iOS-Geräteverwaltung

VMware Workspace ONE UEM

Die aktuellste technische Dokumentation finden Sie auf der VMware-Website unter:

https://docs.vmware.com/de/

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware Global, Inc.
Zweigniederlassung Deutschland
Willy-Brandt-Platz 2
81829 München
Germany
Tel.: +49 (0) 89 3706 17 000
Fax: +49 (0) 89 3706 17 333
www.vmware.com/de

Inhalt

Einführung in die Verwaltung von iOS-Geräten

1

Workspace ONE UEM powered by AirWatch bietet Ihnen eine Reihe leistungsfähiger Mobilitätsverwaltungslösungen zum Registrieren, Sichern, Konfigurieren und Verwalten der iOS-Geräte in Ihrer Umgebung.

Über die Workspace ONE UEM Console können Sie folgende Aktionen ausführen:

- Verwalten des gesamten Lebenszyklus von unternehmens- und mitarbeitereigenen Geräten
- Endbenutzer dazu befähigen, Aufgaben selber auszuführen, zum Beispiel die Registrierung mit dem Self-Service Portal (SSP)
- Sicherstellen, dass Geräte konform sind und gesichert werden, indem bestimmten Gruppen und Einzelpersonen in Ihrer Organisation Profile zugewiesen werden.
- Integrieren Ihrer vorhandenen Unternehmensanwendungen in das Workspace ONE UEM Software Development Kit (SDK), um ihre Funktionalität zu verbessern
- Einsetzen von Tools und eines durchsuchbaren, anpassbaren Dashboards für die laufende Wartung und Verwaltung Ihrer Geräteflotte.

Unterstützte iOS-Geräte

Workspace ONE UEM unterstützt iPhone-, iPad- und iPod touch-Geräte mit iOS v.5.0 und höher. Für bestimmte Workspace ONE UEM- und iOS-Funktionen sind neuere Versionen der Software erforderlich. Welche Funktionen hiervon betroffen sind und inwiefern, können Sie den Vermerken in diesem Dokument entnehmen.

Dieses Kapitel enthält die folgenden Themen:

Voraussetzungen für iOS-Administratoraufgabe

Sie benötigen folgende Informationen, um die Aufgaben auszuführen. Bereiten Sie diese Informationen vor, bevor Sie fortfahren.

- **UEM-Konsole** – Ihr Zugriff auf die AirWatch Konsole erfolgt mit Administratorrechten, mit denen Sie Profile und Richtlinien erstellen sowie Geräte in der Workspace ONE UEM-Umgebung verwalten können.
- **Anmeldedaten**: Diese Kombination aus Benutzername und Kennwort ermöglicht Ihnen den Zugriff auf Ihre UEM-Konsolenumgebung. Diese Anmeldedaten dürfen die gleichen sein wie die Ihrer Netzwerkverzeichnisdienste oder können in der UEM-Konsole eindeutig definiert werden.
- **APNS-Zertifikat (Apple Push-Benachrichtigungsdienst)** – Dieses Zertifikat ist das für Ihre Organisation herausgegebene Zertifikat, mit dem die Nutzung des Apple Cloud-Messagingdiensts autorisiert wird.

Überblick über die Registrierung von iOS-Geräten

2

Jedes in Ihrem Unternehmen eingesetzte Gerät muss in der Registrierungsumgebung des Unternehmens registriert werden, bevor es mit Workspace ONE UEM kommunizieren kann und über Mobile Device Management (MDM) Zugriff auf interne Inhalte und Funktionen erhält. iOS-Geräte werden mithilfe der im Betriebssystem integrierten MDM-Funktion registriert.

Registrierungsanforderungen

Wenn Sie ein iOS-Gerät registrieren möchten, müssen Sie oder die Endbenutzer zunächst gewisse Informationen erfassen. Welche Informationen die Benutzer benötigen, hängt davon ab, ob Sie ihre Umgebung für die AutoErmittlung mit einer E-Mail-Domäne verknüpft haben.

Wenn Sie Ihrer Umgebung eine E-Mail-Domäne zuordnen, müssen Endbenutzer zum Abschließen der Registrierung ihre E-Mail-Adresse und Anmeldedaten eingeben (und ggf. eine Gruppen-ID aus einer Liste auswählen). Dies kann die Registrierung vereinfachen, da den Endbenutzern diese Informationen wahrscheinlich bereits zur Verfügung stehen.

Sollten Sie für die Registrierung hingegen keine E-Mail-Domäne einrichten, so werden die Endbenutzer dazu aufgefordert, die Registrierungs-URL und die Gruppen-ID einzugeben, die ihnen seitens der Administratoren zur Verfügung gestellt werden müssen.

Weitere Informationen zu den Registrierungsanforderungen finden Sie unter iOS-Geräteregistrierungsanforderungen.

Registrieren eines einzelnen Geräts

Je nachdem, für welche Art der Registrierung Sie sich entscheiden, stehen Ihnen unterschiedliche Funktionen zur Verwaltung der registrierten Geräte zur Verfügung. Workspace ONE UEM bietet eine Matrix, in der unterstützte Funktionen bei Hub-basierten und agentlosen Registrierungstypen verglichen werden. Verwenden Sie diese Matrix, um zu ermitteln, welcher Registrierungstyp für die Anforderungen Ihrer Organisation geeignet ist.

Weitere Informationen zur Gegenüberstellung der Hub-basierten und der browserbasierten Registrierung finden Sie unter Auf dem Registrierungstyp basierende Funktionen für iOS-Geräte.

Hub-basierte Registrierung

Bei der Hub-basierten Registrierung wird über die Workspace ONE Intelligent Hub-Anwendung eine sichere Verbindung zwischen Ihren iOS-Geräten und Ihrer Workspace ONE UEM-Umgebung hergestellt. Die Workspace ONE Intelligent Hub-Anwendung vereinfacht die Registrierung und ermöglicht die Echtzeitverwaltung sowie den Zugriff auf relevante Gerätedaten. Die Hub-basierte Registrierung eignet sich am besten für Umgebungen, deren Benutzer über eine Apple-ID verfügen, da diese für das Herunterladen der Workspace ONE Intelligent Hub-Anwendung aus dem App Store erforderlich ist.

Weitere Informationen zur Hub-basierten Registrierung finden Sie unter Workspace ONE Intelligent Hub für iOS und Registrieren eines iOS-Geräts mit dem Workspace ONE Intelligent Hub.

Browserbasierte Registrierung

Sie haben auch die Möglichkeit der browserbasierten Registrierung mithilfe des systemeigenen Safari-Browsers der iOS-Geräte. Diese Vorgehensweise ist am besten für solche Bereitstellungen geeignet, bei denen Benutzer über keine Apple-ID zum Herunterladen von Workspace ONE Intelligent Hub verfügen.

Weitere Informationen zur browserbasierten Registrierung finden Sie unter Registrieren eines iOS-Geräts mit dem Safari-Browser.

Registrieren mehrerer Geräte gleichzeitig

Je nachdem, ob sich die Geräte in Privat- oder Firmenbesitz befinden, und je nach Art der Bereitstellung empfiehlt es sich unter Umständen, alle Geräte gleichzeitig zu registrieren. Workspace ONE UEM ermöglicht die Registrierung mehrerer Geräte gleichzeitig mithilfe von Apple Configurator 2 und dem Apple Business Manager-Programm zur Geräteregistrierung (DEP).

Registrieren mehrerer Geräte gleichzeitig mithilfe von Apple Configurator 2

Mit Workspace ONE UEM können Unternehmen von den einzigartigen Einrichtungsfunktionen von Apple Configurator 2 profitieren und beispielsweise die iOS-Versionierung durchsetzen und umfassende Sicherungsfunktionen nutzen. Mit Apple Configurator 2 können Sie auf einem Computer mit macOS über eine USB-Verbindung mehrere Geräte gleichzeitig registrieren.

Weitere Informationen zur Verwendung von Apple Configurator für die Massenregistrierung finden Sie unter Mehrere iOS-Geräte mit Apple Configurator gleichzeitig registrieren.

Registrieren von mehreren Geräten gleichzeitig mit dem Apple-Programm zur Geräteregistrierung (DEP)

Die Registrierung von mehreren Geräten gleichzeitig über das Apple-Programm zur Geräteregistrierung (DEP) hat den Vorteil, dass Sie auf den Geräten ein MDM-Profil installieren können, das nicht vom Endbenutzer vom Gerät entfernt werden kann. Zudem können Sie die Geräte im Überwachungsmodus bereitstellen, sodass Ihnen zusätzliche Sicherheits- und Konfigurationseinstellungen zur Verfügung stehen.

Weitere Informationen zur Registrierung mit dem Apple Business Manager finden Sie unter Registrieren von Geräten mit dem Apple Business Manager-Programm zur Geräteregistrierung (DEP).

Dieses Kapitel enthält die folgenden Themen:

- iOS-Geräteregistrierungsanforderungen
- Auf dem Registrierungstyp basierende Funktionen für iOS-Geräte
- Registrieren eines iOS-Geräts mit dem Workspace ONE Intelligent Hub
- Registrieren eines iOS-Geräts mit dem Safari-Browser
- Mehrere iOS-Geräte mit Apple Configurator gleichzeitig registrieren
- Registrieren von Geräten mit dem Apple Business Manager-Programm zur Geräteregistrierung (DEP)
- Benutzerregistrierung

iOS-Geräteregistrierungsanforderungen

Um ein iOS-Gerät zu registrieren, benötigen Sie oder Ihre Endbenutzer Informationen, die abhängig davon sind, ob Sie im Rahmen der AutoErmittlung ihrer Umgebung eine E-Mail-Domäne zuordnen.

Ist ihrer Umgebung eine E-Mail-Domäne zugeordnet, benötigen die Benutzer Folgendes:

- **E-Mail-Adresse** – E-Mail-Adresse, die mit Ihrer Organisation verbunden ist. Zum Beispiel LieschenMueller@mueller.de.
- **QR Code** – Benutzer können einen QR-Code einlesen, der von der UEM-Konsole generiert und über E-Mail empfangen wird.
- **Apple-ID** – Diese Apple-ID wird für jeden Benutzer benötigt, der eine Hub-basierte Registrierung ausführt.

Bei einer Ihrer Umgebung nicht zugeordneten E-Mail-Domäne:

Sollte einer Umgebung keine Domäne zugeordnet sein, wird der Endbenutzer aufgefordert, eine E-Mail-Adresse einzugeben. Da AutoErmittlung nicht aktiviert ist, werden Endbenutzer aufgefordert, folgende Informationen einzugeben:

- **Registrierungs-URL** – Dies ist die für die Registrierungsumgebung Ihrer Organisation eindeutige URL. Sie leitet den Benutzer direkt zur Registrierungsseite. Beispiel: **https://<environment name > .com/enroll**.
- **Gruppen-ID** – Diese Gruppen-ID ordnet das Gerät eines Benutzers seiner Unternehmensrolle zu und wird in der UEM-Konsole für eine bestimmte Unternehmensgruppe festgelegt. Zeigen Sie auf das Dropdown-Menü „Unternehmensgruppe“, um die Gruppen-ID der aktuellen Gruppe zu sehen.
- **Apple-ID** – Diese Apple-ID wird für jeden Benutzer benötigt, der eine Hub-basierte Registrierung ausführt.

Auf dem Registrierungstyp basierende Funktionen für iOS-Geräte

Folgende Matrix führt die unterstützten Funktionen für Hub-basierte und agentlose Registrierungstypen auf: Verwenden Sie diese Matrix, um zu ermitteln, welcher Registrierungstyp für die Anforderungen Ihrer Organisation geeignet ist.

Funktion	Hub-basiert	Agentlos
Registrierung		
Erfordert Apple-ID	Erforderlich	Optional
Zustimmung der Nutzungsbedingungen durchsetzen	Ja	Ja
Active-Directory/LDAP/SAML-Integration	Ja	Ja
Zweistufige Authentifizierung	Ja	Ja
Unterstützung für BYOD	Ja	Ja
Unterstützung für Geräte-Staging	Ja[9]	Ja
Branding	Teilweise	Ja
Konfigurationsprofilverwaltung		
Profile prüfen und verwalten	Ja	Ja
Sicherheitseinstellungen (Datenverschlüsselung, Kennwortrichtlinie usw.)	Ja	Ja
Geräterestriktionen	Ja	Ja
Zertifikatsverwaltung	Ja	Ja
E-Mail- und Exchange ActiveSync-Verwaltung	Ja	Ja
Gerätedaten		
Gerätedaten (Modell, Seriennummer, IMEI-Nummer usw.)	Ja	Ja
GPS-Nachverfolgung	Ja	Nein

Funktion	Hub-basiert	Agentlos
Telefonnummer	Ja	Ja
Speicherdaten	Ja	Ja
Akkudaten	Ja	Ja
UDID	Ja	Ja
Gefahren-/Jailbreak-Erkennung	Ja	Ja†
Aktivierungssperrstatus	Ja	Ja
Status von „Mein iPhone suchen“	Ja	Ja
iCloud Backup-Status	Ja	Ja
Zeitpunkt der letzten Sicherung	Ja	Ja
Netzwerkdaten		
Mobilfunkdaten (MCC/MNC, SIM-Karteninfo usw.)	Ja	Ja
Telekommunikation – Roamingdaten	Ja	Ja
Telekommunikation – Nutzungsdaten	Ja	Ja†
IP-Adresse	Ja	Ja†
Bluetooth-MAC-Adresse	Ja	Ja
WLAN-MAC-Adresse	Ja	Ja
Verwaltungsbefehle		
Gerät auf Werkseinstellungen zurücksetzen	Ja	Ja
Enterprise Wipe	Ja	Ja
Gerät sperren	Ja	Ja
Kennung löschen	Ja	Ja
E-Mail-Messaging	Ja	Ja
SMS-Messaging	Ja	Ja
APNS-Push-Messaging	Ja	Ja†
Remoteansicht	Ja	Nein
Gerätenamen festlegen	Ja	Ja
Kennungsrestriktionen löschen	Ja	Ja
Verwaltung von Anwendungen		
Anwendungen prüfen und verwalten	Ja	Ja
Programm für Volumenlizenzen (VPP)	Ja	Ja
Anwendungsliste	Ja	Ja
Nummern-Badging für Anwendungs-Updates	Ja	Ja†
Inhaltsverwaltung		
Inhaltsverwaltung	Ja*	Ja*

[0] Erfordert, dass der Endbenutzer Einkäufe bei der ersten Synchronisierung überträgt.

† Erfordert eine im Workspace ONE UEM SDK eingebettete Datei auf dem Gerät.

* Erfordert die VMware Content Locker-Anwendung von iTunes.

Registrieren eines iOS-Geräts mit dem Workspace ONE Intelligent Hub

Die Hub-basierte Registrierungsmethode sichert eine Verbindung zwischen einem iOS-Gerät und Ihrer Workspace ONE UEM-Umgebung. Die Workspace ONE Intelligent Hub-Anwendung erleichtert die Registrierung und ermöglicht die Echtzeitverwaltung sowie den Zugriff auf relevante Gerätedaten.

Wenn Sie die Workspace ONE Intelligent Hub-Funktionen umfassend nutzen und gleichzeitig auch die Webregistrierung zulassen möchten, sollten Sie festlegen, dass sich Benutzer nur über Workspace ONE Intelligent Hub registrieren können. So können sich Endbenutzer nur registrieren, wenn sie Workspace ONE Intelligent Hub heruntergeladen haben.

Navigieren Sie zu **Gruppen & Einstellungen > Alle Einstellungen > Geräte & Benutzer > Allgemein > Registrierung > Authentifizierung** und wählen Sie **Hub-Registrierung für iOS anfordern**.

Um ein iOS-Gerät mit dem Workspace ONE Intelligent Hub zu registrieren, führen Sie die folgenden Schritte aus:

Verfahren

1. Navigieren Sie im Safari-Browser zu **getwsone.com**. Workspace ONE UEM fordert den Endbenutzer automatisch auf, zum App Store zu wechseln und die Workspace ONE Intelligent Hub-Anwendung herunterzuladen. Befolgen Sie die Anweisungen zum Herunterladen. Eine Apple-ID ist erforderlich, um den Workspace ONE Intelligent Hub vom iTunes Store herunterzuladen.
2. Wählen Sie die Workspace ONE Intelligent Hub-Anwendung aus, und wählen Sie dann eine der folgenden Authentifizierungsmethoden aus:
    a. **E-Mail-Adresse** – Wählen Sie dies, wenn in Ihrer Umgebung AutoErmittlung konfiguriert ist. Außerdem werden Sie möglicherweise dazu aufgefordert, aus einem Menü Ihre Gruppe auszuwählen.
    b. **Serverdetails** – Wählen Sie diese Option, um die Registrierung über eine Server-URL durchzuführen. Die Server-URL ist der Netzwerkstandort der Workspace ONE UEM-Instanz Ihrer Organisation und die Gruppen-ID der mit Ihrem Gerät verbundenen Gruppe.
    c. **QR-Code** – Wählen Sie diese Option und verwenden Sie das Gerät, um den per E-Mail oder über die Registerkarte „Support“ erhaltenen QR-Code zu scannen.

3 Geben Sie die Anmeldedaten ein, die aus einem **Benutzernamen** und einem **Kennwort** oder einem **Token** oder einer Kombination von beiden bestehen können, um das Gerät zu authentifizieren.

   a Wenn Sie die Anmeldedaten nicht ordnungsgemäß eingeben, wird ein CAPTCHA-Code angezeigt. Geben Sie den angezeigten Captcha-Code ein, um die Authentifizierung abzuschließen.

4 Halten Sie nach Anweisung durch den Administrator den folgenden Verfahrensablauf ein: Wählen Sie **Weiter**, nachdem Sie die jeweilige Seite ausgefüllt haben.

   a Wählen Sie gegebenenfalls den Typ Ihres **Gerätebesitzes**.

   b Akzeptieren Sie gegebenenfalls die **Nutzungsbedingungen** Ihres Unternehmens.

   c Geben Sie gegebenenfalls die **Inventarnummer** des Geräts ein.

5 Wählen Sie nach der Überprüfung der Informationen zur Datenschutzerklärung **Weiter** aus.

6 Sobald Sie zu Safari WebView umgeleitet wurden, werden Sie aufgefordert, das MDM-Profil herunterzuladen. Die folgende Meldung wird angezeigt:

   Diese Website versucht, eine Konfigurationsdatei herunterzuladen. Möchten Sie diesen Vorgang erlauben?

7 Tippen Sie auf **Erlauben** und tippen Sie nach Abschluss des Downloads auf **Schließen**.

   a Tippen Sie für iOS 12.2-Geräte und höher auf **Fortfahren** und öffnen Sie den Hub, um die Bildschirmanweisungen zum Installieren des MDM-Profils zu befolgen, und akzeptieren Sie die MDM-Warnmeldung, indem Sie **Installieren** wählen.

   b Installieren Sie für Geräte unter iOS 12.2 das MDM-Profil, wenn Sie dazu aufgefordert werden, und akzeptieren Sie die MDM-Warnmeldung, indem Sie **Installieren** wählen.

8 Wählen Sie **Zulassen**, um das MDM-Profil herunterzuladen.

9 Installieren Sie das MDM-Profil. Akzeptieren Sie eventuelle Vertrauensnachfragen.

10 Sobald das MDM-Profil installiert ist, navigieren Sie zurück zum Hub.

11 Wählen Sie **Fertig**, um die Registrierung abzuschließen. In einer Meldung wird der Erfolg des Vorgangs angezeigt. Die Registrierung in Workspace ONE UEM ist nun abgeschlossen.

   a Wenn Sie aufgefordert werden, geben Sie eine **Kennung** oder zusätzliche Anmeldedaten für Gemeinschaftsgeräte ein. Um eine Kennung einzurichten, melden Sie sich beim Self-Service-Portal an und befolgen Sie die Anweisungen.

   b Wählen Sie optional **Öffnen** aus, um die Workspace ONE Intelligent Hub-Details anzuzeigen.

Registrieren eines iOS-Geräts mit dem Safari-Browser

Sie können Geräte mit einem webbasierten Registrierungsverfahren registrieren, wobei der systemeigene Safari-Browser des iOS-Geräts genutzt wird. Diese Vorgehensweise ist am besten

für solche Bereitstellungen geeignet, bei denen Benutzer über keine Apple-ID zum Herunterladen von Workspace ONE Intelligent Hub verfügen.

Um ein iOS-Gerät mithilfe eines webbasierten Registrierungsvorgangs zu registrieren, führen Sie die folgenden Schritte aus:

Verfahren

1 Öffnen Sie den Safari-Browser auf dem iOS-Gerät.

2 Navigieren Sie zu **https://<Umgebungs-URL>.com/enroll**.

3 Wählen Sie **Gruppen-ID** oder Ihre **E-Mail-Adresse** aus (wenn die automatische Erkennung für Ihre Umgebung eingerichtet ist), um Ihr iOS-Gerät zu registrieren. Wählen Sie **Weiter**.

4 Geben Sie die Anmeldedaten ein, die aus einem **Benutzernamen** und einem **Kennwort** oder einem **Token** oder einer Kombination von beiden bestehen können, um das Gerät zu authentifizieren.

   a Wenn Sie die Anmeldedaten nicht ordnungsgemäß eingeben, wird ein CAPTCHA-Code angezeigt. Geben Sie den angezeigten Captcha-Code ein, um die Authentifizierung abzuschließen.

5 Halten Sie nach Anweisung durch den Administrator den folgenden Verfahrensablauf ein: Wählen Sie **Weiter**, nachdem Sie die jeweilige Seite ausgefüllt haben.

   a Wählen Sie gegebenenfalls den Typ Ihres **Gerätebesitzes**.

   b Geben Sie gegebenenfalls die **Inventarnummer** des Geräts ein.

   c Akzeptieren Sie die **Nutzungsbedingungen** Ihrer Organisation, falls zutreffend.

6 Laden Sie bei Aufforderung das MDM-Profil herunter. Die folgende Meldung wird angezeigt:

   Diese Website versucht, eine Konfigurationsdatei herunterzuladen. Möchten Sie den Vorgang erlauben?

7 Tippen Sie auf **Erlauben** und tippen Sie nach Abschluss des Downloads auf **Schließen**.

   Sie haben das Profil erfolgreich installiert. Sie können das Profil in den **Einstellungen** anzeigen und mit der Installation fortfahren.

8 Laden Sie das MDM-Profil herunter und installieren Sie es. Akzeptieren Sie eventuelle Vertrauensnachfragen.

   - Installieren Sie für Geräte unter iOS 12.2 das MDM-Profil, wenn Sie dazu aufgefordert werden, und akzeptieren Sie die MDM-Warnmeldung, indem Sie **Installieren** wählen.

- Befolgen Sie für iOS Geräte 12.2 und höher die Bildschirmanweisungen, um das MDM-Profil zu installieren, und akzeptieren Sie die MDM-Warnmeldung, indem Sie **Installieren** wählen.

Hinweis Sie können auch eine agentenlose Registrierung ohne Verwendung von Workspace ONE Intelligent Hub für die webbasierte Registrierung durchführen. Um eine agentenlose Registrierung durchzuführen, navigieren Sie zu **Gruppen & Einstellungen > Alle Einstellungen > Geräte & Benutzer > Allgemein** und stellen sicher, dass das Kontrollkästchen **Hub-Registrierung für iOS** nicht aktiviert ist.

Mehrere iOS-Geräte mit Apple Configurator gleichzeitig registrieren

Mit Apple Configurator können Sie auf einem Computer mit macOS mehrere iOS-Geräte gleichzeitig registrieren, konfigurieren und einsetzen. Kombinieren Sie Apple Configurator mit Workspace ONE UEM, profitieren Sie auch weiterhin von Transparenz für die Verwaltung von Geräten, umfassenden Sicherungsoptionen und fortlaufendem Lebenszyklusmanagement, auch nach der ersten Konfiguration.

Apple Configurator hat folgende Optionen:

- Erstellen Sie ein einziges, zentrales Sicherungs-Image für die einheitliche Konfiguration aller Geräte.
- Installieren Sie das Workspace ONE UEM MDM-Profil als Teil der Konfiguration, um Geräte zu registrieren und zu verwalten.
- Ordnen Sie Geräte bestimmten Benutzern zu, indem Sie Details von eingetragenen Geräten, wie Seriennummer oder IMEI, dem registrierten Gerät eines Benutzers in der UEM-Konsole vor der Registrierung mit Configurator hinzufügen.
- Konfigurieren und aktualisieren Sie Geräteeinstellungen und Anwendungen des Unternehmens Over-the-Air in Workspace ONE UEM.

Anweisungen für die Verwendung des Apple Configurator mit Workspace ONE UEM und weitere Informationen finden Sie im Dokument **VMware Workspace ONE UEM Integration with Apple Configurator**.

Registrieren von Geräten mit dem Apple Business Manager-Programm zur Geräteregistrierung (DEP)

Das Geräteregistrierungsprogramm (Device Enrollment Program, DEP) maximiert die Vorteile der in der Mobilgeräteverwaltung (Mobile Device Management, MDM) registrierten Apple-Geräte.

Das DEP ermöglicht Folgendes:

- Installieren eines vom Endbenutzer nicht löschbaren MDM-Profils auf einem Gerät

- Bereitstellen von Geräten im Überwachungsmodus (nur iOS-). Geräte im Überwachungsmodus können auf zusätzliche Sicherheits- und Konfigurationseinstellungen zugreifen.
- Durchsetzen der Registrierung für alle Endbenutzer
- Optimieren des Registrierungsprozesses und Anpassen an die Anforderungen Ihres Unternehmens
- Verhindern der iCloud-Sicherung durch Deaktivieren der Anmeldung von Benutzern mit ihrer Apple-ID beim Generieren eines DEP-Profils
- Erzwingen von iOS-Updates für alle Endbenutzer

Weitere Informationen finden Sie unter den folgenden Themen:

- Apple Business Manager-Geräteregistrierungsprogramm unter *Einführung in Apple Business Manager*.
- Im Apple Business Support Portal.
- Im Handbuch zum Apple-Geräteregistrierungsprogramm, oder wenden Sie sich an Ihren Apple-Vertreter.

Benutzerregistrierung

Bei der Benutzerregistrierung handelt es sich um eine neue Registrierungsmethode für Geräte mit iOS 13 und höher, mit der Sie Einstellungen, Anwendungen und Unternehmensdaten effektiv verwalten und gleichzeitig die persönlichen Daten des Benutzers schützen können. Mit der Benutzerregistrierung sind Sie berechtigt, Anwendungen zu installieren, Profile zu konfigurieren und Befehle nur für einen verwalteten Benutzercontainer auf dem Gerät und nicht für das gesamte Gerät auszustellen.

Die Benutzerregistrierung erfolgt über MDM und bietet im MDM-Profil, das während der Registrierung auf dem Gerät installiert ist, einen Benutzerkontext, der als „Verwaltete Apple-ID“ bezeichnet wird. Der Benutzerkontext weist das Gerät an, den Benutzer zur Eingabe seiner verwalteten Apple-ID-Anmeldedaten aufzufordern, um das MDM-Profil zu installieren. Nach der Registrierung wird ein spezielles Apple File System (APFS)-Volume für die verwalteten Daten erstellt. Daten im persönlichen Volume können nicht vom verwalteten Volume aus abgerufen werden, sodass die Benutzerdaten privat bleiben.

Aufgrund der Erstellung des neuen verwalteten Datenvolumes sind mehrere vorhandene Verwaltungsfunktionen aus Datenschutzgründen nicht möglich. Wenn beispielsweise eine App manuell vom Benutzer über den App Store installiert wird, wird diese App als persönlich betrachtet und kann nicht von MDM verwaltet werden. Solche benutzerinstallierten Apps müssen zuerst deinstalliert und dann von Workspace ONE UEM neu installiert werden, um verwaltet werden zu können.

Aus diesem Grund lässt Workspace ONE die Benutzerregistrierung über die Intelligent Hub-App nicht zu. Wenn der Intelligent Hub bereits vom Benutzer installiert wurde, deinstallieren Sie den Hub über MDM, und installieren Sie ihn neu, damit die App-Daten von anderen Workspace ONE SDK-fähigen Apps abgerufen werden können.

Einstellungen für die Benutzerregistrierung

Aktivieren Sie die Option „Benutzerregistrierung“ für iOS-Geräte, indem Sie die Seite „Registrierungseinstellungen“ auf der Workspace ONE UEM Console öffnen (**Gruppen und Einstellung > Alle Einstellungen > Geräte und Benutzer > Allgemein > Registrierung**). Wenn Sie die Option aktivieren, können die unterstützten Geräte mit iOS 13 und höher mithilfe der Benutzerregistrierungsmethode von Apple bei der Organisationsgruppe registriert werden. Die Benutzerregistrierung verwendet die verwalteten Apple-IDs der Benutzer anstelle des Registrierungsbenutzernamens, um anzugeben, für welchen Benutzer das Gerät registriert wird. Die verwaltete Apple-ID sollte der E-Mail-Adresse eines Benutzers in Workspace ONE UEM entsprechen.

Registrieren eines iOS-Geräts mithilfe der Benutzerregistrierung

Registrieren Sie ein Gerät mit iOS 13 und höher mit verwalteten Apple-IDs im mit Azur AD verbundenen Apple Business Manager. Das benutzerregistrierte Gerät ermöglicht einen erweiterten Datenschutz für Benutzer, indem verwaltete Daten von persönlichen Daten getrennt werden und gleichzeitig die Kernverwaltungsfunktionen bereitgestellt werden, wie z. B. das Installieren von Apps, Konfigurieren des WLANs und Anfordern einer Kennung.

So registrieren Sie ein iOS-Gerät:

Voraussetzungen

Stellen Sie vor der Benutzerregistrierung sicher, dass Sie die folgenden Voraussetzungen erfüllt sind:

- Apple Business Manager im Verbund mit Azure AD
- Azure AD
- Unbeaufsichtigtes Gerät mit iOS 13 und höher
- Genau ein Registrierungsbenutzer mit einer E-Mail-Adresse, die mit einer verwalteten Apple-ID in Apple Business Manager übereinstimmt

Verfahren

1. Öffnen Sie den Safari-Browser auf dem Gerät mit iOS 13 oder höher, und navigieren Sie zur Benutzerregistrierungs-URL Ihrer Umgebung. Die URL ist der Hostname Ihres Gerätedienst, an den der `/enroll/user`-Pfad angehängt wird.

   Zum Beispiel:

   ```
   https://ds22.awmdm.com/enroll/user
   ```

2 Geben Sie die E-Mail-Adresse des Registrierungsbenutzers ein, die einer verwalteten Apple-ID entspricht.

   Geben Sie optional die Gruppen-ID einer Organisationsgruppe in oder unter der Organisationsgruppe des Registrierungsbenutzers ein. Andernfalls wird die Registrierungsorganisationsgruppe des Benutzers verwendet.

3 Bestätigen Sie den Download des MDM-Profils für die Benutzerregistrierung.

4 Navigieren Sie in der App zu **Einstellungen**, und tippen Sie auf **Bei {Ihr Unternehmen} registrieren**.

5 Tippen Sie auf die Eingabeaufforderungen, um die Eingabeaufforderungen für Authentifizierung und bedingten Zugriff zu Azure AD umzuleiten.

   Azure-AD-Konfigurationen, Benutzertyp, Gerät oder Organisation bestimmen den Typ und die Anzahl der Eingabeaufforderungen.

Ergebnisse

Die Benutzerregistrierung ist jetzt abgeschlossen. Das Gerät beginnt, die Befehle von der UEM Console zu empfangen.

App-Verwaltung auf benutzerregistrierten Geräten

Von Workspace ONE UEM auf benutzerregistrierten Geräten installierte Anwendungen werden verwaltet und mit der verwalteten Apple-ID verknüpft, die zur Registrierung des Geräts verwendet wurde. Anwendungen, die vom Benutzer über den App Store installiert werden, sind mit der persönlichen Apple-ID des Benutzers verknüpft und können nicht verwaltet werden.

Da die Benutzerregistrierung die verwaltete Anwendung mit einer verwalteten Apple-ID verknüpfen muss, wird nur die verwaltete Verteilung mit benutzerbasierten Lizenzen, die in Apple Business Manager erworben wurden, unterstützt. Beispielsweise werden Anwendungen, die über die Registerkarte **Öffentlich** unter der Seite **Ressourcen > Apps** in der UEM Konsole zugewiesen wurden, auf vom Benutzer registrierten Geräten nicht unterstützt. Es gibt keine Unterschiede zwischen der Verwaltung benutzerbasierter Lizenzen für die Benutzerregistrierung im Vergleich zur Geräteregistrierung. Wenn die Anwendung einem benutzerregistrierten Gerät zugewiesen wird, wird der verwalteten Apple-ID, die dem Gerät zugeordnet ist, eine VPP-Lizenz zugewiesen und die App wird installiert.

Weitere Informationen finden Sie im Abschnitt *Verwaltete Verteilung nach Apple-IDs* im Handbuch *Integration in Apple Business Manager*.

Geräteprofile

3

Geräte werden hauptsächlich mit Profilen verwaltet. Konfigurieren Sie Profile, damit Ihre iOS-Geräte sicher bleiben und an Ihre Einstellungen angepasst sind. Sie können Profile als Einstellungen und Regeln betrachten, die Ihnen zusammen mit Konformitätsrichtlinien dabei helfen, betriebliche Regeln und Verfahren durchzusetzen. Sie enthalten Einstellungen, Konfigurationen und Restriktionen, die Sie auf Geräten durchsetzen sollten.

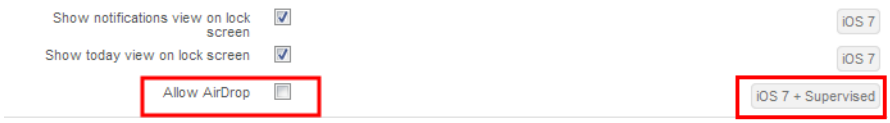
Ein Profil besteht aus den allgemeinen Profileinstellungen und einer spezifischen Nutzlast. Profile funktionieren am besten, wenn sie nur eine einzige Nutzlast enthalten.

iOS-Profile werden auf Benutzerebene oder Geräteebene auf ein Gerät angewendet. Bei der Erstellung von iOS-Profilen wählen Sie die Ebene aus, auf die das Profil angewendet werden soll. Einige Profile können nur auf die Benutzerebene oder nur die Geräteebene angewendet werden.

Anforderung des Überwachungsmodus für Profile

Sie können einige oder alle iOS-Geräte im **Überwachungsmodus** bereitstellen. Der überwachte Modus ist eine Einstellung auf Geräteebene, die Administratoren erweiterte Verwaltungsmöglichkeiten und Restriktionen einräumt.

Bestimmte Profileinstellungen sind nur auf überwachten Geräten verfügbar. Die Einstellung „Überwacht“ auf einem Gerät wird mit einem Symbol auf der rechten Seite markiert, das die Mindest-iOS-Anforderungen für die Erzwingung anzeigt.



Beispielsweise können Sie verhindern, dass Endbenutzer AirDrop verwenden, um Dateien für andere macOS-Computer und iOS-Geräte freizugeben, indem Sie das Kontrollkästchen neben **AirDrop zulassen** deaktivieren. Das Symbol **iOS 7 + überwacht** bedeutet, dass nur Geräte unter iOS 7, die mit Apple Configurator im „Überwacht“-Modus aufgesetzt wurden, von dieser Restriktion betroffen sind. Weitere Informationen finden Sie in den Handbüchern zu **Integration in Apple Configurator** oder **Apple Business Manager**. Eine komplette Liste von Systemanforderungen für iOS und die Überwachungsfunktion finden Sie im Kapitel 10 iOS-Funktionalität: „Überwacht“ im Vergleich zu „Nicht überwacht“.

Gerätezugriff

Mit einigen Geräteprofilen können die Einstellungen für den Zugriff auf ein iOS-Gerät konfiguriert werden. Verwenden Sie diese Profile, um sicherzustellen, dass der Zugriff auf ein Gerät auf autorisierte Benutzer beschränkt wird.

Nachfolgend finden Sie Beispiele für Gerätezugriffsprofile:

- Sichern Sie ein Gerät mit einem Kennungsprofil. Weitere Informationen finden Sie unter Konfigurieren eines Gerätekennungsprofils
- Begrenzen des Geräts auf eine einzige Anwendung mit einem Einzelanwendungsmodus-Profil. Weitere Informationen finden Sie unter Konfigurieren eines Einzelanwendungsmodus-Profils.

Gerätesicherheit

Gewährleisten Sie die Sicherheit Ihrer iOS-Geräte mithilfe von Geräteprofilen. Mit diesen Profilen konfigurieren Sie über Workspace ONE UEM die systemeigenen iOS-Sicherheitsfunktionen oder die vom Unternehmen festgelegten Sicherheitseinstellungen auf einem Gerät.

Nachfolgend finden Sie Beispiele für Gerätesicherheitsprofile:

- Verwenden eines WLAN-Profils zum Verbinden registrierter Geräte mit Ihrem Unternehmens-WLAN, ohne Anmeldedaten für das Netzwerk an Benutzer zu senden. Weitere Informationen finden Sie unter Konfigurieren eines WLAN-Profils.
- Implementieren Sie digitale Zertifikate zum Schutz des Unternehmensinventars. Weitere Informationen finden Sie unter Konfigurieren eines SCEP/Anmeldedaten-Profils
- Sicherstellen des Zugriffs auf interne Ressourcen für Ihre Geräte mit dem VPN-Profil. Weitere Informationen finden Sie unter Konfigurieren eines VPN-Profils (virtuelles privates Netzwerk).

Gerätekonfiguration

Konfigurieren Sie die verschiedenen Einstellungen Ihrer iOS-Geräte mit den Konfigurationsprofilen. Diese Profile konfigurieren die Geräteeinstellungen entsprechend Ihren Unternehmensanforderungen.

Nachfolgend finden Sie Beispiele für Gerätekonfigurationsprofile:

- Einrichten eines Exchange-Kontos auf einem Gerät mit einem Exchange ActiveSync-Profil. Weitere Informationen finden Sie unter Konfigurieren eines EAS Mail-Profils für den systemeigenen Mailclient.
- Setzen Sie eine spezielle Gruppe von Geräten auf die Whitelist, um Apple TV Broadcast-Rechte mit dem AirPlay-Profil zu erhalten. Weitere Informationen finden Sie unter Konfigurieren eines AirPlay Whitelist-Profils.
- Gewährleisten Sie mithilfe des iOS Udates-Profils, dass die Geräte immer auf dem neuesten Stand sind. Weitere Informationen finden Sie unter BS-Update Management.

Dieses Kapitel enthält die folgenden Themen:

Gerätekennungs-Profile

Geräte-Passcode-Profile sichern iOS-Geräte und ihre Inhalte. Konfigurieren Sie die Sicherheitsebene basierend auf den Bedürfnissen Ihres Benutzers.

Wählen Sie strenge Optionen für Mitarbeiter mit hohem Sicherheitsbedarf und flexiblere Optionen für andere Geräte oder jene Mitarbeiter, die an einem BYOD-Programm teilnehmen. Wenn auf einem iOS-Gerät eine Kennung festgelegt ist, stellt diese darüber hinaus eine Hardwareverschlüsselung für das Gerät bereit und erstellt zudem einen Geräteindikator vom Typ **Datensicherheit ist aktiviert** auf der Registerkarte **Sicherheit** der Seite **Gerätedetails**.

Erstellen Sie eine Kennung und führen Sie folgende Konfiguration durch:

- **Komplexität** – Verwenden Sie einfache Kennungen zum schnellen Zugriff oder alphanumerische Kennungen zur Sicherheit. Sie können eine beliebige Mindestanzahl an komplexen Zeichen (@, #, &,! , ,?) für die Kennung verlangen. Zum Beispiel können von Benutzern mit Zugriff auf vertrauliche Inhalte strengere Kennungen verlangt werden.
- **Maximale Anzahl an Fehlversuchen** – Verhindern Sie nicht autorisierten Zugriff, indem Sie nach einer festgelegten Anzahl von Versuchen das Gerät komplett löschen oder blockieren. Diese Option funktioniert gut für unternehmenseigene Geräte, aber nicht für Geräte von Mitarbeitern, die in einem BYOD-Programm registriert sind. Beispiel: Wenn ein Gerät auf fünf Kennungsversuche begrenzt ist und ein Benutzer fünfmal hintereinander eine falsche Kennung eingibt, wird auf dem Gerät ein vollständiger Geräte-Wipe durchgeführt. Wenn einfach das Sperren des Geräts vorzuziehen ist, legen Sie für diese Option **Keine** fest. Das bedeutet, dass Sie die Kennung unbegrenzt häufig wiederholen können.
- **Maximales Kennungsalter** – Damit erzwingen Sie die Kennungserneuerung in einem ausgewählten Intervall. Häufig geänderte Kennungen sind meistens gegenüber nicht autorisierten Parteien weniger anfällig.
- **AutoSperre (Min.)** – Damit sperren Sie das Gerät automatisch nach Ablauf der Zeitperiode. Diese Sperre kann die Gefährdung von Inhalten verhindern, wenn ein Endbenutzer versehentlich sein Telefon irgendwo liegen lässt.

Konfigurieren eines Gerätekennungsprofils

Geräte-Passcode-Profile sichern iOS-Geräte und ihre Inhalte. Konfigurieren Sie einige Einstellungen im Rahmen einer Kennungsnutzlast, um Gerätekennungen basierend auf den Anforderungen Ihrer Benutzer zu erzwingen.

Verfahren

1. Navigieren Sie zu **Ressourcen** > **Profile und Baselines** > **Profile** > **Hinzufügen**. Wählen Sie **Apple iOS**.
2. Konfigurieren Sie die Einstellungen des Profils unter **Allgemein**.
3. Wählen Sie die Nutzlast **Kennung** aus der Liste.

4 Konfigurieren Sie die **Kennungs**einstellungen wie folgt:

Einstellung	Beschreibung
Kennung auf Gerät verlangen	Aktivieren Sie den obligatorischen Kennungsschutz.
Einfachen Wert zulassen	Gestatten Sie dem Endbenutzer, eine einfache numerische Kennung anzuwenden.
Alphanumerischen Wert verlangen	Erlegen Sie dem Endbenutzer eine Beschränkung für die Verwendung von Leerstellen und nicht alphanumerischen Zeichen in der Kennung auf.
Minimale Kennungslänge	Legen Sie die minimal erforderliche Anzahl der Zeichen für die Kennung fest.
Minimale Anzahl komplexer Zeichen	Wählen Sie die Mindestanzahl von komplexen Zeichen (#, $, !, @), die für einen Passcode erforderlich sind.
Maximales Kennungsalter (Tage)	Wählen Sie die maximale Anzahl der Tage, für die die Kennung aktiv sein darf.
AutoSperre (Min.)	Wählen Sie, wie lange das Gerät im Leerlauf sein darf, bevor der Bildschirm automatisch gesperrt wird.
Kennungsverlauf	Wählen Sie die Anzahl der Kennungen, die im Verlauf gespeichert werden und vom Endbenutzer nicht erneut verwendet werden können.
Toleranzperiode für Gerätesperre (Min.)	Wählen Sie eine Dauer in Minuten, für die ein Gerät inaktiv sein kann, bevor es vom System gesperrt wird und der Endbenutzer seine Kennung erneut eingeben muss.
Maximale Anzahl an Fehlversuchen	Wählen Sie die maximale Anzahl an fehlgeschlagenen Versuchen. Wenn der Endbenutzer diese Anzahl an falschen Kennungseingaben vornimmt, wird das Gerät automatisch auf Werkseinstellungen zurückgesetzt.

5 Wählen Sie **Speichern und veröffentlichen**.

Geräterestriktionsprofile

Restriktionsprofile begrenzen, wie Mitarbeiter ihre iOS-Geräte verwenden können. Sie bieten den Administratoren die Möglichkeit, die systemeigene Funktionalität von iOS-Geräten zu sperren und die Vorbeugung gegen Datenverlust zu erzwingen.

Für bestimmte Restriktionsoptionen wird auf der Seite **Restriktionsprofil** rechts ein Symbol gezeigt, welches die minimale iOS-Version zur Erzwingung dieser Restriktion anzeigt. Beispiel: Das Symbol **iOS 7 + überwacht** neben dem Kontrollkästchen **AirDrop zulassen** bedeutet, dass nur Geräte, die unter iOS 7 ausgeführt werden und darauf eingestellt sind, mit Hochladen eines signierten Apple Configurator-Profils auf die UEM-Konsole oder dem Registrieren von Geräten mit dem Apple Business Manager-Programm zur Geräteregistrierung (DEP) von Apple im Überwachungsmodus ausgeführt zu werden, von dieser Restriktion betroffen sind.

Die hier aufgelisteten schrittweisen Anleitungen zeigen nur einige Funktionsbeispiele der Einstellungen, die Sie einschränken können. Eine komplette Liste von Anforderungen für die iOS-Version und die Überwachungsfunktion finden Sie im Kapitel 10 iOS-Funktionalität: „Überwacht“ im Vergleich zu „Nicht überwacht“.

Restriktionsprofilkonfigurationen

Ein Restriktionsprofil kann angepasst werden, um zu steuern, auf welche Anwendungen, Hardware und Funktionen Ihre Endbenutzer zugreifen können. Verwenden Sie diese Restriktionen, um die Produktivität zu steigern, Endbenutzer und Geräte zu schützen und persönliche von Unternehmensdaten zu trennen.

Informationen zum Erstellen eines Restriktionsprofils finden Sie unter Konfigurieren eines Geräte-Restriktionsprofils.

Die folgenden Restriktionen sind Beispiele und keine erschöpfende Aufzählung.

Restriktionen für Betriebssysteme

Restriktionen zum Hinauszögern von Software auf Betriebssystemebene, mit denen Sie dafür sorgen können, dass Endbenutzer iOS-Updates für eine bestimmte Anzahl von Tagen nicht erkennen können.

Einstellungen	Beschreibung
Verzögerung bei Updates (in Tagen)	Aktivieren Sie diese Option und geben Sie die Anzahl der Tage an, um die das Software-Update verzögert werden soll. Anzahl der Tage reicht von 1 bis 90. (iOS 11.3 und höher, überwachte Geräte). Die Anzahl der Tage bestimmt die Zeitdauer nach der Veröffentlichung des Software-Updates und nicht nach dem Zeitpunkt der Installation des Profils.

Restriktionen der Gerätefunktionen

Restriktionen auf Geräteebene können wichtige Gerätefunktionen deaktivieren, wie zum Beispiel Kamera, FaceTime, Siri und Einkäufe aus Anwendungen, um Produktivität und Sicherheit zu erhöhen.

- Schränken Sie die Änderung von Bluetooth-Einstellungen an Endgeräten für Endanwender ein. (iOS 10 und höher)
- Sperren von Bildschirmaufnahmen auf Geräten, um auf dem Gerät gespeicherte, dem Unternehmen gehörende Inhalte zu schützen.
- Deaktivieren von Siri bei einem gesperrten Gerät, um den Zugang zu E-Mail, Telefon und Hinweisen ohne Sicherheitskennung zu verhindern (iOS 7 und höher).

  Standardmäßig können Endbenutzer zur Verwendung von Siri bei einem gesperrten Gerät den **Start**-Button gedrückt halten. Diese Funktion könnte nicht autorisierten Benutzern die Möglichkeit geben, Zugriff auf vertrauliche Informationen zu erlangen und Aktionen auf einem Gerät auszuführen, das ihnen nicht gehört. Wenn Ihre Organisation strenge Sicherheitsanforderungen hat, erwägen Sie, ein **Restriktionsprofil** einzusetzen, das die Nutzung von Siri beschränkt, wenn ein Gerät gesperrt ist.

- Verhindern von automatischer Synchronisierung während des Roamings zur Reduktion von Datenkosten.
- Verhindert, dass ein Gerät mit Touch-ID entsperrt wird (iOS 7 und höher).
- Beschränken Sie die Benutzer auf das Ändern der Einstellung für den persönlichen Hotspot auf dem Gerät (iOS 12.2 und höher, überwacht). Egal ob die Einschränkung im Profil aktiviert oder deaktiviert ist, Sie können die Einstellung für den persönlichen Hotspot mit dem Befehl „PersonalHotspot Managed Settings“ außer Kraft setzen.
- Beschränken Sie die Protokollierungsanforderung des Endbenutzers auf Siri-Server. Wenn die Einschränkung deaktiviert ist, protokolliert Siri keine Endbenutzer-Protokollierungsdaten auf dem Server.
- Hindern Sie Endbenutzer daran, das WLAN in den Einstellungen oder im Kontrollzentrum (oder sogar beim Ein-/Ausschalten des Flugmodus) zu (de)aktivieren, indem Sie in der UEM-Konsole (iOS 10.3 und höher) **WLAN ein erzwingen** aktivieren.
- Deaktivieren Sie **Zugriff auf Dateien im Netzwerklaufwerk**, um Benutzer an der Verbindung zu Netzwerklaufwerken in der Dateien-App (iOS 10.3 und höher) zu hindern.

Beschriebene Restriktionen für iOS 8-Geräte

- Deaktivieren von Handoff, Was benutzt werden kann, um eine Aktivität auf einem Gerät zu starten, andere Geräte zu suchen und die Aktivitäten auf gemeinsam genutzten Anwendungen wieder aufzunehmen.
- Deaktivieren von Internetsuchergebnissen in Spotlight. Diese Restriktion verhindert bei einer Suche mit Spotlight die Anzeige empfohlener Websites. (iOS 8 und höher, überwacht).
- Deaktivieren der Konfiguration von Restriktionseinstellungen. Diese Berechtigung ermöglicht es Administratoren, die Konfiguration persönlicher Restriktionen über das Menü „Einstellungen“ des Geräts zu überschreiben (iOS 8 und höher, überwacht).
- Verhindern, dass der Endbenutzer alle Inhalte und Einstellungen auf dem Gerät löscht. Diese Einschränkung verhindert, dass Benutzer das Gerät löschen und die Registrierung aufheben (iOS 8 und höher, überwacht)
- Deaktivieren der lokalen Datenspeicherung durch Sichern verwalteter Anwendungen mit iCloud.
- Deaktivieren des Backups von Unternehmensbüchern mit iCloud.
- Verhindern, dass Benutzer Notizen und Markierungen in Unternehmensbüchern mit iCloud synchronisieren.
- Deaktivieren des Hinzufügens oder Entfernens bestehender Touch-ID-Informationen (überwachte iOS 8.1.3 und höher, überwacht).
- Deaktivieren von Podcasts. Diese Restriktion verhindert den Zugriff auf die Podcast-Anwendung von Apple (nur überwacht).

Empfohlene Restriktionen für iOS 9

- Deaktivieren der Kennungsänderungen, womit das Hinzufügen, Ändern oder Entfernen eines Gerätekennungen verhindert wird (nur überwachte Geräte).
- Ausblenden des App Stores. Diese Restriktionen deaktiviert den App Store und entfernt das Symbol aus der Startseite. Endbenutzer können weiterhin MDM verwenden, um ihre Anwendungen zu installieren oder zu aktualisieren, sodass die vollständige Kontrolle der Anwendungen auf den Administrator übergeht (nur überwachte Geräte).
- Deaktivieren des automatischen App-Downloads. Diese Restriktion verhindert, dass Anwendungen, die auf anderen Geräten gekauft wurden, automatisch synchronisieren. Diese Restriktion beeinträchtigt die Aktualisierungen bestehender Anwendungen nicht (nur überwachte Geräte).
- Deaktivieren von Änderungen des Gerätenamens. Diese Restriktion hindert Endbenutzer daran, den Gerätenamen zu ändern. Diese Restriktion ist für die Bereitstellung von gemeinsam genutzten und vorübergehend bereitgestellten Geräten empfohlen (nur überwachte Geräte).
- Deaktivieren der Änderungen von Hintergrundbildern. Diese Restriktion hindert Endbenutzer daran, die Geräte-Hintergrundbilder zu ändern (nur überwachte Geräte).
- Deaktivieren von AirDrop als nicht verwaltetes Drop-Ziel, wodurch Benutzer daran gehindert werden, Unternehmensdaten oder Anhänge aus einer verwalteten Anwendung an AirDrop zu senden. Diese Restriktion erfordert auch die Restriktion der verwalteten „Öffnen in“-Funktion von Apple.
- Deaktivieren von Tastaturkürzeln, um Benutzer daran zu hindern, Tastaturkürzel zu erstellen und zu nutzen (nur überwachte Geräte).
- Deaktivieren von News, um den Zugriff auf die News-Anwendung von Apple zu verhindern (überwachte Geräte).
- Deaktivieren der iCloud-iPhoto-Bibliothek. Mit dieser Restriktion wird verhindert, dass Fotos, die nicht vollständig aus der Bibliothek heruntergeladen wurden, lokal gespeichert werden.
- Deaktivieren der Vertrauenswürdigkeit von externen Unternehmensanwendungen, womit verhindert wird, dass Endbenutzer nicht vertrauenswürdige, vom Unternehmen signierte, nicht verwaltete Anwendungen installieren. Verwaltete unternehmenseigene Anwendungen sind automatisch vertrauenswürdig.
- Deaktivieren der Videoaufzeichnung durch Restriktionen von Bildschirmkopien, damit Endbenutzer die Geräteanzeige nicht kopieren können.
- Deaktivieren des Music-Dienstes, sodass die Music-Anwendung nicht installiert werden kann (iOS 8.3.3+, nur überwachte Geräte).

Beschreibung von iOS 9.3-Restriktionen

- Deaktivieren des iTunes Radio-Dienstes, sodass iTunes Radio nicht installiert werden kann. Wenn Apple Music keiner Restriktion unterliegt, wird der Radio-Dienst in der Apple Music-Anwendung angezeigt (nur überwachte Geräte).

Beschreibung von watchOS-Restriktionen

- Deaktivieren von Apple Watch-Kopplung, womit eine derzeit gekoppelte Apple Watch entkoppelt und gelöscht wird (überwachte iOS 9 und höher, überwacht).
- Erzwingen der Handgelenkerkennung, wodurch eine Apple Watch gesperrt wird, wenn sie nicht getragen wird.

Restriktionen auf Anwendungsebene

Durch Restriktionen auf Anwendungsebene werden bestimmte Anwendungen wie YouTube, iTunes und Safari bzw. einige ihrer Funktionen deaktiviert, um Richtlinien des Unternehmens durchzusetzen. Die verfügbaren Restriktionen sind:

- Deaktivieren von AutoAusfüllen gewährleistet, dass vertrauliche Informationen in bestimmten Formularen nicht automatisch erscheinen.
- Aktivieren der Funktion „Betrugswarnung erzwingen“ gewährleistet, dass Safari eine Warnung anzeigt, wenn Endbenutzer vermutete Phishing-Websites besuchen.
- Steuern der Cookie-Akzeptanz in Safari. Sie können Safari so einrichten, dass keine Cookies bzw. Cookies nur von bestimmten Websites akzeptiert werden.
- Sperren des Zugriffs auf das Game-Center und Spiele mit mehreren Spielern, um Unternehmensrichtlinien für die Gerätenutzung während der Arbeit durchzusetzen.
- Aktivieren oder deaktivieren Sie die einzelnen, nativen und anderen Anwendungen, indem Sie sie im Abschnitt **Apps anzeigen** oder **Apps ausblenden** hinzufügen. Mit dieser Einschränkung können Sie Anwendungen nach Bedarf anzeigen oder ausblenden (für iOS 9.3 und höher, nur überwachte Geräte).
    - Um die Webclips der Whitelist hinzuzufügen, fügen Sie die Paket-ID **com.apple.webapp** im Textfeld **Apps anzeigen** hinzu.

iCloud-Restriktionen

Benutzer mit Geräten mit iOS 7 und höher können Daten in der iCloud – einer Sammlung von Apple-Servern – speichern, sichern oder mit dieser synchronisieren. Beispiele sind Fotos, Videos, Geräteeinstellungen, Anwendungsdaten, Nachrichten, Dokumente und andere Daten. Für den Fall, dass Ihre Unternehmensanforderungen Restriktionen erforderlich machen, bietet Workspace ONE UEM diese für Geräte mit iOS 7 und höher, die iCloud oder iCloud-Funktionen ggf. deaktivieren können.

Exchange ActiveSync-Inhalte (Mail, Kontakte, Kalender, Aufgaben) und mobile Bereitstellungsprofile werden nicht mit der iCloud eines Endbenutzers synchronisiert.

Administrative Anforderung	Restriktion	Einstellung deaktiviert auf dem Gerät
Restriktion der iCloud-Konfiguration (Restriktion der Gerätefunktionen)		
Restriktion der Fähigkeit, sich anzumelden und iCloud-Einstellungen zu konfigurieren	Kontoänderung zulassen (erfordert Überwachung)	Deaktiviert die iCloud-Option unter den Geräteeinstellungen (iOS 7 und höher, überwacht) Diese Restriktion verhindert auch die Änderung anderer Konten wie beispielsweise E-Mail in den Geräteeinstellungen.
iCloud Management (granulare iCloud-Restriktionen)		
Verhindern, dass Benutzer Daten in der iCloud sichern	Backup zulassen	Deaktiviert die „Backup“-Option in den iCloud-Einstellungen (iOS 7)
Verhindert, dass Benutzer Dokumente und Daten im iCloud Drive speichern	Dokumentsynchronisierung zulassen	Entfernt die „iCloud Drive“-Option aus den iCloud-Einstellungen (iOS 7)
Verhindert, dass Benutzer Kennwort- und Kreditkartendaten in der iCloud speichern	Synchronisierung der Schlüsselsammlung zulassen	Entfernt die „Schlüsselsammlung“-Option unter den iCloud-Einstellungen (iOS 7)
Benutzer von verwalteten Anwendungen daran hindern, Dokumente in der iCloud zu speichern	Verwalteten Anwendungen erlauben, Daten zu speichern	Verhindert, dass verwaltete Anwendungen Dokumente in iCloud Drive speichern (iOS 8)
Verhindern, dass Benutzer Daten Unternehmensbücher in der iCloud sichern	Sicherung der Unternehmensbücher zulassen	Verhindert, dass verwaltete Bücher über iCloud oder iTunes (iOS 8) gesichert werden
Verhindert das Synchronisieren von Unternehmensbüchern, Notizen und Markierungen	Synchronisierung von Notizen und Markierungen in Unternehmensbüchern zulassen	Deaktiviert Notizen und Markierungen für Unternehmensbücher in iBooks (iOS 8)
Verhindert, dass Benutzer Fotos mit der iCloud synchronisieren	Fotostream zulassen und Freigegebenen Fotostream zulassen	Entfernt die „Fotos“-Option aus den iCloud-Einstellungen (iOS 7)
Verhindert das automatische Hochladen von neuen Fotos und das Versenden auf iCloud-Geräte	Freigegebenen Fotostream zulassen	Deaktiviert „Mein Fotostream“ in „Fotos“ in den iCloud-Einstellungen (iOS 7)

iCloud Backups finden nur unter folgenden Bedingungen statt:

- Für iCloud Backup sind keine Restriktionen vorhanden.
- Die iCloud-Umschalteinstellung ist in**Einstellungen > iCloud > Sicherung** auf dem Gerät aktiviert.
- WLAN ist aktiviert.
- Das Gerät ist mit einer Stromquelle verbunden und gesperrt.

Sicherheits- und Datenschutzrestriktionen

Auf Sicherheit und Datenschutz basierte Restriktionen können Endbenutzer daran hindern, bestimmte Aktionen auszuführen, die gegen Unternehmensrichtlinien verstoßen und ihre Geräte anderweitig gefährden. Die verfügbaren Restriktionen umfassen:

- Verhindern, dass Benutzer von iOS 11.4.1 und höheren Geräten eine Kennung eingeben, um sich erstmals mit USB-Zubehör zu verbinden oder die Verbindung dazu aufrechtzuerhalten, solange das Gerät gesperrt ist.
- Benutzer daran hindern, nicht verwalteten Unternehmensanwendungen zu vertrauen.
- Verhindern der Erzwingung eines iTunes Store-Kennworteintrags.
- Verhindern Sie, dass diagnostische Daten – unter anderem Standort- und Nutzungsdaten – an Apple gesendet werden, um bei der Verbesserung der iOS-Software zu helfen.
- Hindern Sie Endbenutzer daran, nicht vertrauenswürdige TLS-Zertifikate zu akzeptieren, sodass sie auf Websites mit ungültigen SSL-Zertifikaten nicht zugreifen können. Wenn Sie nicht vertrauenswürdige TLS-Zertifikate zulassen, werden Benutzer weiterhin über ungültige Zertifikate informiert, können aber, wenn erforderlich, fortfahren.
- Verhindern Sie Over-the-Air-PKI-Aktualisierung.
- Erzwingen Sie verschlüsselte Datensicherung Verschlüsselte Sicherung gewährleistet, dass alle persönliche Daten, wie E-Mail-Kontokennwörter und Kontaktinformationen, beim Sichern und Speichern auf Geräten verschlüsselt sind.
- Verhindern Sie Koppelung mit Nichtkonfigurator-Host.
- Verhindern Sie, dass iOS 10.3 und höhere Geräte Verbindungen zu unbekannten oder böswilligen Netzwerken herstellen. Geräte, für die diese Restriktion aktiviert ist, können sich nur mit verwalteten WLAN-Netzwerken verbinden. Aktivieren Sie **WLAN-Whitelist erzwingen**, um diese Restriktion durchzusetzen.

Restriktionen von Medieninhalten

Auf Bewertung basierte Restriktionen können den Zugriff auf bestimmte Inhalte je nach Bewertung verhindern. Diese wird nach Region verwaltet. Die verfügbaren Restriktionen sind:

- Beschränken Sie den Gerätezugriff auf anstößige bzw. nicht jugendfreie Inhalte von unternehmenseigenen Geräten als Teil einer Unternehmensrichtlinie.
- Verhindern Sie den Zugriff auf Anwendungen mit einer Altersfreigabe von 17 Jahren während der normalen Geschäftszeit.
- Blockieren des Zugriffs auf zweckwidrige oder anstößige iBook-Inhalte von unternehmenseigenen Geräten.

Konfigurieren eines Geräte-Restriktionsprofils

Restriktionsprofile begrenzen, wie Mitarbeiter ihre iOS-Geräte verwenden können. Sie bieten den Administratoren die Möglichkeit, die systemeigene Funktionalität von iOS-Geräten zu sperren und die Vorbeugung gegen Datenverlust zu erzwingen.

Verfahren

1. Gehen Sie zu **Ressourcen** > **Profile und Baselines** > **Profile** und wählen Sie **Hinzufügen**. Wählen Sie **Apple iOS**.
2. Konfigurieren Sie die Einstellungen des Profils unter **Allgemein**.
3. Wählen Sie die **Restriktions**-Nutzlast in der Liste. Sie können mehrere Restriktionen als Teil einer einzelnen Restriktionsnutzlast auswählen.
4. Konfigurieren Sie die **Restriktions**-Einstellungen. Weitere Informationen zu Restriktionen finden Sie unter Restriktionsprofilkonfigurationen.
5. Wählen Sie **Speichern und veröffentlichen**.

Konfigurieren eines WLAN-Profils

Mit einem konfigurieren WLAN-Profil können Geräte mit Unternehmensnetzwerken verbunden werden, sogar wenn sie verborgen, verschlüsselt oder kennwortgeschützt sind. Diese Nutzlast ist sinnvoll für Endbenutzer, die unterwegs sind und ihr eigenes Drahtlosnetzwerk verwenden, oder für Endbenutzer in einem Büro, wo eine automatische Verbindung mit einem Drahtlosnetzwerk vor Ort möglich ist.

Verfahren

1. Gehen Sie zu **Ressourcen > Profile und Baselines > Profile > Hinzufügen**. Wählen Sie **Apple iOS**.
2. Konfigurieren Sie die Einstellungen des Profils unter **Allgemein**.
3. Wählen Sie die **WLAN**-Nutzlast aus der Liste.
4. Konfigurieren Sie die **WLAN**-Einstellungen.

Einstellung	Beschreibung
Service Set-Bezeichner	Geben Sie den Namen des Netzwerks ein, mit dem das Gerät verbunden wird.
Ausgeblendetes Netzwerk	Geben Sie eine Verbindung zu einem Netzwerk ein, das nicht offen ist oder nicht sendet.
AutoVerknüpfung	Legen Sie fest, ob das Gerät beim Starten automatisch eine Verbindung zum Netzwerk herstellt. Das Gerät hält die Verbindung aufrecht, bis es neu gestartet oder eine andere Verbindung manuell ausgewählt wird.
Sicherheitstyp	Wählen Sie den Typ des zu verwendenden Zugriffsprotokolls aus. Geben Sie das **Kennwort** ein oder wählen Sie die **Protokolle** aus, die für Ihr WLAN-Netzwerk gelten.

Einstellung	Beschreibung
Protokolle	Wählen Sie Protokolle für den Netzwerkzugriff aus. ■ Diese Option wird angezeigt, wenn **WLAN** oder **Sicherheitstyp** als **Enterprise**-Auswahl angegeben ist. Diese Option wird auch angezeigt, wenn **Ethernet** ausgewählt ist.
WLAN Hotspot 2.0	Damit aktivieren Sie die WLAN Hotspot 2.0-Funktionalität. Die Option ist nur auf iOS 7-Geräten und höher verfügbar. Hotspot 2.0 ist ein WLAN-Typ für öffentlichen Zugriff, mit dem Geräte nahtlos Zugriffspunkte mit bester Übereinstimmung identifizieren und sich damit verbinden. Ihr Anbieter muss Hotspot 2.0 unterstützen, um eine fehlerfreie Funktion zu gewährleisten.
Domänenname	Geben Sie den Domänennamen des Passpoint-Anbieters ein.
Verbindung mit Partner-Passpoint-Netzwerken im Roamingbetrieb zulassen	Damit aktivierten Sie das Roaming in Partner-Passpoint-Netzwerken.
Angezeigter Betreibername	Geben Sie den Namen des WLAN-Hotsport-Anbieters ein.
Organisations-ID des Roaming-Konsortiums	Geben Sie die Roaming Consortium-OI ein.
Netzwerkzugriff ID	Geben Sie die Netzwerkzugriff-ID-Bereichsnamen ein.
MCC/MNC	Geben Sie den 6-stelligen Mobile Country Code bzw. Mobile Network Configuration ein.
Authentifizierung	Konfigurieren Sie die Einstellungen für die **Authentifizierung**. Diese variieren je nach Protokoll.
Benutzername	Geben Sie den Benutzernamen für das Konto ein.
Benutzerkennwort pro Verbindung	Fordern Sie das Kennwort während der Verbindung an und senden Sie es mit der Authentifizierung.
Kennwort	Geben Sie das Kennwort für die Verbindung ein.
Identitätszertifikat	Wählen Sie das Zertifikat für die Authentifizierung.
Äußere Identität	Wählen Sie die externe Authentifizierungsmethode.
Minimale TLS-Version	Wählen Sie die minimale TLS-Version 1.0, 1.1 und 1.2 aus. Wenn kein Wert ausgewählt wird, wird als Mindestversion standardmäßig 1.0 verwendet. **Hinweis** Maximale TLS-Versionen können nur für die Protokolltypen TLS, TTLS, EAP-Fast und PEAP konfiguriert werden.
Maximale TLS-Version	Wählen Sie die maximale TLS-Version 1.0, 1.1 und 1.2 aus. Wenn kein Wert ausgewählt wird, wird als Maximalversion standardmäßig 1.2 verwendet.
Vertrauenswürdige Zertifikate	Dies sind die vertrauenswürdigen Serverzertifikate für Ihr WLAN-Netzwerk.
Zertifikatnamen des vertrauenswürdigen Servers	Geben Sie die Zertifikatnamen des vertrauenswürdigen Servers ein..
Ausnahmen zur Vertrauenswürdigkeit zulassen	Gestatten Sie den Endbenutzern, selbst Entscheidungen zur Vertrauenswürdigkeit zu treffen.

5 Konfigurieren Sie die **Proxy**-Einstellungen mit **Manuell** oder **Automatisch**.

6 Wenn Sie eine Cisco-Infrastruktur verwenden, konfigurieren Sie die QoS-Markierungs-Richtlinie (iOS v11 und höher).

Einstellung	Beschreibung
Fastlane QoS-Kennzeichnung	Wählen Sie die gewünschten Markierungseinstellungen aus.
QoS-Markierung aktivieren	Wählen Sie diese Option zur Auswahl von Anwendungen für prioritäre Datenzuweisungen.
Apple-Anruf per Whitelist zulassen	Wählen Sie „Apple-Anruf per Whitelist zulassen“, um Apple-WLAN-Anruf Ihrer QoS Whitelist hinzuzufügen.
Anwendungen zur QoS-Markierung per Whitelist zulassen	Suchen Sie nach Anwendungen für die Zuweisung prioritärer Daten und fügen Sie diese hinzu.

7 (Optional) Konfigurieren Sie ein **Captive Portal**, um das Portal zu umgehen.

8 Wählen Sie nach Abschluss des Vorgangs **Speichern und veröffentlichen**, um das Profil per Push auf die Geräte zu übertragen.

Konfigurieren eines VPN-Profils (virtuelles privates Netzwerk)

Virtuelle private Netzwerke (VPNs) bieten Geräten einen sicheren und verschlüsselten Tunnel zum Zugriff auf interne Ressourcen. VPN-Profile ermöglichen, dass alle Geräte so funktionieren, als ob sie über das Netzwerk vor Ort verbunden sind. Ein konfiguriertes VPN-Profil gewährleistet, dass Endbenutzer einen nahtlosen Zugriff auf E-Mails, Dateien und Inhalte haben.

Verfahren

1 Navigieren Sie zu **Ressourcen > Profile und Baselines Profile** > **Hinzufügen**. Wählen Sie **Apple iOS**.

2 Konfigurieren Sie die Einstellungen des Profils unter **Allgemein**.

3 Wählen Sie die **VPN**-Nutzlast.

4 Konfigurieren Sie die **Verbindungsinformationen** wie folgt:

Die angezeigten Einstellungen hängen von dem von Ihnen gewählten **Verbindungstyp** ab. Weitere Informationen zur Verwendung von Forcepoint oder Blue Coat zum Filtern von Inhalten finden Sie unter Konfigurieren eines Forcepoint-Inhaltsfilterprofils und Konfigurieren eines Blue Coat Inhaltsfilterprofils.

Einstellungen	Beschreibung
Verbindungsname	Geben Sie den Namen der Verbindung ein, der auf dem Gerät angezeigt werden soll.
Verbindungstyp	Verwenden Sie das Dropdown-Menü, um die Netzwerkverbindungsmethode auszuwählen.
Server	Geben Sie den Hostnamen oder die IP-Adresse des Servers ein.

Einstellungen	Beschreibung
Konto	Geben Sie den Namen des VPN-Kontos ein.
Gesamten Datenverkehr senden	Sendet den gesamten Datenverkehr über das angegebene Netzwerk.
Verbindung bei Leerlauf abbrechen	Ermöglichen Sie es dem VPN, nach einer bestimmten Zeitdauer eine automatische Trennung durchzuführen. Die Unterstützung für diesen Wert hängt vom VPN-Anbieter ab.
Automatisch verbinden	Wählen Sie diese Option, um es dem VPN zu gestatten, automatisch eine Verbindung zu den folgenden Domänen herzustellen. Diese Option wird angezeigt, wenn **Pro-App-VPN-Regeln** aktiviert ist. ■ Safari-Domänen ■ E-Mail-Domänen ■ Kontaktdomänen ■ Kalenderdomänen
Anbietertyp	Wählen Sie den Typ des VPN-Diensts aus. Wenn es sich bei dem VPN-Diensttyp um einen App-Proxy handelt, tunnelt der VPN-Dienst den Datenverkehr auf Anwendungsebene. Wenn es sich um einen Paket-Tunnel handelt, tunnelt der VPN-Dienst den Datenverkehr auf der IP-Ebene.
Per-App-VPN-Regeln	Aktiviert das Per-App-VPN für Geräte. Weitere Informationen finden Sie unter Konfigurieren eines Per-App VPN-Profils.
Authentifizierung	Wählen Sie die Methode zur Authentifizierung für Endbenutzer aus. Halten Sie sich an die entsprechenden Eingabeaufforderungen, um ein **Identitätszertifikat** hochzuladen, oder geben Sie eine **Kennwort**-Information bzw. den **Gemeinsamen geheimen Schlüssel** ein, der den Endbenutzern den VPN-Zugriff ermöglicht.
VPN-On-Demand aktivieren	Aktivieren Sie VPN-ONnDemand, um Zertifikate für die automatische Einrichtung von VPN-Verbindungen gemäß dem Abschnitt Konfigurieren eines Per-App VPN-Profils in diesem Leitfaden zu verwenden.
Proxy	Wählen Sie zur Konfiguration mit dieser VPN-Verbindung als Proxytyp **Manuell** oder **Automatisch** aus.
Server	Geben Sie die URL für den Proxyserver ein.
Port	Geben Sie den Port ein, der für die Kommunikation mit dem Proxy verwendet wird.
Benutzername	Geben Sie den Benutzernamen für die Verbindung mit dem Proxyserver ein.
Kennwort	Geben Sie das Kennwort für die Authentifizierung ein.
Anbieterschlüssel	Wählen Sie diese Option, um benutzerdefinierte Schlüssel zu erstellen, die in das Konfigurationswörterbuch für Anbieter aufgenommen werden.
Schlüssel	Geben Sie den spezifischen Schlüssel ein, der vom Anbieter bereitgestellt wurde.
Wert	Geben Sie den VPN-Wert für jeden Schlüssel ein.
Lokale Netzwerke ausschließen	Aktivieren Sie die Option, um alle Netzwerke zur Weiterleitung des Netzwerkdatenverkehrs außerhalb des VPN einzubeziehen.
Alle Netzwerke einbeziehen	Aktivieren Sie die Option, um alle Netzwerke zur Weiterleitung des Netzwerkdatenverkehrs über das VPN einzubeziehen.

Hinweis Wenn Sie als Typ IKEv2 ausgewählt haben, sind Sie berechtigt, die minimale und maximale TLS-Version für die VPN-Verbindungen einzugeben. Vor der Eingabe der TLS-Version müssen Sie das Kontrollkästchen **EAP aktivieren** aktivieren.

5 Wählen Sie **Speichern und veröffentlichen**. Endbenutzer haben jetzt Zugriff auf zulässige Sites.

Konfigurieren eines Forcepoint-Inhaltsfilterprofils

Mit der Integration von Workspace ONE UEM in Forcepoint können Sie Ihre vorhandenen Inhaltsfilterkategorien in Forcepoint nutzen und diese auf Geräte anwenden, die Sie in der UEM-Konsole verwalten.

Erlauben oder blockieren Sie Zugriff auf Websites nach den von Ihnen in Forcepoint konfigurierten Regeln und setzen Sie dann eine VPN-Nutzlast ein, um Geräte zu zwingen, diese Regeln zu befolgen. Bei Workspace ONE UEM registrierte Verzeichnisbenutzer werden mit Forcepoint abgeglichen, um nach dem bestimmten Endbenutzer zu bestimmen, welche Inhaltsfilterregeln angewendet werden sollen.

Sie können das Filtern von Inhalten mit Forcepoint auf eine der beiden folgenden Arten erzwingen.

- Verwenden Sie das **VPN**-Profil wie in diesem Thema beschrieben. Das Durchsetzen von Inhaltsfilterung mithilfe des VPN-Profils kann auf sämtlichen Webverkehr mit anderen Browsern als dem VMware Browser angewendet werden.
- Konfigurieren Sie die Seite **Einstellungen und Richtlinien**, die für sämtlichen Webverkehr mit anderen Browsern als dem VMware Browser gilt. Weiterführende Informationen über die Konfiguration von **Einstellungen und Richtlinien** finden Sie im **VMware Browser Guide**.

Verfahren

1 Gehen Sie zu **Ressourcen > Profile und Baselines** > **Profile > Hinzufügen**. Wählen Sie **Apple iOS**.

2 Konfigurieren Sie die Einstellungen des Profils unter **Allgemein**.

3 Wählen Sie die **VPN**-Nutzlast.

4 Wählen Sie **Websense (Forcepoint)** als **Verbindungstyp**.

5 Konfigurieren Sie die **Verbindungsdaten** wie folgt:

Einstellungen	Beschreibung
Verbindungsname	Geben Sie den Namen der Verbindung ein, der angezeigt werden soll.
Benutzername	Geben Sie den Benutzernamen für die Verbindung mit dem Proxyserver ein.
Kennwort	Geben Sie das Kennwort für die Verbindung ein.

6 (Optional) Sie können auch **Verbindung testen** auswählen.

7 Konfigurieren Sie die Einstellungen **Anbieterkonfigurationen**.

Einstellung	Beschreibung
Anbieterschlüssel	Erstellen Sie benutzerdefinierte Schlüssel und fügen Sie diese dem Konfigurationswörterbuch für Anbieter hinzu.
Schlüssel	Geben Sie den spezifischen Schlüssel ein, der vom Anbieter bereitgestellt wurde.
Wert	Geben Sie den VPN-Wert für jeden Schlüssel ein.

8 Wählen Sie **Speichern und veröffentlichen**. Verzeichnisbasierte Endbenutzer haben jetzt Zugriff auf zulässige Sites auf Grundlage Ihrer Forcepoint-Kategorien.

Konfigurieren eines Blue Coat Inhaltsfilterprofils

Workspace ONE UEM-Integration mit Blue Coat ermöglicht Ihnen, Ihre vorhandenen Inhaltsfilterkategorien in Blue Coat zu nutzen.

Erlauben oder blockieren Sie Zugriff auf Websites nach den von Ihnen in Blue Coat konfigurierten Regeln und setzen Sie dann eine VPN-Nutzlast ein, um Geräte zu zwingen, diese Regeln zu befolgen.

Verfahren

1 Gehen Sie zur Seite **Ressourcen** > **Profile und Baselines > Profile > Hinzufügen**. Wählen Sie **Apple iOS**.

2 Konfigurieren Sie die Einstellungen des Profils unter **Allgemein**.

3 Wählen Sie die **VPN**-Nutzlast.

4 Wählen Sie **Blue Coat** als **Verbindungstyp**.

Einstellung	Beschreibung
Blue Coat-Kunden-ID	Greifen Sie auf diesen Wert zu, indem Sie sich auf der Blue Coat-Website anmelden und zum Abschnitt API Token & Keys gehen, wo Sie einen MDM-Partner hinzufügen und die Kennung erhalten können. Weitere Informationen und Hilfestellung erhalten Sie von Blue Coat.
Per-App VPN	Optional aktivieren Sie Per-App-VPN. Weitere Informationen finden Sie unter Konfigurieren eines Per-App VPN-Profils.

5 Sie können optional auch **Verbindung testen** auswählen.

6 Konfigurieren Sie **Anbieterkonfigurationen**:

Einstellung	Beschreibung
Anbieterschlüssel	Wählen Sie diese Option, um benutzerdefinierte Schlüssel zu erstellen, die in das Konfigurationswörterbuch für Anbieter aufgenommen werden.
Schlüssel	Geben Sie den spezifischen Schlüssel ein, der vom Anbieter bereitgestellt wurde.
Wert	Geben Sie den VPN-Wert für jeden Schlüssel ein.

7 Wählen Sie **Speichern und veröffentlichen**. Die Endbenutzer haben jetzt Zugriff auf genehmigte Sites auf Grundlage Ihrer Blue Coat-Inhaltsfilterregeln.

Konfigurieren eines VPN-On-Demand-Profils

VPN-On-Demand ist die Methode, mit der eine VPN-Verbindung für bestimmte Domänen automatisch hergestellt wird. Um Sicherheit und Bedienkomfort zu erhöhen, nutzt VPN-On-Demand Zertifikate zur Authentifizierung anstelle einfacher Kennungen.

Voraussetzungen

Stellen Sie sicher, dass Ihre Zertifizierungsstellen und Zertifikatsvorlagen in Workspace ONE UEM ordnungsgemäß zur Zertifikatsverteilung konfiguriert sind. Machen Sie die Drittanbieter-VPN-App Ihrer Wahl für Endbenutzer verfügbar, indem Sie die App auf Geräte übertragen und sie in Ihrem Unternehmens-App-Katalog empfehlen.

Verfahren

1 Gehen Sie zu **Ressourcen > Profile und Baselines > Profile > Hinzufügen** und dann **iOS**.

2 Wählen Sie die **VPN**-Nutzlast aus der Liste.

3 Konfigurieren Sie Ihr Konfigurieren eines VPN-Profils (virtuelles privates Netzwerk) entsprechend.

4 Wählen Sie **Zertifikat** aus dem Dropdown-Menü **Benutzerauthentifizierung**. Navigieren Sie zur **Anmeldedaten**-Nutzlast.

   a Wählen Sie aus dem Dropdown-Menü **Quelle der Anmeldedaten** die Option **Festgelegte Zertifizierungsstelle**.

   b Wählen Sie die **Zertifizierungsstelle** und **Zertifikatsvorlage** aus den entsprechenden Dropdown-Menüs.

   c Navigieren Sie zurück zur **VPN**-Nutzlast.

5 Wählen Sie das **Identitätszertifikat** gemäß der Angabe in der **Anmeldedaten**-Nutzlast, wenn Sie die Zertifikatauthentifizierung auf das VPN-Profil anwenden.

6 Aktivieren Sie das Kontrollkästchen **VPN-On-Demand aktivieren**.

7 Konfigurieren Sie die Option **Neue On-Demand-Schlüssel verwenden (iOS 7)**, um eine VPN-Verbindung zu aktivieren, wenn Endbenutzer auf eine der angegebenen Domäne zugreifen:

Einstellung	Beschreibung
Neue On-Demand-Schlüssel verwenden (iOS 7 und höher)	Wählen Sie diese Option, um die neue Syntax zu verwenden, die detailliertere VPN-Regeln ermöglichen.
On-Demand-Regel/Aktion	Wählen Sie eine **Aktion** zur Definition des VPN-Verhaltens, die auf die VPN-Verbindung angewendet werden soll, basierend auf den definierten Kriterien. Wenn die Kriterien zutreffen, wird die festgelegte Aktion durchgeführt. ■ **Verbindung bewerten**: Die VPN-Tunnelverbindung wird automatisch basierend auf den Netzwerkeinstellungen und den Eigenschaften jeder Verbindung eingerichtet. Die Bewertung erfolgt jedes Mal, wenn eine VPN-Verbindung mit einer Website erfolgt. ■ **Verbinden**: Die VPN-Tunnelverbindung wird beim nächsten Netzwerkversuch automatisch erstellt, wenn das Netzwerkkriterium eingehalten wird. ■ **Trennen**: Die VPN-Tunnelverbindung wird automatisch deaktiviert und nicht wieder auf Anfrage hergestellt, wenn die Netzwerkkriterien eingehalten werden. ■ **Ignorieren**: Die bestehende VPN-Verbindung wird beibehalten, aber eine erneute Verbindung auf Anfrage wird nicht hergestellt, solange die Netzwerkkriterien eingehalten werden.

Einstellung	Beschreibung
Aktionsparameter	Konfigurieren Sie **Aktionsparameter** für die angegebenen Domänen, um einen VPN-Verbindungsversuch auszulösen, wenn die Auflösung des Domänennamens fehlschlägt, beispielsweise wenn der DNS-Server angibt, dass er die Domäne nicht auflösen kann, mit einer Umleitung auf einen anderen Server reagiert oder gar nicht antwortet (Zeitablauf). Wenn Sie **Verbindung bewerten** auswählen, werden die folgenden Optionen angezeigt: ■ Wählen Sie **Verbindung herstellen, wenn nötig/Nie verbinden** und geben Sie weitere Informationen ein: ■ **Domänen** – Geben Sie die Domänen ein, für die diese Bewertung gilt. ■ **URL-Test** – Geben Sie die HTTP- oder HTTPS-URL (bevorzugt) zum Testen ein und verwenden Sie eine GET-Abfrage. Wenn der Hostname der URL nicht aufgelöst werden kann, der Server nicht erreichbar ist oder nicht mit einem 200 HTTP-Statuscode reagiert, wird als Reaktion eine VPN-Verbindung eingerichtet. ■ **DNS-Server** – Geben Sie eine Reihe von IP-Adressen für DNS-Server ein, die für die Auflösung der angegebenen Domänen verwendet werden sollen. Diese Server müssen nicht Teil der aktuellen Netzwerkkonfiguration des Geräts sein. Wenn diese DNS-Server nicht erreichbar sind, wird als Reaktion eine VPN-Verbindung eingerichtet. Diese DNS-Server müssen entweder interne DNS-Server oder vertrauenswürdige externe DNS-Server sein. (Optional)
Kriterien/Wert für Parameter	■ **Schnittstellenübereinstimmung** – Wählen Sie den Typ der Verbindung aus, der mit dem aktuellen Adapter des Gerätnetzwerks übereinstimmt. Die verfügbaren Werte sind **Beliebig**, **WLAN**, **Ethernet** und **Mobilfunknetz**. ■ **URL-Test** – Geben Sie die festgelegte URL für die Kriterien ein, die eingehalten werden sollen. Wenn die Kriterien eingehalten werden, wird ein 200 HTTP-Statuscode zurückgegeben. Dieses Format umfasst das Protokoll (HTTPS). ■ **Übereinstimmung bei SSID** – Geben Sie die aktuelle Netzwerk-ID des Geräts ein. Damit die Kriterien eingehalten werden, muss mindestens ein Wert in der Reihe zutreffen. ■ Verwenden Sie das Symbol **+**, um gegebenenfalls mehrere SSIDs einzugeben. ■ **Übereinstimmung bei DNS-Domänen** – Geben Sie die Suchdomäne des aktuellen Netzwerks des Geräts ein. Ein Platzhalter kann verwendet werden (*.example.com). ■ **Übereinstimmung bei DNS-Adressen** – Geben Sie die DNS-Adresse ein, die mit der IP-Adresse des aktuellen DNS-Servers des Geräts übereinstimmt. Damit die Kriterien eingehalten werden, sind alle aufgelisteten IP-Adressen des Geräts einzugeben. Die Übereinstimmung mithilfe eines einzelnen Platzhalters wird unterstützt (17.*).

8 Als Alternative können Sie die veraltete Option **VPN-On-Demand** verwenden:

Einstellung	Beschreibung
Domäne oder Host abstimmen	On-Demand-Aktion ■ **Bei Bedarf herstellen** oder **Immer herstellen** – Initiiert eine VPN-Verbindung nur, wenn die angegebene Seite nicht direkt erreicht werden kann. ■ **Nie herstellen** – Errichtet keine VPN-Verbindung für Adressen, die mit der angegebenen Domäne übereinstimmen. Wenn das VPN bereits aktiv ist, kann es jedoch verwendet werden.

9 Verwenden Sie das Symbol **+**, um gegebenenfalls zusätzliche **Regeln** und **Aktionsparameter** hinzuzufügen.

10 Wählen Sie einen **Proxy-Typ**:

Einstellung	Beschreibung
Proxy	Wählen Sie den Proxytyp **Manuell** oder **Automatisch** zur Konfiguration mit dieser VPN-Verbindung.
Server	Geben Sie die URL für den Proxyserver ein.
Port	Geben Sie den Port ein, der für die Kommunikation mit dem Proxy verwendet wird.
Benutzername	Geben Sie den Benutzernamen für die Verbindung mit dem Proxyserver ein.
Kennwort	Geben Sie das Kennwort für die Authentifizierung ein.

11 Richten Sie die **Anbieterkonfigurationen** ein. Diese Werte sind für jeden VPN-Anbieter eindeutig.

Einstellung	Beschreibung
Anbieterschlüssel	Wählen Sie diese Option, um benutzerdefinierte Schlüssel zu erstellen, die in das Konfigurationswörterbuch für Anbieter aufgenommen werden.
Schlüssel	Geben Sie den spezifischen Schlüssel ein, der vom Anbieter bereitgestellt wurde.
Wert	Geben Sie den VPN-Wert für jeden Schlüssel ein.

12 Klicken Sie auf **Speichern und veröffentlichen**. Sobald das Profil auf dem Gerät installiert wird, erscheint automatisch eine VPN-Verbindungsaufforderung, wenn der Benutzer zu einer Site navigiert, die diese verlangt, wie beispielsweise SharePoint.

Konfigurieren eines Per-App VPN-Profils

Bei iOS 7-Geräten und höher können Sie ausgewählte Anwendungen zur Verbindung mit dem VPN Ihres Unternehmens erzwingen. Ihr VPN-Anbieter muss diese Funktion unterstützen und Sie müssen die Anwendungen als verwaltete Anwendungen veröffentlichen.

Verfahren

1 Gehen Sie zur Seite **Ressourcen** > **Profile und Baselines > Profiles > Hinzufügen** und wählen Sie **iOS**.

2 Wählen Sie die **VPN**-Nutzlast aus der Liste.

3 Konfigurieren Sie Ihr Konfigurieren eines VPN-Profils (virtuelles privates Netzwerk) entsprechend.

4 Wählen Sie **Pro-App-VPN**, um eine VPN-UUID für die aktuellen VPN-Profileinstellungen zu generieren. Die VPN-UUID ist ein eindeutiger Bezeichner für diese bestimmte VPN-Konfiguration.

5 Wählen Sie **Automatisch verbinden**, um Textfelder für die **Safari-Domänen** anzuzeigen, die interne Sites sind und eine automatische VPN-Verbindung auslösen.

6 Wählen Sie einen **Anbietertyp**, um festzulegen, wie der Datenverkehr definiert wird, entweder über eine Anwendungsebene oder über eine IP-Ebene.

7 Wählen Sie **Speichern und veröffentlichen**.

   Falls dieser Vorgang als Aktualisierung auf ein vorhandenes VPN-Profil gespeichert wurde, werden alle vorhandenen Geräte/Anwendungen aktualisiert, die dieses Profil verwenden. Alle Geräte/Anwendungen, die bisher keine VPN-UUID verwendet haben, werden auch aktualisiert, um das VPN-Profil zu verwenden.

Konfigurieren von öffentlichen Anwendungen zur Verwendung des Pro-App-Profils

Nachdem Sie ein Pro-App-Tunnelprofil erstellt haben, können Sie es bestimmten Anwendungen auf der Konfigurationsseite der Anwendung zuordnen. Damit wird angegeben, dass das definierte VPN-Profil beim Einrichten von Verbindungen über die Anwendung verwendet werden muss.

Verfahren

1 Gehen Sie zu **Ressourcen > Apps > Native**.

2 Wählen Sie den Tab **Öffentlich**.

3 Wählen Sie **Anwendung hinzufügen**, um eine Anwendung hinzuzufügen, oder **Bearbeiten**, für eine bestehende App.

4 Wählen Sie auf dem Tab „Einsatz“ die Option **VPN verwenden** und danach das Profil, das Sie oben erstellt haben.

5 Wählen Sie **Speichern** und veröffentlichen Sie Ihre Änderungen.

Nächste Schritte

Weitere Informationen zum Hinzufügen oder Bearbeiten von Anwendungen finden Sie im Handbuch **Mobile Application Management**.

Konfigurieren von internen Anwendungen zur Verwendung des Pro-App-Profils

Nachdem Sie ein Pro-App-Tunnelprofil erstellt haben, können Sie es bestimmten Anwendungen auf der Konfigurationsseite der Anwendung zuordnen. Damit wird angegeben, dass das definierte VPN-Profil beim Einrichten von Verbindungen über die Anwendung verwendet werden muss.

Verfahren

1. Gehen Sie zu **Ressourcen >** Apps **> Native**.
2. Wählen Sie den Tab **Intern**.
3. Wählen Sie **Anwendung hinzufügen** und fügen Sie eine Anwendung zu.
4. Wählen Sie **Speichern und zuweisen**, um zur Seite „Zuweisung“ zu gehen.
5. Wählen Sie **Zuweisung hinzufügen** und dann **Pro-App-VPN-Profil** im Abschnitt **Erweitert**.
6. **Speichern und veröffentlichen** Sie die Anwendung.

Nächste Schritte

Weitere Informationen zum Hinzufügen oder Bearbeiten von Apps finden Sie im Handbuch **Mobile Anwendungsverwaltung** in der Dokumentation zu VMware AirWatch.

Konfigurieren eines E-Mail-Kontoprofils

Erstellen Sie ein E-Mail-Profil für iOS-Geräte, um E-Mail-Einstellungen auf dem Gerät zu konfigurieren.

Verfahren

1. Gehen Sie zur Seite **Ressourcen** > **Profile und Baselines** > **Profile** und wählen Sie **Hinzufügen**. Wählen Sie **Apple iOS**.
2. Konfigurieren Sie die Einstellungen des Profils unter **Allgemein**.
3. Wählen Sie die **E-Mail**-Nutzlast.
4. Konfigurieren Sie die E-Mail-Kontoeinstellungen wie folgt:

Einstellungen	Beschreibungen
Kontobeschreibung	Geben Sie eine kurze Beschreibung des E-Mail-Kontos ein.
Kontotyp	Verwenden Sie das Dropdown-Menü, um IMAP oder POP auszuwählen.
Pfadpräfix	Geben Sie den Namen des Stammordners für das E-Mail-Konto ein (nur IMAP).
Anzeigename des Benutzers	Geben Sie den Namen des Endbenutzers ein.
E-Mail-Adresse	Geben Sie die Adresse für das E-Mail-Konto ein.

Einstellungen	Beschreibungen
Verschieben von Nachrichten verhindern	Wählen Sie diese Option, damit der Benutzer E-Mails nicht weiterleiten oder in Anwendungen von Drittanbietern öffnen kann.
Synchronisierung jüngster Adressen verhindern	Wählen Sie diese Option, damit der Benutzer E-Mail-Kontakte nicht mit seinem persönlichen Gerät synchronisieren kann.
Verwendung in Drittanbieter-Apps verhindern	Wählen Sie diese Option, damit Benutzer Unternehmens-E-Mails nicht auf andere E-Mail-Clients verschieben können.
Mail Drop verhindern	Wählen Sie diese Option, damit Benutzer die Apple-Funktion „Mail-Ablage“ nicht benutzen können.
S/MIME verwenden	Wählen Sie diese Option, um zusätzliche Verschlüsselungszertifikate zu verwenden.
Hostname	Geben Sie den Namen des E-Mail-Servers ein.
Port	Geben Sie die Nummer des Ports ein, der für eingehende E-Mails zugewiesen ist.
Benutzername	Geben Sie den Benutzernamen für das E-Mail-Konto ein.
Authentifizierungstyp	Verwenden Sie das Dropdown-Menü, um auszuwählen, wie der Inhaber des E-Mail-Kontos authentifiziert wird.
Kennwort	Geben Sie das zur Authentifizierung des Endbenutzers erforderliche Kennwort ein.
SSL verwenden	Wählen Sie diese Option, um Secure Socket Layer für eingehende E-Mails zu nutzen.
Hostname	Geben Sie den Namen des E-Mail-Servers ein.
Port	Geben Sie die Nummer des Ports ein, der für ausgehende E-Mails zugewiesen ist.
Benutzername	Geben Sie den Benutzernamen für das E-Mail-Konto ein.
Authentifizierungstyp	Verwenden Sie das Dropdown-Menü, um auszuwählen, wie der Inhaber des E-Mail-Kontos authentifiziert wird.
Ausgehendes und eingehendes Kennwort identisch	Wählen Sie diese Option, um das Kennwort in das Textfeld automatisch einzutragen.
Kennwort	Geben Sie das zur Authentifizierung des Endbenutzers erforderliche Kennwort ein.
SSL verwenden	Wählen Sie diese Option, um Secure Socket Layer für ausgehende E-Mails zu nutzen.

EAS-Mail (Exchange ActiveSync) für iOS-Geräte

Das zur E-Mail-Synchronisierung auf Mobilgeräten entworfene Industriestandardprotokoll nennt sich **Exchange ActiveSync (EAS))**. Mit EAS-Profilen können Sie Geräte aus der Ferne konfigurieren, um mit Ihrem Mailserver E-Mails, Kalender und Kontakte zu synchronisieren.

Das EAS-Profil nutzt Informationen von jedem Benutzer, wie beispielsweise Benutzername, E-Mail-Adresse und Kennwort. Integrieren Sie Workspace ONE UEM in die Active Directory-Dienste, so werden diese Benutzerinformationen für den Benutzer automatisch eingetragen. Diese Informationen können unter Verwendung von Suchwerten im EAS-Profil festgelegt werden.

Erstellen eines generischen EAS-Profils für mehrere Benutzer

Bevor Sie ein EAS-Profil erstellen, das es Geräten automatisch ermöglicht, Daten von Ihrem E-Mail-Server abzurufen, müssen Sie zuerst sicherstellen, dass die Kontodatensätze der Benutzer die entsprechenden Informationen enthalten. Für **Verzeichnisbenutzer** oder Benutzer, die sich mit ihren Verzeichnisanmeldedaten registriert haben (beispielsweise Active Directory), werden diese Informationen automatisch bei der Registrierung ausgefüllt. Diese Informationen sind jedoch bei **Standardbenutzern** nicht automatisch bekannt und müssen mit einer der folgenden zwei Vorgehensweisen ausgefüllt werden:

- Sie können jeden Benutzerdatensatz bearbeiten und die Textfelder **E-Mail-Adresse** und **E-Mail-Benutzername** ausfüllen.
- Sie können die Benutzer auffordern,, diese Informationen beim Registrieren einzugeben. Navigieren Sie dazu zu **Geräte > Geräteeinstellungen > Allgemein > Registrierung** und aktivieren Sie unter dem Tab **Optionale Eingabeaufforderung** das Kontrollkästchen **Eingabeaufforderung für Registrierungs-E-Mail aktivieren**.

Konfigurieren eines EAS Mail-Profils für den systemeigenen Mailclient

Erstellen Sie ein E-Mail-Konfigurationsprofil für den systemeigenen Mailclient auf iOS-Geräten.

Verfahren

1. Gehen Sie zu **Ressourcen > Profile und Baselines > Profile > Hinzufügen.**Wählen Sie **Apple iOS**.
2. Konfigurieren Sie die Einstellungen des Profils unter **Allgemein**.
3. Wählen Sie die **Exchange ActiveSync**-Nutzlast.
4. Wählen Sie **Systemeigener Mailclient** als **Mailclient**. Geben Sie in das Textfeld **Kontoname** eine Beschreibung dieses Mailkontos ein. Füllen Sie das Feld **Exchange ActiveSync Host** mit der externen URL des ActiveSync-Servers Ihres Unternehmens aus.

   Der ActiveSync Server kann jeder beliebige Server sein, der das ActiveSync-Protokoll implementiert, wie Lotus Notes Traveler, Novell Data Synchronizer oder Microsoft Exchange. Im Fall von SEG-Einsätzen (Secure Email Gateway) verwenden Sie die SEG-URL anstelle der E-Mail-Server-URL.
5. Aktivieren Sie das Kontrollkästchen **SSL verwenden**, um Secure Sockets Layer-Nutzung für eingehenden E-Mail-Verkehr zu aktivieren.

6 Aktivieren Sie zur Benutzung weiterer Verschlüsselungszertifikate das Kontrollkästchen **S/MIME verwenden**. Stellen Sie vor Aktivieren dieser Option unter den Profileinstellungen für die **Anmeldedaten** sicher, dass Sie die erforderlichen Zertifikate hochgeladen haben.

   a Wählen Sie das **S/MIME-Zertifikate** zum Signieren der E-Mail-Nachrichten.

   b Wählen Sie das **S/MIME-Verschlüsselungszertifikat** sowohl zum Signieren als auch zum Verschlüsseln von E-Mail-Nachrichten.

   c Wählen Sie das Kontrollkästchen **Pro-Nachricht-Schalter**, damit Endbenutzer auswählen können, welche individuellen E-Mail-Nachrichten mit dem systemeigenen iOS-Mailclient signiert oder verschlüsselt werden sollen (nur überwachte Geräte ab iOS 8).

7 Aktivieren Sie das Kontrollkästchen **OAuth verwenden**, um die URL "Anmelden" und "Token" einzubeziehen.

   a **OAuth Sign In URL**: Geben Sie die URL für das OAuth Sign In ein.

   b **OAuth Token URL**: Geben Sie die URL des OAuth Token ein.

8 Tragen Sie die **Anmeldedaten**, einschließlich **Domänenname, Benutzername und E-Mail-Adresse**, unter Verwendung von Suchwerten ein. Suchwerte beziehen die Informationen direkt vom Datensatz des Benutzerkontos. Bei der Verwendung der Suchwerte {EmailDomain}, {EmailUserName} und {EmailAddress} stellen Sie sicher, dass Ihre Workspace ONE UEM-Benutzerkonten festgelegte E-Mail-Adressen und E-Mail-Benutzernamen haben.

9 Lassen Sie das Feld **Kennwort** leer, um den Benutzer zum Eingeben eines Kennworts aufzufordern.

10 Wählen Sie das **Nutzlastzertifikat**, um ein Zertifikat zur zertifikatbasierten Authentifizierung zu bestimmen, nachdem das Zertifikat der **Anmeldedaten**-Nutzlast hinzugefügt wurde.

11 Konfigurieren Sie nach Bedarf folgende optionale Einstellungen unter **Einstellungen und Sicherheit**:

   a **Vergangene Tage mit ausstehender Mail-Synchronisierung** – Lädt die festgelegte Menge an Mail herunter. Beachten Sie, dass längere Zeitperioden höheren Datenverbrauch zur Folge haben, während das Gerät Mail herunterlädt.

   b **Verhindern, dass Nachrichten verschoben werden** – Verhindert, dass Mail von einer Exchange-Mailbox in eine andere Mailbox auf dem Gerät verschoben wird.

   c **Nutzung in Drittanbieteranwendungen verhindern** – Verhindert, dass andere Anwendungen die Exchange-Mailbox zum Senden von Nachrichten verwenden.

   d **Synchronisierung jüngster Adressen verhindern** – Verhindert Kontaktempfehlungen beim Senden von Mail in Exchange.

   e **Mail Drop verhindern** – Deaktiviert die Funktion von Apple Mail Drop.

   f (iOS 13) **Mail aktivieren** – Aktiviert die Konfiguration einer separaten Mail-App für das Exchange-Konto.

g (iOS 13) **Umschalten von Mail zulassen** – Wenn diese Option deaktiviert ist, können Benutzer Mails nicht ein- oder ausschalten.

h (iOS 13) **Kontakte aktivieren** – Aktiviert die Konfiguration einer separaten Kontakt-App für das Exchange-Konto.

i (iOS 13) **Umschalten von Kontakten zulassen** – Wenn diese Option deaktiviert ist, können Benutzer Kontakte nicht ein- oder ausschalten.

j (iOS 13) **Kalender aktivieren** – Aktiviert die Konfiguration einer separaten Kalender-App für das Exchange-Konto.

k (iOS 13) **Umschalten von Kalendern zulassen** – Wenn diese Option deaktiviert ist, können Benutzer Kalender nicht ein- oder ausschalten.

l **Notizen aktivieren** – Aktiviert die Konfiguration einer separaten Notizen-App für das Exchange-Konto.

m (iOS 13) **Umschalten von Notizen zulassen** – Wenn diese Option deaktiviert ist, können Benutzer Notizen nicht ein- oder ausschalten.

n (iOS 13) **Erinnerungen aktivieren** – Aktiviert die Konfiguration einer separaten Erinnerungs-App für das Exchange-Konto.

o (iOS 13) **Umschalten von Erinnerungen zulassen** – Wenn diese Option deaktiviert ist, können Benutzer Erinnerungen nicht ein- oder ausschalten.

12 Weisen Sie eine **Standardanwendung für Audio-Anrufe** zu, die Ihr systemeigenes EAS-Konto verwendet, um Anrufe durchzuführen, wenn Sie eine Telefonnummer in einer Nachricht auswählen.

13 Klicken Sie auf **Speichern und veröffentlichen**, um das Profil auf Geräte zu schieben.

Konfigurieren eines Benachrichtigungsprofils

Verwenden Sie dieses Profil, um Benachrichtigungen für spezifische Anwendungen zu ermöglichen, die auf der gesperrten Startseite enthalten sein sollen.

Bestimmen Sie, wann und wie die Benachrichtigungen angezeigt werden. Dieses Profil ist auf überwachte Geräte unter iOS 9.3 + anzuwenden.

Verfahren

1 Navigieren Sie zu **Ressourcen** > **Profile und Baselines** > **Profile** > **Listenansicht** > **Hinzufügen**. Wählen Sie **Apple iOS**.

2 Konfigurieren Sie die Einstellungen des Profils unter **Allgemein**.

3 Wählen Sie die **Benachrichtigungen**-Nutzlast in der Liste.

4 Wählen Sie **Anwendung auswählen.** Ein neues Fenster wird angezeigt.

Einstellung	Beschreibung
Anwendung auswählen	Wählen Sie die App, die Sie konfigurieren möchten.
Benachrichtigungen zulassen	Wählen Sie, ob Benachrichtigungen zugelassen sind.
Im Benachrichtigungscenter anzeigen	Wählen Sie, ob Benachrichtigungen im Benachrichtigungscenter angezeigt werden dürfen.
In Sperrbildschirm anzeigen	Wählen Sie, ob Benachrichtigungen im Sperrbildschirm angezeigt werden dürfen.
Ton zulassen	Wählen Sie, ob die Benachrichtigung mit einem Tonsignal angekündigt wird.
Badging zulassen	Wählen Sie, ob auf dem App-Symbol Badges angezeigt werden dürfen.
Benachrichtigungsart bei Entsperrung	Wählen Sie die Art der Benachrichtigung beim Entsperren. ■ **Banner** – Ein quer über die Startseite verlaufender Banner informiert den Benutzer. ■ **Modale Benachrichtigung** – Ein Fenster wird auf der Startseite eingeblendet. Der Benutzer muss mit dem Fenster interagieren, bevor er fortfahren kann.

5 Wählen Sie **Speichern**, um die Nutzlast auf das Gerät zu übertragen.

Konfigurieren eines Profils mit LDAP-Einstellungen

Konfigurieren Sie ein LDAP-Profil, um Endbenutzern den Zugriff auf und die Integration mit Ihren Unternehmens-LDAPv3-Verzeichnisdaten zu ermöglichen.

Verfahren

1 Gehen Sie zu **Ressourcen** > **Profile und Baselines** > **Profile** und wählen Sie **Hinzufügen**. Wählen Sie **Apple iOS**.

2 Konfigurieren Sie die Einstellungen des Profils unter **Allgemein**.

3 Wählen Sie die **LDAP**-Nutzlast.

4 Konfigurieren Sie die LDAP-Einstellungen wie folgt:

Einstellung	Beschreibung
Kontobeschreibung	Geben Sie eine Kurzbeschreibung des LDAP-Kontos ein.
Konto-Hostname	Geben Sie den Namen des Servers für die Active Directory-Nutzung ein bzw. zeigen Sie ihn an.
Kontobenutzername	Geben Sie den Benutzernamen für das Active Directory-Konto an.
Kontokennwort	Geben Sie das Kennwort für das Active Directory-Konto an.
SSL verwenden	Aktivieren Sie dieses Kontrollkästchen, um Secure Socket Layer zu nutzen.
Sucheinstellungen	Geben Sie Einstellungen für die Suche in Active Directory vom Gerät aus ein.

5 Wählen Sie **Speichern und veröffentlichen**.

Konfigurieren eines CalDAV- oder CardDAV-Profils

Setzen Sie ein CalDAV- oder CardDAV-Profil ein, um Endbenutzern zu ermöglichen, Einträge im Unternehmenskalender bzw. Kontakte zu synchronisieren.

Verfahren

1 Gehen Sie zur Seite **Ressourcen** > **Profile und Baselines** > **Profile** und wählen Sie **Hinzufügen**. Wählen Sie **Apple iOS**.

2 Konfigurieren Sie die Einstellungen des Profils unter **Allgemein**.

3 Wählen Sie die **CalDAV- oder CardDAV**-Nutzlast.

4 Konfigurieren Sie folgende **CalDAV**- oder **CardDAV**-Einstellungen:

Einstellung	Beschreibung
Kontobeschreibung	Geben Sie eine kurze Beschreibung des Kontos ein.
Konto-Hostname	Geben Sie den Namen des Servers für die CalDAV-Nutzung ein bzw. zeigen Sie ihn an.
Port	Geben Sie die Portnummer an, für die Kommunikation mit dem CalDAV-Server zugewiesen wurde.
Haupt-URL	Geben Sie Standort des CalDAV-Servers im Internet an.
Kontobenutzername	Geben Sie den Benutzernamen für das Active Directory-Konto an.
Kontokennwort	Geben Sie das Kennwort für das Active Directory-Konto an.
SSL verwenden	Wählen Sie diese Option, um Secure Socket Layer zu nutzen.

5 Wählen Sie **Speichern und veröffentlichen**.

Konfigurieren eines Profils für abonnierte Kalender

Verteilen Sie die mit der Kalender-Anwendung in macOS vorgenommene Kalenderabonnements auf Ihre iOS-Geräte, indem Sie diese Nutzlast konfigurieren.

Verfahren

1 Gehen Sie zu **Ressourcen** > **Profile und Baselines** > **Profile** und wählen Sie **Hinzufügen**. Wählen Sie **Apple iOS**.

2 Konfigurieren Sie die Einstellungen des Profils unter **Allgemein**.

3 Wählen Sie die **Abonnierte Kalender**-Nutzlast

4 Konfigurieren Sie die Kalendereinstellungen wie folgt:

Einstellung	Beschreibung
Beschreibung	Geben Sie eine Kurzbeschreibung der abonnierten Kalender ein.
URL	Geben Sie die URL des Kalenders ein, den Sie abonniert haben.

Einstellung	Beschreibung
Benutzername	Geben Sie den Benutzernamen des Endbenutzers für die Authentifizierung ein.
Kennwort	Geben Sie das Kennwort des Endbenutzers für die Authentifizierung ein.
SSL verwenden	Aktivieren Sie diese Option, um die gesamte Datenkommunikation über SSL abzuwickeln.

5 Wählen Sie **Speichern und veröffentlichen**.

Konfigurieren eines Webclip-Profils

Webclips sind Web-Lesezeichen, die Sie auf Geräte schieben können und die dann entweder auf dem Geräte-Springboard oder in Ihrem App Catalog als Symbol angezeigt werden.

Verfahren

1 Navigieren Sie zu **Ressourcen** > **Profile und Baselines Profile** > **Hinzufügen**. Wählen Sie **Apple iOS**.

2 Konfigurieren Sie die Einstellungen des Profils unter **Allgemein**.

3 Wählen Sie die **Webclips**-Nutzlast von der Liste.

4 Konfigurieren Sie **Webclip**-Einstellungen, einschließlich:

Einstellung	Beschreibung
Bezeichnung	Geben Sie den Text ein, der dann unter dem Symbol „Webclip" auf dem Gerät des Endbenutzers erscheint. Beispiel: „AirWatch Self-Service Portal“.
URL	Geben Sie die URL des Webclips ein, der erscheinen soll. Es folgen einige Beispiele für Workspace ONE UEM-Seiten: ■ Verwenden Sie für das SSP https://<Airwatch Environment>/mydevice/ ■ Verwenden Sie für den App Catalog https://<Environment>/Catalog/ViewCatalog/{SecureDeviceUdid}/{DevicePlatform} ■ Verwenden Sie für den Book Catalog https://<Environment>/Catalog/BookCatalog?uid={DeviceUUID}
Entfernbar	Ermöglichen Sie Endbenutzern, per Langdruckfunktion den Webclip von ihren Geräten zu entfernen.
Symbol	Wählen Sie diese Option zum Hochladen als Webclip-Symbol. Laden Sie das benutzerdefinierte Symbol im .GIF-, .JPG- oder .PNG-Format für die Anwendung hoch. Die besten Ergebnisse erreichen Sie mit einem quadratischen Bild von nicht mehr als 400 Pixel auf beiden Seiten und weniger als 1 MB bei Nichtkomprimierung. Die Grafik wird automatisch skaliert und zugeschnitten sowie in das .PNG-Format konvertiert. Webclip-Symbole betragen 104 x 104 Pixel bei Geräten mit Retina-Anzeige oder 57 x 57 Pixel bei allen anderen Geräten.
Vorerstelltes Symbol	Wählen Sie diese Option zum Anzeigen des Symbols ohne jegliche visuelle Effekte.
Vollbild	Wählen Sie diese Option zum Starten der Webseite im Vollbildmodus.

5 Wählen Sie **Speichern und veröffentlichen**.

Konfigurieren eines SCEP/Anmeldedaten-Profils

Obwohl Sie Ihre geschäftliche E-Mail, WLAN und VPN mit sicheren Kennwörtern und anderen Restriktionen schützen, bleibt Ihre Infrastruktur für Brute-Force- und Wörterbuchangriffe anfällig. Und natürlich können auch Mitarbeiter Fehler machen. Zur erhöhten Sicherheit können Sie digitale Zertifikate implementieren, um Ihr Unternehmensinventar zu schützen.

Für eine Zuweisung von Zertifikaten müssen Sie zunächst eine Zertifizierungsstelle definieren. Dann konfigurieren Sie eine **Anmeldedaten**-Nutzlast zusätzlich zu Ihrer **Exchange ActiveSync (EAS)**-, **WLAN**- oder **VPN**-Nutzlast. Jede dieser Nutzlasten weist Einstellungen auf, mit denen die in der **Anmeldedaten**-Nutzlast definierte Zertifizierungsstelle zugeordnet wird.

Um Zertifikate per „Push“ an Geräte zu übertragen, müssen Sie eine **Anmeldedaten**- oder **SCEP**-Nutzlast als Teil der von Ihnen für EAS-, WLAN- und VPN-Einstellungen erstellten Profile konfigurieren. So erstellen Sie ein zertifikatsfähiges Profil:

Verfahren

1 Gehen Sie zu **Ressourcen** > **Profile und Baselines** > **Profile** > **Hinzufügen** und wählen Sie **iOS** aus der Liste der Plattformen.

2 Konfigurieren Sie die Einstellungen des Profils unter **Allgemein**.

3 Wählen Sie zur Konfiguration eine **EAS**-, **WLAN**- oder **VPN**-Nutzlast. Füllen Sie die erforderlichen Informationen aus – je nach der von Ihnen ausgewählten Nutzlast.

4 Wählen Sie die **Anmeldedaten**- (oder **SCEP**)-Nutzlast.

5 Wählen Sie eine Option aus dem Menü **Anmeldedatenquelle**:

   a Wählen Sie das **Hochladen** eines Zertifikats und geben Sie den **Zertifikatnamen** ein.

   b Wählen Sie **Definierte Zertifizierungsstelle** und dann die geeignete **Zertifizierungsstelle** und **Zertifikatvorlage**.

   c Wählen Sie **Benutzerzertifikat** und den Zweck für das **S/MIME**-Zertifikat.

   d Wählen Sie **Abgeleitete Anmeldedaten** und auf Basis der Verwendung des Zertifikats die entsprechende **Schlüsselverwendung** aus. Schlüsselverwendungsoptionen sind **Authentifizierung**, **Signierung** und **Verschlüsselung**.

6 Navigieren Sie zurück zur vorherigen Nutzlast für **EAS**, **WLAN** oder **VPN**.

7 Geben Sie das Identitätszertifikat in der Nutzlast an:

   a **EAS** – Wählen Sie das **Nutzlastzertifikat** unter den Anmeldeinformationen.

   b **Wi-Fi** – Wählen Sie einen kompatiblen **Sicherheitstyp** („WEP Enterprise“, „WPA/WPA2 Enterprise“ oder „Beliebig [Enterprise]“) und dann das **Identitätszertifikat** unter Authentifizierung.

   c **VPN** – Wählen Sie einen kompatiblen **Verbindungstyp** (z.B. CISCO AnyConnect, F5 SSL) und **Zertifikat** aus der Dropdown-Liste „Benutzerauthentifizierung“. Wählen Sie das **Identitätszertifikat** aus.

8 Navigieren Sie zurück zu **Anmeldedaten**- (oder **SCEP**-)Nutzlast.

9 Wählen Sie **Speichern und veröffentlichen**, nachdem Sie eventuelle restliche Einstellungen konfiguriert haben.

Konfigurieren eines globalen HTTP Proxy-Profils

Konfigurieren Sie einen globalen HTTP-Proxy und sorgen Sie so dafür, dass der gesamte HTTP-Datenverkehr von überwachten Geräten mit iOS 7 und höher über einen designierten Proxy geleitet wird. Eine Schule kann beispielsweise einen globalen Proxy so einstellen, dass beim Webbrowsen der Webverkehr durch dessen Web-Inhaltsfilter geleitet wird.

Verfahren

1 Gehen Sie zu **Ressourcen** > **Profile und Baselines** > **Profile** >**Hinzufügen**. Wählen Sie **Apple iOS**.

2 Konfigurieren Sie die Einstellungen des Profils unter **Allgemein**.

3 Wählen Sie die **Globaler HTTP-Proxy**-Nutzlast aus der Liste.

4 Konfigurieren Sie die Proxy-Einstellungen wie folgt:

Einstellung	Beschreibung
Proxytyp	Wählen Sie für die Proxy-Konfiguration **Auto** oder **Manuell**.
Proxy-Server	Geben Sie die URL für den Proxyserver ein. Dieses Textfeld wird angezeigt, wenn der **Proxy-Typ** auf **Manuell** eingestellt ist.
Proxyserver Port	Geben Sie den Port ein, der für die Kommunikation mit dem Proxy verwendet wird. Dieses Textfeld wird angezeigt, wenn der **Proxy-Typ** auf **Manuell** eingestellt ist.
Proxy-Benutzername/Kennwort	Falls der Proxy Anmeldedaten verlangt, können Sie Suchwerte verwenden, um die Authentifizierungsmethode zu definieren. Dieses Textfeld wird angezeigt, wenn der **Proxy-Typ** auf **Manuell** eingestellt ist.
Umgehung des Proxys zum Zugriff auf Captive-Netzwerke zulassen	Aktivieren Sie dieses Kontrollkästchen, um dem Gerät die Umgehung der Proxy-Einstellungen zu ermöglichen und auf ein bekanntes Netzwerk zuzugreifen. Dieses Textfeld wird angezeigt, wenn der **Proxy-Typ** auf **Manuell** eingestellt ist.

Einstellung	Beschreibung
Proxy PAC-Datei-URL	Geben Sie die URL der Proxy PAC-Datei ein, damit ihre Einstellungen automatisch angewendet werden. Dieses Textfeld wird angezeigt, wenn der **Proxy-Typ** auf **Manuell** eingestellt ist.
Direkte Verbindung bei unerreichbarer PAC zulassen	Wählen Sie diese Option, wenn iOS-Geräte den Proxyserver umgehen sollen, falls die PAC-datei nicht erreicht werden kann. Dieses Textfeld wird angezeigt, wenn der **Proxy-Typ** auf **Manuell** eingestellt ist.
Umgehung des Proxys zum Zugriff auf Captive-Netzwerke zulassen	Aktivieren Sie dieses Kontrollkästchen, um dem Gerät die Umgehung der Proxy-Einstellungen zu ermöglichen und auf ein bekanntes Netzwerk zuzugreifen. Dieses Textfeld wird angezeigt, wenn der **Proxy-Typ** auf **Manuell** eingestellt ist.

5 Wählen Sie **Speichern und veröffentlichen**.

Konfigurieren eines Einzelanwendungsmodus-Profils

Der Einzelanwendungsmodus bietet ermöglicht es, Geräte so bereitzustellen, dass diese nur auf eine einzige Anwendung ihrer Wahl zugreifen können. Der Einzelanwendungsmodus deaktiviert die Schaltfläche „Starten“ und zwingt das Gerät, direkt in die designierte Anwendung zu booten, wenn der Benutzer einen manuellen Neustart versucht.

Voraussetzungen

Diese Funktion gewährleistet, dass das Gerät nicht außerhalb der gewünschten Anwendung verwendet wird und dass das Gerät nicht unbeabsichtigt auf andere Anwendungen, Geräteeinstellungen oder einen Internetbrowser zugreift. Diese Funktion ist für Restaurants und Läden sinnvoll. Im Bildungsbereich können Studierende Geräte verwenden, die gesperrt und nur für ein bestimmtes Spiel, ein eBook oder eine Übung freigegeben sind.

- Ein im Modus „Überwacht“ konfiguriertes Gerät mit iOS 7 und höher. (Für erweiterte Optionen und autonomen Einzelanwendungsmodus iOS 7 und höher erforderlich.)

Verfahren

1 Gehen Sie zu **Ressourcen** > **Profile und Baselines** > **Profile** >**Hinzufügen.**Wählen Sie **Apple iOS**.

2 Konfigurieren Sie die Einstellungen des Profils unter **Allgemein**.

3 Wählen Sie die **Einzelanwendungsmodus**-Nutzlast

4 Konfigurieren Sie die Einstellungen für den Einzelanwendungsmodus wie folgt:

Einstellung	Beschreibung
Filtertyp	Wählen Sie einen Filter, entweder **Gerät auf eine Einzelanwendung festlegen** oder **Zulässige Anwendungen für autonomen Einzelanwendungsmodus**: ■ **Gerät auf eine Einzelanwendung festlegen** – Legen Sie Geräte auf eine einzige öffentliche, interne, gekaufte oder systemeigene Anwendung fest, bis das Profil mit dieser Nutzlast entfernt wird. Die „Start“-Taste wird deaktiviert und das Gerät kehrt vom Energiesparmodus oder nach einem Neustart immer zu der vorgegebenen Anwendung zurück. ■ **Zulässige Anwendungen für autonomen Einzelanwendungsmodus** – Ermöglichen Sie es Anwendungen von der Whitelist, den Einzelanwendungsmodus basierend auf einem Ereignis auszulösen, dass festlegt, wann der Einzelanwendungsmodus auf dem Gerät ein- und ausgeschaltet werden soll. Dieser Vorgang erfolgt in der Anwendung selbst in der vom App-Entwickler festgelegten Form.
Anwendungspaket-ID	Geben Sie die Paket-ID ein oder wählen Sie eine aus dem Dropdown-Menü. Die Paket-ID erscheint im Dropdown-Menü, nachdem die Anwendung in die UEM-Konsole hochgeladen wurde. Beispiel: **com.air-watch.secure.browser**.
Optionale Einstellungen	Wählen Sie optionale Einstellungen für überwachte Geräte unter iOS 7 und höher.

5 Wählen Sie **Speichern und veröffentlichen**. Jedes mit diesem Profil versehene Gerät wechselt in den Einzelanwendungsmodus.

Neustarten eines Geräts im Einzelanwendungsmodus

Das Kaltstartverfahren wird verwendet, um ein Gerät neu zu starten, das im Einzelanwendungsmodus betrieben wird.

Verfahren

1 Halten Sie die Home-Taste und den Ein-/Ausschalter gleichzeitig gedrückt.

2 Halten Sie weiterhin beide Tasten, bis sich das Gerät aus- und wieder einschaltet.

3 Lassen Sie die Tasten los, wenn Sie das silberfarbene Apple-Logo sehen. Es kann etwas dauern, bis die Hauptseite geladen wird.

Deaktivieren des Einzelanwendungsmodus auf iOS-Geräten

Endbenutzer sind nicht in der Lage, bei aktiviertem Einzelanwendungsmodus die Anwendung zu verlassen. Workspace ONE UEM bietet zwei Optionen für das Beenden des Einzelanwendungsmodus, je nachdem, welchen Einzelanwendungsmodus Sie aktivieren.

Sie können den Einzelanwendungsmodus vorübergehend deaktivieren, wenn Sie die festgelegte Anwendung auf eine neue Version aktualisieren möchten. Deaktivieren Sie wie folgt den Einzelanwendungsmodus, installieren Sie die neue Anwendungsversion und reaktivieren Sie den Einzelanwendungsmodus.

Verfahren

1 Gehen Sie zu **Ressourcen** > **Profile und Baselines** > **Profile** . Klicken Sie in der Reihe für das Einzelanwendungsmodusprofil auf das Symbol **Geräte anzeigen**.

2 Wählen Sie **Profil entfernen** für das Gerät, von dem Sie die Einstellung entfernen möchten.

3 Aktualisieren Sie die Anwendung auf die gewünschte Version.

4 Installieren Sie das Profil erneut unter Beachtung der Schritte in Konfigurieren eines Einzelanwendungsmodus-Profils.

Geräteadministrator dazu berechtigen, den Einzelanwendungsmodus vom Gerät zu beenden

Sie können einen Administrator berechtigen, den Einzelanwendungsmodus durch Eingabe einer Kennung auf dem Gerät selbst zu verlassen. Diese Option ist nur verfügbar, wenn Sie den autonomen Einzelanwendungsmodus als **Filterart** für das Einzelanwendungsmodusprofil aktivieren.

Verfahren

1 Gehen Sie zur Seite **Ressourcen** > **Profile und Baselines** > **Profile** > **hinzufügen.**Wählen Sie **Apple iOS**.

2 Konfigurieren Sie die Einstellungen des Profils unter **Allgemein**.

3 Wählen Sie die **Einzelanwendungsmodus**-Nutzlast

4 Wenn Sie **Zulässige Apps für autonomen Einzel-App-Modus** ausgewählt haben, geben Sie die Paket-ID einer Anwendung, die den autonomen Einzel-App-Modus unterstützt, unter **Zulässige Apps** ein.

5 Wählen Sie **Speichern und veröffentlichen**, um dieses Profil per Push auf die zugewiesenen Geräte zu übertragen.

6 Gehen Sie zur Seite **Ressourcen** > **Apps** > **Native** > **Public** für öffentliche Apps, oder **Ressourcen** >**Apps** >**Native erworben** für Anwendungen, die über VPP verwaltet werden.

7 Suchen Sie die vom autonomen Einzelanwendungsmodus unterstützte Anwendung, und wählen Sie das Symbol **Zuweisung bearbeiten** aus. Das Fenster „Zuweisung bearbeiten“ wird angezeigt.

8 Wählen Sie die Registerkarte **Zuweisung** und erweitern Sie den Abschnitt **Richtlinien**.

9 Wählen Sie **Aktiviert** für **Anwendungskonfiguration senden**, geben Sie **AdminPasscode** als **Konfigurationsschlüssel** ein und legen Sie den **Werttyp** mit **Zeichenfolge** fest.

10 Geben Sie die Kennung ein, den Administratoren verwenden, um den Einzelanwendungsmodus zu verlassen, als **Konfigurationswert**. Der Wert kann numerisch oder alphanumerisch sein. Wählen Sie **Hinzufügen**.

11 Wählen Sie **Speichern und veröffentlichen**, um die Anwendungskonfiguration per Push zu übertragen.

Konfigurieren eines Web-Inhaltsfilterprofils

Sie können zulassen oder verhindern, dass Endanwender auf bestimmte URLs mit Webbrowsern zugreifen, indem Sie eine Web-Inhaltsfilter-Nutzlast konfigurieren, die auf Geräte angewendet wird. Alle URLs müssen mit http:// oder https:// beginnen. Wenn nötig, müssen Sie separate Einträge für sowohl die HTTP- als auch die HTTPS-Versionen der gleichen URL erstellen. Die Web-Inhaltsfilter-Nutzlast erfordert überwachte iOS 7+-Geräte.

Verfahren

1 Navigieren Sie zu **Ressourcen** > **Profile und Baselines** > **Profile** > **Hinzufügen.**Wählen Sie **iOS** aus.

2 Konfigurieren Sie die Einstellungen des Profils unter **Allgemein**.

3 Wählen Sie die **Inhaltsfilter-Nutzlast**.

4 Wählen Sie das Dropdown-Menü **Filtertyp**:

   a Integriert: Websites zulassen

   b Integriert: Websites verweigern

   c Plug-Ins

Integriert: Websites zulassen

Erstellen Sie eine Whitelist von URLs, damit die Endbenutzer nur diese spezifischen Websites von der Liste aufrufen können, andere hingegen nicht.

Verfahren

1 Wählen Sie **Integriert: Websites zulassen** im Dropdown-Menü **Filtertyp**, um auszuwählen, auf welche Plug-Ins zugegriffen werden kann.

2 Wählen Sie **Hinzufügen** und konfigurieren Sie eine Liste zugelassener Websites:

Einstellung	Beschreibung
Zulässige URLs	Die URL einer Website von der Whitelist
Titel	Titel des Lesezeichens
Lesezeichenpfad	Der Ordner, in dem das Lesezeichen in Safari hinzugefügt wird

Integriert: Websites verweigern

Konfigurieren Sie eine Blacklist von URLs, um zu verhindern, dass Benutzer diese festgelegten Websites aufrufen. Alle anderen Websites bleiben aber für Endbenutzer verfügbar. Websites mit obszönen Inhalten werden automatisch ausgefiltert, sofern nicht eine Ausnahme zugelassen wird.

Verfahren

- Wählen Sie **Integriert: Website verweigern** im Dropdown-Menü **Filtertyp** und konfigurieren Sie Websites von Blacklists:

Einstellung	Beschreibung
Nicht zulässige URLs	Geben Sie **Nicht zulässige URLs** ein und trennen Sie diese durch neue Zeilen, Leerzeichen und Kommas.
Unangemessene Websites automatisch filtern	Wählen Sie den Filter für nicht jugendfreie Websites.
Lesezeichenpfad	Geben Sie den Ordnerpfad ein, in dem das Lesezeichen in Safari hinzugefügt wird
Zulässige URLs	Geben Sie alle Websites ein, die als Ausnahmen zum automatischen Filter zulässig sein könnten.

Plug-Ins

Diese Nutzlast ermöglicht Ihnen die Integration mit einem Web-Inhaltsfilter-Plug-In eines Drittanbieters mit Safari.

Wenn Sie eine spezifische Integration in Inhaltsfilter Konfigurieren eines Forcepoint-Inhaltsfilterprofils oder Konfigurieren eines Blue Coat Inhaltsfilterprofils vornehmen möchten, sehen Sie sich die entsprechenden Abschnitte in diesem Leitfaden an.

Verfahren

1. Wählen Sie **Plug-In** im Dropdown-Menü **Filtertyp**, um auszuwählen, auf welche Plug-Ins zugegriffen werden kann. Sie müssen Webkit- oder Socket-Datenverkehrsanforderungen aktivieren, damit die Nutzlast funktioniert.

Einstellung	Beschreibung
Filtername	Geben Sie den Namen des Filters ein, der auf dem Gerät angezeigt wird.
Bezeichner	Geben Sie die Paket-ID des Bezeichners des Plug-Ins an, das einen Filterdienst bereitstellt.
Dienstadresse	Geben Sie den Hostnamen, die IP-Adresse oder die URL für den Dienst ein.
Organisation	Wählen Sie die Organisationszeichenfolge, die für das Plug-In eines Drittanbieters übergeben wird.
WebKit-Verkehr filtern	Wählen Sie die Option, um auszuwählen, ob Webkit-Datenverkehr gefiltert wird.
Socket-Verkehr filtern	Wählen Sie diese Option, um auszuwählen, ob Socket-Datenverkehr gefiltert wird.

2 Konfigurieren Sie die **Authentifizierungsdaten** wie folgt:

Einstellung	Beschreibung
Benutzername	Verwenden Sie Suchwerte, die die Informationen direkt vom Datensatz des Benutzerkontos beziehen. Stellen Sie sicher, dass Ihre Workspace ONE UEM-Benutzerkonten über eine bestimmte E-Mail-Adresse und einen bestimmten E-Mail-Benutzernamen verfügen.
Kennwort	Geben Sie das Kennwort für dieses Konto ein.
Nutzlastzertifikat	Wählen Sie das Authentifizierungszertifikat.

3 Fügen Sie **benutzerdefinierte Daten** hinzu, die die von Filterdiensten von Drittanbietern verlangten Schlüssel enthalten. Diese Informationen gehen zum Anbieterkonfigurationsverzeichnis.

4 Wählen Sie **Speichern und veröffentlichen**.

Konfigurieren eines Profils für verwaltete Domänen

Verwaltete Domänen stellen eine weitere Funktion von Workspace ONE UEM dar, um die Verwaltungsfunktion „Öffnen in“ von Apple auf iOS 8-Geräten mithilfe zu verbessern. Wenn Sie die Funktion „Öffnen in“ mit verwalteten Domänen verwenden, können Sie Unternehmensdaten schützen, indem Sie kontrollieren, welche Anwendungen von Unternehmensdomänen mit Safari heruntergeladene Dokumente öffnen können.

Geben Sie URLs und Unterdomänen an, um zu bestimmen, wie Dokumente, Anlagen und Downloads vom Browser geöffnet werden. In verwalteten E-Mail-Domänen kann außerdem eine farbkodierte Warnanzeige in E-Mail-Nachrichten angezeigt werden, die an nicht verwaltete Domänen gesendet werden. Diese Tools helfen Endbenutzern, schnell zu bestimmen, welche Dokumente mit Unternehmensanwendungen geöffnet werden können und welche Dokumente privat sind und in persönlichen Anwendungen geöffnet werden können.

Verfahren

1 Navigieren Sie zu **Ressourcen** > **Profile und Baselines** > **Profile** > **Listenansicht** > **Hinzufügen** . Wählen Sie **Apple iOS**.

2 Konfigurieren Sie die Einstellungen des Profils unter **Allgemein**.

3 Wählen Sie die **Verwaltete Domänen**-Nutzlast aus der Liste.

Einstellung	Beschreibung
Verwaltete E-Mail-Domänen	Geben Sie Domänen ein, um festzulegen, welche E-Mail-Adressen Unternehmensdomänen sind. Beispiel: **exchange.acme.com**. E-Mails, die an Adressen gesendet werden und hier nicht angegeben sind, sind in der E-Mail-Anwendung markiert, um anzuzeigen, dass die Adresse nicht zur Unternehmensdomäne gehört.
Verwaltete Web-Domänen	Geben Sie Domänen ein, um spezifische URLs oder Subdomänen auszuwählen, die als verwaltet angesehen werden können. Beispiel: **sharepoint.acme.com**. Alle Dokumente oder Anlagen von diesen Domänen gelten als verwaltet.
Safari-Kennwortdomänen	Geben Sie das Kennwort für die Domänen ein, die Sie Safari zum Speichern angeben. Diese Option gilt nur für überwachte Geräte.

4 Wählen Sie **Speichern und veröffentlichen**.

Konfigurieren eines Profils für Netzwerknutzungs-Regeln

Konfigurieren Sie Netzwerknutzungs-Regeln, um zu steuern, welche Anwendungen und SIM-Karten basierend auf dem Netzwerkverbindungstyp oder beim Roaming des Geräts auf Daten zugreifen dürfen. Diese Funktion ermöglicht es Administratoren, die Kosten für Datenübertragungen zu verwalten, wenn Mitarbeiter Geräte für die Arbeit verwenden. Verwenden Sie detaillierte Steuerelemente, um je nach Bedarf verschiedene Regeln auf verschiedene Anwendungen und SIMs anzuwenden.

Verfahren

1 Gehen Sie zu **Ressourcen** > **Profile und Baselines** > **Profile** > **Listenansicht** > **Hinzufügen**. Wählen Sie **Apple iOS**.

2 Konfigurieren Sie die Einstellungen des Profils unter **Allgemein**.

3 Wählen Sie die **Netzwerknutzungs-Regeln**-Nutzlast aus der Liste.

4 Geben Sie unter den App-Nutzungsregeln den **Anwendungsbezeichner** für alle öffentlichen, internen oder gekauften Anwendungen ein.

5 Aktivieren Sie **Mobilfunkdaten zulassen** und **Datennutzung im Roamingbetrieb**. Beide Optionen sind standardmäßig ausgewählt.

6 Geben Sie unter den SIM-Nutzungsregeln die **ICCIDs** der SIM-Karten (physische und eSIM-Karten) an, und geben Sie den Typ der **Wi-Fi Assist**-Funktion an, entweder **Standard** oder **Unbegrenzte Mobilfunkdaten**.

7 Wählen Sie **Speichern und veröffentlichen**.

Konfigurieren eines macOS-Serverkonto-Profils

Fügen Sie ein macOS-Serverkonto direkt von der UEM-Konsole hinzu, um Ihr MDM-Framework zu verwalten. Verwenden Sie dies, um die Anmeldedaten hinzuzufügen, damit Endbenutzer auf Dateifreigabe auf macOS zugreifen können.

Verfahren

1 Gehen Sie zu **Ressourcen** > **Profile und Baselines**>**Profile**>**Hinzufügen**. Wählen Sie **Apple iOS**.

2 Konfigurieren Sie die Einstellungen des Profils unter **Allgemein**.

3 Wählen Sie die **macOS-Serverkonto**-Nutzlast aus der Liste.

Einstellung	Beschreibung
Kontobeschreibung	Geben Sie den Anzeigenamen für das Konto ein.
Hostname	Geben Sie die Serveradresse ein.
Benutzername	Geben Sie den Anmeldenamen des Benutzers ein.
Kennwort	Geben Sie das Kennwort des Benutzers ein.
Port	Bezeichnet die Portnummer, die beim Kontakt mit dem Server zu verwenden ist.

4 Wählen Sie **Speichern und veröffentlichen**.

Konfigurieren eines Single-Sign-On-Profils

Aktivieren Sie Single Sign-On für Unternehmensanwendungen, um einen nahtlosen Zugriff ohne Authentifizierungserfordernis bei jeder Anwendung zu ermöglichen. Verteilen Sie dieses Profil, um Endbenutzer über die Kerberos-Authentifizierung zu authentifizieren anstatt Kennwörter auf Geräten zu speichern. Weitere Informationen zu Single Sign-On-Einstellungen finden Sie im **VMware Workspace ONE UEM Mobile Application Management Guide**.

Verfahren

1 Gehen Sie zu **Ressourcen** > **Profile und Baselines** > **Profile** > **Hinzufügen** und wählen Sie **Apple iOS**.

2 Konfigurieren Sie die Einstellungen des Profils unter **Allgemein**.

3 Wählen Sie die **Single-Sign-On**-Nutzlast.

4 Geben Sie die **Verbindungsdaten** ein:

Einstellung	Beschreibung
Kontoname	Geben Sie den Namen an, der auf dem Gerät erscheinen soll.
Kerberos-Prinzipalname	Geben Sie den Kerberos-Prinzipalnamen ein.

Einstellung	Beschreibung
Bereich	Geben Sie den Kerberos-Domänenbereich ein. Dieser Parameter muss durchgehend in Großbuchstaben geschrieben werden.
Erneuerungszertifikat	Auf iOS 8+-Geräten wählen Sie das Zertifikat, das für die automatische neuerliche Authentifizierung des Benutzers ohne Interaktion verwendet wird, wenn die Single Sign-On-Sitzung des Benutzers abläuft. Konfigurieren Sie ein Erneuerungszertifikat (beispielsweise .pfx) mithilfe einer Konfigurieren eines SCEP/Anmeldedaten-Profils-Nutzlast.

5 Geben Sie die **URL-Präfixe** ein, die zur Nutzung dieses Kontos zur Kerberos-Authentifizierung über HTTP angeglichen werden müssen. Zum Beispiel: **http://sharepoint.mueller.de/**. Wird dieses Feld freigelassen, ist das Konto in der Lage, alle HTTP- und HTTPS-URLs abzugleichen.

6 Geben Sie die **Anwendungspaket-ID** ein oder wählen Sie eine aus dem Dropdown-Menü. Die Paket-ID erscheint im Dropdown-Menü, nachdem die Anwendung in die UEM-Konsole hochgeladen wurde. Beispiel: **com.air-watch.secure.browser**. Die angegebenen Anwendungen müssen die Kerberos-Authentifizierung unterstützen.

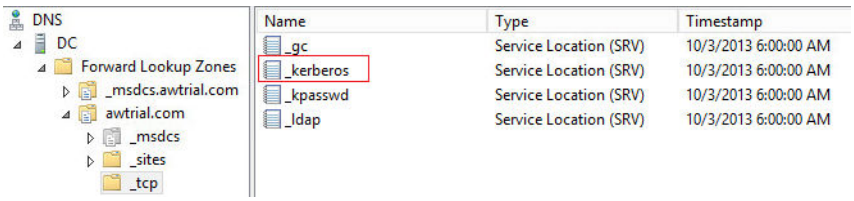
7 Wählen Sie **Speichern und veröffentlichen**.

Beispiel

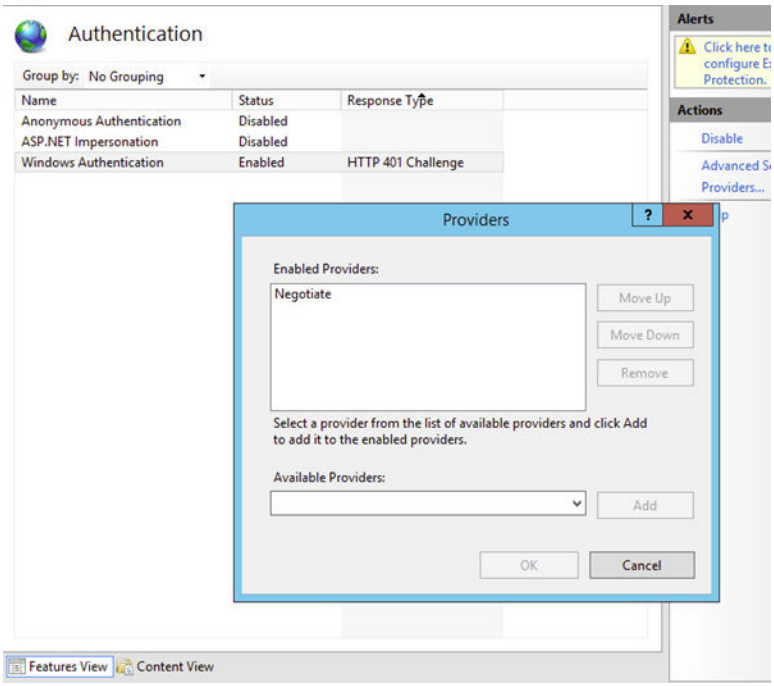
Wenn bei einem Webbrowser die Endbenutzer zu einer in der Nutzlast angegebene Website navigieren, werden sie aufgefordert, das Kennwort ihres Domänenkontos einzugeben. Danach brauchen Sie Ihre Anmeldedaten nicht erneut einzugeben, um auf eine der Websites zuzugreifen, die in der Nutzlast angegeben sind.

Hinweis

- Wenn Geräte Kerberos-Authentifizierung nutzen, müssen Sie mit dem Unternehmensnetzwerk (über WLAN oder VPN) verbunden sein.
- Der DNS-Server muss einen Datensatz der Kerberos-Dienste (KDC-Server) enthalten.



- Sowohl die Anwendung auf dem mobilen Gerät als auch die Website müssen Kerberos/ Negotiate-Authentifizierung unterstützen.



Konfigurieren eines SSO-Erweiterungsprofils

Um eine Anwendung auf dem Gerät so zu konfigurieren, dass Single Sign-on (SSO) mit der Kerberos-Erweiterung durchgeführt wird, konfigurieren Sie das SSO-Erweiterungsprofil. Mit dem SSO-Erweiterungsprofil müssen Benutzer Ihren Benutzernamen und Ihr Kennwort nicht angeben,

um auf bestimmte URLs zugreifen zu können. Dieses Profil gilt nur für Geräte mit iOS 13 und höher.

Verfahren

1 Gehen Sie zu **Ressourcen** > **Profile und Baselines** > **Profile** und wählen Sie **Hinzufügen**> **Apple iOS**.

2 Konfigurieren Sie die Einstellungen des Profils unter **Allgemein**.

3 Wählen Sie als Nutzlast **SSO-Erweiterung** aus.

4 Konfigurieren Sie die Profileinstellungen.

Einstellung	Beschreibung
Erweiterungstyp	Wählen Sie den Typ der SSO-Erweiterung für die Anwendung aus. Wenn Sie „Generisch“ auswählen, geben Sie im Feld **Erweiterungsbezeichner** die Paket-ID der Anwendungserweiterung an, die SSO für die angegebenen URLs ausführt. Wenn „Kerberos“ ausgewählt ist, geben Sie den Active Directory-Bereich und die Domänen an.
Typ	Wählen Sie als Erweiterungstyp entweder „Anmeldedaten“ oder „Umleiten“ aus. Die Erweiterung „Anmeldedaten“ wird für Authentifizierung per Aufforderung/Rückmeldung verwendet. Die Erweiterung „Umleiten“ kann die OpenID Connect-, Oauth- und SAML-Authentifizierung verwenden.
Team-Bezeichner	Geben Sie den Team-Bezeichner der Anwendungserweiterung ein, die SSO für die angegebenen URLs ausführt.
URLs	Geben Sie ein oder mehrere URL-Präfixe von Identitätsanbietern ein, bei denen die Anwendungserweiterung SSO ausführt.
Zusätzliche Einstellungen	Geben Sie zusätzliche Einstellungen für das Profil in XML-Code ein, der dem ExtensionData-Knoten hinzugefügt wird.
Active Directory-Bereich	Diese Option wird nur angezeigt, wenn „Kerberos“ als Erweiterungstyp ausgewählt ist. Geben Sie den Namen für den Kerberos-Bereich ein.
Domänen	Geben Sie die Hostnamen oder die Domänennamen ein, die über die Anwendungserweiterung authentifiziert werden können.
Site-AutoErmittlung verwenden	Aktivieren Sie die Option, damit die Kerberos-Erweiterung automatisch LDAP und DNS verwendet, um den Namen der Active Directory-Site zu ermitteln.
Automatische Anmeldung zulassen	Aktivieren Sie die Option, damit Kennwörter im Schlüsselbund gespeichert werden können.
Benutzer-Touch-ID oder -kennwort anfordern	Aktivieren Sie die Option, damit der Benutzer die Touch ID, die FaceID oder die Kennung für den Zugriff auf den Schlüsselbundeintrag bereitstellen kann.
Zertifikat	Wählen Sie das Zertifikat aus, das auf das Gerät übertragen werden soll, das sich im selben MDM-Profil befindet.
Zulässige Paket-IDs	Geben Sie eine Liste der Anwendungspaket-IDs ein, um den Zugriff auf das Kerberos Ticket Granting Ticket (TGT) zuzulassen.

5 Klicken Sie auf **Speichern und veröffentlichen**.

Konfigurieren eines AirPlay Whitelist-Profils

Beim Konfigurieren der AirPlay-Nutzlast können Sie eine bestimmte Gruppe von Geräten per Whitelist sperren, sodass diese nach Geräte-ID Übertragungsrechte erhalten. Daher gilt: Falls der Anzeigezugriff auf Ihr Apple TV kennwortgeschützt ist, können Sie das Kennwort im Voraus eingeben, ohne nicht autorisierten Parteien die PIN anzuzeigen.

Diese Nutzlast funktioniert sogar, wenn Sie Ihren Apple TV nicht bei Workspace ONE UEM registrieren. Weitere Informationen zu tvOS-Funktionen finden Sie im Handbuch **tvOS Management**.

Hinweis AirPlay-Whitelisting gilt derzeit nur für überwachte iOS 7- und iOS 8-Geräte.

Verfahren

1 Gehen Sie zu **Ressourcen** > **Profile und Baselines** > **Profile**>**Hinzufügen**. Wählen Sie **Apple iOS** aus der Plattformliste.

2 Konfigurieren Sie die Einstellungen des Profils unter **Allgemein**.

3 Wählen Sie die Registerkarte **AirPlay Mirroring-Nutzlast**.

4 Konfigurieren Sie die Einstellungen der **Kennwörter** für iOS 7-Geräte und **Whitelists** für überwachte iOS 7+-Geräte:

Einstellung	Beschreibung
Gerätename	Geben Sie den Gerätenamen für das AirPlay-Ziel ein.
Kennwort	Geben Sie das Kennwort für das AirPlay-Ziel ein. Wählen Sie **Hinzufügen**, um zusätzliche Geräte von der Whitelist hinzuzufügen.
Anzeigename	Geben Sie den Namen des Zielbildschirms ein. Der Name muss dem Namen des tvOS-Geräts entsprechen, wobei die Groß- und Kleinschreibung beachtet werden muss. Den Gerätenamen können Sie den Einstellungen des tvOS-Geräts entnehmen. (Überwachte iOS 7+-Geräte)
Geräte-ID	Geben Sie die Geräte-ID (einschließlich MAC-Adresse oder Ethernet-Adresse im Format XX:XX:XX:XX:XX:XX) für den Ziel-Bildschirm ein. Wählen Sie **Hinzufügen**, um zusätzliche Geräte von der Whitelist hinzuzufügen. (Überwachte iOS 7+-Geräte)

5 Nun, da die AirPlay-Ziel-Whitelist festgelegt ist, verwenden Sie für überwachte iOS 7+-Geräte die Gerätesystemsteuerung, um AirPlay manuell zu aktivieren oder zu deaktivieren.

   a Navigieren Sie zu **Geräte > Listenansicht**, ermitteln Sie den Standort des Geräts für AirPlay und wählen Sie den Anzeigenamen des Geräts.

   b Wählen Sie **Support** und **AirPlay starten** aus der Liste der Support-Funktionen.

c Wählen Sie das **Ziel**, das im AirPlay-Profil erstellt wurde, geben Sie erforderlichenfalls das **Kennwort** ein, und wählen Sie die **Scanzeit**. Optional wählen Sie **Benutzerdefiniert** aus der Zielliste, um ein benutzerdefiniertes Ziel für dieses bestimmte Gerät zu erstellen.

d Wählen Sie **Speichern** und akzeptieren Sie die Eingabeaufforderung, um AirPlay zu aktivieren.

6 Um AirPlay auf dem Gerät manuell zu deaktivieren, kehren Sie zur Systemsteuerung des Geräts zurück, wählen Sie **Support** und dann **AirPlay beenden**.

Konfigurieren des AirPrint-Profils

Konfigurieren Sie eine AirPrint-Nutzlast für ein Apple-Gerät, sodass Computer einen AirPrint-Drucker automatisch erkennen – sogar dann, wenn sich das Gerät in einem anderen Subnetz befindet als der AirPrint-Drucker.

Verfahren

1 Gehen Sie zu **Ressourcen** >**Profile und Baselines** >**Profile** >**Listenansicht** >**Hinzufügen** und fügen Sie dann die geeignete Plattform hinzu. Wenn Sie Apple macOS auswählen, entscheiden Sie auch, ob dieses Profil nur auf den Registrierungsbenutzer auf dem Gerät (**Benutzerprofil**) oder auf das gesamte Gerät (**Geräteprofil**) angewendet wird.

2 Konfigurieren Sie die Einstellungen des Profils unter **Allgemein**.

3 Wählen Sie die Registerkarte **AirPrint**-Nutzlast.

Einstellung	Beschreibung
IP-Adresse	Geben Sie die IP-Adresse ein (XXX.XXX.XXX.XXX).
Ressourcenpfad	Geben Sie den dem AirPrint-Drucker zugeordneten Ressourcenpfad (z.B. ipp/printer oder printers/Canon_MG5300_series) ein. Informationen zum Auffinden des Ressourcenpfads und der IP-Adressinformationen eines Druckers finden Sie im Abschnitt Abrufen von AirPrint-Druckerinformationen.

4 Wählen Sie **Speichern und veröffentlichen**.

Abrufen von AirPrint-Druckerinformationen

Führen Sie die in diesem Abschnitt erwähnten Schritte aus, um die Informationen des AirPrint-Druckers zu ermitteln, wie IP-Adresse und Ressourcenpfad.

1 Verbinden Sie ein iOS-Gerät mit dem lokalen Netzwerk (Subnetz), in dem sich die AirPrint-Drucker befinden.

2 Öffnen Sie das Terminal-Fenster (unter /Programme/Dienstprogramme/), geben Sie den folgenden Befehl ein, und drücken Sie die Eingabetaste.

```
ippfind
```

Hinweis Notieren Sie sich die Druckerinformationen, die über den Befehl abgerufen werden. Der erste Teil ist der Name Ihres Druckers, und der letzte Teil ist der Ressourcenpfad.

```
ipp://myprinter.local.:XXX/ipp/portX
```

3 Geben Sie zum Abrufen der IP-Adresse den folgenden Befehl und den Namen Ihres Druckers ein.

```
ping myprinter.local.
```

Hinweis Notieren Sie sich die IP-Adressinformationen, die über den Befehl abgerufen werden.

```
PING myprinter.local (XX.XX.XX.XX)
```

4 Geben Sie die IP-Adresse (XX.XX.XX.XX) und den Ressourcenpfad (/ipp/portX), die aus den Schritten 2 und 3 abgerufen wurden, in den AirPrint-Nutzlasteinstellungen ein.

Konfigurieren eines Profils für Mobilfunkeinstellungen

Erstellen Sie eine Mobilfunknetz-Nutzlast, um Mobilfunknetzeinstellungen auf Geräten zu konfigurieren und festzulegen, wie Ihr Gerät auf Daten im Mobilfunknetz Ihres Mobilfunkanbieters zugreift.

Übertragen Sie diese Nutzlast, um einen anderen APN vom Standardpunkt aus zu verwenden. Bei falschen APN-Einstellungen verlieren Sie möglicherweise Funktionalität. Fragen Sie bei Ihrem Betreiber nach, welche APN-Einstellungen Sie verwenden können. Weiterführende Informationen zu Einstellungen für Mobilfunkgeräte finden Sie im Artikel aus der Apple-Wissensdatenbank.

Verfahren

1 Gehen Sie zur Seite **Ressourcen** > **Profile und Baselines** > **Profile** und wählen Sie **Hinzufügen**. Wählen Sie **Apple iOS**.

2 Konfigurieren Sie die Einstellungen des Profils unter **Allgemein**.

3 Wählen Sie eine **Mobilfunknetz**-Nutzlast für Geräte, die iOS 7 oder höher verwenden.

4 Konfigurieren Sie die Einstellungen für die Mobilfunknetz-Nutzlast.

Einstellung	Beschreibung
Zugriffspunktname (APN)	Geben Sie den APN ein, den Sie von Ihrem Mobilfunkanbieter erhalten haben. (Beispiel: come.moto.mobilfunknetz)
Authentifizierungstyp	Wählen Sie das Authentifizierungsprotokoll.
Zugriffspunktbenutzername	Geben Sie den Benutzernamen ein, der für die Authentifizierung verwendet wird.
Kennwort des Zugriffpunkts	Geben Sie das APN-Kennwort ein, das für die Authentifizierung verwendet wird.
Name des Zugriffspunkts	Geben Sie den APN ein, den Sie von Ihrem Mobilfunkanbieter erhalten haben. (Beispiel: come.moto.mobilfunknetz)
Zugriffspunktbenutzername	Geben Sie den Benutzernamen ein, der für die Authentifizierung verwendet wird.
Authentifizierungstyp	Wählen Sie das Authentifizierungsprotokoll.
Kennwort	Geben Sie das APN-Kennwort ein, das für die Authentifizierung verwendet wird.
Proxy-Server	Geben Sie die Proxyserver-Details ein.
Proxyserver Port	Geben Sie den Proxyserver-Port für alle Verbindungen ein. Wählen Sie **Hinzufügen**, um diesen Prozess fortzusetzen.

5 Wählen Sie **Speichern und veröffentlichen**.

Konfigurieren eines Layout-Profils für die Startseite (iOS überwacht)

Verwenden Sie diese Nutzlast, um die Startseite zu konfigurieren. Wenn Sie diese Funktion aktivieren, können Sie Anwendungen je nach Ihren organisatorischen Bedürfnissen gruppieren.

Beim Einlesen der Nutzlast in das Gerät wird die Startseite gesperrt, sodass die Benutzer ihre persönliche Konfiguration nicht ändern können. Diese Nutzlast ist auf überwachte Geräte unter iOS 9.3 + anzuwenden.

Verfahren

1 Gehen Sie zu **Ressourcen** > **Profile und Baselines** > **Profile** > **Listenansicht** > **Hinzufügen**. Wählen Sie **Apple iOS**.

2 Konfigurieren Sie die Einstellungen des Profils unter **Allgemein**.

3 Wählen Sie die Nutzlast **Startseiten-Layout** aus der Liste.

Einstellung	Beschreibung
Dock	Wählen Sie, welche Anwendungen im Dock erscheinen sollen.
Seite	Wählen Sie, welche Anwendungen Sie dem Gerät hinzufügen möchten. Sie können weitere Seiten einfügen, um mehr Anwendungsgruppen einzurichten.
Ordner hinzufügen	Konfigurieren Sie einen neuen Ordner, um ihn auf der ausgewählten Seite dem Gerätebildschirm hinzuzufügen. ■ Verwenden Sie das **Stiftsymbol** in der grauen Leiste, um den Namen des Ordners zu erstellen oder zu bearbeiten.

4 Wählen Sie **Seite hinzufügen**, um gegebenenfalls dem Gerät weitere Seiten hinzuzufügen.

5 Wählen Sie **Speichern und veröffentlichen**, um dieses Profil per Push auf die Geräte zu übertragen.

Erstellen eines Meldungsprofils für den Sperrbildschirm

Passen Sie den Sperrbildschirm der Endbenutzer-Geräte mit Informationen an, die Ihnen dabei helfen können, verloren gegangene Geräte zu finden.

Verfahren

1 Gehen Sie zu **Ressourcen** > **Profile und Baselines** > **Profile** und wählen Sie **Hinzufügen**. Wählen Sie **Apple iOS**.

2 Konfigurieren Sie die Profileinstellungen **Allgemein**.

3 Konfigurieren Sie die Meldung für den Sperrbildschirm:

Einstellung	Beschreibung
Nachricht für „Falls verloren, bitte an folgende Adresse senden“	Zeigen Sie einen Namen oder eine Organisation an, an die ein gefundenes Gerät zurückgegeben werden sollte. Dieses Feld unterstützt Nachschlagewerte.
Anlagen-Tag-Information	Zeigen Sie die Bestandskennzeicheninformationen des Geräts auf dem Sperrbildschirm des Geräts an. Dieses Bestandskennzeichen kann ein physisches Bestandskennzeichen, das sich auf dem Gerät befindet, duplizieren oder ersetzen. Dieses Feld unterstützt Nachschlagewerte.

4 Wählen Sie **Speichern und veröffentlichen**.

Konfigurieren eines Support-Profils für ein Google-Konto (iOS)

Damit ermöglichen Sie es einem Endanwender, sein Google-Konto über seine systemeigene E-Mail-Anwendung auf seinem iOS-Gerät zu nutzen. Fügen Sie ein Google-Konto direkt über die UEM-Konsole hinzu.

Verfahren

1 Gehen Sie zu **Ressourcen** > **Profile und Baselines** > **Profile** >**Hinzufügen**. Wählen Sie **Apple iOS** als Plattform aus.

2 Konfigurieren Sie die Einstellungen des Profils unter **Allgemein**.

3 Konfigurieren Sie die Kontoinformationen des Benutzers:

Einstellung	Beschreibung
Kontoname	Geben Sie den vollständigen Benutzernamen für das Google-Konto ein. Dies ist der Benutzername, der erscheint, wenn Sie eine E-Mail-Nachricht versenden.
Kontobeschreibung	Geben Sie eine Beschreibung für das Google-Konto ein, die in E-Mail-Nachrichten und den Einstellungen angezeigt wird.
E-Mail-Adresse	Geben Sie die vollständige Google E-Mail-Adresse für das Konto ein.
Standard-App für Audio-Anrufe	Wählen Sie eine Anwendung aus, die als Standardanwendung für Anrufe aus dem konfigurierten Google-Konto verwendet wird.

4 Wählen Sie **Speichern und veröffentlichen**.

Konfigurieren eines Profils mit benutzerdefinierten Einstellungen

Die Nutzlast **Benutzerdefinierte Einstellungen** kann verwendet werden, wenn Apple neue iOS-Funktionalität oder -Funktionen freigibt, die Workspace ONE UEM momentan nicht durch systemeigene Nutzlasten unterstützt. Falls Sie auf die aktuellste Workspace ONE UEM-Version warten möchten, um diese Einstellungen zu kontrollieren, können Sie die Nutzlast der **benutzerdefinierten Einstellungen** und XML-Code verwenden, um bestimmte Einstellungen manuell zu aktivieren oder zu deaktivieren.

Voraussetzungen

- Sie können an einer Kopie Ihres Profils arbeiten und sie unter einer „Test“-Organisationsgruppe speichern, um zu vermeiden, dass Benutzer beeinflusst werden, bevor Sie zum Speichern und Veröffentlichen bereit sind.
- Weisen Sie Smartgroups keine Profile zu, da dies beim Anzeigen von XML einen verschlüsselten Wert geben könnte.

Verfahren

1 Gehen Sie zu **Ressourcen** >**Profile Und Baselines**> **Profile** > **Hinzufügen.** > **Profil hinzufügen** > **iOS**.

2 Konfigurieren Sie die Einstellungen des Profils unter **Allgemein**.

3 Konfigurieren Sie die entsprechende Nutzlast (z.B. Restriktionen oder Kennung).

4 Klicken Sie auf **Speichern und veröffentlichen**.

Hinweis Stellen Sie sicher, dass das in den Schritten 1–4 erstellte-Profile keiner Smartgroup zugewiesen ist. Andernfalls können die Daten beim Anzeigen von XML verschlüsselt sein.

5 Navigieren Sie zurück zur Seite „Profile“ und wählen Sie mit dem Optionsfeld neben dem Profilnamen ein Profil aus. Die Menüoptionen werden oberhalb der Liste angezeigt.

6 Wählen Sie **</> XML** aus den Menüoptionen. Ein Dialogfeld **XML-Profil anzeigen** wird angezeigt.

7 Finden und kopieren Sie den Abschnitt des von Ihnen zuvor konfigurierten Texts, der mit <dict> ... </dict> anfängt, zum Beispiel "Restriktionen" oder "Passcode". Dieser Text enthält einen Konfigurationstyp, der dessen Zweck identifiziert, zum Beispiel "Restriktionen". Sie müssen einen einzelnen Wörterbuchinhalt innerhalb des PayloadContent kopieren, wie im Beispiel gezeigt.

```
<plist version="1.0">
  <dict>
    <key>PayloadContent</key>
    <array>
      <dict>
        <key>safariAcceptCookies</key>
        <real>2</real>
        <key>safariAllowAutoFill</key>
        <true />
        <key>PayloadDisplayName</key>
        <string>Restrictions</string>
        <key>PayloadDescription</key>
        <string>RestrictionSettings</string>
        <key>PayloadIdentifier</key>
        <string>745714ad-e006-463d-8bc1-495fc99809d5.Restrictions</string>
        <key>PayloadOrganization</key>
        <string></string>
        <key>PayloadType</key>
        <string>com.apple.applicationaccess</string>
        <key>PayloadUUID</key>
        <string>9dd56416-dc94-4904-b60a-5518ae05ccde</string>
        <key>PayloadVersion</key>
        <integer>1</integer>
      </dict>
    </array>
    <key>PayloadDescription</key>
    <string></string>
    <key>PayloadDisplayName</key>
    <string>Block Camera/V_1</string>
    <key>PayloadIdentifier</key>
    <string>745714ad-e006-463d-8bc1-495fc99809d5</string>
    <key>PayloadOrganization</key>
    <string></string>
    <key>PayloadRemovalDisallowed</key>
    <false />
    <key>PayloadType</key>
```

```
    <string>Configuration</string>
    <key>PayloadUUID</key>
    <string>86a02489-58ff-44ff-8cd0-faad7942f64a</string>
    <key>PayloadVersion</key>
    <integer>1</integer>
  </dict>
</plist>
```

Weitere Beispiele und Informationen zum XML-Code finden Sie im KB-Artikel: https://support.workspaceone.com/articles/115012790248.

8 Wenn Sie verschlüsselten Text zwischen dict-Tags im XML-Fenster sehen, können Sie den entschlüsselten Text generieren, indem Sie die Einstellungen auf der Seite „Profile“ ändern. Dazu gehen Sie wie folgt vor:

   a Navigieren Sie zu **Gruppen & Einstellungen** > **Alle Einstellungen** > **Geräte** > **Benutzer** > **Apple** > **Profile**.

   b Überschreiben Sie die Option für benutzerdefinierte Einstellungen.

   c Deaktivieren Sie die Option „Profile verschlüsseln“ und speichern Sie dann.

9 Navigieren Sie zurück zu **Benutzerdefinierte Einstellungen** und fügen Sie in das Textfeld den zuvor kopierten XML-Code ein. Der hinzugefügte XML-Code sollte den vollständigen Code-Block enthalten, von <dict> bis </dict>.

10 Entfernen Sie die konfigurierte originale Nutzlast, indem Sie den unteren Nutzlastenabschnitt auswählen, beispielsweise „Restriktionen“ oder „Kennung“, und auf die Schaltfläche „Minus“ [-] klicken. Sie können jetzt das Profil aufwerten, indem Sie für die neue Funktionalität einen benutzerdefinierten XML-Code hinzufügen.

11 Klicken Sie auf **Speichern und veröffentlichen**.

Konformitätsrichtlinien

4

Die Compliance Engine ist ein automatisches Tool von Workspace ONE UEM powered by AirWatch, welches sicherstellt, dass alle Geräte Ihre Richtlinien erfüllen. Bei diesen Richtlinien kann es sich um grundlegende Sicherheitseinstellungen wie etwa das Vorhandensein einer Kennung und die Festlegung einer Mindestdauer für eine Gerätesperre handeln.

Auf bestimmten Plattformen möchten Sie eventuell spezielle Vorsichtsmaßnahmen festlegen und durchsetzen. Diese Vorsichtsmaßnahmen bestehen unter anderem aus der Festlegung einer Kennwortstärke, dem Hinzufügen bestimmter Anwendungen zu Blacklists und dem Einsatz von Eincheck-Intervallen für Geräte, um zu gewährleisten, dass die Geräte sicher und mit Workspace ONE UEM verbunden sind. Sobald festgestellt wird, dass Geräte den Konformitätsanforderungen nicht entsprechen, fordert die Compliance Engine die Benutzer zur Behandlung von Konformitätsfehlern auf, um disziplinarische Maßnahmen auf dem Gerät zu verhindern. Die Compliance Engine kann beispielsweise eine Nachricht auslösen, anhand derer der Benutzer benachrichtigt wird, dass sein Gerät nicht konform ist.

Darüber hinaus kann nicht konformen Geräten kein Geräteprofil zugewiesen und es können keine Anwendungen auf ihnen installiert werden. Sollten die Probleme im angegebenen Zeitraum nicht behoben werden, kann mit dem Gerät nicht mehr auf bestimmte Benutzerdefinierte Inhalte und Funktionen zugegriffen werden. Die verfügbaren Konformitätsrichtlinien und -aktionen variieren je nach Plattform.

Weitere Informationen zu Konformitätsrichtlinien und Unterstützung von Richtlinien und Aktionen für eine bestimmte Plattform finden Sie in der Dokumentation **Geräteverwaltung** unter docs.vmware.com.

Anwendungen für iOS

5

Kombinieren Sie Workspace ONE UEM MDM-Funktionen mit Workspace ONE UEM-Anwendungen, um die Sicherheit und Funktionalität noch weiter zu verbessern. Verwalten Sie problemlos Workspace ONE UEM-Anwendungen über den gesamten Lebenszyklus für Geräte im Eigentum der Mitarbeiter und des Unternehmens sowie Gemeinschaftsgeräte aus der UEM-Konsole.

Workspace ONE UEM-Anwendungen bieten Ihnen und Ihren Endbenutzern Folgendes:

- Erkunden Sie den VMware Workspace ONE Content zum Synchronisieren eines Ordners mit persönlichem Inhalt.
- Konfigurieren Sie VMware Workspace ONE Web für sichere Internetsuchen.
- Aktivieren Sie VMware Workspace ONE Boxer zur Konfiguration von E-Mail.
- Verwenden Sie AirWatch Container als Alternative zu MDM durch Trennung von Unternehmensdaten und privaten Daten auf einem Gerät bei vollumfänglichem Schutz der Privatsphäre des Benutzers.

Weiterführende Informationen über das Verwalten von Anwendungen finden Sie im Handbuch **Mobile Anwendungsverwaltung**.

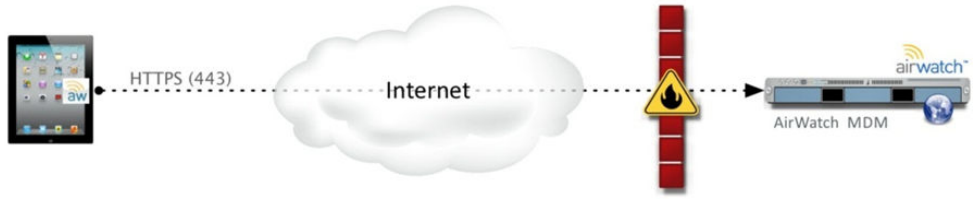
Dieses Kapitel enthält die folgenden Themen:

Workspace ONE Intelligent Hub für iOS

Der Workspace ONE Intelligent Hub für iOS erfasst Geräteinformationen und sendet sie an die UEM-Konsole. Da diese Informationen sensible Daten enthalten können, ergreift Workspace ONE

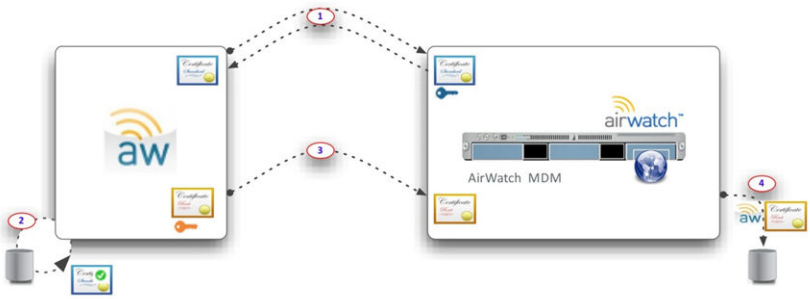
UEM umfangreiche Maßnahmen, um sicherzustellen, dass diese Daten verschlüsselt sind und von einer vertrauenswürdigen Quelle stammen.

Workspace ONE UEM nutzt ein eindeutiges Zertifikatspaar, um die Kommunikation zwischen Workspace ONE Intelligent Hub für iOS und dem Server zu signieren und zu verschlüsseln. Diese Zertifikate geben dem Server auch die Möglichkeit, die Identität und Echtheit aller in Workspace ONE UEM registrierten Geräte zu überprüfen. In dieser Übersicht werden die Vorteile und Erfordernisse beider Sicherheitserweiterungen genau aufgeführt.



Funktionsweise des Zertifikatsaustauschs

Bevor Daten übertragen werden, tauschen die Workspace ONE Intelligent Hub-Anwendung und der Server personalisierte Zertifikate aus. Diese Beziehung wird festgelegt, wenn sich Workspace ONE Intelligent Hub für iOS beim Workspace ONE UEM-Server während der Registrierung zum ersten Mal anmeldet.



1 Workspace ONE Intelligent Hub für iOS kommuniziert mit dem Workspace ONE UEM-Server, um den öffentlichen Schlüssel des Serverzertifikats abzurufen. Sowohl Workspace ONE Intelligent Hub für iOS als auch der Workspace ONE UEM-Server vertrauen dem öffentlichen Schlüssel des AirWatch-Stammzertifikats, das die Echtheit aller Zertifikate überprüft, die in den Datenaustausch zur Registrierung einbezogen werden.

2 Workspace ONE Intelligent Hub für iOS überprüft das Serverzertifikat mit dem Workspace ONE UEM-Stamm-ZS-Zertifikat.

3 Workspace ONE Intelligent Hub für iOS sendet einen eindeutigen öffentlichen Schlüssel des Zertifikats an den Workspace ONE UEM-Server.

4 Der Workspace ONE UEM-Server verknüpft das Zertifikat von Workspace ONE Intelligent Hub mit diesem Gerät in der Datenbank.

Sichern von Daten bei der Übertragung

Nach einem erstmaligen Austausch von Zertifikaten werden alle Daten, die an die UEM-Konsole gesendet werden, ab diesem Zeitpunkt verschlüsselt. In der folgenden Tabelle sehen Sie die beiden betroffenen Zertifikate und ihre Aufgaben bei der Transaktion.

	Hub-Zertifikat	Serverzertifikat
Workspace ONE Intelligent Hub	Signieren der Daten	Verschlüsselung der Daten
Workspace ONE UEM-Server	Überprüfung des Datenursprungs	Entschlüsselung der Daten

APIs und Anwendungsfunktionen

Es gibt zwei Kategorien von APIs, die Workspace ONE UEM auf iOS-Geräten als Verwaltungs- und Nachverfolgungsfunktionen nutzt:

- **OTA-MDM-APIs (Over-the-Air)** werden mit der Registrierungsmethode aktiviert, unabhängig davon, ob Workspace ONE Intelligent Hub für iOS verwendet wird.
- **Systemeigene iOS-SDK-APIs** stehen allen Drittanbieter-Anwendungen zur Verfügung, einschließlich der Workspace ONE Intelligent Hub-Anwendungen und anderer Anwendungen, die das Workspace ONE UEM Software Development Kit (SDK) verwenden.

Workspace ONE Intelligent Hub für iOS fungiert als Broker-Anwendung, die in die systemeigene Verwaltungsschicht iOS SDK API integriert ist. Wenn Workspace ONE Intelligent Hub für iOS in Kombination mit Workspace ONE UEM SDK für iOS genutzt wird, können Administratoren die Vorteile weiterer MDM-Funktionen für Anwendungen nutzen, die über das hinausgehen, was in der Over-the-Air (OTA) MDM API-Schicht angeboten wird.

Konfigurieren der Workspace ONE Intelligent Hub-Einstellungen für iOS-Geräte

Sie können die Workspace ONE Intelligent Hub-Einstellungen in der UEM-Konsole anpassen. Sie können beispielsweise ein SDK-Profil angeben, das mit Workspace ONE Intelligent Hub zur Nutzung von Workspace ONE UEM-Funktionen verwendet wird.

Verfahren

1 Navigieren Sie zu **Geräte > Geräteeinstellungen > Apple > Apple iOS > Hub-Einstellungen**.

2 Konfigurieren Sie die folgenden Einstellungen für den Workspace ONE Intelligent Hub:

Tabelle 5-1. Allgemein

Einstellung	Beschreibung
Aufhebung der Registrierung in Hub deaktivieren	Diese Einstellung deaktiviert die Fähigkeit des Benutzers, seine Registrierung bei Workspace ONE UEM MDM über den Workspace ONE Intelligent Hub aufzuheben. Diese Einstellung ist nur in Workspace ONE Intelligent Hub v4.9.2 und höher verfügbar.
Anwendung im Hintergrund aktualisieren	Diese Einstellung teilt Workspace ONE Intelligent Hub das maximal zulässige Zeitintervall für die Aktualisierung des App-Inhalts mit. Einige Anwendungen laufen über eine kurze Zeitperiode, bevor sie in den angehaltenen Status wechseln. „Anwendung im Hintergrund aktualisieren“ ist eine Funktion in iOS, mit der die Anwendung selbst aus ihrem angehaltenen Status wieder aktiv wird. Während dieser Aktualisierung übermittelt Workspace ONE Intelligent Hub Informationen wie Gefahrenerkennung, Hardwaredetails, GPS, iBeacon und Telekommunikation an die UEM-Konsole. Die Frequenz, mit der der Workspace ONE Intelligent Hub aktualisiert, wird durch das Betriebssystem gesteuert und nur wenn das Gerät an eine Stromquelle angeschlossen wird, eine bestimmte Häufigkeit der Nutzung vorliegt oder eine Verbindung mit einem WLAN erfolgt. Um die Funktion „Anwendung im Hintergrund aktualisieren“ nutzen zu können, muss diese Einstellung in der UEM-Konsole aktiviert sein, kann Workspace ONE Intelligent Hub auf dem Gerät nicht heruntergefahren werden und muss die Funktion „Anwendung im Hintergrund aktualisieren“ auf dem Gerät für den Workspace ONE Intelligent Hub unter **Einstellungen > Allgemein > Anwendung im Hintergrund aktualisieren** aktiviert sein.
Minimales Aktualisierungsintervall	Wählen Sie die Mindestzeit, die verstreichen muss, bevor das Gerät versucht, den App-Inhalt zu aktualisieren.
Nur über WLAN übertragen	Aktivieren Sie die Hintergrundaktualisierung nur über WLAN-Verbindungen.

3 Passen Sie die folgenden zusätzlichen Workspace ONE Intelligent Hub-Konfigurationen wie in diesem Leitfaden beschrieben in der UEM-Konsole auf der Seite **Einstellungen und Richtlinien** für Erzwingen von Kennungen für Single-Sign-On auf Anwendungsebene an.

Nächste Schritte

Weiterführende Informationen zu Offline-Zugang, Branding sowie sonstigen Einstellungen und Richtlinien finden Sie im **Leitfaden für VMware AirWatch Mobile Application Management** .

Workspace ONE Intelligent Hub Mobile Application für iOS

Nach der Registrierung des Workspace ONE Intelligent Hub wechselt die Anwendung standardmäßig zum Bildschirm **Mein Gerät**. Hier sehen Sie Echtzeitinformationen über Ihr Gerät, synchronisieren das Gerät, registrieren das Gerät erneut und lesen Nachrichten, die von der UEM-Konsole gesendet wurden.

Das Kontrollkästchen **Self-Service aktiviert** muss unter **Hub-Einstellungen** in der UEM-Konsole ausgewählt sein, damit alle Statusinformationen angezeigt werden.

Hinweis Wenn die Option **Hub-Registrierung aufheben** unter **Hub-Einstellungen** nicht aktiviert ist, wählen Sie **Geräteregistrierung aufheben**, bevor Sie die Registrierung bei Workspace ONE Intelligent Hub v4.9.2 erneut vornehmen.

Funktionen für „Meine Geräte“

- Tippen Sie auf das **Status**-Menü, um den Status und Optionen für Self-Service-Diagnosen anzuzeigen.
  - **Gerät synchronisieren** – Tippen Sie auf diese Aktion, um eine Anforderung zur erneuten Synchronisierung des Geräts mit der UEM-Konsole abzusenden.
  - **Aktueller Status** – Verwenden Sie die Menüs, um Informationen über die Registrierung, die erneute Registrierung von Geräten, die Anzeige von Konten und die Konformität zu finden.
  - **Diagnose** – Verwenden Sie diese Menüs, um die Konnektivität zu testen, den Internetzugang anzuzeigen, Probleme mit der Konnektivität zu erkennen, Serverinformationen anzuzeigen sowie Hub- und Geräte-Protokolle anzuzeigen und zu senden.
- Tippen Sie auf das Menü **Gerätedetails**, um verschiedene Statusoptionen anzuzeigen:
  - **Netzwerk** – Hier können Sie Netzwerkadapter und IP-Adressen anzeigen.
  - **Erweitert** – Verwenden Sie diese Menüs, um Informationen über den Akku, den Arbeitsspeicher und den Festplattenspeicher des Geräts anzuzeigen.
  - **Standort** – Hiermit zeigen Sie die GPS-Koordinaten Ihres Geräts für den laufenden und frühere Zeiträume an.
  - **iBeacon** – Damit zeigen Sie den Namen der iBeacon-Region an. Wenn iBeacon konfiguriert ist, aber Standortdaten nicht konfiguriert wurden, zeigt das Gerät nur den iBeacon-Bereich an. Wenn iBeacon- und Standortdaten aktiviert sind, zeigt das Gerät den iBeacon-Bereich und die Karte mit dem Standort des Geräts an.
- Verwenden Sie das **Dock** unten auf dem Bildschirm, um zusätzliche Informationen anzuzeigen:
  - **Nachrichten** – Lesen Sie Benachrichtigungen von der UEM-Konsole. Sie erhalten zum Beispiel möglicherweise Nachrichten im Message-Center, die Sie auffordern, die Konformität zu überprüfen, um zu gewährleisten, dass Ihr Gerät erfolgreich überwacht werden kann.
  - **Info** – Mithilfe dieser Option werden Informationen über die Workspace ONE Intelligent Hub-Anwendung sowie Rechtsvermerke angezeigt.

VMware Workspace ONE Content

VMware Workspace ONE Content ist eine App, die Endbenutzern den Zugriff auf wichtige Inhalte auf ihren Geräten ermöglicht und dabei Ihrer Organisation den Schutz von Dateien gewährleistet.

Endbenutzer können in die UEM-Konsole hochgeladene Inhalte, Inhalte von synchronisierten Unternehmens-Repositorys sowie ihre eigenen persönlichen Inhalte in Workspace ONE Content öffnen.

Verwenden Sie die UEM-Konsole, um Inhalte hinzuzufügen, Repositorys zu synchronisieren und die Aktionen zu konfigurieren, die Endbenutzer für die in der Anwendung geöffneten Inhalte ausführen können. Diese Konfigurationen verhindern, dass Inhalte ohne Genehmigung kopiert, freigegeben oder gespeichert werden.

Weitere Informationen zu MCM und zur Konfiguration von VMware Workspace ONE Content finden Sie im **Leitfaden für VMware Workspace ONE UEM Mobile Content Management**.

VMware Workspace ONE Web

VMware Workspace ONE Web ist eine Anwendung, die eine verwaltbare und sichere Alternative für systemeigene Webbrowser bietet. Sie ermöglicht das sichere Surfen auf Anwendungs-, Tunnel- und Website-Ebene.

Sie können Workspace ONE Web an spezielle Geschäftsanforderungen anpassen, indem Sie den Webzugriff auf Websites beschränken und ein sicheres Internetportal für mobile Point-of-Sale-Geräte bereitstellen. Bieten Sie Benutzern eine standardmäßige Surferfahrung, einschließlich Unterstützung für Browsen mit mehreren Registerkarten und JavaScript-Dialogfelder. Zur maximalen Sicherheit auf Ihren Android- und iOS-Geräten empfehlen wir den Einsatz von Workspace ONE Web mit dem Restriktionsprofil, das den systemeigenen Browser blockiert.

Weitere Informationen darüber, wie Sie Workspace ONE Web für den Einsatz vorbereiten und konfigurieren, finden Sie im **VMware Workspace ONE Web Admin Guide**.

VMware Workspace ONE Boxer

VMware Workspace ONE Boxer ist eine E-Mail-Anwendung, die nutzerorientierte mobile Produktivität mit Unternehmenssicherheit in Form von AES-256-Bit-Verschlüsselung bietet. Diese Anwendung containerisiert Geschäftsdaten von persönlichen Daten und bietet dabei reibungslosen Zugriff auf Unternehmens-E-Mails, -kalender und -kontakte im Besitz des Unternehmens und der Mitarbeiter.

Workspace ONE Boxer lässt sich an individuelle Bedürfnisse anpassen, zum Beispiel mit benutzerdefinierten Wischgesten, Kontaktavataren, individualisierbaren Smartordnern und verschiedenen Kontofarben. Die All-in-One-Anwendung für E-Mail, Kalender und Kontakte bietet ein intuitives Benutzererlebnis im Einklang mit den systemeigenen Designvorgaben von Geräten.

Weitere Informationen zu VMware Workspace ONE Boxer finden Sie im *VMware Workspace ONE Boxer Admin Guide*.

AirWatch Container für iOS

AirWatch Container bietet einen flexiblen Ansatz für Bring Your Own Device-Management (BYOD), wobei ein sicherer Arbeitsbereich auf ein persönliches Gerät übertragen wird. Unternehmen können für die Mitarbeiter Workspace ONE UEM-Anwendungen und interne Anwendungen an AirWatch Container zur Verwendung auf ihren Mobilgeräten verteilen.

Anwendungen sind innerhalb und außerhalb von AirWatch Container sichtbar. Die Unternehmensanwendungen werden durch einen gemeinsamen SDK-Framework und eine Containerkennung geschützt. Diese Anwendungen können durch Single Sign-On-Authentifizierung nahtlos interagieren und sich mit dem Internet durch ein App-Tunnel-VPN sicher verbinden.

Weitere Informationen zum AirWatch Container finden Sie im **VMware AirWatch Container Admin Guide**.

Erzwingen von Kennungen für Single-Sign-On auf Anwendungsebene

Mit Single Sign-On (SSO) können Endbenutzer auf Workspace ONE UEM-Anwendungen, umhüllte Anwendungen und SDK-fähige Anwendungen zugreifen, ohne Anmeldedaten für jede Anwendung eingeben zu müssen. Durch Nutzung von Workspace ONE Intelligent Hub oder AirWatch Container als „Broker-Anwendung“ wird es Endbenutzern ermöglicht, sich einmal pro Sitzung mit ihren normalen Anmeldedaten oder eine SSO-Kennung zu authentifizieren.

Aktivieren Sie SSO als Teil der **Sicherheitsrichtlinien**, die Sie für alle Workspace ONE UEM-Anwendungen, umhüllten Anwendungen und SDK-aktivierten Anwendungen mit einem Standard-SDK-Profil konfigurieren.

Verfahren

1. Navigieren Sie zu **Gruppen und Einstellungen > Alle Einstellungen > Anwendungen > Einstellungen und Richtlinien > Sicherheitsrichtlinien**.
2. Setzen Sie **Single Sign-On** auf **Aktiviert**, um Endbenutzern den Zugriff auf alle Workspace ONE UEM-Anwendungen und eine beständige Anmeldung zu ermöglichen.
3. (Optional) Legen Sie den **Authentifizierungstyp** auf **Kennung** und den **Kennungsmodus** auf **Numerisch** oder **Alphanumerisch** fest, um eine SSO-Kennung auf dem Gerät durchzusetzen. Wenn Sie SSO, aber keinen Authentifizierungstyp aktivieren, verwenden die Endbenutzer ihre regulären Anmeldedaten (entweder Verzeichnisdienst- oder Workspace ONE UEM-Konto), um sich zu authentifizieren. Es gibt dann keine SSO-Kennung.

Ergebnisse

Sobald sich ein Benutzer über eine an SSO teilnehmende Anwendung authentifiziert hat, wurde eine Sitzung eröffnet. Diese Sitzung bleibt aktiv, bis das im SDK-Profil gesetzte **Authentifizierungs-Timeout** erreicht wurde oder der Benutzer die Anwendung manuell sperrt.

Überblick über Apple Configurator

Workspace ONE UEM und Apple Configurator sind integrierbar, und daher können Sie skalierte Bereitstellungen von Apple iOS-Geräten überwachen und verwalten. Administratoren können Konfigurationsprofile erstellen, vorhandene Profile vom iPhone-Konfigurationsprogramm importieren, Versionen von bestimmten Betriebssystemen installieren und iOS-Gerätesicherheitsrichtlinien erzwingen.

Installieren Sie Apple Configurator 2 von einem macOS-Notebook und führen Sie das Programm aus, um die Integration in die Workspace ONE UEM-Konsole vorzunehmen und damit ein oder mehr Geräte gleichzeitig zu überwachen und zu konfigurieren.

- Installieren Sie das Workspace ONE UEM-Profil als Teil der Konfiguration, um Geräte unbeaufsichtigt zu registrieren.
- Überwachen Sie für Ihre Branche dedizierte Geräte, welche von verschiedenen Benutzern gemeinsam verwendet werden.
- Erstellen Sie Konfigurationsprofile zum Ändern der Geräteeinstellungen für WLAN-Netzwerke, Vorkonfigurationen von E-Mail, Microsoft Exchange-Einstellungen und mehr.
- Verteilen Sie öffentliche Anwendungen mit dem Configurator, ohne eine Apple ID in das Gerät einzugeben.
- Erstellen Sie Blueprints zur Automatisierung des Gerätemanagements. Verwenden Sie Blueprints als Vorlagen, um Profile und Anwendungen zu konfigurieren sowie im Handumdrehen per Push auf Geräte zu übertragen.
- Fügen Sie die Überwachung zu Geräten hinzu und nutzen Sie den Vorteil von noch mehr Managementfunktionen wie Anzeigen oder Ausblenden von Anwendungen, Ändern des Gerätenamens, Hintergrundbilder, Kennungen, Tastenkürzel und mehr.
- Sichern Sie Benutzereinstellungen und Anwendungsdaten, einschließlich neuer benutzererstellter Daten, mit dem Configurator.

Apple Configurator 2 funktioniert auch mit dem Apple Device Enrollment Program (DEP) zur Automatisierung der Registrierung mit Mobile Device Management (MDM) und dem Volume Purchase Program (VPP) durch Zuordnung verwalteter Lizenzanwendungen zu Geräten.

Eine vollständige Liste der für überwachte und nicht überwachte Geräte verfügbaren Funktionen finden Sie im Kapitel 10 iOS-Funktionalität: „Überwacht“ im Vergleich zu „Nicht überwacht“.

Informationen zum Registrieren von iOS-Geräten mit Apple Configurator finden Sie unter Mehrere iOS-Geräte mit Apple Configurator gleichzeitig registrieren und **Integration in Apple Configurator**.

Hochladen eines signierten Apple Configurator-Profils auf die UEM-Konsole

Sie können ein signiertes Profil vom Apple Configurator (oder IPCU) direkt zur UEM-Konsole exportieren.

Verfahren

1 Konfigurieren Sie Überwachungs- und Verwaltungseinstellungen in Apple Configurator (oder IPCU).

2 Exportieren und speichern Sie das neu erstellte Profil in einem leicht zugänglichen Ort in Ihrem Computer.

3 Gehen Sie in der UEM-Konsole zu **Ressourcen** > **Profile und Baselines** > **Profile** und wählen Sie **Hochladen**.

4 Geben Sie die Gruppe **Verwaltet von** ein und wählen Sie **Hochladen**, um das von Apple Configurator (oder IPCU) exportierte Profil zu suchen und hochzuladen. Klicken Sie auf **Weiter**.

5 Geben Sie eine allgemeine Profilbeschreibung ein, einschließlich Name, Beschreibung und zugewiesenen Organisationsgruppen.

6 Klicken Sie auf **Speichern und veröffentlichen**, um das Profil an die zugewiesenen Geräte zu senden.

iOS-Gerätekonfigurationen

6

Workspace ONE UEM unterstützt Sie bei der Konfiguration von wichtigen Elementen zur Verwaltung der Nutzererfahrung mit Endgeräten, damit Sie die Ziele Ihres Unternehmens umsetzen können. Die in diesem Abschnitt beschriebenen Funktionen umfassen detaillierte Beschreibungen der Schnittstelle und der Nutzererfahrung mit Ihren verwalteten Geräten.

Diese Konfigurationen sind oft nur bei bestimmten Einsatztypen verfügbar, beispielsweise Apple DEP-Einsätze oder Apple School Manager-Einsätze.

Dieses Kapitel enthält die folgenden Themen:

Apple-Branchenvorlagen

Wählen Sie Branchenvorlagen, um das Verfahren für den Einsatz zu beschleunigen.

Apple-Branchenvorlagen bündeln automatisch empfohlene mobile Anwendungen, Profile und Konformitätsrichtlinien, damit sie gleichzeitig an die erforderliche Organisationsgruppe übermittelt werden können.

- Auf der UEM-Konsole V8.2.2 sind als Branchenvorlagen Gesundheitswesen und Einzelhandel verfügbar.

- Auf der UEM-Konsole V8.3+ sind als Branchenvorlagen Gesundheitswesen, Einzelhandel, Bildung, Gastgewerbe und Außendienst verfügbar.

Typen von Vorlagen

Verwenden Sie die folgende Tabelle, um zu ermitteln, welche Art von Vorlage und Initiative am besten zu der mobilen Konfiguration passt, die Sie benötigen. Jede Vorlage enthält empfohlene Anwendungen und Sicherheitsrichtlinien basierend auf Untersuchungen von Experten, Branchenstandards und bewährten Verfahren.

Branche	Initiative	Beschreibung
Gesundheitswesen	Klinische Zusammenarbeit	Bereitstellung rechtzeitiger Kommunikation für Mitarbeiter im Gesundheitswesen und Patienten, um sicherzustellen, dass eine optimale Pflege ohne Kompromisse bei der Sicherheit gewährleistet ist. (UEM-Konsole v8.2.2+)
Mobile klinische Workflows	Ärzte, Krankenpflegepersonal, Apotheker und andere Fachleute können Kommunikation in Echtzeit verwenden, um Patienten zu versorgen, die zu Hause oder in einer anderen medizinischen Einrichtung gepflegt werden. (UEM-Konsole v8.2.2+)	
Patientenversorgung	Mithilfe von iPads und mobilen Anwendungen für eine bessere Patientenversorgung verbessern Sie das Therapieergebnis und die Zufriedenheit der Patienten. (UEM-Konsole v8.2.2+)	
Education	Digitales Klassenzimmer	iPads und mobile Anwendungen werden für die Kommunikation von Lehrkräften, Schülern und Eltern für Schulaufgaben, das Verhalten der Schüler und andere Einsätze verwendet. (UEM-Konsole v8.3+)
Freude am Lernen bereiten	Mit digitalem Lernen und digitaler Zusammenarbeit wecken Sie das Interesse der Studierenden und fördern ihre Konzentration. (UEM-Konsole v8.3+)	
Mobile Registrierkasse	Versetzen Sie Mitarbeiter in die Lage, an jedem beliebigen Standort zu verkaufen, beispielsweise in einer Buchhandlung oder einem Verwaltungsbüro. (UEM-Konsole v8.3+)	
Gastgewerbe	Gästeerlebnis	Machen Sie Ihre Gäste zu treuen Stammgästen, indem Sie ihnen ermöglichen, ihre eigenen Dienstleistungen zu planen, nach Sehenswürdigkeiten zu suchen oder Stammkundenrabatte in Anspruch zu nehmen. (UEM-Konsole v8.3+)

Branche	Initiative	Beschreibung
Hotelmanagement	Verwalten Sie Buchungen und den Zeitplan von Mitarbeitern, die Aufgabenplanung für Arbeitsschichten und Sonderwünsche in Echtzeit. (UEM-Konsole v8.3+)	
Mobile Zahlungen	Integrieren Sie mobile Zahlungslösungen in POS-Systeme, damit Gästen eine schnelle Zahlungsmöglichkeit zur Verfügung steht, oder rüsten Sie Mitarbeiter aus, um überall als Verkäufer agieren zu können. (UEM-Konsole v8.3+)	
Einzelhandel	Mobile Einkaufserfahrung	Stellen Sie Dienstleistungen für Kunden an jeder Stelle im Geschäft bereit, um ihnen die Produktsuche, Produktinformationen, Preisüberprüfungen und einen Kauf zu ermöglichen. (UEM-Konsole v8.3+)
Mobile Registrierkasse	Erstellen Sie mobile Verkaufsstellen und machen Sie im Laden mehr Platz für Waren frei. (UEM-Konsole v8.2.2+)	
Geschäfts-Manager	Ermöglichen Sie Ihren Filialleitern die Arbeit an Berichten, Einsatzplänen für die Mitarbeiter und Lohnverrechnung überall im Laden. (UEM-Konsole v8.2.2+)	
Außendienst	Außendienstmitarbeiter	Erhöhen Sie die Effizienz für Vertriebsmitarbeiter, Servicetechniker und andere mit papierlosen Serviceeinsätzen und Echtzeitdaten für Kunden. (UEM-Konsole v8.3+)
Außendienstleiter	Ermöglichen Sie dynamische Zeitplanung und Echtzeit-Berichterstellung für Außendienstleiter zur Kommunikation mit Mitarbeitern, Ermittlung von Standorten, Bearbeitung von Zeitplänen und Zuweisung von Aufgaben. (UEM-Konsole v8.3+)	

Arbeiten mit Profilen und Konformitätsrichtlinien für Branchenvorlagen

- **Profile** – Die Fähigkeit zum Hinzufügen oder Bearbeiten von Profilen ist in der UEM-Konsole nur auf der Seite **Listenansicht** vorhanden. Änderungen werden auf der Seite **Listenansicht** in der Benutzeroberfläche der Branchenvorlage unter **Hub** nicht dargestellt.
- **Konformitätsrichtlinien** – Die einzige Konformitätsrichtlinie, die vorgegeben und für die Anzeige in Branchenvorlagen verfügbar ist, ist „Gefährdungsstatus“ in der UEM-Konsole 8.2.2+. Wie bei den Profilen ist die Möglichkeit zum Hinzufügen oder Bearbeiten von Konformitätsrichtlinien nur auf der Seite **Listenansicht** möglich. Änderungen werden auf der Seite **Listenansicht** in der Benutzeroberfläche der Branchenvorlage unter **Hub** nicht dargestellt.

Weitere Informationen zum Einrichten von Profilen und Konformitätsrichtlinien finden Sie im **VMware Workspace ONE UEM Mobile Device Management Guide** in den Workspace ONE UEM-Ressourcen.

Erstellen einer Apple-Branchenvorlage

Konfigurieren Sie mithilfe einer Vorlage spezifische Einstellungen für Initiativen. Danach erstellen Sie eine Patientenversorgung-Vorlage, die an Patienten übermittelt wird. Sie können beispielsweise eine Vorlage für die klinische Zusammenarbeit erstellen und an eine Benutzergruppe von Ärzten und eine Benutzergruppe von Krankenpflegepersonal übermitteln.

Voraussetzungen

Denken Sie daran, Ihre Benutzergruppen zu erstellen, bevor Sie mit diesem Prozess beginnen.

Verfahren

1. Navigieren Sie zu **Hub > Branchenvorlagen > Listenansicht > Vorlage hinzufügen**. Das Dialogfeld **Vorlage hinzufügen** wird angezeigt.
2. Wählen Sie die geeignete Branchenkategorie aus. Das Dialogfeld **Erste Schritte mit Branchenvorlagen** wird angezeigt.
   a. Wenn Sie eine andere Branche auswählen und andere Initiativen verwenden möchten, verwenden Sie die Option **Wählen Sie eine andere Branche** unten im Dialogfeld, um gegebenenfalls die angezeigte Branche zu überschreiben.
3. Wählen Sie die Geschäftsinitiative, die Sie konfigurieren möchten, und dann **Optionen**.
4. Wählen Sie **Weiter**, nachdem Sie den Überblick über die Vorlage gelesen haben. Ein neues Dialogfeld erscheint, in dem Sie die Vorlage anpassen können.
5. Legen Sie den **freundlichen Namen** fest, der in der UEM-Konsole angezeigt werden soll.
6. Wählen Sie, welche **Anwendungen** an Ihre Benutzer übermittelt werden sollen, indem Sie Anwendungen aus- oder abwählen. Alle vorbereiteten Anwendungen sind empfohlen und standardmäßig vorausgewählt. Sie können aber auch **Anwendung hinzufügen** auswählen, um im App Store nach öffentlich verfügbaren Anwendungen zu suchen oder interne Anwendungen hochzuladen.
   a. Wählen Sie **Weitere Optionen**, um die Anwendung im **Auto**- oder **Nach Bedarf**-Modus zu übertragen, und erstellen Sie eine benutzerdefinierte **Anwendungskonfiguration**, um die wichtigsten Wertepaare einzugeben.

   Hinweis: Wenn Sie die Vorlage „Mobile Einkaufserfahrung“ ausgewählt haben und danach VMware Browser im Einzelanwendungsmodus auswählen, konfigurieren Sie die URL, bevor Sie die Vorlage an Geräte übertragen, indem Sie zu **Gruppen & Einstellungen > Alle Einstellungen > Anwendungen > Browser > Modus > Startseiten-URL** navigieren. Diese Geräte müssen im Überwachungsmodus konfiguriert werden.
7. Überprüfen Sie die **Richtlinien**, die auf die ausgewählte Vorlage zutreffen.

8 Weisen Sie **Benutzer** oder Benutzergruppen für die Bereitstellung zu oder erstellen Sie Benutzer. Verzeichnisdienste müssen bereits konfiguriert sein, damit Sie Verzeichnisbenutzer hinzufügen können. Wenn ein Benutzer oder eine Benutzergruppe erstellt wird, erscheint er oder sie auf der Seite **Konten > Listenansicht** in der UEM-Konsole, auch wenn die Branchenvorlage noch nicht eingesetzt ist.

9 Wählen Sie **Weiter**, nachdem Sie Ihre Auswahl bestätigt haben.

10 Wählen Sie **Veröffentlichen**. Die neue Vorlage erstellt eine intelligente Gruppe, der alle Anwendungen, Profile, Richtlinien, Benutzer und Benutzergruppen zugewiesen werden. Die neue Vorlage wird jetzt in **Branchenvorlagen > Listenansicht** angezeigt.

Denken Sie daran, einer Gerätegruppe eine Vorlage zuzuweisen, sodass jedem Gerät nur eine geschäftliche Initiative zugewiesen ist. Wenn Sie jedoch mehr als eine Vorlage derselben Gruppe zuweisen, werden alle Anwendungen von beiden Vorlagen installiert und die restriktiven Richtlinien werden an das Gerät übertragen.

Bearbeiten von Anwendungslisten in Apple-Branchenvorlagen

Sie können die von Ihnen erstellten Branchenvorlagen mit spezifischen Konfigurationen für den Einsatz von Anwendungen individuell anpassen.

Verfahren

1 Sie können eine öffentliche Anwendung schnell entfernen und die aktualisierte Anwendungsliste sofort an die Benutzer übermitteln.

a Navigieren Sie zu **Hub > Branchenvorlagen > Listenansicht**.

b Wählen Sie die **Stiftschaltfläche** oder den Vorlagennamen, um die Vorlage zu bearbeiten.

c Wählen Sie die Anwendung ab. Das Häkchen in der Ecke verschwindet.

d Wählen Sie **Weiter > Veröffentlichen**, um die Vorlage zu speichern und erneut zu veröffentlichen.

2 Laden Sie eine neue Anwendungsversion einer internen Anwendung hoch, nachdem Sie die alte Version gelöscht haben.

a Wählen Sie die **Stiftschaltfläche** oder den Vorlagenlink, um die Vorlage zu bearbeiten.

b Wählen Sie **Weitere Optionen**. Ein Abfallkorbsymbol erscheint auf der internen App.

c Wählen Sie **Entfernen** und befolgen Sie die Eingabeaufforderungen, um die Anwendung aus der Liste zu löschen.

d Wählen Sie **Anwendung hinzufügen**, um die aktualisierte Anwendung hochzuladen.

e Wählen Sie **Weiter > Veröffentlichen**, um die Vorlage mit der neuen Anwendungsversion zu speichern und erneut zu veröffentlichen.

Beachten Sie, dass das Bearbeiten von Anwendungen nur in der Branchenvorlage erfolgen sollte. Anwendungen können jedoch auch über **Ressourcen > Apps > Native** in der UEM Console bearbeitet werden. Änderungen an Anwendungen auf der systemeigenen Seite „Listenansicht“ werden in der Benutzeroberfläche der Branchenvorlage nicht angezeigt.

Löschen einer Apple-Branchenvorlage

Sie können Vorlagen nur auf der aktuellen oder untergeordneten Ebene der Organisationsgruppe bearbeiten und löschen. Sie können Vorlagen nicht bearbeiten oder löschen, die In einer höheren Organisationsgruppe erstellt wurden, sondern diese nur anzeigen.

Verfahren

1. Navigieren Sie zu **Hub > Branchenvorlagen > Listenansicht**.
2. Wählen Sie die **Optionsschaltfläche**. Die Schaltfläche **Löschen** erscheint oben in der Liste.
3. Wählen Sie **Löschen** und befolgen Sie die Eingabeaufforderungen, um die Vorlage zu löschen. Das Löschen einer Vorlage löscht auch die dazugehörigen Anwendungen und Richtlinien von zugewiesenen Geräten.

   Das Löschen einer Vorlage entfernt die Anwendung nicht aus **Anwendungen > Systemeigen** und die Smartgroup nicht aus **Gruppen > Listenansicht**.

Überblick über Apple iBeacon

Apple iBeacon mit Workspace ONE Intelligent Hub v5.1+ wird zur Verwaltung der Standorterkennung für Geräte eingesetzt. Mithilfe von Bluetooth Low Energy (BLE) bieten iBeacons eine effizientere Methode zur Verfolgung von Geräten als Geofencing.

Bluetooth Low Energy verkürzt die Akkulebensdauer eines Geräts nicht und Sie können iBeacons einrichten, um mehrere Regionen gleichzeitig zu überwachen und damit die Überwachungspräzision zu erhöhen. Für Endbenutzer bietet diese Funktionalität mehr Datenschutz, weil Geräte nicht ständig überwacht, sondern nur verfolgt werden, wenn das Gerät an bestimmte Standorte verbracht oder von dort weggebracht wird.

Nach dem Einrichten eines iBeacon eines Drittanbieters konfigurieren Sie den iBeacon in der UEM-Konsole. Danach erstellen Sie die iBeacon-Regionen, die zu überwachen sind. Zuletzt verteilten Sie die Geräteprofile mit iBeacon-Funktionen, um iBeacons in den konfigurierten Regionen mit Workspace ONE Intelligent Hub zu verwalten. Erkennen Sie, wenn das Gerät in diesen Bereich verbracht wird, und benutzen Sie die Ereignisprotokolle des Geräts, um Änderungen der iBeacon-Bereiche zu finden.

Voraussetzungen für iBeacon

- Workspace ONE UEM-Konsole v8.1+
- iBeacons von einem Drittanbieter
- Workspace ONE Intelligent Hub v5.1 + für iOS

- Ortungsdienste auf dem Gerät müssen aktiviert sein
- Bluetooth muss aktiviert sein
- iPhone 4S+, iPad mini+, iPad 3. Generation+, iPod touch 5. Generation+

Details zur Verwendung von iBeacon

- Maximal 20 Bereiche, einschließlich Geofencing und iBeacon-Gruppen, können dem Gerät zugewiesen werden. Dies ist die maximale Anzahl, die Apple zulässt. Eine große Anzahl von iBeacon-Gruppen, die dem Gerät zugewiesen ist, erhöht den Akkuverbrauch auf dem Gerät.
- Der Workspace ONE Intelligent Hub überwacht nur iBeacons. Er nutzt nicht die Bereichstechnik, die die Nähe des Geräts zum iBeacon-Sender festlegt.
- Wenn Workspace ONE Intelligent Hub heruntergefahren wird, bevor das Gerät die iBeacon-Gruppe verlässt, wird das Gerät erst erkannt, wenn Workspace ONE Intelligent Hub erneut gestartet wird.

Aktivieren von iBeacon für iOS-Geräte

Um iBeacon zu konfigurieren, aktivieren Sie erst Workspace ONE Intelligent Hub, damit iBeacon-Gruppen erkannt werden, die Broadcasts empfangen. Danach fügen Sie eine Anzahl von iBeacon-Gruppen für das zu überwachende Gerät hinzu.

Verfahren

1. Navigieren Sie zu **Gruppen & Einstellungen > Alle Einstellungen > Geräte & Benutzer > Apple > Apple iOS > Hub-Einstellungen**.
2. Rollen Sie bis **Bereich** ab und wählen Sie **iBeacon-Bereich** ermitteln, um einen iBeacon für die Organisationsgruppe zu aktivieren.
3. Wählen Sie **Speichern**.
4. Gehen Sie zu **Ressourcen** > **Profile und Baselines** > **Einstellungen Bereiche**.
5. Wählen Sie **Hinzufügen > iBeacon-Gruppe**. Wählen Sie **Hinzufügen > Profil hinzufügen** oder **Bearbeiten** eines existierenden Profils mithilfe der Stiftschaltfläche auf der linken Seite des Profils. Ein Profilfenster **Allgemein** wird eingeblendet.
6. Konfigurieren Sie die **iBeacon-Gruppe**-Einstellungen.

Einstellung	Beschreibung
Gruppenname	Geben Sie den Namen für die jeweilige iBeacon-Gruppe ein.
iBeacon-Name	Geben Sie den Namen des iBeacons ein.
UUID	Geben Sie die eindeutige Kennung für den iBeacon ein, der freigegeben werden soll.

Einstellung	Beschreibung
Major-Wert	Geben Sie eine Kennung ein, um den Bereich des iBeacons weiter zu unterteilen.
Minor-Wert	Geben Sie eine zusätzliche Kennung ein, um den Bereich des iBeacons weiter zu unterteilen.

7 Wählen Sie **Speichern**. Kehren Sie zu **Bereich** zurück. Bearbeiten und löschen Sie gegebenenfalls iBeacon-Gruppen mithilfe der Menüschaltflächen auf der linken Seite.

Zuweisen von iBeacon-Gruppen zu Geräteprofilen

Sobald die iBeacon-Gruppe eingerichtet ist, können Sie die Gruppe einem Geräteprofil zuweisen. Dieses Profil wird dann auf dem Gerät installiert, wenn es in die iBeacon-Gruppe kommt, und wird entfernt, wenn es die Gruppe verlässt.

Verfahren

1 Navigieren Sie zu **Ressourcen** > **Profile und Baselines** > **Profile** . Wählen Sie **Hinzufügen** **Profil hinzufügen** oder **Bearbeiten** eines existierenden Profils mithilfe der Stiftschaltfläche auf der linken Seite des Profils. Ein Profilfenster **Allgemein** wird eingeblendet.

2 Rollen Sie bis zum Abschnitt **Zusätzliche Zuweisungskriterien** auf der Registerkarte **Allgemein** ab.

3 Unter **Nur auf Geräten innerhalb der ausgewählten Bereiche installieren** wählen Sie den iBeacon aus **Zugewiesener Geofence-Bereich**.

4 Konfigurieren Sie die Nutzlast nach Ihren Wünschen.

5 Wählen Sie **Speichern und veröffentlichen**. Jetzt können Sie Geräte in der iBeacon-Gruppe im Workspace ONE Intelligent Hub verwalten.

Hinzufügen von Konformitätsrichtlinien für iBeacon-Gruppen

Nachdem die iBeacon-Gruppe eingerichtet wurde, fügen Sie Konformitätsrichtlinien hinzu, um Aktionen mit dem Gerät zu erzwingen, wenn es in die iBeacon-Gruppe kommt oder sie verlässt.

Verfahren

1 Navigieren Sie zu **Geräte > Konformitätsrichtlinien > Listenansicht** und wählen Sie **Hinzufügen** und dann **Apple iOS**.

2 Wählen Sie **Beliebig** oder **Alle** für die zu verwendenden Regeln.

3 Wählen Sie **iBeacon-Bereich** und **in/nicht in** für eine spezifische iBeacon-Gruppe. Anschließend wählen Sie **Weiter**.

4 Wählen Sie die Registerkarte **Aktion** und Aktionen, die in der iBeacon-Gruppe vorkommen können. Detaillierte Informationen zu den anwendbaren Aktionen unter Apple iOS finden Sie im Abschnitt *Konformitätsrichtlinienaktionen nach Plattform* der Dokumentation *Geräte verwalten*.

5 Wählen Sie **Beenden und aktivieren**, wenn Sie die Konfiguration der Konformitätsrichtlinie abgeschlossen haben. Überprüfen Sie, ob die Richtlinie auf der Seite „Gerätedetails“ in der UEM-Konsole verfügbar ist.

Überblick über die Aktivierungssperre

Die Aktivierungssperre ist eine Sicherheitsfunktion von Geräten, auf denen iOS 7 oder höher ausgeführt wird und die Funktion „Mein iPhone suchen“ aktiviert ist. Sollte das Gerät jemals gestohlen werden oder verloren gehen, erschwert diese Funktion nicht autorisierten Personen den Zugriff auf dieses Gerät.

Ist die Aktivierungssperre aktiviert, muss der Endbenutzer zum Entsperren des Geräts seine Apple-ID und das zugehörige Kennwort eingeben – selbst dann, wenn sämtliche Daten vom Gerät gelöscht wurden oder das Gerät auf die Werkseinstellungen zurückgesetzt wurde. Dies gilt auch für Geräte im DFU-Modus. Weitere Informationen zur Aktivierungssperre von iOS-Geräten finden Sie im Apple-Supportartikel Aktivierungssperre von „Mein iPhone suchen“.

Voraussetzungen

Die Aktivierungssperre kann nur verwendet werden, wenn Folgendes auf die Geräte zutrifft:

- Das Gerät wurde mit einer gültigen Apple-ID und dem zugehörigen Kennwort verknüpft.
- Die Funktion „Mein iPhone suchen“ ist aktiviert.

Aktivierungssperre für überwachte und nicht überwachte Geräte – ein Vergleich

Wie weit Sie Geräte mit Aktivierungssperre verwalten können, hängt davon ab, ob die Geräte überwacht oder nicht überwacht sind. Die folgende Tabelle zeigt die Unterschiede:

Nicht überwachtes	Überwacht
■ Endbenutzer müssen die Funktion „Mein iPhone suchen“ aktivieren. ■ Administratoren können prüfen, ob die Aktivierungssperre auf einem bestimmten Gerät aktiviert ist. ■ Um sämtliche Daten von einem Gerät löschen zu können, müssen Administratoren zunächst eine Warnmeldung bestätigen, die Sie darüber informiert, dass ein Gerät mit aktivierter Aktivierungssperre nur durch Eingabe der ursprünglichen Apple-ID und dem zugehörigen Kennwort erneut aktiviert werden kann.*	■ Die Aktivierungssperre kann vom Administrator aktiviert werden. Dadurch wird auch automatisch die Funktion „Mein iPhone suchen“ aktiviert. ■ Administratoren können prüfen, ob die Aktivierungssperre auf einem bestimmten Gerät aktiviert ist. ■ Administratoren können die Aktivierungssperre mithilfe drei verschiedener Methoden aufheben.

* Wie Sie die Verknüpfung eines Geräts mit der Apple-ID des Vorbesitzers aufheben, um es zu reaktivieren, erfahren Sie im Apple-Supportartikel Aktivierungssperre „Mein iPhone suchen“ deaktivieren.

Aktivierungssperre von iOS-Geräten aktivieren

Für überwachte Geräte mit iOS 7 und höher können Sie die Aktivierungssperre konfigurieren und ihre Aktivierung erzwingen.

Verfahren

1 Navigieren Sie zu **Gruppen & Einstellungen > Alle Einstellungen > Geräte und Benutzer > Apple > Apple iOS > Verwaltete Einstellungen**.

2 Wählen Sie die Einstellung **Aktivierungssperre**.

3 Wählen Sie **Speichern**.

Anzeigen des Aktivierungssperrstatus

Sowohl bei nicht überwachten als auch überwachten Geräten unter iOS 7 und höher können Sie sehen, ob die Aktivierungssperre auf dem Gerät aktiviert ist.

Verfahren

1 Navigieren Sie zu **Geräte > Listenansicht**.

2 Wählen Sie ein iOS-Gerät.

Ergebnisse

Im Abschnitt „Sicherheit“ können Sie sehen, ob die Aktivierungssperre aktiviert ist.

Aktivierungssperre von iOS-Geräten aufheben

Für überwachte Geräte mit iOS 7 und höher können Sie die Aktivierungssperre mit einer von drei Methoden zurücksetzen:

Verfahren

1 Verwenden Sie den Befehl „Aktivierungssperre aufheben“.

2 Geben Sie einen Aktivierungssperren-Umgehungscodes direkt auf dem Gerät ein.

3 Führen Sie einen Geräte-Wipe-Befehl durch und wählen Sie eine Option zum Aufheben der Aktivierungssperre aus.

Verwenden des Befehls „Aktivierungssperre aufheben“

Mit dem Befehl „Aktivierungssperre aufheben“ können Sie die Aktivierungssperre auf einem Gerät löschen, ohne ein Geräte-Wipe durchführen zu müssen. Dieser Befehl kann sinnvoll sein, wenn Sie wissen, wo das Gerät ist, und seine Inhalte nicht vollständig löschen möchten, um die Aktivierungssperre aufzuheben.

Dieser Befehl funktioniert auch, wenn die Registrierung des Geräts in Workspace ONE UEM MDM aufgehoben wurde.

Verfahren

1 Navigieren Sie zu **Geräte > Listenansicht**.

2 Wählen Sie ein iOS-Gerät.

3 Die Seite „Gerätedetails“ wird angezeigt. Wählen Sie die Dropdown-Liste **Mehr**, um eine Liste der verfügbaren Remotebefehle anzuzeigen.

4 Wählen Sie **Aktivierungssperre aufheben**.

5 Wählen Sie **Deaktivieren**.

Eingeben eines Aktivierungssperren-Umgehungscodes

Die Eingabe eines Aktivierungssperren-Umgehungscodes kann sinnvoll sein, wenn die Registrierung des Geräts in Workspace ONE UEM MDM aufgehoben wurde und es keine Möglichkeit gibt, den Befehl „Aktivierungssperre aufheben“ oder ein Geräte-Wipe durchzuführen.

Verfahren

1 Navigieren Sie zu **Geräte > Listenansicht**.

2 Wählen Sie ein iOS-Gerät. Die Seite „Gerätedetails“ wird angezeigt.

3 Wählen Sie die Dropdown-Liste **Mehr**, um eine Liste der verfügbaren Remotebefehle anzuzeigen.

4 Wählen Sie **Aktivierungssperre aufheben**. Der Aktivierungssperren-Umgehungscode wird auf dem Bildschirm angezeigt.

Nächste Schritte

Reaktivieren Sie das Gerät, sobald es mit MDM auf die Werkseinstellungen zurückgesetzt wurde. Wenn Sie den Bereich „iPhone aktivieren“ im Setup-Assistenten erreicht haben, geben Sie den Umgehungscode als Kennwort für die Aktivierungssperre ein und lassen Sie das Textfeld „Apple-ID“ leer.

Durchführen eines Geräte-Wipe-Befehls

Wenn Sie den Befehl für ein Geräte-Wipe ausführen, haben Sie auch die Option, die Aktivierungssperre auf einem Gerät aufzuheben.

Verfahren

1 Navigieren Sie zu **Geräte > Listenansicht**.

2 Wählen Sie ein iOS-Gerät. Die Seite „Gerätedetails“ wird angezeigt.

3 Wählen Sie die Dropdown-Liste **Mehr**, um eine Liste der verfügbaren Remotebefehle anzuzeigen.

4 Wählen Sie **Geräte-Wipe**. Die Seite „Geräte-Wipe“ wird angezeigt.

5 Wählen Sie **Aktivierungssperre aufheben**. Geben Sie Ihre **Sicherheits-PIN** ein und das Gerät wird vollständig gelöscht.

Aktivierungssperre – Workflow-Matrix für den Löschbefehl

Die folgende Matrix zeigt den Workflow zur Prüfung des Codes zur Umgehung der Aktivierungssperre vor dem Absetzen eines Löschbefehls für das Gerät über die UEM Console.

Die Prüfung des Umgehungscodes kann auf der Seite „Gerätelistenansicht“ oder „Gerätedetails“ gestartet werden.

Tabelle 6-1. Matrix zur Prüfung des Codes zur Umgehung der Aktivierungssperre

Befehl	**Workflow für den Code zur Umgehung der Aktivierungssperre**	
	Gerätelistenansicht	**Seite „Gerätedetails“**
Gerätezurücksetzung	Nicht zutreffend	1 Sendet eine Abfrage an das Gerät, um den Code zur Umgehung der Aktivierungssperre abzurufen. 2 Das Gerät ist in der UEM Console als **Gerätelöschung gestartet** markiert. 3 Wenn der Löschschutz auf dem Gerät deaktiviert ist, antwortet das Gerät mit dem Umgehungscode in der UEM Console. 4 Die UEM Console sendet den Befehl zum Löschen des Geräts an das Gerät. 5 Das Gerät antwortet mit der erfolgreichen Löschmeldung in der UEM Console. 6 Das Gerät ist in der UEM Console als **Nicht registriert** markiert.
Enterprise Wipe	1 Sendet eine Abfrage an das Gerät, um den Code zur Umgehung der Aktivierungssperre abzurufen. 2 Das Gerät ist in der UEM Console als **Enterprise Wipe gestartet** markiert. 3 Wenn der Löschschutz auf dem Gerät deaktiviert ist, antwortet das Gerät mit dem Umgehungscode in der UEM Console. 4 Die UEM Console sendet den Enterprise Wipe-Befehl an das Unternehmen. 5 Das Gerät antwortet mit der erfolgreichen Löschmeldung in der UEM Console. 6 Das Gerät ist in der UEM Console als **Nicht registriert** markiert.	1 Sendet eine Abfrage an das Gerät, um den Code zur Umgehung der Aktivierungssperre abzurufen. 2 Das Gerät ist in der UEM Console als **Enterprise Wipe gestartet** markiert. 3 Wenn der Löschschutz auf dem Gerät deaktiviert ist, antwortet das Gerät mit dem Umgehungscode in der UEM Console. 4 Die UEM Console sendet den Enterprise Wipe-Befehl an das Unternehmen. 5 Das Gerät antwortet mit der erfolgreichen Löschmeldung in der UEM Console. 6 Das Gerät ist in der UEM Console als **Nicht registriert** markiert.

Senden einer AirPlay-Anforderung an ein iOS-Gerät

Mithilfe des AirPlay-Befehls können Administratoren problemlos den Bildschirm eines macOS-Computers auf ein tvOS-Gerät übertragen, das sich im selben Subnetzwerk befindet wie das iOS 7+-Gerät.

Wenn ein Endbenutzer Unterstützung benötigt, senden Sie einfach eine AirPlay-Anforderung von der UEM-Konsole an das Gerät, um Ihren Bildschirm auf dem Gerät eines Endbenutzers zu teilen.

Verfahren

1. Navigieren Sie zu **Geräte > Listenansicht > Gerät auswählen > Support > Mehr > AirPlay starten.** Das Dialogfeld **AirPlay** wird aufgerufen.
2. Wählen Sie **Ein Ziel hinzufügen**, um Ziele zum Anzeigen hinzuzufügen. Das Dialogfeld **Neues AirPlay Ziel hinzufügen** wird aufgerufen.
3. Geben Sie den **Zielnamen** ein, den freundlichen Namen des Geräts.
4. Geben Sie die **Zieladresse** ein, also die MAC-Adresse des anzuzeigenden Geräts.
5. Geben Sie das **Kennwort** für das Ziel ein.
6. Legen Sie die **Scanzeit** für die Dauer der Suche des Geräts nach dem Ziel fest. Der Standardwert ist 30 Sekunden.
7. Aktivieren Sie das Kontrollkästchen **Als Standard festlegen**, damit das aktuelle Ziel zum Standardziel wird. Wenn AirPlay das nächste Mal verwendet wird, erscheint das Standardziel als **Zielname**. Es muss nicht erneut eingegeben werden.
8. Wählen Sie **Speichern und starten**, um die AirPlay-Anforderung an das Gerät zu senden.
   a. Dieses Ziel wird für die nächste Anforderung im Dropdown-Menü **Zielname** gespeichert.
9. Für die Option **AirPlay beenden** auf überwachten iOS 7+-Geräten navigieren Sie zurück zur UEM-Konsole. Navigieren Sie zu **Geräte > Listenansicht > Gerät auswählen > Support > Mehr > AirPlay beenden.**
10. Zu **AirPlay-Ziel bearbeiten**
    a. Navigieren Sie zu **Geräte > Listenansicht > Gerät auswählen > Support > Mehr > AirPlay.** Das Dialogfeld **AirPlay** wird aufgerufen.
    b. Wählen Sie das zu bearbeitende **Gerätеziel** aus dem Dropdown-Menü.
    c. Wählen Sie **Bearbeiten**, um mit der Bearbeitung der Zieleinstellungen zu beginnen. Das Dialogfeld **AirPlay Ziel bearbeiten** wird aufgerufen.
    d. Wählen Sie **Speichern und starten**, um die AirPlay-Anforderung an das Gerät zu senden.

Remoteansicht

Mit der Funktion „Remoteansicht“ können Administratoren mühelos bei der Fehlerbehebung helfen, indem sie ein per MDM verwaltetes Gerät eines Endbenutzers über die in das

Partnersystem integrierte UEM-Konsole anzeigen. Die Integration zwischen dem Partnersystem und der UEM-Konsole bietet eine umfassende Remoteverwaltungssuite mit Remoteansichtsfunktionen.

Weitere Informationen zur Konfiguration und Integration von Remoteverwaltungsdiensten unter Verwendung des Partnersystems in Verbindung mit der UEM-Konsole finden Sie im **Leitfaden für VMware AirWatch Advanced Remote Management** auf docs.vmware.com.

Vorbedingungen zum Einleiten der Remoteansicht

- Für die UEM-Konsole müssen der entsprechende Hostname und alle erforderlichen Zertifikate des Partnersystems bereitgestellt werden.
- Die Endbenutzergeräte müssen über den Workspace ONE Intelligent Hub beim Partnersystem registriert werden.

Geräteanforderungen für Remoteansicht

- Auf den Geräten muss Workspace ONE Intelligent Hub v5.8 oder höher installiert sein und im Vordergrund laufen, wenn Sie versuchen, die Remoteansicht einzuleiten.
- Geräte unter iOS 11 und höher müssen den Befehl **Remoteansicht starten** ausführen.
- Für überwachte Geräte unter iOS 11 und höher müssen die Administratoren den Befehl **Remoteansicht stoppen** ausführen. Dieser Befehl wird auf der Konsole des Partnersystems angezeigt.

Konfigurieren der UEM console mit Remoteansicht

Stellen Sie für lokale Bereitstellungen in der Gruppe „Globale Organisation“ auf der Seite „Site-URLs“ die Site-URLs mit dem richtigen Hostnamen für das Partnersystem bereit.

Verfahren

1 Navigieren Sie zu **Gruppen & Einstellungen > Alle Einstellungen > System > Erweitert > Site-URLs**.

2 Konfigurieren Sie im Abschnitt **Workspace ONE Assist** die Einstellungen für die Remoteverwaltung.

Einstellungen	Beschreibung
Hostname der Konsolenverbindung	Geben Sie den vollqualifizierten Domänennamen (FQDN) des Remoteverwaltungsservers plus „/t10“ ein. Zum Beispiel: `https://rmstage01.awmdm.com/t10`
Hostname der Geräteverbindung	Geben Sie den vollqualifizierten Domänennamen (FQDN) des ARM-Servers ein. Zum Beispiel: `https://rmstage01.awmdm.com` Der Hostname des Geräts ist die einzige URL, die für die Geräteregistrierung verwendet wird. Er wird an alle Geräte in der Organisationsgruppe übermittelt, wenn das Partnersystem bereitgestellt wird.

3 Wählen Sie **Speichern**.

Wenn die Seite „Site-URLs“ gespeichert wird, wird die Site-URL zusammen mit den folgenden Daten an das Einstellungsprofil von Workspace ONE Intelligent Hub übertragen. Die Geräte, die bereits beim Workspace ONE Intelligent Hub registriert sind, übernehmen ab diesem Zeitpunkt das aktualisierte Hub-Einstellungsprofil.

- **Hostname des Geräts** – Hostname für das Gerät, das kontaktiert wird, wenn eine Remoteansichtssitzung über die UEM-Konsole eingeleitet wird.
- **Umgebungsname** – Name der Umgebung für das Partnersystem, damit das Gerät in die richtige Organisationsgruppe gestellt wird, wenn das Gerät eine Anfrage für die Remoteansicht stellt.

Konfigurieren von Endbenutzergeräten

Nachdem die Konsole konfiguriert ist, müssen Sie den iOS-spezifischen Hub auf den Geräten installieren, damit sie remote verwaltet werden können.

Verfahren

1 Auf der My Workspace ONE™-Seite sind alle Geräte-Agents aufgeführt. (https://my.workspaceone.com/products/AirWatch-Agent.

2 Laden Sie Workspace ONE Intelligent Hub aus dem App Store unter iOS für Ihre Bereitstellung herunter.

Weitere Informationen zur App-Verwaltung finden Sie im Handbuch **Mobile Anwendungsverwaltung** in der Dokumentation zu VMware AirWatch.

3 Passen Sie das Control Center zum Starten des Bildschirm-Broadcast an:

   a Navigieren Sie zu **Einstellungen > Control Center > Steuerelemente anpassen**.

   b Fügen Sie **Bildschirmaufzeichnung** hinzu.

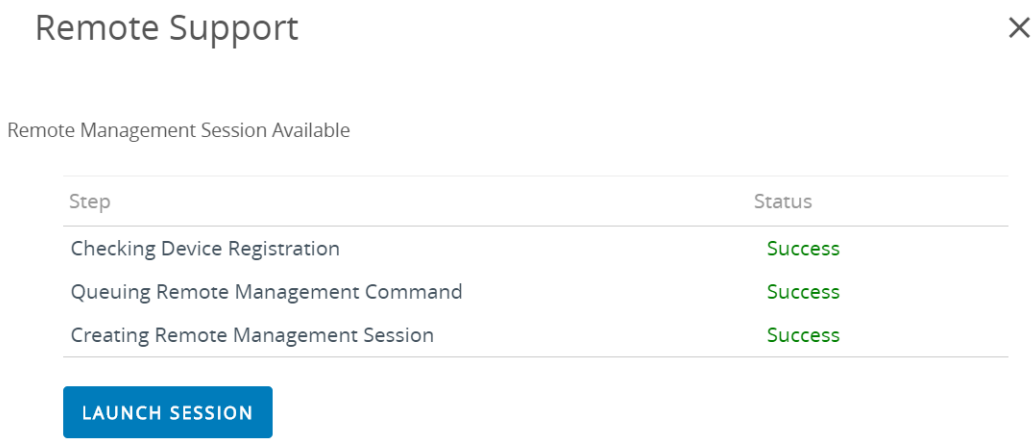
Einleiten einer Remoteansichtssitzung

Über die Remoteansichtssitzung können Sie einen Endbenutzer ganz unkompliziert bei der Fehlerbehebung unterstützen, indem Sie dessen Gerät in der UEM-Konsole anzeigen.

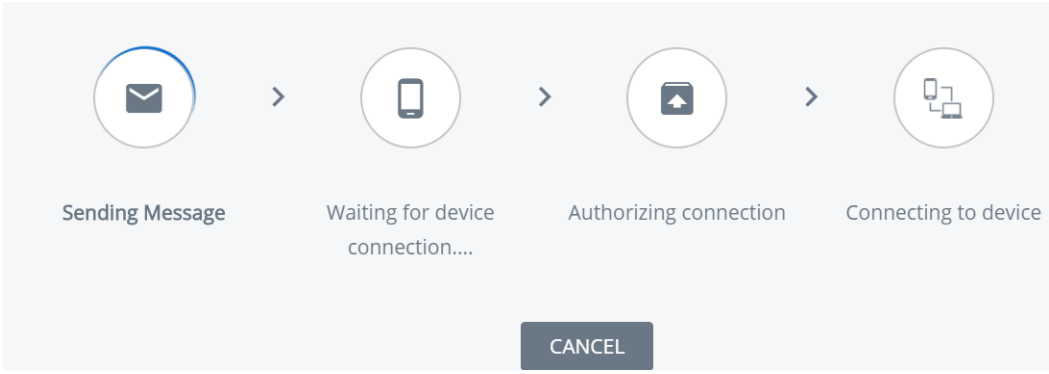
Verfahren

1 Navigieren Sie zu **Geräte > Listenansicht > Gerät auswählen > Weitere Aktionen > Support > Remoteansicht starten**.

   Das Fenster **Remote-Support** wird angezeigt. Die UEM-Konsole überprüft vor dem Start des Broadcast die Fähigkeiten des Geräts. Gleichzeitig wird über Workspace ONE Intelligent Hub eine Push-Benachrichtigung an das Endbenutzergerät gesendet, um den Broadcast zu starten. Der Benutzer muss auf das Gerätesteuerungscenter zugreifen und auf die Bildschirmaufnahme tippen. Um den Broadcast auf den Gerätebildschirm zu starten, wählen Sie **Hub-Broadcast > Broadcast starten**. Das Gerät beginnt mit der Erfassung der Benutzeroberfläche und gibt diese für den Workspace ONE Intelligent Hub frei, der mit dem Advanced Remote Management-Server verbunden ist.



2 Wählen Sie im Fenster „Remote-Support“ die Option **Sitzung starten** aus, um die Remoteansichtssitzung zu starten. Sobald die Verbindung hergestellt ist, wird der Remote Management-Client auf der Konsole geöffnet und der gespiegelte Gerätebildschirm angezeigt.



Hinweis Sie müssen den Kunden anweisen, die vierstellige PIN, die auf der UEM-Konsole angezeigt wird, in sein Gerät einzugeben. Durch diese Aktion erhalten Sie die Autorisierung des Kunden, sein Gerät remote zu verwalten.

3 Wählen Sie **Abbrechen**, falls Sie die Sitzung beenden müssen.

Konfigurieren von verwalteten Einstellungen für iOS-Geräte

Über die Seite „Verwaltete Einstellungen“ in der UEM-Konsole können Sie einige zusätzliche Einstellungen im Zusammenhang mit Workspace ONE Intelligent Hub und der Verwaltung von iOS-Geräten vornehmen.

Verfahren

1 Navigieren Sie zu **Geräte > Geräteeinstellungen > Geräte & Benutzer > Apple > Apple iOS > Verwaltete Einstellungen > Standardmäßig verwaltete Einstellungen**.

2 Konfigurieren Sie nach Besitztyp („Unternehmen – Dediziert“, „Unternehmen – Gemeinschaftsgerät“, „Mitarbeitereigen“ und „Unbekannt“), für welche Geräte die Einstellungen gelten sollen.

3 Aktivieren oder deaktivieren:

   a Sprachroaming (iOS 5+)

   b Datenroaming (iOS 5+)

   c Persönlicher Hotspot (iOS 7)

   d Aktivierungssperre (iOS 7 und überwacht)

   e (Überwachte iOS 11.3+-Geräte)

4 Wählen Sie **Speichern**, um die Einstellungen auf Geräten in der aktuellen Organisationsgruppe zu speichern.

Überschreiben von Standard-Roamingeinstellungen (iOS)

Überschreiben Sie Standardeinstellungen, um Roamingrechte für ein einzelnes iOS-Gerät zu ändern.

Ändern Sie die Einstellungen zur Verwaltung des Roamingstatus, der keine dauerhaften Restriktionen erfordert.

Verfahren

1 Navigieren Sie zu **Geräte** > **Listenansicht**. Filtern Sie **Plattform** zur Ermittlung des gewünschten Geräts. Wählen Sie seinen **freundlichen Namen**, um das Gerätebedienfeld zu starten.

2 Wählen Sie **MehrVerwaltete Einstellungen**.

3 Wählen Sie die Optionsschaltfläche **Aktivieren** oder **Deaktivieren** zum Überschreiben der aktuellen Einstellungen **Sprachroaming zulässig**, **Datenroaming zulässig** und **Persönlicher Hotspot zulässig**. Klicken Sie auf **Speichern**.

Einstellen eines Standardhintergrundbilds

Wählen Sie ein Standardbild für gesperrte Bildschirme oder ein Bild für den Startbildschirm der überwachten Geräte unter iOS 7+, um die Branding-Vorgaben Ihres Unternehmens einzuhalten.

Verfahren

1 Navigieren Sie zu **Geräte > Geräteeinstellungen > Geräte & Benutzer > Apple > Apple iOS > Verwaltete Einstellungen**. Rollen Sie bis zum Abschnitt „Standardhintergrundbild“ ab.

2 Laden Sie ein **Bild des Sperrbildschirms** oder ein **Bild der Startseite** hoch.

3 Wählen Sie **Speichern**.

Einstellen der Standard-Organisationsinformationen

Erstellen Sie benutzerdefinierte Organisationsinformationen für MDM-Eingabeaufforderungen für iOS 7+-Geräte.

Verfahren

1 Navigieren Sie zu **Geräte > Geräteeinstellungen > Apple > Apple iOS > Verwaltete Einstellungen** und rollen Sie ab bis zum Abschnitt **Standard-Organisationsinformationen**.

2 Geben Sie Ihre Organisationsinformationen ein, einschließlich Name, Rufnummer und E-Mail.

3 Wählen Sie **Speichern**.

Installieren von Schriftarten auf iOS-Geräten

Diese Funktion ist speziell für macOS Yosemite-Geräte und Geräte mit iOS 7 oder höher verfügbar. Mit der UEM-Konsole können Sie Schriftarten hochladen und auf Geräten installieren. Mit bestimmten Schriftarten können Benutzer Texte lesen, die standardmäßig nicht unterstützt werden.

Kompatible Schriftartdateiformate sind unter anderem .ttf oder .otf. Sie können eine unbegrenzte Anzahl von Schriftarten auf Geräten installieren und eine Schriftart jederzeit entfernen.

Verfahren

- So installieren Sie Schriftarten:
  a. Navigieren Sie zu **Geräte > Geräteeinstellungen > Apple > Schriftarten installieren**.
  b. Ziehen Sie per Drag-and-drop eine unterstützte Schriftartendatei (`.ttf` oder `.otf`) auf den Bildschirm.
  c. Suchen Sie die Schriftartendatei und wählen Sie **Speichern**, um die Schriftart an alle bei der aktuellen Organisationsgruppe registrierten Geräte zu senden.

Cisco QOS-Markierung für iOS-Anwendungen

Apple und Cisco haben gemeinsame Anstrengungen übernommen, um eine bessere Erfahrung mit Anwendungen und Sprachübertragung auf iOS-Geräten in Unternehmensnetzwerken über das QoS Fastlane-Netzwerk von Cisco zu entwickeln. Workspace ONE UEM ermöglicht es Ihnen, Audio- und Video-Anwendungen auszuwählen, für die priorisierte Datenzuweisungen erfolgen.

Mit Workspace ONE UEM MDM haben Kunden mit der Cisco-Infrastruktur folgende Möglichkeiten:

- Aktivieren oder Deaktivieren der Verwendung des QoS Fastlane-Netzwerkes von Cisco
- Freigabe von Anwendungen, damit für diese die L2- und L3-Markierung berücksichtigt wird
- Aktivieren von Audio- und Video Datenverkehr für integrierte Dienste wie FaceTime und WLAN-Anrufe für die L2- und L3-Markierung für Datenverkehr, der über das WLAN gesendet wird

Wie Sie Cisco-QoS-Markierungen für Anwendungen konfigurieren, erfahren Sie unter Konfigurieren eines WLAN-Profils.

Apple Push-Benachrichtigungsdienst (APNs) 7

Apple Push Notification Service (APNs) ist das von Apple erstellte MDM-Protokoll zur Verwaltung von Apple-Geräten. Es erfordert, dass der MDM-Anbieter ein gültiges APNs-Zertifikat konfiguriert hat, und leitet alle Befehle über die zentralen Cloud-Messaging-Server von Apple weiter.

Das Initiieren eines APNs-Befehls führt zu Folgendem:

- Wenn ein iOS-Gerät registriert wird, wird ein APNs-Token generiert, das mit einem bestimmten Gerät verbunden ist. Das generierte Token ist sowohl für Workspace ONE UEM console als auch für die APNs-Server bekannt.
- Nach der Registrierung weist ein Gerät immer eine aktive Verbindung zu den APNs-Servern von Apple auf.
- Wenn ein Befehl in der UEM-Konsole initiiert wird (z. B. ein Profil-Push oder ein Gerätesperrbefehl), geschieht Folgendes:
  - Ein Eintrag wird in der Geräte-Befehlswarteschlange in der UEM-Datenbank gespeichert. Der Eintrag enthält eine bestimmte ID, die mit dem Typ des initiierten Befehls verknüpft ist.
  - Der UEM-Server (entweder Konsole oder Gerätedienste, je nachdem wo der Befehl initiiert wurde) erreicht die APNs-Server mit dem APNs-Token, das mit diesem bestimmten Gerät verknüpft ist.
- Der APNs-Server validiert das Token und informiert das Gerät über die Verbindung zum MDM-Server, um einen Befehl zu erhalten.
- Das Gerät stellt eine Verbindung mit dem Gerätedienstserver her. Beim Herstellen dieser Verbindung empfängt das Gerät alle ausstehenden Befehle aus der Geräte-Befehlswarteschlange.

Zertifikat für Apple Push-Benachrichtigungsdienst (Apple Push Notification- oder APNs-Zertifikat)

Um iOS-Geräte zu verwalten, müssen Sie zuerst ein APNs-Zertifikat (Apple Push Notification Service, Apple-Push-Benachrichtigungsdienst) einholen. Ein APNs-Zertifikat ermöglicht der UEM Console, sicher mit Apple-Geräten zu kommunizieren und Informationen an die UEM Console zu übermitteln.

Laut Apple-Enterprise-Entwicklerprogramm ist ein APNs-Zertifikat ein Jahr lang gültig und muss dann erneuert werden. Die UEM-Konsole sendet Erinnerungen über die Benachrichtigungsfunktion, wenn das Ablaufdatum bevorsteht. Ihr aktuelles Zertifikat wird nach der Erneuerung im Apple Development Portal gesperrt, d.h., dass Geräte erst verwaltet werden, wenn Sie das neue Zertifikat hochgeladen haben. Planen Sie, Ihr Zertifikat sofort nach seiner Erneuerung hochzuladen. Verwenden Sie am besten für jede Umgebung ein anderes Zertifikat, falls Sie separate Produktions- und Testumgebungen einsetzen.

Dieses Kapitel enthält die folgenden Themen:

Workflow des Apple Push-Benachrichtigungsdiensts

Machen Sie sich mit dem Backend-Workflow des Apple Push-Benachrichtigungsdienstes vertraut, bevor Sie das MDM-Management auf Apple-Geräten initiieren.

Verfahren

1. Der Systemadministrator führt Remote-MDM-Aktionen wie z. B. Gerät sperren, Gerätekennung löschen, Gerätezurücksetzung und Unterbrechungs-MDM von der UEM-Konsole aus.

   Eine Benachrichtigung wird in einer Warteschlange in **FastLaneAPNsOutBound** gespeichert, die vom **Workspace ONE Messaging Service** abgeholt und an den APNs-Server gesendet wird. Später wird ein Befehl in die Warteschlange **AWEventLog** gereiht und dann vom Dienst **EntityChangeQueueMonitor** abgerufen. Dieser Dienst stellt den Befehl im Workspace ONE-Datenbankserver in die Warteschlange.
2. Das Gerät hat immer eine aktive Verbindung zu APNs. Die gesamte Kommunikation mit APNs ist eingehend und wird ständig mit APNs überprüft. Die Server lassen das Gerät wissen, wann ein Befehl auf das Gerät von MDM wartet.
3. Sobald das Gerät die Push-Benachrichtigung erhält, checkt es auf dem Gerätedienstserver des Workspace ONE-Geräts ein.
4. Der Gerätedienstserver überprüft, ob ein beliebiger Befehl in die Warteschlange für dieses bestimmte Gerät (basierend auf der Geräte-Nr.) im Workspace ONE-Datenbankserver gestellt wird.
5. Der Gerätedienstserver ruft den Befehl ab, der für dieses Gerät bereits vom Workspace ONE-Datenbankserver in die Warteschlange gestellt wurde.
6. Der Gerätedienst generiert eine XML-Datei und sendet sie an das Gerät. Der native MDM-Agent (auf dem Gerät installiertes MDM-Profil) führt dann die erforderliche Aktion auf dem Gerät aus.

Geräteverwaltung

8

Nachdem Sie Geräte registriert und konfiguriert haben, verwalten Sie diese mit der Workspace ONE ™ UEM-Konsole. Mit den Verwaltungstools und -funktionen können Sie Geräte überwachen und administrative Aufgaben remote ausführen.

Sie können Ihre gesamten Geräte in der UEM-Konsole verwalten. Das Dashboard ist eine durchsuchbare, anpassbare Ansicht, mit der Sie bestimmte Geräte filtern und suchen können. Diese Funktion erleichtert die Ausführung administrativer Funktionen auf einem bestimmten Satz an Geräten. In der Gerätelistenansicht werden alle Geräte angezeigt, die aktuell in der Workspace ONE UEM-Umgebung registriert sind, sowie der zugehörige Status. Die Seite **Gerätedetails** enthält gerätespezifische Informationen, wie Profile, Anwendungen, Workspace ONE Intelligent Hub-Version und Version jedes derzeit auf dem Gerät installierten OEM-Dienstes. Außerdem können Sie auf der Seite „Gerätedetails“ plattformspezifische Remote-Aktionen ausführen.

Dieses Kapitel enthält die folgenden Themen:

Geräte-Dashboard

Sie können neu registrierte Geräte über das **Geräte-Dashboard** in Workspace ONE UEM powered by AirWatch verwalten.

Das **Geräte-Dashboard** bietet einen Überblick über Ihre gesamte Geräteflotte sowie eine schnelle Möglichkeit, Aktionen für einzelne Geräte auszuführen.

Sie können grafische Darstellungen relevanter Gerätedaten zu Ihrer Flotte prüfen, wie beispielsweise Gerätebesitztyp, Konformitätsstatistiken sowie Plattform- und Betriebssystemstrukturen. Sie können auf die einzelnen Gerätesätze in den dargestellten Kategorien zugreifen, indem Sie eine der verfügbaren Datenansichten vom **Geräte-Dashboard** auswählen.

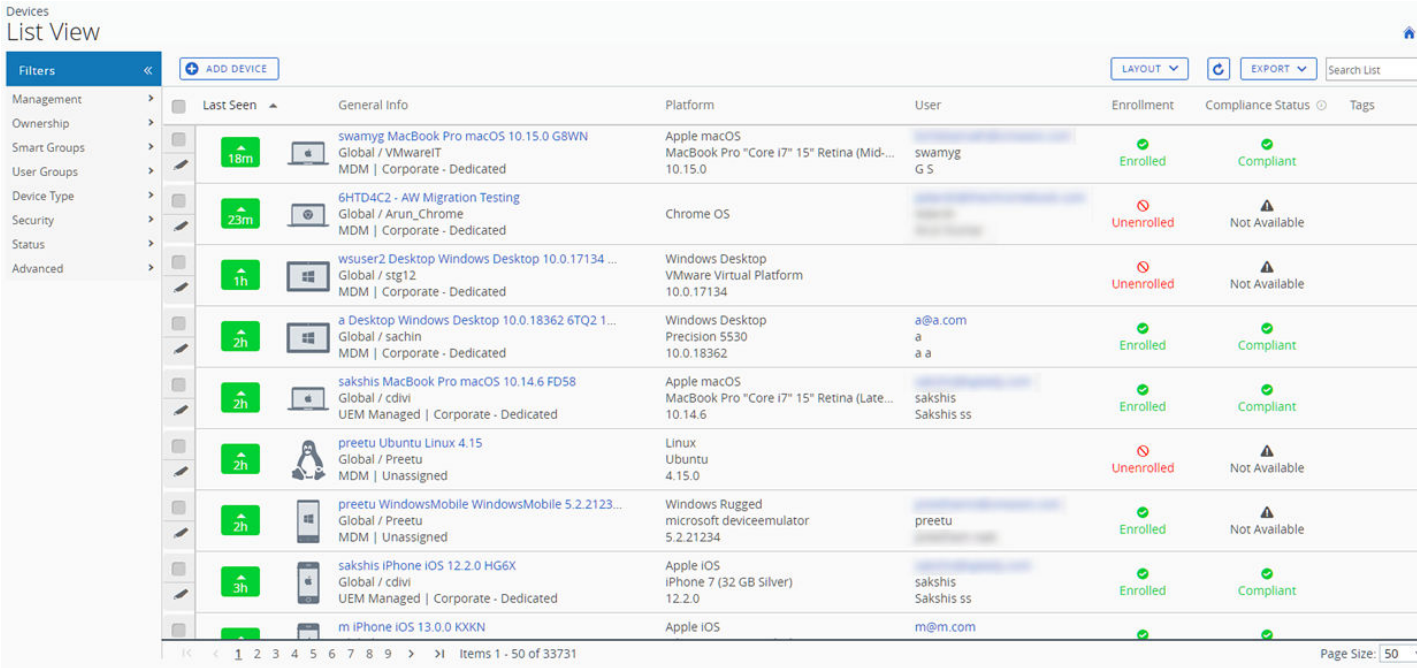
In dieser **Listenansicht** können Sie administrative Aktionen ausführen, wie Nachrichten senden, Geräte sperren, Geräte löschen und zum Gerät gehörende Gruppen ändern.

- **Sicherheit** – Sehen Sie die häufigsten Ursachen für Sicherheitsprobleme in Ihrer Geräteflotte ein. Wählen Sie ein Ringdiagramm. Daraufhin wird eine gefilterte **Gerätelistenansicht** mit den von dem ausgewählten Sicherheitsproblem betroffenen Geräten angezeigt. Falls die Plattform dies unterstützt, können Sie über eine Konformitätsrichtlinie Maßnahmen für diese Geräte ergreifen.
  - **Kompromittiert** – Anzahl und Prozentsatz der kompromittierten Geräte (mit Jailbreak oder Rootzugriff)) in Ihrer Bereitstellung.
  - **Keine Kennung** – Anzahl und Prozentsatz der Geräte ohne eine zur Sicherheit konfigurierte Kennung
  - **Keine Verschlüsselung** – Anzahl und Prozentsatz der nicht zur Sicherheit verschlüsselten Geräte. Die Android-SD-Kartenverschlüsselung wird in dieser gemeldeten Zahl nicht berücksichtigt. Nur Android Geräte, die über keine Festplattenverschlüsselung verfügen, werden in dem Ringdiagramm angezeigt.

  Besitz – Sehen Sie die Gesamtzahl der Geräte in allen Besitzkategorien ein. Wählen Sie einen Teil des Balkendiagramms aus. Daraufhin wird eine gefilterte **Gerätelistenansicht** mit den kompromittierten Geräten angezeigt, die von dem ausgewählten Besitztyp betroffen sind.
- **Übersicht „Zuletzt gesehen“ / Aufgliederung „Zuletzt gesehen“** – Sehen Sie Anzahl und Prozentsatz der Geräte ein, die vor kurzem mit dem Workspace ONE UEM MDM-Server kommuniziert haben. Wenn mehrere Geräte beispielsweise seit über 30 Tagen nicht gesehen wurden, wählen Sie das entsprechenden Balkendiagramm aus, um nur diese Geräte anzuzeigen. Sie können dann alle gefilterten Geräte auswählen und einen Abfragebefehl senden, damit die Geräte eingecheckt werden können.
- **Plattformen** – Sehen Sie die Gesamtzahl der Geräte in allen Geräteplattformkategorien ein. Wählen Sie ein Balkendiagramm. Daraufhin wird eine gefilterte **Listenansicht für Geräte** von kompromittierten Geräten unter der ausgewählten Plattform angezeigt.
- **Registrierung** – Sehen Sie die Gesamtzahl der Geräte in den einzelnen Registrierungskategorien ein. Wählen Sie ein Balkendiagramm. Daraufhin wird eine gefilterte **Listenansicht für Geräte** von kompromittierten Geräten mit dem ausgewählten Registrierungsstatus angezeigt.
- **Aufgliederung der Betriebssysteme** – Sehen Sie die Geräte in Ihrer Flotte auf Grundlage des Betriebssystems ein. Für jedes unterstützte Betriebssystem gibt es separate Diagramme. Wählen Sie ein Balkendiagramm. Daraufhin wird eine gefilterte **Listenansicht für Geräte** von kompromittierten Geräten mit der ausgewählten BS-Version angezeigt.

Gerätelistenansicht

Wählen Sie die Gerätelistenansicht in Workspace ONE UEM powered by AirWatch, um eine vollständige Auflistung aller Geräte in der momentan ausgewählten Organisationsgruppe einzusehen.



Die Spalte **Zuletzt gesehen** gibt an, vor wie vielen Minuten das Gerät zuletzt eingecheckt wurde. Je nach Dauer der Inaktivität des Geräts ist der Indikator rot oder grün. Der Standardwert ist 480 Minuten (8 Stunden). Sie können dies jedoch anpassen, indem Sie zu **Gruppen & Einstellungen > Alle Einstellungen > Geräte & Benutzer > Allgemein > Erweitert** navigieren und den Wert für **Zeitüberschreitung bei Geräteinaktivität (Min.)** ändern.

Wählen Sie jedes Mal, wenn Sie die Detailseite für dieses Gerät öffnen möchten, den erwarteten Anzeigenamen eines Geräts in der Spalte **Allgemeine Info**. Der **erwartete Anzeigename** ist die Bezeichnung, die Sie einem Gerät zuweisen, damit Sie es von anderen Geräten desselben Herstellers und Modells unterscheiden können.

Sortieren Sie nach Spalten, und konfigurieren Sie Informationsfilter, um Aktivitäten auf Grundlage bestimmter Informationen zu prüfen. So können Sie beispielsweise nach der Spalte **Konformitätsstatus** sortieren, um nur die Geräte anzuzeigen, die zurzeit nicht konform sind, und ausschließlich für diese Geräte Maßnahmen zu ergreifen. Durchsuchen Sie alle Geräte nach einem freundlichen Namen oder Benutzernamen, um ein Gerät oder einen Benutzer herauszufiltern.

Anpassen des Layouts der Gerätelistenansicht

Sie können die vollständige Liste sichtbarer Spalten in der **Gerätelistenansicht** anzeigen, indem Sie die Schaltfläche **Layout** und anschließend die Option **Benutzerdefiniert** wählen. In dieser Ansicht können Sie Spalten der Geräteliste nach Ihren Wünschen aus- und einblenden.

Sie haben auch die Möglichkeit, Ihre angepasste Spaltenansicht für alle Administratoren auf und unter der momentanen Organisationsgruppe (OG) anzuwenden. Sie können z. B. „Anlagennummer“ aus der **Geräteliste** der aktuellen Organisationsgruppe und aus allen untergeordneten Organisationsgruppen ausblenden.

Wenn Sie alle Anpassungen vorgenommen haben, wählen Sie die Schaltfläche **Akzeptieren**, um Ihre Spalteneinstellungen zu speichern und diese neue Spaltenansicht anzuwenden. Sie können jederzeit zu den Einstellungen für die Schaltfläche **Layout** zurückkehren und Ihre Spaltenanzeigeeinstellungen anpassen.

Nachfolgend einige wichtige benutzerdefinierte Layout-Spalten der Gerätelistenansicht:

- Android Management
- SSID (Service Set Identifier oder WLAN-Netzwerkname)
- WLAN MAC-Adresse
- WLAN-IP-Adresse
- Öffentliche IP-Adresse

Listenansicht exportieren

Wählen Sie die Schaltfläche **Export**, um eine XLSX- oder CSV-Datei (kommagetrennte Werte) der gesamten **Gerätelistenansicht** zu speichern, die dann mit MS Excel angezeigt und analysiert werden kann. Wenn Sie einen Filter auf die **Gerätelistenansicht** angewendet haben, enthält die exportierte Liste die gefilterten Ergebnisse.

Durchsuchen der Gerätelistenansicht

Sie können nach einem einzelnen Gerät suchen, um schnell auf dessen Informationen zuzugreifen und Remoteaktionen auf dem Gerät auszuführen.

Um eine Suche auszuführen, navigieren Sie zu **Geräte > Listenansicht**, wählen Sie die Leiste **Liste durchsuchen**, und geben Sie einen Benutzernamen, einen benutzerfreundlichen Gerätenamen oder ein beliebiges anderes Element zur Identifizierung des Geräts ein. Durch diese Aktion wird eine Suche auf allen Geräten mit Ihrem Suchparameter in der aktuellen Organisationsgruppe und in allen untergeordneten Gruppen gestartet.

Aktionsschaltflächen-Cluster für Gerätelistenansicht

Wenn ein oder mehrere Geräte in der Gerätelistenansicht ausgewählt sind, können Sie allgemeine Aktionen mit dem Aktionsschaltflächen-Cluster ausführen, einschließlich Abfragen, [Nachricht] Senden, Sperren und weitere Aktionen, auf die über die Schaltfläche **Weitere Aktionen** zugegriffen wird.

Die verfügbaren Geräteaktionen variieren je nach Plattform, Gerätehersteller, Modell, Registrierungsstatus sowie der jeweiligen Konfiguration von Workspace ONE UEM Console.

Remote Assist

Sie können eine **Remote Assist**-Sitzung auf einem einzelnen qualifizierenden Gerät starten, sodass Sie sich den Bildschirm remote anzeigen lassen und das Gerät steuern können. Diese Funktion ist ideal für die Fehlerbehebung und die Durchführung erweiterter Konfigurationen auf Geräten in Ihrer Geräteflotte.

Um diese Funktion verwenden zu können, müssen Sie die folgenden Anforderungen erfüllen:

- Sie müssen über eine gültige Lizenz für Workspace ONE Assist verfügen.
- Sie müssen ein Administrator mit einer zugewiesenen Rolle sein, die die entsprechenden Assist-Berechtigungen enthält.
- Die Assist-App muss auf dem Gerät installiert sein.
- Unterstützte Geräteplattformen:
  - Android
  - iOS
  - macOS
  - Windows 10
  - Windows Mobile

Aktivieren Sie das Kontrollkästchen links neben einem qualifizierten Gerät in der **Gerätelistenansicht**, und die Schaltfläche **Remote Assist** wird angezeigt. Wählen Sie diese Schaltfläche, um eine Remote-Assist-Sitzung zu beginnen.

Weitere Informationen finden Sie im Handbuch für **Workspace ONE Assist**, verfügbar unter docs.VMware.com.

Verwenden der Seite „Gerätedetails“ für iOS-Geräte

Verwenden Sie die Seite „Gerätedetails“, um detaillierte Geräteinformationen nachzuvollziehen und schnell auf Benutzer- und Geräteverwaltungsaktionen zuzugreifen.

So gelangen Sie zur Seite der Gerätedetails: Wählen Sie den Anzeigenamen eines Geräts auf der Seite **Listenansicht**, aus einem der verfügbaren Dashboards oder mit einem der Suchtools in der UEM-Konsole.

Anzeigen von Geräteinformationen

Verwenden Sie die Registerkarten des Menüs „Gerätedetails“, um auf bestimmte Geräteinformationen zuzugreifen, einschließlich:

- **Zusammenfassung** – Allgemeine Statistiken anzeigen, wie z. B.:
  - Konformität
  - Registrierungsstatus

- Zuletzt gesehen
- Plattform/Modell/Betriebssystem
- Verwaltung
- Überwachung
- Aktivierungssperre
- Mein iPhone suchen
- iCloud-Sicherung (halten Sie den Mauszeiger über den iCloud-Sicherungsstatus, um den letzten Sicherungsstatus anzuzeigen)
- Datenschutz
- Verschlüsselung
- Kontaktdaten
- Organisationsgruppe und Smartgroup
- Telefonnummer (für die Geräte wie z. B. iPhone XS, XR oder XS Max, die mehrere SIM-Karten einschließlich eSIM unterstützen, werden die Telefonnummern aller dem Gerät zugeordneten SIM-Karten angezeigt)
- Seriennummer, UDID und Asset-Nummer
- Status der Stromversorgung
- Speicherkapazität
- Verfügbare Updates des Betriebssystems (Geräte mit iOS 11 und höher)
- Informationen zum physischen Arbeitsspeicher und zum virtuellen Arbeitsspeicher und zur Garantie

  Wenn die Informationen von Apple Global Service Exchange zugänglich sind, wählen Sie den Garantie-Link, um zu sehen, wann der Status das letzte Mal aktualisiert wurde. Danach verwenden Sie die Schaltfläche **Aktualisieren**, um die neuesten Informationen zu erhalten.

  - Ein Enterprise Wipe oder Zurücksetzung des Geräts auf Werkseinstellungen fordert einen Aktivierungssperre-Umgehungscode an und wechselt dann in den Modus „Wipe ausstehend“ auf **überwachten** Geräten.
  - Wenn die Aktivierungssperre von „Mein iPhone suchen“ in iOS 7+-Geräten aktiviert ist, erscheint eine Warnung, sobald ein Befehl zum Geräte-Wipe auf einem **nicht überwachten** Gerät ausgeführt wird. Diese Warnung informiert Sie darüber, dass ein Gerät mit aktivierter Aktivierungssperre ohne originale Apple-ID und Kennwort nicht erneut aktiviert werden kann. Dies gilt auch, wenn Sie das Gerät komplett auf Werkseinstellungen zurücksetzen. Weitere Informationen finden Sie unter Überblick über die Aktivierungssperre .

- **Konformität**: Prüfen Sie Status, Richtlinienname, Datum der vorherigen und kommenden Konformitätsüberprüfung sowie die bereits auf dem Gerät ausgeführten Aktionen.

- **Profile**: Prüfen Sie alle derzeit auf einem Gerät installierten Profile.
- **Apps**: Zeigen Sie den App-Status, den App-Namen, den App-Typ (öffentlich oder intern), die App-Version, den App-Bezeichner und die Größe der App an. Für Geräte mit iOS 11.und höher zeigt die UEM-Konsole verfügbare Anwendungsaktualisierungen an (es wird angegeben, ob die installierte Version die neueste Version ist oder ob ein Update zur Verfügung steht) sowie die Anwendungsquelle (ob die Anwendung über den App-Store installiert, als Beta-Anwendung verteilt, Ad-hoc über ein Enterprise-Konto signiert oder unter Verwendung einer gerätebasierten VPP-Lizenz verwaltet wurde).

  Hinweis Aufgrund der Art und Weise, wie der Anwendungsstatus auf iOS-Geräten gemeldet wird, erreicht eine Anwendung den Status **Installiert** erst, wenn der Installationsvorgang vollständig abgeschlossen ist. Das heißt, wenn die Workspace ONE UEM console das Anwendungslistenbeispiel des Geräts abfragt und die Anwendung noch heruntergeladen wird, gibt die Anwendung den Status „Wird installiert“ aus. Bei einer erfolgreichen Anwendungsinstallation gibt das Gerät den Anwendungsstatus als **Installiert** aus, der in der Workspace ONE UEM console so markiert wird.

- **Updates** – Zeigen Sie die für das Gerät verfügbaren iOS-Updates an, einschließlich Betriebssystemversion, Produktschlüssel, Build-Version, letzte Aktualisierung, Download-Prozentsatz und Fortschrittsstatus.
- **Inhalte** – Prüfen Sie Status, Typ, Name, Priorität, Einsatz, letztes Update sowie Zeit und Datum der Ansichten. Diese Funktion bietet auch eine Symbolleiste für administrative Aktionen (Inhalte installieren oder deinstallieren).
- **Standort**: Prüfen Sie den aktuellen Standort oder Standortverlauf eines Geräts.
- **Benutzer**: Greifen Sie auf Informationen zum Benutzer eines Geräts sowie auf den Status der anderen für diesen Benutzer registrierten Geräte zu.

Auf die Registerkarten des Menüs unten greifen Sie über die Schaltfläche **Mehr** auf der Seite „Gerätedetails“ zu:

- **Netzwerk** – Prüfen Sie den aktuellen Netzwerkstatus eines Geräts (Mobilfunk, WLAN, Bluetooth). Für iOS 12.1 und neuere Geräte wie iPhone XS, XR oder XS Max, die mehrere SIM- und eSIM-Karten unterstützen, können Sie den Netzwerkstatus der SIM-Karten auf der UEM-Konsole anzeigen und verfolgen.
- **Sicherheit** – Prüfen Sie den aktuellen Sicherheitsstatus eines Geräts auf Grundlage der Sicherheitseinstellungen.
- **Restriktionen** – Zeigen Sie die Typen von Restriktionen an, die derzeit für das Gerät gelten.
- **Telekommunikation**: Prüfen Sie alle mit dem Gerät gesendeten und empfangenen Anrufe, Daten und Nachrichten.
- **Hinweise** – Prüfen Sie Hinweise bezüglich des Geräts, und fügen Sie solche Hinweise hinzu. Vermerken Sie beispielsweise den Versandstatus, oder dass sich das Gerät momentan in Reparatur befindet oder es außer Betrieb ist.

- **Zertifikate** – Identifizieren Sie Gerätezertifikate nach Name und Aussteller. Dieser Tab gibt auch Auskunft über den Ablauf des Zertifikats.
- **Nutzungsbedingungen**: Zeigen Sie eine Liste der Nutzungsbedingungen an, die bei der Registrierung des Geräts akzeptiert wurden.
- **Warnungen** – Prüfen Sie alle mit dem Gerät zusammenhängenden Warnungen.
- **Bücher** – Prüfen Sie alle internen Bücher auf dem Gerät.
- **Gemeinschaftsgeräteprotokoll** – Prüfen Sie den Verlauf bezüglich Gemeinschaftsgeräten, einschließlich vergangener Check-ins und Check-outs sowie des Status.
- **Restriktionen** – Prüfen Sie alle aktuell auf ein Gerät angewendeten Restriktionen. Dieser Tab zeigt bestimmte Restriktionen je nach Gerät, Anwendungen, Bewertungen und Kennung.
- **Statusverlauf** – Prüfen Sie den Geräteverlauf bezüglich des Registrierungsstatus.
- **Gezielte Protokollierung** – Prüfen Sie die Protokolle von Konsole, Katalog, Gerätediensten, Geräteverwaltung und Self-Service-Portal. Sie müssen die gezielte Protokollierung in den Einstellungen aktivieren. Zu diesem Zweck wird ein Link angegeben. Sie müssen dann die Schaltfläche **Neues Protokoll erstellen** auswählen und eine Zeitdauer für die Protokollerfassung auswählen.
- **Fehlerbehebung** – Prüfen Sie Protokollierungsinformationen unter **Ereignisprotokoll** und **Befehle**. Diese Seite enthält Export- und Suchfunktionen, die Ihnen gezielte Suchvorgänge und Analysen ermöglicht.
  - **Ereignisprotokoll** – Sehen Sie detaillierte Fehlerbehebungsinformationen und Server-Check-ins ein, einschließlich **Filter** nach **Ereignisgruppentyp**, **Datumsbereich**, **Schweregrad**, **Modul** und **Kategorie**.

    In der **Ereignisprotokoll**-Auflistung befinden sich in der Spalte **Ereignisdaten** eventuell Hypertextlinks, über die Sie weitere Details zum Ereignis in einem separaten Fenster anzeigen können. Diese Informationen ermöglichen Ihnen eine tiefgreifendere Fehlerbehebung, zum Beispiel bei der Nachforschung, warum ein Profil nicht installiert wurde.
  - **Befehle** – Sehen Sie eine detaillierte Auflistung ausstehender, in Warteschlange befindlicher und abgeschlossener Befehle, die an das Gerät gesendet wurden. Enthält einen **Filter**, mit dem Sie Befehle nach **Kategorie**, **Status** und einem bestimmten **Befehl** filtern können.
- **Anlagen** – Verwenden Sie diesen Speicherplatz auf dem Server für Screenshots, Dokumente, Anzeige der Hub-Protokolle, die von Intelligent Hub gesendet wurden, und Links zur Fehlerbehebung und für andere Zwecke, ohne dafür Speicherplatz auf dem Gerät in Anspruch zu nehmen.

Ausführen von Remoteaktionen

Die Dropdown-Liste **Weitere Aktionen** auf der Seite „Gerätedetails“ ermöglicht es Ihnen, Remoteaktionen Over-the-Air auf dem ausgewählten Gerät auszuführen. Es folgen detaillierte Informationen zu allen Fernaktionen. Die im Folgenden aufgeführten Aktionen hängen von bestimmten Faktoren ab, wie Geräteplattform, Einstellungen der UEM-Konsole und Registrierungsstatus.

- **Alle abfragen**: Senden Sie einen Abfragebefehl an das Gerät, um eine Liste aller installierten Anwendungen (einschließlich Workspace ONE Intelligent Hub, sofern zutreffend), Bücher, Zertifikate, Gerätedaten, Profile und Sicherheitsmaßnahmen zurückzugeben.
- **Geräteinformationen (Abfrage)**: Senden Sie einen MDM-Abfragebefehl an das Gerät, um Geräteinformationen wie Anzeigename, Plattform, Modell, Organisationsgruppe, Version des Betriebssystems und Besitzstatus zurückzugeben.
- **Sicherheit (Abfrage)**: Senden Sie einen MDM-Abfragebefehl an das Gerät, um eine Liste mit den aktiven Sicherheitsmaßnahmen (Gerätemanager, Verschlüsselung, Kennung, Zertifikate usw.) abzurufen.
- **Profile (Abfrage)** – Senden Sie einen MDM-Abfragebefehl an das Gerät, um eine Liste mit installierten Geräteprofilen zurückzugeben.
- **Anwendungen (Abfrage)**: Senden Sie einen MDM-Abfragebefehl an das Gerät, um eine Liste der installierten Anwendungen abzurufen.
- **Zertifikate (Abfrage)** – Senden Sie einen MDM-Abfragebefehl an das Gerät, um eine Liste der installierten Zertifikate zurückzugeben.
- **Kennung löschen (Restriktionseinstellung)** – Durch Löschen des Kennungsbefehls wird die Anmeldekennung auf dem Gerät gelöscht. Das Gerät muss überwacht werden.
- **Benutzerlisten (Abfrage)** – Ein Abfragebefehl wird an das Gerät gesendet, um eine Liste von Benutzern zu erhalten, die sich bei dem Gerät angemeldet haben (nur für freigegebene Geräte).
- **Gerät sperren** – Senden Sie einen MDM-Befehl, um ein ausgewähltes Gerät zu sperren. Es kann dann erst wieder verwendet werden, wenn es entsperrt wurde.
- **SSO sperren**: Sperren Sie den Zugriff auf den Workspace ONE UEM-Container und alle beteiligten Anwendungen für den Gerätebenutzer.
- **Enterprise Wipe** – Heben Sie die Registrierung eines Geräts auf und entfernen Sie alle verwalteten Unternehmensressourcen, einschließlich Anwendungen und Profile. Diese Aktion

kann nicht rückgängig gemacht werden. Eine erneute Registrierung ist zur Verwaltung dieses Geräts durch Workspace ONE UEM erforderlich. Diese Geräteaktion beinhaltet Optionen zur Vermeidung einer zukünftigen erneuten Registrierung und das Textfeld **Notizbeschreibung**, in das Sie Informationen über die Aktion hinzufügen können.

  - Enterprise-Löschung wird nicht für Geräte, die in Clouddomänen eingebunden sind, unterstützt.

- **iOS-Updates** – Wählen Sie einzelne Geräte oder Gerätesammlungen aus, um Updates an Geräte zu senden, die über Apple Business Manager registriert wurden.
- **Verwaltete Einstellungen** – Aktivieren oder deaktivieren Sie Sprachroaming, Datenroaming und private Hotspots.
- **Geräte-Wipe** – Senden Sie einen MDM-Befehl, um alle Daten und das Betriebssystem von einem Gerät zu entfernen. Dadurch wird das Gerät in einen Zustand versetzt, in dem die Wiederherstellungspartition benötigt wird, um das Betriebssystem neu zu installieren. Diese Aktion kann nicht rückgängig gemacht werden. Die Wiederherstellungspartition ist nur auf Mac-Geräten und nicht auf iOS-Geräten erforderlich.
  - Aspekte bei einer iOS-Geräte-Löschung
    - Bei Geräten mit iOS 11 und älteren Versionen werden durch den Befehl für die Geräte-Löschung darüber hinaus auch die Apple SIM-Daten gelöscht, die den Geräten zugeordnet sind.
    - Bei Geräten mit iOS 11 und höher besteht die Option zum Beibehalten des Apple SIM-Datentarifs (sofern auf den Geräten vorhanden). Aktivieren Sie dazu auf der Seite „Geräte-Wipe“ das Kontrollkästchen **Datentarif beibehalten**, bevor Sie den Wipe-Befehl senden.
    - Bei Geräten mit iOS 11.3 und höher besteht außerdem die Option, beim Senden des Wipe-Befehls das Überspringen des Bildschirms **Proximity einrichten** zu aktivieren oder zu deaktivieren. Wenn die Option aktiviert ist, wird der Bildschirm „Proximity einrichten“ im Setup-Assistenten übersprungen, sodass dem Gerätebenutzer die Option „Proximity einrichten“ nicht angezeigt wird.

Weitere Informationen zur Fehlerbehebung bei Geräte-Löschungen, zu diesbezüglichen Berechtigungen und zu Meldungen zu Geräte-Löschungen in der UEM-Konsole finden Sie im folgenden Artikel in der Workspace ONE UEM-Wissensdatenbank: https://support.workspaceone.com/articles/115012396488.

- **iOS-Updates** – Einlesen eines iOS-Updates auf ein Gerät, das nicht über DEP registriert wurde. Weitere Informationen finden Sie unter BS-Update Management.
- **eSIM aktualisieren** – Senden einer Abfrage an eine Carrier-eSIM-Server-URL, um die aktiven eSIM-Mobilfunktarifprofile auf dem Gerät zu aktualisieren.
- **Nachricht senden** – Senden Sie eine Nachricht an den Benutzer des ausgewählten Geräts. Wählen Sie zwischen **E-Mail**, **Push-Benachrichtigung** (über AirWatch Cloud Messaging) und **SMS**. Die Push-Benachrichtigung erfordert AirWatch-Anwendungen wie Hub, Boxer usw., die mindestens einmal gestartet worden sein müssen.
- **Geräte suchen**: Senden Sie eine Textnachricht an die entsprechende Workspace ONE UEM-Anwendung zusammen mit einem akustischen Ton, der dem Benutzer dabei helfen soll, ein falsch platziertes Gerät zu finden. Zu den akustischen Tonoptionen gehören eine konfigurierbare Anzahl an Wiederholungen des akustischen Tons sowie die Länge des Abstands zwischen den Tönen in Sekunden.
- **Geräte-Check-in anfordern** – Anforderung eines Check-ins des ausgewählten Geräts in der UEM-Konsole und Aktualisierung der Spalte **Zuletzt**. Durch diese Aktion wird auch die Geräteregistrierung auf den Staging-Benutzer zurückgesetzt.
- **Gerät synchronisieren** – Synchronisieren Sie das ausgewählte Gerät mit der UEM-Konsole, wodurch der Status **Zuletzt gesehen** angeglichen wird.
- **Remote-Ansicht**: Aktivieren Sie einen aktiven Stream der Geräteausgabe an ein Ziel Ihrer Wahl, damit Sie sehen können, was der Benutzer beim Betrieb des Geräts sieht. Zu den Zielparametern gehören IP-Adresse, Port, Audioport, Kennwort und Prüfungszeit.
- **Organisationsgruppe wechseln**: Ändern Sie die Startorganisationsgruppe des Geräts in eine andere, bereits vorhandene OG. Weist eine Option zum Auswählen einer statischen oder dynamischen OG auf.
  - Wenn Sie die Organisationsgruppe für mehrere Geräte gleichzeitig ändern möchten, müssen Sie Geräte für die Massenaktion mithilfe der Blockauswahlmethode (Umschalttaste verwenden) anstelle des Kontrollkästchens „Global“ (neben der Spalte mit der Überschrift „Zuletzt angezeigt“ in der Gerätelistenansicht) auswählen.
- **Tag hinzufügen**: Weisen Sie einem Gerät ein anpassbares Tag zu, das zur Identifizierung eines bestimmten Geräts in Ihrer Flotte verwendet werden kann.
- **Gerät bearbeiten**: Bearbeiten Sie Gerätedaten wie **Anzeigename**, **Anlagennummer**, **Gerätebesitz**, **Gerätegruppe** und **Gerätekategorie**.

- **Gerät löschen** – Löschen Sie ein Gerät und heben Sie die Registrierung dieses Geräts in der Konsole auf. Sendet den Enterprise Wipe-Befehl an das Gerät, das beim nächsten Einchecken gelöscht wird, und markiert das Gerät in der Konsole als **Wird gelöscht**. Wenn der Löschschutz auf dem Gerät deaktiviert ist, führt der ausgegebene Befehl sofort einen Enterprise Wipe durch und entfernt die Gerätedarstellung in der Konsole.
- **Aktivierungssperre aufheben** – Heben Sie die Aktivierungssperre auf einem iOS-Gerät auf. Ist die Aktivierungssperre aktiviert, so benötigt der Benutzer eine Apple-ID sowie ein Kennwort, bevor folgende Aktionen ausgeführt werden können: Deaktivieren von „Mein iPhone suchen“, Zurücksetzen des Geräts auf die Werkseinstellungen und Reaktivieren zur Benutzung des Geräts.
- **Gerät konfiguriert** – Senden Sie diesen Befehl, wenn ein Gerät im Status „Warten auf Konfiguration“ festgefahren ist.
- **Modus „Verloren“ aktivieren/deaktivieren**: Verwenden Sie diese Option zum Sperren eines Geräts und zum Senden einer Nachricht, Rufnummer oder SMS an den Sperrbildschirm. Der Endbenutzer des Geräts kann den Verloren-Modus nicht deaktivieren. Wenn ein Administrator den Modus „Verloren“ deaktiviert, kehrt das Gerät zur normalen Funktionalität zurück. Benutzer erhalten eine Nachricht, in der Sie darüber informiert werden, dass der Standort ihres Geräts freigegeben wurde. (Überwachte iOS 9.3+-Geräte)
  - **Gerätestandort anfordern** – Fragen Sie ein Gerät im Modus „Verloren“ ab und verwenden Sie die Registerkarte „Standort“, um das Gerät ausfindig zu machen. (Überwachte iOS 9.3+-Geräte)
- **Benutzer abmelden** – Melden Sie den Benutzer erforderlichenfalls vom Gerät ab.

Konfigurieren von benutzerdefinierten Befehlen und Ausführung dieser auf verwalteten Geräten

Mit Workspace ONE UEM können Administratoren benutzerdefinierte XML-Befehle auf verwalteten Apple-Geräten ausführen. Benutzerdefinierte Befehle ermöglichen eine präzisere Steuerung der Geräte in Ihrem Unternehmen.

Zudem können Sie mithilfe benutzerdefinierter Befehle Geräteaktionen unterstützen, die von der UEM-Konsole derzeit noch nicht unterstützt werden. Nutzen Sie die benutzerdefinierten Befehle nicht, um Befehle zu senden, die bereits über die Geräteaktionen der UEM-Konsole ausgeführt werden können. Beispiele für XML-Code, den Sie für benutzerdefinierte Befehle verwenden können, finden Sie in der Workspace ONE UEM-Wissensdatenbank unter https://kb.vmware.com/s/article/2960669.

Wichtig Beachten Sie bitte, dass das Senden eines falsch formatierten oder nicht unterstützten Befehls sich möglicherweise nachteilig auf Nutzbarkeit und Leistung der verwalteten Geräte auswirken wird. Testen Sie einen benutzerdefinierten Befehl zunächst an einem einzelnen Gerät, bevor Sie ihn auf zahlreichen Geräten gleichzeitig ausführen.

Verfahren

1. Navigieren Sie in der UEM-Konsole zu **Geräte > Listenansicht**.
2. Wählen Sie beliebig viele macOS- oder iOS-Geräte aus, indem Sie die Kontrollkästchen in der linken Spalte aktivieren.
3. Wählen Sie im Dropdown-Menü **Weitere Aktionen** die Option **Benutzerdefinierte Befehle**. Daraufhin wird das Dialogfenster für benutzerdefinierte Befehle geöffnet.
4. Geben Sie den XML-Code für die Aktion ein, die Sie bereitstellen möchten, und wählen Sie den Befehl **Senden** aus, um den Befehl auf Geräten bereitzustellen.

   Beispiele für XML-Code, den Sie für benutzerdefinierte Befehle verwenden können, finden Sie in der Workspace ONE UEM-Wissensdatenbank unter https://kb.vmware.com/s/article/2960669.

   Sollte der benutzerdefinierte Befehl nicht erfolgreich ausgeführt werden, löschen Sie den Befehl wie folgt. Navigieren Sie zu **Geräte > Listenansicht**. Wählen Sie das Gerät, auf dem Sie den Befehl ausgeführt haben. Wählen Sie in der **Detailansicht** des Geräts **Mehr > Fehlerbehebung > Befehle**. Wählen Sie zunächst den Befehl aus, den Sie entfernen möchten, und anschließend **Löschen**. Beachten Sie, dass Sie nur benutzerdefinierte Befehle löschen können, die mit dem Status „Ausstehend“ gekennzeichnet sind.

BS-Update Management

Mit dem System zur Verwaltung von Updates des Betriebssystems können Administratoren auf überwachten iOS-Geräten iOS-Updates blockieren und erzwingen, um eine einheitliche Verwaltung zu gewährleisten und dafür zu sorgen, dass auf allen Geräten dieselbe iOS-Version installiert ist. Durch die Verwaltung des Betriebssystems wird sichergestellt, dass Probleme der Gerätesicherheit mit iOS-Updates der Nebenversion behoben werden und die Geräte immer auf dem neuesten Stand sind.

Die Verwaltung von Updates des Betriebssystems ist eine ideale Lösung für Administratoren, um folgende Aspekte zu gewährleisten:

- Erkennung von neuen, von Apple veröffentlichten iOS-Updates auf Endbenutzergeräten sperren. Weitere Informationen zur Konfiguration von Restriktionsprofilen zum Blockieren von Endbenutzern finden Sie unter Restriktionsprofilkonfigurationen.
- Abrufen von Informationen über aktuelle, für Geräte verfügbare Patches/Updates.
- Veröffentlichen von iOS-Updates auf Endbenutzergeräten.

Funktionen der Verwaltung von iOS-Updates

Die wichtigsten verfügbaren Funktionen lauten:

- **Update sperren** – Konfigurieren Sie das Gerät so, dass es ein Update bis zu 90 Tage ab dem Veröffentlichungsdatum durch Apple nicht erkennt. Weitere Informationen zur Konfiguration von Restriktionsprofilen zum Blockieren von Updates finden Sie unter Restriktionsprofilkonfigurationen
- **Liste verfügbarer Updates** – Listet alle verfügbaren Updates von Apple und die Geräte auf, die für die entsprechenden Updates qualifiziert sind.
- **BS-Updateaktion** – Definieren Sie die Aktion zur Aktualisierung des Betriebssystems: nur Download, nur Installation oder sofortiger Download inklusive Installation.
- **Überwachen** – Zeigt den Status des Updates eines Betriebssystems auf zugewiesenen Geräten an.

Voraussetzungen für die Verwaltung von iOS-Updates

Bevor Sie auf verwalteten Geräten mit der Verwaltung von Updates des Betriebssystems über die UEM-Konsole beginnen, vergewissern Sie sich, dass die in diesem Abschnitt erläuterten Mindestanforderungen erfüllt sind.

Unterstützte Geräte

- iOS 11.3 und höher, überwacht
- Das Gerät muss über mindestens 50 Prozent Akkuladestand verfügen.

Netzwerkanforderungen

Informationen zur Netzwerkarchitektur und ihren Anforderungen finden Sie im Handbuch über die *Empfohlene Architektur*.

Anzeigen der verfügbaren iOS-Updates

Zeigen Sie für alle von Ihnen verwalteten und qualifizierten Geräte den aktuellen Stand der Liste der von Apple bereitgestellten aktuellen oder aktiven iOS-Updates an.

Gehen Sie zur Seite **Ressourcen** >**Geräte-Updates** >**iOS**, um die verfügbaren iOS-Updates sowie andere Details anzuzeigen, darunter:

- **Update** – Name des Updates.
- **Version** – Version des Updates.
- **Veröffentlichungsdatum** – Datum, an dem das Update veröffentlicht wird.
- **Ablaufdatum** – Datum, an dem das Update abläuft.
- **Update-Status** – Status des iOS-Updates, der angibt, ob es von Apple verfügbar gemacht wurde oder nicht.

- **Zuweisungen** – Anzahl der Zuweisungen, die auf ein Update angewendet werden.
- **Zuweisungsstatus** – Status der Zuweisungen, die auf das Update angewendet wurden, z. B. „Zugewiesen“, „Nicht zugewiesen“ oder „Angehalten“.

Hinweis Die Liste der iOS-Updatedetails wird von Apple mithilfe der Scheduler-Aufgabe „Geräte-Updates synchronisieren“ im angegebenen Intervall abgerufen, das in einem Intervall von 6 bis 24 Stunden ausgeführt wird (Datenabruf bei Apple).

Wählen Sie ein OS-Update von der Seite **Geräte-Updates** >**iOS** aus, um zusätzliche Informationen anzuzeigen. Im Abschnitt „Details“ werden die Details des Updates des Betriebssystems angezeigt (z. B. Versionsdetails, unterstützte Geräte usw.). Die Diagramme unterhalb des Abschnitts „Details“ enthalten folgende Informationen:

- **Gerätebereitschaft** – Stellt Informationen im Zusammenhang mit dem Update und den Geräten bereit, die in der Organisationsgruppe und darunter registriert sind. Dazu gehören Geräte, die für den Empfang des Updates qualifiziert sind, Geräte, die ungeeignet sind (z. B. nicht überwachte Geräte, inkompatible Hardware usw.), Geräte, die schon eine höhere Version besitzen, oder Geräte, die die ausgewählte Version bereits aufweisen.
- **Gerätestatus** – Stellt Informationen über den Status des Updates des Betriebssystems auf den zugewiesenen qualifizierten Geräten bereit. Dies umfasst Geräte, auf die das Update heruntergeladen wurde, auf denen das Update installiert wurde bzw. auf denen das Update mit einem angegebenen Fehlercode fehlgeschlagen ist.
- **Geräte** – Die Tabelle zeigt den Status der durch eine Zuweisung ausgelösten iOS-Updates auf qualifizierten und nicht qualifizierten Geräten an.

Durch Auswahl von **Zuweisungen verwalten** werden Updates der Geräte mithilfe von Smartgroups mit bevorzugten Bereitstellungsparametern zugewiesen. Weitere Informationen zur Zuweisung finden Sie unter Zuweisen und Veröffentlichen von iOS-Updates.

Zuweisen und Veröffentlichen von iOS-Updates

Um ein Update des Betriebssystems bereitzustellen, weisen Sie einem iOS-Update mindestens eine Smartgroup zu und veröffentlichen Sie es auf dem Gerät.

So weisen Sie Smartgroups zu und stellen die iOS-Updates bereit:

Verfahren

1. Gehen Sie zur Seite **Ressourcen** >**Geräte-Updates** > **iOS**.
2. Wählen Sie ein iOS-Update aus, indem Sie das entsprechende Optionsfeld auswählen. Oben auf der Seite wird die Option **Zuweisungen verwalten** angezeigt.
3. Wählen Sie **Zuweisungen verwalten** für die anzuzeigende Zuweisungsseite aus.
4. Wählen Sie **Neue Zuweisung** im Abschnitt **Zuweisung** aus. Die Seite **Zuweisung hinzufügen** wird angezeigt.

5 Geben Sie auf der Registerkarte **Definition** den Namen der Zuweisung ein, und wählen Sie mindestens eine Smartgroup aus. Wählen Sie **Weiter**.

6 Geben Sie auf der Registerkarte **Bereitstellung** Datum und Uhrzeit für den Beginn der Bereitstellung ein, und wählen Sie eine Bereitstellungsmethode aus. Die verfügbaren Bereitstellungsmethoden lauten:

Methode	Beschreibung
Herunterladen und installieren	Das iOS-Update wird heruntergeladen und auf dem Gerät installiert.
Nur herunterladen	Das iOS-Update wird nur heruntergeladen, aber nicht auf dem Gerät installiert.
Nur installieren	Die iOS-Updates werden nur dann auf dem Gerät installiert, wenn Sie bereits über MDM oder manuell heruntergeladen wurden.

7 Aktivieren oder deaktivieren Sie auf der Registerkarte **Benachrichtigung** die Benachrichtigung für den erfolgreichen Download- oder Installationsstatus, und geben Sie in das Feld **Push-Benachrichtigung** den Benachrichtigungstext ein.

8 Klicken Sie auf **Speichern**, um das iOS-Update zu veröffentlichen.

Ergebnisse

Die Zuweisung wird für das ausgewählte iOS-Update in der UEM console gespeichert, und alle zugewiesenen qualifizierten Geräte, die einchecken, erhalten das angegebene Update der iOS-Version. Der Status des iOS-Updates ändert sich in „Zugewiesen“, und der Status für zugewiesene Geräte kann auf der Seite „Updatedetails“ überwacht werden.

Hinweis Diese Einstellungen können jederzeit geändert werden, nachdem das Update veröffentlicht wurde.

Wenn für Geräte mehrere Zuweisungen von iOS-Updates vorliegen, werden Bereitstellungseinstellungen und iOS-Version mit der folgenden Priorität ausgewertet:

1 Neueste iOS-Version (iOS 13.3 hat z. B. Priorität gegenüber iOS 13.1).

2 Zuweisung mit der geringsten Distanz an oder oberhalb der Organisationsgruppe, bei der das Gerät registriert ist. (Wenn z. B. ein Gerät bei einer untergeordneten Organisationsgruppe registriert ist, übernimmt das Gerät die Zuweisung der untergeordneten Organisationsgruppe anstatt von einer übergeordneten Ebene. Dies gilt unter der Voraussetzung, dass sich die Zuweisungen auf dieselbe iOS-Version beziehen.)

3 Höchste Priorität innerhalb der ausgewählten Zuweisung, basierend auf den ersten beiden Kriterien mit einer aufsteigenden Priorität (Priorität 1 besitzt z. B. eine höhere Priorität als Priorität 2).

Anhalten und Fortsetzen von iOS-Updates

Als Administrator können Sie alle zugewiesenen Updates anhalten. Dadurch werden alle Updates, die noch nicht an iOS-Geräte gesendet wurden, solange unterbrochen, bis die Unterbrechung aufgehoben wird.

So halten Sie ein iOS-Update an:

Verfahren

1 Gehen Sie zur Seite **Ressourcen** > **Geräte-Updates** > **iOS**.

2 Wählen Sie ein zugewiesenes iOS-Update aus.

3 Wählen Sie oben auf der Seite die Option **PAUSE** aus.

Hinweis Durch diesen Vorgang werden keine Updates angehalten, die bereits auf dem Gerät verarbeitet wurden, z. B., wenn das Update bereits auf das Gerät heruntergeladen wurde. Stattdessen werden nur zugewiesene zukünftige Downloads von Updates angehalten.

Überwachen von Zuweisungen von iOS-Updates

Nachdem iOS-Updates Geräten zugewiesen und veröffentlicht wurden, besteht der nächste Schritt darin, Ihre Bereitstellung zu überwachen.

Um den Status einer Bereitstellung anzuzeigen, wählen Sie auf der Seite **Ressourcen** > **Geräte-Updates** > **iOS** ein iOS-Update aus, um weitere Informationen anzuzeigen. Im Abschnitt „Details“ werden die Details des iOS-Updates angezeigt (z. B. Versionsdetails, unterstützte Geräte usw.). Die Diagramme unterhalb des Abschnitts „Details“ dienen der Überwachung und Ergreifung von Maßnahmen für die zugewiesenen Geräte. Diese Diagramme zeigen:

- **Gerätebereitschaft** – Stellt Informationen im Zusammenhang mit dem Update und den Geräten bereit, die in der Organisationsgruppe und darunter registriert sind. Dazu gehören Geräte, die für den Empfang des Updates qualifiziert sind, Geräte, die ungeeignet sind (z. B. nicht überwachte Geräte, inkompatible Hardware usw.), Geräte, die schon eine höhere Version besitzen, oder Geräte, die die ausgewählte Version bereits aufweisen.
- **Gerätestatus** – Stellt Informationen über den Status des iOS-Updates auf den zugewiesenen, qualifizierten Geräten bereit. Dies umfasst Geräte, auf die das Update heruntergeladen wurde, auf denen das Update installiert wurde bzw. auf denen das Update mit einem angegebenen Fehlercode fehlgeschlagen ist.
- **Geräte** – Die Tabelle zeigt den Status des durch eine Zuweisung ausgelösten iOS-Updates auf qualifizierten und nicht qualifizierten Geräten an. Die Werte dieser Tabelle lauten:

Werte	Beschreibung
Zuletzt angezeigt	Das letzte Mal, dass das Gerät an Workspace ONE UEM geantwortet hat.
Gerätename	Der freundliche Name des Geräts

Werte	Beschreibung
Benutzer	Der Vor- und Nachname des Registrierungsbenutzers, der dem Gerät zugewiesen ist.
Status	Der aktuelle Status, der für das Update dieser iOS-Version empfangen wurde.
Ursache	Zusätzlicher Kontext für den Status eines Updates, wenn ein Fehler aufgetreten ist.
Nächster Wiederholungsversuch	Der geschätzte Zeitpunkt, zu dem das System bei einem Fehler versucht, das Update erneut an das Gerät zu senden. Dies kann häufiger als hier angegeben versucht werden.

Die Tabelle wird auch verwendet, um Aktionen für Geräte für das ausgewählte Update durchzuführen. Dies betrifft die folgenden Aktionen:

- **Abfrage** – Fordern Sie die aktuellen Informationen für das Gerät im Zusammenhang mit dem iOS-Update an.
- **Überschreiben** – Lösen Sie einen Download- und/oder Installationsbefehl für das Gerät aus. Dabei werden alle Zuweisungen ignoriert, die für das Gerät zuvor vorgenommen wurden.

Verwaltung von iOS-Updates für einzelne Geräte

Die Verwaltung von iOS-Updates kann als direkterer Ansatz auf der Ebene des einzelnen Geräts erfolgen, um sicherzustellen, dass auf ein verwaltetes Gerät die neuesten Updates und ihre Funktionalitäten angewendet werden. Diese Updates können für ein einzelnes Gerät bereitgestellt und überwacht werden, indem Sie zu **Geräte > Listenansicht > Gerät auswählen > Updates** navigieren.

Veröffentlichen von iOS-Updates für ein Gerät

So veröffentlichen Sie ein bestimmtes Update für ein ausgewähltes Gerät:

1 Wechseln Sie zur Registerkarte **Updates**, um den aktuellen Stand der verfügbaren Updates des Betriebssystems im Detail anzuzeigen.

2 Wählen Sie den Namen eines Updates des Betriebssystems aus, und klicken Sie auf **Veröffentlichen**. Die Seite **Update** wird angezeigt.

3 Wählen Sie die bevorzugte **Geräteinstallationsmethode** aus.

Hinweis Die Option **Herunterladen/Installieren** für Update-Zuweisungen führt entweder Download- oder Installationsaktionen aus, abhängig vom Update-Status des Betriebssystems auf dem Gerät.

Wenn das Update des Betriebssystems bereits heruntergeladen wurde, installiert der Befehl das Update des Betriebssystems. Wenn die Aktualisierung des Hosts jedoch noch nicht heruntergeladen wurde, führt der Befehl stattdessen zum Download. Senden Sie den Befehl erneut, nachdem der Download abgeschlossen ist, um die Installation auszulösen.

4 Wählen Sie **Senden** aus, um das Update des Betriebssystems auf dem Gerät zu veröffentlichen.

5 Wählen Sie **Updatefortschritt abfragen** aus, um den aktuellen Status für das Update anzufordern.

Hinweis Dies wirkt sich nicht auf die auf dem Gerät zugewiesenen iOS-Updates aus. Die Veröffentlichung von Zuweisungen auf Geräten wird so lange fortgesetzt, bis die Version der zugewiesenen iOS-Version entspricht oder jünger ist.

Verfolgen des Status von iOS-Updates

Der Status von iOS-Updates wird erst angezeigt, wenn Sie ein Update in der UEM-Konsole planen, unabhängig davon, ob Sie eine manuelle Veröffentlichung durchführen oder dem Gerät ein Update zuweisen. Wenn ein Update manuell auf ein iOS-Gerät heruntergeladen wird, wird der Status dieses Updates nicht in der Ansicht Liste **Updates** angezeigt. Sobald ein Administrator das Update plant, wird der Status in der Konsole aktualisiert. Wenn ein Update manuell installiert wird, wird dies in der Übersicht über die Gerätedetails angezeigt.

Problembehandlung

Alle Befehle und Antworten können in Ereignisdaten angezeigt werden. Navigieren Sie dazu zur Registerkarte **Gerätedetails** → **Mehr** → **Fehlerbehebung**.

iOS-Updates verzögern

Mithilfe eines Konfigurationsprofils können Administratoren iOS-Updates bis zu 90 Tage nach der Veröffentlichung des Updates durch Apple hinauszögern.

So zögern Sie ein iOS-Update hinaus:

Verfahren

1 Navigieren Sie zu **Ressourcen** > **Profile und Baselines Profile** > **Hinzufügen** .

2 Wählen Sie **Apple** > **iOS** aus, und konfigurieren Sie die Einstellungen für **Restriktionen**.

3 Wählen Sie im Unterabschnitt **Restriktionen bei BS-Updates** die Option **Verzögerung bei Updates (in Tagen)** aus.

4 Aktivieren Sie die Verzögerung von Updates und geben Sie die Anzahl der Tage an, um die das Software-Update verzögert werden soll. Anzahl der Tage reicht von 1 bis 90. Die Anzahl der Tage gibt die Dauer nach der Veröffentlichung des Software-Updates und nicht nach dem Zeitpunkt der Installation des Profils an.

Einrichten des Gerätenamens eines überwachten iOS-Geräts

Legen Sie automatisch oder manuell fest, dass der Name eines überwachten iOS 8+-Geräts mit dem Anzeigenamen in der UEM-Konsole übereinstimmt. Diese Funktion ist hilfreich, wenn es

darum geht, vom Gerät selbst Inventarnachverfolgung auszuführen. Der Gerätename erscheint, wenn das Gerät mit iTunes verbunden ist, und kann auch in iTunes bearbeitet werden.

Verfahren

1 Navigieren Sie zu **Gruppen & Einstellungen > Alle Einstellungen > Allgemein > Geräte & Benutzer > Anzeigename**.

2 Wählen Sie **Benutzerdefinierten freundlichen Namen des Smartphones aktivieren**, um den Gerätenamen als freundlichen Namen festzulegen.

3 Geben Sie das **Format des freundlichen Namens des Smartphones** an, indem Sie den Registrierungsbenutzer, das Gerätemodell und Informationen zum Betriebssystem des Geräts eingeben.

4 Wählen Sie die Einstellung **Gerätenamen auf Anzeigenamen festlegen**, um diesen Namen als Gerätenamen für den Anzeigenamen festzulegen.

5 Wählen Sie **Speichern**, um den Namen zu aktualisieren.

AppleCare GSX

Apple Global Service Exchange (GSX) ermöglicht es Administratoren, Gerätedetails in Bezug auf den Displaymodellnamen, den Gerätekauf und den Garantiestatus direkt aus der UEM-Konsole abzurufen.

Wenn Geräte in einer Organisationsgruppe keinen Displaymodellnamen haben, läuft ein Zeitplan in periodischen Abständen, um diese Namen anhand der GSX-Informationen, die für die Geräte auf dieser Ebene der Organisationsgruppe konfiguriert wurden, zu suchen und zu aktualisieren.

Nur autorisierte Apple-Mitarbeiter oder Organisationen, die sich beim Self-Servicing Account Program von Apple angemeldet haben, können auf GSX-Informationen zugreifen.

Erstellen eines GSX-Kontos

Bevor Sie Ihren Einsatz integrieren können, müssen Sie ein Apple GSX-Konto erstellen. Um ein GSX-Konto beantragen zu können, benötigen Sie einen Servicevertrag mit Apple. Wenden Sie sich an Ihren Apple Account Executive, um mehr über GSX zu erfahren.

Zum Beantragen eines GSX-Kontos besuchen Sie http://www.apple.com/support/programs/ssa/.

Erhalten Sie ein Apple-Zertifikat für die Integration von AppleCare GSX

Um AppleCare GSX in Ihre Workspace ONE UEM-Bereitstellung zu integrieren, müssen Sie zuerst ein Apple-Zertifikat erhalten und in das Format .p12 konvertieren.

Weitere Informationen finden Sie unter Erhalten Sie ein Apple-Zertifikat für die Integration von AppleCare GSX.

Konfigurieren von AppleCare in der UEM-Konsole

Nachdem Sie ein Apple-Zertifikat erhalten und konfiguriert haben, müssen Sie das Zertifikat in die UEM-Konsole hochladen und Ihre AppleCare-Instanz konfigurieren.

Weitere Informationen finden Sie unter Konfigurieren von AppleCare GSX in der UEM-Konsole.

Erhalten Sie ein Apple-Zertifikat für die Integration von AppleCare GSX

Um AppleCare GSX in Ihre Workspace ONE UEM-Bereitstellung zu integrieren, müssen Sie zuerst ein Apple-Zertifikat erhalten und in das Format .p12 konvertieren.

Verfahren

1. Erstellen Sie mithilfe von OpenSSL oder Java Keytool eine Zertifikatsignieranfrage (CSR).
2. Senden Sie die CSR und die folgenden GSX-Kontoinformationen an Apple, um Apple-Zertifikate (.pem-Dateien) zu erhalten.
   a. GSX-Käuferkontonummer
   b. Name des Hauptansprechpartners für IT
   c. E-Mail-Adresse des Hauptansprechpartners für IT
   d. Telefonnummer des Hauptansprechpartners für IT
   e. Ausgehende statische IP-Adresse des Servers, der Anforderungen an die GSX-Produktion sendet

      Wenn Ihre Umgebung auf dem AW SaaS gehostet wird, finden Sie die IP-Adresse in folgendem Dokument: https://support.air-watch.com/articles/115001662168. Wenn der IP-Adressbereich für Ihre Umgebung nicht in der Liste enthalten ist, öffnen Sie bitte ein Support-Ticket, damit unsere für den Netzwerkbetrieb zuständigen Mitarbeiter den Adressbereich einrichten können.

      Apple erstellt das Apple-Zertifikat (.pem) und sendet ein signiertes Zertifikat sowie ein Kettenzertifikat an Sie zurück. Um die spätere Verwendung zu vereinfachen, sollten Sie die Dateien „cert.pem“ und „chain.pem“ umbenennen.

      Möglicherweise erhalten Sie darüber hinaus eine Datei mit der Bezeichnung „issuer“ (Aussteller), die für diesen Vorgang jedoch nicht benötigt wird.

3 Konvertieren Sie die Apple-Zertifikate in das Format .p12.

   a Erstellen Sie eine .p12-Datei mithilfe des privaten Schlüssels und der Apple-Zertifikate, indem Sie folgenden Befehl ausführen:`sudo openssl pkcs12 –export –inkey privatekey.pem –in cert.pem –certfile chain.pem –out GSX_Cert.p12`

   b Das Zertifikat wird als .p12-Datei an dem von Ihnen angegebenen Speicherort gespeichert.

   Wenn Sie bei der Ausführung des Konvertierungsbefehls keinen Pfad vor dem Dateinamen angeben, wird die Datei in Ihrem Arbeitsverzeichnis gespeichert.

Konfigurieren von AppleCare GSX in der UEM-Konsole

Nachdem Sie ein Apple-Zertifikat erhalten und konfiguriert haben, müssen Sie das Zertifikat in die UEM-Konsole hochladen und Ihre AppleCare-Instanz konfigurieren.

Verfahren

1 Navigieren Sie zu **Gruppen & Einstellungen > Alle Einstellungen > Geräte & Benutzer > Apple > AppleCare**.

   Um eine GSX-Verbindung mit der UEM-Konsole herzustellen, müssen Sie ein GSX-Konto mit Manager-Zugangsberechtigungen, Zugriff auf Webdienste und Zugriff auf Serviceabdeckungs- und Garantieinformationen haben.

2 Geben Sie die **GSX-Einstellungen** mit folgenden Informationen ein:

Einstellung	Aktion
GSX-Benutzer-ID	Geben Sie die Benutzer-ID des Kontos ein.
GSX-Kennwort	Geben Sie das Kontokennwort ein.
Käuferkontonummer	Geben Sie die zehnstellige Dienstkontonummer ein. Diese Kontonummer finden Sie im GSX-Portal unten auf der Webseite.
Zeitzone	Verwenden Sie das Dropdown-Menü, um die gewünschte Zeitzone auszuwählen.
Sprache	Verwenden Sie das Dropdown-Menü, um eine Sprache auszuwählen.

3 Wählen Sie **Speichern**, um die Integration in AppleCare abzuschließen.

4 Navigieren Sie zur **Listenansicht**, wählen Sie ein Gerät aus und verwenden Sie das Menü **Mehr**, um Informationen über **AppleCare** in der UEM-Konsole zu finden.

5 Navigieren Sie zu **Konten** > **Administratoren** und ziehen Sie die Informationen aus dem Abschnitt **Details**.

6 Fügen Sie auf der Seite **Admin hinzufügen/bearbeiten** die GSX-Benutzer-ID hinzu und klicken Sie auf **Speichern**.

   Sie können jetzt GSX API-Aufrufe tätigen.

Gemeinschaftsgeräte

9

Die Funktionalität für Gemeinschafts-/Mehrbenutzergeräte in Workspace ONE UEM powered by AirWatch sorgt dafür, dass Sicherheit und Authentifizierung für jeden einzelnen Endbenutzer gewährleistet werden. Gemeinschaftsgeräte können auch nur bestimmten Endbenutzern den Zugriff auf vertrauliche Informationen erlauben.

Jedem Mitarbeiter in gewissen Organisationen ein Gerät zu geben, kann sich zum einem kostenintensiven Unterfangen entwickeln. Mit Workspace ONE UEM powered by AirWatch können Sie Mobilgeräte zur Nutzung durch mehrere Endbenutzer auf zwei Weisen einsetzen: mit einer einzigen festen Konfiguration für alle Endbenutzer oder mit einer eindeutigen Konfigurationseinstellung für jeden einzelnen Benutzer.

Bei der Verteilung von Gemeinschaftsgeräten müssen Sie die Geräte zuerst mit entsprechenden Anwendungseinstellungen und -restriktionen versehen, bevor Sie sie für Endbenutzer bereitstellen. Einmal bereitgestellt, verwendet Workspace ONE UEM einen einfachen An- oder Abmeldeprozess für freigegebene Geräte, in dem Endbenutzer zur Anmeldung einfach ihre Anmeldedaten für Verzeichnisdienste oder dedizierte Anmeldedaten eingeben. Von der Rolle des Endbenutzers hängt die Ebene des Zugriffs auf Unternehmensressourcen wie Inhalte, Funktionen und Anwendungen ab. Auf Basis dieser Rolle werden beim Anmelden des Endbenutzers automatisch die Funktionen und Ressourcen konfiguriert, die ihm dann nach der Anmeldung zur Verfügung stehen.

Die An- und Abmeldefunktionen sind innerhalb von Workspace ONE Intelligent Hub eigenständig. Die Eigenständigkeit stellt sicher, dass der Registrierungsstatus nie betroffen ist und dass das Gerät unabhängig davon verwalten wird, ob es verwendet wird oder nicht.

Gemeinschaftsgerätefunktionen sind auf Apple iPads, die in Apple Business Manager integriert sind, auch von vornherein möglich. Diese Funktionalität wird Gemeinsam genutzte iPads für Unternehmen genannt, nutzt die Managed Apple ID des Benutzers für die Anmeldung und findet im VMware Workspace One Intelligent Hub keine Anwendung für das Anmelden und Abmelden. Weitere Informationen zum Konfigurieren von Gemeinsam genutzte iPads für Unternehmen mit dem Apple Business Manager und zu den Schritten, um diese Funktionalität zu erreichen, finden Sie unter **Gemeinsam genutzte iPads für Unternehmen** im *Introduction to Apple Business Manager Guide*, der auf docs.VMware.com zur Verfügung steht.

Gemeinschaftsgeräte – Funktionalität

Es gibt grundlegende Funktionen im Bereich der Funktionalität und Sicherheit von Geräten, die auf mehrere Benutzer zutreffen müssen. Diese Funktionen bieten überzeugende Gründe, Gemeinschaftsgeräte als kosteneffiziente Lösung zur bestmöglichen Ausschöpfung von Unternehmensmobilität zu erwägen.

Funktionalität

- Individualisieren Sie das Benutzererlebnis des einzelnen Endbenutzers, ohne Unternehmenseinstellungen zu verlieren.
- Bei der Anmeldung auf einem Gerät wird das Gerät je nach Endbenutzerrolle und Organisationsgruppe (OG) mit bestimmten Unternehmenszugriffsrechten sowie Einstellungen, Anwendungen und Inhalten konfiguriert.
- Ermöglichen Sie einen eigenständigen An- und Abmeldevorgang in Workspace ONE Intelligent Hub oder Workspace ONE Access.
- Nachdem sich der Endbenutzer vom Gerät abgemeldet hat, werden die Konfigurationseinstellungen dieser Sitzung gelöscht. Danach kann sich ein anderer Endbenutzer an diesem Gerät anmelden.

Sicherheit

- Versehen Sie Geräte mit Einstellungen für Gemeinschaftsgeräte, bevor Sie diese den Endbenutzern zur Verfügung stellen.
- Endbenutzer können sich ohne Auswirkungen auf die Geräteregistrierung bei Workspace ONE UEM auf Geräten an- und abmelden.
- Endbenutzer können sich bei der Anmeldung über Verzeichnisdienste oder dedizierte Workspace ONE UEM Anmeldedaten authentifizieren.
- Authentifizieren Sie Endbenutzer mithilfe von Workspace One Access.
- Verwalten Sie ein Gerät sogar, wenn es nicht angemeldet ist.

Plattformen, die Gemeinschaftsgeräte unterstützen

Folgende Geräte unterstützen Funktionalität für Gemeinschafts-/ Mehrbenutzergeräte.

- Android 4.3 oder höher
- iOS-Geräte mit Workspace ONE Intelligent Hub 4.2 oder höher.
  - Weitere Informationen zum Anmelden und Abmelden bei gemeinsam genutzten iOS-Geräten finden Sie im Thema *Anmelden und Abmelden bei gemeinsam genutzten iOS-Geräten* im **iOS-Plattformhandbuch** unter docs.vmware.com.
- macOS-Geräte mit Workspace ONE Intelligent Hub 2.1 oder höher.

Dieses Kapitel enthält die folgenden Themen:

Festlegen der Gemeinschaftsgerätehierarchie

Obwohl dies rein optional ist, bietet eine Organisationsgruppe (OG) speziell für freigegebene Geräte viele Vorteile aufgrund von Mehrmandantenfähigkeit und geerbten Geräteeinstellungen.

Wenn Sie über eine große Anzahl von gemeinsam genutzten Geräten verfügen und diese unabhängig von den Einzelbenutzergeräten verwalten möchten, können Sie eine freigegebene gerätespezifische OG erstellen. Das Erstellen einer freigegebenen Gerätehierarchie in Ihrer OG-Struktur ist optional. Funktionen wie intelligente Gruppen und Benutzergruppen bedeuten, dass Sie sich nicht unbedingt auf das Design der OG-Hierarchie verlassen müssen, um die Geräteverwaltung zu vereinfachen.

Die Verwendung einer gemeinsam genutzten Geräte-OG (oder verschachtelter OGs) vereinfacht jedoch die Geräteverwaltung, da Sie die Gerätefunktionalität über Profile, Richtlinien und Gerätevererbung ohne den von einer intelligenten Gruppe oder einer Benutzergruppe benötigten Verarbeitungsaufwand standardisieren können.

Verfahren

1. Navigieren Sie zu **Gruppen und Einstellungen > Gruppen > Organisationsgruppen > Organisationsgruppendetails**.

   Hier wird eine OG angezeigt, die für Ihr Unternehmen steht.
2. Überprüfen Sie die Genauigkeit der angezeigten **Organisationsgruppendetails** und nehmen Sie mithilfe der verfügbaren Einstellungen die gewünschten Änderungen vor. Falls Sie Änderungen vornehmen, klicken Sie danach auf **Speichern**.
3. Wählen Sie **Untergeordnete Organisationsgruppe hinzufügen**.

4 Geben Sie für die OG auf der nächsthöchsten Ebene unter Ihrer Organisationsgruppe der höchsten Ebene folgende Informationen ein.

Einstellung	Beschreibung
Name	Geben Sie den Namen für die untergeordnete Organisationsgruppe (OG) ein, der angezeigt werden soll. Verwenden Sie nur alphanumerische Zeichen. Verwenden Sie keine Sonderzeichen.
Gruppen-ID	Geben Sie eine Bezeichnung für die OG ein, die Endbenutzer bei der Geräteanmeldung angeben müssen. Gruppen-IDs werden während der Registrierung von Gruppengeräten in der entsprechenden OG verwendet. Stellen Sie sicher, dass alle Benutzer, die Geräte gemeinsam nutzen, die **Gruppen-ID** erhalten, da diese möglicherweise zur Geräteanmeldung erforderlich ist (je nach Konfiguration der Gemeinschaftsgeräte). Wenn Sie sich nicht in einer lokalen Umgebung befinden, identifiziert die Gruppen-ID Ihre Organisationsgruppe über die gesamte gemeinsam genutzte SaaS-Umgebung hinweg. Aus diesem Grund müssen alle Gruppen-IDs eindeutig benannt sein.
Typ	Wählen Sie den vorkonfigurierten OG-Typ, der der Kategorie der untergeordneten OG entspricht.
Land	Wählen Sie das Land der OG.
Gebietsschema	Wählen Sie die Sprachenklassifikation für das ausgewählte Land.
Branche des Kunden	Diese Einstellung ist nur verfügbar, wenn für **Typ** „Kunde“ gewählt ist. Wählen Sie eine Option aus der Liste mit Kundenbranchen.
Zeitzone	Wählen Sie die Zeitzone für den Standort der Organisationsgruppe aus.

5 Erstellen Sie auf die gleiche Weise weitere Gruppen und Untergruppen, um die hierarchische Struktur Ihres Unternehmens auszubauen.

   a Wenn Sie eine **feste Organisationsgruppe** konfigurieren, achten Sie darauf, dass Sie nur eine Organisationsgruppe erstellen, über die sich Endbenutzer anmelden und abmelden.

   b Wenn Sie **Benutzer zur Eingabe bezüglich Organisationsgruppe auffordern** konfigurieren, achten Sie darauf, dass Sie alle Organisationsgruppen erstellen, über die sich die verschiedenen Endbenutzer anmelden bzw. abmelden müssen. Weitere Informationen finden Sie unter Konfigurieren von Gemeinschaftsgeräten.

6 Wählen Sie **Speichern**.

Konfigurieren von Gemeinschaftsgeräten

Ähnlich wie beim Staging eines Einzelbenutzergeräts ermöglicht Mehrbenutzerstaging (ein „Gemeinschaftsgerät“) den IT-Administratoren, Geräte zur Verwendung durch mehr als einen Benutzer bereitzustellen.

Verfahren

1 Navigieren Sie zu **Gruppen und Einstellungen > Alle Einstellungen > Geräte und Benutzer > Allgemein > Gemeinschaftsgerät**.

2 Wählen Sie **Überschreiben**, und füllen Sie den Abschnitt **Gruppierung** aus.

Einstellung	Beschreibung
Gruppen-ID-Zuweisungsmodus	Konfigurieren Sie Geräte mit einer der drei folgenden Methoden: ■ Wählen Sie **Benutzer zur Eingabe bezüglich Organisationsgruppe auffordern**, um festzulegen, dass der Endbenutzer bei jeder Anmeldung auf dem Gerät die Gruppen-ID für die Organisationsgruppe eingeben muss. Mit dieser Methode haben Sie die Flexibilität, Zugriff auf die Einstellungen, Anwendungen und Inhalte der eingegebenen Organisationsgruppe zu geben. Des Weiteren sind Endbenutzer nicht auf den Zugang zu den Einstellungen, Anwendungen und Inhalten der Organisationsgruppe beschränkt, bei der sie registriert sind. ■ Wählen Sie **Feste Organisationsgruppe**, um Ihre verwalteten Geräte auf die Einstellungen und Inhalte einzuschränken, die für eine einzelne Organisationsgruppe gelten. Jeder Endbenutzer, der sich auf einem Gerät anmeldet, hat Zugriff auf dieselben Einstellungen, Anwendungen und Inhalte. Diese Methode ist beispielsweise in einem Anwendungsfall für den Einzelhandel vorteilhaft, wo Mitarbeiter Geräte für ähnliche Zwecke, wie Bestandsprüfung, gemeinsam benutzen. ■ Wählen Sie **Benutzergruppen-Organisationsgruppe**, um Funktionen basierend sowohl auf Benutzergruppen als auch Organisationsgruppen in der gesamten Hierarchie zu aktivieren. Wenn sich ein Endbenutzer bei einem Gerät anmeldet, hat er Zugang zu spezifischen Einstellungen, Anwendungen und Inhalten basierend auf ihren jeweils zugewiesenen Rollen in der Hierarchie. Ein Endbenutzer gehört beispielsweise zur Benutzergruppe „Verkauf“ und diese Benutzergruppe ist der Organisationsgruppe „Standardzugriff“ zugeordnet. Bei der Anmeldung des Benutzers wird das Gerät mit den Einstellungen, Anwendungen und Inhalten konfiguriert, die für die Organisationsgruppe „Standardzugriff“ verfügbar sind. Sie können Benutzergruppen in der UEM-Konsole bestimmten Organisationsgruppen zuordnen. Navigieren Sie zu **Gruppen & Einstellungen > Alle Einstellungen > Geräte und Benutzer > Allgemein > Registrierung**. Wählen Sie den Tab **Gruppierung**, und geben Sie die erforderlichen Details ein.
Nutzungsbedingungen immer einblenden	Fordert Endbenutzer dazu auf, Ihre **Nutzungsbedingungen** zu akzeptieren, bevor sie sich bei einem Gerät anmelden.

3 Füllen Sie gegebenenfalls den Abschnitt **Sicherheit** aus.

Einstellung	Beschreibung
Gemeinschaftsgeräte-Passcode verlangen	Verlangt, dass Benutzer im Self-Service-Portal eine Gemeinschaftsgerätekennung erstellen, um Geräte auszuchecken. Diese Kennung unterscheidet sich von einer Single Sign-On-Kennung oder einer Kennung der Geräteebene.
Sonderzeichen verlangen	Legen Sie fest, dass Kennungen für Gemeinschaftsgeräte Sonderzeichen wie @, %, & usw. enthalten müssen.
Minimallänge für Gemeinschaftsgerätekennung	Legen Sie die minimale Zeichenlänge der Gemeinschaftsgerätekennungen fest.

Einstellung	Beschreibung
Ablaufzeit (in Tagen) der Gemeinschaftsgeräte kennungen	Legen Sie die Zeit (in Tagen) fest, nach der die Gemeinschaftsgerätekennung ablaufen soll.
Gemeinschaftsgeräte kennung für Minimalzeit (in Tagen) beibehalten	Legen Sie einen Mindestzeitraum (in Tagen) fest, für den eine Kennung für Gemeinschaftsgeräte mindestens gültig sein muss.
Anwender auffordern,, ihr Gemeinschaftsgeräte-Passcode x (Tage) vor Ablauf zu ändern	**(Nur für iOS-Geräte)** Legen Sie fest, wie viele Tage vorher der Benutzer daran erinnert wird, seine Gemeinschaftsgerätekennung zu ändern, bevor dieser verfällt. Legen Sie am besten einen Wert fest, der niedriger als die Differenz zwischen Ablaufzeit und Mindestzeit ist, in der Sie die Gemeinschaftsgerätekennung beibehalten können.
Kennungsverlauf	Legen Sie die Anzahl der Kennungen fest, die vom System gespeichert werden, um die Sicherheit der Umgebung dadurch zu erhöhen, dass der Benutzer ältere Kennungen nicht erneut verwenden kann.
Automatische Abmeldung	Legen Sie fest, dass Benutzer nach einer bestimmten Zeitspanne automatisch abgemeldet werden.
Automatische Abmeldung nach	Legen Sie die Zeitspanne fest, die verstreichen muss, bevor die Funktion **Automatisches Abmelden** aktiviert wird. Diese können Sie in **Minuten**, **Stunden** oder **Tagen** angeben.
iOS-Einzel-App-Modus	Aktivieren Sie dieses Kontrollkästchen, um den Einzelanwendungsmodus zu konfigurieren. Dadurch wird das Gerät auf eine einzige Anwendung beschränkt, wenn sich ein Endbenutzer auf dem Gerät anmeldet. Um ein iOS-Gerät im Einzelanwendungsmodus auszuchecken, müssen sich Endbenutzer mit ihren Anmeldedaten anmelden. Wenn das Gerät erneut eingecheckt wird, kehrt es in den Einzelanwendungsmodus zurück. Durch die Aktivierung des Einzelanwendungsmodus wird auch die Starttaste auf dem Gerät deaktiviert. **Hinweis** Der Einzelanwendungsmodus wird nur auf überwachte iOS-Geräte angewendet.

4 Konfigurieren Sie gegebenenfalls die **Abmelde-Einstellungen**.

Einstellung	Beschreibung
Android App-Daten löschen	Löschen Sie die Anwendungsdaten, wenn sich der Benutzer von einem gemeinsam genutzten Gerät abmeldet (eincheckt).
Android-Apps neu installieren	Verwenden Sie das Dropdown-Menü, um auszuwählen, ob die Anwendung bei Benutzerwechseln immer oder nie neu installiert werden soll. Bei Android (Legacy)-Bereitstellungen können Sie die APP neu installieren, wenn der Hub bei Benutzerwechseln keine Anwendungsdaten löschen kann.
Android-Gerätekennung löschen	Diese Einstellung steuert, ob die aktuelle Android-Gerätekennung gelöscht wird, wenn der Benutzer ein von mehreren Benutzern verwendetes Gerät abmeldet (eincheckt).
iOS-Gerätekennung löschen	Diese Einstellung steuert, ob die aktuelle iOS-Gerätekennung gelöscht wird, wenn der Benutzer ein von mehreren Benutzern verwendetes Gerät abmeldet (eincheckt).

5 Wählen Sie **Speichern**.

Nächste Schritte

Spezifische Informationen zur Bereitstellung von Geräten für Einzelbenutzergeräte- und Mehrbenutzergeräte-Staging finden Sie in in den Themen auf Bereitstellen eines Einzelbenutzergeräts (Staging) und Bereitstellen eines Mehrbenutzergeräts (Staging).

Anmelden bei und Abmelden von iOS-Gemeinschaftsgeräten

Sie können sich bei einem iOS-Gerät an- und abmelden, das von mehreren Benutzern verwendet wird.

Verfahren

1 Führen Sie den Workspace ONE Intelligent Hub auf dem Gerät aus.

2 Geben Sie die Anmeldedaten des Endbenutzers ein.

Wenn das Gerät bereits beim Workspace ONE Intelligent Hub angemeldet ist, wird der Benutzer dazu aufgefordert, eine SSO-Kennung einzugeben. Ist das Gerät nicht angemeldet, wird der Benutzer dazu aufgefordert, seinen Benutzernamen und sein Kennwort einzugeben. Die den einzelnen Benutzern zugeordneten Profile werden per „Push“ und je nach Smartgroup- und Benutzergruppenzugehörigkeit übertragen.

Hinweis Wenn **Benutzer zur Eingabe bezüglich Organisationsgruppe auffordern** aktiviert ist, müssen Endbenutzer zur Anmeldung auf dem Gerät eine **Gruppen-ID** eingeben.

3 Wählen Sie **Anmelden** und akzeptieren Sie die **Nutzungsbedingungen**.

Hinweis Wenn Benutzer zur Eingabe einer Kennung aufgefordert werden, können sie eine im Self-Service-Portal erstellen. Diese Kennungen haben eine Ablaufdauer. Wenn der Ablauftermin näher rückt, fordert Workspace ONE Intelligent Hub die Benutzer auf, die Kennung auf dem Gerät zu ändern. Wenn Benutzer ihre Kennung vor dem Ablauftermin nicht ändern, müssen sie zum Self-Service-Portal zurückkehren, um eine neue Kennung zu erstellen.

Nächste Schritte

Um sich von einem iOS-Gerät abzumelden, führen Sie Workspace ONE Intelligent Hub aus, und wählen Sie unten die Option **Abmelden**.

iOS-Funktionalität: „Überwacht“ im Vergleich zu „Nicht überwacht“ 10

Die folgende Tabelle zeigt alle verfügbaren iOS-Profilfunktionen, die Sie über die UEM-Konsole steuern können, sowie die erforderliche Mindestversion von iOS.

Funktionen und Funktionalität	Erfordert keine Überwachung	Erfordert Überwachung	Anmerkungen bzgl. BS
Kennung			
Kennungseinstellungen	✓		-
WLAN			
WLAN-Einstellungen	✓		-
AutoVerknüpfung	✓		iOS 7
Einstellungen des WLAN Hotspot 2.0	✓		iOS 7
Proxyeinstellungen	✓		iOS 7
QoS-Markierungs-Richtlinie	✓		iOS 10
VPN			
VPN-Einstellungen	✓		-
Pro-App VPN	✓		iOS 7
Automatisch verbinden	✓		iOS 7
E-Mail			
E-Mail-Einstellungen	✓		-
Verschieben von Nachrichten verhindern	✓		iOS 7
Aktuelle Kontaktsynchronisierung deaktivieren	✓		iOS 7
Verwendung in Drittanbieteranwendungen verhindern	✓		iOS 7
S/MIME verwenden	✓		iOS 7
Exchange ActiveSync			
EAS-Einstellungen	✓		-
S/MIME verwenden	✓		iOS 7
Pro-Nachricht S/MIME	✓		iOS 8
Verschieben von Nachrichten verhindern	✓		iOS 7

Funktionen und Funktionalität	Erfordert keine Überwachung	Erfordert Überwachung	Anmerkungen bzgl. BS
Verwendung in Drittanbieteranwendungen verhindern	✓		iOS 7
Aktuelle Kontaktsynchronisierung deaktivieren	✓		iOS 7
Mail Drop verhindern	✓		iOS 9
Standardmäßige Anrufanwendung	✓		iOS 10
LDAP			
LDAP-Einstellungen	✓		-
CalDAV			
CalDAV-Einstellungen	✓		-
Abonnierte Kalender			
Einstellungen für abonnierten Kalender	✓		-
CardDAV			
CalDAV-Einstellungen	✓		-
Webclips			
Webclipeinstellungen	✓		-
Anmeldedaten			
Anmeldedaten-Zertifikatseinstellungen	✓		-
SCEP			
SCEP-Einstellungen für Zertifizierungsstelle	✓		-
Globaler HTTP-Proxy			
Einstellungen für globalen HTTP-Proxy		✓	iOS 7
Einzelanwendungsmodus			
Einzelanwendungsmodus – Gerät auf eine einzige Anwendung beschränken		✓	iOS 7
Optionale Einstellungen für "Gerät auf eine einzige Anwendung beschränken"		✓	iOS 7
Autonomer Einzelanwendungsmodus		✓	iOS 7
Webinhaltsfilter			
Einstellungen für Webinhaltsfilter (Whitelist, Blacklist, Zulässige URLs)		✓	iOS 7
Webinhaltsfilter mit Drittanbieter		✓	iOS 8
Verwaltete Domänen			
Verwaltete E-Mail-Domänen	✓		iOS 8
Verwaltete Web-Domänen	✓		iOS 8
Verwaltete Safari-Kennwortdomänen	✓		iOS 9.3

Funktionen und Funktionalität	Erfordert keine Überwachung	Erfordert Überwachung	Anmerkungen bzgl. BS
Netzwerknutzungs-Regeln			
Regeln zur Netzwerknutzung	✓		iOS 9
macOS-Serverkonten			
macOS-Serverkonten	✓		iOS 9
Single Sign-On			
Single Sign-On-Einstellungen mit Kerberos-Authentifizierung	✓		iOS 7
Single Sign-On-Einstellungen mit Erneuerungszertifikaten	✓		iOS 8
AirPrint			
AirPrint-Zieleinstellungen	✓		iOS 7
AirPlay Mirroring			
AirPlay-Zieleinstellungen (Whitelist)		✓	iOS 7
AirPlay-Kennwörter	✓		
Access Point			
Erweiterte Zugriffspunkteinstellungen	✓		
Anwendunginstallations-Einstellungen			
Unbeaufsichtigte Anwendunginstallation		✓ +VPP	
Mobilfunkeinstellungen kontrollieren			
Sprachroaming	✓	✓	iOS 7
Datenroaming	✓	✓	iOS 7
Persönlicher Hotspot	✓	✓	iOS 7
Hintergrundbildeinstellungen			
Sperrbildschirmbild festlegen		✓	iOS 7
Nachricht bezüglich Bildschirmsperre festlegen		✓	iOS 9.3+
Startseitenbild festlegen		✓	iOS 7
Startseiten-Layout festlegen		✓	iOS 9.3+
Benachrichtigungen			
Einstellungen für Benachrichtigungen		✓	iOS 9.3+
Abfragen und Befehle			
Überwachungsstatus	✓		iOS 7
Status des persönlichen Hotspots	✓		iOS 7
Aktivierungssperre aufheben		✓	iOS 7
Kennungsrestriktionen löschen		✓	iOS 8

Funktionen und Funktionalität	Erfordert keine Überwachung	Erfordert Überwachung	Anmerkungen bzgl. BS
iOS-Updates konfigurieren		✓	iOS 9 Vor iOS 10.3 ist auch DEP erforderlich.
iOS-Updates verzögern		✓	iOS 11.3+
Benutzerdefinierte Schriftarten und Messaging			
Installation von benutzerdefinierten Schriftarten	✓		iOS 7
Benutzerdefinierte Registrierungsnachrichten	✓		iOS 7
Benutzerdefinierte MDM-Eingabeaufforderungen	✓		iOS 7
Aktivierungssperrwarnung	✓		iOS 7