# Moderne Verwaltung

## 3 Vorteile der Einführung einer deklarativen Geräteverwaltung

Laut Apple ist die deklarative Geräteverwaltung (DDM) die Zukunft der Geräteverwaltung. Obwohl DDM noch in den Kinderschuhen steckt, ist Ihre Organisation durch die heutige Investition in DDM für die Zukunft gerüstet.

### Was ist deklarative Geräteverwaltung?

Die Grundlage von DDM sind proaktive, autonome Geräte. Ein autonomes Gerät arbeitet nach vorher festgelegten Anweisungen und wendet eine programmierte Verwaltungslogik an, um Aktionen durchzuführen, ohne sich bei einem Server einzuchecken, um zu berichten und Anweisungen zu erhalten.

### Was ist der Unterschied zwischen Mobilgeräteverwaltung (MDM) mit DDM und MDM allein?

Man kann mit Sicherheit sagen, dass MDM, das DDM nutzt, das Gegenteil von traditionellem MDM ist.

**Wie funktioniert sie? Was macht sie so leistungsfähig?**

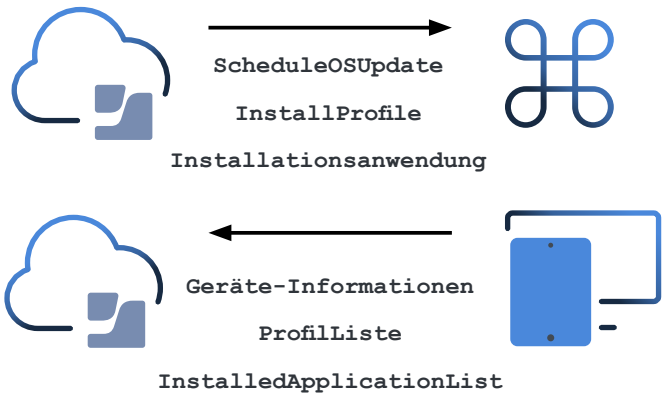
**Und was können Sie heute mit DDM erreichen?**

## Traditionelles MDM

Zunächst wird bei MDM allein vorausgesetzt, dass ein Management Server Apple dazu auffordert, ein Gerät bei dem Server weitere Anweisungen abfragen zu lassen. Das Gerät empfängt einen Ping, bittet den Server um Anweisungen und führt diese aus.

Um herauszufinden, wann und ob die Anweisungen abgeschlossen wurden, fordert der Server Apple auf, das Gerät erneut anzupingen. Das Gerät antwortet mit einer Berichterstattung. Auf der Grundlage dieses Berichts kann der Server noch mehr Antworten oder Aktionen verlangen.

Dies führt zu einem hohen Verkehrsaufkommen im Netzwerk und kann sehr viel Zeit in Anspruch nehmen.




## MDM mit DDM Technologie

DDM ermöglicht eine einfache Kommunikation zwischen dem Server und den Geräten sowie eine autonome Entscheidungsfindung aufseiten der einzelnen Geräte.

Administrator*innen senden also dauerhafte Anweisungen an Geräte, die auf der Logik "wenn dies, dann das" basieren. Ändern sich die Bedingungen, kann das Gerät autonom die vorgeschriebene Aktion ausführen und den Server direkt darüber informieren, welche Änderung eingetreten ist und welche Aktionen es daraufhin durchgeführt hat.


## Ein Kraftpaket für Apple Admins

DDM erlaubt es Apple Admins, Geräte zu instruieren, wie sie sich verhalten sollen:

- Wie die wichtigsten Bestandswerte an den Management Server zurückgemeldet werden können
- Wie lassen sich planmäßige Updates mit nativem Feedback für Endbenutzer*innen durchsetzen?
- Wie lässt sich die Verwaltung neuer Geräte, die mit vorhandenen Geräten gepaart werden könnten, vorhersehen und aktivieren?
- Wie man proaktiv auf Malware und andere Angriffe reagiert

## Was macht DDM zu einer Grundlage für moderne Verwaltung?

Arbeitsplätze haben sich über gewöhnliche Büroräumlichkeiten hinaus ausgeweitet und werden es immer weiter tun. Angemessene Cybersicherheit erfordert sorgfältige Proaktivität und nicht nur zunehmend blitzschnelle Reaktionen auf widrige Umstände, um die Sicherheit von Daten und Netzwerken zu gewährleisten. Die Arbeitsfunktionen von Computern und Mobilgeräten werden immer differenzierter und komplexer.

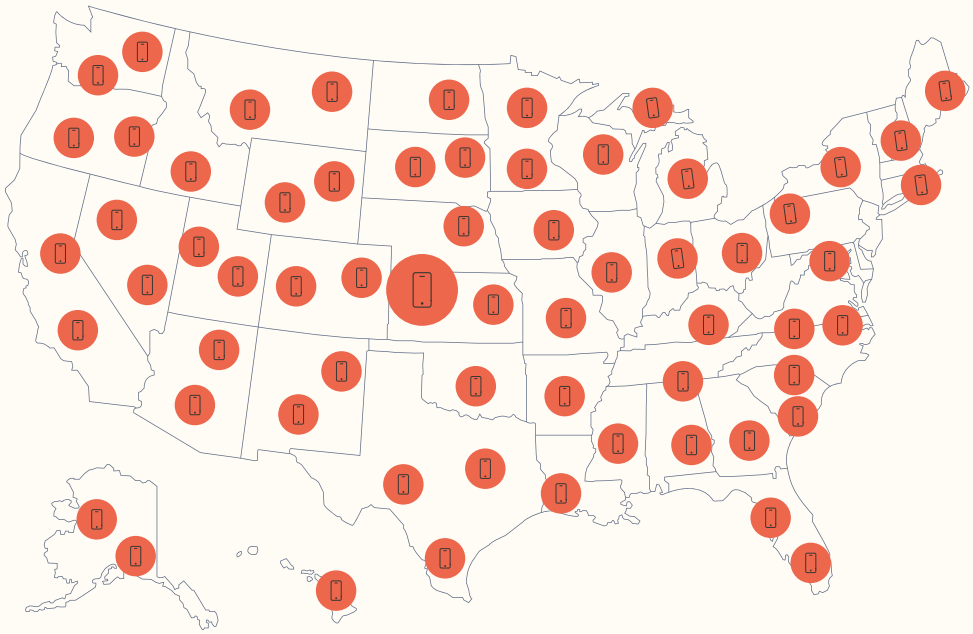
Die Fähigkeit von DDM, Geräte zu autonomem Handeln zu befähigen, ist für eine Organisation absolut unerlässlich, um mit den Marktbedingungen, der Realität der Arbeitskräfte und den höheren Erwartungen von Mitarbeitern*innen und Kund*innen gleichermaßen fertig zu werden.

Es ist die Managementmethode der Zukunft, und wenn man sich jetzt nicht darauf vorbereitet, werden die Organisationen nicht in der Lage sein, sie zu übernehmen, obwohl sie mehr Leads verfolgen und mehr Beziehungen aufbauen könnten.

In dem Maße, wie Apple weitere Funktionalitäten für DDM einführt, werden wir weitere wirklich transformative Fähigkeiten entdecken.

**Aber bei DDM geht es nicht nur um die Zukunft. Hier sind drei wirklich coole Dinge, die Sie jetzt mit DDM machen können.**

**1.**



### Reaktionsfähiger Bestand

Mit DDM können Admins eine Deklaration erstellen, die das verwaltete Gerät anweist, den Management Server autonom zu warnen, wenn sich Schlüsselwerte (z. B. die OS-Version) geändert haben, und so einen reaktionsschnellen Inventarisierungsanwendungsfall schaffen, der die Compliance sicherstellt.
**Schauen wir uns ein Jamf-Beispiel an.**

Ein großes Versorgungsunternehmen in den Vereinigten Staaten ist Jamf Kund*in.

Die Hunderte von Außendiensttechniker*innen tragen alle iPhones. Ihre IT unterstützt eine sehr große und weit verstreute Arbeitskraft.

Aufgrund der gesetzlichen Anforderungen in ihrer Industrie legt diese/r Kund*in großen Wert auf Compliance, z. B. **OS Updates für die Sicherheit**.

## OS Updates für die Sicherheit

Da sie auf die Einhaltung von Vorschriften angewiesen sind, müssen sie Software-Updates innerhalb eines engen Zeitfensters durchsetzen, da Software-Updates in der Regel wichtige Sicherheitsverbesserungen enthalten.

## Komplikationen

Hier werden die Dinge ein wenig kompliziert.

Sie haben benutzerdefinierte Apps benötigt, die nicht immer sofort mit den neuesten OS Updates kompatibel sind. Einige Endbenutzer*innen haben es sich sogar zur Gewohnheit gemacht, Software-Updates zu vermeiden, um die kritischen Apps, die sie täglich benötigen, nicht zu zerstören.

## Kampf gegen schlechte Gewohnheiten

Um diese Gewohnheit zu bekämpfen und sicherzustellen, dass die Geräte auf dem neuesten Stand bleiben, hat die IT Organisation einen wirklich cleveren Workflow entwickelt. Wenn ein Gerät nicht innerhalb des erforderlichen Compliance-Fensters aktualisiert wurde, würde der Server dies tun:

- Fügen Sie das Gerät zu einer Liste von Apps hinzu, die von der Verwaltung ausgeschlossen sind, und führen Sie diesen Befehl aus
- Übermitteln Sie eine Hintergrundmitteilung, die das Update erfordert
- Bieten Sie IT-Kontaktinformationen an.

Ehrlich gesagt, ist dieser Workflow wirklich clever. Sie schützten die organisatorischen Daten unter Einhaltung der Sicherheitsstandards und kommunizierten effektiv mit den Endbenutzer*innen. Großartig!

## Aber es hat nicht funktioniert. Warum?

Endbenutzer*innen reagierten, indem sie das erforderliche Update herunterluden. Aber sie hatten keinen unmittelbaren Zugang zu den Apps, die sie für die Erfüllung ihrer Aufgaben benötigten.

Denken Sie daran, dass die empfohlene Zeit für die Berichterstattung über den Bestand bei älteren MDM-Systemen einmal pro Tag ist. Alle 24 Stunden wendet sich der MDM-Server an Apple und bittet es, das iPhone anzuweisen, eine Abfrage des Bestands zu beantworten, und erst dann den Zugang wiederherzustellen.

Wenn also Mitarbeiter*innen nicht auf magische Weise kurz vor dem täglichen Einchecken des Bestands ein Update vornahmen, müssten sie sofort die IT anrufen, um ein manuelles Update durchzuführen. Dies würde für die IT einen hohen manuellen und damit zeitlichen Aufwand bedeuten.

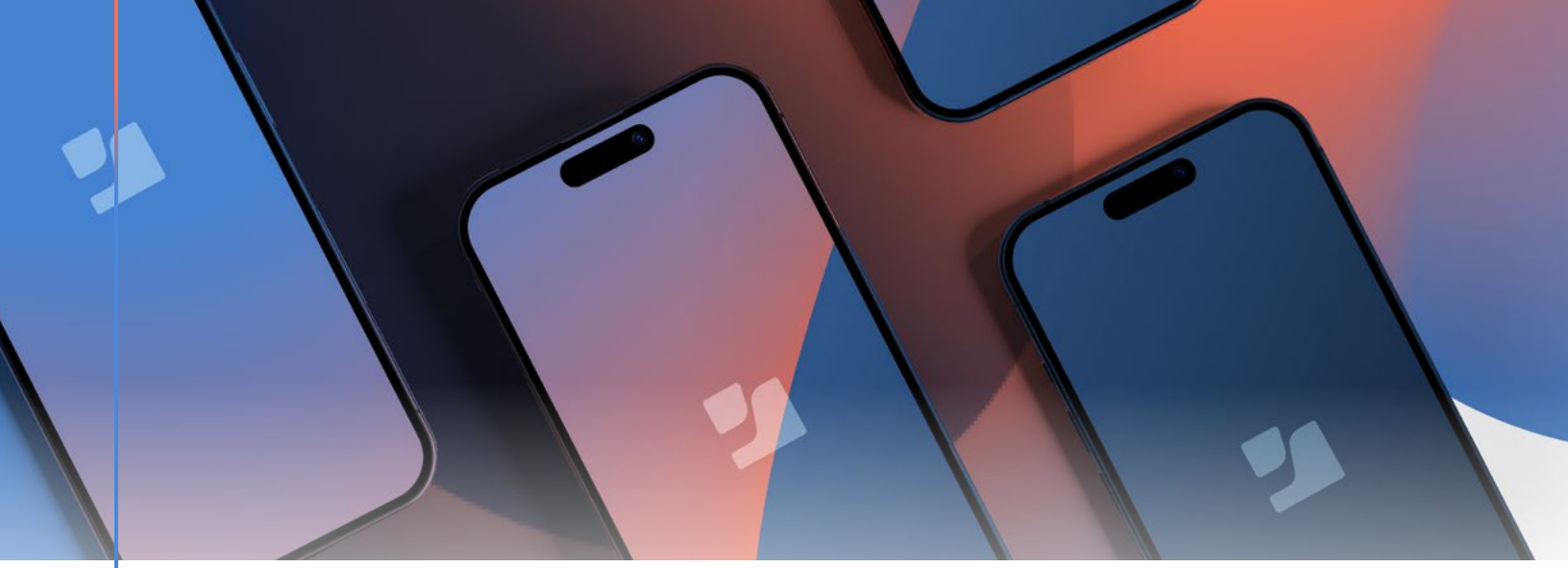
Das IT-Team könnte Möglichkeiten zum Update des Bestandes über API und Marketplace Integrationen von Jamf Marketplace implementieren. Aber wäre es nicht cool, wenn das Gerät dem Management Server einfach von sich aus mitteilen würde, dass das OS Update durchgeführt wurde?

## Was funktioniert hat: Statusberichte.

Jamf Kund*innen implementierten DDM und verwendeten Statusberichte: eine Form der Deklaration, die das verwaltete Gerät anweist, den Management Server autonom zu warnen, wenn sich Schlüsselwerte (wie die OS-Version) geändert haben.

Die Endbenutzer*innen führten das Update wie angewiesen durch und konnten innerhalb weniger Sekunden nach Abschluss des Updates wieder die volle Funktionalität des iPhones nutzen.

Im Hintergrund meldete das iPhone während des Neustarts proaktiv dem Verwaltungsserver die neue Version des Betriebssystems und dass das Gerät wieder die Compliance erfüllt. Der Management Server entfernte das Gerät von der Liste derjenigen, die von den verwalteten Apps ausgeschlossen waren, ohne dass ein weiteres Eingreifen der IT erforderlich war.



## 2. Softwareaktualisierungen

Die Durchsetzung von Software-Updates ist für viele Admins, die eine ältere MDM-Technologie verwenden, seit langem eine Herausforderung.

### Das Problem mit Software aktualisieren

Eine Zeit lang funktionierten Software Aktualisierungen über Skript-Workflows recht gut. Apple hat jedoch zunehmend sowohl Admin-Rechte als auch MDM-Befehle verlangt, um administrative Aktionen auf Macs auszulösen, was Skripte weniger effektiv macht.

Außerdem riskiert die IT stundenlange Arbeitsausfälle, wenn sie ein Update aufruft, während der/die Benutzer*in gerade mit wichtigen Aufgaben beschäftigt ist. Deshalb sind MDM-Befehle zur Erzwingung kritischer Updates ein letzter Ausweg.

### Die Lösung: DDM

Zum Glück kann die deklarative Verwaltung diese Aufgabe erleichtern.

Denken Sie daran, dass die deklarative Verwaltung die Möglichkeit bietet, komplizierte Anweisungen zu erstellen, die einem Gerät vorschreiben, wie es sich zu verhalten hat, und das Gerät eine interne Logik verwendet, um diesen Anweisungen autonom zu folgen.

Nehmen wir an, die Geräte einer Organisation müssen zu einem bestimmten Zeitpunkt einen wichtigen Patch für eine App implementieren. Bei einem von DDM gesteuerten Update erfolgt das Update sofort, ohne dass eine Kommunikation mit dem/der Endbenutzer*in erforderlich ist, um sicherzustellen, dass es wie geplant abläuft. Keine verlorene Arbeit, kein mühsames Aufspüren und Aufräumen von Nachzüglern.

**So funktioniert es:**
Ein Update, das durch eine Erklärung aufgerufen wird, erlaubt es der IT, eine erzwungene Zeit und ein Datum für eine App-Version festzulegen. Vor diesem Datum kommuniziert das Gerät mithilfe einer vom Server bereitgestellten Logik in immer kürzeren Abständen mit dem/der Endbenutzer*in, um diese(n) zum einen über das bevorstehende Ereignis zu warnen und ihr/m zum anderen die Möglichkeit zu geben, das Update vorzeitig durchzuführen, wenn dies bequemer ist.

Uhrzeit und Datum der Vollstreckung sind für die Kund*innen lokal. Selbst wenn Sie über Arbeitskräfte auf der ganzen Welt verfügen oder Benutzer*innen auf Reisen sind, erfolgt das Update innerhalb eines für die Endbenutzer*in geeigneten Wartungszeitfensters außerhalb der Arbeitszeiten.

Das Update wird auf Geräten erzwungen, die während des Erzwingungszeitraums ausgeschaltet sind, nachdem sie wieder online sind.

Die Geräte melden sich automatisch mit einem Update auf die geänderte Version der App beim Management Server zurück. Auf diese Weise erhält man den genauesten Überblick über eine verwaltete Flotte, wenn kritische Updates ausgeführt werden müssen, um Sicherheitsrisiken auszugleichen.

3.

## Verwaltung der Apple Watch

Apple hat neuere Optionen für die Geräteverwaltung angeboten, da sie weiterhin DDM unterstützen, und diejenige mit dem größten Potenzial ist die Verwaltung der Apple Watch.

Apple Watch für die Arbeit? Ganz genau.

Apple Watches sind leistungsstarke, tragbare Geräte. Sie können Kommunikations-, Sicherheits- und Identifizierungs-Workflows besser ermöglichen als viele andere Optionen.

Wenn ein Gerät verloren geht oder gestohlen wird, kann die IT die Werkeinstellungen aus der Ferne zurücksetzen und so alle Daten und Zugänge des Unternehmens schützen, die sich auf diesen Geräten befinden könnten. Außerdem unterstützt Apple jetzt das Ausschalten der Aktivierungssperre im Apple Business Manager oder Apple School Manager für Geräte, die sich im Besitz einer Institution befinden. Somit können Organisationen die Vorteile der Aktivierung von Wo ist? nutzen, ohne befürchten zu müssen, dass ein Gerät unbrauchbar wird, wenn es noch gesperrt ist.

### Wie nutzen Unternehmen die Apple Watch?

Dank der kontinuierlichen Entwicklung von DDM nutzen Jamf Kund*innen die Apple Watch für eine Vielzahl von arbeitsbezogenen Zwecken, darunter:

- Mitarbeiter*innen, die mit schweren Maschinen arbeiten oder Handarbeit verrichten, tragen die Apple Watch, um beide Hände frei zu haben und sicher Mitteilungen zu erhalten
- Krankenschwestern und -pfleger*innen oder andere Klinikmitarbeiter*innen erhalten Benachrichtigungen und Warnungen über anstehende Termine oder Notfälle von Patient*innen
- Arbeiter*innen aller Art nutzen die Apple Watch als elektronischen Ausweis, um sichere Bereiche zu betreten

Das Spannende daran ist, dass dies nur ein paar frühe und offensichtliche Beispiele sind. Jamf Kund*innen zeigen uns immer wieder neue, kreative Anwendungsfälle, wenn sie verwaltete Geräte in die Hände (oder an die Handgelenke) ihrer Benutzer*innen bringen. Wir gehen davon aus, dass diese Liste in den kommenden Monaten noch wachsen wird.

## Wie verwaltet die IT die Apple Watch?

Die Verwaltung einer Apple Watch bedeutet eigentlich die Verwaltung eines angeschlossenen iPhones.

In **Jamf Pro** verwenden Administratoren Smart Device Groups, um die Registrierung der Apple Watch für Geräte zu ermöglichen, die mit unternehmenseigenen und überwachten iPhones mit iOS 17 gepaart sind. Dies ermöglicht auch eine Erklärung, die jede Apple Watch mit watchOS 10 oder höher, die mit einem dieser Geräte gepaart ist, als verwaltet bezeichnet.

Nach dem Paaren werden diese Apple Watches überwacht und sie übernehmen automatisch die Einstellungen des iPhones, wie z. B. die Durchsetzung von Passwörtern und sogar WLAN- und Zertifikats-Payloads. Diese Geräte sollten in Bezug auf Bestand, Gruppierung und Berichterstattung als ein abgestimmtes Paar betrachtet werden.

Die Apple Watch bietet immer mehr Vorteile im Unternehmen. Wir bei Jamf sind gespannt, wie unsere Kund*innen sie weiterhin nutzen werden, unterstützt durch DDM und die Leistungsfähigkeit der Apple Services.

## Welche Rolle spielt Jamf?

Jamf Pro **aktiviert automatisch deklarative Geräteverwaltungsfunktionen für kompatible verwaltete Geräte.** Als Organisation, die Zero-Day-Support für alle Apple Updates anbietet, sind wir weiterhin auf dem neuesten Stand der DDM-Technologie.

## Mit DDM der Zeit voraus sein

Es ist klug, in die Zukunft zu investieren und **DDM auf Ihren Apple Geräten** zu aktivieren, aber noch klüger ist es, alle Fähigkeiten zu nutzen, die jetzt schon zur Verfügung stehen.

Haben Sie Fragen zur Implementierung von **responsiven Beständen**, zur Verbesserung von **Software-Update-Workflows** oder zur Integration der **Apple Watch-Verwaltung?**

**Jamf steht Ihnen zur Seite**