Modern Management:

3 Benefits of Adopting Declarative Device Management Today

Apple says Declarative Device Management (DDM) is the future of device management. Although DDM is still in early stages, investing in DDM today will prepare your organization too meet the future.

What is Declarative Device Management (DDM)?

DDM's foundation is proactive, autonomous devices. An autonomous device works from pre-determined instructions and applies programmed management logic to take action without checking in with a server to report and receive instructions.

How does Mobile Device Management (MDM) using DDM compare to MDM alone?

It might be safe to say that MDM that leverages DDM is the opposite of traditional MDM on its own.

How does it work?
What makes it so powerful?

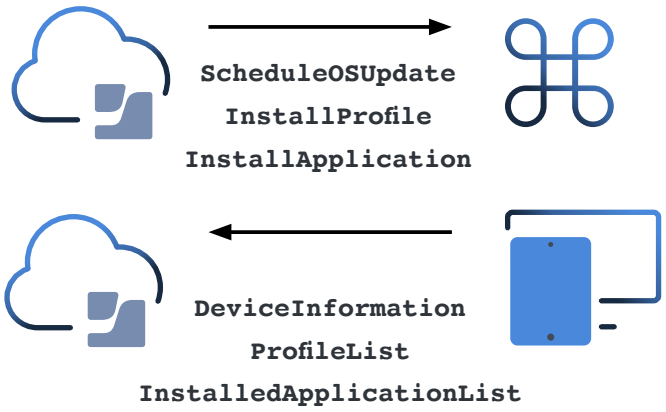
And what can you accomplish with DDM today?

Traditional MDM

MDM alone requires that the management server ask Apple to tell a device to call into the server for instructions. The device receives a ping, asks the server for instructions, and then completes the instructions.

To find out when and if the instructions were completed, the server asks Apple to ping the device again. The device responds with a report. Based on that report, the server may require even more answers or actions.

This results in a great deal of network traffic, and can take a very long time.



MDM using DDM technology

DDM enables straightforward communication between the server and devices, as well as autonomous decision-making on the part of each device.

So the MDM administrator sends persistent instructions to devices based on ‘if this, then that’ logic. If conditions change, the device can autonomously execute the prescribed action and inform the server directly what change occurred and what actions that it took in response.

A power pack for Apple Admins

DDM allows Apple admins to instruct devices on behavior such as:

- How to report key inventory values back to the management server
- How to enforce updates on a schedule with native feedback to end users
- How to anticipate and activate management on new devices that might get paired to existing devices
- How to proactively respond to malware and other attacks

What makes DDM a foundation for Modern Management?

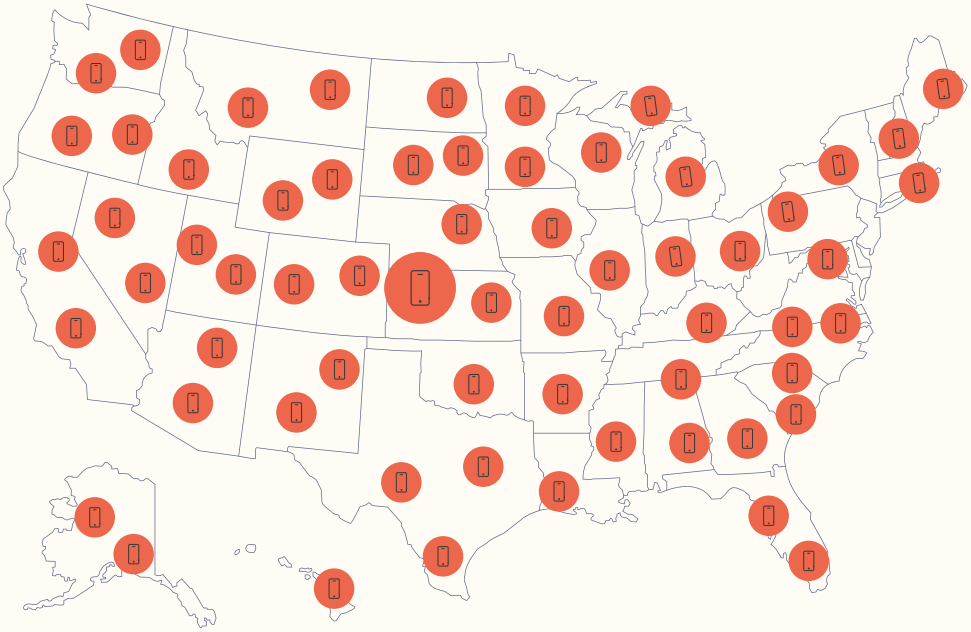
Workplaces have expanded beyond traditional office walls and continue to expand further and further. Proper cybersecurity requires diligent proactivity, not just increasingly lightning-quick reactions to adverse conditions to preserve data and network safety. Computer and mobile device work functions are becoming more and more nuanced and involved.

The nature of DDM's ability to empower devices to act autonomously is absolutely vital for an organization to cope with market conditions, workforce realities and higher expectations from employees and customers alike.

It's the management mode of the future, and failure to prepare for it now will leave organizations scrambling to adopt it when they could be pursuing more leads and strengthening more relationships.

As Apple rolls out more functionality for DDM, we will discover more truly transformative capabilities.

But DDM is not just about the future. Here are three really cool things you can do with DDM right now.



1.

Responsive inventory

DDM allows admins to create a declaration that instructs the managed device to autonomously alert the management server when key values (such as OS version) have changed, creating a responsive inventory use-case that proactive ensure compliance. **Let's look at a Jamf example.**

A large utility in the United States is a Jamf customer.

Their hundreds of field technicians all carry iPhones. Their IT supports a very large and highly-distributed workforce.

And because of their industry's regulatory requirements, this customer is highly focused on compliance, like **OS updates for security**.

OS updates for security

Given that they are compliance-driven, they must enforce software updates within a strict window of time as software updates tend to deliver key security fixes.

Complications

Here's where things get a little complicated.

They have required custom apps that aren't always immediately compatible with the latest OS updates. Some of their end users have actually developed a habit of avoiding software updates so as not to break these critical apps they need every day.

Combating bad habits

To combat this habit and make sure devices stay updated, the IT organization built a really clever workflow. If a device wasn't updated within the required compliance window, the server would:

- Add the device to a list of those excluded from managed apps and execute that command
- Deliver a wallpaper message requiring the update
- Offer IT contact information.

Honestly, this workflow is really smart. They protected organizational data complied with security standards and communicated with the end-user effectively. Great!

But it didn't work. Why?

End users responded by downloading the required update. But they didn't have immediate access to the apps they needed to perform their work duties.

Keep in mind that, with legacy MDM, the recommended inventory reporting time is once per day. Once every 24 hours, the MDM server would reach out to Apple and ask it to instruct the iPhone to answer an inventory query, and only then would it restore access.

Therefore, unless an employee magically updated right before the daily inventory check, they would immediately call IT for a manual update. This created a great deal of manual work — and therefore time — for IT.

The IT team could implement ways to update inventory by API and integrations from the Jamf Marketplace. But wouldn't it be cool if the device simply informed the management server on its own that the OS had been updated?

What did work: status reports.

Jamf's customer implemented DDM and used status reports: a form of declaration that instructs the managed device to autonomously alert the management server when key values (such as OS version) have changed.

Now, the end users updated as instructed and within seconds after the update is complete, they were able to use the iPhone's full functionality again.

In the background, during the reboot the iPhone proactively alerted the management server what the new operating system version was, and that the device was back in compliance. The management server removed the device from the list of those excluded from managed apps with no further IT intervention required.

2. Software updates

Enforcing software updates has been a longtime challenge for a lot of admins using legacy MDM technology.

The problem with software updates

For a while, software updates via scripted workflows worked pretty well. However, Apple has increasingly required both admin rights or MDM commands to invoke administrative actions on Macs which renders scripts less effective.

In addition, IT can risk creating hours of lost work if it invokes an update while the user is in the middle of critical work. That's why MDM commands to force critical updates are a last resort.

The solution: DDM

Thankfully, declarative management has the power to make this easier.

Remember that declarative management offers the ability to create intricate instructions that tell a device how to behave, and the device uses internal logic to autonomously follow those instructions.

Let's say an organizations' devices need to implement a vital application patch at a specific time. With an update driven by DDM, they update immediately without any need for an end-user communication to make sure it goes as planned. No lost work, no messy tracking and cleanup of stragglers.

Here's how it works:
An update invoked by a declaration will permit IT to set an enforced time and date for an app version. Before that date, using server-provided logic, the device communicates with the end user on an increasingly frequent basis, both alerting the end user of the upcoming event and allowing them to perform the update ahead of time if it's more convenient.

The time and date of enforcement is local to the client. Even if you have a global workforce or users who are traveling, the update will occur within an outside-of-work-hours maintenance window that's appropriate for the end user.

The update will be enforced on devices that are powered off during the enforcement period after they come back online.

Devices will automatically reach back to the management server with an update to the changed version of the app. This creates the most accurate view of a managed fleet when critical updates must execute to offset security risks.

3.

Apple Watch management

Apple has offered newer device management options as they continue to support DDM, and the one with the most potential is management of Apple Watch.

Apple watch for work? Absolutely.

Apple Watches are powerful, portable devices. They can enable communications, safety and identification workflows better than many other options.

Under management, if one is ever lost or stolen IT can remotely wipe it, protecting any organizational data or access that might be on those devices. And Apple now supports turning off Activation Lock within Apple Business Manager or Apple School Manager for institutionally-owned devices. This allows organizations to receive the benefits of enabling Find My without worrying that a device will become unusable if it's still locked.

How do companies use Apple Watch?

Thanks to the continuing development of DDM, Jamf customers use Apple Watch for a variety of work-related purposes, including:

- Employees working with heavy machinery or doing manual labor wear Apple Watch to keep both hands free while safely receiving notifications
- Nurses or other clinicians receive alerts about upcoming appointments or patient emergencies
- Workers of all kinds use Apple Watch as a electronic badge to enter secure areas

The exciting part is that these are just a few early and obvious examples. Jamf customers continue to show us new, creative use cases when they get managed devices in the hands (or on the wrists) of their users. We expect this list to grow in the coming months.

How does IT manage Apple Watch?

Managing an Apple Watch actually means managing a connected iPhone.

In **Jamf Pro**, admins use Smart Device Groups to enable Apple Watch enrollment for devices paired with institutionally-owned and supervised iPhones running iOS 17. This also enables a declaration designating any Apple Watch running watchOS 10 or later that pairs with one of those devices as managed.

After pairing, those Apple Watches are supervised and automatically inherit settings from the iPhone like passcode enforcement, even Wi-Fi and certificate payloads. These devices should be considered as a matched pair in regard to inventory, grouping, and reporting.

Apple Watch offers increasing benefits in the enterprise space. We at Jamf are excited to see how our customers will continue to use them, all backed by DDM and the power of Apple's services.

How does Jamf fit in?

Jamf Pro **automatically enables Declarative Device Management capabilities** for compatible managed devices. As an organization that offers zero-day support for all Apple updates, we continue to be on the cutting edge of DDM technology.

Stay ahead of the curve with DDM

It's smart to invest in the future by enabling **DDM on your Apple devices**, but it's even smarter to take advantage of all of the capabilities that are available right now.

Questions about how to implement **responsive inventory**, improve **software update workflows** or incorporate **Apple Watch management?**

Jamf is here to help.