for specific device settings: WLAN profiles, email/Exchange profiles, VPN settings, and more. Preconfigured settings reduce support workload, prevent errors, and ensure uniform, secure device integration.



Test internally

Before the pilot phase, test policies and profiles internally with IT team devices. Assign distinct roles and verify that settings work as intended. Example: confirm that blocked device functions really don't work (kiosk test).

Adjust policies if needed. The goal is a consistent, practical rule set that delivers the required security without disrupting daily work.

Once policies and profiles are completed, the base configuration of your MDM system is complete. The next step is to test it in real-world conditions.

7. Conducting the Pilot Phase

An MDM solution should never be introduced with a “big bang” and no prior testing. A pilot phase is essential to validate the setup under real conditions and gather feedback. In this stage, you roll out the MDM to a controlled group.

Define the pilot group

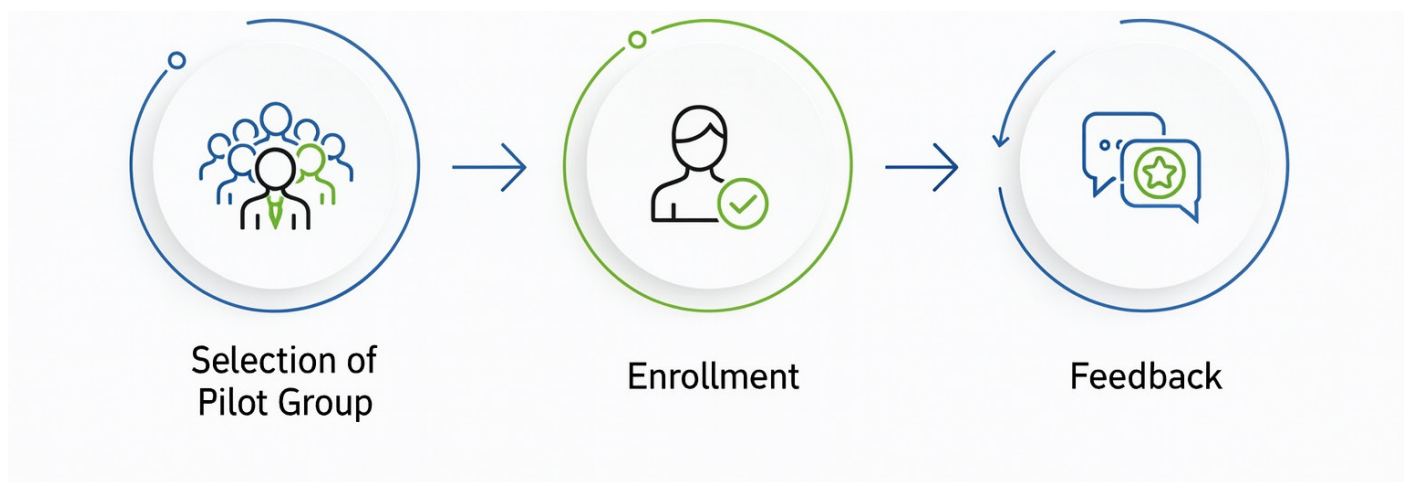


Figure 4 Pilot phase

Choose a representative pilot group – large enough to cover different scenarios but small enough to manage issues effectively. This is often a single department or 20–50 users.

Diversity is key: include different device types and platforms (e.g., iPhones and Android devices) and a variety of business areas. Many companies start piloting within the IT department because of higher technical expertise and faster support. It's important that pilot participants are open to the project and willing to give feedback.

Communicate with participants

Inform pilot participants clearly about the initiative. Explain that a new MDM solution is being introduced, what changes to expect (e.g., a new company app or certain restrictions), and who to contact with questions or problems.

Emphasize that feedback is welcome and that the pilot's purpose is to refine the setup. Provide short training or guides so users know, for example, how to register their device or what to do in case of loss.

Cortado supports this phase with a self-service portal and dedicated end-user instructions.

Device enrollment in the pilot

Enroll pilot devices into the MDM system. Enrollment methods vary depending on device type:

- **New, company-owned devices:** usually registered automatically via Apple DEP/ADE or Android Zero-Touch, arriving preconfigured for end users.
- **Existing or BYOD devices:** typically registered manually via an invitation link and self-service portal.

Ensure all devices appear in your MDM console. Cortado also offers an API to let you know by email when new devices are added.

This onboarding is the first real-world test – watch for problems like unreliable push notifications or error messages. Document the process and the time it takes (Cortado averages under 3 minutes per user).

Pilot operation and testing

Let pilot users work with managed devices for several weeks. Check whether policies are applied as intended. Spot-check compliance in the MDM console; any deviations should be intentional and approved.

Gather feedback on user experience: Are policies too restrictive? Are self-service features being used?

Also monitor technical performance: Do settings slow devices down? Are there battery drain issues? Do push notifications work promptly?

Pilot-phase support

Offer enhanced support during the pilot. The IT project team should be easy to reach (hotline, chat group, etc.) and track all issues.

For example, if users report unclear enrollment instructions, improve documentation before the full rollout. If a critical app is blocked, adjust policies.

Cortado provides close vendor support during this stage, drawing on experience from hundreds of successful projects.

Analyze feedback and optimize

Collect feedback throughout, but conduct a structured review at the end of the pilot. Use surveys or interviews to ask: How satisfied are users? What worked well? What didn't?

Use this input to fine-tune policies, fix problems, and update documentation. A successful pilot builds confidence for the main rollout and reduces the risk of unpleasant surprises—since critical issues have already been found and resolved.

8. Training and Documentation

Before starting the full rollout, prepare training and documentation – for both administrators/support staff and end users. Well-informed teams and educated users are key to a smooth transition into daily MDM operations.

Admin and IT training

Make sure the IT staff responsible for the MDM – including administrators and helpdesk/support—are thoroughly trained. Arrange vendor-led training sessions to build deep knowledge. Cortado offers various options, with participants receiving a certificate upon completion.

Admins should be confident in all platform functions – from creating new policies to troubleshooting connectivity issues.

Creating internal admin handbooks or knowledge base articles (e.g., “set up device for a new employee,” “wipe device on termination,” “check for compliance violations”) isn't strictly necessary with Cortado, since the solution includes extensive, freely accessible [documentation in both German and English](#). This ensures consistency and helps new team members onboard quickly.

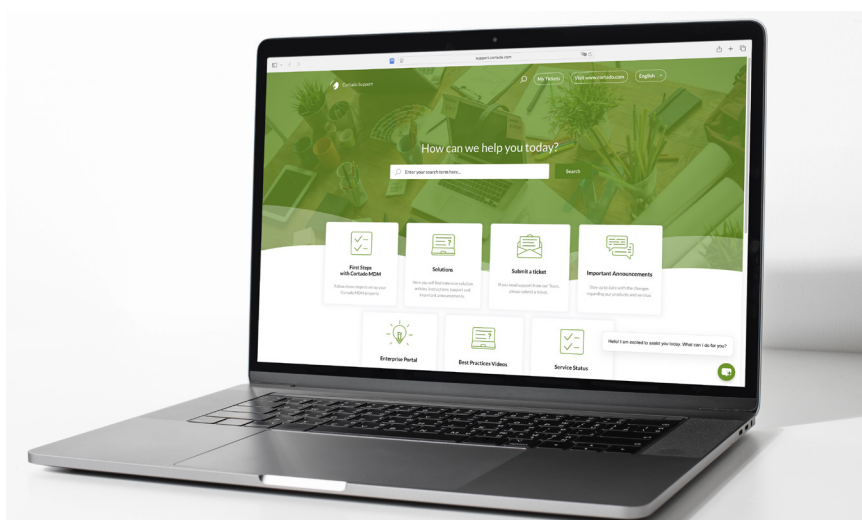


Figure 5 Cortado offers you a comprehensive knowledge base with helpful articles, step-by-step instructions, and practical solutions for common use cases.

End-user training and communication

Most employees don't need deep technical training – but they do need clear, simple instructions on what's expected and how to use their managed device correctly and securely.

Typical topics include:

- **How to register my device:** A step-by-step guide with screenshots prevents confusion during enrollment.
- **What does device management mean for me:** Explain what IT can access and what stays private—this builds trust and reduces concerns.
- **Who to contact for problems:** Provide clear support contacts (hotline or central email).
- **What rules I need to follow:** For example, no rooting/jailbreaking, follow policy guidelines to avoid compliance violations.

Avoid unnecessary technical jargon and keep the language straightforward.

Depending on your audience and the scope of changes, additional formats like short webinars, live demos, e-learning modules, or team kickoff sessions may be useful. Cortado can provide ready-to-use presentation slides and templates for these.

Prepare IT support

Bring your helpdesk fully up to speed: Support staff should be able to handle typical MDM issues such as:

- "I lost my device—what should I do?"
- "I can't install an app because MDM is blocking it."
- "My email stopped working after MDM enrollment."

Create standard operating procedures (SOPs) for these scenarios to enable quick 1st-level resolution.

For larger projects, consider a dedicated rollout support team to handle the higher ticket volume during the transition. The support team should maintain close contact with the vendor during this phase.

Document the system

Document the final MDM architecture, all settings, and active policies – including values. Keep track of access rights (e.g., who can be an MDM admin) and process descriptions (e.g., enrollment steps for new devices). Cortado’s reporting function provides much of this information automatically.

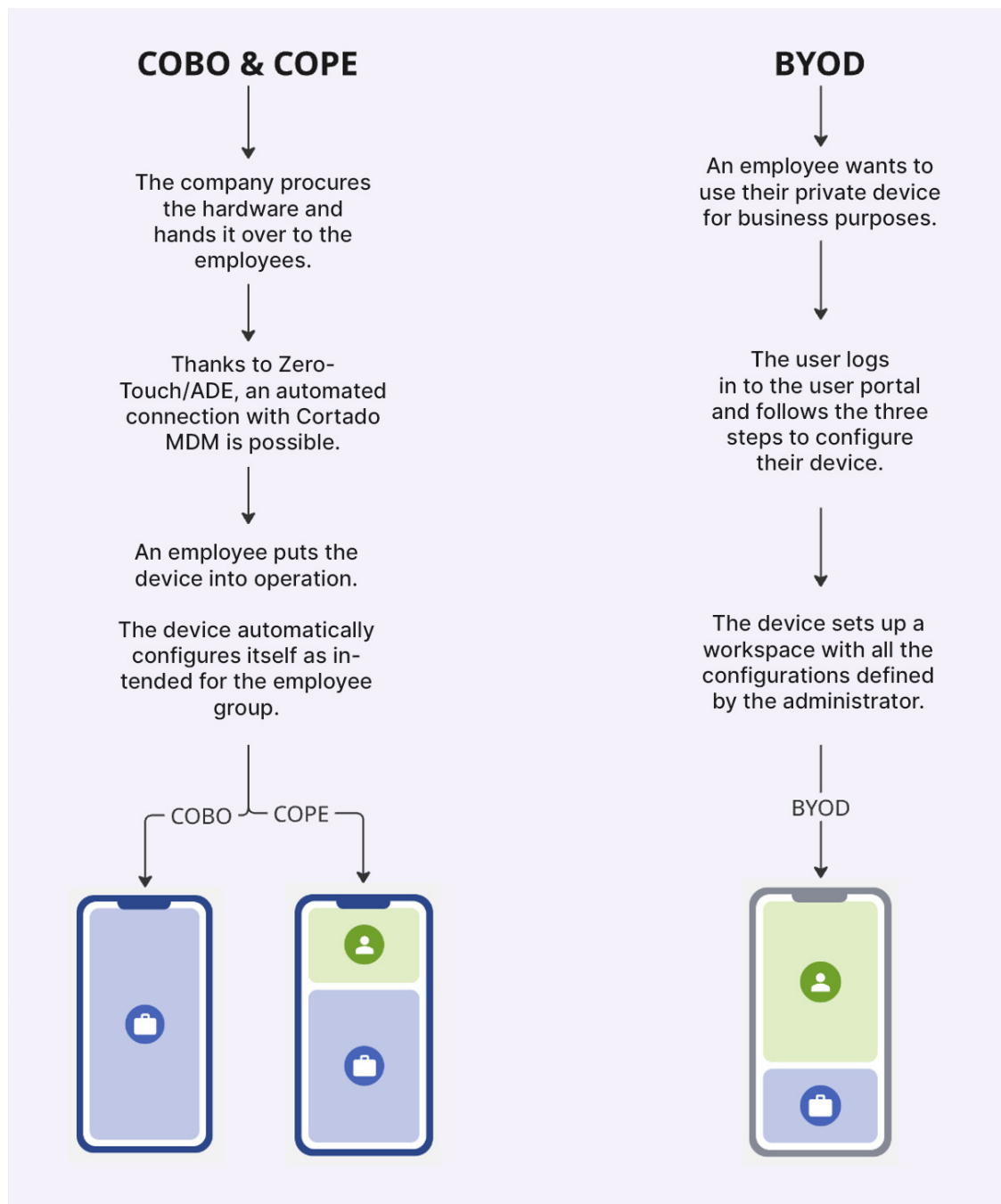


Figure 6 Example of the enrollment process for new devices with Cortado

User agreement/policy document

Many companies require a user agreement or updated IT policy for mobile devices. This defines allowed uses, enforcement measures, and consequences for violations.

Employees should ideally confirm acceptance – via the intranet or during device enrollment. Work with HR, the employee representatives and legal to ensure the document is clear and compliant.

Cortado offers a [template](#) for BYOD use cases, saving time and legal costs.

By the end of this phase, all stakeholders are prepared for the actual rollout. Investing in training and documentation pays off through fewer errors, higher adoption, faster rollout, and more efficient MDM use.

9. Planning and Executing the Rollout

Now comes the critical step: rolling out the Cortado MDM solution to all intended devices. Using lessons from the pilot phase, the goal is to make the transition as smooth as possible for the wider user base.

Define your rollout strategy

Choose an approach:

- Step-by-step in waves – recommended for larger environments.
- All at once – only advisable in special cases.



For deployments involving thousands of devices, a phased rollout is best—e.g., by department or location in multiple waves. This lets IT handle volumes in manageable chunks, learn from each wave, and make immediate improvements.

Example rollout criteria:

- 100 devices per week.
- Start with headquarters, then branch offices.
- Enroll all iOS devices first, then Android (if separate handling is needed).

This plan should be documented in the project schedule.

Pre-rollout communication

Notify each affected user well in advance – ideally personalized or at least targeted to their group. Several weeks before their enrollment date, they should know what’s coming:

“Hi First_Name, on DD/MM/YYYY your work smartphone will be enrolled in our new Mobile Device Management system.”

Briefly restate the benefits and key points from the user guide. Remind them just before the date – include instructions for backing up personal data if a complete reset is needed (more common for company devices than BYOD).

Executing the rollout

Follow the plan consistently.

- For company-owned devices, the rollout can often be done remotely by sending enrollment links to users.
- For new or replacement devices, use automated provisioning such as Apple ADE or Android Zero-Touch.

In some cases, on-site support is helpful—especially for less tech-savvy users. You could host “MDM helpdesk” days where IT assists with device setup.

Monitoring during rollout

Actively track progress:

- How many devices have successfully enrolled?
- Where are errors occurring?

React quickly to anomalies – if 50 devices of one type all fail, it might be a manufacturer issue.

Keep in close contact with the support team and hold daily rollout review meetings to address problems and adjust as needed. Stay in communication with the MDM vendor for rapid assistance.

Stay flexible

Unexpected obstacles can arise. Be ready to adapt the rollout plan – pause the next wave if significant issues occur, fix them, then proceed. Communicate changes transparently to stakeholders.

Remember: quality over speed. It's better to extend the rollout by a week than to leave hundreds of users with broken devices and no resolution.

Completion and handover

When all planned devices are enrolled, the rollout is complete – celebrate this milestone!

If a separate project team handled the rollout, formally hand over to the operations team. Transfer all relevant documentation, close out pending items, and ensure no devices or special cases are left unaddressed.

10. Establishing Operations and Monitoring

Once all planned devices are enrolled in the MDM system, the focus shifts from project mode to ongoing operations. The goal now is to keep the environment stable, maintain security, and establish processes for day-to-day device management.

Monitor compliance and security

In Cortado, set up reports that clearly show the status of all devices. Key metrics include:

- Time of last device connection.
- Pending OS updates.
- Failed policy pushes.

Assign clear responsibilities: Who checks reports daily or weekly? Who responds to anomalies? The security team should always be involved in high-priority alerts (e.g., “Device XYZ reported as lost”).

Incident management

Define clear processes for mobile security incidents. A typical example is device loss or theft. Many Cortado customers use this workflow:

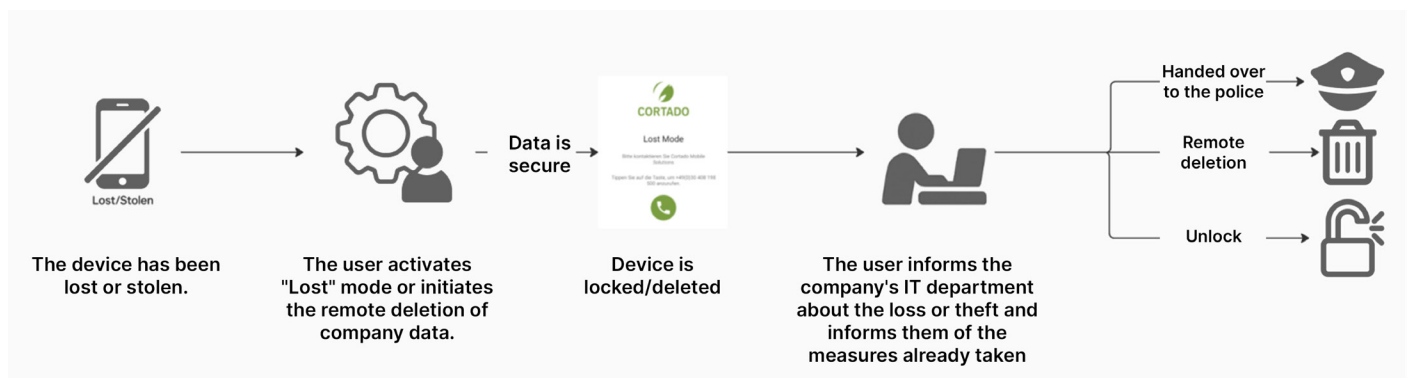


Figure 7 Process in case of device loss/theft

- Define when a device is considered lost/stolen.
- Define who authorizes data wipe actions.

Test these procedures regularly, for example by simulating a lost device.

For contingency planning: As a cloud solution, Cortado handles MDM database backups. If Cortado’s MDM servers are ever unavailable, this won’t immediately affect device operation – devices stay functional, but you can’t add new devices or send new commands during the outage.

Updates and maintenance

Cortado MDM is fully cloud-based (SaaS). Updates and patches are applied automatically by the provider – no infrastructure maintenance on your side.

On the devices, OS updates should also be deployed quickly. Cortado supports automated, scheduled rollouts, ensuring security updates are applied promptly. For major OS upgrades, roll out in waves – especially if compatibility testing is needed. Automating updates (e.g., overnight) improves patch compliance significantly. Experience shows automation can raise update compliance from ~67% to over 95%.

Regular audits

Perform periodic (e.g., quarterly) reviews of MDM settings and devices:

- Do policies still match corporate requirements?
- Are all employee devices enrolled, or are there gaps?

In regulated industries and critical infrastructure environments, MDM audits may be mandatory parts of security reviews. Document results and follow up with corrective actions.

KPIs and reporting

Establish key performance indicators for MDM, such as:

- Percentage of managed devices vs. total devices.
- Average provisioning time for new devices.
- Number of security incidents per quarter.
- User satisfaction with support (e.g., ticket ratings).

Report these KPIs to management to show MDM value, e.g.:

- “Since deploying Cortado, there have been no data losses from lost devices.”
- “Onboarding a new employee now takes minutes instead of days.”

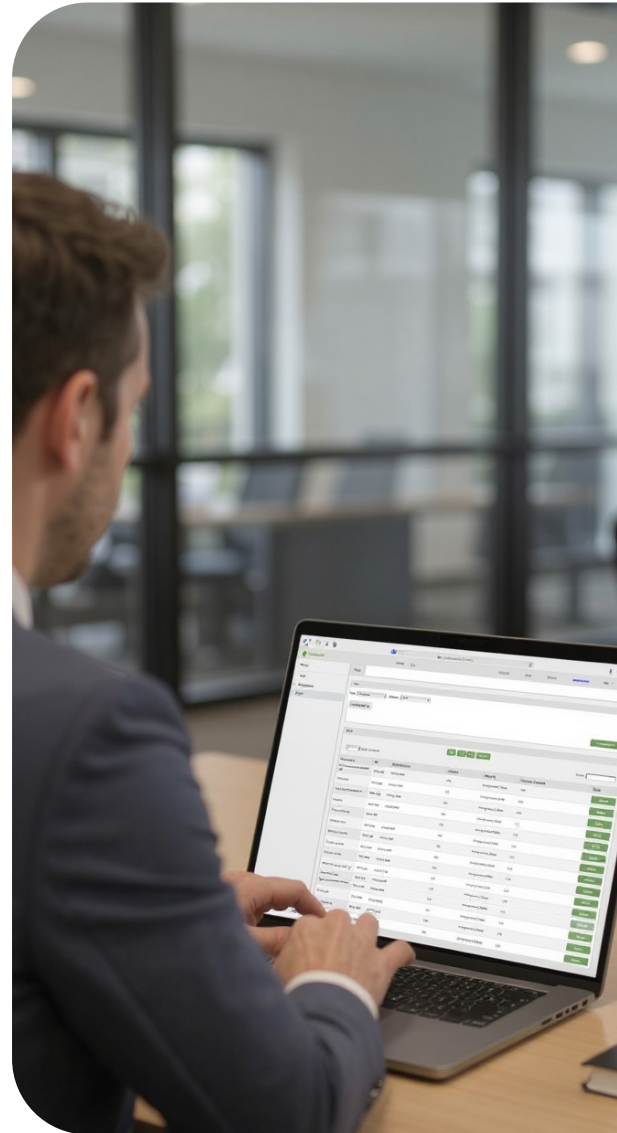
Continuous improvement

An MDM system isn’t static—adjust policies and processes as needs change. New threats may require tighter security; user feedback may justify relaxing certain rules.

MDM should integrate with broader security strategies such as zero-trust architecture or MFA. Updates in these areas should also be reflected in mobile policies.

By maintaining vigilant monitoring and proactive maintenance, you ensure the MDM system continues to protect devices and data without disrupting business operations—while enabling mobile and agile work.

Tip: Cortado offers regular webinars on new features and use cases. Use these as training sessions to refine your setup.



11. Review & Optimization

After the project is complete and the MDM has been in production for some time, it's important to review results and plan for continuous improvement. In IT, no project is ever truly “finished” – requirements and technologies are always evolving. Forward-thinking IT leadership should schedule regular reviews and optimization cycles.

Post-project review

About 1–2 months after the rollout, hold a “lessons learned” meeting with the project team and MDM vendor. Discuss openly: What went well? What could have been done better?

Document these insights for future projects. Perhaps the pilot phase was too short, or early involvement of business units and employees proved especially valuable.

And don't forget to celebrate successes – such as enrolling the first 1,000 devices within weeks or achieving significantly better protection of corporate data.

Check against goals

Compare actual results with the goals set in Phase 1, ideally using measurable KPIs. Examples:

- “100% of devices are encrypted and protected with passcodes.”
- “The device inventory is always up to date and complete.”

If goals weren't met, analyze the reasons and decide whether to adjust the measures or the goals themselves. Soft targets like “improved employee satisfaction” can be measured with targeted surveys.

End-user feedback and adoption

After a few months of operations, it's worth surveying employees specifically about MDM:

- How do they rate the solution?
- Are there misunderstandings or suggestions for improvement?

Such feedback can reveal areas for improvement—e.g., in communication, training materials, or overly strict restrictions. If many users need a blocked app and it's safe, you might approve it later. Positive feedback can also be used to promote the system internally—via management reports or success stories on the intranet.



Technical optimization

Regularly check your MDM configuration:

- Are there new features or modules from Cortado that could add value?
- Are there new integrations or APIs that could improve efficiency?

Cortado evolves continuously—new best practices can often be implemented quickly.

Adjust policies

Use operational data to refine policies. Examples:

- **If cameras are rarely needed**, consider disabling them by default to reduce data leak risks.
- **If maintaining a blacklist is too time-consuming**, switch to an allowlist.

Always coordinate significant policy changes with data protection, employee representatives and legal. Test changes with a pilot group before rolling them out broadly.

Regular audit & optimization cycle

Establish a continuous improvement process for your MDM strategy:

- Annual strategy reviews with management.
- Quarterly technical reviews with the admin team and Cortado to fine-tune configuration.
- Ongoing monitoring as described in Phase 10.

This ensures your MDM strategy keeps pace with the fast-changing mobile landscape and that your organization gets the full value from the solution.



Conclusion

A successfully implemented MDM system is a true enabler for modern, mobile work practices. By following the steps outlined in this guide – from clearly defining goals to building a solid technical foundation, through training, operations, and continuous optimization – you position yourself as both a thought leader and a hands-on practitioner in your company.

You demonstrate that high security and user-friendliness are not mutually exclusive – when approached methodically, they can go hand in hand. This way, your MDM project becomes not just an IT success, but a win for the entire organization.

And the best part: you're not on your own!

At Cortado, we've been successfully supporting companies of all sizes and industries for many years in implementing their MDM solutions – from planning to rollout and beyond.

We're happy to share our experience with you! Just get in touch with us – together we'll find the most efficient solution for your needs and get your project to its goal quickly and securely.



Let's take the next step together.

Book a no-obligation consultation with our Cortado experts – whether it's to optimize your existing MDM environment, strategically plan a rollout, or clarify technical details.

Benefit from our experience in countless projects and work with us to find the most efficient solution for your company.

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