



iPad en iOS

Upgradegids voor beginners

Alles wat je nodig hebt om je voor te bereiden op iOS en iPadOS 18



Ben je klaar om iOS en iPadOS te upgraden?

Apple brengt elk jaar grote iOS- en iPadOS-versies uit. IT- en beveiligingsleiders moeten eindgebruikers voorzien van deze nieuwe systemen en de bijbehorende functies, zonder workflows te onderbreken of de productiviteit te vertragen.

Waarom een Apple upgrade anders is

In tegenstelling tot andere ecosystemen worden grote versies van Apple's besturingssystemen, ook wel bekend als een upgrade, jaarlijks uitgebracht. Dit omvat macOS, iPadOS, iOS, tvOS, watchOS en vision OS. Wanneer apparaten verouderde software gebruiken, kan dit ten koste gaan van de consistentie, beveiliging en gebruikerservaring. Wanneer organisaties verschillende apparaattypen en meerdere regio's moeten ondersteunen, is het des te belangrijker dat de upgrades eenvoudig kunnen worden geïnstalleerd.

De combinatie van het eenvoudige upgradepad en het feit dat upgrades van het Apple-OS niets kosten, draagt bij aan de toonaangevende adoptiegraad voor consumenten. Eindgebruikers willen graag de nieuwste functies gebruiken, maar jij moet als eerste altijd zorgen voor hoogwaardige beveiliging en een correcte systeeminventaris.

Zoals de meeste IT-teams weten, is dit makkelijker gezegd dan gedaan, vooral als het aankomt op upgraden in het tempo dat je Apple gebruikers verwachten. Maar natuurlijk hebben we ook goed nieuws.

Bij Jamf doen we dit al twintig jaar. We zijn hier om stapsgewijze begeleiding te bieden voor succesvolle Apple upgrades, ongeacht of dit je eerste upgraderonde is of dat je een professional bent die op zoek is naar snelle opfrisinformatie.

Er zijn vier belangrijke redenen waarom organisaties upgrades moeten omarmen en de IT-afdeling of eindgebruikers in staat moeten stellen om apparaten bij te werken wanneer nieuwe besturingssystemen worden uitgebracht:

- 1. Terugdringen van kwetsbaarheden op het gebied van beveiliging**
- 2. Eindgebruikers tevredenstellen**
- 3. Gebruikers productief houden**
- 4. Profiteren van nieuwe IT-beheersfuncties**

In deze gids wordt grondig uitgelegd hoe je een nieuw besturingssysteem voor iOS- en iPadOS-apparaten kunt voorbereiden en implementeren. Je leert hoe je onderbrekingen tot een minimum kunt beperken en ongeplande downtime kunt voorkomen, terwijl je de kennis opdoet om organisatorische waarde te leveren en gebruikers te ondersteunen bij het upgraden van hun apparaten naar iOS en iPadOS 18.

Beter met bèta

Bewapen jezelf met voorvertoningen van aankomende releases van het Apple Beta-softwareprogramma om in een vroeg stadium te zien hoe nieuwe versies van besturingssystemen en functies van invloed zullen zijn op je organisatie.

Apple werkt zijn besturingssystemen regelmatig bij. Door deel te nemen aan het bètaprogramma kun je maandenlang testen voordat een besturingssysteem wordt uitgebracht. Apple biedt zowel betaalde bètaprogramma's voor ontwikkelaars als gratis publieke bètaprogramma's voor macOS, iPadOS, iOS, tvOS, watchOS en visionOS.

Waarom meedoen aan het bètaprogramma?

- 1. De bètacyclus voor deze besturingssystemen verloopt meestal in meerdere fasen.** Door vroegtijdig deel te nemen en feedback te sturen naar Apple, vergroot je de kans dat de functies en problemen die voor jou het meest van belang zijn, worden aangepakt. En als je als eerste een bugrapport bij Apple indient, heb je inzicht in de status van je ticket terwijl dubbele bugrapporten worden gesloten.
- 2. Deelname aan de bèta geeft je niet alleen vroegtijdige toegang om nieuwe functies en compatibiliteit te testen, maar het biedt ook een beter begrip van hoe de ervaring van de eindgebruiker zal worden beïnvloed.** Als je weet welke nieuwe instellingen zijn toegevoegd, welke functies zijn verplaatst of welke wijzigingen er zijn aangebracht in labels, kun je het trainingsmateriaal, de onboarding-kits, het IT-beleid en dergelijke bijwerken.

Dit helpt je organisatie zich optimaal voor te bereiden op veranderingen in de eindgebruikerservaring, zodat je een meer gebruikersgericht ondersteuningsmodel en communicatieplan kunt uitvoeren.
- 3. Tot slot is het testen van de compatibiliteit van apps, infrastructuur, beheer en beveiliging, naast nieuwe instellingen en functies van besturingssystemen, van cruciaal belang voor de continuïteit met het huidige softwareaanbod in je omgeving.** We raden je aan de bèta's van Apple te gebruiken om hun geïmplementeerde apps te testen op problemen. Als je problemen meteen meldt aan de betreffende leveranciers, zorg je ervoor dat de apps werken op het moment dat Apple ze officieel uitbrengt.

Als je nog niet hebt deelgenomen aan [de bètaprogramma's van Apple](#), kun je dat altijd gratis doen en behaal je voordeel bij toekomstige OS-tests. De feedback die je geeft over kwaliteit en gebruiksvriendelijkheid helpt Apple bij het identificeren van problemen, het oplossen ervan en het nog beter maken van Apple software voor je en je gebruikers.

Testen

Voor het beste resultaat en om te voorkomen dat de upgrade een onverwachte impact heeft op aspecten van de workflows van je eindgebruikers, moet je je hele techstack testen, met inbegrip van:

1 Infrastructuur

Hierbij gaat het om alles rondom je apps, zoals VPN of het testen van printerdrivers (die je altijd moet testen bij een nieuw besturingssysteem). Het testen van infrastructuur is minder belangrijk voor organisaties die overstappen op cloudhosting.

2 Toepassingen

Dit omvat zowel web- als niet-webgebaseerde apps. Als je onvoldoende tijd hebt om alle apps te testen, moet je prioriteiten stellen op basis van uitspraken van de leverancier over de compatibiliteit van de app. Voor leveranciers die de geplande compatibiliteit niet proactief promoten op hun website, in documentatie of in directe communicatie, is het het beste om de apps zelf te valideren.

3 beheer

Controleer of je oplossing voor apparaatbeheer de mogelijkheid biedt om nieuwe beperkingen, beheermogelijkheden en functies te testen.

4 Beveiliging

Omvat identiteit en toegang, eindpuntbeveiliging, preventie van bedreigingen en het filteren van inhoud. Controleer, net als bij je beheerprovider, of je beveiligingsoplossing de mogelijkheid biedt om nieuwe beveiligingsmogelijkheden en -functies te testen.

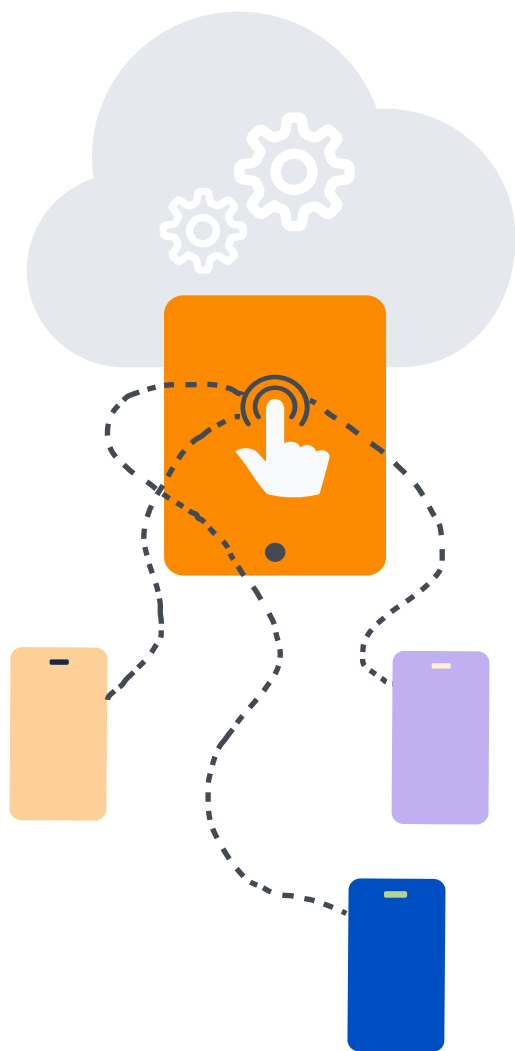
De volgorde van je tests

Waarschijnlijk gebruikt je organisatie allerlei verschillende apps. Jullie hebben tenslotte een verscheidenheid aan teams die apparaten op heel verschillende en individuele manieren gebruiken. De volgorde van de tests van de verscheidene apps is van cruciaal belang.

Sommigen kiezen voor een rangschikking van apps in categorieën van hoog, gemiddeld en laag belang, terwijl anderen kijken naar het gebruik van elke app en op basis daarvan prioriteiten stellen. Zodra dat is besloten en uitgesplitst, kan het werven van vertegenwoordigers van elke afdeling (Financiën, Marketing, Verkoop, enz.) om te testen helpen bij het begrijpen van de verschillen in de dagelijkse behoeften van hun gebruikers en ervoor zorgen dat alles zo soepel mogelijk verloopt.

Vanwege de architectuur van iPadOS-, iOS- en tvOS-apps zijn lichte tests wellicht geschikter voor deze platforms dan macOS.





Beheerde software-updates met declaratief apparaatbeheer

Klanten van Jamf Cloud kunnen een upgrade downloaden en de installatie ervan plannen met behulp van beheerde software-updates, aangedreven door het declaratief-apparaatbeheerprotocol. Op die manier kun je Jamf Pro gebruiken om eenvoudig en in één handeling een specifieke updateversie en -deadline te richten op een groep apparaten.

Zodra het updateplan is gedefinieerd, zorgt iOS voor gebruikersmeldingen en herinneringen om de eindgebruiker te informeren over de uiteindelijke deadline voor de afdwinging en de update. Apparaten geven proactief en automatisch feedback aan Jamf Pro over de voortgang van de update.

Hiervoor zijn mobiele apparaten met iOS 17 of iPadOS 17 of hoger vereist. tvOS, visionOS en watchOS worden niet ondersteund. Alleen beschikbaar voor Jamf Cloud-klanten.

Upgraden naar OS 18

Als het aankomt op het daadwerkelijk uitrollen en uitvoeren van de upgrade voor iPad- en iPhone-apparaten, zijn er twee opties. Je bepaalt gewoon of je wilt dat gebruikers of IT de upgrade uitvoeren.



Voordat we dieper ingaan op elke upgrade-optie, moet je weten dat als je nog aan het testen bent of nog niet klaar bent om te upgraden, je de mogelijkheid hebt om updates uit te stellen tot na de release van Apple als je een beheeroplossing zoals Jamf gebruikt. Tijdens dit uitstel kunnen gebruikers hun apparaat niet upgraden. Zodra je besluit om te updaten, kun je ervoor kiezen om een specifieke versie van het besturingssysteem te implementeren.

Klaar voor de upgrade?

Als je eenmaal hebt besloten om verder te gaan met een upgrade, moet je bepalen of je wilt dat gebruikers of IT de upgrade uitvoeren.

Upgrade door gebruiker

Als je je gebruikers de upgrades laat uitvoeren, kunnen ze gewoon naar de Systeeminstellingen op hun apparaat(en) gaan en de installatie starten. Er is geen IT-interactie nodig.

Upgrade door IT

Als je apparaten worden beheerd door Apple Business Manager of Apple School Manager, heeft IT de mogelijkheid om een MDM-opdracht te sturen om te downloaden en een nieuw besturingssysteem te installeren.

Deze opdracht kan naar individuele apparaten of groepen gestuurd worden, zodat je de controle hebt om je aangepaste upgradeplan te gebruiken.

Opmerking: Als er geen wachtwoord is, kun je de installatie automatisch uitvoeren. Als het apparaat een wachtwoordcode heeft, zet Jamf Pro of Jamf School de update in de wachtrij en wordt de gebruiker gevraagd zijn wachtwoordcode in te voeren om de installatie te starten.

Nog niet klaar om te upgraden?



Klaar wanneer jij dat bent, maar toch doorlopend beveiligd

De RecommendationCadence-sleutel van Apple in configuratieprofielen geeft IT-beheerders extra mogelijkheden bij het overwegen van updates voor gebruikers.

Door apparaten bij te werken naar een nieuw besturingssysteem zodra dit beschikbaar is, zorg je ervoor dat gebruikers over alle nieuwste functies en beveiligingsinstellingen beschikken zodra deze beschikbaar zijn. Klinkt geweldig, maar wat als je nog niet klaar bent voor de uitrol in de productieomgeving en meer tijd nodig hebt? Wat als er beveiligingsupdates zijn die moeten worden toegepast voordat je de sprong waagt naar een volledige update?

Hier is een optie voor. IT-beheerders kunnen ervoor kiezen om apparaten gebruik te laten blijven maken van eerdere besturingssystemen, maar wel bij te werken met de essentiële beveiligingsinstellingen. Als je iPhone-apparaten onder toezicht bijvoorbeeld iOS 17.4 gebruikt, heb je de mogelijkheid om die bij te werken naar iOS 17.5 voordat je een grote upgrade naar iOS 18 uitvoert.

Dit geeft je extra tijd om de overstap te maken zodra je er klaar voor bent, zonder dat je beveiligingsupdates hoeft te missen.

Communicatie met eindgebruikers

Een laatste opmerking, waar je je gedurende dit proces heel bewust van moet zijn, is dat het essentieel is om open, transparant en vaak met je eindgebruikers te communiceren over wat er met hun apparaten en hun rol gaat gebeuren in de upgrade.

Of je nu met ze bespreekt wanneer ze kunnen upgraden, hoe dat proces verloopt of waarom ze nog even niet kunnen upgraden, het hele proces zal soepeler verlopen als je goed met hen communiceert.

Een van de belangrijkste zaken die je met communicatie inperkt, is simpelweg het aantal helpdesktickets of de vragen die je over dit onderwerp krijgt. En door dergelijke verzoeken en vragen voor te zijn, blijven je eindgebruikers tevreden en betrokken bij het proces, voor het geval dat je hun hulp op een bepaald moment nodig hebt.

Stappen om eindgebruikers voor te bereiden

- 1.** Niet elke eindgebruiker weet hoelang een upgrade duurt. Vertel gebruikers hoeveel tijd een upgrade in beslag neemt en geef tips over het beste tijdstip om te upgraden.
- 2.** Raad je eindgebruikers aan een back-up van hun appara(a)t(en) te maken voordat ze deze updaten. Dit geldt voor zowel lokale als iCloud-back-ups.
- 3.** Implementeer een beleid om eindgebruikers te verplichten te updaten binnen 30 dagen vanaf de startdatum die jij hebt bepaald, of laat hen weten dat jij voor hen een update uitvoert. Voor compliance van PCI DSS moet dit binnen 30 dagen gebeuren.

Gebruik e-mail, het intranet of je Jamf Self Service-appcatalogus om gebruikers te waarschuwen en aanbevelingen te doen voordat OS-upgrades worden toegepast. Ze zullen je er dankbaar voor zijn.



Upgrade, verbeter en geniet

iOS 18 en iPadOS 18 brengen verbeteringen en workflowuitbreidingen om van je apparaten de flexibele machine op maat te maken die je nodig hebt en verwacht van Apple.

Met een naadloos upgradeproces voor je organisatie zorg je niet alleen voor veilige systemen, het behoud van een correcte voorraad en continuïteit, je laat ook zien wie je bent: een echte IT-held. De speciaal ontwikkelde beheeroplossing voor zakelijke Apple apparaten geeft je de noodzakelijke instrumenten om optimaal gebruik te maken van de nieuwste besturingssystemen van Apple, zonder een negatieve impact op de eindgebruikers of overmatige werkbelasting voor het IT-personeel.

Jamf is de enige beheer- en beveiligingsoplossing op schaal die de volledige levenscyclus van Apple automatiseert, inclusief upgrades van het besturingssysteem, zonder workflows te onderbreken of de ervaring van de eindgebruiker negatief te beïnvloeden. Jamf heeft meer dan 20 jaar ondersteuning op dezelfde dag en compatibiliteit met de releasedata van besturingssystemen van Apple.



[Aan de slag](#)

Of neem contact op met je favoriete geautoriseerde reseller van Apple-apparaten om Jamf te proberen.