Översikt av driftsättning av iOS i företag

iPad och iPhone kan förändra din verksamhet och hur dina medarbetare jobbar. De kan öka produktiviteten avsevärt och ge medarbetarna frihet och flexibilitet att jobba på nya sätt. Det här nya sättet att arbeta kan innebära fördelar för hela organisationen. Användarna får bättre tillgång till information, så de känner att de har större inflytande och kan lösa problem på kreativa sätt. IT-avdelningar som har stöd för iOS kan ge användarna tillgång till de bästa verktygen för deras arbete och samtidigt hålla företagsdata skyddade. I slutändan tjänar alla på det, med entusiastiska medarbetare och nya affärsmöjligheter överallt.

Det här dokumentet ger råd om viktiga saker att tänka på för att få ut mesta möjliga av din iOS-driftsättning. Följande ämnen tas upp:

- Driftsättningsmodeller
- Förberedning av infrastrukturen
- Första inställning
- Konfiguration och hantering
- Distribution av appar och böcker
- Löpande hantering
- Supportalternativ

Driftsättningsmodeller

Att utvärdera olika driftsättningsmodeller och välja den som passar bäst för din organisation är ett viktigt första steg. Det finns flera olika driftsättningsmetoder beroende på vem som äger enheterna och vilket scenario du föredrar. Börja med att utvärdera och identifiera de bästa driftsättningsmodellerna för din organisation.

Det finns tre vanliga driftsättningsscenarion för iOS-enheter inom större organisationer:

- Anpassade enheter (BYOD)
- Anpassade enheter (företagsägda)
- Icke-anpassade enheter (delade)

De flesta organisationer föredrar en viss modell, men det kan hända att flera modeller används i din miljö. Till exempel kan en detaljhandelskedja driftsätta en strategi med anpassade enheter (BYOD) så att medarbetarna kan ställa in iPad-enheter för eget bruk samtidigt som företagsresurser skyddas och hanteras utan att det påverkar användarens privata appar och data. Ute i butikerna kanske man däremot driftsätter en strategi med icke-anpassade enheter (delade), där iPad-enheterna delas av flera medarbetare som hanterar kundtransaktioner.

Genom att utforska de olika modellerna ingående kan du hitta den som passar bäst för just din miljö och sedan välja lämpliga program och verktyg i den tekniska referensguiden för driftsättning av iOS som du hittar online.

Teknisk referensguide för driftsättning av iOS: https://help.apple.com/deployment/ios

Anpassade enheter (BYOD)

En BYOD-driftsättning, som är det vanligaste scenariot, innebär att användarna själva ställer in sina enheter med sina Apple-ID:n. För att få tillgång till företagsresurser kan användarna konfigurera inställningar manuellt, installera en konfigurationsprofil eller, som är det vanligaste, registrera sina enheter med en Mobile Device Management-lösning (MDM).

En fördel med att använda MDM till att registrera personliga enheter är att företagsresurser och -data då kan hanteras på ett säkert sätt, samtidigt som användarens data och appar förblir privata. IT-avdelningen kan styra inställningar, övervaka policyefterlevnad och ta bort data och appar som tillhör företaget utan att röra personlig information och appar.

Följande schema visar de olika ansvarsområdena för både administratören och användaren i en BYOD-driftsättning.

Förberedning av infrastrukturen

Administratör:

- Utvärdera den befintliga infrastrukturen, inklusive Wi-Fi, VPN och e-post- och kalenderservrar.
- Undersök, köp in och driftsätt en MDM-lösning, till exempel Profilhanteraren.
- Registrera dig för programmet för volyminköp (VPP).

Användare:

- Packa upp och aktivera enheten.
- Skapa Apple-ID:n samt konton för iTunes Store och iCloud (om tillämpligt).

Installera och konfigurera

Administratör:

- Registrera enheter med självbetjäningsfunktionen: konfigurera konton, inställningar och begränsningar trådlöst med hjälp av MDM baserat på användar-/gruppolicyer som utarbetats av institutionen.
- Alternativt kan organisationer ge användarna tillgång till inställningar för enskilda konton medan policyer kan skickas via Exchange eller installeras med hjälp av en konfigurationsprofil.

Användare:

- Registrera med MDM.
- Inställningar och konfigurationer för enheter tas emot automatiskt från MDM.
- Användarna kan också installera konfigurationsprofiler manuellt eller konfigurera inställningar som du ger dem tillgång till.

Distribution av appar och böcker

Administratör:

- Köp appar och böcker via VPP och tilldela dem till användare med MDM.
- Skicka VPP-inbjudningar till användare. Om du använder inlösenkoder distribuerar du dem via mejl eller en intern webbplats.
- Distribuera interna appar från iOS Developer Enterprise Program (iDEP) och interna böcker genom att publicera dem på en webbserver eller med din MDM-lösning.
- Installera Caching Server så går det snabbare att leverera innehåll över det lokala nätverket.

Användare:

- Godkänn inbjudan till VPP.
- Ladda ner och installera appar och böcker som institutionen har tilldelat dig.

Löpande hantering

Administratör:

- Återkalla appar och tilldela dem till nya användare efter behov med MDM.
- Med MDM kan en administratör begära att hanterade enheter övervakar regelefterlevnad eller skickar varningar om användare lägger till appar eller innehåll som inte godkänts.
- MDM kan också låsa enheter eller återställa lösenord på dem, fjärradera hanterade konton eller data samt radera allt innehåll på en enhet.

Användare:

- Säkerhetskopiera enheten till iTunes eller iCloud för att spara dokument och annat privat innehåll.
- Om enheten tappas bort eller blir stulen kan användaren söka rätt på den med hjälp av Hitta min iPhone.
- När MDM-anslutningen tas bort raderas hanterade konton och data, men användarens privata appar, böcker, data och innehåll finns kvar.

Anpassade enheter (företagsägda)

Du kan också använda modellen med anpassade enheter om du driftsätter iOS-enheter som ägs av organisationen. IT-avdelningen kan konfigurera enheterna med grundinställningar innan de delas ut till användarna eller, som med BYOD, tillhandahålla anvisningar eller konfigurationsprofiler som användarna själva kan tillämpa.

Användarna kan också själva registrera enheten med en MDM-lösning som skickar organisationens inställningar och appar trådlöst. Om enheterna köpts direkt från Apple eller en medverkande Apple-auktoriserad återförsäljare eller operatör kan du också dra nytta av programmet för enhetsregistrering (DEP) för att automatiskt registrera nya enheter i din MDM-lösning. När enheterna väl konfigurerats kan användarna anpassa dem med egna appar och data utöver eventuella företagskonton eller appar som tillhandahålls av organisationen.

Följande schema visar de olika ansvarsområdena för både administratören och användaren i en driftsättning med anpassade enheter (företagsägda):

Förberedning av infrastrukturen

Administratör:

- Utvärdera den befintliga infrastrukturen, inklusive Wi-Fi, VPN och kalender- och e-postservrar.
- Undersök, köp in och driftsätt en MDM-lösning, till exempel Profilhanteraren.
- Registrera dig för DEP och VPP.

Användare:

- Skapa Apple-ID:n samt konton för iTunes Store och iCloud (om tillämpligt).

Installera och konfigurera

Administratör:

- Länka företagets virtuella servrar till företagets MDM-lösning via webbplatsen för DEP.
- Förenkla registreringen via programmet för enhetsregistrering genom att tilldela enheter till de virtuella MDM-servrarna efter beställnings- eller serienummer.
- Välj ut enheter i DEP som ska användas till att övervaka och förenkla registreringen i MDM.
- Konfigurera och övervaka enheten med hjälp av Apple Configurator (alternativ till ovannämnda).
- Konfigurera och installera konton, inställningar och begränsningar trådlöst med MDM eller använd USB med Apple Configurator.

Användare:

- Användaren får en iOS-enhet. Om enheten ställdes in med hjälp av Apple Configurator behöver användaren inte göra några fler inställningar.
- Ange institutionens inloggningsuppgifter i inställningsassistenten för DEP (valfritt).
- Anpassa enheten med hjälp av inställningsassistenten och ange ett personligt Apple-ID.
- Registrera med MDM.
- Inställningar och konfigurationer för enheter tas emot automatiskt från MDM.

Distribution av appar och böcker

Administratör:

- Köp appar och böcker via VPP och tilldela dem till användare med MDM.
- Ladda ner organisationens token från VPP-butiken och länka den till MDM-lösningen.
- Skicka VPP-inbjudningar till användare. Om du använder inlösenkoder distribuerar du dem via mejl eller en intern webbplats.
- Distribuera interna appar från iOS Developer Enterprise Program (iDEP) och interna böcker genom att publicera dem på en webbserver eller med din MDM-lösning.
- Installera Caching Server så går det snabbare att leverera innehåll över det lokala nätverket.

Användare:

- Godkänn inbjudan till VPP.
- Ladda ner och installera appar och böcker som du har tilldelats av organisationen.
- Appar kan installeras automatiskt på användarens enhet.

Löpande hantering	
Administratör:	**Användare:**
• Återkalla appar och tilldela dem till nya användare efter behov med MDM. • Med MDM kan en administratör begära att hanterade enheter övervakar regelefterlevnad eller skickar varningar om användare lägger till appar eller innehåll som inte godkänts. • MDM kan också låsa enheter eller återställa lösenord på dem, fjärradera hanterade konton eller data samt radera allt innehåll på en enhet.	• Säkerhetskopiera enheten till iTunes eller iCloud för att spara dokument och annat privat innehåll. • Om enheten tappas bort eller blir stulen kan användaren söka rätt på den med hjälp av Hitta min iPhone.

Icke-anpassade enheter (delade)

För enheter som delas av flera personer eller som används i ett enda syfte (till exempel på en restaurang eller ett hotell) brukar IT-administratörer vanligtvis konfigurera och hantera enheterna centralt istället för att låta användarna själva ställa in dem. I driftsättningsscenarion med icke-anpassade enheter har användarna som regel inte tillstånd att installera appar eller lagra privata data på enheten.

Icke-anpassade enheter registreras vanligtvis i en MDM-lösning och övervakas med hjälp av Apple Configurator. Det gör det möjligt att uppdatera eller återskapa innehållet på enheten om det ändrats av en användare.

Följande schema visar de olika ansvarsområdena för både administratören och användaren i en driftsättning med icke-anpassade enheter (delade):

Förberedning av infrastrukturen	
Administratör:	**Användare:**
• Utvärdera den befintliga infrastrukturen, inklusive Wi-Fi, VPN och kalender- och e-postservrar. • Undersök, köp in och driftsätt en MDM-lösning, till exempel Profilhanteraren. • Registrera dig för programmet för volyminköp (VPP).	• Inga åtgärder krävs i det här skedet.
Installera och konfigurera	
Administratör:	**Användare:**
• Packa upp och förse eventuellt enheten med en serviceetikett. • Konfigurera och övervaka enheterna med hjälp av Apple Configurator. • Registrera enheterna i MDM med hjälp av Apple Configurator (valfritt). • Använd Apple Configurator eller MDM för att installera konton, inställningar och begränsningar.	• Inga åtgärder krävs i det här skedet.
Distribution av appar och böcker	
Administratör:	**Användare:**
• Köp appar och böcker via VPP och driftsätt dem med hjälp av inlösenkoder så kan du installera och hantera dem med Apple Configurator. • Distribuera interna appar från iOS Developer Enterprise Program (iDEP) med hjälp av Apple Configurator. • Distribuera interna böcker genom att publicera dem på en webbserver eller med din MDM-lösning. • Lägg till Apple Configurator för böcker precis som för appar.	• Inga åtgärder krävs i det här skedet.

Löpande hantering	
Administratör: • Uppdatera iOS på enheten med Apple Configurator. • Återställ regelbundet enheterna till standard-konfigurationen med hjälp av Apple Configurator. • Med MDM kan du begära att hanterade enheter övervakar regelefterlevnad eller skickar varningar om användare lägger till appar eller innehåll som inte godkänts. • MDM kan också låsa enheter eller återställa lösenord på dem, fjärradera hanterade konton eller data samt radera allt innehåll på en enhet. • Tänk på att regelbundet säkerhetskopiera Mac-datorn med Apple Configurator eftersom VPP-inköp hanteras lokalt. • MDM kan övervaka enheter med hjälp av enappsläget.	**Användare:** • Inga åtgärder krävs i det här skedet.

Förberedning av infrastrukturen

Efter att du har valt lämplig driftsättningsmodell går du igenom den befintliga infrastrukturen för att se till att organisationen drar full nytta av allt som iOS har att erbjuda. iPhone och iPad kan smidigt integreras i de flesta vanligt förekommande IT-miljöerna i företag. Det kan dock finnas sätt att optimera nätverksmiljön så att den stöder viktiga tekniker i iOS.

Wi-Fi och nätverk

Kontinuerlig och tillförlitlig åtkomst till ett trådlöst nätverk är avgörande för att ställa in och konfigurera iOS-enheter. Bekräfta att företagets Wi-Fi-nätverk har stöd för flera enheter med samtidiga anslutningar från alla användare. Du kan behöva konfigurera företagets webbproxyserver eller brandvägg om enheterna inte kan ansluta till Apples aktiveringsservrar, iCloud eller iTunes Store.

Undersök VPN-infrastrukturen för att se till att användarna har säker fjärråtkomst till företagets resurser på sina iOS-enheter. Överväg att använda funktionen VPN On Demand i iOS så att en VPN-anslutning bara öppnas vid behov. Om du planerar att använda VPN per app måste du se till att VPN-nätverksnoderna stöder den här funktionen och att du har tillräckligt med licenser för att täcka rätt antal användare och anslutningar.

Se även till att företagets nätverksinfrastruktur fungerar med Bonjour, Apples standardbaserade, konfigurationsfria nätverksprotokoll. Bonjour gör det möjligt för enheter att automatiskt hitta tjänster i ett nätverk. iOS-enheter använder Bonjour för att ansluta till AirPrint-kompatibla skrivare och AirPlay-kompatibla enheter, som Apple TV. Vissa appar använder Bonjour för att upptäcka andra enheter för samarbete och delning.

Mer information om Wi-Fi och nätverk i företagsmiljöer finns i den tekniska referensguiden för iOS-driftsättning. Bilaga A, ”Wi-Fi-infrastruktur”, förklarar vilka trådlösa tekniker och standarder som används av iOS-enheter och innehåller information om planering av trådlösa nätverk.

Den tekniska referensguiden för iOS-driftsättning finns på webben: www.help.apple.com/deployment/ios

Läs mer om Bonjour: www.apple.com/se/support/bonjour

E-post, kontakter och kalendrar

Om du använder Microsoft Exchange bör du kontrollera att ActiveSync-tjänsten är uppdaterad och konfigurerad så att den stöder alla användare i nätverket. Om du använder den molnbaserade Office 365-tjänsten bör du se till att det finns tillräckligt med licenser för det förväntade antalet anslutna iOS-enheter. Om du inte använder Exchange kan du ändå använda iOS med standardbaserade servrar som stöder IMAP, POP, SMTP, CalDAV, CardDAV och LDAP.

Mobile Device Management (MDM)

Du kan konfigurera och hantera iOS-enheter trådlöst med hjälp av en MDM-lösning (Mobile Device Management). MDM ger organisationer möjlighet att på ett säkert sätt registrera enheter i en företagsmiljö, konfigurera och uppdatera inställningar trådlöst, övervaka policyefterlevnad, driftsätta appar och böcker samt fjärradera eller fjärrlåsa hanterade enheter.

En rad olika MDM-lösningar från tredje part finns tillgängliga för olika typer av serverplattformar. Hanteringskonsoler, funktioner och prissättning skiljer sig åt mellan de olika lösningarna. Innan du väljer en lösning bör du gå igenom resurserna som listas nedan och avgöra vilka hanteringsfunktioner som är viktigast för din organisation.

Utöver tredjepartslösningarna har Apple en egen MDM-lösning som ingår i OS X Server: Profilhanteraren. Med Profilhanteraren är det enkelt att konfigurera iOS-enheter så att de har organisationens inställningar. Profilhanteraren använder tre komponenter: ett webbaserat administratörsverktyg, en självbetjäningsportal där användare kan registrera enheter och en MDM-server.

Läs mer om Mobile Device Management på: www.apple.com/ipad/business/it/management.html

Läs mer om Profilhanteraren på: www.apple.com/se/osx/server/features/#profile-manager

Caching Server

Funktionen Caching Server, som ingår i OS X Server, sparar en lokal kopia av innehåll som ofta efterfrågas från Apples servrar, vilket minskar bandbredden som behövs för att ladda ner innehåll i ditt nätverk. Caching Server snabbar upp ner- och uppladdning av mjukvara via App Store, Mac App Store, iTunes Store och iBooks Store. Den kan även cachelagra mjukvaruuppdateringar för snabbare nerladdning till iOS-enheter.

Läs mer om Caching Server: www.apple.com/se/osx/server/features/#caching-server

Stöd för iTunes

Enheter med iOS 5 eller senare kräver inte iTunes, men du kanske vill stöda det så att användarna kan aktivera enheter, synkronisera medier eller säkerhetskopiera sina enheter till en dator.

iTunes stöder flera olika konfigurationsalternativ för driftsättning som passar för användning inom organisationer, till exempel är det möjligt att förhindra åtkomst till olämpligt innehåll, definiera vilka nätverkstjänster användare har tillgång till via iTunes samt bestämma om användarna ska kunna installera nya mjukvaruuppdateringar.

Läs mer om att driftsätta iTunes: help.apple.com/iosdeployment/itunes

Första inställning

Efter att ha förberett infrastrukturen måste du driftsätta iOS-enheter till användarna. Den första enhetsinställningen kan göras på flera olika sätt, beroende på vem som äger enheten och vilken driftsättningsmodell du föredrar. Undersök de olika möjligheterna innan du sätter igång.

Inställningsassistent

Användare kan aktivera sina enheter direkt efter att de har packat upp dem, konfigurera grundinställningar och börja jobba direkt med Inställningsassistent i iOS. Förutom att göra grundinställningar kan användarna även anpassa andra inställningar, till exempel språk, plats, Siri, iCloud och Hitta min iPhone. Med inställningsassistenten kan användarna också skapa ett personligt Apple-ID om de inte har något. När enheterna har registrerats i programmet för enhetsregistrering (DEP) kan de automatiskt registreras i MDM direkt i inställningsassistenten.

Konfigurera enheter med Apple Configurator

Om enheterna inom organisationen hanteras centralt av IT-avdelningen och inte ställs in av användarna kan du använda Apple Configurator för att snabba aktivera enheter, definiera och tillämpa konfigurationer, övervaka enheter, installera appar och uppdatera enheter till den senaste versionen av iOS. Apple Configurator är en kostnadsfri app för OS X som kan laddas ner från Mac App Store. Enheterna måste anslutas till en Mac via USB när du utför dessa åtgärder. Du kan också återskapa en säkerhetskopia till enheterna med appdata, enhetsinställningar och hemskärmslayout.

Apple-ID

Ett Apple-ID är en identifikationsmetod som används för att logga in till en rad Apple-tjänster, såsom FaceTime, iMessage, iTunes Store, App Store, iBooks Store och iCloud. Dessa tjänster ger användarna tillgång till ett brett utbud av innehåll som hjälper dem att effektivisera affärsuppgifter, öka produktiviteten och utöka samarbetet.

För att få ut så mycket som möjligt av de här tjänsterna ska användarna helst logga in med sitt eget Apple-ID. Om de inte har något kan de skapa ett innan de får en enhet eller använda den inbyggda inställningsassistenten i iOS. Det är ett enkelt och smidigt sätt för användarna att skapa ett Apple-ID direkt från en iOS-enhet. Användarna behöver inte något bankkort för att skapa ett Apple-ID.

Om enheterna inte anpassas av användarna, till exempel vid driftsättningar med delade enheter, kan Apple Configurator användas för att installera appar och innehåll på flera enheter med ett enda administratörs-Apple-ID.

Läs om hur du skapar ett Apple-ID på: appleid.apple.com/se

iCloud

Med iCloud kan användare automatiskt synka dokument och personligt innehåll, som kontakter, kalendrar, dokument och bilder, och hålla allt uppdaterat på flera enheter.* Användare kan också säkerhetskopiera en iOS-enhet automatiskt om den är ansluten till Wi-Fi och använda Hitta min iPhone för att leta rätt på en borttappad eller stulen iPhone, iPad, iPod touch eller Mac.

En del tjänster, exempelvis Bildström, iCloud-nyckelring, iCloud Drive och Säkerhetskopia kan avaktiveras genom begränsningar som antingen ställs in manuellt på enheten eller centralt via konfigurationsprofiler. En MDM-lösning kan också förhindra att hanterade appar säkerhetskopieras till iCloud. Användarna kan då dra nytta av fördelarna med iCloud för personliga data samtidigt som företagsinformationen hålls utanför molnet. Data från företagskonton, såsom Exchange, eller data som lagras i interna företagsappar säkerhetskopieras inte heller till iCloud.

Obs! iCloud är inte tillgängligt överallt och funktionerna i iCloud kan variera beroende på område.

Läs mer om iCloud på: www.apple.com/se/icloud

Konfiguration och hantering

När enheterna har ställts in för att tas i bruk finns det flera olika alternativ för att konfigurera och hantera åtkomst till företagstjänster. IT-avdelningen kan antingen distribuera konfigurationsprofiler eller ställa in enheter på distans via MDM. För övervakade enheter finns det ytterligare konfigurationsalternativ.

Konfigurationsprofiler

En konfigurationsprofil är en XML-fil som gör det möjligt att distribuera konfigurationsinformation till en iOS-enhet. Konfigurationsprofiler automatiserar konfigurering av inställningar, konton, begränsningar och inloggningsuppgifter. Konfigurationsprofiler kan installeras via en e-postbilaga, laddas ner från en webbsida eller installeras på enheter via Apple Configurator. Om du behöver konfigurera många enheter eller helt enkelt föredrar en enkel trådlös driftsättningsmodell kan du tillhandahålla konfigurationsprofiler via MDM.

Konfigurera enheter med MDM

MDM ger organisationer möjlighet att säkert registrera och konfigurera enheter som ägs av medarbetare och av organisationen i arbetsmiljön. Med en MDM-lösning kan IT-administratörer konfigurera och uppdatera inställningar, övervaka att företagspolicyer efterlevs och fjärradera eller fjärrlåsa hanterade enheter. MDM kan också användas till att konfigurera appar som köpts via programmet för volyminköp eller utvecklats internt.

För att möjliggöra hantering registreras enheterna med en MDM-server med hjälp av en konfigurationsprofil för registrering. Användarna kan registrera sig direkt, men MDM-registreringen kan också automatiseras för företagsägda enheter via programmet för enhetsregistrering. Så fort en administratör initierar en MDM-policy, ett alternativ eller ett kommando skickas en notis om åtgärden till iOS-enheten via tjänsten Apple Push Notification (APNs) så att enheten kan kommunicera direkt med MDM-servern via en säker anslutning. Om enheten har nätverksåtkomst kan den ta emot APNs-kommandon överallt i världen. Däremot överförs ingen konfidentiell eller företagsintern information via APNs.

Övervakade enheter

Övervakning erbjuder en högre grad av enhetshantering för företagsägda enheter, vilket gör det möjligt att införa ytterligare begränsningar som avaktivering av iMessage eller Game Center och förbud för användare att ändra kontoinställningar. Från början är alla iOS-enheter oövervakade. Du kan kombinera övervakning med fjärrhantering via MDM och sköta ytterligare inställningar och begränsningar. Tack vare programmet för enhetsregistrering kan övervakningen aktiveras trådlöst på enheten under inställningen eller via Apple Configurator.

Programmet för enhetsregistrering

Programmet för enhetsregistrering (DEP) gör det möjligt för organisationer som har köpt iOS-enheter direkt från Apple eller en medverkande Apple-auktoriserad återförsäljare eller operatör att enkelt registrera dem i MDM och ställa in, konfigurera och övervaka enheter trådlöst. Tack vare programmet för enhetsregistrering kan alla organisationens enheter konfigureras istället för att varje enhet hanteras individuellt.

Processen är enkel: efter att organisationen har gått med i programmet loggar administratörerna in på programmets webbplats, länkar programmet till organisationens MDM-server och tilldelar användare enheter. När användarna har fått enheter kan de köra inställningsassistenten på sina enheter. Eventuella MDM-angivna konfigurationer, begränsningar eller kontroller installeras automatiskt.

Läs mer om programmet för enhetsregistrering: www.apple.com/business/dep

Apple Configurator

Med Apple Configurator, en kostnadsfri OS X-app som finns på Mac App Store, kan administratörer ställa in och konfigurera flera iOS-enheter samtidigt via USB innan de delas ut till användarna. Verktyget gör det möjligt för IT-personalen att snabbt konfigurera och uppdatera flera enheter till den senaste versionen av iOS, konfigurera enhetsinställningar och begränsningar samt installera appar och innehåll.

Apple Configurator passar perfekt för scenarion där användare delar iOS-enheter som behöver uppdateras med rätt inställningar, policyer, appar och data. Innan du hanterar inställningar, policyer och appar med MDM kan du använda Apple Configurator för att aktivera enhetsövervakning som ger dig tillgång till fler begränsningar och kontroller.

Läs mer om Apple Configurator: help.apple.com/configurator/mac

Distribution av appar och böcker

Apple erbjuder omfattande program som hjälper din organisation att dra nytta av de suveräna apparna och innehållet som finns tillgängligt för iOS. Det gör det möjligt att leverera appar och innehåll direkt till medarbetarnas enheter trådlöst och ge dem tillgång till allt de behöver för att jobba effektivt.

Programmet för volyminköp (VPP)

Programmet för volyminköp (VPP) gör det möjligt för företag att köpa stora mängder av olika iOS-appar och böcker samt distribuera dem till sina medarbetare.

Du kan också skaffa anpassade B2B-appar för iOS som har byggts särskilt för organisationen av tredjepartsutvecklare och som du kan köpa privat via VPP-butiken. Utvecklare som är registrerade i iOS Developer Enterprise Program kan skicka in appar för B2B-distribution via iTunes Connect, samma process som användas för att skicka in andra appar till App Store.

MDM-lösningar integrerar med VPP och kan användas till att distribuera appar och böcker till användare. Om en användare inte längre behöver vissa appar kan du återkalla dem via MDM och tilldela dem till en annan användare. Varje app är automatiskt tillgänglig för nerladdning på alla användarenheter, utan extra kostnad eller arbetsinsatser. Organisationen kan också köpa inlösenkoder via VPP för användning med Apple Configurator.

Läs mer om programmet för volyminköp: www.apple.com/se/business/vpp

iOS Developer Enterprise Program

Utveckla interna iOS-appar för användning av ditt företag via iOS Developer Enterprise Program. Programmet erbjuder en fullständig och integrerad process för utveckling, testning och distribution av interna iOS-appar för medarbetare i organisationen. Interna appar skickas inte till App Store och granskas, godkänns och förmedlas inte heller av Apple.

Du kan distribuera interna appar antingen genom att publicera dem på en intern webbserver eller genom att använda en MDM- eller apphanteringslösning från tredje part. Fördelarna med att hantera interna appar med MDM är bland annat att du kan konfigurera appar på distans, hantera versioner, konfigurera engångsinloggning, ange policyer för nätverksåtkomst (till exempel VPN per app) och bestämma vilka appar som kan användas till att exportera dokument. Vilken lösning som kommer att fungera bäst beror på organisationens specifika krav, infrastruktur och nivån på apphanteringen.

Läs mer om iOS Developer Enterprise Program samt utveckling och driftsättning av interna iOS-appar: developer.apple.com/programs/ios/enterprise/

Distribuera appar och böcker via hanterad distribution

MDM-servrar kan driftsätta både App Store-appar och internutvecklade företagsappar trådlöst. Både avgiftsbelagda och kostnadsfria App Store-appar kan hanteras av en MDM-server med hjälp av hanterad distribution via VPP. Se avsnittet Programmet för volyminköp ovan för mer information om hanterad distribution med MDM.

Du kan installera appar som köpts via VPP på tre olika sätt. Användare med egna enheter får en uppmaning av MDM att installera appen från App Store med sina personliga Apple-ID:n. På övervakade enheter som är registrerade med MDM installeras appen automatiskt. Om enheten inte är knuten till MDM kan användarna installera betalappar med en inlösenkod. Appen knyts sedan till användarens personliga Apple-ID.

Installera appar och innehåll med Apple Configurator

Utöver att göra grundläggande inställningar och konfigureringar kan du också använda Apple Configurator till att installera appar och innehåll. Det behövs oftast i situationer där Apple Configurator övervakar en enhet som inte ska anpassas av användaren. När du konfigurerar enheter med Apple Configurator kan du installera kostnadsfria appar, betalappar med inlösenkoder, interna appar samt dokument. Du kan också hämta dokument från tilldelade iOS-enheter. Dokument kan hämtas och uppdateras på samma sätt som när du delar dokument genom att importera och exportera till iTunes.

Löpande hantering

När användarna väl kommit igång finns det en rad olika administratörsfunktioner för att hantera enheter genom hela deras livscykel. Det går bland annat att begära information från enheter, starta säkerhetsåtgärder, som fjärradering, samt utföra specifika uppgifter för appar.

Anrop

En MDM-server kan begära en mängd olika uppgifter från enheter. Detta omfattar hårdvaruinformation som serienummer, enhetens UDID eller Wi-Fi-MAC-adress, samt mjukvaruinformation som iOS-version och en detaljerad lista över alla installerade appar. Denna information kan användas för att kontrollera att användarna har de appar de ska ha på sina enheter.

Kommandon

På hanterade enheter kan en MDM-server utföra en mängd olika administratörskommandon, till exempel konfigurera inställningar automatiskt utan att användaren behöver göra något, fjärrlåsa eller fjärradera en enhet eller radera lösenkoder så att användare kan återställa bortglömda lösenord. En MDM-server kan också begära att en iOS-enhet speglar innehållet till en specifik målenhet via AirPlay eller avslutar en pågående AirPlay-session.

Hanterade appar

Organisationer behöver ofta distribuera appar som hjälper användarna att jobba effektivare. Samtidigt måste organisationer kunna styra hur apparna ansluter till interna resurser eller hur datasäkerheten hanteras när en användare lämnar organisationen. Genom att hantera apparna i iOS kan en organisation distribuera gratis- och betalappar samt organisationsspecifika appar trådlöst med hjälp av MDM och samtidigt behålla balansen mellan skydd av företagsdata och skydd av användarens privata appar och data.

Hanterade appar kan fjärraderas av en MDM-server eller genom att användare tar bort sina enheter från MDM. När en app tas bort raderas även alla data kopplade till appen. Om en app fortfarande är tilldelad en användare genom VPP eller om användaren löser in en appkod med sitt personliga Apple-ID kan appen laddas ner igen från App Store, men hanteras inte av MDM.

iOS och organisationens MDM-lösning ger fler möjligheter att hantera appar, utöka säkerheten och ge användarna en bättre upplevelse:

- **Administrerad öppning.** Den här begränsningen skyddar företagsdata genom att kontrollera vilka appar och konton som kan användas till att öppna dokument och bilagor. IT-organisationer kan konfigurera en lista över tillgängliga appar i delningspanelen så att arbetsdokument begränsas till företagsappar och så att personliga dokument inte öppnas i hanterade appar. Den här policyn gäller också dokumentappar och tangentbordsappar från tredje part i iOS 8.
- **Appkonfiguration.** Apputvecklare kan skapa inställningar i appar som kan aktiveras om appen installeras som en hanterad app. Dessa konfigurationsinställningar kan installeras före eller efter att den administrerade appen installeras. IT-avdelningen kan till exempel definiera en uppsättning med förvalda inställningar för en Sharepoint-app så att användaren inte behöver konfigurera några serverinställningar manuellt.
- **Enappsläge.** Hjälper användaren att fokusera på en specifik uppgift på en iOS-enhet. Inställningen begränsar iOS-enheten till en enda app. Utvecklare kan också aktivera den här funktionen inuti sina appar så att enskilda appar kan starta och avsluta enappsläget.
- **Förhindra säkerhetskopiering.** Den här begränsningen förhindrar att hanterade appar säkerhetskopierar data till iCloud eller iTunes. Genom att förhindra säkerhetskopiering kan inte data från en hanterad app återskapas om appen raderas via MDM och sedan installeras på nytt av användaren.

Supportalternativ

Apple erbjuder en rad olika program och supportalternativ för iOS-användare och IT-administratörer.

AppleCare OS Support

Med AppleCare OS Support får IT-avdelningen support via telefon och e-post på företagsnivå för driftsättningar med iOS, OS X och OS X Server. AppleCare OS Support kan hjälpa IT-personalen att effektivisera driftsättning och hantering av enheter samt problemlösning genom att de får direkt tillgång till tekniker för frågor om integrering, migrering och avancerade serverproblem.

AppleCare Help Desk Support

AppleCare Help Desk Support ger förtur till Apples mest erfarna personal för teknisk support per telefon. Det innehåller också en uppsättning verktyg för diagnostik och felsökning av Apples hårdvara så att stora organisationer kan administrera sina resurser effektivare, förkorta svarstiderna och minska utbildningskostnaderna. I AppleCare Help Desk Support ingår ett obegränsat antal supporttillfällen för diagnos av mjuk- och hårdvara samt hjälp med att identifiera problem med iOS-enheter.

AppleCare för användare av iOS-enheter

Varje iOS-enhet levereras med 90 dagars kostnadsfri teknisk telefonsupport och ett års begränsad garanti. Avtalet kan förlängas till två år från inköpsdatumet med AppleCare+ för iPhone, AppleCare+ för iPad eller AppleCare Protection Plan (APP) för iPod touch. Du kan ringa Apples tekniska support så ofta du vill och få svar på dina frågor. Apple erbjuder också smidiga servicealternativ för enheter som kräver reparation. Utöver detta ger AppleCare+ för iPhone och AppleCare+ för iPad skydd för upp till två fall av oavsiktliga skador (för varje fall tillkommer en självrisk).

iOS Direct Service-programmet

Tillsammans med AppleCare+ och AppleCare Protection Plan hjälper iOS Direct Service-programmet företagets helpdesk att övervaka problem med enheterna utan att personalen behöver ringa AppleCare eller besöka en Apple Store-butik. Vid behov kan företaget direkt beställa ett utbyte av iPhone, iPad, iPod touch eller medföljande tillbehör.

Läs mer om AppleCare: www.apple.com/se/support/products

Sammanfattning

Oavsett om ditt företag driftsätter iOS-enheter till en grupp användare eller inom hela organisationen finns det många alternativ som gör det enkelt att driftsätta och hantera enheter. Genom att välja strategier som passar företaget kan du hjälpa medarbetarna att bli produktivare och utföra sina arbetsuppgifter på helt nya sätt.

Läs mer om att integrera iOS i olika företags IT-miljöer: www.apple.com/ipad/business/it

Detaljerad teknisk information om att driftsätta iOS finns i den tekniska referensguiden för driftsättning av iOS på: https://help.apple.com/deployment/ios

*En del funktioner kräver Wi-Fi-anslutning. En del funktioner är inte tillgängliga i alla länder. För vissa tjänster är åtkomsten begränsad till tio enheter.