



Deklarative Geräteverwaltung (DDM)

Der Einfluss von DDM auf das moderne Management kann gar nicht hoch genug eingeschätzt werden.

Mobile Device Management (Mobilgeräteverwaltung, MDM) ist bereits ein leistungsstarkes Werkzeug.

Mobile Device Management (Mobilgeräteverwaltung, MDM) für Apple, unter der Leitung von Jamf, hat sich von einem erzwungenen Gerätemanagement mit Binärdateien zu einer flexiblen, leistungsstarken und benutzerfreundlichen Lösung entwickelt, die weit über das hinausgeht, was man sich vorher vorstellen konnte.

MDM hat den Apple Administrator*innen eine Automatisierung, Kontrolle und Transparenz ermöglicht, die sie vorher nicht hatten. Es reduziert die sich wiederholenden Aufgaben, beseitigt menschliche Fehlerfaktoren und unterstützt strenge Sicherheitsmaßnahmen.

Aber die Arbeit hat sich von einem Büroschreibtisch zu einer weltweit verteilten Belegschaft gewandelt. Und weil sich die Anforderungen geändert haben, müssen Unternehmen die Art und Weise, wie sie Geräte verwalten, auf ein flexibleres, mobiles und sichereres Modell umstellen:

modernes Management.

Was ist moderne Verwaltung?

Modernes Management ist eine Strategie, die sich an die aktuellen Gegebenheiten des Arbeitsplatzes anpasst und den Arbeitsplatz der Zukunft plant.

Es verwaltet und sichert Geräte, Benutzer*innen, Betriebssysteme und Apps über die Cloud. Die Integration dieser Elemente verbessert die Sicherheit, die Verwaltung und das Situationsbewusstsein der IT-Abteilungen. Dieser ganzheitliche Ansatz ermöglicht mehr Transparenz und schnellere Reaktionen.

[Lesen Sie unseren ausführlichen Artikel über modernes Management. >](#)



Wie kann eine moderne Verwaltung die traditionelle Geräteverwaltung verbessern?

Das traditionelle Gerätemanagement konzentrierte sich auf unternehmenseigene Geräte, die den Mitarbeiter*innen zugewiesen werden. Nur diese autorisierten Geräte konnten auf das firmeneigene Netzwerk zugreifen. Eine Zeit lang war dies eine hervorragende Möglichkeit, Geräte zu verwalten.

Der Arbeitsplatz hat sich jedoch dramatisch verändert. Hybride und standortferne Arbeitsgruppen sind heute gang und gäbe, und selbst Unternehmen mit traditionellen Büroumgebungen müssen Wege finden, die es jedem Benutzertyp ermöglichen, produktiv zu bleiben, ohne die Unternehmensdaten zu gefährden.

Die moderne Verwaltung verlagert alles in die Cloud und auf sicherere, verschlüsselte Verbindungen. Cloudimplementierungen bieten eine Reihe von Sicherheitsvorteilen gegenüber lokalen Implementierungen wie:

- **Überprüfte Registrierung.** Die Verwendung integrierter Anmeldemethoden gewährleistet die Integrität jedes in Ihrer Organisation verwalteten Geräts .
- **Identitäts- und Zugriffsmanagement.** Die IT-Abteilung kontrolliert, wer auf der Grundlage der individuellen Cloud Identität Zugriff auf was hat.
- **Verwaltung von Privilegien.** Die Nutzer*innen haben nur so viel Zugriff, wie sie benötigen, wodurch auch sensiblere Daten geschützt werden.
- **Granulare Zugriffsrichtlinien für Arbeitsapps und Daten.** Die Beschränkung des App- und Datenzugriffs auf autorisierte Benutzer*innen auf vertrauenswürdigen Geräten erhöht die Sicherheit.
- **Sicherer Netzwerkverkehr.** Sichere Verschlüsselungen verhindern unbefugten Zugriff.
- **Bedingter Zugriff.** Die automatische Beschränkung des Zugriffs auf der Grundlage von Echtzeit-Datenrisikoschwellenwerten sorgt für sichere Netzwerke.

Ein modernes Management ermöglicht weitaus mehr Flexibilität in Bezug auf den Standort, die Arbeitszeiten oder sogar die Frage, ob die Geräte dem Unternehmen oder dem Nutzer/der Nutzerin gehören.

Aber erst als Apple das [deklarative Gerätemanagement](#) (DDM) einführte, konnte die Zukunft des modernen Managements vollständig realisiert werden.

Was ist deklaratives Gerätemanagement?

Apple beschreibt DDM als ein „transformatives Update“ des bestehenden MDM-Protokolls, das es den Geräten ermöglicht, proaktiv und autonom zu handeln.

„Die Zukunft der
Geräteverwaltung
ist die deklarative
Verwaltung.“

— Apple auf der WWDC 2021



Wir von Jamf können dem nur zustimmen.

Deshalb waren wir vom ersten Tag an bereit, DDM zu unterstützen.

Proaktive, autonome Geräte sind die Grundlage der deklarativen Geräteverwaltung. Ein autonomes Gerät hat die Anweisung, auf seine eigenen Zustandsänderungen zu reagieren. Anschließend wendet es eine programmierte Verwaltungslogik an, um die erforderlichen Maßnahmen zu ergreifen.

Wenn das Gerät beispielsweise gegen die Vorschriften verstößt oder Aktivitäten feststellt, die als mögliche Malware definiert sind, kann es sofort Maßnahmen ergreifen. Es muss nicht mehr auf einen Serverstatus-Ping warten, einen Bericht erstellen und dann auf eine Eingabeaufforderung des Servers mit Anweisungen zu den zu ergreifenden Maßnahmen warten.

Damit werden drei wichtige Dinge erreicht:

1.

Entlastung des Datenverkehrs zwischen Server und Gerät, was sich positiv auf die Leistung auswirkt

2.

Ermöglicht schnelleres Sandboxing und die Beseitigung möglicher Malware und erhöht die Sicherheit

3.

Dadurch wird eine schnellere Skalierbarkeit ermöglicht, die weniger Ressourcen erfordert

Wie funktioniert DDM?

DDM stützt sich in erster Linie auf drei Säulen: **Deklarationen, Status, Erweiterbarkeit.**

Deklarationen

Deklarationen sind serverdefinierte Nutzdaten, die an Geräte gesendet werden. Sie definieren Richtlinien, die direkt auf den Geräten durchgesetzt werden sollen, wie Konten, Einstellungen und Einschränkungen.

Diese können an alle Benutzer*innen, kleinere Gruppen oder sogar an einen einzelnen Benutzer/eine einzelne Benutzerin oder ein einzelnes Gerät verteilt werden.

Sie alle haben drei **erforderliche** Eigenschaften:

- 1.** **Typ:** legt fest, welche Richtlinie eine Konfiguration darstellt.
- 2.** **Identifikatorschlüssel:** identifiziert eine bestimmte Erklärung innerhalb einer Menge. Sie werden verwendet, um Deklarationen mit dem Server zu synchronisieren.
- 3.** **Wert:** Schränkt Daten auf einen Bereich oder eine bestimmte Gruppe von Werten ein. Dabei kann es sich um Zeichenketten, Zahlen, Boolesche Werte, Arrays oder Wörterbücher handeln.

Arten von Erklärungen



Aktivierungen

Aktivierungen sind automatisch angewendete Sätze von Konfigurationen und referenzierten Assets, die alle gültig sein müssen, um angewendet zu werden. Zum Beispiel kann eine Aktion nur für einen bestimmten Gerätetyp oder ein bestimmtes Betriebssystem gültig sein, für eine bestimmte Betriebssystemversion. Dadurch wird die Last vom Server auf das Gerät selbst verlagert: Es entscheidet je nach den Anforderungen, welche Maßnahmen zu ergreifen sind.



Assets

Assets beziehen sich auf Daten, die Konfigurationen benötigen, um zu funktionieren. Wenn die Daten groß sind, liefert die Asset-Deklaration eine URL an einen Server, bei dem es sich um den MDM-Server oder einen separaten Content-Delivery-Server handeln kann, zum Download. Bei den Vermögenswerten kann es sich um eine beliebige Anzahl von Dingen wie Namen, E-Mail-Adressen, Passwörter oder Zertifikate handeln.



Konfigurationen

Konfigurationen ähneln den bestehenden Profil-Payloads von MDM und beschreiben die auf das Gerät anzuwendenden Richtlinien wie Konten, Einstellungen oder Einschränkungen.



Verwaltung

Verwaltungserklärungen bestimmen den allgemeinen Verwaltungsstatus jedes Geräts. Sie vermitteln statische Server- und Organisationsinformationen.

Status Channel

Der Statuskanal verfolgt den Übergang des Gerätezustands. Die Geräte senden Statusberichte an den Server, die der Server filtern kann, indem er nur die Aktualisierungen abonniert, die ihn am meisten betreffen, wie z. B. Betriebssystemversionen, ungewöhnliche Aktivitäten oder die Nichteinhaltung von der Compliance.

Das Gerät meldet sich dann inkrementell: Es werden nur Änderungen nach der ersten Statusmeldung gemeldet, anstatt eine vollständige Beschreibung des Gerätestatus zu senden. Dies führt dazu, dass sachdienliche Informationen sehr viel schneller zur Verfügung stehen. Asynchrone Aktualisierungen, die von den Geräten ausgelöst werden, ermöglichen es den Servern, die Geräte genauer zu überwachen, während gleichzeitig das Datenrauschen und ein großer Teil des Netzverkehrs entfällt. **Dies wiederum verbessert die Leistung.**

Erweiterbarkeit

Nur sehr wenige Unternehmen haben Apple Produkte oder Betriebssystemversionen, die in ihrer gesamten Flotte identisch sind. Apple Produkte bleiben schließlich lange Zeit nützlich. Um den größtmöglichen Nutzen aus Ihren Investitionen in Geräte zu ziehen, müssen Sie die Kompatibilität zwischen verschiedenen Softwareversionen und unterschiedlichen Hardwarefunktionen sicherstellen.

Da Geräte und Server Änderungen selbständig mit DDM kommunizieren, wissen sie sofort, wenn neue Funktionen verfügbar sind. Es besteht keine Notwendigkeit, Softwareversionen oder Hardware-Abhängigkeiten zu programmieren.

Ein Beispiel: Wenn die IT-Abteilung den Server aktualisiert, werden die geänderten Funktionen automatisch mit dem Gerät synchronisiert, und das Gerät kann alle nützlichen neuen Funktionen sofort nutzen. Und umgekehrt: Wenn ein Gerät aktualisiert wird, weiß der Server sofort, welche coolen neuen Dinge das Gerät tun kann.

Die inhärente Erweiterbarkeit des deklarativen Datenmodells stellt sicher, dass Ihre Struktur für die Gegenwart gebaut und für die Zukunft gerüstet ist.





Ein heller neuer Horizont mit DDM

Wir stehen erst am Anfang der gemeinsamen Entwicklung von DDM und MDM. Stellen Sie sich die Möglichkeiten einer Modalität vor, die:

- Unterstützt neue, komplexe Managementstrategien auf einfache und rationelle Weise
- Verbessert die Benutzererfahrung auf verwalteten Geräten: sowohl unternehmenseigene als auch private Geräte
- Unterstützt ein reaktionsschnelleres und zuverlässigeres Erlebnis für die Nutzer*innen
- Beschleunigt das Onboarding
- Entlastet die IT-Abteilung von sich wiederholenden, mühsamen Aufgaben, sodass sie sich auf Innovationen und die erforderlichen Geräteverwaltungsfunktionen konzentrieren kann

Was könnte Ihre IT-Abteilung tun, wenn sie mehr Zeit hätte, wirklich groß zu denken?

Wenn Sie sich für DDM-Strategien entscheiden, eröffnen sich für Ihr Unternehmen neue Möglichkeiten. Ihr Unternehmen kann mit dem Wachstum von DDM mitwachsen - mit der Geschwindigkeit von Apple.

Welches Potenzial sehen Sie für Ihr Unternehmen am Horizont? Für Ihre eigenen Ziele? Für die Welt der Arbeit selbst?

Wir sind davon überzeugt, dass wir nur einen Schimmer des Potenzials dieser Technologie sehen, die Arbeit zu verändern und die sich ständig weiterentwickelnden Anforderungen des modernen Managements zu unterstützen. Hier ein kleiner Vorgeschmack auf das, was unserer Meinung nach auf uns zukommen könnte.

Wie wird DDM die Zukunft von MDM gestalten?

Zwar hat niemand eine Kristallkugel, aber man kann davon ausgehen, dass Apple mit den Möglichkeiten von DDM neuen Raum für großartige Ideen schaffen wird. Hier sind einige Bereiche, von denen wir glauben, dass sie für alle Apple Nutzer*innen und Manager*innen wachsen werden.

Verbesserte Sicherheit

Kombiniert man die DDM-Funktionen mit anderen aktuellen Änderungen, ergibt sich ein Muster.

Apple Silicon hat im Wesentlichen alle unbeaufsichtigten Aktualisierungen blockiert, die durch ein Skript oder einen lokalen Agenten mit Root-Rechten ausgelöst werden. Dadurch werden einige der beliebtesten Malware-Strategien von Hacker*innen unterbunden und unsichere Praktiken wie die Verwendung von Kernel-Erweiterungen, die die Integrität des Betriebssystems gefährden, verhindert.

Es ist zu erwarten, dass Verwaltungsmaßnahmen in Zukunft immer häufiger ein angemessenes Verwaltungsinstrumentarium erfordern, das das Risiko verringert.

Differenzierterer Zugang

Es ist davon auszugehen, dass Unternehmen, die sich auf verwaltete Apple IDs stützen, den Zugang zu Diensten (und Einrichtungen) mit iCloud Schlüsselbund und Apple Wallet Unterstützung immer besser kontrollieren können.

Das bedeutet aber nicht zwangsläufig, dass sie auch härter durchgreifen werden. DDM hat es den Apple Administrator*innen ermöglicht, die Zugriffskontrolle weitaus differenzierter zu gestalten und zu steuern.

Verbesserte Identitätsunterstützung verbessert das Nutzererlebnis

Der Apple Business Manager und der Apple School Manager erleichtern die Unterstützung benutzerdefinierter Identitäten. Jeder Identitätsanbieter/jede Identitätsanbieterin wie Microsoft, Google, Okta, Open ID/SKIM kann jetzt eine Verbindung herstellen und einfach verwaltete IDs erstellen: die beste Möglichkeit, Apple Geräte und Benutzer*innen zu verwalten. Nutzer*innen, die mit einem einzigen Schlüssel auf alles zugreifen können, was sie für ihre Arbeit benötigen, sind zufriedenerer Nutzer*innen und im Übrigen auch sicherer.

Diese Entwicklung in Bezug auf die Perspektiven und Kapazitäten bedeutet, dass MDM eine wichtige Rolle spielen wird:

- **Sicherer** (durch die Möglichkeit, dass Deklarationen die Compliance von vornherein festlegen, und durch die Begrenzung der programmatischen Interaktionen mit Low-Level-Binärprogrammen)
- **Mehr Nativität** durch Ermöglichung von Endbenutzerinteraktionen auf der Grundlage von Erklärungen
- **Mehr Nutzen** im Laufe der Zeit (durch Erweiterung der bereits soliden Grundlage von MDM mit DDM)

Weitere Einzelheiten zu den Auswirkungen dieses tiefgreifenden Wandels finden Sie in der JNUC-Präsentation 2023: „**Wie geht es weiter mit MDM?**“

Die Zukunft ist jetzt.

Einer der besten Aspekte dieses enormen Fortschritts ist, dass bestehende MDM-Anbieter*innen seit gestern deklarative Verwaltungsfunktionen nutzen können. Die Arbeit mit einem neuen Protokoll oder einer neuen Serverinfrastruktur muss nicht unterbrochen werden, und Deklarationen und der Statuskanal können Seite an Seite mit bereits vorhandenen MDM-Befehlen und -Profilen verwendet werden. **DDM beeinflusst das Verhalten von MDM nicht im Geringsten.**

Das bedeutet, dass die IT-Abteilung DDM in dem Tempo einführen kann, das für sie am besten geeignet ist, ohne dass alle bestehenden MDM-Workflows auf einmal aktualisiert werden müssen.

Und noch besser: Sie können sofort loslegen!

Wie unterstützt Jamf DDM?

Die enge Zusammenarbeit von Jamf mit Apple bedeutet, dass wir vom ersten Tag an bereit sind, Innovationen von Apple zu unterstützen.

Unterstützung von Anfang an

Jamf Pro aktiviert seit Oktober 2022 automatisch deklarative Geräteverwaltungsfunktionen für kompatible verwaltete Geräte. Geräte mit aktiviertem deklarativem Gerätemanagement melden ihre Zustandsänderungen automatisch an den MDM-Server, und wenn bestimmte Änderungen auftreten, werden sie proaktiv gemeldet und in den Gerätebestandsinformationen aufgeführt. Admins können diese Gerätezustände anpassen.

Kanalunterstützung für drei neue Felder

Insbesondere hat Jamf Pro mit [Jamf Pro 10.46](#) die Unterstützung von DDM-Statuskanälen eingeführt, um drei neue Felder zu melden:

```
`SupplementalBuildVersion`
```

```
`SupplementalOSVersionExtra`
```

```
`Passcode Compliance`
```

Diese neuen Statuskanalelemente werden automatisch aktiviert, sodass die Geräte Jamf Pro sofort selbstständig mit neuen Zuständen aktualisieren können.

iOS spezifische Unterstützung

DDM kann so viel, und es verändert sich so schnell! Im Folgenden finden Sie einige Beispiele dafür, wie wir DDM zur Verbesserung der Benutzerfreundlichkeit und Sicherheit eingesetzt haben:

- Updates auf iOS basierten Geräten verwenden den Passcode auf dem Sperrbildschirm des Geräts, um ein Autorisierungstoken zu generieren, das nach einer bestimmten Zeit abläuft, um die Sicherheit zu erhöhen
- Dieses Token ermöglicht nach Aktivierung durch den Endnutzer/die Endbenutzerin Updates, ohne dass der Nutzer/die Nutzerin sein/ihr Gerät entsperren muss
- Geräte, die für einen bestimmten Zeitraum nicht entsperrt wurden, erhalten diese Updates nicht mehr und der Benutzer/die Benutzerin wird aufgefordert, sie beim Entsperren seines Geräts zuzulassen.

Verwaltete Software-Updates mit DDM

Bevor Apple die DDM-Funktionen einführte, mussten Jamf Administrator*innen entweder eine Massenaktion oder eine Richtlinie senden. Verwaltete Software-Updates, die von DDM unterstützt werden, bieten uns noch mehr Möglichkeiten:

- Die Konfiguration des Software-Aktualisierungsplans ist viel einfacher
- Endnutzer*innen haben nuancierte Aufschuboptionen
- Neue Automatisierungs- und Durchsetzungsfunktionen ermöglichen IT-Administrator*innen mehr Kontrolle
- Proaktive Berichte von Geräten über den Aktualisierungsfortschritt bieten Administrator*innen mehr Transparenz



Blick nach vorn

Da sich das DDM-Protokoll immer weiter ausbreitet, wird Jamf es bestmöglich nutzen und es bei jedem Schritt unterstützen. Zum Beispiel zeigen wir weiterhin unser Engagement, mit Apple Schritt zu halten, indem wir neue Gerätetypen für die Arbeit ermöglichen, wie Apple Vision Pro und Apple Watch, die es den Endnutzern ermöglichen, so produktiv zu sein, wie sie am besten arbeiten.

Die Verwaltung von Apple Geräten war noch nie so spannend wie heute.

Das deklarative Gerätemanagement hat der Entwicklung hin zu einer modernen Verwaltung einen enormen Schub gegeben. Manche würden sie sogar als raketentriebenen bezeichnen.

Wir haben uns von der traditionellen Geräteverwaltung gelöst. Von mehreren Pings und umfangreicher Kommunikation zwischen verwalteten Geräten und Apple und dem MDM-Server sind wir über Nacht zu autonomen Geräten übergegangen. Wir haben uns proaktiv der Zukunft zugewandt.

Die Zukunft von Management und MDM wird in diesem Moment erschaffen, und wir haben die Chance, sie gemeinsam zu gestalten!

Und das Zeitalter des modernen Managements ist angebrochen.

Unternehmen, die in der Lage sind, diese beispiellose Wachstumsphase zu nutzen, werden für die Zukunft gerüstet sein, und die Einführung einer Apple Flotte ist der Weg dorthin.

Zu beachtende Dinge

Werfen Sie einen Blick auf Ihre derzeitige technische Strategie. Ist sie flexibel? Ist es tragbar? Entspricht sie einem modernen Managementansatz für die Verwaltung und den Schutz von Geräten?

Wenn nicht, was könnten Sie durch die Einführung eines modernen Managementansatzes gewinnen? Die Fähigkeit, schnell zu wachsen? Auf der Stelle treten? Um die besten Talente anzuziehen und alle zu vernetzen und zu schützen?

Was könnten Sie verlieren, wenn Sie nicht mithalten?

Das Zeitalter des modernen Managements ist angebrochen. Es liegt an Ihnen, die Chance zu ergreifen und zu sehen, wohin sie Sie führt.

Und Jamf wird Sie bei jedem Schritt unterstützen.

Wenn Sie bereit sind, sich Apple und Jamf auf dem Weg zu einer **modernen Verwaltung** anzuschließen und alle Vorteile der Cloud und von DDM nutzen möchten, können wir Ihnen helfen!