Oversigt over implementering af iOS og iPadOS

Indledning

Indhold

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. Brugerne har bedre adgang til information, så de føler sig bedre rustet og kan bruge deres kreativitet til at løse problemer.

Ved at understøtte iOS og iPadOS 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 (MDM) fra en tredjepartsleverandør gør det nemt for din virksomhed at implementere iOS-enheder, iPadOS-enheder og apps i større mængder.

- Administration af mobile enheder 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.
- Apple Business Manager gør det muligt at købe apps og bøger i større mængder og distribuere dem trådløst til brugerne.
- Med Apple Business Manager kan du også oprette administrerede Apple-id'er for medarbejdere ved hjælp af godkendelse fra organisationsnetværket med Microsoft Azure AD.

Dette dokument vejleder dig i at implementere iOS- og iPadOS-enheder i din virksomhed og hjælper dig med at udarbejde en implementeringsplan, der passer perfekt til jeres virksomhedsmiljø. Emnerne i dette dokument er beskrevet mere udførligt i online-vejledningen om implementering af iPhone og iPad: support.apple.com/guide/deployment-reference-ios

Ejerskabsmodeller

At vurdere ejerskabsmodeller og vælge den rigtige model for jeres 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 identificere, hvad der er bedst for jeres virksomhed.

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

- Virksomhedsejet
- Brugerejet

Selvom mange virksomheder har én model, de foretrækker, kan det være, at der anvendes forskellige modeller i jeres 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-og iPadOS-enheder for at gennemføre kundernes betalinger.

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

Virksomhedsejede enheder

Med en virksomhedsejet model kan du udstyre medarbejderne med enheder til hverdagsbrug, lade medarbejderne deles om enheder til ordinære opgaver eller konfigurere enheder til et specifikt formål ved at fastlåse dem i én bestemt app. Når en enhed tildeles til en enkelt bruger, kan den tilpasses personligt af slutbrugeren. Enheder, der er låst i en enkelt app eller deles blandt flere brugere, bliver normalt ikke tilpasset af slutbrugeren. Med en kombination af disse modeller, centrale 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 – denne funktion kaldes automatisk tilmelding af enheder. Når disse enheder er konfigureret, kan brugerne tilføje deres egne apps og data i tillæg til en hvilken som helst virksomhedskonto eller apps 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 fra centralt hold i stedet for at lade den enkelte bruger stå for indstillingen. Ved ikke-individualiseret implementering er det normalt ikke tilladt for brugerne at installere apps eller gemme private data på enheden. Automatisk tilmelding af enheder via Apple Business Manager kan også være med til at automatisere indstillingen af ikke-individualiserede enheder. Diagrammet nedenfor illustrerer de handlinger, der kræves af både administratoren og brugeren ved 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
Forberedelse	• Evaluering af infrastrukturen • Valg af en MDM-løsning • Tilmelding til Apple Business Manager	• Kræver ingen brugerhandling
Indstilling	• Konfiguration af enheder • Distribuering af apps og bøger	• Kræver ingen brugerhandling
Implementering	• Distribuering af enhederne **Kun med personlig tilpasning** • Giv brugerne mulighed for at tilpasse enhederne	**Kun med personlig tilpasning** • Download og installation af apps og bøger • Brug af Apple-id, App Store og iCloud-konti, hvis det er relevant **Kun ved ikke-individualiseret** • Kræver ingen brugerhandling
Administration	• Administration af enheder • Implementering og administration af yderligere indhold	**Kun med personlig tilpasning** • Find andre nyttige apps **Kun ved ikke-individualiseret** • Kræver ingen brugerhandling

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 gennem den nye funktion til brugertilmelding i iOS 13 og iPadOS.

En BYOD-løsning giver brugerne mulighed for at indstille og konfigurere deres egne enheder. Brugerne 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. Brugerne skal vælge at tilmelde sig virksomhedens MDM-løsning.

Brugertilmelding for personlige enheder betyder, at virksomhedens ressourcer og data kan administreres på sikre måder, samtidig med at brugerens private oplysninger, personlige data og apps respekteres. IT-afdelingen kan kun styre bestemte indstillinger, kontrollere, at virksomhedens politikker bliver overholdt og kun fjerne virksomhedsdata og -apps, og dette vil ikke berøre personlige data og apps på den enkelte brugers enhed.

Brugertilmelding omfatter følgende:

- **Administreret Apple-id.** Brugertilmelding er integreret med administreret Apple-id for at etablere en brugeridentitet på enheden og give adgang til Apple-tjenester. Det administrerede Apple-id kan bruges sammen med et personligt Apple-id, som brugeren allerede har logget ind med. Administrerede Apple-id'er oprettes i Apple Business Manager og leveres via godkendelse fra organisationsnetværket til Microsoft Azure Active Directory.
- **Adskillelse af data.** Brugertilmelding skaber et adskilt APFS-drev til administrerede konti, apps og data på enheden. Dette administrerede drev adskilles kryptografisk fra resten af enheden.
- **Udvalgt administration for BYOD.** Brugertilmelding er udviklet specielt til brugerejede enheder, så IT-afdelingen kan administrere et udvalg af konfigurationer og retningslinjer og samtidig sætte begrænsninger for visse administrative opgaver, f.eks. fjernsletning af alt på en enhed eller indsamling af personoplysninger.

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

	Administrator	Bruger
Forberedelse	• Evaluering af infrastrukturen • Valg af en MDM-løsning • Tilmelding til Apple Business Manager	• Brug af personligt Apple-id og administreret Apple-id, App Store og iCloud-konti, hvis det er relevant
Indstilling	• Konfiguration af enhedsindstillinger • Distribuering af apps og bøger	• Tilmelding til virksomhedens MDM-løsning • Download og installation af apps og bøger
Implementering	• Kræver ingen administratorhandling	• Kræver ingen brugerhandling
Administration	• Administration af enheder • Implementering og administration af yderligere indhold	• Find andre nyttige apps

Læs mere om brugertilmelding i MDM:
support.apple.com/guide/mdm

Læs mere om godkendelse fra organisationsnetværket:
support.apple.com/guide/apple-business-manager

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 enhederne. 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 jeres 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 og iPadOS har at byde på.

Wi-Fi og netværk

Velfungerende og pålidelig adgang til et trådløst netværk er afgørende for indstillingen og konfigurationen af iOS- og iPadOS-enheder. Undersøg, om din virksomheds Wi-Fi-netværk understøtter flere enheder ad gangen med samtidige forbindelser fra alle jeres brugere. Du skal muligvis konfigurere dine webproxy- eller firewall-porte, hvis enhederne ikke kan få adgang til Apples aktiveringsservere, iCloud eller App 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 jeres VPN-infrastruktur for at sikre, at brugerne kan få sikker ekstern adgang til virksomhedens ressourcer via deres iOS- og iPadOS-enheder. Overvej at bruge funktioner som VPN On Demand eller Pr.-app-VPN i iOS og iPadOS, så der kun oprettes en VPN-forbindelse, når det er nødvendigt. Hvis du har planer om at anvende Pr.-app-VPN, skal du sikre dig, at jeres VPN-gateways understøtter disse funktioner, og at I køber tilstrækkeligt mange licenser til antallet af brugere og forbindelser.

Du skal også sørge for, at jeres 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- og iPadOS-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.

Læs mere om Wi-Fi og netværk:
support.apple.com/guide/deployment-reference-ios

Læs mere om Bonjour:
developer.apple.com/library

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 I har licenser nok til at understøtte det forventede antal iOS- og iPadOS-enheder, som vil blive tilsluttet. iOS og iPadOS understøtter også moderne Office 365-godkendelse og gør brug af OAuth 2.0 og multifaktorgodkendelse. Hvis I ikke bruger Exchange, fungerer iOS og iPadOS 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 og Apple Books.

Denne funktion kan også lagre softwareopdateringer, så du opnår hurtigere overførsel til iOS- og iPadOS-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- og iPadOS-enheder tilsluttet via USB.

Læs mere om indlæsning af indhold i buffer:
support.apple.com/guide/deployment-reference-macos

Læs mere om tethered caching:
support.apple.com/HT207523

Valg af en MDM-løsning

Med Apples administrationsplatform for iOS og iPadOS 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 jeres 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:
apple.com/dk/business/docs/resources/Administration af enheder og virksomhedsdata i iOS.pdf

Tilmelding til Apple Business Manager

Apple Business Manager er en webbaseret portal, hvor IT-afdelinger kan implementere iPhone, iPad, iPod touch, Apple TV og Mac fra ét centralt sted. Apple Business Manager, der fungerer problemfrit med jeres løsning til administration af mobile enheder (MDM), gør det nemt at automatisere implementering af enheder, købe apps/programmer og distribuere indhold samt oprette administrerede Apple-id'er for medarbejdere.

Apples tilmeldingsordning for enheder (DEP) og mængdekøbsordningen (VPP) er nu helt integreret i Apple Business Manager, så organisationer kan samle alt det, de skal bruge til at implementere Apple-enheder. Disse ordninger vil ikke længere være tilgængelige fra og med den 1. december 2019.

Enheder

Apple Business Manager giver mulighed for automatisk tilmelding af enheder, hvor virksomheder får en hurtig og effektiv metode til at implementere virksomhedsejede Apple-enheder og tilmelde dem i MDM, uden at man behøver at få hver enhed i hånden eller klargøre den.

- Gør opsætningsprocessen for brugere mere enkel ved at effektivisere trin i indstillingsassistenten, så medarbejderne er sikre på at modtage de rette konfigurationer, så snart enhederne aktiveres. IT-afdelinger kan nu tilpasse denne oplevelse yderligere ved at levere tekst om samtykke, virksomhedsbranding eller moderne godkendelse til medarbejderne.
- Giv mulighed for kontrol af virksomhedsejede enheder på et højere niveau ved hjælp af overvågning, som giver yderligere kontrolfunktioner til administration af enheder, der ikke er tilgængelige for andre implementeringsmodeller, herunder 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 I nu tilmelde iPhone, iPad og Apple TV manuelt ved hjælp af Apple Configurator 2, uanset hvordan I har anskaffet dem.

Indhold

Apple Business Manager gør det nemt for virksomheder at købe indhold i store mængder. Hvad enten jeres medarbejderstab bruger iPhone, iPad eller Mac, kan I levere fantastisk indhold, som er klar til brug i arbejdsopgaverne med fleksible og sikre distributionsmuligheder.

- Køb apps, programmer, bøger og tilpassede apps og programmer i større mængder, herunder apps og programmer, I udvikler internt. Det er nemt at overføre app- og programlicenser 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 med MDM.
- Overfør apps, programmer og bøger direkte til administrerede enheder eller autoriserede brugere, og hold nemt styr på, hvilket indhold der er tildelt til hvilken bruger eller enhed. Med administreret distribution kan I styre hele distributionsprocessen, så jeres virksomhed fortsat har fuldt ejerskab og kontrol over de apps og programmer, den har købt. Apps og programmer, der

ikke er nødvendige for en enhed eller bruger, kan inddrages og tildeles til andre inden for organisationen.

- Betal med forskellige betalingsmetoder, herunder betalingskort og købsordrer. Virksomheder kan købe mængdekøbskredit (hvor det er tilgængeligt) fra Apple eller fra en autoriseret Apple-forhandler som specifikke beløb i den lokale valuta, der sendes elektronisk til kontohaveren som VPP-kredit.
- Et program eller en app kan tildeles til enheder eller brugere i alle lande, hvor programmet/appen er tilgængelig, så de kan distribueres multinationalt inden for virksomheden. Udviklere kan gøre deres apps og programmer tilgængelige i flere lande gennem App Store-standardprocessen for udgivelse.

Bemærk: Køb af bøger i Apple Business Manager er ikke tilgængelig i visse lande eller regioner. Du kan læse mere om tilgængelige funktioner og indkøbsmetoder på support.apple.com/HT207305.

Personer

Apple Business Manager giver virksomheder mulighed for at oprette og administrere konti for medarbejdere, som kan integreres med eksisterende infrastruktur og give adgang til Apples apps og tjenester samt Apple Business Manager.

- Opret administrerede Apple-id'er for medarbejdere, så de kan samarbejde med Apples apps og tjenester samt få adgang til arbejdsdata i administrerede apps, der bruger iCloud Drive. Disse konti ejes og styres af den enkelte virksomhed.
- Udnyt godkendelse fra organisationsnetværket ved at forbinde Apple Business Manager med Microsoft Azure Active Directory. Administrerede Apple-id'er vil blive oprettet automatisk, når den enkelte medarbejder logger ind for første gang med sine eksisterende brugeroplysninger på en kompatibel Apple-enhed.
- Brug administrerede Apple-id'er på en enhed, der ejes af en medarbejder, sammen med et personligt Apple-id ved hjælp af de nye funktioner til brugertilmelding i iOS 13, iPadOS og macOS Catalina. Som alternativ kan administrerede Apple-id'er bruges på en hvilken som helst enhed som det primære (og eneste) Apple-id. Administrerede Apple-id'er kan også give adgang til iCloud på internettet, efter at der er logget ind på en Apple-enhed for første gang.
- Tildel andre roller til IT-afdelinger i jeres virksomhed for at administrere enheder, apps og konti på effektive måder i Apple Business Manager. Brug rollen som Administrator til at acceptere vilkår og betingelser, hvis det er nødvendigt, og til nemt at videregive ansvar, hvis en medarbejder forlader organisationen.

Bemærk: iCloud Drive understøttes p.t. ikke med brugertilmelding. iCloud Drive kan bruges med et administreret Apple-id, når det er enhedens eneste Apple-id.

Læs mere om Apple Business Manager: www.apple.com/dk/business/it

Tilmelding til Apple Developer Enterprise Program

Apple Developer Enterprise Program tilbyder et komplet sæt værktøjer til udvikling, test og distribuering af apps/ programmer til brugerne. I kan distribuere apps og programmer ved enten at hoste dem på en webserver eller

via en MDM-løsning. Programmer til Mac og installationsprogrammer kan signeres og bekræftes med jeres udvikler-id til Gatekeeper, som er med til at beskytte macOS mod malware.

Læs mere om Developer Enterprise Program:
developer.apple.com/programs/enterprise

2. Indstilling

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

Indstil jeres 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 jeres enheder er tilmeldt en MDM-server på sikker vis, aktiveres administrationen ved hjælp af konfigurationsbeskrivelser – dvs. en XML-fil med konfigurationsoplysninger for en iOS- eller iPadOS-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- og iPadOS-enheder, der føjes til Apple Business Manager, er altid overvåget, og MDM-tilmelding er obligatorisk.
- **Brugerejede enheder.** Medarbejderne kan selv bestemme, om de vil tilmelde deres enheder 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.

Når en enhed er tilmeldt, kan en administrator aktivere en MDM-regel, -indstilling eller -kommando. De administrative handlinger, der kan vælges for en enhed, vil variere afhængigt af overvågnings- og tilmeldingsmetoden. Derefter modtager iOS- eller iPadOS-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 oplysninger eller proprietære data via APNs.

Konfiguration af enheder med Apple Configurator 2 (valgfrit)
Til den indledende lokale implementering af flere enheder kan virksomheder bruge Apple Configurator 2. Med dette gratis macOS-program kan du koble iOS- og iPadOS-enheder til en Mac-computer via USB og opdatere dem til den nyeste version af iOS og iPadOS, 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. Der kan laves brugerdefinerede processer i Apple Configurator 2 ved hjælp af Blueprints, så separate opgaver kan kombineres.

Læs mere om Apple Configurator 2:
support.apple.com/da-dk/apple-configurator

Overvågede enheder
Overvågning giver adgang til yderligere administrationsfunktioner for iOS- og iPadOS-enheder, der ejes af virksomheden, så du kan bruge forskellige begrænsninger såsom at deaktivere AirDrop eller indstille enheden til enkel app-funktion. Det giver også mulighed for at aktivere et webfilter gennem en global proxy, f.eks. for at sikre, at brugernes internettrafik holder sig inden for virksomhedens retningslinjer, forhindre brugerne i at gendanne enhedens fabriksindstillinger og meget mere. Som standard er alle iOS- og iPadOS-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 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.

Læs mere om begrænsninger for overvågede enheder:
support.apple.com/guide/mdm

Distribuering af apps og bøger

Apple tilbyder omfattende ordninger for at hjælpe din virksomhed med at udnytte de fantastiske apps og ressourcer, der fås til iOS og iPadOS. 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 appen er tilgængelig. 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 funktion 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 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, f.eks. i forbindelse med en franchising-forretning. 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 koderne 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 hele indstillingen af jeres enheder 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 for apps, som understøtter fildeling. For at gennemgå eller hente dokumenter fra iOS- og iPadOS-enheder skal du forbinde dem med en Mac med Apple Configurator 2.

3. Implementering

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

Distribuer jeres 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
Brugere kan aktivere deres enheder, konfigurere grundlæggende indstillinger og begynde at arbejde med det samme ved hjælp af indstillingsassistenten. 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.

Apple-id og administreret Apple-id
Når medarbejdere bruger et Apple-id til at logge ind på Apple-tjenester som FaceTime, iMessage, App Store og iCloud, har de adgang til et stort udvalg af indhold, der kan effektivisere arbejdsopgaver, øge produktiviteten og bruges til samarbejde.

På samme måde som andre Apple-id'er bruges administrerede Apple-id'er til at logge ind på en personlig enhed. De bruges også til at få adgang til Apple-tjenester – herunder iCloud og samarbejde med iWork og Noter – og Apple Business Manager. Til forskel fra almindelige Apple-id'er ejes og styres administrerede Apple-id'er af din organisation. Dette gælder bl.a. nulstilling af adgangskoder og rollebaseret administration. Administrerede Apple-id'er har visse begrænsede indstillinger.

Enheder, der tilmeldes via brugertilmelding, kræver et administreret Apple-id. Ved brugertilmelding kan dette bruges parallelt med et personligt Apple-id. Andre tilmeldingsmuligheder understøtter enten brug af et personligt Apple-id eller et administreret Apple-id. Det er altså kun brugertilmelding, der understøtter flere Apple-id'er.

For at få mest muligt ud af disse tjenester bør brugere anvende deres egne Apple-id'er eller administrerede Apple-id'er, der oprettes for dem. 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 har et. Brugerne behøver ikke at have et betalingskort for at oprette et Apple-id.

Læs mere om administrerede Apple-id'er:
support.apple.com/guide/apple-business-manager

iCloud

Med iCloud kan brugerne automatisk synkronisere dokumenter og personligt indhold – f.eks. kontakter, kalendere, dokumenter og billeder – og holde dem opdateret på flere enheder. Find min-funktionen gør brugerne i stand til at lokalisere en mistet eller stjålet Mac, iPhone, iPad eller iPod touch. Specifikke elementer i iCloud – f.eks. iCloud-nøglering og iCloud Drive – kan slås fra ved hjælp af begrænsninger, der angives manuelt på enheden eller indstilles via MDM. Dette giver organisationer større kontrol over, hvilke data der lagres på hvilken konto.

Læs mere om administration af iCloud:
support.apple.com/guide/deployment-reference-ios

4. Administration

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

Administrer jeres 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- eller iPadOS-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, f.eks. for at 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 softwareopdatering 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 også anmode en iPhone eller iPad 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- eller iPadOS-opdatering. Du kan dog ændre standardværdien for det antal dage, du ønsker at forhindre opdateringer, fra 1 dag til 90 dage. Du kan også planlægge softwareopdateringer på overvågede enheder via jeres MDM-løsning.

Funktionen Mistet

Med jeres MDM-løsning kan du 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 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 har interne app-portaler som en del af deres løsning. Ellers kan du oprette en intern app-portal til jeres medarbejdere, hvor de nemt kan finde apps til deres iPhone eller iPad. Fra denne portal kan der linkes til interne apps, URL-adresser til apps fra App Store, Apple Business Manager-koder eller specialudviklede apps, 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 og iPadOS kan en virksomhed bruge administrerede apps, som gør det muligt at distribuere gratis, betalte og interne apps helt trådløst med MDM, mens man både beskytter virksomhedens data og respekterer brugernes privatliv. Administrerede apps kan fjernes eksternt af MDM-serveren, eller når en bruger fjerner sin 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 indløste 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 leverandør og integrationen med jeres 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 pr. mail via administrerede konti. Når der ikke længere er behov for materialerne, kan de fjernes eksternt. Bøger, der er købt gennem Apple Business Manager, kan distribueres gennem administreret bogdistribution, men de kan ikke inddrages 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 konfiguration af apps

App-udviklere kan specificere indstillinger og funktioner for den enkelte app, som kan aktiveres, når den 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 et standardskema, som alle appudviklere kan bruge for at understøtte konfiguration af administrerede apps. 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

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 cloud-tjenester.

- **Administreret åbning.** Funktionen til 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-funktion.** Denne indstilling begrænser iOS- eller iPadOS-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 af sig selv kan skifte til og fra Enkel app-funktion.
- **Forhindring af sikkerhedskopiering.** Denne begrænsning forhindrer administrerede apps i at sikkerhedskopiere data til iCloud eller en computer. 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- og iPadOS-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 for meget presserende spørgsmål. Denne serviceordning giver support til 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 til jeres IT-afdeling for hændelser i hele virksomheden ved implementering af iOS og iPadOS, 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 virksomheden direkte adgang til teknikere, som kan svare på spørgsmål om problemer med integration, migrering og avanceret serverdrift. Og det kan øge jeres IT-medarbejderes effektivitet i forbindelse med implementering og administration af enheder og problemløsning.

AppleCare Help Desk Support

AppleCare Help Desk Support giver prioriteret adgang til Apples mest erfarne tekniske supportmedarbejdere via 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 svartiden og reducere omkostningerne til uddannelse. AppleCare Help Desk Support dækker et ubegrænset antal supportkrævende hændelser for hardware- og softwarediagnostik samt fejlfinding og fejlisolering på iOS- og iPadOS-enheder.

AppleCare til brugere af iOS- og iPadOS-enheder

Alle iOS- og iPadOS-enheder leveres med et års begrænset garanti og 90 dages gratis teknisk telefonsupport fra købsdatoen. Dækningen kan udvides til to år fra den originale købsdato med AppleCare+ til iPhone, AppleCare+ til iPad eller AppleCare+ til iPod touch. Du kan ringe til eksperterne hos Apples tekniske support lige så tit, du vil, for at få besvaret dine spørgsmål. Apple har også praktiske servicemuligheder, når enheder skal repareres. Derudover dækker ordningerne op til to hændelige skader mod betaling af servicegebyr.

iOS Direct Service-ordning

Som en af fordelene ved AppleCare+ betyder iOS Direct Service-ordningen, at jeres helpdesk har mulighed for at tjekke enheder for problemer uden at skulle ringe til AppleCare eller besøge 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:
apple.com/dk/support/professional

Opsummering

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

Læs mere om iOS og iPadOS angående implementering, administration og sikkerhedsfunktioner:
support.apple.com/guide/deployment-reference-ios

Læs mere om indstillinger for administration af mobile enheder til IT-afdelingen:
support.apple.com/guide/mdm

Læs mere om Apple Business Manager:
support.apple.com/guide/apple-business-manager

Læs mere om administrerede Apple-id'er til erhvervslivet:
apple.com/business/docs/site/Overview_of_Managed_Apple_IDs_for_Business.pdf

Læs mere om Apple at Work:
www.apple.com/dk/business/

Læs mere om IT-funktioner:
www.apple.com/dk/business/it/

Læs mere om sikkerheden på Apples platforme:
www.apple.com/security/

Se de forskellige AppleCare-ordninger:
www.apple.com/dk/support/professional/

Bliv klogere på Apple Training and Certification:
training.apple.com

Kontakt Apple Professional Services:
consultingservices@apple.com