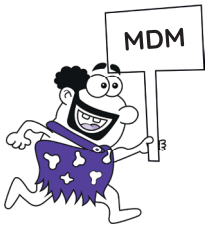
Mobile Device Management (MDM)

TEDKOM

Die zentralisierte Verwaltung Ihrer mobilen Geräteflotte.

Erfahren Sie mehr!

Allgemeines über Mobile Device Management



Was bedeutet Mobile Device Management (MDM)?

- Mobile Device Management (MDM) steht für die zentralisierte Verwaltung von Mobilgeräten wie Smartphones, Notebooks, PDA´s oder Tablets durch einen oder mehrere Administratoren.
- Die Verwaltung bezieht sich auf die Inventarisierung von mobilen Geräten in Organisationen, die Software-, Daten- und Richtlinienverteilung sowie den Schutz der Daten auf diesen Geräten.
- Das Mobile Device Management ist ein Modul von mehreren, welches zum Enterprise Mobility Management (EMM) zählt.

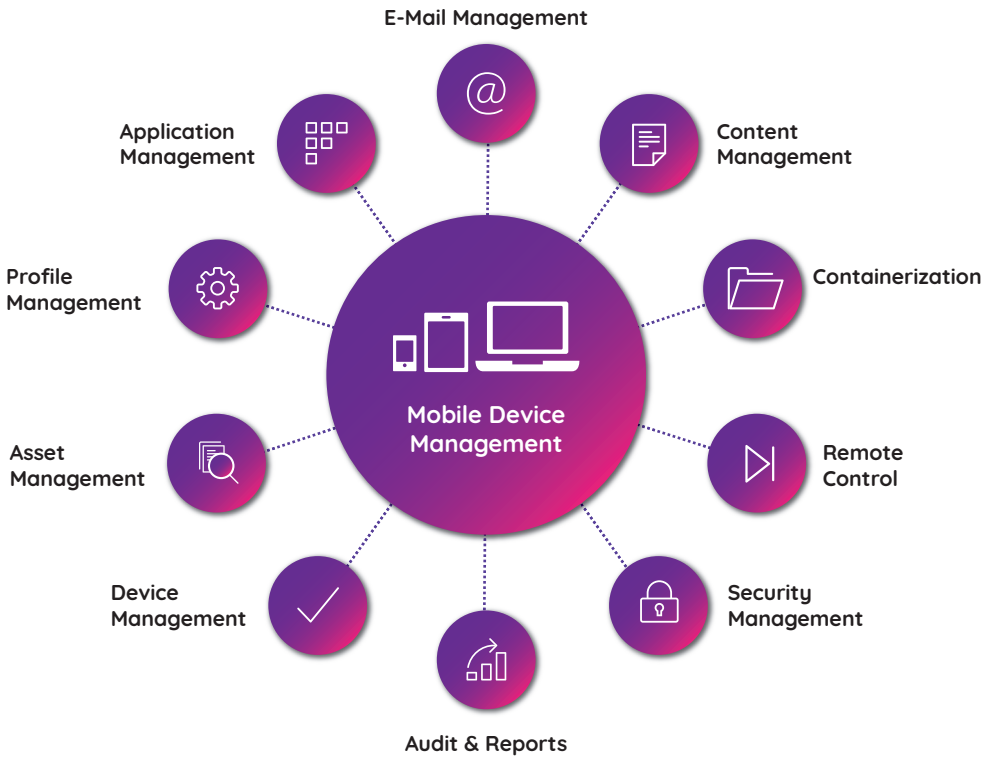
Enterprise Mobility Management (EMM)

- MDM – Mobile Device Management
- MAM – Mobile Application Management
- MCM – Mobile Content Management
- IAM – Identy Access Management

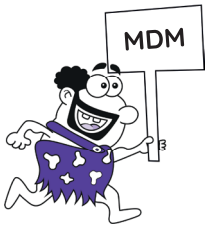
Mobile Device Management - Aufgaben und Vorteile

Mobile Device Management bietet eine elegante Lösung zum Thema Sicherheitsbedenken und möglicher Zugriffe, die mit Unternehmensmobilität einhergehen.

- Verwalten Sie große Mobilgerätebereitstellungen von einer einzigen Konsole aus.
- Registrieren Sie Geräte in Ihrer Unternehmensumgebung schnell und mühelos.
- Konfigurieren und aktualisieren Sie Geräteeinstellungen Over-the-Air.
- Setzen Sie Sicherheits- und Konformitätsrichtlinien durch.
- Sichern Sie den mobilen Zugriff auf Unternehmensressourcen.
- Führen Sie Remote-Sperren und -Wipes verwalteter Geräte aus.



Unser Vorschlag für Ihr Mobile Device Management



Die MDM-Applikation AirWatch® by VMware®

AirWatch® wurde als das erfolgreichste System für Software und Stand-Alone Management-Systeme für Inhalte, Anwendungen und E-Mail durch VMware® aufgekauft und weitergeführt.

AirWatch® by VMware® ist das führende Mobile Device Management auf dem Markt, die Enterprise Mobility Management (EMM) Technologie, auf der VMware® Workspace ONE™ basiert.

Problemlose Echtzeit-Verwaltung von mobilen Geräten im Unternehmen. Schnelle Inbetriebnahme, Over-the-Air Konfiguration und mehr.

Es unterstützt die gängigen Betriebssysteme.

airwatch by vmware

Workspace ONE™ UEM

Unsere Service-Klassen: Standard, Premium und Premium+

Weitere Unternehmenssysteme zur Integration

1

Profitieren Sie von der erweiterten MDM-Funktionalität, indem Sie Ihre AirWatch® Umgebung in vorhandene Unternehmensinfrastrukturen integrieren, einschließlich E-Mail-Verwaltung in SMTP, Verzeichnisdienste und Inhaltsverwaltungs-Repositorys. AirWatch® kann in folgende interne Komponenten integriert werden:

- **E-Mail-Relay (SMTP)**
  Bieten Sie Sicherheit, Transparenz und Kontrolle für E-Mails, die über die Mobilfunkverbindung gesendet werden.
- **Verzeichnisdienste (LDAP/AD)**
  Nutzen Sie vorhandene Unternehmensgruppen, um Anwender und Geräte zu verwalten.
- **Microsoft® Zertifikatsdienste**
  Nutzen Sie Ihre bestehende Microsoft® Zertifikats-infrastruktur für die AirWatch® Bereitstellung.
- **Simple Certificate Enrollment Protocol (SCEP PKI)**
  Konfigurieren Sie Zertifikate für WLAN, VPN, Microsoft® EAS und mehr.
- **E-Mail Management Exchange 2010 (PowerShell)**
  Stellen Sie eine sichere Verbindung mit AirWatch® her, um Richtlinien mit Unternehmens-E-Mail-Servern durchzusetzen.
- **BlackBerry® Enterprise Server (BES)**
  Integrieren Sie AirWatch® in BES zur optimierten BlackBerry® Verwaltung.

Weitere Unternehmenssysteme zur Integration

2

- **Drittanbieter-Zertifikatsdienste**
  Importieren Sie Zertifikatsverwaltungssysteme, die mithilfe der Konsole verwaltet werden sollen.

- **Lotus® Domino-Webdienst (HTTPS)**
  Greifen Sie mit Ihrer AW-Bereitstellung auf Lotus® Domino Inhalte und Funktionen zu.

- **Inhalts-Repositorys**
  Integrieren Sie AirWatch® in SharePoint, Google™ Drive, SkyDrive® , Dateiserver und Netzwerkfreigaben.

- **Syslog (Ereignisprotokolldaten)**
  Exportieren Sie die Ereignisprotokolldaten, sodass diese über alle integrierten Server und Systeme hinweg eingesehen werden können.

- **Unternehmensnetzwerke**
  Konfigurieren Sie WLAN- und VPN-Einstellungen und stellen Sie Geräteprofile mit Anwenderanmelde-daten für den Zugriff bereit.

- **Security Information and Event Management (SIEM)**
  Erfassen und kompilieren Sie Geräte- und Konsolen-daten, um Sicherheit und Konformität mit Vorschriften und Unternehmensrichtlinien zu gewährleisten.

Datenschutz und Datenerfassung

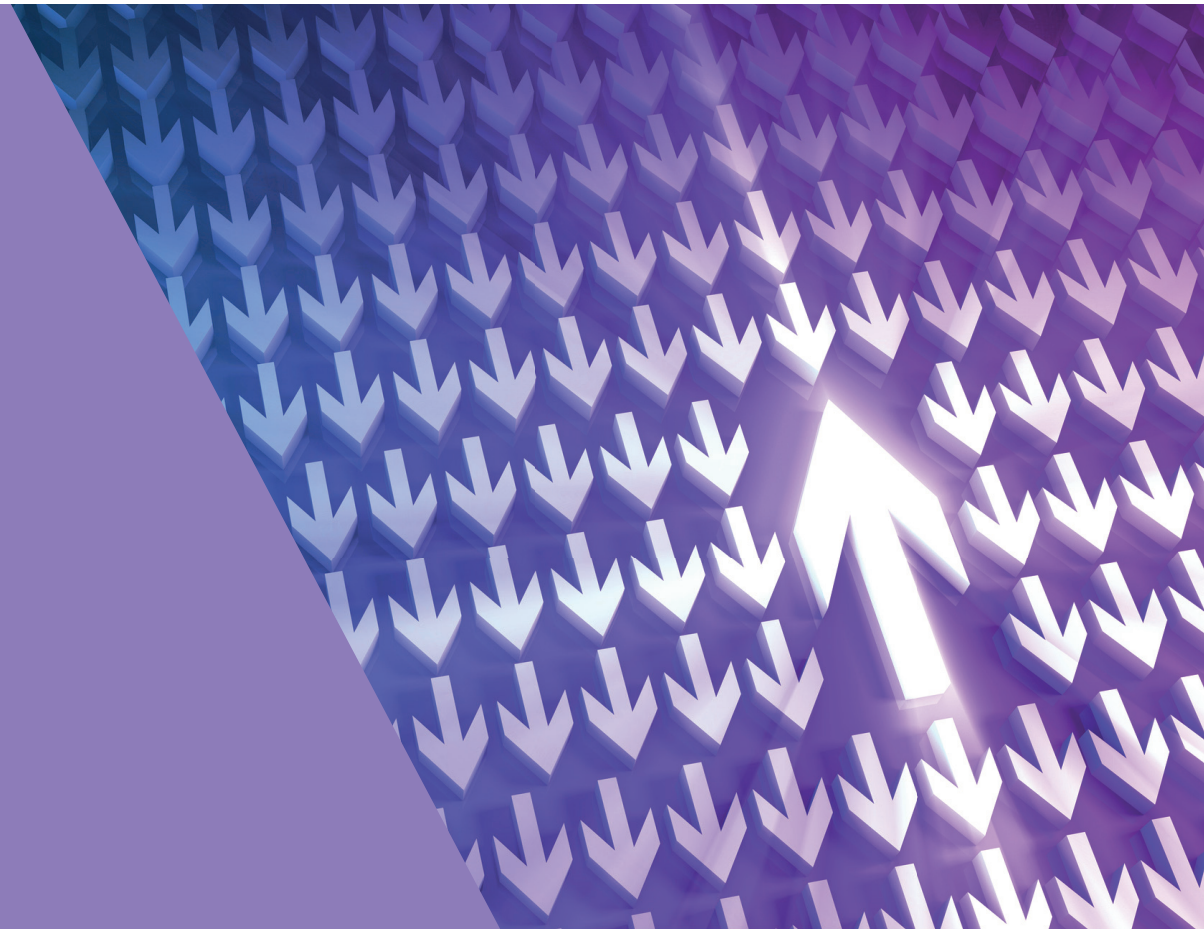
- Es ist wichtig, dass Sie Ihre Endanwender bei der Registrierung bei AirWatch® darüber informieren, wie Ihre Daten erfasst und gespeichert werden.

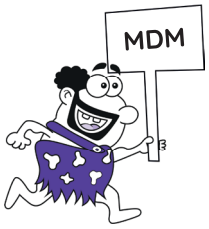
- Die AirWatch® Konsole ermöglicht Ihnen die Erstellung eines anwenderdefinierten Datenschutz-hinweises, um Anwender darüber zu informieren, welche Daten Ihr Unternehmen von registrierten Geräten erfasst.

- Hierbei unterscheidet man, ob das Gerät vom Unternehmen gestellt wurde oder vom Mitarbeiter ins Unternehmen gebracht wurde (bring your own device).

- Des Weiteren empfiehlt es sich Nutzungsbedingungen anzulegen, die durch den Anwender bestätigt werden müssen.

Implementierung und Anwendung der MDM Applikation





Benutzer in der Mobile Device Management Applikation

Die Anlage von Benutzern kann auf unterschiedliche Art und Weise durchgeführt werden. Entweder automatisiert über eine Schnittstelle oder auch über das Portal.

Standard-Anwenderkonten
Erstellen Sie für Ihre Endanwender Standard-Anwenderkonten in AirWatch®, wenn keine Integration in einen Verzeichnisdienst vorhanden ist. Standard-Anwenderkonten sind auch für Testzwecke nützlich, da sie schnell erstellt und im Anschluss gelöscht werden können.

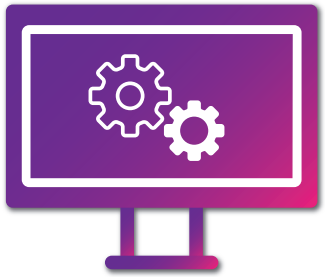
Verzeichnisbasierte Anwenderkonten
Durch die Integration in einen bestehenden Verzeichnisdienst können Anwender automatisch importiert werden. So müssen Anwender nicht manuell zur AirWatch® Konsole hinzugefügt werden.

Unterschiede der Betriebssysteme

Generell unterscheidet man zwischen folgenden Betriebssystemen:

- Android™
- Android™ (Legacy)
- Apple® iOS
- Apple® macOS®
- Apple® tvOS™
- BlackBerry®
- BlackBerry 10™
- Tizen™
- Windows 10™
- Google™ Chrome OS (Legacy)

Jedes Betriebssystem unterscheidet sich in den Einstellmöglichkeiten zu den anderen.
So ist Apple® iOS zum Beispiel in den Restriktionen viel umfangreicher als Android™.



Zuweisungsgruppen

Zuweisungsgruppen ist ein Oberbegriff, der zur Kategorisierung bestimmter Gruppierungsstrukturen der Verwaltung innerhalb von AirWatch® verwendet wird.

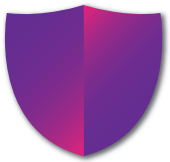
Organisations-, Smart- und Anwendergruppen weisen eigene umfassende Funktionsgruppen und Eigenschaften auf und sind unverwechselbar. Ihre Gemeinsamkeit besteht in der Art und Weise in der sie verwendet werden können, um mühelos Inhalte an Anwendergeräte zuzuweisen.

Die Funktion Zuweisungsgruppen ermöglicht einem Administrator die Verwaltung dieser drei Gruppierungsstrukturen von einer zentralen Stelle.

Geräte-Registrierung

AirWatch® bietet mehrere Optionen für die Registrierung eines Geräts, die für dessen Verwaltung erforderlich ist. Folgende Optionen stehen zur Auswahl:

- Registrieren von Geräten mit AirWatch® Agent
- Registrierung auf Aufforderung per Benachrichtigung
- „Einfachklick“ Registrierung
- Web-Registrierung
- 2-Faktor-Authentifizierung
- Endanwender-Registrierung
- Einzelanwender-Geräte-Staging
- Mehranwender-Geräte-Staging



Profile und Ressourcen

Geräte werden hauptsächlich mit Geräteprofilen verwaltet. Sie stellen Einstellungen dar, die Ihnen zusammen mit Konformitätsrichtlinien dabei helfen, Unternehmensregeln und -verfahren durchzusetzen. Erstellen Sie Profile für alle Plattformtypen und konfigurieren Sie dann eine Nutzlast, die aus den von Ihnen für jedes einzelne Profil konfigurierten, individuellen Einstellungen für die einzelnen Plattformtypen besteht.

Bei der Profilanlage unterscheidet man nach den unterschiedlichen Nutzlasten. Beispiele für Nutzlasten:

- Restriktionen
- WLAN
- VPN
- E-Mail
- ...

Konformitätsrichtlinien

Die Compliance Engine ist ein automatisches Tool von AirWatch®, welches sicherstellt, dass alle Geräte Ihre Richtlinien erfüllen. Diese Richtlinien enthalten möglicherweise grundlegende Sicherheitseinstellungen wie z. B. die Anforderung eines Passcodes sowie das Vorhandensein einer Mindestsperrdauer für Geräte.

Eventuell möchten Sie bestimmte spezielle Vorsichtsmaßnahmen festlegen und durchsetzen. Bei diesen Vorsichtsmaßnahmen handelt es sich beispielsweise um die Festlegung einer Kennwortstärke, das Sperren bestimmter Anwendungen per Blacklist und das Anfordern regelmäßiger Geräte-Check-Ins, um sicherzustellen, dass die Geräte sicher und mit AirWatch® verbunden sind.

Sobald festgestellt wird, dass Geräte nicht konform sind, fordert die Compliance Engine die Anwender zur Behandlung von Konformitätsfehlern auf, um disziplinarische Maßnahmen auf dem Gerät zu verhindern. Die Compliance Engine kann beispielsweise eine Nachricht auslösen, die den Anwender darüber verständigt, dass sein Gerät nicht konform ist.

Sie können Eskalationen automatisieren, falls keine Korrekturen vorgenommen werden. Dabei wird das Gerät gesperrt und der Anwender aufgefordert, sich zur Entsperrung des Geräts an Sie zu wenden. Diese Eskalationsschritte, Disziplinarmaßnahmen, Toleranzperioden und Nachrichten sind bei der AirWatch® Konsole alle anpassbar.

Methoden zur Messung

- **Echtzeitkonformität (Real Time Compliance, RTC)**
  Ungeplante Stichproben vom Gerät werden verwendet, um zu bestimmen, ob das Gerät konform ist. Die Proben werden vom Administrator auf Wunsch angefordert.

- **Modulkonformität**
  Die Compliance Engine, ein Software-Algorithmus, der geplante Stichproben erhält und misst, bestimmt hauptsächlich die Konformität eines Geräts. Die Zeitintervalle, in denen der Zeitplaner gestartet wird, werden vom Administrator in der Konsole festgelegt.

Durchsetzung mobiler Sicherheitsrichtlinien

- **Plattform auswählen**
  Bestimmen Sie, auf welcher Plattform Sie Konformität durchsetzen möchten. Nachdem Sie eine Plattform ausgewählt haben, wird Ihnen niemals eine Option angezeigt, die nicht für diese Plattform gilt.

- **Richtlinien erstellen**
  Passen Sie Ihre Richtlinien so an, dass alle der folgenden Aspekte berücksichtigt werden: Anwendungsliste, Gefährdungsstatus, Verschlüsselung, Hersteller, Modell- und BS-Version, Passcode und Roaming.

- **Eskalation festlegen**
  Konfigurieren Sie zeitbasierte Aktionen in Minuten, Stunden oder Tagen und wählen Sie für diese Aktionen einen mehrstufigen Ansatz.

- **Aktionen bestimmen**
  Senden Sie eine SMS, E-Mail oder Push-Benachrichtigung an das Gerät des Anwenders oder senden Sie nur dem Administrator eine E-Mail. Fordern Sie an, dass Geräte einchecken. Entfernen oder blockieren Sie bestimmte Profile. Installieren Sie Konformitätsrichtlinien. Entfernen oder blockieren Sie Anwendungen und führen Sie ein Enterprise Wipe durch.

- **Zuweisungen konfigurieren**
  Weisen Sie Ihre Konformitätsrichtlinie nach Organisations- oder Smartgruppe zu und bestätigen Sie dann die Zuweisung nach Gerät.

TEDKOM

... mit dem besten TEDKOM-Service.

Maßgeschneiderte Kommunikation für Ihr Business.

TEDKOM

Telekommunikation & Dienstleistung
Franz-Sigel-Straße 21
68753 Waghäusel

Telefon 07254 77 446 0
support@tedkom.de
www.tedkom.de