# Declarative Device Management (DDM)

## DDM's impact on modern management is hard to overstate.

### Mobile Device Management (MDM) is already a powerful tool.

Mobile Device Management (MDM) for Apple, led by Jamf, has grown from forced-pull device management using the binary into a flexible, powerful, and user-friendly solution far beyond what anyone had imagined before.

MDM has given Apple administrators automation, control and visibility they never had before. It cuts down on repetitive tasks, removes human error factors and supports for strong security measures.

But work has changed from an office desk to a globally distributed workforce. And because needs have changed, organizations must change the way they manage devices to a more flexible, more portable and more secure model: **modern management**.

### What is modern management?

Modern management is a strategy that adapts to current realities of the workplace and plans for the workplace of the future.

It manages and secures devices, users, operating systems and applications from the cloud. Integrating these elements enhances security, management, and situational awareness for IT departments. This holistic approach enables more visibility and faster responsive actions.

Read our in-depth paper on modern management. >

## How does modern management improve on traditional device management?

Traditional device management focused on corporate-owned devices that are assigned to employees. Only these authorized devices could access the company's on-premises network. For a while, this was an excellent way to manage devices.

However, the workplace changed dramatically. Hybrid and remote workforces are now commonplace, and even those with traditional in-office environments need ways to allow every user type to remain productive without endangering company data.

Modern management moves everything to the cloud and to more secure, encrypted connections. Cloud deployments offer a number of security advantages over on-premises deployments such as:

- **Verified enrollment.** The use of built-in enrollment methods ensure the integrity of every device managed within your organization.
- **Identity and access management.** IT controls who has access to what, based on individual cloud identity.
- **Privilege management.** Users access only as much as they need, which protects more sensitive data.
- **Granular access policies for apps and data.** Limiting app and data access to only authorized users on trusted devices boosts security.
- **Secure network traffic.** Secure encryptions prevent unauthorized access.
- **Conditional access.** Automatically limiting access based on real-time data risk thresholds keeps networks secure.

Modern management allows for far more flexibility in location, working hours or even whether or not the devices are corporate- or user-owned.

But it wasn't until Apple released declarative device management (DDM), that the future of modern management could be fully realized.

## What is declarative device management?

Apple describes DDM as a “transformative update” to the existing MDM protocol that allows devices to act proactively and autonomously.

> “The future of device management is declarative management.”
>
> — Apple at WWDC 2021


Here at Jamf, we couldn’t agree more. That’s why we were ready to support DDM from day one.

**Proactive, autonomous devices is declarative device management’s foundation.** An autonomous device has instructions to react to its own state changes. It then applies programmed management logic to take any action required.

For instance, if the device drops out of compliance or experiences activity defined as possible malware, it can take action immediately. It no longer has to wait for a server status ping, report, and then wait for a prompt from the server with instructions on what actions to take.

This does three important things:

1. Frees up server-device traffic, which positively effects performance
2. Allows faster sandboxing and remediation of possible malware, increasing security
3. Thereby allowing for faster scalability that requires fewer resources

## How does DDM work?

DDM primarily uses three pillars: **declarations, status, extensibility.**

### Declarations

Declarations are server-defined payloads sent to devices. They define policies meant to be enforced directly on devices such as accounts, settings, and restrictions. These can be distributed to all users, smaller groups, or even for a single user or device.

They all have three **required** properties:

1. **Type:** defines which policy a configuration represents.
2. **Identifier key:** identifies a specific declaration within a set. They're used to synchronize declarations with the server.
3. **Value:** Constrains data by range or to a specific set of values. These can be strings, numbers, booleans, arrays, or dictionaries.

### Declaration Types

#### Activations

Activations are automatically-applied sets of configurations and referenced assets that must all be valid to be applied. For example, an action can only be valid on a specific device type or OS, to a particular OS version. This shifts burden on the the server to the device itself: it determines which ones to apply, based on requirements.

#### Assets

Assets refer to data that configurations need in order to work. If the data is large, the asset declaration delivers a URL to a server, which can be the MDM server or a separate content delivery server, for download. Assets can be any number of things such as name, email address, passwords, or certificates.

#### Configurations

Configurations are similar to MDM's existing profile payloads and describe the policies to be applied to the device such as accounts, settings or restrictions.

#### Management

Management declarations determine overall management state of each device. They convey static server and organizational information.

## Status Channel

The status channel tracks device state transition. Devices send status reports to the server, which the server can filter by subscribing only to the updates that concern it most such as OS versions, unusual activity or falling out of compliance.

The device then reports in incrementally: only changes are reported after the initial status report, rather than sending a complete description of the device status. This results in more pertinent information delivered far more quickly. Asynchronous updates triggered by the devices allow servers to monitor devices more closely even as it removes data noise and a great deal of network traffic. **This, in turn, improves performance.**

## Extensibility

Very few organizations will have Apple products or OS versions that are identical throughout their entire fleet. Apple products remain useful for a long time, after all. To get the most out of your investment in devices, you need to maintain compatibility between different versions of software and different hardware capabilities.

Because devices and servers communicate changes autonomously with DDM, each will know when new features are available right away. There's no need to hardcode software versions or hardware dependencies.

For example: when IT upgrades the server, it automatically synchronizes changed capabilities to the device, and the device can immediately use any useful new features. And the reverse is true: when a device updates, the server knows what cool new things the device can do immediately.

**The inherent extensibility of the declarative data model ensures that your structure is built for the present—and ready for the future.**

## A bright new horizon with DDM

We are only at the beginning of the combined evolution of DDM and MDM. Imagine the possibilities in a modality that:

- Supports new, complex management strategies in a simple and streamlined manner
- Enhances user experience on managed devices: both corporate- and personally-owned
- Supports a more responsive and reliable experience for users
- Speeds onboarding
- Removes IT from repetitive, tedious tasks, freeing them to innovate and focus on needed device management features

**What might your IT department do with more time to really think big?**

When you commit to DDM strategies, possibilities open up for your organization. Your business can grow alongside DDM's growth— at the speed of Apple.

What potential do you see on the horizon for your organization? For your own goals? For the world of work itself?

We believe that we're only seeing a glimmer of the potential for this technology to transform work and support the ever-evolving needs of modern management. Here's a little glimpse of what we think might be coming ahead.

## How will DDM shape the future of MDM?

While nobody has a crystal ball, it's safe to assume that Apple will be opening up new space for great ideas with DDM's capabilities. Here's a few areas we believe will grow for all Apple users and managers.

### Enhanced security

When you combine DDM capabilities with other recent changes, a pattern emerges.

Apple Silicon has essentially blocked any unattended updates triggered by a script or local agent with root privileges. This cuts off some of hacker's favorite malware strategies and also discourages unsafe practices such as the use of kernel extensions— which puts the integrity of the OS at risk.

Moving forward, expect administrative actions to increasingly require proper administrative tooling which decreases risk.

### More nuanced access

It would be wise to assume that, leaning on Managed Apple IDs, organizations will only increase in their ability to control access to services (and facilities) with iCloud keychains passkeys and Apple wallet support.

This doesn't necessarily mean that they will be more heavy-handed, either. DDM has enabled Apple admins to be far more nuanced in how and where they control access.

### Increasing identity support enhances the user experience

Apple Business Manager and Apple School manager makes custom identity support easy. Any identity provider such as Microsoft, Google, Okta, Open ID/ SKIM can now connect and easily create managed IDs: the best way to manage Apple devices and users. Users who can use one key to access everything they need for work are happier users and, incidentally, safer.

This evolution in outlook and capacity means that MDM will be:

- **More secure** by permitting declarations to set compliance out of the box and by limiting programmatic interactions with low-level binaries
- **More native** by enabling end-user interactions based on declarations
- **More useful** over time by iterating on the already strong foundation of MDM with DDM

To see more detail about the implications of this profound transformation, view the 2023 JNUC presentation: **"What's next for MDM?"**

## The future is now.

One of the best parts of this enormous leap forward is that existing MDM vendors can use declarative management features starting, well, yesterday. There's no need to disrupt work with a new protocol or server infrastructure, and declarations and the status channel can work side-by-side with already existing MDM commands and profiles. **DDM doesn't impact MDM behavior one iota.**

This means that IT can adopt DDM at the pace that feels best for them without requiring updates of all of their existing MDM workflows at once.

**And even better: it means you can dive in and get started right away!**

## How does Jamf support DDM?

Jamf's close, collaborative relationship with Apple means that we are always ready to support Apple innovation from day one.

### Support from the start

Jamf Pro has automatically enabled declarative device management capabilities for compatible managed devices since October of 2022. Devices with declarative device management enabled report their state changes automatically to the MDM server, and when certain changes occur they proactively report them and list them in device inventory information. Admins can customize these device states.

### Channel support for three new fields

Specifically, Jamf Pro introduced DDM status channel support to report three new fields with Jamf Pro 10.46:

`SupplementalBuildVersion`

`SupplementalOSVersionExtra`

`Passcode Compliance`

These new status channel items are automatically enabled so that devices can autonomously update Jamf Pro with new statuses immediately.

### iOS-specific support

DDM can do so much, and it's changing so rapidly! Here are a few specific ways in which we've used DDM to increase ease-of-use and safety:

- Updates on iOS-based devices use the passcode on device lock screens to generate an authorization token, which expires after a certain time for added security
- This token, after activated by the end user, allows updates without any need for the user to unlock their device
- Devices that have not been unlocked for a pre-determined timeframe will no longer receive these updates and the user will be prompted to allow them upon unlocking their device.

### Managed Software Updates powered by DDM

Before Apple introduced DDM capabilities, Jamf admins would either send a mass action or policy. Managed software updates powered by DDM provide us with even more capabilities:

- Software update plan configuration is much simpler
- End users have nuanced deferral options
- New automation and enforcement capabilities allow IT admins more control
- Proactive reporting from devices on update progress offer admins more visibility

## Looking ahead

As the DDM protocol continues to expand, Jamf will make the best use of it, supporting it every step of the way. For example, we continue to show our commitment to keeping the pace with Apple by enabling new device types for work, such as Apple Vision Pro and Apple Watch, giving end users the ability to be productive however they work best.

## There has never been a more exciting time to manage Apple devices.

Declarative device management has given the move toward modern management a tremendous boost. Some might even call it rocket-powered.

We've broken away from traditional device management. We went from multiple pings and voluminous communication back and forth between managed devices and Apple and the MDM server to autonomous devices overnight. We've proactively embraced the future.

The future of management and MDM is being built as we speak, and we're getting the chance to build it together!

And the age of modern management is upon us.

Fleet-footed organizations that are able to take advantage of this unprecedented time of growth will be ready for what the future brings, and adopting an Apple fleet is how to get there.

## Things to consider

Take a look at your current tech strategy. Is it flexible? Is it portable? Does it reflect a modern management approach to managing and securing devices?

If not, what might you gain from adopting a modern management approach? The ability to grow quickly? To turn on a dime? To attract the best talent and to keep everyone connected and secure?

What might you lose if you don't keep up?

The age of modern management is upon us. It's up to you to seize the opportunity and see where it takes you.

And Jamf will be supporting you every step of the way.

If you're ready to **join Apple and Jamf** on the transformative journey to **modern management**, and you want to take advantage of all that the cloud and DDM has to offer, **we can help!**

jamf