iOS- en iPadOS-implementatieoverzicht

Inleiding

Inhoud

iPhone en iPad kunnen uw bedrijf en de manier waarop uw medewerkers hun werk doen naar een hoger plan tillen. Ze kunnen zorgen voor een aanzienlijke productiviteitsverhoging en bieden uw medewerkers de vrijheid en flexibiliteit om op nieuwe manieren te werken – op kantoor of onderweg. De hele organisatie heeft er baat bij als deze moderne manier van werken wordt geïntegreerd. Gebruikers hebben betere toegang tot informatie, voelen zich zelfstandiger en kunnen problemen op een creatieve manier oplossen.

IT-afdelingen die iOS en iPadOS ondersteunen, worden beschouwd als afdelingen die de bedrijfsstrategie vormgeven en echte problemen oplossen, niet als afdelingen die zich alleen richten op reparaties en kostenbesparingen. Uiteindelijk heeft iedereen er baat bij. Het personeel is gemotiveerd en overal ontstaan er nieuwe zakelijke mogelijkheden.

Het is nog nooit zo eenvoudig geweest om iPhone en iPad in uw hele bedrijf te configureren en te implementeren. Dankzij Apple Business Manager in combinatie met een MDM-oplossing (Mobile Device Management) van een andere fabrikant vormt de grootschalige implementatie van iOS- en iPadOS-devices en -apps geen enkel probleem.

- Met Mobile Device Management kunt u uw devices configureren en beheren, en draadloos apps distribueren en beheren.
- Via Apple Business Manager kunt u de implementatie stroomlijnen door de aanmelding van Apple devices bij uw MDM-oplossing te automatiseren, zodat er geen aparte configuratie door het IT-team meer nodig is.
- Met Apple Business Manager kunt u apps en boeken in bulk aankopen en die draadloos onder gebruikers distribueren.
- Met Apple Business Manager kunt u ook beheerde Apple ID's voor medewerkers aanmaken met behulp van gebundelde authenticatie en Microsoft Azure AD.

Dit document bevat richtlijnen voor de implementatie van iOS- en iPadOS-devices binnen uw organisatie en suggesties voor het opstellen van een implementatieplan dat optimaal aansluit bij uw omgeving. Deze onderwerpen worden in meer detail beschreven in de Implementatiehandleiding voor iPhone en iPad: support.apple.com/guide/deployment-reference-ios

Eigendomsmodellen

Het evalueren van eigendomsmodellen en het kiezen van een geschikt model voor uw organisatie is een belangrijke eerste stap in de implementatie. U kunt de implementatie op verschillende manieren aanpakken, afhankelijk van wie de eigenaar is van het device. Allereerst moet u bepalen wat het beste is voor uw organisatie.

In het bedrijfsleven zien we twee veelgebruikte eigendomsmodellen voor iOS- en iPadOS-devices:

- Eigendom van organisatie
- Eigendom van gebruiker

De meeste organisaties hebben een voorkeur voor een specifiek model, maar mogelijk komt u in uw eigen omgeving meerdere modellen tegen. Het hoofdkantoor van een winkelbedrijf kan bijvoorbeeld een strategie met devices in eigendom van gebruikers hanteren door medewerkers toestemming te geven een eigen iPad te configureren, waarbij de bedrijfsvoorzieningen beveiligd en beheerd worden zonder dat dit invloed heeft op de persoonsgegevens en apps van de gebruiker. In de winkels van het bedrijf kan echter zijn gekozen voor een strategie met devices in eigendom van de organisatie, zodat de winkelmedewerkers op de aanwezige iOS- en iPadOS-devices klanttransacties kunnen verwerken.

Door deze modellen te bestuderen kunt u gemakkelijker bepalen welk model het meest geschikt is voor uw eigen omgeving. Nadat u het juiste implementatiemodel voor uw organisatie hebt gekozen, kan uw team de implementatie- en beheermogelijkheden van Apple tot in detail bekijken.

Devices in eigendom van de organisatie

Als devices eigendom van het bedrijf blijven, kunt u een device aan één medewerker toewijzen voor dagelijks gebruik, devices gezamenlijk door verschillende medewerkers met dezelfde taken laten gebruiken, of devices speciaal voor één doel of app configureren. Een device dat aan één gebruiker is toegewezen, kan door die gebruiker worden gepersonaliseerd. Devices die zijn beperkt tot één app of door medewerkers worden gedeeld, worden meestal niet door de gebruiker gepersonaliseerd. Wanneer u kiest voor een combinatie van deze modellen, de speciale technologie van Apple en een MDM-oplossing, kunt u de devices volledig automatisch instellen en configureren.

Gepersonaliseerd. Wanneer u een gepersonaliseerde implementatie gebruikt, kunt u elke gebruiker zijn eigen device laten kiezen en zijn device laten aanmelden bij een MDM-oplossing die de bedrijfsinstellingen en zakelijke apps draadloos aanlevert. Als devices rechtstreeks bij Apple of bij deelnemende door Apple erkende resellers of providers zijn gekocht, kunt u ook gebruikmaken van Apple Business Manager om automatisch nieuwe devices bij uw MDM-oplossing aan te melden. Zodra de devices zijn geconfigureerd, kunnen de gebruikers er hun eigen apps en gegevens op zetten, naast een eventuele bedrijfsaccount of apps van uw organisatie.

Niet-gepersonaliseerd. Als devices door verschillende mensen worden gedeeld of uitsluitend voor één doeleinde worden ingezet (zoals in een hotel of restaurant), worden ze doorgaans centraal geconfigureerd en beheerd door een IT-medewerker, niet door een individuele gebruiker. Op zulke devices mogen gebruikers meestal geen apps installeren of eigen gegevens bewaren. Ook kan automatische device-aanmelding met Apple Business Manager handig uitkomen voor het configureren van niet-gepersonaliseerde devices. In het onderstaande overzicht ziet u welke handelingen de beheerder en gebruiker moeten uitvoeren bij elke stap van een implementatie waarbij de organisatie eigenaar is van de devices. De stappen gelden voor zowel een *gepersonaliseerde* als een *niet-gepersonaliseerde* implementatie, tenzij anders aangegeven.

	Beheerder	Gebruiker
Voorbereiden	• Uw infrastructuur evalueren • MDM-oplossing kiezen • Aanmelden bij Apple Business Manager	• Geen actie door gebruiker vereist
Configureren	• Devices configureren • Apps en boeken distribueren	• Geen actie door gebruiker vereist
Implementeren	• Devices distribueren **Alleen bij gepersonaliseerde implementatie** • Personaliseren toestaan	**Alleen bij gepersonaliseerde implementatie** • Apps en boeken downloaden en installeren • Apple ID, App Store- en iCloud-accounts gebruiken indien van toepassing **Alleen bij niet-gepersonaliseerde implementatie** • Geen actie door gebruiker vereist
Beheren	• Devices beheren • Extra content distribueren en beheren	**Alleen bij gepersonaliseerde implementatie** • Aanvullende apps zoeken **Alleen bij niet-gepersonaliseerde implementatie** • Geen actie door gebruiker vereist

Devices in eigendom van gebruikers

Als de devices door de gebruikers zelf worden aangeschaft en geconfigureerd (dit wordt vaak een BYOD-implementatie (Bring-Your-Own-Device) genoemd), kunt u de gebruikers via MDM en de nieuwe feature voor gebruikersinschrijving in iOS 13 en iPadOS toegang bieden tot bedrijfsvoorzieningen zoals wifi, e-mail en agenda's.

Bij een BYOD-implementatie kunnen gebruikers hun eigen device instellen en configureren. Ze kunnen hun device aanmelden bij de MDM-oplossing van uw organisatie om toegang te krijgen tot bedrijfsvoorzieningen, bepaalde instellingen te configureren of een configuratieprofiel of bedrijfsapps te installeren. Gebruikers moeten zich daarvoor actief aanmelden bij de MDM-oplossing van uw organisatie.

Met gebruikersinschrijving voor persoonlijke devices kunnen bedrijfsvoorzieningen worden beheerd op een veilige manier die de privacy en persoonlijke gegevens van de gebruiker respecteert. De IT-afdeling kan specifieke instellingen afdwingen, de naleving van het bedrijfsbeleid controleren, en alleen bedrijfsgegevens en -apps verwijderen terwijl de persoonsgegevens en apps op de afzonderlijke devices ongemoeid blijven.

Gebruikersinschrijving omvat het volgende:

- **Beheerde Apple ID.** Gebruikersinschrijving wordt gecombineerd met het gebruik van beheerde Apple ID's om de identiteit van de gebruiker vast te stellen op het device en toegang te bieden tot Apple diensten. De beheerde Apple ID kan naast de persoonlijke Apple ID worden gebruikt. Beheerde Apple ID's worden in Apple Business Manager gemaakt en ingericht via gebundelde authenticatie met Microsoft Azure Active Directory.
- **Gegevensscheiding.** Bij de inschakeling van gebruikersinschrijving wordt op het device een apart APFS-volume aangemaakt voor beheerde accounts, apps en gegevens. Dit beheerde volume is cryptografisch gescheiden van de overige gegevens op het device.
- **Uitgekiend beheer voor BYOD.** Gebruikersinschrijving is ontworpen voor devices die eigendom zijn van de gebruiker, zodat de IT-afdeling bepaalde configuratieopties en beleidsrichtlijnen kan beheren, maar andere beheertaken niet kan uitvoeren, zoals het volledige device op afstand wissen of persoonlijke gegevens verzamelen.

In het onderstaande overzicht ziet u welke handelingen de beheerder en gebruiker moeten uitvoeren bij elke stap van een BYOD-implementatie.

	Beheerder	Gebruiker
Voorbereiden	• Uw infrastructuur evalueren • MDM-oplossing kiezen • Aanmelden bij Apple Business Manager	• Apple ID, beheerde Apple ID, App Store- en iCloud-accounts gebruiken indien van toepassing
Configureren	• Device-instellingen configureren • Apps en boeken distribueren	• Aanmelden bij MDM-voorziening van het bedrijf • Apps en boeken downloaden en installeren
Implementeren	• Geen actie door beheerder vereist	• Geen actie door gebruiker vereist
Beheren	• Devices beheren • Extra content distribueren en beheren	• Aanvullende apps zoeken

Lees meer over gebruikersinschrijving in MDM:
support.apple.com/nl-nl/guide/mdm

Lees meer over gebundelde authenticatie:
support.apple.com/guide/apple-business-manager

Implementatiestappen

In dit gedeelte vindt u uitgebreide informatie over de vier stappen om devices en content te implementeren: het voorbereiden van de omgeving en het configureren, implementeren en beheren van de devices. Welke stappen u moet uitvoeren, is afhankelijk van de vraag of de devices eigendom zijn van de organisatie of van de gebruikers.

1. Voorbereiden

Nadat u het juiste implementatiemodel voor uw organisatie hebt gekozen, voert u de volgende stappen uit om de implementatie voor te bereiden. Dit kunt u al doen voordat de devices aanwezig zijn.

Uw infrastructuur evalueren

In de meeste standaard IT-bedrijfsomgevingen kunnen iPhone en iPad probleemloos worden geïntegreerd. Het is belangrijk om een goed beeld te krijgen van uw bestaande infrastructuur, zodat er maximaal kan worden geprofiteerd van de mogelijkheden van iOS en iPadOS.

Wifi en netwerk

Stabiele, betrouwbare toegang tot een draadloos netwerk is essentieel voor het instellen en configureren van iOS- en iPadOS-devices. Controleer of het wifinetwerk van uw bedrijf ondersteuning biedt voor meerdere devices met gelijktijdige verbinding van alle gebruikers. Mogelijk moet u de webproxy of firewall-poorten configureren als devices geen toegang hebben tot de activeringsservers van Apple, iCloud of de App Store. Daarnaast hebben Apple en Cisco de communicatie van iPhone en iPad met draadloze Cisco-netwerken geoptimaliseerd. Hierdoor zijn ook andere geavanceerde netwerkfeatures mogelijk, zoals snelle roaming en Quality of Service-optimalisatie (QoS) voor apps.

Neem de VPN-infrastructuur onder de loep, zodat u zeker weet dat gebruikers via hun iOS- of iPadOS-device ook op afstand veilig toegang hebben tot de informatie en voorzieningen van uw instelling. Gebruik eventueel de feature voor VPN on Demand of app-gebonden VPN in iOS en iPadOS, zodat er alleen een VPN-verbinding wordt opgezet als dat echt noodzakelijk is. Als u van plan bent gebruik te maken van app-gebonden VPN, moet u zorgen dat de VPN-gateways deze mogelijkheden ondersteunen, en dat u voldoende licenties aanschaft voor het betreffende aantal gebruikers en verbindingen.

Verder moet u controleren of uw netwerkinfrastructuur zodanig is ingesteld dat Bonjour wordt ondersteund (het op standaarden gebaseerde netwerkprotocol van Apple waarbij geen configuratie nodig is). Dankzij Bonjour kunnen devices automatisch voorzieningen op een netwerk opsporen. iOS- en iPadOS-devices maken via Bonjour verbinding met AirPrint-printers en AirPlay-devices zoals Apple TV. Sommige apps gebruiken Bonjour ook om andere devices op te sporen om daarmee samen te werken en gegevens uit te wisselen.

Lees meer over wifi en netwerk: support.apple.com/guide/deployment-reference-ios/

Lees meer over Bonjour: developer.apple.com/library

Mail, contacten en agenda's

Als u gebruikmaakt van Microsoft Exchange, controleer dan of de ActiveSync-voorziening up-to-date is en of de configuratie geschikt is voor ondersteuning van alle gebruikers in het netwerk. Als u gebruikmaakt van Office 365 in de cloud, zorg dan dat u over voldoende licenties beschikt voor het verwachte aantal iOS- en iPadOS-devices dat verbinding maakt. iOS en iPadOS ondersteunen ook moderne Office 365-verificatie op basis van OAuth 2.0 en meerstapsverificatie. Mocht u geen Exchange gebruiken: iOS en iPadOS zijn compatibel met op standaarden gebaseerde servers zoals IMAP, POP, SMTP, CalDAV, CardDAV en LDAP.

Materiaalcaching

Materiaalcaching is een feature van macOS High Sierra of hoger waarmee lokaal een kopie wordt bewaard van materiaal dat vaak van Apple servers wordt opgevraagd. Hierdoor is er minder bandbreedte nodig om materiaal naar uw netwerk te downloaden. Materiaalcaching versnelt het downloaden en distribueren van software via de App Store, de Mac App Store en Apple Books.

Daarnaast kunnen software-updates in een cache worden geplaatst, zodat deze sneller op iOS- en iPadOS-devices kunnen worden gedownload. Materiaalcaching omvat tethered caching. Dit houdt in dat een Mac zijn internetverbinding kan delen met verschillende iOS- en/of iPadOS-devices die via USB zijn aangesloten.

Lees meer over materiaalcaching:
support.apple.com/guide/deployment-reference-macos

Lees meer over tethered caching:
support.apple.com/HT207523

MDM-oplossing kiezen

Het Apple beheerframework voor iOS en iPadOS biedt organisaties de mogelijkheid devices veilig aan te melden bij de bedrijfsomgeving, instellingen draadloos te configureren en bij te werken, te controleren of aan het beleid wordt voldaan, apps en boeken te implementeren en op afstand gegevens van beheerde devices te wissen of de toegang ertoe met een code te beveiligen. Deze beheerfeatures worden door MDM-oplossingen van andere fabrikanten mogelijk gemaakt.

Er zijn diverse MDM-oplossingen van andere fabrikanten beschikbaar voor verschillende serverplatforms. De beheerconsoles, features en prijsstelling verschillen per oplossing. Neem voordat u een oplossing kiest eerst onderstaande informatie door om te beoordelen welke beheerfeatures voor uw organisatie een rol kunnen spelen. Naast oplossingen van andere fabrikanten is er ook een MDM-oplossing van Apple met de naam Profielbeheer. Dit is een feature van macOS Server.

Lees meer over het beheren van devices en bedrijfsgegevens:
apple.com/nl/business/docs/resources/Managing_Devices_and_Corporate_Data_on_iOS.pdf

Aanmelden bij Apple Business Manager

Apple Business Manager is een webportal waarmee IT-beheerders iPhone, iPad, iPod touch, Apple TV en Mac vanuit één locatie kunnen implementeren. Apple Business Manager werkt naadloos samen met uw MDM-oplossing (Mobile Device Management). Met Apple Business Manager kunt u moeiteloos de implementatie van devices automatiseren, apps kopen en content distribueren, en beheerde Apple ID's voor medewerkers aanmaken.

Het Device Enrollment Program (DEP) en het Volume Purchase Program (VPP) zijn nu volledig geïntegreerd in Apple Business Manager, zodat organisaties alles wat ze nodig hebben voor de implementatie van Apple devices centraal kunnen regelen. Deze programma's zijn vanaf 1 december 2019 niet meer beschikbaar.

Devices

Met Apple Business Manager kunnen organisaties de aanmelding van devices automatiseren. Hiermee beschikken ze over een snelle en gestroomlijnde manier om Apple devices in eigendom van het bedrijf te implementeren en bij MDM aan te melden, zonder elk device afzonderlijk te hoeven voorbereiden.

- Het configuratieproces voor gebruikers kan worden vereenvoudigd door de stappen in de configuratie-assistent te stroomlijnen, zodat medewerkers direct na de activering de juiste configuratie ontvangen. Bovendien kan de IT-afdeling deze procedure nu nog verder op de medewerkers afstemmen door ze toestemmingsinformatie, corporate branding of moderne authenticatie aan te bieden.
- Het beheer van devices in eigendom van het bedrijf kan met behulp van supervisie op een hoger plan worden getild. Hiermee krijgt u aanvullende beheervoorzieningen (zoals niet-verwijderbare MDM-voorzieningen) die niet beschikbaar zijn in andere implementatiemodellen.
- U kunt standaard-MDM-servers op een eenvoudigere manier beheren door een standaardserver in te stellen op basis van het devicetype. En het is nu ook mogelijk om iPhones, iPads en Apple TV's handmatig via Apple Configurator 2 aan te melden, ongeacht de manier waarop u ze hebt gekocht.

Content

Met Apple Business Manager wordt het voor organisaties gemakkelijk om content in bulk aan te schaffen. Of uw medewerkers nu met iPhone, iPad of Mac werken, u kunt ze prachtige, kant-en-klare content bieden via flexibele en veilige distributieopties.

- U kunt grote aantallen apps, boeken en apps op maat aanschaffen – ook intern ontwikkelde apps. U kunt heel eenvoudig app-licenties overzetten naar een andere locatie en licenties delen met andere gebruikers binnen één locatie. U kunt een gecompileerde lijst van de aankoopgeschiedenis bekijken, met daarin onder andere het aantal licenties dat via MDM in gebruik is.
- U distribueert apps en boeken rechtstreeks naar beheerde devices of geautoriseerde gebruikers en houdt eenvoudig bij welke content aan welke gebruiker of welk device is toegewezen. Met beheerde distributie hebt u het gehele distributieproces onder controle, terwijl de apps volledig uw eigendom

blijven. Apps die niet meer nodig zijn op een device of voor een gebruiker, kunnen worden ingetrokken en opnieuw worden toegewezen binnen de organisatie.

- Betalen kan op verschillende manieren, bijvoorbeeld met een creditcard of via een inkooporder. Organisaties kunnen bij Apple of een erkende Apple reseller volumekrediet kopen voor een bepaald bedrag in de lokale valuta. Dit wordt vervolgens elektronisch overgemaakt naar de accounthouder als Store-tegoed. Deze optie is niet overal beschikbaar.
- U kunt een app distribueren naar devices of gebruikers in elk land waar de app beschikbaar is, zodat de apps ook internationaal kunnen worden gedistribueerd. Ontwikkelaars kunnen hun apps in meerdere landen beschikbaar maken via het normale App Store-publicatieproces.

Opmerking: De mogelijkheid om boeken aan te schaffen via Apple Business Manager is in bepaalde landen niet beschikbaar. Ga naar support.apple.com/HT207305 voor informatie over de beschikbaarheid van features en aanschafmethoden.

Gebruikers

Met Apple Business Manager kunnen organisaties werknemersaccounts maken en beheren die aansluiten op de bestaande infrastructuur en toegang bieden tot zowel de apps en voorzieningen van Apple als Apple Business Manager.

- Voor werknemers kunt u beheerde Apple ID's maken, zodat ze kunnen samenwerken via apps en voorzieningen van Apple en toegang krijgen tot werkgegevens in beheerde apps die gebruikmaken van iCloud Drive. Deze accounts zijn eigendom van en worden beheerd door de betreffende organisatie.
- Door Apple Business Manager aan Microsoft Azure Active Directory te koppelen, kunt u gebundelde authenticatie toepassen. Beheerde Apple ID's worden automatisch aangemaakt wanneer werknemers zich voor de eerste keer aanmelden bij een compatibel Apple device met hun bestaande inloggegevens.
- Met de nieuwe features voor gebruikersinschrijving in iOS 13, iPadOS en macOS Catalina kunnen beheerde Apple ID's naast een persoonlijke Apple ID worden gebruikt op devices die eigendom zijn van werknemers. Beheerde Apple ID's kunnen ook op elk device worden gebruikt als primaire (en enige) Apple ID. Beheerde Apple ID's hebben na de eerste aanmelding op een Apple device bovendien toegang tot iCloud op het web.
- U kunt andere rollen aan IT-teams binnen de organisatie toewijzen voor een effectief beheer van devices, apps en accounts binnen Apple Business Manager. U gebruikt de beheerdersrol om waar nodig algemene voorwaarden te accepteren en gemakkelijk de verantwoordelijkheid over te dragen als iemand de organisatie verlaat.

Opmerking: iCloud Drive wordt momenteel niet ondersteund met gebruikersinschrijving. iCloud Drive kan met een beheerde Apple ID worden gebruikt wanneer dit de enige Apple ID op een device is.

Lees meer over Apple Business Manager: www.apple.com/nl/business/it/

Aanmelden bij het Apple Developer Enterprise Program

Het Apple Developer Enterprise Program biedt een complete set tools voor het ontwikkelen, testen en distribueren van apps. U kunt apps distribueren via een MDM-oplossing of door ze te hosten op een webserver. Mac-apps en installatieprogramma's kunnen met uw Developer ID voor Gatekeeper worden ondertekend en geauthenticeerd, zodat macOS nog beter wordt beschermd tegen malware.

Lees meer over het Developer Enterprise Program:
developer.apple.com/programs/enterprise

2. Configureren

Bij deze stap kunt u Apple Business Manager, een MDM-oplossing of eventueel Apple Configurator 2 gebruiken om uw devices te configureren en uw content te distribueren. U kunt de configuratie op verschillende manieren aanpakken. Dit is afhankelijk van wie de eigenaar is van de devices en van het gewenste implementatietype.

Devices configureren

De toegang van gebruikers tot bedrijfsvoorzieningen kunt u op verschillende manieren configureren. De IT-afdeling kan de devices instellen door configuratieprofielen te distribueren. Voor devices onder supervisie zijn aanvullende configuratieopties aanwezig.

Devices configureren met MDM

Zodra uw devices veilig bij een MDM-server zijn aangemeld, komen ze onder beheer te staan via configuratieprofielen: xml-bestanden die gegevens over de configuratie van een iOS- of iPadOS-device bevatten. Met configuratieprofielen wordt de configuratie van instellingen, accounts, beperkingen en inloggegevens geautomatiseerd. Ze kunnen draadloos worden overgezet via uw MDM-oplossing, zodat meerdere devices eenvoudig kunnen worden geconfigureerd. Profielen kunnen ook als e-mailbijlage worden verstuurd, van een website worden gedownload of op devices worden geïnstalleerd met Apple Configurator 2.

- **Devices in eigendom van de organisatie.** Met Apple Business Manager kunt u devices van gebruikers na activering automatisch aanmelden bij MDM. Alle iOS- en iPadOS-devices die aan Apple Business Manager worden toegevoegd, staan altijd onder supervisie en MDM-aanmelding is verplicht.
- **Devices in eigendom van gebruikers.** Medewerkers kunnen zelf kiezen of ze hun devices bij MDM willen aanmelden. En ze kunnen de MDM-koppeling bovendien op elk gewenst moment verwijderen door het configuratieprofiel van hun device te verwijderen. Hiermee worden tevens alle bedrijfsgegevens en -instellingen verwijderd. U wordt echter geadviseerd gebruikers aan te sporen het MDM-beheer ingeschakeld te houden. U kunt bijvoorbeeld MDM-aanmelding voor toegang tot het wifinetwerk vereisen door de inloggegevens daarvoor automatisch via MDM te verstrekken.

Nadat een device bij MDM is aangemeld, kan de beheerder een MDM-beleidsinstelling, -optie of -commando initiëren. De beheertaken die beschikbaar zijn voor een device zijn afhankelijk van het type supervisie en aanmelding. Het iOS- of iPadOS-device ontvangt vervolgens een melding van de actie van de beheerder via de Apple Push Notification-service (APNs). Zo kan het device via een beveiligde verbinding rechtstreeks communiceren met de MDM-server. Als er een netwerkverbinding is, kunnen devices overal ter wereld APNs-commando's ontvangen. Er wordt echter geen vertrouwelijke informatie via de APNs verstuurd.

Devices configureren met Apple Configurator 2 (optioneel)

Voor de lokale eerste implementatie van meerdere devices kunnen organisaties gebruikmaken van Apple Configurator 2. Met deze gratis macOS-app kunt u iOS- en iPadOS-devices via USB op een Mac aansluiten en er de nieuwste versie van iOS of iPadOS op installeren, device-instellingen en -beperkingen

configureren, en apps en andere content installeren. Na de eerste installatie kunt u verder alles draadloos beheren via MDM.

Met Apple Configurator 2 krijgt u meer zicht op uw devices en de specifieke taken die u daarop wilt uitvoeren. De app werkt naadloos samen met Apple Business Manager. Devices worden automatisch aangemeld bij MDM met de instellingen van uw organisatie. In Apple Configurator 2 kunt u via blauwdrukken aangepaste workflows met een aantal specifieke taken maken.

Lees meer over Apple Configurator 2:
support.apple.com/nl-nl/apple-configurator

Devices onder supervisie
Supervisie biedt meer mogelijkheden voor het beheer van iOS- en iPadOS-devices die in het bezit zijn van de organisatie. Er kunnen beperkingen worden ingesteld, zoals de één-app-modus of het uitschakelen van AirDrop. Ook bestaat de mogelijkheid om via een globale proxy een webfilter in te schakelen. Zo kunt u er bijvoorbeeld voor zorgen dat het webverkeer van gebruikers binnen de richtlijnen van de organisatie blijft en dat de gebruikers niet de fabrieksinstellingen van hun device kunnen terugzetten. iOS- en iPadOS-devices staan standaard niet onder supervisie. U kunt supervisie inschakelen via Apple Business Manager of handmatig inschakelen met Apple Configurator 2.

Ook als u niet van plan bent features te gebruiken die alleen voor devices onder supervisie beschikbaar zijn, kunt u overwegen supervisie tijdens de configuratie in te schakelen zodat u deze features in de toekomst alsnog kunt benutten. Anders zult u de reeds ingezette devices eerst moeten wissen. Bij supervisie gaat het niet om het vergrendelen van een device. Het gaat juist om het verbeteren van devices van de organisatie door de beheermogelijkheden ervan uit te breiden. Op de lange termijn biedt supervisie nog meer opties voor uw onderneming.

Lees meer over beperkingen voor devices onder supervisie:
support.apple.com/guide/mdm

Apps en boeken distribueren

Apple biedt diverse programma's waarmee uw organisatie de apps en content die voor iOS en iPadOS beschikbaar zijn optimaal kan benutten. Met deze voorzieningen kunt u zowel apps die u via Apple Business Manager hebt gekocht als intern ontwikkelde apps distribueren naar devices en gebruikers, zodat gebruikers alles in handen hebben om goed te kunnen werken. U moet uw distributiemethode bepalen op het moment van aankoop: beheerde distributie of inwisselcodes.

Beheerde distributie

Bij beheerde distributie gebruikt u uw MDM-oplossing of Apple Configurator 2 om apps en boeken te beheren die in de Apple Business Manager-store zijn gekocht in een land waar de app verkrijgbaar is. Om beheerde distributie in te schakelen, moet u uw MDM-oplossing eerst met een veilig token aan uw Apple Business Manager-account koppelen. Nadat de verbinding met uw MDM-server tot stand is gebracht, kunt u apps en boeken uit de Apple Business Manager-store toewijzen, zelfs als de App Store op het device is uitgeschakeld.

- **Apps aan devices toewijzen.** Met behulp van uw MDM-oplossing of Apple Configurator 2 kunt u apps direct aan devices toewijzen. U hoeft een aantal stappen van de eerste implementatie dan niet uit te voeren. Zo verloopt de implementatie aanzienlijk makkelijker en sneller en hebt u het volledige beheer over uw devices en materiaal. Nadat een app aan een device is toegewezen, wordt die via MDM naar het device gepusht. Een gebruikersuitnodiging is niet nodig. Iedereen die het device gebruikt, heeft toegang tot de app.
- **Apps en boeken aan gebruikers toewijzen.** U kunt ook uw MDM-oplossing gebruiken om gebruikers via e-mail of een pushmelding uit te nodigen om apps en boeken te downloaden. De gebruikers melden zich met hun eigen Apple ID aan op hun device om de uitnodiging te accepteren. De Apple ID wordt geregistreerd bij de Apple Business Manager-service, maar blijft verder volkomen afgeschermd en onzichtbaar voor de beheerder. Gebruikers die de uitnodiging accepteren, worden met uw MDM-server verbonden en kunnen de apps en boeken ontvangen die u aan ze toewijst. Apps zijn automatisch beschikbaar om te worden gedownload op alle devices van de gebruiker, zonder extra inspanningen of kosten van uw kant.

Wanneer de apps die aan een device of gebruiker zijn toegewezen niet meer nodig zijn, kunt u die intrekken en aan andere devices of gebruikers toewijzen. Uw organisatie blijft dus eigenaar en behoudt de volledige controle over gekochte apps. Boeken die eenmaal zijn gedistribueerd, blijven echter het eigendom van de ontvanger. Boeken kunnen niet worden ingetrokken of opnieuw worden toegewezen.

Inwisselcodes

U kunt content ook distribueren via inwisselcodes. Dit is handig als uw organisatie geen gebruik kan maken van MDM op het device van de eindgebruiker, bijvoorbeeld in het geval van een franchise. Bij deze methode wordt een app of een boek definitief overgedragen aan de gebruiker die de code inwisselt. Inwisselcodes worden aangeleverd in de vorm van een spreadsheet. Voor elke app of elk boek wordt een unieke code geleverd in de aangekochte hoeveelheid. Telkens als een code wordt ingewisseld, wordt de spreadsheet in de Apple Business Manager-store bijgewerkt, zodat u altijd kunt zien hoeveel codes er zijn ingewisseld. U kunt codes distribueren via MDM, Apple Configurator 2, e-mail of een interne website.

Apps en content installeren met Apple Configurator 2 (optioneel)
Behalve voor de eerste configuratie kan Apple Configurator 2 ook worden gebruikt om apps en content te installeren voor devices die u namens de gebruiker wilt configureren. Bij gepersonaliseerde implementaties kunt u apps vooraf installeren, zodat u tijd en bandbreedte bespaart. En bij niet-gepersonaliseerde implementaties kunt u uw devices volledig configureren, inclusief het beginscherm. Als u devices configureert met Apple Configurator 2, kunt u apps uit de App Store, interne apps en documenten installeren. Voor toegang tot apps uit de App Store is Apple Business Manager vereist. De documenten zijn beschikbaar voor apps die bestandsdeling ondersteunen. U kunt documenten inzien of ophalen van iOS- en iPadOS-devices door deze aan te sluiten op een Mac met Apple Configurator 2.

3. Implementeren

iPhone en iPad zijn zo gebruiksvriendelijk dat medewerkers hun device na het uitpakken direct kunnen gebruiken, zonder dat de IT-afdeling daarbij hoeft te helpen.

Devices distribueren

Zodra de devices in de eerste twee stappen zijn voorbereid en geconfigureerd, zijn ze klaar voor distributie. Bij gepersonaliseerde implementaties geeft u de devices aan de gebruikers. Met de gestroomlijnde configuratie-assistent kunnen ze hun device verder personaliseren en de configuratie voltooien. Bij niet-gepersonaliseerde implementaties distribueert u de devices onder de medewerkers die dienst hebben of legt u ze in speciale kiosken waarin de devices kunnen worden opgeladen en bewaard.

Configuratie-assistent
Gebruikers kunnen met behulp van de configuratie-assistent hun device activeren en de basisinstellingen configureren, zodat ze direct aan de slag kunnen.
De gebruikers doorlopen de eerste installatie, waarna ze hun eigen voorkeuren kunnen opgeven, bijvoorbeeld voor de taal, locatie, Siri, iCloud en Zoek mijn iPhone. Devices die bij Apple Business Manager zijn aangemeld, kunnen vanuit de configuratie-assistent automatisch worden aangemeld bij MDM.

Personaliseren toestaan
Bij gepersonaliseerde en BYOD-implementaties kunnen gebruikers hun device met hun eigen Apple ID personaliseren, waardoor de productiviteit omhoog gaat. Gebruikers bepalen dan namelijk zelf met welke apps en materialen ze hun taken het best kunnen uitvoeren om hun doelen te behalen.

Apple ID en beheerde Apple ID
Wanneer werknemers met een Apple ID inloggen bij Apple diensten zoals FaceTime, iMessage, de App Store en iCloud, hebben ze toegang tot allerlei materiaal waarmee ze hun werk kunnen stroomlijnen, hun productiviteit kunnen vergroten en gemakkelijker kunnen samenwerken.

Net als andere Apple ID's worden beheerde Apple ID's gebruikt voor aanmelding bij een eigen device. Ook worden ze gebruikt voor toegang tot Apple diensten, zoals iCloud en de samenwerkingsvoorzieningen in iWork en Notities, en voor Apple Business Manager. Anders dan gewone Apple ID's zijn beheerde Apple ID's eigendom van uw organisatie en worden ze door de organisatie beheerd – inclusief wachtwoordherstel en beheer op basis van rollen. Voor beheerde Apple ID's gelden bovendien bepaalde beperkingen.

Voor devices die zijn aangemeld via gebruikersinschrijving is een beheerde Apple ID nodig. Gebruikersinschrijving ondersteunt een optionele persoonlijke Apple ID. Andere aanmeldingsmethoden ondersteunen ofwel een persoonlijke Apple ID ofwel een beheerde Apple ID. Alleen gebruikersinschrijving is geschikt voor het gebruik van meerdere Apple ID's.

Om deze voorzieningen optimaal te benutten, moeten gebruikers hun eigen Apple ID of de voor hen aangemaakte beheerde Apple ID gebruiken. Gebruikers die geen Apple ID hebben, kunnen er al een aanmaken voordat ze een device krijgen. De configuratie-assistent biedt eveneens de mogelijkheid om een persoonlijke Apple ID aan te maken. Voor het aanmaken van een Apple ID is geen creditcard nodig.

Meer informatie over beheerde Apple ID's:
support.apple.com/guide/apple-business-manager

iCloud

Met iCloud kunnen gebruikers automatisch documenten en persoonlijke content synchroniseren, zoals contacten, agenda's, documenten en foto's, en die gegevens actueel houden op meerdere devices. Met 'Zoek mijn' kunnen gebruikers een verloren of gestolen Mac, iPhone, iPad of iPod touch terugvinden. Specifieke onderdelen van iCloud, zoals iCloud-sleutelhanger en iCloud Drive, kunnen worden uitgeschakeld via beperkingen die handmatig of via MDM op het device zijn ingesteld. Zo hebben organisaties meer controle over welke gegevens in welke account zijn opgeslagen.

Lees meer over het beheer van iCloud:
support.apple.com/guide/deployment-reference-ios

4. Beheren

Zodra uw gebruikers aan de slag zijn, hebt u allerlei mogelijkheden tot uw beschikking voor het beheer van de devices en de content.

Devices beheren

Een beheerd device kan aan de hand van een aantal specifieke taken worden beheerd door een MDM-server. Denk hierbij aan het opvragen van informatie van devices en het initiëren van taken om devices te beheren die niet in overeenstemming zijn met het beleid of die kwijt zijn geraakt of zijn gestolen.

Informatieverzoeken

Een MDM-server kan allerlei informatie van een device opvragen, waaronder hardwaregegevens, zoals het serienummer, de UDID van het device of het MAC-adres voor wifi, en softwaregegevens, zoals de iOS- of iPadOS-versie en een lijst met alle apps die op het device geïnstalleerd zijn. Uw MDM-oplossing gebruikt deze gegevens om voorraadgegevens up-to-date te houden, gefundeerde beheerbeslissingen te nemen en bepaalde beheertaken te automatiseren, zoals controleren of gebruikers de juiste set apps gebruiken.

Beheertaken

Bij beheerde devices kan een MDM-server allerlei beheertaken uitvoeren, zoals het automatisch wijzigen van de configuratie-instellingen (zonder tussenkomst van de gebruiker), het bijwerken van software op devices die met een toegangscode zijn vergrendeld, het op afstand vergrendelen of wissen van een device en het verwijderen van het codeslot van de gebruiker zodat deze een nieuw wachtwoord kan instellen. Ook kan een MDM-server een iPhone of iPad opdracht geven om te beginnen met synchrone AirPlay-weergave op een specifiek doeldevice of om een AirPlay-sessie te beëindigen.

Beheerde software-updates

U kunt uitstellen dat gebruikers zelf een device onder supervisie bijwerken via het draadloze netwerk. Als u deze beperking toepast, is de uitstelperiode standaard 30 dagen. Deze gaat in op het moment dat Apple een iOS- of iPadOS-update uitbrengt. U kunt de duur van de periode desgewenst wijzigen tot maximaal 90 dagen. Met een MDM-oplossing kunt u ook geplande software-updates uitvoeren op devices onder supervisie.

Verloren-modus

Uw MDM-oplossing kan een device dat onder supervisie staat, op afstand in de Verloren-modus zetten. Met deze handeling wordt het device vergrendeld en kan er een bericht met een telefoonnummer op het toegangsscherm worden geplaatst. Met de Verloren-modus kunnen devices onder supervisie bij verlies of diefstal worden gelokaliseerd: de MDM-server vraagt de locatie op waar ze voor het laatst online waren. Voor de Verloren-modus hoeft Zoek mijn iPhone niet ingeschakeld te zijn.

Activeringsslot

Met iOS 7.1 of hoger kunt u MDM gebruiken om het activeringsslot in te schakelen als een gebruiker de Zoek mijn-optie inschakelt op een device dat onder supervisie staat. Zo kan uw organisatie profiteren van de antidiefstalfunctionaliteit van het activeringsslot, terwijl deze feature ook kan worden omzeild als een gebruiker de identiteitscontrole met Apple ID niet kan uitvoeren.

Extra content distribueren en beheren

Organisaties willen vaak apps distribueren onder de gebruikers, zodat die productief kunnen werken. Maar tegelijkertijd moeten organisaties de controle houden over de manier waarop die apps verbinding maken met interne voorzieningen of waarop gegevens worden beveiligd wanneer een gebruiker de organisatie verlaat. Daarnaast is er sprake van bedrijfssoftware en persoonlijke apps en gegevens op één device.

Interne app-portals

De meeste MDM-oplossingen bieden standaard een interne app-portal. U kunt echter ook een eigen interne app-portal maken voor uw medewerkers waar ze gemakkelijk apps voor hun iPhone of iPad kunnen vinden. Bedrijfsapps, url's voor apps uit de App Store, Apple Business Manager-codes en interne apps kunnen in één portal worden ondergebracht, zodat de gebruiker alleen hier hoeft te zoeken. U kunt zo'n portal centraal beheren en beveiligen. Een interne app-portal stelt medewerkers in staat om zelf goedgekeurd materiaal te vinden, zonder eerst goedkeuring van de IT-afdeling te hoeven vragen.

Beheerd materiaal

Het beheer van content gaat over het installeren, configureren, beheren en eventueel verwijderen van apps, accounts, boeken en documenten die afkomstig zijn uit de App Store of die intern zijn ontwikkeld.

- **Beheerde apps.** Met beheerde apps in iOS en iPadOS kan een organisatie gratis apps, betaalde apps en bedrijfsapps draadloos distribueren via MDM en daarbij de juiste balans vinden tussen de beveiliging van bedrijfsgegevens en de privacy van de gebruiker. Beheerde apps kunnen op afstand worden verwijderd door een MDM-server of wanneer de gebruiker zijn of haar device afmeldt bij MDM. Als de app wordt verwijderd, worden ook alle bijbehorende gegevens verwijderd. Als een app nog steeds via Apple Business Manager aan de gebruiker is toegewezen of als de gebruiker een app-code heeft ingewisseld met behulp van de eigen Apple ID, kan de app opnieuw uit de App Store worden gedownload, maar in dat geval wordt de app niet langer beheerd via MDM.
- **Beheerde accounts.** Met MDM kunnen e-mailaccounts en andere gebruikersaccounts automatisch worden ingesteld, zodat de gebruikers binnen uw organisatie snel aan de slag kunnen. Afhankelijk van de MDM-leverancier en de integratie met uw interne systemen kunnen de accountgegevens vooraf worden aangevuld met de naam en het e-mailadres van de gebruiker, en eventueel ook met certificaatidentiteiten voor identiteitscontrole en ondertekening.
- **Beheerde boeken en documenten.** MDM-tools, boeken, ePub-boeken en pdf-documenten kunnen automatisch naar het device van uw medewerkers worden gepusht, zodat die altijd alle benodigde materialen hebben. Beheerde boeken kunnen echter alleen worden gedeeld met andere beheerde apps of worden gemaild via beheerde accounts. Als een bestand niet meer nodig is, kan het op afstand worden verwijderd. Boeken die via Apple Business Manager worden gekocht, kunnen worden gedistribueerd via beheerde boekdistributie, maar kunnen niet worden ingetrokken en opnieuw worden toegewezen. Een boek dat al door de gebruiker is gekocht, kan alleen worden beheerd als het via Apple Business Manager expliciet aan de gebruiker wordt toegewezen.

Beheerde appconfiguratie

App-ontwikkelaars kunnen aangeven welke instellingen en voorzieningen van apps kunnen worden ingeschakeld als de app als beheerde app wordt geïnstalleerd. Deze configuratie-instellingen kunnen voor of na de installatie van de beheerde app worden opgegeven. De IT-afdeling kan bijvoorbeeld een reeks standaardvoorkeuren installeren voor een SharePoint-app, zodat de gebruiker de serverinstellingen niet handmatig hoeft te configureren.

Gerenommeerde MDM-leveranciers hebben de AppConfig Community in het leven geroepen en een standaardschema opgesteld dat door alle app-ontwikkelaars kan worden gebruikt voor de ondersteuning van de configuratie van beheerde apps. De AppConfig Community richt zich op het bieden van tools en beproefde methoden rond native functionaliteit in mobiele besturingssystemen. De community draagt bij aan een consistentere, transparantere en eenvoudigere manier om mobiele apps te configureren en te beveiligen, zodat mobiele devices gemakkelijker in het bedrijfsleven kunnen worden ingezet.

Lees meer over de AppConfig Community:
appconfig.org

Beheerde gegevensstroom

MDM-oplossingen bieden specifieke features waarmee bedrijfsgegevens op detailniveau beheerd kunnen worden, zodat deze niet naar de persoonlijke apps en cloudservices van de gebruiker uitlekken.

- **Open in-functie.** Voor het beheer van de Open in-functie wordt gebruikgemaakt van een reeks beperkingen waarmee voorkomen wordt dat bijlagen en documenten uit beheerde bronnen worden geopend op niet-beheerde bestemmingen, en omgekeerd. U kunt bijvoorbeeld voorkomen dat een vertrouwelijke bijlage bij een mail in de beheerde mailaccount van uw organisatie wordt geopend in een persoonlijke app van een gebruiker. Het bedrijfsdocument kan alleen worden geopend met apps die via MDM zijn geïnstalleerd én via MDM worden beheerd. De onbeheerde persoonlijke apps van de gebruiker worden niet eens weergegeven in de lijst met apps waarmee de bijlage kan worden geopend. Naast beheerde apps, accounts, boeken en domeinen maken ook verschillende extensies gebruik van de beperkingen van de beheerde Open in-functie.
- **Eén-app-modus.** Met deze instelling kan een iOS- of iPadOS-device worden beperkt tot één app. Dit is ideaal voor kiosken of devices die voor één enkel doeleinde worden ingezet, bijvoorbeeld bij een verkooppunt in een winkel of bij de receptie van een ziekenhuis. Ontwikkelaars kunnen deze functie ook inschakelen binnen hun apps, zodat apps zelfstandig de één-app-modus kunnen starten en beëindigen.
- **Reservekopie voorkomen.** Met deze beperking wordt voorkomen dat er een reservekopie van beheerde apps wordt bewaard in iCloud of op een computer. Wanneer het maken van reservekopieën niet is toegestaan, is het niet mogelijk om gegevens uit een beheerde app terug te zetten als de app via MDM wordt verwijderd en later door de gebruiker opnieuw geïnstalleerd wordt.

Ondersteuningsopties

Apple biedt een scala aan programma's en ondersteuningsopties voor iOS- en iPadOS-gebruikers en IT-beheerders.

AppleCare for Enterprise

Bedrijven die optimaal gedekt willen zijn, kunnen met AppleCare for Enterprise de werklast van hun interne helpdesk verlichten. Medewerkers krijgen namelijk 24 uur per dag, zeven dagen per week technische ondersteuning via de telefoon, met een reactietijd van één uur voor problemen met de hoogste prioriteit. IT-medewerkers worden geholpen bij problemen met alle hardware en software van Apple, en u krijgt ondersteuning bij complexe implementatie- en integratiescenario's, inclusief MDM en Active Directory.

AppleCare OS Support

Via AppleCare OS Support beschikt uw IT-afdeling over professionele ondersteuning per telefoon en e-mail voor implementaties van iOS en iPadOS, macOS en macOS Server. U krijgt tot 24 uur per dag en 7 dagen per week ondersteuning en een eigen Technical Account Manager, afhankelijk van het gekozen ondersteuningsniveau. Via AppleCare OS Support heeft uw IT-personeel direct contact met technici voor vragen over integratie, migratie en geavanceerde serverproblemen, en kan het veel efficiënter te werk gaan bij de implementatie en het beheer van devices en het oplossen van problemen.

AppleCare Help Desk Support

Met AppleCare Help Desk Support kunt u met voorrang telefonisch contact opnemen met ervaren ondersteuningsmedewerkers van Apple. Bovendien krijgt u de beschikking over een verzameling tools voor het opsporen en oplossen van problemen met hardware van Apple. Hierdoor kunnen grote instellingen problemen sneller en efficiënter oplossen en blijven de opleidingskosten beperkt. Met het AppleCare Help Desk Support-plan kunt u een onbeperkt aantal aanvragen indienen voor het opsporen en verhelpen van problemen met hardware en software en het isoleren van problemen met iOS- of iPadOS-devices.

AppleCare voor gebruikers van iOS- en iPadOS-devices

Elk iOS- en iPadOS-device wordt geleverd met een beperkte garantie van één jaar en gratis telefonische ondersteuning gedurende 90 dagen na de aankoopdatum. U kunt deze dekking uitbreiden tot twee jaar vanaf de oorspronkelijke aankoopdatum met AppleCare+ voor iPhone, AppleCare+ voor iPad of AppleCare+ voor iPod touch. U kunt zo vaak als u wilt bellen met onze deskundigen om uw vragen voor te leggen. Daarnaast biedt Apple handige serviceopties als een device gerepareerd moet worden. Bovendien bieden deze abonnementen aanvullende dekking voor maximaal twee schadevoorvallen als gevolg van een ongelukje. Per incident worden servicekosten in rekening gebracht.

iOS Direct Service-programma

Met het iOS Direct Service-programma, een aanvulling op AppleCare+, kan uw helpdesk devices screenen op problemen zonder dat u AppleCare hoeft te bellen of een Apple Store hoeft te bezoeken. Indien nodig kan uw organisatie rechtstreeks een vervangende iPhone, iPad, iPod touch of vervangend standaardaccessoire bestellen.

Lees meer over de AppleCare-programma's:
apple.com/nl/support/professional/

Samenvatting

Ongeacht of uw bedrijf iPhone of iPad implementeert onder een beperkte groep gebruikers of binnen de gehele organisatie, u beschikt altijd over een groot aantal opties om devices eenvoudig te implementeren en te beheren. Als u de juiste strategieën kiest voor uw organisatie, kunnen uw werknemers productiever en op een heel andere manier werken.

Lees meer over implementatie, beheer en beveiliging van iOS en iPadOS:
support.apple.com/guide/deployment-reference-ios

Lees meer over MDM-instellingen voor IT:
support.apple.com/guide/mdm

Lees meer over Apple Business Manager:
support.apple.com/guide/apple-business-manager

Lees meer over beheerde Apple ID's voor bedrijven:
apple.com/business/docs/site/Overview_of_Managed_Apple_IDs_for_Business.pdf

Lees meer over Apple at Work:
www.apple.com/nl/business/

Lees meer over features voor IT:
www.apple.com/nl/business/it/

Lees meer over Apple platformbeveiliging:
support.apple.com/guide/security

Bekijk de beschikbare AppleCare-programma's:
www.apple.com/nl/support/professional/

Bekijk de Apple cursussen en certificering:
training.apple.com

Neem contact op met Apple Professional Services:
consultingservices@apple.com