Aktuelle Herausforderungen

Immer mehr Mitarbeiter nutzen mobile Endgeräte, um auf Unternehmensressourcen zuzugreifen und ihre Aufgaben zu erledigen. Viele Unternehmen begreifen dies als Chance, die Produktivität ihrer Mitarbeiter zu verbessern, und fördern Praktiken wie Corporate Owned Personal Enabled (COPE) und Bring Your Own Device (BYOD). Allerdings birgt der einfache Zugriff auf Unternehmensressourcen – den Mitarbeiter quasi immer mit sich herumtragen – auch verschiedene Gefahren für den Datenschutz und die Sicherheit Ihres Unternehmens.

Abhilfe schafft eine umfassende, integrierte Mobile-Device-Management(MDM)-Lösung, die Ihre IT-Abteilung bei allen Aspekten rund um die Nutzung mobiler Endgeräte unterstützt – von der Registrierung neuer Geräte bis zum Löschen von Unternehmensdaten, wenn ein Mitarbeiter Ihr Unternehmen verlässt.

Wie Mobile Device Manager Plus in Ihre IT-Umgebung passt

Mit Mobile Device Manager Plus können Sie Ihre gesamten mobilen Endgeräte sicher in die Unternehmens-IT einbinden und verwalten. Gleichzeitig hilft die Enterprise-Mobility-Management-Lösung die IT-Abteilung bei administrativen Aufgaben zu entlasten, die Sicherheit der Geräte zu verbessern und das Risiko eines Datenverlusts zu reduzieren.

Highlights

Unterstützte Betriebssysteme

- iOS 4.0 und höher
- Android 4.1 und höher
- Windows Phone 8.0 und höher
- Chrome OS, macOS und Windows 10 Desktops/Laptops
- Samsung Knox
- iPadOS

Compliance mit

CJIS, HIPAA, PCI DSS COMPLIANT, ISO

Ausgezeichnet von

FORRESTER, IDC Analyze the Future, EMA

Mehr als **10 Jahre** Erfahrung im Enterprise Mobility Management

Weltweit vertrauen mehr als **10.000** IT-Experten auf Mobile Device Manager Plus

Derzeit werden mehr als **500.000** mobile Endgeräte mit der ManageEngine-Lösung verwaltet

Unterstützung von **17** Sprachen

In **185** Ländern im Einsatz

Kostenlose Verwaltung von bis zu 25 Endgeräten.

Verwaltung mobiler Apps

- Erstellen Sie Ihren eigenen, vom Unternehmen autorisierten App-Katalog.
- Verwalten Sie Unternehmens- und Store-Apps (kostenlos/bezahlt) sowie App-Lizenzen umfassend.
- Integrieren Sie Apple Business Manager (ABM), Managed Google Play, Chrome Web Store und Windows Business Store.
- Laden Sie mehrere Versionen von Unternehmens-Apps hoch und testen Sie diese, bevor Sie sie in der Produktivumgebung bereitstellen.
- Installieren/Deinstallieren Sie Apps ohne Benutzereingriff.
- Beschränken Sie die Verwendung bestimmter Geräte mit dem Kioskmodus auf eine einzelne Anwendung oder mehrere Apps.
- Beschränken Sie Geräte für eine bestimmte Dauer auf die Ausführung einer einzigen App.
- Passen Sie das Layout von Apps und Web-Verknüpfungen auf Geräten im Kioskmodus an, um ein einheitliches Benutzererlebnis zu ermöglichen.
- Konfigurieren Sie App-Einstellungen und -Konfigurationen bereits während der Installation mit Managed App Configurations.
- Stellen Sie Apps und Daten auf Geräten in Containern bereit, um einen Zugriff auf Unternehmensdaten durch Unbefugte zu verhindern.
- Blockieren Sie Apps, die nicht den Sicherheitsvorschriften Ihres Unternehmens entsprechen, und stellen Sie sicher, dass Benutzer nur Apps aus vertrauenswürdigen Quellen installieren.

Zuverlässiger Support für mobile Endgeräte

- Überwachen Sie Geräte mit aktuellen Geräteinformationen.
- Erkennen Sie Geräte-, Benutzer- oder Anwendungsprobleme über eine zentrale Plattform.
- Vermeiden Sie Probleme mit dem Schutz vor dem Zurücksetzen auf die Werkseinstellungen.
- Aktualisieren Sie Konfigurationseinstellungen in Echtzeit.

Sicherheitsmanagement für mobile Endgeräte

- Erzwingen Sie Passwörter, die den Sicherheitsstandards Ihres Unternehmens entsprechen.
- Schränken Sie Gerätefunktionen wie die Verwendung der Kamera, von iCloud, Passbook, iTunes etc. ein.
- Erfassen Sie bei Bedarf den geografischen Standort der verwalteten Geräte und lassen Sie sich eine Historie der von den Unternehmensgeräten durchlaufenen Standorten erstellen.
- Stellen Sie sicher, dass Unternehmensdaten innerhalb des Firmengeländes oder eines definierten virtuellen geografischen Bereichs bleiben, indem Sie einen Geofence für bestimmte Gerätegruppen definieren.
- Erkennen Sie Root- und Jailbreak-Geräte und entfernen Sie diese umgehend aus dem Unternehmensnetzwerk.
- Verhindern Sie Datenverlust oder -diebstahl durch vollständiges Löschen von Geräten oder der gesamten Unternehmensdaten auf einem Gerät.
- Sperren Sie Geräte aus der Ferne, um einen Missbrauch von verlorenen oder gestohlenen Geräten zu verhindern.
- Sichern Sie Unternehmensdaten auf Ihren Mac-Computern, indem Sie diese direkt verschlüsseln und das Starten von einem internen oder externen Speichergerät verhindern.
- Generieren und verteilen Sie benutzerspezifische Zertifikate, indem Sie CA-Server in MDM integrieren.

Sichere Content-Verteilung

- Erstellen Sie ein Content-Repository zur Speicherung von Dokumenten und Medien.
- Verteilen Sie Dokumente in verschiedenen Formaten auf sichere Weise.
- Gewährleisten Sie den Benutzern einen sicheren Zugriff auf die über MDM verteilten Inhalte, indem Sie Sicherheitsrichtlinien konfigurieren.
- Kontrollieren Sie die Weitergabe von Inhalten an nicht verwaltete Geräte und Cloud-Dienste von Drittanbietern.

Verfügbare Produktvarianten

On-Premises | SaaS(Cloud) | MSP

Smartes Enrollment von mobilen Geräten

- Registrieren Sie Geräte over-the-air (OTA) per E-Mail oder SMS.
- Automatisieren Sie die Registrierung von mehreren Apple-, Android- und Windows-Geräten auf einmal mit Apple Business Manager (ABM), Windows AutoPilot (Azure), Zero Touch Enrollment und Samsung Knox Enrollment.
- Nutzen Sie Einmal-Passwörter (OTP) oder die Active Directory (AD)-Zugangsdaten des Benutzers für die Authentifizierung der Geräteanmeldung.
- Erlauben Sie Ihren Benutzern, ihre eigenen Geräte über ein Self-Service-Portal zu registrieren.
- Registrieren und verwalten Sie mehrere Geräte für einen Benutzer.

Vollständige und sichere E-Mail-Verwaltung

- Richten Sie over-the-air (OTA) E-Mail-Sicherheitsrichtlinien für Geräte ein.
- Stellen Sie E-Mail-Anwendungen in Containern bereit, um unbefugten Zugriff auf E-Mails zu verhindern.
- Verhindern Sie, dass Anwender Änderungen an einem Firmen-E-Mail-Konto oder an den verwendeten Konfigurationen vornehmen.
- Lassen Sie sich E-Mail-Anhänge sicher anzeigen und speichern Sie diese direkt in der „ME MDM"-App.
- Ermöglichen Sie einen eingeschränkten Zugriff auf Exchange On-Premise und Office 365.

Unterstützte Browser

Um Mobile Device Manager Plus nutzen zu können, muss einer der folgenden Browser installiert sein:

- Internet Explorer 7 oder höher
- Google Chrome 20 oder höher
- Mozilla Firefox 4 oder höher
- Apple Safari 5 oder höher

Hardware-Anforderungen

Mobile Device Manager Plus läuft in der On-Premises-Variante unter Microsoft Windows.
Detaillierte Informationen zu den Hardware-Anforderungen finden Sie hier.

Sofortiges Aktualisieren von Betriebssystemen auf mobilen Geräten

- Installieren Sie Betriebssystem-Updates unbemerkt auf verwalteten mobilen Geräten.
- Schränken Sie die Möglichkeiten für Benutzer ein, ihr mobiles Betriebssystem selbst zu aktualisieren.
- Benachrichtigen Sie Anwender, wenn Updates für mobile Betriebssysteme verfügbar sind.
- Wählen Sie die sofortige, verzögerte oder zeitlich begrenzte Bereitstellung von mobilen Betriebssystemen.

Effizientes Verwalten mobiler Geräte

- Verfolgen Sie Details zu mobilen Geräten wie Zertifikate, installierte Anwendungen und Speichernutzung, um auf dem Laufenden zu bleiben.
- Erhalten Sie detaillierte Berichte über das Hardware- und Software-Inventar.
- Erstellen Sie benutzerdefinierte Berichte für alle spezifischen Anforderungen Ihres Unternehmens.
- Überwachen Sie den Akkuladezustand von Geräten und lassen Sie sich benachrichtigen, wenn der Batteriestand unter einen bestimmten Wert fällt.
- Beheben Sie Gerätefehler aus der Ferne in Echtzeit.
- Benachrichtigen Sie Benutzer über Notfälle und geplante Wartungsarbeiten, indem Sie Ankündigungen an die Geräte senden.
- Nutzen Sie iPads als gemeinsam genutzte Geräte, indem Sie mehreren Benutzern Zugriff auf ein Gerät ermöglichen und dabei die Privatsphäre der Benutzer gewährleisten.

Integrationen

- Helpdesk-Lösungen: Spiceworks, ServiceNow, ServiceDesk Plus, Jira Servicedesk und Zendesk.
- Business-Process-Automation-Anwendungen: Zoho Creator und Zoho CRM
- Analyse-Software: Analytics Plus
- Öffentliche APIs ermöglichen Integrationen von Drittanbieter-Anwendungen

Versionen

Mobile Device Manager Plus ist in 3 Versionen erhältlich

Free Edition
Vollständige Verwaltung von bis zu 25 Geräten

Standard Edition
Basisfunktionen für das Mobile Device Management

Professional Edition
Alle Funktionen, die Sie für die Verwaltung der mobilen Endgeräte Ihres Unternehmens benötigen.

Kontakt

Weitere Informationen

www.manageengine.de/mobiledevicemanagerplus

Ihr ManageEngine-Partner:

MicroNova AG
Unterfeldring 6, D-85256 Vierkirchen
Tel.: +49 8139 9300-456
E-Mail: **sales-ManageEngine@micronova.de**
Support: **www.manageengine.de/support**

ManageEngine
IT Management, Simplified