



Oversigt

# Implementering af iOS

# Oversigt

## Indhold

[Oversigt](#)

[Ejerskabsmodeller](#)

[Trin i implementeringen](#)

[Muligheder for support](#)

[Opsummering](#)

iPhone og iPad kan fuldstændigt forandre, hvordan virksomheden fungerer, og hvordan medarbejderne arbejder. De kan øge produktiviteten betydeligt og give dine medarbejdere frihed og fleksibilitet til at arbejde på nye måder, uanset om de er på kontoret eller på farten. Når du udnytter denne moderne tilgang til arbejdet, gavner det hele virksomheden. Brugere har bedre adgang til information, så de føler sig bedre rustet og kan bruge deres kreativitet til at løse problemer. Ved at understøtte iOS bliver IT-afdelingerne betragtet som dem, der udformer virksomhedens strategi og løser de reelle problemer frem for blot at lave reparationer og omkostningsbesparelser. I sidste ende gavner det alle: Medarbejderne oplever ny energi i virksomheden, og der opstår nye forretningsmuligheder overalt.

Det har aldrig været nemmere at indstille og implementere iPhone og iPad i hele virksomheden. Apple Business Manager og en løsning til administration af mobile enheder fra en tredjepartsleverandør gør det nemt for virksomheden at implementere iOS-enheder og apps i et stort omfang.

- Administration af mobile enheder (MDM) giver dig mulighed for at konfigurere og administrere enhederne samt at distribuere og administrere apps helt trådløst.
- Apple Business Manager automatiserer tilmeldingen af Apple-enheder til jeres MDM-løsning og gør dermed implementeringen nemmere, idet konfigurationen kan ske uden fysisk håndtering i IT-afdelingen.
- Med Apple Business Manager kan du også købe apps og bøger i store mængder og distribuere dem trådløst til brugere.

Dette dokument vejleder dig i at implementere iOS-enheder i din virksomhed og hjælper dig med at lave en implementeringsplan, der passer perfekt til dit virksomhedsmiljø. De ordninger og værktøjer, som er nævnt i afsnittet Trin i implementeringen i denne oversigt, beskrives mere udførligt i online-vejledningen iOS – Håndbog om implementering:

[help.apple.com/deployment/ios](https://help.apple.com/deployment/ios)

# Ejerskabsmodeller

At vurdere ejerskabsmodeller og vælge den rigtige model for din virksomhed er et vigtigt første skridt i implementeringsprocessen. Implementering kan gribes an på forskellige måder, alt efter hvem der ejer de enkelte enheder. Som det første skal du fastslå, hvad der er bedst for din virksomhed.

Der anvendes typisk to ejerskabsmodeller til iOS-enheder i virksomheder:

- Virksomhedsejet
- Brugerejet

Selvom mange virksomheder har én model, de foretrækker, kan det være, at der anvendes forskellige modeller i dit miljø. En virksomhedsafdeling kan for eksempel anvende en brugerejet strategi, hvor medarbejderne kan indstille en personlig iPad, samtidig med at virksomhedens ressourcer beskyttes og administreres uden at påvirke brugernes private data og apps. Samtidig vil virksomhedens detailbutikker måske anvende en virksomhedsejet strategi, så flere medarbejdere kan dele iOS-enheder for at gennemføre kundernes betalinger.

Ved at se nærmere på disse modeller kan du finde den bedste løsning til netop dit miljø. Når du har fundet den rette model for din virksomhed, kan dit team se nærmere på Apples funktioner til implementering og administration.

## Virksomhedsejede enheder

Med en virksomhedsejet model kan du købe enheder hos Apple eller en autoriseret Apple-forhandler eller udbyder, som er med i ordningen. I disse tilfælde kan du give en enhed til hver bruger (dette kaldes implementering med personlig tilpasning) eller lade enhederne gå på skift mellem brugerne (dette kalder vi ikke-individualiseret implementering). Med en kombination af disse modeller, essentielle teknologier fra Apple og en MDM-løsning kan du få indstilling og konfiguration af enhederne til at ske helt automatisk.

**Enhed med personlig tilpasning.** Når du bruger en strategi med personlig tilpasning, kan du lade hver bruger vælge sin egen enhed og tilmelde den til en MDM-løsning, som trådløst overfører virksomhedens indstillinger og apps til hver enhed. I forbindelse med enheder, som er købt direkte hos Apple eller autoriserede Apple-forhandlere eller udbydere, der deltager i ordningen, kan du også med fordel anvende Apple Business Manager til automatisk at tilmelde nye enheder til jeres MDM-løsning. Når disse enheder er konfigureret, kan brugerne tilføje deres egne apps og data i tillæg til en hvilken som helst virksomhedskonto eller app fra din virksomhed.

**Ikke-individualiseret.** Når enheder deles af flere personer eller bruges til et bestemt formål (f.eks. i en restaurant eller på et hotel), vil IT-administratorer typisk konfigurere og administrere dem centralt i stedet for at skulle regne med, at den enkelte bruger foretager indstillingen. Ved ikke-individualiseret implementering er det normalt ikke tilladt for brugerne at installere apps eller gemme nogen private data på enheden. Følgende diagram illustrerer de handlinger, der kræves af både administratoren og brugeren under hvert trin i en strategi med virksomhedsejede enheder. Medmindre andet er angivet, gælder handlingerne for begge typer implementering, altså både *med personlig tilpasning* og *ikke-individualiseret*.

	Administrator	Bruger
<b>Forberedelse</b>	<ul style="list-style-type: none"> <li>• Evaluering af infrastrukturen</li> <li>• Valg af en MDM-løsning</li> <li>• Tilmelding til Apple Business Manager</li> </ul>	<ul style="list-style-type: none"> <li>• Ingen handling påkrævet</li> </ul>
<b>Indstilling</b>	<ul style="list-style-type: none"> <li>• Konfiguration af enheder</li> <li>• Distribuering af apps og bøger</li> </ul>	<ul style="list-style-type: none"> <li>• Ingen handling påkrævet</li> </ul>
<b>Implementering</b>	<ul style="list-style-type: none"> <li>• Distribuering af enhederne</li> </ul> <p><b>Kun med personlig tilpasning</b></p> <ul style="list-style-type: none"> <li>• Giv brugerne mulighed for at tilpasse enhederne</li> </ul>	<p><b>Kun med personlig tilpasning</b></p> <ul style="list-style-type: none"> <li>• Download og installation af apps og bøger</li> <li>• Brug af Apple-id, iTunes Store og iCloud-konti, hvis det er relevant</li> </ul> <p><b>Kun ved ikke-individualiseret</b></p> <ul style="list-style-type: none"> <li>• Ingen handling påkrævet</li> </ul>
<b>Administration</b>	<ul style="list-style-type: none"> <li>• Administration af enheder</li> <li>• Implementering og administration af yderligere indhold</li> </ul>	<p><b>Kun med personlig tilpasning</b></p> <ul style="list-style-type: none"> <li>• Find nye nyttige apps</li> </ul> <p><b>Kun ved ikke-individualiseret</b></p> <ul style="list-style-type: none"> <li>• Ingen handling påkrævet</li> </ul>

## Brugerejede enheder

Når enheder købes og indstilles af brugerne – normalt kaldet BYOD (Bring Your Own Device) – kan du stadig give adgang til virksomhedens tjenester såsom Wi-Fi, mail og kalendere via MDM. Brugere skal vælge at tilmelde sig din virksomheds MDM-løsning.

**Egne enheder medbringes – BYOD.** En BYOD-løsning giver brugerne mulighed for at indstille og konfigurere deres egne enheder. Brugere kan tilmelde deres enheder til din virksomheds MDM-løsning for at få adgang til virksomhedens ressourcer, konfigurere forskellige indstillinger, installere en konfigurationsbeskrivelse eller installere virksomhedsapps.

En fordel ved at bruge MDM til tilmelding af personlige enheder er, at det bliver muligt at administrere virksomhedens ressourcer og data på en sikker måde, som samtidig respekterer brugernes privatliv, personlige data og apps. IT-afdelingen kan ændre indstillinger, kontrollere, at virksomhedens politikker bliver overholdt, og fjerne virksomhedsdata og apps, at imens de private data og apps på hver brugers enhed fortsat er uberørte.

Følgende diagram illustrerer de handlinger, der kræves af både administratoren og brugeren under hvert trin i en implementering med brugerejede enheder.

	<b>Administrator</b>	<b>Bruger</b>
<b>Forberedelse</b>	<ul style="list-style-type: none"><li>• Evaluering af infrastrukturen</li><li>• Valg af en MDM-løsning</li><li>• Tilmelding til Apple Business Manager</li></ul>	<ul style="list-style-type: none"><li>• Brug af Apple-id, iTunes Store og iCloud-konti, hvis det er relevant</li></ul>
<b>Indstilling</b>	<ul style="list-style-type: none"><li>• Konfiguration af enheder</li><li>• Distribuering af apps og bøger</li></ul>	<ul style="list-style-type: none"><li>• Tilmelding til virksomhedens MDM-løsning</li><li>• Download og installation af apps og bøger</li></ul>
<b>Implementering</b>	<ul style="list-style-type: none"><li>• Ingen handling påkrævet</li></ul>	<ul style="list-style-type: none"><li>• Ingen handling påkrævet</li></ul>
<b>Administration</b>	<ul style="list-style-type: none"><li>• Administration af enheder</li><li>• Implementering og administration af yderligere indhold</li></ul>	<ul style="list-style-type: none"><li>• Find nye nyttige apps</li></ul>

# Trin i implementeringen

I dette afsnit kan du læse flere detaljer om hvert af de fire trin til implementering af enheder og indhold: forberedelse af miljøet samt indstilling, implementering og administration af enheder. De trin, du skal følge, afhænger af, om virksomheden eller brugerne ejer enhederne.

## 1. Forberedelse

Når du har fundet frem til den rette implementeringsmodel for din virksomhed, skal du følge disse trin for at klargøre fundamentet for implementeringen. Det kan gøres, allerede inden du har enhederne i hånden.

### Evaluering af infrastrukturen

iPhone og iPad integreres problemfrit i de fleste almindelige IT-miljøer hos virksomhederne. Det er vigtigt at evaluere jeres eksisterende netværksinfrastruktur for at sikre, at virksomheden får fuldt udbytte af alt det, iOS har at byde på.

### Wi-Fi og netværk

Velfungerende og pålidelig adgang til et trådløst netværk er afgørende for indstillingen og konfigurationen af iOS-enheder. Undersøg, om din virksomheds Wi-Fi-netværk understøtter flere enheder ad gangen med samtidige forbindelser fra alle dine brugere. Du skal muligvis konfigurere dine webproxy- eller firewall-porte, hvis enhederne ikke kan få adgang til Apples aktiveringsservere, iCloud eller iTunes Store. Apple og Cisco har også optimeret den måde, iPhone og iPad kommunikerer med Ciscos trådløse netværk på, og det baner vejen for andre avancerede netværksfunktioner såsom hurtig roaming og QoS-optimering (Quality of Service) til apps.

Evaluer din VPN-infrastruktur for at sikre, at brugerne kan få sikker ekstern adgang til virksomhedens ressourcer via deres iOS-enheder. Overvej at bruge funktioner som VPN on Demand eller Pr.-app-VPN i iOS, så der kun oprettes en VPN-forbindelse, når det er nødvendigt. Hvis du overvejer at bruge Pr.-app-VPN, skal du sørge for, at dine VPN-gateways understøtter disse funktioner, og købe tilstrækkeligt mange licenser til antallet af brugere og forbindelser.

Du skal også sørge for, at din netværksinfrastruktur er konfigureret til at fungere korrekt med Bonjour, Apples standardbaserede netværksprotokol uden behov for konfiguration. Med Bonjour kan enhederne automatisk finde tjenester på et netværk. iOS-enheder bruger Bonjour til at oprette forbindelse til AirPrint-kompatible printere og AirPlay-kompatible enheder såsom Apple TV. Nogle apps bruger også Bonjour til at finde andre enheder til samarbejde og deling.

For yderligere oplysninger om Wi-Fi og netværk til implementeringer i virksomheder henvises der til iOS – Håndbog om implementering: [help.apple.com/deployment/ios](http://help.apple.com/deployment/ios)

Læs mere om Bonjour:  
[apple.com/dk/support/bonjour](http://apple.com/dk/support/bonjour)

### Mail, kontakter og kalendere

Hvis I bruger Microsoft Exchange, skal du kontrollere, at ActiveSync-tjenesten er opdateret og konfigureret til at understøtte alle brugere på netværket. Hvis I bruger det cloud-baserede Office 365, skal du sørge for at have licenser nok til at understøtte det forventede antal iOS-enheder, der skal tilsluttes. iOS understøtter også moderne Office 365-godkendelse og gør brug af OAuth 2.0 og multifaktorgodkendelse. Hvis du ikke bruger Exchange, fungerer iOS med standardbaserede servere, herunder IMAP, POP, SMTP, CalDAV, CardDAV og LDAP.

### Indlæsning af indhold i buffer

I macOS High Sierra eller nyere sørger en integreret funktion – indlæsning af indhold i buffer – for at lagre en lokal kopi af ofte anvendt indhold fra Apple-servere, så systemet kræver mindre båndbredde, når det overfører indhold på netværket. Indlæsning af indhold i buffer gør det hurtigere at hente og levere software via App Store, Mac App Store, iTunes Store og Apple Books.

Denne funktion kan også lagre softwareopdateringer, så du opnår hurtigere overførsel til iOS-enheder. Indlæsning af indhold i buffer omfatter tjenesten tethered caching, som gør en Mac i stand til at dele sin internetforbindelse med et stort antal iOS-enheder tilsluttet via USB.

Læs mere om indlæsning af indhold i buffer:

[support.apple.com/da-dk/HT208025](https://support.apple.com/da-dk/HT208025)

Læs mere om tethered caching:

[support.apple.com/da-dk/HT207523](https://support.apple.com/da-dk/HT207523)

### iTunes-understøttelse

iTunes er ikke nødvendig på enheder med iOS 5 eller nyere, men du kan vælge at understøtte iTunes, så brugerne kan aktivere enheder, synkronisere medier eller sikkerhedskopiere deres enheder til en computer.

iTunes understøtter adskillige muligheder for konfiguration ved implementering, som er hensigtsmæssige i virksomheder, herunder deaktivering af adgang til bestemt indhold, fastlæggelse af, hvilke netværkstjenester brugerne kan tilgå i iTunes, og krav om krypterede sikkerhedskopier.

### Valg af en MDM-løsning

Med Apples administrationsplatform for iOS kan virksomheder implementere enheder i virksomhedsmiljøet på en sikker måde, konfigurere og opdatere indstillinger trådløst, holde øje med overholdelsen af politikker, installere apps og bøger og slette eller låse administrerede enheder eksternt. Disse administrationsfunktioner udføres via MDM-løsninger fra tredjepartsleverandører.

Der findes et udvalg af MDM-løsninger fra tredjeparter, som understøtter forskellige serverplatforme. Hver løsning byder på forskellige administrationskonsoller, funktioner og priser. Inden du vælger en løsning, kan du bruge nedenstående ressourcer til at vurdere, hvilke MDM-funktioner der er mest relevante for din virksomhed. Udover MDM-løsninger fra tredjepartsleverandører findes der en løsning fra Apple – den hedder Profile Manager og er en funktion i macOS Server.

Læs mere om administration af enheder og virksomhedsdata i iOS:

[images.apple.com/dk/business/resources/docs/Managing\\_Devices\\_and\\_Corporate\\_Data\\_on\\_iOS.pdf](https://images.apple.com/dk/business/resources/docs/Managing_Devices_and_Corporate_Data_on_iOS.pdf)

Læs mere om Profile Manager:

[www.apple.com/macos/server/features/#profile-manager](https://www.apple.com/macos/server/features/#profile-manager)

### Tilmelding til Apple Business Manager

Apple Business Manager er et nyt sted, hvor IT-teams kan automatisere implementering af enheder, købe og distribuere indhold samt administrere de forskellige roller i deres organisation. Apple Business Manager fungerer perfekt sammen med dit system til administration af mobile enheder (MDM) og gør det nemt at tilmelde enheder, implementere indhold og tildele administrative rettigheder.

Apples tilmeldingsordning for enheder (DEP) og mængdekøbsordningen (VPP) er integreret i Apple Business Manager, så alt, hvad du behøver for at implementere iOS-enheder, Mac-computere og Apple TV, er nu samlet på ét sted.

### Enheder

Tilmeldingen af enheder er nu en del af Apple Business Manager og giver en hurtig og effektiv måde at implementere virksomhedsejede Apple-enheder på.

- Du kan automatisk tilmelde enheder til MDM uden at have enhederne i hånden eller klargøre dem, før de distribueres til brugerne. Det sikrer, at alle brugere får din organisations konfigurationer med det samme, når de aktiverer deres enhed.
- Du kan forenkle konfigurationsprocessen for brugerne ved at fjerne visse trin i indstillingsassistenten, så brugerne hurtigt kan komme i gang. Og enhedsovervågning giver flere muligheder for administration af iOS- og tvOS-enheder, f.eks. MDM, som ikke kan fjernes.
- Det er nemmere at administrere standard MDM-servere ved at installere en standardserver, der er baseret på enhedstype. Desuden kan du nu tilmelde iOS-enheder og Apple TV manuelt ved hjælp af Apple Configurator 2, uanset hvordan du har anskaffet dem.

### Indhold

Sektionen Apps og bøger i Apple Business Manager gør det lettere for organisationer at købe indhold i store mængder. Hvad enten din medarbejderstab bruger iPhone, iPad eller Mac, kan du levere fantastisk indhold, som er klar til brug i arbejdsopgaverne med fleksible og sikre distributionsmuligheder. Bemærk: Køb af bøger i Apple Business Manager er ikke tilgængelig i visse lande. Du kan læse mere om tilgængelige funktioner og indkøbsmetoder på [support.apple.com/da-dk/HT207867](https://support.apple.com/da-dk/HT207867).

- Køb apps, bøger og specialudviklede apps i store mængder. Det er nemt at overføre appicenser mellem forskellige lokaliteter samt at dele licenser mellem købere på samme lokalitet. Du kan også se en samlet liste over købshistorikken, herunder antallet af licenser, der bruges via MDM.



- Overfør apps og bøger direkte til administrerede enheder eller autoriserede brugere, og hold nemt styr på, hvilket indhold der er blevet tildelt til hvilken bruger eller enhed. Med administreret distribution kan du styre hele distributionsprocessen, så jeres organisation fortsat har fuldt ejerskab og kontrol over de apps, den har købt. Og apps, der ikke er nødvendige for en enhed eller bruger, kan tilbagekaldes og tildeles til andre inden for organisationen.
- Betal med forskellige betalingsmetoder, herunder betalingskort og købsordrer. Virksomheder kan købe mængdekøbskredit (hvor det er tilgængeligt) direkte fra Apple eller fra en autoriseret Apple-forhandler i specifikke dollarbeløb, der sendes elektronisk til kontohaveren som VPP-kredit.
- En app kan tildeles til enheder eller brugere i alle lande, hvor appen er tilgængelig, så den kan distribueres multinationalt i virksomheden. Udviklere kan gøre deres apps og programmer tilgængelige i flere lande gennem App Store-standardprocessen for udgivelse.

### Roller

Med Apple Business Manager kan du oprette konti, som din organisation ejer og administrerer for flere administratorer. Der introduceres også nogle ændringer i de roller, du tildeler dine brugere.

- Tilføj yderligere konti til administration af enheder eller indhold, tildel rettigheder og videregiv ansvar på en nem måde, hvis en person forlader virksomheden.
- Tildel roller via Apple Business Manager på et detaljeret niveau, så du kan tildele rettigheder til administration af enheder eller indhold til specifikke personer eller lokaliteter.
- Deaktiver og slet brugerkonti, så de pågældende brugere ikke kan logge ind.

I Apples implementeringsordninger var Agent den højeste grad af administrativ adgang. Agenten kunne acceptere vilkår og betingelser på organisationens vegne. Denne rolle kaldes nu for Administrator. Din organisation kan have op til fem administratorer i Apple Business Manager.

Apples implementeringsordninger omfattede administratorer for DEP og VPP. Administratorer kaldes nu for ansvarlige ledere i Apple Business Manager. Ved opgraderingen konverteres DEP-administratorer til Enhedsansvarlige, og VPP-administratorer konverteres til Indholdsansvarlige. Alle administratorer i Apples implementeringsordninger, der kunne oprette andre administratorer, bliver Personansvarlige.

En bruger kan have flere roller i Apple Business Manager. Alle de brugere, der var administratorer i mere end én ordning, vil få tildelt alle de tilsvarende roller i Apple Business Manager. Administratoren kan tilføje, fjerne eller ændre lederroller efter opgraderingen. Personansvarlige kan også ændre i andre lederroller, men ikke i administratorer.

Når din tidligere agent eller dine tidligere administratorer logger ind på Apple Business Manager for første gang, konverteres deres Apple-id'er til administrerede Apple-id'er. Hvis deres konti ikke var konfigureret til totrinsgodkendelse førhen, skal de nu konfigureres til totrinsgodkendelse.

Administrerede Apple-id'er er primært til brug for IT-administratorer, som administrerer funktioner i Apple Business Manager. De bør ikke anvendes til tjenester som iCloud eller af almindelige medarbejdere, der ikke administrerer funktioner i Apple Business Manager.

Læs mere om Apple Business Manager:

[www.apple.com/dk/business/it](http://www.apple.com/dk/business/it)

### Tilmelding til Apple Developer Enterprise Program

Du kan udvikle interne iOS-apps til din virksomhed ved hjælp af Apple Developer Enterprise Program. Dette program byder på en komplet og integreret proces til udvikling, test og distribution af iOS-apps til medarbejderne i din virksomhed. Interne apps indsendes ikke til App Store og bliver ikke gennemgået, godkendt eller distribueret af Apple.

Distribuer dine interne apps enten ved at hoste din app på en enkel intern webserver eller ved hjælp af en MDM-tredjepartsløsning. Fordelene ved at administrere interne apps med MDM er blandt andet muligheden for at konfigurere apps eksternt, administrere softwareversioner, konfigurere single sign-on, indstille retningslinjer for netværksadgang (f.eks. Pr.-app-VPN) og muligheden for at styre, hvilke apps der kan eksportere dokumenter. Din virksomheds specifikke krav, infrastruktur og niveau af app-administration afgør, hvilken løsning der egner sig bedst.

Læs mere om Apple Developer Enterprise Program:

[developer.apple.com/programs/enterprise](http://developer.apple.com/programs/enterprise)

## 2. Indstilling

Til dette trin kan du bruge Apple Business Manager, en MDM-løsning eller eventuelt Apple Configurator 2 til at indstille dine enheder og distribuere indhold. Indstillingsprocessen kan gribes an på forskellige måder, alt efter hvem der ejer de enkelte enheder, og hvilken implementeringsmetode du foretrækker.

### Konfigurer dine enheder

Der er flere muligheder for konfiguration af brugeradgang til virksomhedstjenester. IT-afdelingen kan indstille enheder ved at distribuere konfigurationsbeskrivelser. Der findes yderligere konfigurationsmuligheder til overvågede enheder.

### Konfiguration af enheder med MDM

Når dine enheder er tilmeldt en MDM-server på sikker vis, aktiveres administrationen ved hjælp af konfigurationsbeskrivelser – dvs. en XML-fil med konfigurationsoplysninger for en iOS-enhed. Disse beskrivelser automatiserer konfigurationen af indstillinger, konti, begrænsninger og brugeroplysninger. De kan leveres trådløst fra jeres MDM-løsning, og denne metode er ideel til konfiguration med minimal fysisk håndtering af flere enheder. Konfigurationsbeskrivelserne kan også sendes via mail, downloades fra en webside eller installeres på enheder gennem Apple Configurator 2.

- **Virksomhedsejede enheder.** Brug Apple Business Manager til at slå automatisk MDM-tilmelding til på brugernes enheder, når de aktiverer dem. Alle de iOS-enheder, der føjes til Apple Business Manager, er altid overvåget, og MDM-tilmelding er obligatorisk.

- **Brugerejede enheder.** Medarbejderne kan bestemme, om de vil tilmelde deres enhed til MDM eller ej. Og de kan til enhver tid afslutte forbindelsen til MDM ved ganske enkelt at fjerne konfigurationsbeskrivelsen fra deres enhed, og dermed bliver virksomhedsdata og -indstillinger også fjernet. Du bør dog overveje incitamenter til, at brugerne fortsat vælger løsningen med administration af deres enheder. Du kan for eksempel kræve, at brugerne tilmelder sig MDM for at få adgang til et Wi-Fi-netværk – ved at få jeres MDM-løsning til automatisk at levere brugeroplysningerne til det trådløse netværk.

Så snart en enhed er tilmeldt, kan en administrator aktivere en MDM-regel, -indstilling eller -kommando. Derefter modtager iOS-enheden meddelelser om administratorens handlinger gennem Apples tjeneste til push-meddelelser (APNs), så den kan kommunikere direkte med sin MDM-server via en sikker forbindelse. Med en netværksforbindelse kan enhederne modtage APNs-kommandoer hvor som helst i verden. Men der overføres ingen fortrolige eller proprietære oplysninger via APNs.

### Konfiguration af enheder med Apple Configurator 2 (valgfrit)

Til den lokale indledende implementering af flere enheder kan virksomheder bruge Apple Configurator 2. Med dette gratis macOS-program kan du koble iOS-enheder til en Mac-computer via USB og opdatere iOS-enheder til den nyeste version af iOS, konfigurere enhedsindstillinger og -begrænsninger samt installere apps og andet indhold. Efter den første indstilling kan du fortsætte med at administrere alting trådløst ved hjælp af MDM.

Apple Configurator 2 har en brugergrænseflade, hvor der er fokus på dine enheder og de separate opgaver, du gerne vil udføre på dem. Programmet er integreret med Apple Business Manager, så enheder kan tilmeldes automatisk til MDM med din virksomheds indstillinger. I Apple Configurator 2 kan der laves brugerdefinerede processer ved hjælp af Blueprints, så separate opgaver kan kombineres.

Læs mere om Apple Configurator 2:

[support.apple.com/da-dk/apple-configurator](https://support.apple.com/da-dk/apple-configurator)

### Overvågede enheder

Overvågning giver adgang til yderligere administrationsfunktioner for iOS-enheder, der ejes af din virksomhed, så du kan bruge forskellige begrænsninger såsom at deaktivere AirDrop eller sætte enheden i enkelt app-tilstand. Det giver også mulighed for at aktivere et webfilter gennem en global proxy, som sikrer, at brugernes internettrafik holder sig inden for virksomhedens retningslinjer, forhindrer brugerne i at gendanne enhedens fabriksindstillinger og meget mere. Som standard er alle iOS-enheder ikke-overvågede. Du kan enten bruge Apple Business Manager til at aktivere overvågning eller aktivere overvågning manuelt ved hjælp af Apple Configurator 2.

Selvom du måske ikke lige nu har planer om at bruge funktioner, der kun er tilgængelige i overvågningstilstand, bør du overveje at vælge overvågning af dine enheder, når du indstiller dem. Dermed kan du senere hen udnytte funktioner, der kun er tilgængelige på overvågede enheder. Ellers vil du være nødt til at slette de enheder, der allerede er taget i brug. Overvågning drejer sig ikke om at låse en enhed – det er i stedet et spørgsmål om at gøre virksomhedsejede enheder bedre ved at udvide administrationsfunktionerne. På længere sigt vil overvågning give din virksomhed endnu flere muligheder.

Se hele listen over overvågede indstillinger i [iOS – Håndbog om implementering](#).

## Distribuering af apps og bøger

Apple tilbyder omfattende ordninger for at hjælpe din virksomhed med at udnytte de fantastiske apps og ressourcer til iOS. Ved hjælp af disse funktioner kan du distribuere apps og bøger, der er købt gennem Apple Business Manager, eller apps, der er udviklet internt i virksomheden, til enheder og brugere for at give dem alt det, de skal bruge for at øge produktiviteten. På købstidspunktet skal du vælge din distributionsmetode: administreret distribution eller indløsningskoder.

### Administreret distribution

Med administreret distribution bruger du jeres MDM-løsning eller Apple Configurator 2 til at administrere de apps og bøger, der er købt gennem Apple Business Manager i et hvilket som helst land, hvor disse apps er tilgængelige. For at aktivere administreret distribution skal du først knytte jeres MDM-løsning til jeres Apple Business Manager-konto ved hjælp af et sikkert token. Når du har forbindelse til MDM-serveren, kan du tildele apps og bøger købt gennem Apple Business Manager, også selvom App Store er deaktiveret på selve enheden.

- **Tildel apps til enheder.** Tildel apps direkte til enheder ved hjælp af jeres MDM-løsning eller Apple Configurator 2. Denne metode springer flere trin over ved den første udrulning, så implementeringen bliver betydeligt nemmere og hurtigere, samtidig med at du har fuld kontrol over administrerede enheder og administreret indhold. Når en app er tildelt til en enhed, bliver appen overført til den pågældende enhed via MDM, og det er ikke nødvendigt at invitere brugeren. Alle brugere af denne enhed har adgang til appen.
- **Tildel apps og bøger til brugerne.** En anden metode er at bruge jeres MDM-løsning til at invitere brugere til at downloade apps og bøger gennem en mail eller en push-meddelelse. For at acceptere invitationen skal brugerne logge ind på deres enheder med et personligt Apple-id. Apple-id'et er registreret i Apple Business Manager, men det er stadig helt privat og kan ikke ses af administratoren. Når brugerne accepterer invitationen, får de forbindelse til MDM-serveren, så de kan modtage tildelte apps og bøger. Disse apps er automatisk tilgængelige til download på alle brugernes enheder – uden yderligere besvær eller omkostninger for dig.

Når en enhed eller bruger ikke længere har behov for apps, du har tildelt, kan de inddrages og tildeles til andre enheder og brugere, så din virksomhed beholder den fulde ejendomsret og kontrol over købte apps. Når købte bøger er blevet distribueret, tilhører de imidlertid modtageren, og de kan ikke inddrages og tildeles igen.

### Indløsningskoder

Du kan også distribuere indhold ved hjælp af indløsningskoder. Det er især praktisk, hvis virksomheden ikke kan bruge MDM på slutbrugerens enhed, for eksempel i forbindelse med franchising. Denne metode overfører permanent en app eller en bog til den bruger, der indløser koden. Indløsningskoderne leveres i et regneark. Der gives en unik kode for alle købte apps eller bøger i det antal, som købes. Hver gang en kode bliver indløst, opdateres regnearket i Apple Business Manager-butikken, så du til hver en tid kan se antallet af indløste koder. Du kan distribuere koder via MDM, Apple Configurator 2, mail eller et internt website.

### Installation af apps og indhold med Apple Configurator 2 (valgfrit)

Udover grundlæggende indstilling og konfiguration kan Apple Configurator 2 også bruges til at installere apps og indhold på enheder, du vil indstille på brugernes vegne. Ved implementeringer med personlig tilpasning kan du forudinstallere apps og dermed spare tid og netværksbåndbredde. I forbindelse med ikke-individualiserede løsninger kan du også udføre indstillingen af iOS-enhederne helt frem til hjemmeskærmen. Når enheder konfigureres med Apple Configurator 2, kan du installere apps fra App Store, interne apps og dokumenter. Apps fra App Store kræver Apple Business Manager. Dokumenter er tilgængelige til apps, som understøtter iTunes-fildeling. For at gennemgå eller hente dokumenter fra iOS-enheder skal du forbinde dem med en Mac med Apple Configurator 2.

## 3. Implementering

iOS gør det let for medarbejderne at begynde at bruge deres enheder direkte fra æsken, uden at det kræver assistance fra IT-afdelingen.

### Distribuer dine enheder

Når enhederne er klargjort og indstillet som beskrevet i de første to trin, er de klar til at blive distribueret. Ved implementeringer med personlig tilpasning skal du udlevere enhederne til brugerne, der så hver især kan bruge den effektive indstillingsassistent til at tilpasse deres enheder yderligere og afslutte indstillingen. Ved ikke-individualiseret implementering skal du distribuere enhederne til medarbejdere, der arbejder på skift, eller placere enhederne i standere, der er beregnet til at oplade og beskytte dem.

### Indstillingsassistent

iOS-brugere kan aktivere deres enhed, konfigurere grundlæggende indstillinger og begynde at arbejde med det samme med indstillingsassistenten i iOS. Efter den første indstilling kan brugerne også indstille deres personlige præferencer såsom sprog, placering, Siri, iCloud og Find min iPhone. Enheder, der er tilmeldt Apple Business Manager, bliver automatisk tilmeldt MDM direkte i indstillingsassistenten.

### Giv brugerne mulighed for at tilpasse enhederne

Ved implementeringer med personlig tilpasning og BYOD vil det øge produktiviteten, hvis brugerne får lov til at tilpasse deres enheder med deres eget Apple-id, fordi brugerne dermed kan vælge de apps og det indhold, der bedst muligt hjælper dem med at udføre deres opgaver og nå deres mål. Virksomhedsdata bliver ved med at være separate fra private data i iOS.

### Apple-id

Et Apple-id er en identitet, som anvendes til at logge ind på forskellige Apple-tjenester såsom FaceTime, iMessage, iTunes Store, App Store, Apple Books og iCloud. Disse tjenester giver brugere adgang til et bredt udvalg af indhold, der kan effektivisere arbejdsopgaver, øge produktiviteten og bruges til samarbejde.

For at få mest muligt ud af disse tjenester bør brugerne anvende deres eget Apple-id. Brugere, der ikke har et Apple-id, kan oprette et, allerede inden de modtager en enhed. Indstillingsassistenten gør det også muligt for brugerne at oprette et personligt Apple-id, hvis de ikke allerede har et. Brugere behøver ikke at have et betalingskort for at oprette et Apple-id.

Læs, hvordan du får et Apple-id uden et betalingskort:

[support.apple.com/da-dk/ht204034](https://support.apple.com/da-dk/ht204034)

Få et Apple-id:

[support.apple.com/da-dk/ht204316](https://support.apple.com/da-dk/ht204316)

### iCloud

Med iCloud kan brugerne automatisk synkronisere dokumenter og personligt indhold – såsom kontakter, kalendere, dokumenter og billeder – og holde dem opdateret mellem flere enheder. Brugere kan også sikkerhedskopiere en iOS-enhed automatisk, når den er forbundet til Wi-Fi, og bruge Find min iPhone til at finde en mistet eller stjålet iPhone, iPad, iPod touch eller Mac.

Nogle tjenester – f.eks. Fotostream, iCloud-nøglering, iCloud Drive og iCloud-sikkerhedskopiering – kan deaktiveres ved at bruge begrænsninger, som enten indtastes manuelt på enheden eller indstilles via konfigurationsbeskrivelser. Desuden kan en MDM-løsning forhindre, at administrerede apps bliver sikkerhedskopieret til iCloud. Denne funktion er fordelagtig for brugerne, fordi de kan bruge iCloud til deres private data og undgå, at virksomhedsoplysningerne gemmes i iCloud. Data fra virksomhedskonti, f.eks. Exchange, eller data, som er lagret i interne virksomhedsapps, bliver ikke sikkerhedskopieret til iCloud.

Læs mere om iCloud:

[www.apple.com/dk/icloud](https://www.apple.com/dk/icloud)

## 4. Administration

Når brugerne er kommet godt i gang, findes der en lang række administrative funktioner til administration og vedligeholdelse af enhederne og indhold over længere tid.

### Administrer dine enheder

En administreret enhed kan administreres af MDM-serveren gennem en række specifikke opgaver. Disse opgaver består bl.a. i at sende forespørgsler om oplysninger til enheder samt at starte administrationsopgaver, der giver mulighed for at administrere enheder, som ikke følger retningslinjerne, er mistet eller stjålet.

### Forespørgsler

En MDM-server kan anmode enheder om en række oplysninger, herunder hardwareoplysninger – f.eks. serienummer, enheds-UDID eller Wi-Fi-MAC-adresse – samt softwareoplysninger, f.eks. iOS-versionen og en detaljeret liste over alle de apps, der er installeret på enheden. Jeres MDM-løsning kan bruge disse oplysninger til at holde lageroplysningerne opdaterede, træffe velinformerede beslutninger om administration og automatisere administrationsopgaver, der f.eks. skal sikre, at brugerne har de rette apps installeret.

### Administrationsopgaver

Når en enhed bliver administreret, kan en MDM-server udføre mange forskellige administrationsopgaver, herunder automatisk ændring af konfigurationsindstillingerne uden brugerinteraktion, installation af en iOS-opdatering på enheder låst med adgangskode, ekstern låsning eller sletning af en enhed eller fjernelse af en adgangskodelås, så brugere kan nulstille glemte adgangskoder. En MDM-server kan anmode en iOS-enhed om at starte AirPlay-skærmdublering til en bestemt destination eller afslutte en aktuel AirPlay-session.

### Administrerede softwareopdateringer

Du kan forhindre, at brugere opdaterer en overvåget enhed manuelt og trådløst inden for et bestemt tidsrum. Når du implementerer denne begrænsning, er udsættelsen som standard 30 dage, og den træder i kraft i det øjeblik, Apple frigiver en iOS-opdatering. Du kan dog ændre standardværdien for det antal dage, du ønsker at forhindre opdateringer, inden for et interval på én til 90 dage. Du kan også planlægge softwareopdateringer på overvågede enheder via jeres MDM-løsning.

### Funktionen Mistet

Jeres MDM-løsning kan eksternt slå funktionen Mistet til på en overvåget enhed. Denne handling låser enheden og giver tilladelse til, at der vises en besked med et telefonnummer på låseskærmen. Ved hjælp af funktionen Mistet kan du finde overvågede enheder, der er blevet væk eller stjålet, fordi MDM sender eksterne forespørgsler om deres placering, sidst de var online. Funktionen Mistet kræver ikke, at Find min iPhone er aktiveret.

### Aktiveringslås

Med iOS 7.1 eller nyere kan du bruge MDM til at slå Aktiveringslås til, når en bruger slår Find min iPhone til på en overvåget enhed. Dermed kan virksomheden få gavn af tyverisikringen i Aktiveringslås, mens du stadig kan omgå funktionen, f.eks. hvis en bruger ikke kan godkendes med sit Apple-id.

### Implementering og administration af yderligere indhold

Virksomheder har ofte behov for at distribuere apps for at gøre deres brugere mere produktive. Samtidig skal virksomhederne kunne kontrollere, hvordan apps opretter forbindelse til interne ressourcer, eller hvordan data håndteres på sikker vis, når en bruger forlader virksomheden – alt sammen side om side med brugerens personlige apps og data.

### Interne app-portaler

De fleste MDM-servere giver adgang til interne app-portaler som en del af deres løsning, og ellers kan du oprette din egen interne app-portal for dine medarbejdere, hvor de nemt kan finde apps til deres iOS-enheder. På denne portal kan der linkes til interne apps, URL-adresser til apps fra App Store, Apple Business Manager-koder eller brugerdefinerede B2B Apple Business Manager-koder, så brugerne har alt på ét sted. Du kan administrere og sikre dette website centralt. En intern app-portal gør det nemt for medarbejderne at finde de godkendte ressourcer, de har brug for, uden at skulle kontakte IT-afdelingen.

### Administreret indhold

Administreret indhold omfatter installation, konfiguration, administration og fjernelse af indhold fra App Store og specialudviklede interne apps, konti, bøger og dokumenter.

- **Administrerede apps.** I iOS kan en virksomhed bruge administrerede apps, som gør det muligt at distribuere gratis, betalte og interne apps trådløst ved hjælp af MDM, mens man både beskytter virksomhedens data og respekterer brugernes privatliv. Administrerede apps kan fjernes eksternt af MDM-serveren, eller når brugerne fjerner deres egen enhed fra MDM. Fjernelsen af appen fjerner også de data, som er tilknyttet appen. Hvis en app fortsat er tildelt brugeren gennem Apple Business Manager, eller hvis brugeren indlæste en appkode ved hjælp af et personligt Apple-id, kan appen downloades igen fra App Store, men den vil ikke længere være administreret af MDM.
- **Administrerede konti.** MDM kan hjælpe dine brugere hurtigt i gang ved at indstille deres mail og andre konti helt automatisk. Afhængigt af MDM-løsningens udbyder og integrationen med dine interne systemer kan kontodata også udfyldes automatisk med brugerens navn, mailadresse og eventuelle certifikat-ID'er til godkendelse og signering.
- **Administrerede bøger og dokumenter.** MDM-værktøjer, bøger, ePub-bøger og PDF-dokumenter kan automatisk overføres til brugernes enheder, så medarbejderne altid har det materiale, de har brug for. Samtidig kan administrerede bøger kun deles med andre administrerede apps eller sendes via mail gennem administrerede konti. Når materialerne ikke længere er nødvendige, kan de fjernes eksternt. Bøger, der er købt gennem Apple Business Manager, kan distribueres gennem administreret bogdistribution, men de kan ikke tilbagekaldes eller tildeles til andre. En bog, der allerede er købt af brugeren, kan ikke administreres, medmindre brugeren får den tildelt direkte gennem Apple Business Manager.

### Administreret app-konfiguration

App-udviklere kan specificere app-indstillinger og -funktioner, som kan aktiveres, når appen installeres som en administreret app. Sørg for at installere disse konfigurationsindstillinger enten før eller efter, at den administrerede app bliver installeret. IT-afdelingen kan f.eks. oprette et sæt standardpræferencer for en SharePoint-app, så brugeren ikke behøver at konfigurere serverindstillingerne manuelt.

Førende udbydere af MDM-løsninger står bag AppConfig Community og tilbyder en skabelon, som alle app-udviklere kan bruge til understøttelse af administreret app-konfiguration. AppConfig Community fokuserer på at udarbejde værktøjer og best practice-løsninger i forbindelse med indbyggede funktioner i styresystemer til mobile enheder. Denne sammenslutning er med til at åbne døren for en mere ensartet, åben og enkel måde at konfigurere og sikre mobile apps på – med henblik på at få flere virksomheder til at indføre mobil teknologi.

Læs mere om AppConfig Community:

[www.appconfig.org](http://www.appconfig.org)



## Administrerede datastrømme

MDM-løsninger indeholder særlige funktioner, der gør det muligt at administrere virksomhedsdata på et detaljeret niveau, så de ikke finder vej til brugernes personlige apps eller tjenester i skyen.

- **Administreret åbning.** Administreret åbning anvender en række begrænsninger, der forhindrer, at vedhæftede bilag eller dokumenter fra administrerede kilder bliver åbnet på ikke-administrerede destinationer og omvendt. Du kan f.eks. forhindre, at et fortroligt bilag, der hører til en mail på jeres virksomheds administrerede mailkonto, bliver åbnet i nogen af brugernes personlige apps. Det er kun de apps, der er installeret og administreret via MDM, som kan åbne dette arbejdsdokument. Brugernes ikke-administrerede personlige apps vises ikke på listen over apps, der kan åbne det vedhæftede bilag. Ud over administrerede apps, konti, bøger og domæner findes der adskillige udvidelser, som overholder begrænsningerne for administreret åbning.
- **Enkel app-tilstand.** Denne indstilling begrænser iOS-enheder til en enkelt app. Den er ideel til standere eller enheder til bestemte formål, f.eks. ved kassen i en detailbutik eller til at tjekke ind på et hospital. Og udviklerne kan slå denne funktion til i deres apps for at sikre, at disse apps selvstændigt kan skifte til og fra Enkel app-tilstand.
- **Forhindring af sikkerhedskopiering.** Denne begrænsning forhindrer sikkerhedskopiering af administrerede apps til iCloud eller iTunes. Ved at deaktivere sikkerhedskopiering forhindrer man, at data fra administrerede apps kan gendannes, hvis appen fjernes via MDM, men senere bliver geninstalleret af brugeren.

# Muligheder for support

Apple tilbyder en række ordninger og muligheder for support for iOS-brugere og IT-administratorer.

## AppleCare for Enterprise

AppleCare for Enterprise er for virksomheder, der ønsker support med fuld dækning. AppleCare for Enterprise kan reducere belastningen af den interne helpdesk gennem teknisk support til medarbejderne over telefonen, 24 timer i døgnet og syv dage om ugen, og med en svartid på maks. en time ved meget presserende spørgsmål. Denne serviceordning giver support til hele IT-afdelingen for al Apple-hardware og -software samt support til komplekse scenarier med implementering og integration, bl.a. MDM og Active Directory.

## AppleCare OS Support

AppleCare OS Support yder telefon- og mailsupport på virksomhedsniveau til din IT-afdeling i forbindelse med implementering af iOS, macOS og macOS Server. Der tilbydes support i op til 24 timer i døgnet og en dedikeret teknisk account manager, alt efter hvilken form for support du vælger. Med AppleCare OS Support får din virksomhed direkte adgang til teknikere, som kan svare på spørgsmål om integration, migration og problemer med avanceret serverdrift. Og det kan øge dine IT-medarbejders effektivitet i forbindelse med implementering og administration af enheder og problemløsning.

## AppleCare Help Desk Support

AppleCare Help Desk Support giver prioriteret adgang til Apples erfarne medarbejdere hos teknisk support over telefonen. Denne service omfatter også en række værktøjer til at diagnosticere og udbedre fejl i Apple-hardware, som kan hjælpe virksomheder med at administrere deres ressourcer mere effektivt, forbedre svartider og reducere udgifter i forbindelse med oplæring af medarbejdere. AppleCare Help Desk Support dækker et ubegrænset antal supporthenvendelser i forbindelse med diagnosticering af hardware og software samt fejlfinding og isolering af problemer på iOS-enheder.

## AppleCare til brugere af iOS-enheder

Alle iOS-enheder leveres med et års begrænset garanti og 90 dages gratis teknisk telefonsupport fra købsdatoen. Du kan ringe til eksperterne hos Apples tekniske support lige så tit, du vil, for at få besvaret dine spørgsmål.

## iOS Direct Service-ordning

Som en fordel ved AppleCare Protection Plan betyder iOS Direct Service-ordningen, at din helpdesk har mulighed for at tjekke enheder for problemer uden at skulle ringe til AppleCare eller tage til en Apple Store. Hvis det er nødvendigt, kan din virksomhed bestille en ny iPhone, iPad, iPod touch eller ekstra tilbehør direkte.

Læs mere om AppleCare-ordningerne:

[www.apple.com/dk/support/professional](http://www.apple.com/dk/support/professional)

# Opsummering

Hvad enten din virksomhed implementerer iOS-enheder til en afgrænset gruppe brugere eller i hele virksomheden, er der mange muligheder for nem implementering og administration af enhederne. Hvis du vælger de rigtige strategier for din virksomhed, kan du hjælpe dine medarbejdere med at blive mere produktive og udføre deres arbejde på helt nye måder.

Læs mere om integration af iOS i virksomheders IT-miljøer:

[www.apple.com/dk/business/products-platform](http://www.apple.com/dk/business/products-platform)

<sup>1</sup>Nogle apps og bøger er muligvis ikke tilgængelige i visse lande og områder eller hos alle udviklere. [Se oversigten over, hvor ordninger og indhold er til rådighed.](#)

<sup>2</sup>Nogle funktioner kræver en Wi-Fi-forbindelse. Nogle funktioner er ikke tilgængelige i alle lande. Du finder de anbefalede systemkrav og minimumskrav til iCloud her: [support.apple.com/da-dk/HT204230](http://support.apple.com/da-dk/HT204230).

© 2018 Apple Inc. Alle rettigheder forbeholdes. Apple, Apple-logoet, AirDrop, AirPlay, AirPrint, Apple TV, Bonjour, FaceTime, iMessage, iPad, iPhone, iPod touch, iTunes, Mac, macOS og Siri er varemærker tilhørende Apple Inc. og registreret i USA og andre lande. tvOS er et varemærke tilhørende Apple Inc. App Store, AppleCare, Apple Store, Apple Books, iCloud, iCloud Drive, iCloud-nøglering og iTunes Store er servicemærker tilhørende Apple Inc. og registreret i USA og andre lande. iOS er et varemærke eller registreret varemærke tilhørende Cisco i USA og andre lande og bruges under licens. Andre nævnte produkt- og firmanavne kan være varemærker tilhørende deres respektive ejere. Produktspecifikationer kan ændres uden varsel. Ikke alle produkter og tjenester er tilgængelige i alle lande. Materialet har kun oplysende karakter, og Apple påtager sig intet ansvar mht. brugen heraf.