# Driftsättning av iOS och iPadOS – översikt

# Introduktion

Innehåll



iPhone och iPad kan förändra verksamheten och medarbetarnas sätt att arbeta. De kan leda till avsevärt högre produktivitet och ge medarbetarna frihet och flexibilitet att arbeta på nya sätt, både på kontoret och utanför. Det här moderna sättet att arbeta innebär fördelar för hela organisationen. Användarna får bättre tillgång till information, så att de känner att de har större inflytande och kan lösa problem på kreativa sätt.

Genom att erbjuda iOS- och iPadOS-support anses it-avdelningar vara delaktiga i att forma affärsstrategin och lösa konkreta problem, snarare än att bara fixa tekniken och bidra till kostnadsbesparingar. I slutändan är det något som alla tjänar på, med entusiastiska medarbetare och nya affärsmöjligheter överallt.

Det har aldrig varit enklare att driftsätta iPhone och iPad i företaget. Med Apple Business Manager och en MDM-lösning (mobil enhetshantering) från en annan tillverkare kan organisationen enkelt driftsätta iOS- och iPadOS-enheter och appar i stor skala.

- Med MDM går det att konfigurera och hantera enheter samt distribuera och hantera appar trådlöst.
- Apple Business Manager automatiserar registreringen av Apple-enheter i MDM-lösningen så att driftsättningen går smidigare. Det innebär bland annat att it-avdelningen inte behöver konfigurera enheterna manuellt.
- Med Apple Business Manager kan man köpa appar och böcker i större volymer och distribuera dem trådlöst till användarna.
- Man kan dessutom skapa hanterade Apple-ID:n åt medarbetare med federerad autentisering via Microsoft Azure AD med Apple Business Manager.

Det här dokumentet innehåller vägledning för hur man driftsätter iOS- och iPadOS-enheter i organisationen och tips på hur man skapar en driftsättningsplan som passar den specifika miljön. I referensdokumentet om driftsättning för iPhone och iPad på support.apple.com/guide/deployment-reference-ios finns mer information om följande ämnen:

# Ägarskapsmodeller

Ett viktigt första steg på vägen till driftsättning är att utvärdera olika ägarskapsmodeller och välja den som passar bäst för din organisation. Driftsättningen kan utföras på flera olika sätt beroende på vem som äger enheten. Börja med att ta reda på vad som passar bäst för din organisation.

Det finns två olika ägarskapsmodeller för iOS- och iPadOS-enheter som företag ofta använder:

- Organisationsägda
- Användarägda

De flesta organisationer föredrar en viss modell, men det kan hända att flera modeller används i din miljö. Till exempel kan huvudkontoret för ett företag välja en driftsättningsstrategi med användarägda enheter, så att medarbetarna kan ställa in personliga iPad-enheter samtidigt som företagsresurser skyddas och hanteras, utan att det påverkar användarens privata appar och data. Företagets butiker kanske istället väljer en driftsättningsstrategi med organisationsägda enheter, där flera medarbetare kan dela på iOS- och iPadOS-enheter för hantering av kundtransaktioner.

Utforska dessa modeller så att du kan hitta de alternativ som passar bäst för just din miljö. När du har bestämt dig för vilken modell som passar din organisation bäst kan ditt team utforska Apples driftsättnings- och hanteringsalternativ mer ingående.

## Organisationsägda enheter

Företag som väljer modellen med organisationsägda enheter kan dela ut enheter till medarbetarna som de kan använda i det dagliga arbetet, låta medarbetarna dela på enheterna för att kunna utföra vanliga arbetsuppgifter eller konfigurera enheterna för ett specifikt syfte i en viss app. Enheter som delas ut till enskilda användare kan anpassas av användaren själv. Enheter som är låsta till en viss app eller som används av flera olika användare kan vanligtvis inte anpassas av användaren. Med dessa modeller, rätt teknik från Apple och en MDM-lösning kan du automatisera inställningen och konfigureringen av enheterna fullt ut.

**Anpassningsbara enheter:** Om du använder en strategi med anpassningsbara enheter kan du låta varje användare själv välja enhet och registrera den med en MDM-lösning som tillhandahåller organisationens inställningar och appar trådlöst (OTA). Du kan också använda Apple Business Manager för att automatiskt registrera nya enheter i institutionens MDM-lösning, om enheterna har köpts direkt från Apple eller från en medverkande auktoriserad Apple-återförsäljare eller operatör. Detta kallas automatisk enhetsregistrering. När enheterna har konfigurerats kan användarna anpassa dem med egna appar och data utöver eventuella företagskonton eller appar som tillhandahålls av organisationen.

**Delade enheter:** När enheter delas av flera personer, eller 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. Vid driftsättning av delade enheter har användarna som regel inte tillstånd att installera appar eller lagra privata data på enheten. Automatisk enhetsregistrering via Apple Business Manager kan också användas till att automatisera installationen av delade enheter. I tabellen nedan visas de åtgärder som krävs av administratören respektive användaren i varje steg av en strategi med organisationsägda enheter. Åtgärderna avser både driftsättningar av *anpassningsbara enheter* och *delade enheter*, om inget annat anges.

| | Administratör | Användare |
|---|---|---|
| **Förbered** | • Utvärdera infrastrukturen<br>• Välj en MDM-lösning<br>• Registrera dig i Apple Business Manager | • Ingen åtgärd krävs från användaren |
| **Ställa in** | • Konfigurera enheter<br>• Distribuera appar och böcker | • Ingen åtgärd krävs från användaren |
| **Driftsätta** | • Distribuera enheter<br>**Endast anpassningsbara enheter**<br>• Tillåt användaranpassning | **Endast anpassningsbara enheter**<br>• Ladda ner och installera appar och böcker<br>• Använd Apple-ID samt konton för App Store och iCloud (om tillämpligt)<br>**Endast delade enheter**<br>• Ingen åtgärd krävs från användaren |
| **Hantera** | • Administrera enheter<br>• Driftsätt och hantera ytterligare innehåll | **Endast anpassningsbara enheter**<br>• Upptäck fler appar att använda<br>**Endast delade enheter**<br>• Ingen åtgärd krävs från användaren |

## Användarägda enheter

När enheter köps och ställs in av användarna själva (BYOD, Bring Your Own Device) kan du fortfarande ge användarna åtkomst till wifi, e-post, kalendrar och andra företagstjänster med MDM tack vare det nya alternativet för användarregistrering i iOS 13 och iPadOS.

Vid en BYOD-driftsättning kan användarna själva ställa in och konfigurera sina enheter. Användarna kan registrera sina enheter i organisationens MDM-lösning för att få tillgång till företagsresurser, konfigurera olika inställningar, installera en konfigurationsprofil eller installera företagsappar. Användarna måste då välja att registrera sina enheter i organisationens MDM-lösning.

Med användarregistrering av privatägda enheter kan företagets data och andra resurser hanteras på ett säkert sätt, samtidigt som användarens integritet, privata data och appar skyddas. It-avdelningen kan bara styra vissa inställningar, övervaka att företagspolicyer efterlevs och endast ta bort data och appar som tillhör företaget utan att röra personlig information och appar.

Detta ingår vid användarregistrering:

- **Hanterat Apple-ID.** Användarregistreringen är integrerad med hanterade Apple-ID:n, som upprättar en användaridentitet på enheten och ger åtkomst till Apples tjänster. Ett hanterat Apple-ID kan användas parallellt med ett personligt Apple-ID som användaren har loggat in med. Hanterade Apple-ID:n skapas i Apple Business Manager och delas ut via federerad autentisering till Microsoft Azure Active Directory.
- **Dataseparering.** I samband med användarregistreringen skapas en separat APFS-volym för hanterade konton, appar och data på enheten. Den hanterade volymen skiljs åt från resten av enheten genom kryptering.
- **Särskild hantering av BYOD-enheter.** Användarregistrering har utformats för användarägda enheter. Syftet är att it-avdelningen ska kunna hantera en begränsad uppsättning inställningar och riktlinjer. De ska däremot inte kunna fjärradera hela enheten, hämta personuppgifter eller utföra vissa andra hanteringsåtgärder.

I tabellen nedan visas de åtgärder som krävs av administratören respektive användaren i varje steg av en strategi med användarägda enheter.

| | Administratör | Användare |
|---|---|---|
| **Förbered** | • Utvärdera infrastrukturen<br>• Välja en MDM-lösning<br>• Registrera dig i Apple Business Manager | • Använd personligt Apple-ID och hanterat Apple-ID, App Store och iCloud-konton (om tillämpligt) |
| **Ställa in** | • Konfigurera enhetsinställningar<br>• Distribuera appar och böcker | • Välj att använda företagets MDM-lösning<br>• Ladda ner och installera appar och böcker |
| **Driftsätta** | • Ingen åtgärd krävs från administratören | • Ingen åtgärd krävs från användaren |
| **Hantera** | • Administrera enheter<br>• Driftsätt och hantera ytterligare innehåll | • Upptäck fler appar att använda |

Läs mer om användarregistrering i MDM:
support.apple.com/guide/mdm

Läs mer om federerad autentisering:
support.apple.com/guide/apple-business-manager

# Driftsättningssteg

Det här avsnittet innehåller mer information om de fyra stegen vid driftsättning av enheter och innehåll: förbereda miljön, ställa in enheter, driftsätta och underhålla. Vilka steg du tillämpar beror på om det är organisationen eller användaren som äger enheterna.

## 1. Förbereda

Följ de här stegen för att förbereda driftsättningen när du har identifierat rätt driftsättningsmodell för din organisation. Du kan börja med dessa förberedelser innan du har fått enheterna.

### Utvärdera infrastrukturen

iPhone och iPad kan smidigt integreras i de flesta vanligt förekommande it-miljöerna i företag. Det är viktigt att du utvärderar den befintliga nätverksinfrastrukturen så att du ser till att din organisation fullt ut utnyttjar allt som iOS och iPadOS har att erbjuda.

#### Wifi och nätverk

En kontinuerlig och tillförlitlig anslutning till trådlösa nätverk är viktigt vid installation och konfiguration av iOS- och iPadOS-enheter. Se till att företagets wifi-nätverk har stöd för anslutning av alla användares enheter samtidigt. Du kan behöva konfigurera företagets webbproxyserver eller brandväggsportar om enheterna inte kan ansluta till Apples aktiveringsservrar, iCloud eller App Store. Apple och Cisco har även optimerat hur iPhone och iPad kommunicerar med ett trådlöst Cisco-nätverk. Det skapar förutsättningar för andra avancerade nätverksfunktioner, till exempel snabb roaming och optimering av appar med QoS (Quality of Service).

Undersök VPN-infrastrukturen för att se till att användarna har säker fjärråtkomst till företagets resurser på sina iOS- och iPadOS-enheter. Överväg att använda någon av funktionerna VPN On Demand eller VPN per app i iOS och iPadOS, så att en VPN-anslutning endast upprättas vid behov. Se till att VPN-nätverksnoderna har stöd för den här funktionen om du planerar att använda VPN per app. Kontrollera också att du har tillräckligt med licenser för alla 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- och iPadOS-enheter använder Bonjour för att ansluta till AirPrint-kompatibla skrivare och AirPlay-kompatibla enheter, såsom Apple TV. Vissa appar använder Bonjour för att upptäcka andra enheter för samarbete och delning.

Läs mer om wifi och nätverk:
support.apple.com/guide/deployment-reference-ios

Läs mer om Bonjour:
developer.apple.com/library

**E-post, kontakter och kalendrar**
Kontrollera att ActiveSync-tjänsten är uppdaterad och konfigurerad så att den fungerar för alla användare i nätverket om du använder Microsoft Exchange. Se till att det finns tillräckligt med licenser för det förväntade antalet anslutna iOS- och iPadOS-enheter om du använder den molnbaserade Office 365-tjänsten. iOS och iPadOS har även stöd för modern autentisering i Office 365 som bygger på standarden OAuth 2.0 och flerfaktorsautentisering. Om du inte använder Exchange fungerar iOS och iPadOS även med IMAP, POP, SMTP, CalDAV, CardDAV, LDAP och andra standardbaserade servrar.

**Innehållscachelagring**
Funktionen innehållscachelagring ingår i macOS High Sierra och senare. Den sparar en lokal kopia av innehåll som ofta efterfrågas från Apples servrar. Detta minskar bandbredden som behövs för att ladda ner innehåll i ditt nätverk. Innehållscachelagring snabbar på ned- och uppladdningen av mjukvara via App Store, Mac App Store och Apple Books.

Dessutom kan mjukvaruuppdateringar cachelagras för snabbare nedladdning till iOS- och iPadOS-enheter. I innehållscachelagring ingår även den kabelbundna cache-tjänsten som gör det möjligt att dela internetanslutningen från en Mac med flera usb-anslutna iOS- och iPadOS-enheter.

Läs mer om innehållscachelagring:
support.apple.com/guide/deployment-reference-macos

Läs mer om delad cachning:
support.apple.com/HT207523

## Välja en MDM-lösning

Apples ramverk för iOS- och iPadOS-hantering ger organisationer möjlighet att på ett säkert sätt registrera enheter i en företagsmiljö, konfigurera och uppdatera inställningar trådlöst, övervaka efterlevnad, driftsätta appar och böcker samt fjärradera eller fjärrlåsa hanterade enheter. Dessa hanteringsfunktioner aktiveras via MDM-lösningar från tredje part.

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. Gå igenom resurserna nedan och avgör vilka hanteringsfunktioner som är viktigast för din verksamhet innan du bestämmer dig för en lösning. Utöver MDM-lösningarna från tredje part finns det en lösning från Apple som ingår i macOS Server: Profilhanteraren.

Läs mer om hur man hanterar enheter och företagsdata:
apple.com/se/business/docs/resources/Managing_Devices_and_Corporate_Data_on_iOS.pdf

### Registrera dig i Apple Business Manager

Apple Business Manager är en webbaserad portal för it-administratörer där de kan driftsätta iPhone, iPad, iPod touch, Apple TV och Mac från ett och samma ställe. Apple Business Manager fungerar smidigt ihop med er MDM-lösning och gör det enkelt att automatisera enhetshantering, köpa appar, distribuera innehåll och skapa hanterade Apple-ID:n åt medarbetare.

Nu är programmet för enhetsregistrering (DEP) och programmet för volyminköp (VPP) helt integrerade i Apple Business Manager, så att organisationer har tillgång till allt de behöver för att driftsätta Apple-enheter. Efter den 1 december 2019 är dessa program inte längre tillgängliga.

## Enheter

Apple Business Manager möjliggör automatisk enhetsregistrering vilket innebär att företag snabbt och smidigt kan driftsätta företagsägda Apple-enheter och registrera dem i MDM utan att behöva hantera de fysiska enheterna eller förbereda dem separat.

- Förenkla inställningsprocessen för användarna genom att effektivisera stegen i inställningsassistenten, så att medarbetarna får rätt konfigurationer direkt när de aktiverar sina enheter. It-team kan nu anpassa processen ytterligare genom att infoga text om samtycke, företagets varumärkesprofil eller modern autentisering.
- Ta större kontroll över företagsägda enheter med hjälp av övervakning, som erbjuder ökad kontroll vid enhetshantering som inte är möjlig med andra driftsättningsmodeller, till exempel permanent MDM.
- Hantera standardservrar för MDM enklare genom att ställa in en standardserver baserad på enhetstyp. Du kan nu även registrera iPhone, iPad och Apple TV med Apple Configurator 2, oavsett hur de är inköpta.

## Innehåll

Med Apple Business Manager kan organisationer enkelt göra volyminköp av innehåll. Du kan ge medarbetarna tillgång till suveränt innehåll som är färdigt att använda med flexibla och säkra distributionsalternativ, oavsett om de använder iPhone, iPad eller Mac.

- Gör volyminköp av appar, böcker och anpassade appar, inklusive de som ni utvecklar internt. Överför enkelt licenser för appar mellan olika platser och dela licenser mellan köpare på samma plats. Visa en lista över köphistorik med bland annat antalet licenser som för närvarande används via MDM.
- Distribuera köpta appar och böcker direkt till hanterade enheter eller auktoriserade användare och håll enkelt reda på vilket innehåll som har tilldelats vilken användare eller enhet. Med hanterad distribution kontrollerar du hela distributionsprocessen och behåller fullständig äganderätt till appar. Appar som inte behövs på en enhet eller av en användare kan återkallas och tilldelas till någon annan i organisationen.

- Det finns flera olika betalningsmetoder att välja mellan, till exempel kreditkort och faktura. Organisationer kan köpa volymkredit (där det erbjuds) från Apple eller från en auktoriserad Apple-återförsäljare i specifika belopp i den lokala valutan. Beloppet levereras sedan elektroniskt till kontoinnehavaren, som kan använda krediten i butiken.
- Du kan distribuera appar i flera länder till enheter eller användare i alla länder där appen är tillgänglig. Utvecklare kan göra sina appar tillgängliga i flera länder via den vanliga publiceringsprocessen för App Store.

Obs! I vissa länder och regioner går det inte att köpa böcker i Apple Business Manager. På support.apple.com/HT207305 finns mer information om vilka funktioner och inköpsmetoder som är tillgängliga.

### Personer

Organisationer kan använda Apple Business Manager till att skapa och hantera konton för medarbetare som kan integreras med den befintliga infrastrukturen och som ger åtkomst till Apples appar och tjänster samt till Apple Business Manager.

- Skapa hanterade Apple-ID:n så att medarbetarna kan använda Apples appar och tjänster och komma åt arbetsrelaterade data i hanterade appar som använder iCloud Drive. Dessa konton ägs och kontrolleras av respektive organisation.
- Utnyttja federerad autentisering genom att ansluta Apple Business Manager till Microsoft Azure Active Directory. Hanterade Apple-ID:n skapas automatiskt första gången medarbetarna loggar in med sina befintliga inloggningsuppgifter på kompatibla Apple-enheter.
- Den nya funktionen för användarregistrering i iOS 13, iPadOS och macOS Catalina gör det möjligt att ha ett hanterat Apple-ID såväl som ett privat Apple-ID på en personlig enhet. Oavsett vilken typ av enhet som används kan man även välja att ha ett hanterat Apple-ID som primärt, och enda, Apple-ID. Medarbetaren kan även använda sitt hanterade Apple-ID för att skaffa åtkomst till iCloud på webben efter att ha loggat in på en Apple-enhet första gången.
- Specificera roller för organisationens it-medarbetare så att de kan hantera enheter, appar och konton i Apple Business Manager på ett effektivt sätt. Använd administratörsrollen för att godkänna eventuella villkor och enkelt överföra ansvaret om någon lämnar organisationen.

Obs! iCloud Drive stöds för närvarande inte vid användarregistrering. iCloud Drive kan användas med ett hanterat Apple-ID under förutsättning att det är det enda Apple-ID som finns på enheten.

Läs mer om Apple Business Manager: www.apple.com/se/business/it

### Registrera dig i Apple Developer Enterprise Program

Apple Developer Enterprise Program omfattar kompletta verktyg för att utveckla, testa och distribuera appar till användare. Du kan distribuera program antingen genom att publicera dem på en webbserver eller via en MDM-lösning. Du kan signera och attestera Mac-appar och Mac-installerare med ditt utvecklar-id för Gatekeeper, vilket bidrar till att skydda macOS mot skadeprogram.

Läs mer om Developer Enterprise Program:
developer.apple.com/programs/enterprise

# 2. Ställa in

I det här steget konfigurerar du enheter och distribuerar innehåll via Apple Business Manager, en MDM-lösning eller Apple Configurator 2. Inställningen kan göras på flera olika sätt, beroende på vem som äger enheterna och vilken driftsättningsmodell man föredrar.

## Konfigurera enheterna

Det finns flera olika alternativ för att konfigurera användaråtkomsten till företagstjänster. It-avdelningen kan ställa in enheter genom att distribuera konfigurationsprofiler. För övervakade enheter finns det ytterligare konfigurationsalternativ.

### Konfigurera enheter med MDM

När enheterna är säkert registrerade i en MDM-lösning aktiverar man hanteringen med hjälp av konfigurationsprofiler, det vill säga en XML-fil med konfigureringsinformation för en iOS- eller iPadOS-enhet. Dessa profiler automatiserar konfigureringen av inställningar, konton, begränsningar och inloggningsuppgifter. De kan levereras trådlöst (OTA) från företagets MDM-lösning, vilket är perfekt för enkel konfigurering av flera enheter. Profiler kan också skickas som e-postbilagor, laddas ner från en webbsida eller installeras på enheter via Apple Configurator 2.

- **Organisationsägda enheter.** Använd Apple Business Manager för att automatiskt registrera dina användares enheter via MDM när de har aktiverats. Alla iOS- och iPadOS-enheter som läggs till i Apple Business Manager är ständigt övervakade och MDM-registreringen är obligatorisk.
- **Användarägda enheter.** Medarbetarna kan bestämma om de vill registrera sina enheter i MDM. De kan även när som helst avregistrera enheterna från MDM genom att ta bort konfigurationsprofilen. Då tas även företagets data och inställningar bort. Fundera på olika sätt att uppmuntra användarna att välja den hanterade lösningen. Du kan till exempel göra det obligatoriskt för användarna att registrera sig i MDM om de vill få tillgång till wifi-nätverket, genom att låta MDM-lösningen automatiskt skicka inloggningsuppgifter till nätverket.

När en enhet är registrerad kan administratören införa en profil, ett alternativ eller ett kommando för MDM. Vilka hanteringsåtgärder som kan väljas för en viss enhet varierar beroende på vilken övervakning och registreringsmetod som har valts. Sedan skickas en notis om åtgärden till iOS- eller iPadOS-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.

### Konfigurera enheter med Apple Configurator 2 (valfritt)

Organisationer kan använda Apple Configurator 2 för lokal inledande driftsättning av flera enheter. Med den här kostnadsfria macOS-appen kan du ansluta iOS- och iPadOS-enheter till en Mac via usb och uppdatera dem till de senaste versionerna av iOS och iPadOS, konfigurera enhetsinställningar och begränsningar samt installera appar och annat innehåll. Efter den inledande inställningen kan du fortsätta att hantera allting trådlöst (OTA) via MDM.

Användargränssnittet i Apple Configurator 2 fokuserar på dina enheter och de olika uppgifter du vill utföra på dem. Appen kan integreras med Apple Business Manager, vilket gör att enheter automatiskt kan registreras i MDM med organisationens inställningar. Du kan skapa anpassade arbetsflöden i Apple Configurator 2 med hjälp av Blueprints-funktionen för att kombinera olika åtgärder.

Läs mer om Apple Configurator 2:
support.apple.com/sv-se/apple-configurator

**Övervakade enheter**

Övervakning erbjuder ytterligare hanteringsmöjligheter för organisationsägda iOS- och iPadOS-enheter. Du kan bland annat införa begränsningar såsom enappsläge eller inaktivera AirDrop. Det blir även möjligt att aktivera ett webbfilter via en global proxy för att se till att användarens surfvanor följer organisationens riktlinjer samt förhindra användarna från att återställa sina enheter till fabriksinställningarna och mycket annat. Som förval är alla iOS- och iPadOS-enheter oövervakade. Du kan antingen aktivera övervakning via Apple Business Manager eller manuellt med hjälp av Apple Configurator 2.

Även om du inte planerar att använda några övervakningsfunktioner i dagsläget bör du överväga att övervaka enheterna när du ställer in dem, så att du kan välja att dra nytta av övervakningsfunktioner längre fram. Annars kan du tvingas radera redan driftsatta enheter. Övervakning handlar inte om att låsa en enhet, utan snarare att förbättra företagsägda enheter med utökade hanteringsmöjligheter. På lång sikt ger övervakning fler alternativ för ditt företag.

Läs mer om begränsningar för övervakade enheter:
support.apple.com/guide/mdm

## Distribuera appar och böcker

Apple erbjuder omfattande program som hjälper din organisation att dra nytta av det stora utbudet av appar och innehåll för iOS och iPadOS. Med dessa funktioner kan du distribuera appar och böcker som du har köpt via Apple Business Manager eller internt utvecklade appar till enheter och användare, så att dina användare har allt de behöver för att vara produktiva. Du väljer önskad distributionsmetod vid köpet: hanterad distribution eller inlösbara koder.

### Hanterad distribution

Med hanterad distribution hanterar du appar och böcker från Apple Business Manager-butiken (i de länder där appen finns tillgänglig) med hjälp av företagets MDM-lösning eller Apple Configurator 2. För att aktivera hanterad distribution måste du först koppla din MDM-lösning till ditt Apple Business Manager-konto med hjälp av en säker token. När du är ansluten till MDM-servern kan du tilldela Apple Business Manager-appar och -böcker även om App Store är inaktiverad på enheten.

- **Tilldela appar till enheter.** Tilldela appar direkt till enheter med hjälp av företagets MDM-lösning eller Apple Configurator 2. Den här metoden sparar flera steg i den initiala driftsättningen och gör distributionen mycket enklare och snabbare, samtidigt som du har fullständig kontroll över hanterade enheter och innehåll. När en app har tilldelats till en enhet skickas appen till enheten via MDM utan att någon inbjudan till användaren behövs. Alla som använder enheten har då tillgång till appen.
- **Tilldela appar och böcker till användare.** Ett alternativ är att via MDM-lösningen bjuda in användare att ladda ner appar och böcker via e-post eller en pushnotis. Användarna tackar ja till denna inbjudan genom att logga in på sina enheter med ett personligt Apple-ID. Detta Apple-ID finns registrerat i Apple Business Manager-tjänsten, men förblir helt privat och är osynligt för administratören. När användarna har tackat ja till inbjudan är de anslutna till MDM-servern och kan börja ta emot tilldelade appar och böcker. Appar är automatiskt tillgängliga för nedladdning på alla användarens enheter, utan extra kostnad eller arbetsinsats från din sida.

När appar du har tilldelat inte längre behövs på en enhet kan de återkallas och tilldelas till andra enheter och användare, så att din organisation behåller fullständig äganderätt till och kontroll över köpta appar. Distribuerade böcker förblir däremot mottagarens egendom och kan inte återkallas eller tilldelas på nytt.

### Inlösenkoder

Du kan också distribuera innehåll med hjälp av inlösenkoder. Det här är praktiskt när organisationen inte kan använda MDM på slutanvändarens enhet, till exempel inom ett franchise-företag. Med den här metoden överförs appen eller boken permanent till den användare som löser in koden. Inlösenkoder levereras i ett kalkylblad. Du får en unik kod för varje app eller bok som ingår i köpet. Varje gång en kod löses in uppdateras kalkylbladet i Apple Business Manager-butiken, så att du närsomhelst kan se antalet inlösta koder. Du kan distribuera koder via MDM, Apple Configurator 2, e-post eller en intern webbplats.

**Installera appar och innehåll med Apple Configurator 2 (valfritt)**
Utöver grundläggande inställningar och konfigurering kan Apple Configurator 2 användas till att installera appar och innehåll på enheter som du ställer in för användarens räkning. Vid driftsättningar av anpassningsbara enheter kan du förinstallera appar, vilket sparar tid och bandbredd i nätverket. Och vid driftsättning av delade enheter kan du ställa in enheterna ända till hemskärmen. När du konfigurerar enheter med Apple Configurator 2 kan du installera App Store-appar, interna appar och dokument. För App Store-appar krävs Apple Business Manager. Dokument är tillgängliga för appar som stöder fildelning. Du kan granska eller ladda ner dokument från iOS- och iPadOS-enheter genom att ansluta dem till en Mac som kör Apple Configurator 2.

# 3. Driftsätta

iPhone och iPad gör det enkelt för medarbetare att börja använda sina enheter utan hjälp från it-avdelningen.

## Distribuera enheterna

När enheterna har förberetts och ställts in i de två inledande stegen är de klara att distribueras. Vid driftsättning av anpassningsbara enheter ger du enheter till användare som kan använda den förenklade inställningsassistenten till att anpassa enheten och slutföra inställningen. Distribuera enheter till skiftmedarbetare eller placera enheter i kiosker som laddar och skyddar enheterna vid driftsättning av delade enheter.

**Inställningsassistent**
Användare kan aktivera sina enheter direkt efter att de har packat upp dem, konfigurera grundinställningar och börja jobba direkt med inställningsassistenten. Efter den inledande inställningen kan användarna också göra personliga inställningar av exempelvis språk, plats, Siri, iCloud och Hitta min iPhone. Enheter i Apple Business Manager registreras automatiskt i MDM direkt i inställningsassistenten.

**Tillåt användaranpassning**
Vid driftsättning av anpassningsbara enheter samt BYOD är det möjligt för användarna att anpassa sina enheter med egna Apple-ID:n, vilket ökar produktiviteten eftersom användarna väljer vilka appar och vilket innehåll de behöver för att klara sina uppgifter och nå sina mål.

**Apple-ID och hanterat Apple-ID**
När medarbetare använder ett Apple-ID för att logga in på FaceTime, iMessage, App Store, iCloud och andra Apple-tjänster får de tillgång till ett brett utbud av innehåll som hjälper dem att effektivisera arbetsuppgifter, öka produktiviteten och utöka samarbetet.

Precis som andra Apple-ID:n används hanterade Apple-ID:n till att logga in på personliga enheter. De ger även åtkomst till Apple-tjänster, däribland iCloud och samarbete i iWork och Anteckningar, samt till Apple Business Manager. Till skillnad från vanliga Apple-ID:n ägs och hanteras dessa Apple-ID:n av organisationen och används till bland annat återställning av lösenord och rollbaserad administration. Hanterade Apple-ID:n har vissa begränsade inställningar.

En enhet som registreras via användarregistrering måste ha ett hanterat Apple-ID, men kan även användas parallellt med ett personligt Apple-ID. Vid andra typer av registrering måste man välja antingen ett personligt Apple-ID eller ett hanterat Apple-ID. Det är endast alternativet med användarregistrering som stöder flera Apple-ID:n.

Användarna ska helst logga in med sina egna Apple-ID:n eller med de hanterade Apple-ID:n som har skapats åt dem för att verkligen kunna dra nytta av de här tjänsterna. Användare kan skapa ett Apple-ID även innan de får en enhet. Med inställningsassistenten kan användarna också skapa ett personligt Apple-ID om de inte har något. Användarna behöver inte något kontokort för att skapa ett Apple-ID.

Läs mer om hanterade Apple-ID:n:
support.apple.com/guide/apple-business-manager

**iCloud**

Med iCloud kan användarna automatiskt synka dokument och personligt innehåll, som kontakter, kalendrar, dokument och bilder, och hålla allt uppdaterat på flera enheter. Hitta min hjälper användaren att leta rätt på en borttappad eller stulen Mac, iPhone, iPad eller iPod touch. Delar av iCloud, som iCloud-nyckelring och iCloud Drive, kan avaktiveras genom begränsningar som ställs in antingen manuellt på enheten eller via MDM. På så sätt kan organisationer enklare kontrollera vilka data som lagras i vilka konton.

Läs mer om hur man hanterar iCloud:
support.apple.com/guide/deployment-reference-ios

# 4. Hantera

När användarna har kommit igång finns många olika administrationsfunktioner för att hantera och underhålla enheterna och innehållet över tid.

## Administrera enheterna

En hanterad enhet kan administreras via MDM-servern med hjälp av en uppsättning specifika åtgärder. Dessa åtgärder omfattar informationsanrop som skickas till enheterna samt initiering av hanteringsuppgifter som gör det möjligt att hantera borttappade eller stulna enheter samt enheter som inte följer riktlinjerna.

### Anrop

En MDM-server kan anropa enheter om en mängd information, bland annat hårdvaruinformation, till exempel serienummer, enhets-UDID eller wifi-MAC-adress. Detsamma gäller för mjukvaruinformation såsom iOS- eller iPadOS-version samt en detaljerad lista över alla appar som är installerade på enheten. Den här informationen kan användas av företagets MDM-lösning för att upprätthålla ett uppdaterat lagerregister, fatta välgrundade hanteringsbeslut och automatisera hanteringsåtgärder såsom att se till att användarna har rätt appar.

### Hanteringsåtgärder

En MDM-server kan användas till att utföra en mängd olika administratörsåtgärder på hanterade enheter. Man kan till exempel konfigurera inställningar automatiskt utan att användaren behöver göra något, uppdatera mjukvara på en enhet som är låst med lösenkod, fjärrlåsa eller fjärradera en enhet eller radera lösenkoder så att användare kan återställa bortglömda lösenord. En MDM-server kan även begära att en iPhone eller iPad ska spegla innehållet till en specifik målenhet via AirPlay eller avsluta en pågående AirPlay-session.

### Hanterade mjukvaruuppdateringar

Du kan hindra användare från att manuellt och trådlöst (OTA) uppdatera en övervakad enhet under en viss tid. När du använder denna begränsning är den förinställda fördröjningen 30 dagar och den träder i kraft så fort Apple släpper en iOS- eller iPadOS-uppdatering. Du kan emellertid själv välja att ställa in mellan 1–90 dagar då uppdateringar inte kan utföras. Det går också att schemalägga uppdateringar på övervakade enheter med en MDM-lösning.

### Förlorat läge

MDM-lösningen kan fjärraktivera Förlorat läge på en övervakad enhet. Åtgärden låser enheten och kan även visa ett meddelande med ett telefonnummer på låsskärmen. Med Förlorat läge kan du lokalisera en övervakad enhet som har tappats bort eller stulits, eftersom MDM anropar enheter trådlöst och efterfrågar deras position senast de var online. Förlorat läge kräver inte att Hitta min iPhone är aktiverat.

### Aktiveringslås

Med iOS 7.1 eller senare kan du använda MDM för att slå på aktiveringslåset när en användare aktiverar Hitta min på en övervakad enhet. Då kan din organisation dra nytta av aktiveringslåsets stöldförebyggande funktion, samtidigt som ni kan kringgå funktionen om en användare inte kan autentisera sig med sitt Apple-ID.

## Driftsätt och hantera ytterligare innehåll

Organisationer behöver ofta distribuera appar så att användarna kan vara produktiva. Dessutom behöver organisationer styra hur apparna ansluter till interna resurser och hur datasäkerheten hanteras när en användare lämnar organisationen. Detta samtidigt som användarens personliga appar och data hanteras.

### Interna app-portaler

De flesta MDM-lösningar erbjuder interna app-portaler. Du kan även skapa en egen intern app-portal för dina medarbetare där de enkelt kan hitta appar till iPhone eller iPad. Interna appar, webbadresser för App Store-appar, Apple Business Manager-koder och skräddarsydda appar kan tillhandahållas via denna portal, vilket gör den till en samlad plats för användarna. Du kan hantera och skydda den här platsen centralt. Med en intern app-portal blir det enkelt för medarbetarna att hitta godkända resurser som de behöver och de slipper kontakta it-avdelningen.

### Hanterat innehåll

Hanterat innehåll omfattar installation, konfiguration, hantering och borttagning av App Store-appar och interna appar, konton, böcker och dokument.

- **Hanterade appar.** Med hanterade appar i iOS och iPadOS kan en organisation distribuera gratisappar, betalappar och företagsappar trådlöst via MDM, med rätt balans mellan skydd av företagsdata och respekt för användarens integritet. 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. En app kan laddas ner igen från App Store om den fortfarande är tilldelad en användare genom Apple Business Manager, eller om användaren löser in en appkod med sitt personliga Apple-ID, men hanteras då inte av MDM.
- **Hanterade konton.** MDM kan automatiskt ställa in användarnas e-post och andra konton så att de kommer igång snabbt. Beroende på leverantör av MDM-lösning och integrering med interna system kan kontons nyttolaster även förkonfigureras med användarens namn, e-postadress och eventuella certifikatidentiteter för autentisering och signering.
- **Hanterade böcker och dokument.** Du kan skicka verktyg, böcker, ePub-böcker och pdf-dokument automatiskt via MDM till användares enheter. På så sätt har medarbetarna alltid vad de behöver. Däremot kan hanterade böcker bara delas med andra hanterade appar och mejlas från hanterade konton. När materialet inte längre används kan det fjärraderas. Böcker som köps in via Apple Business Manager kan tilldelas som hanterade böcker, men de kan inte återkallas eller distribueras till andra användare. En bok som användaren har köpt tidigare kan inte bli hanterad såvida den inte uttryckligen tilldelas användaren via Apple Business Manager.

## Hanterad appkonfiguration

Apputvecklare kan skapa inställningar och funktioner i appar som kan aktiveras om appen installeras som en hanterad app. Ställ in den här konfigurationen innan eller efter att den hanterade appen installeras. It-avdelningen kan till exempel definiera en uppsättning förvalda inställningar för en SharePoint-app så att användaren inte behöver konfigurera några serverinställningar manuellt.

Ledande leverantörer av MDM-lösningar har upprättat AppConfig Community och ett standardschema som alla apputvecklare kan använda som stöd för hanterad appkonfiguration. AppConfig Community utvecklar verktyg och bästa metoder för systemspecifika funktioner hos mobila operativsystem. Det bidrar till ett öppnare, enklare och mer konsekvent sätt att konfigurera och skydda mobilappar och få fler företag att införa mobila lösningar.

Läs mer om AppConfig Community:
appconfig.org

## Hanterat dataflöde

MDM-lösningar har specifika funktioner för detaljerad hantering av företagsdata, så att dessa hindras från att läcka ut till användarens privata appar och molntjänster.

- **Administrerad öppning.** Hanterad öppning tillämpar en uppsättning begränsningar som förhindrar att bilagor och dokument från hanterade källor öppnas på ohanterade platser och vice versa. Du kan exempelvis förhindra att en konfidentiell e-postbilaga i organisationens hanterade e-postkonto öppnas i någon av användarens personliga appar. Arbetsdokumentet kan bara öppnas av appar som är installerade och hanterade av MDM. Användarens ohanterade personliga appar visas inte i listan över appar som kan användas för att öppna bilagan. Utöver hanterade appar, konton, böcker och domäner finns det ett flertal tillägg som respekterar begränsningarna som gäller för administrerad öppning.
- **Enappsläge.** Den här inställningen begränsar iOS- eller iPadOS-enheten till en enda app och är perfekt för kiosker eller enheter som bara har ett syfte, till exempel butikskassor eller enheter för inskrivning av patienter på sjukhus. Utvecklare kan också införa den här funktionen i sina appar, så att apparna kan aktivera och avaktivera enappsläget på egen hand.
- **Förhindra säkerhetskopiering.** Den här begränsningen förhindrar att hanterade appar säkerhetskopierar data till iCloud eller till en dator. Om säkerhetskopiering förhindras 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- och iPadOS-användare och it-administratörer.

## AppleCare for Enterprise

För företag som önskar heltäckande skydd kan AppleCare for Enterprise hjälpa till att minska belastningen på den interna helpdesken genom att ge teknisk support per telefon dygnet runt, med en timmes svarstid för problem med högsta prioritet. Programmet omfattar support till it-avdelningar för all hårdvara och mjukvara från Apple. Dessutom ingår support för komplexa driftsättnings- och integreringsscenarier såsom MDM och Active Directory.

## AppleCare OS Support

Med AppleCare OS Support får it-avdelningen företagssupport per telefon och e-post för driftsättningar med iOS, iPadOS, macOS och macOS Server. Programmet erbjuder support dygnet runt och en särskild Technical Account Manager, beroende på vilken supportnivå du valt. 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 avancerad serverdrift.

## 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- och iPadOS-enheter.

## AppleCare för iOS- eller iPadOS-enheter

Varje iOS- och iPadOS-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 eller iPad och AppleCare+ 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 behöver repareras. Avtalen täcker även upp till två fall av oavsiktlig skada (för varje fall tillkommer en självrisk).

## iOS Direct Service-programmet

iOS Direct Service ingår i AppleCare+ och hjälper er helpdesk att övervaka problem med enheterna utan att ni behöver ringa AppleCare eller besöka en Apple Store-butik. Vid behov kan ni direkt beställa ersättningsprodukter för iPhone, iPad, iPod touch eller tillbehör som levereras tillsammans med dessa.

Läs mer om AppleCare-program:
apple.com/se/support/professional

# Sammanfattning

Oavsett om ditt företag driftsätter iPhone eller iPad till en grupp användare eller inom hela organisationen finns det många alternativ som gör det enkelt att driftsätta och hantera enheterna. 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 driftsättning av iOS och iPadOS samt funktioner för hantering och säkerhet:
support.apple.com/guide/deployment-reference-ios

Läs mer om MDM-inställningar för it-avdelningen:
support.apple.com/guide/mdm

Läs mer om Apple Business Manager:
support.apple.com/guide/apple-business-manager

Läs mer om hanterade Apple-ID:n för företag:
apple.com/business/docs/site/Overview_of_Managed_Apple_IDs_for_Business.pdf

Läs mer om Apple at Work:
www.apple.com/se/business/

Läs mer om it-funktioner:
www.apple.com/se/business/it/

Läs mer om säkerhet på Apple-plattformen:
www.apple.com/security/

Bläddra bland tillgängliga AppleCare-program:
www.apple.com/se/support/professional/

Upptäck Apple-utbildning och certifiering:
training.apple.com

Kontakta Apple Professional Services:
consultingservices@apple.com

Vissa appar och böcker är inte tillgängliga i alla länder och regioner eller hos alla utvecklare. Kontrollera tillgänglighet för program och innehåll. Vissa funktioner kräver wifi-anslutning. En del funktioner finns inte i alla länder. Lägsta samt rekommenderade systemkrav för iCloud finns på support.apple.com/HT204230.