jamf

An MDM Migration Checklist

Introduction

Few processes impact business operations as critically as management and security workflows. MDM manages all your endpoints, so migrating to a new solution involves more than just an IT task and also directly impacts employee productivity.

Because MDM has such a widespread effect on overarching business continuity, it's essential for IT decision makers looking to migrate solutions to cover all the possible angles before, during and after the migration process.

In this guide, we present the following topics in a 10-point, checklist-style format:

Three phases of MDM migration

Common challenges that derail projects

Overcome obstacles to ensure success

Maintain smooth operations post-transition

Pre-Migration (Planning)

> *"Before anything else, preparation is the key to success."*
>
> – ALEXANDER GRAHAM BELL

The pre-migration phase, also referred to as the planning stage, is without a doubt a crucial phase in any MDM migration project. Why is it so crucial? Because planning allows you to set the goal posts in terms of what they want to achieve when migrating from one MDM solution to another. Not only that, but it also allows for data-driven decision-making from deciding the best way how to get there by enabling the development of the metrics necessary to measure the project's success.

Doing so allows stakeholders to monitor progress along the way and adjust accordingly to both minimize interruptions and ensure that migration occurs with as little impact to business operations as possible.

1. Inventory MDM infrastructure

Before anything else, you need to understand and have an up-to-date record of each component that plays a role in your device management infrastructure. This includes the items crucial to the successful operation of your MDM solution, such as:

- **Devices**
- **Settings**
- **Services**
- **Apps**
- **Configurations**
- **Policies**

2. Perform risk assessment

When considering any major change, such as an MDM migration, it is essential to have a current risk assessment performed to identify any concerns that need to be mitigated, as well as to aid in making data-driven decision-making concerning risk appetite and maintaining a strong security posture throughout the project.

3. Determine compliance needs

With a completed inventory and risk assessment, the compliance needs unique to your enterprise can be fully determined. Baking compliance-related decision-making into the testing process (occurring later in the pre-migration phase) ensures organizations identify and maintain industry and/or region-required compliance levels.

4. Set goals and KPIs

Even when meticulously planned, due to the nature of moving resources from one solution to another, some loss of user productivity is inevitable. Setting goals for project completion and implementing metrics to measure success at various intervals of the project is essential to minimize impact and catch/resolve potential issues as they arise.

5. Design data backup strategies

Creating and testing a data backup plan follows the CIA triad (Confidentiality, Integrity, and Availability) and ensures that each tenet is adhered to before, during and after the migration project. Furthermore, when performed in the pre-migration phase, it allows IT to bake it into their workflows and verify the process works both ways (backup and restore) before the migration phase of end-users begins.

6. Develop migration workflows

IT creates and modifies workflows that touch upon each facet of the migration process end users will experience. This is also the perfect time to evaluate scripts, apps and policies used to automate migration as much as possible to remove redundant or outdated processes and maximize efficiencies to scale.

7. Conduct thorough testing

With all the ducks in a row, migration team members walkthrough a completed migration workflow using test devices within a dedicated testing environment to isolate errors and identify issues that invariably creep up during testing.

8. Documentation and iterative improvement

Documenting your findings is table stakes to the success of any business process or plan, and this applies doubly to IT. Recording what occurred during the testing step provides two crucial pieces:

1. **Identifies any issues that were found.**
2. **Provides IT the data necessary to drive iterative improvement.**

Both allow for changes to the migration workflow to occur while still in the testing environment, further reducing future interruptions while increasing the efficiency and likelihood of success during the migration phase.

9. Develop a contingency plan

Despite testing's best efforts, the production environment can (and sometimes does) introduce variables that couldn't be accounted for. This is where a fleshed-out regression plan becomes the saving grace of the project, providing a detailed series of steps that can be deployed to safely roll-back any changes to uphold business continuity.

10. Manage user communications and training

Communication with users can occur at any point throughout the pre-migration phase. In fact, some encourage it to be performed as early as possible. That said, it's important to exercise communication that impacts end users, such as training guidance that sets expectations and clearly communicates their valuable role in the migration phase.

Key considerations addressed during pre-migration

- **Maintain data security**
- **Ensure compatibility**
- **Minimize downtime**
- **Enhance security and compliance**
- **Increase productivity and efficiency**
- **Improve ROI/TCO**

Migration (Execution)

> *"Good tactics can save even the worst strategy. Bad tactics will destroy even the best strategy."*
>
> – GEORGE S. PATTON

Following pre-migration, the next phase is execution, where the actual process of migrating from one MDM solution to the other takes place. During the migration phase the theoretical work performed during pre-migration converts into practical application by executing the various components, workflows and strategies that make up the migration process.

In short: this is the star of the show and the reason for the project itself. Despite carefully laid plans and a smooth testing cycle, migrating MDM solutions in a production environment may pose unique risks introduced by unanticipated variables that could challenge the project's success. But with a solid vision that includes measuring performance and consistent communication with key stakeholders, IT leaders can ensure that each stage of the migration process completes successfully – on time, within budget constraints and with minimal impact to productivity.

1. Setup new MDM solution

Different from the testing environment, this stage requires IT to set up the new MDM solution for production (destination). By mirroring the components used by the previous MDM solution (source), porting over and configuring all the necessary pieces that combine to form a fully functional management solution ensures that the required level of functionality is present to handle the migration workflow.

Examples of critical components:

- Solution settings
- Security permissions
- Service integrations
- Certificates
- User accounts
- Smart Groups
- Apps
- Configurations
- Scripts
- Policies

2. Verify migration via pilot program

A mirrored production environment requires testing to validate the settings and that it will handle migration workflows similarly to how the testing environment fared during pre-migration. A pilot program fulfills this requirement by selecting a cross-section of device types and users from the organization's production pool to perform the migration to rule out any variables that might impact success on a larger scale.

3. Execute data backup (if necessary)

After verifying the fail-safes above, the first step in rolling out migration at scale is to execute data backups on each device that will be migrated from source to destination MDM. Data is the lifeblood of the enterprise and maintaining its security, integrity and availability during and after the migration minimizes data loss and downtime.

4. Prepare managed devices for migration

Managed devices will require differing levels of prep before they can be migrated successfully. Traditionally, scripts may be executed to check system settings or validate certificates. In other cases, devices may be collected by IT, wiped and enrolled, then redistributed back to end users. In other instances, migration workflows do not require wiping and may be transitioned from source to destination in an automated background process that cuts down significantly on scheduled downtime, requiring only a reboot before users are back to work. This stage is highly dependent on the enterprise's unique needs.

5. Unenroll managed devices from source

Whether executed as part of a manual workflow by the end user or performed as a remote command sent by IT from the source MDM, this stage sees the removal of source MDM trust certificate – and profiles installed by it – effectively unenrolling managed devices from the source MDM alongside the removal of their device records from its database.

6. Enroll devices within destination

Like unenrolling, the enrollment stage may be performed as a manual workflow or an automated task following the removal of the source MDM's management profile. This may or may not include issuing a device wipe command previously and remains highly dependent on your enterprise's unique needs.

7. Monitor project progress

While it's generally a good practice to keep tabs on a project, with its close alignment with business operations, the success of your MDM migration hinges upon IT's ability to identify pain points and mitigate them. How quickly these are addressed correlates directly to lessening the impact on productivity and business continuity.

8. Gather and review device inventory

Successfully migrated devices enrolled within the destination MDM will be manageable from this solution moving forward. Performing an inventory for each device provides IT teams with insight into the device's health and configuration status, and verifies managed devices are ready for the final stages of the migration phase.

9. Ensure device compliance

Alongside device inventory is compliance data related to each managed. This measurement provides an accurate snapshot of the level of compliance, both for individual devices but informing the organization's security posture as well compared to enterprise baselines and risk assessment data gathered during pre-migration.

10. Restore backup data

Once devices are confirmed to have migrated to the destination MDM and meet compliance requirements, the final stage of the migration process is the restoration of data backed up earlier. This maintains data security throughout the project and signals to end users that their device is ready for use.

Post-Migration (Review)

"Truth for us is simply a collective name for verification processes."

– WILLIAM JAMES

The final phase of the migration process is post-migration, also referred to as review, because its chief aim is to analyze the data that's been gathered throughout the prior two phases to verify sources of truth relating to the success of the migration project.

Anomalous behaviors do exist. False positives are a classic example of this in real-life IT management and serve as a reminder of the criticality of obtaining evidence that proves a device, or process is compliant during auditing. In this case, the checklist of tasks in post-migration grant IT the verification necessary to ensure that the migration project is completed but that it succeeded in meeting the metrics, such as KPIs, used to measure progress, performance and compliance requirements from beginning to end.

1. Validate migrated device enrollment

To ensure the tasks performed in the stages that proceed occur with minimal impact to end users and the enterprise, it is important to ensure that all devices migrated according to plan. This stage verifies that all devices are accounted for and have been configured in accordance with compliance requirements, as well as identifying any pending stragglers.

2. Ongoing performance monitoring

It is important for management and security workflows that active monitoring continues uninterrupted. This benefits IT by granting insight into performance indicators that impact the users and devices they manage and the infrastructure they communicate on. Also, it ensures that devices remain compliant compared to organizational baselines.

3. Update compliance policies (if necessary)

Change leads to the variables which often affect risk. Whether in a positive or negative way depends on several factors, but the key focus point is to reassess enterprise and device baselines to ascertain what, if any, changes to compliance controls and policies are necessary to address risk levels stemming from migrating to a new MDM solution.

4. Obtain stakeholder feedback

Feedback is imperative to understanding what went right and conversely, how something went wrong. More importantly, it serves as a data point to prioritize resolving pain points (next stage) while driving improvements to processes in the future (occurs in later stages).

5. Resolve outstanding issues/concerns

In this stage, the answers to questions like, "what went wrong?" are put into action by IT with resolutions to pending issues stemming directly or indirectly from the migration process. The severity or volume of issues raised varies from project to project and organization to organization but should be addressed before they can evolve into a management, security or productivity-impacting event.

6. Clean-up source MDM and tools

After validating devices in stage one, IT should take great care to sanitize the source MDM, removing and/or disabling components that are no longer of value or use since they may present risk. Examples of items that should be removed/disabled are:

- User and service accounts
- Access permissions
- Services
- Sensitive data/documents
- Integrations
- Enterprise software and licensing
- Customized scripts and configurations

7. Decommission source MDM solution

With all sensitive and enterprise-specific data, settings and configurations removed from the source MDM, the last step is to completely decommission the solution so that it cannot be used within your organization. This includes any network-specific resources, such as DNS entries, rule sets for security appliances or exceptions contained within hardware/software configurations.

8. Measure ROI/TCO metrics

Return on investment and total cost of ownership serve as important ways to measure the benefits and disadvantages an asset poses to the business. Revisiting these metrics and adjusting them to account for the new MDM solution will be necessary for organizations to gain an accurate valuation moving forward.

9. Document lessons learned

Documenting the entire migration process, wins and losses throughout the project gives IT clarity when it comes to an honest review of the pain points and struggles encountered as well as the highlighting successes. Ultimately, comparing these gives IT a clear picture of where there's room for improvement.

10. Iteratively update processes

The sum-total of the previous stage results in refining the process with iterative changes made to optimize migration processes, effectively minimizing the losses while maximizing the wins to achieve the highest level of success with the least amount of impact on productivity while keeping close alignment with business processes and continuity.

Key considerations addressed during post-migration

- **Maintain compatibility**
- **Ensure compliance**
- **Enhance productivity workflows**
- **Develop efficient processes**
- **Maximize TCO/ROI**

Conclusion

Successfully migrating MDM solutions represents a mission-critical transformation that requires careful planning, precise execution, and thorough review. his guide outlined the three phases of migration:

- **Pre-Migration:** Planning establishes the foundation through careful inventory assessment, risk analysis and workflow development.
- **Migration:** Execution transforms theoretical planning into practical implementation with data security, efficient automation and ongoing performance monitoring.
- **Post-Migration:** Review ensures long-term success through device validation, compliance enforcement and optimization of processes.

Each phase helps IT navigate the complexities of an MDM migration by providing the information needed to maintain security and compliance, minimize disruption, and align with broader business goals.

Key takeaways for a successful MDM migration:

- **Preparation is paramount:** Thorough planning and testing before migration significantly reduces risks and unexpected downtime.
- **Stakeholder communication:** Regular engagement with users and stakeholders ensures smooth transitions and user buy-in.
- **Security and compliance:** Uphold data security and adhere to compliance requirements throughout the migration process.
- **Process documentation:** Detailed documentation enables data-driven decision-making throughout all phases.
- **Continuous improvement:** Use lessons learned and stakeholder feedback to iteratively improve processes.

Migrate smarter: protect your data, minimize disruption, and power a more secure and productive organization.

When you're ready to migrate your MDM, Jamf makes sure you are ready to achieve Apple success, right from the start, offering a wide range of Professional Services designed to help you effectively implement and manage your Jamf solutions. Available at different levels to match your unique needs and budget, **Jamf Premium Services** offer onsite and remote access to a dedicated team of Jamf specialists. Your migration and implementation will benefit from best practice insights developed from hundreds of Apple deployments.

jamf

www.jamf.com

Try Jamf