



Descrição geral da implementação do Mac

Índice

[Introdução](#)

[Primeiros passos](#)

[Passos de implementação](#)

[Opções de assistência](#)

[Resumo](#)

Introdução

Na Apple, acreditamos que o acesso às melhores ferramentas e tecnologias ajuda os funcionários a fazerem o melhor trabalho possível. Todos os nossos produtos foram concebidos para aumentar a criatividade e produtividade dos funcionários e ajudá-los a encontrar novas formas de trabalhar, dentro e fora do escritório. Esta visão está de acordo com a forma como os funcionários preferem trabalhar no mundo atual: com mais acesso à informação, melhores soluções de colaboração e partilha e a liberdade de poderem estar ligados e trabalhar em qualquer lugar.

Nunca foi tão fácil configurar e implementar computadores Mac no ambiente empresarial dos dias de hoje. A sua empresa pode facilmente implementar e prestar assistência ao Mac em escala através dos serviços específicos da Apple e de uma solução de gestão de dispositivos móveis (MDM) de outra empresa. Caso a sua empresa já tenha implementado dispositivos iOS e iPadOS internamente, é provável que a maior parte das infraestruturas necessárias para a implementação do macOS já estejam prontas.

As melhorias recentes da segurança, gestão e implementação do Mac permitem que a empresa faça a transição entre imagens monolíticas e diretórios tradicionais para um modelo de aprovisionamento eficaz e um processo de implementação centrado em cada utilizador e que depende quase exclusivamente de ferramentas integradas no macOS.

Este documento inclui indicações sobre tudo o que é necessário para implementar o Mac em escala, como conhecer a infraestrutura existente, gerir dispositivos e otimizar o aprovisionamento. Os tópicos abordados neste documento são descritos com mais detalhe no Guia de referência para implementação do Mac, disponível online:

support.apple.com/guide/deployment-reference-macos

Primeiros passos

Alguns passos iniciais importantes do processo de implementação são a criação de uma estratégia e de um plano de implementação e a avaliação da utilização atual do macOS por parte dos funcionários. Assegure o envolvimento atempado das equipas necessárias e certifique-se de que apoiam a visão e os objetivos do programa. Algumas equipas começam por efetuar uma pequena prova de conceito para determinar os desafios específicos da empresa. É essencial comunicar com os utilizadores existentes para compreender a utilização atual dos dispositivos na empresa e informar a equipa sobre potenciais problemas.

A informação recolhida pode ajudar a identificar as principais funções que podem tirar partido do Mac. A equipa de TI pode determinar se o macOS deve ser implementado em toda a empresa ou apenas oferecido como opção para funções específicas.

Muitas vezes, esta fase permite criar uma lista abrangente das ferramentas e apps internas que requerem compatibilidade antes da implementação global do Mac. Em primeiro lugar, concentre-se nas principais apps de produtividade, colaboração e comunicação que são utilizadas pela maior parte dos funcionários. Serviços internos essenciais, como a intranet, o diretório e o software de gestão de despesas, também são importantes para garantir a produtividade de uma grande parte da empresa.

Documente e comunique quaisquer soluções ou alternativas para outras ferramentas internas, incentivando os proprietários das apps a fazerem as atualizações necessárias. Informe os utilizadores, de forma transparente, sobre as apps empresariais que vão poder usar se escolherem o Mac, e dê prioridade aos pedidos dos utilizadores nos esforços de modernização. Quando necessário, crie um plano em conjunto com os proprietários das apps para determinar a forma como podem atualizar as apps, tirando partido do macOS SDK e Swift, bem como da grande variedade de parceiros empresariais que podem contribuir para o desenvolvimento.

Normalmente, os computadores Mac são atribuídos como dispositivos que são propriedade da empresa. Algumas empresas podem permitir que os funcionários utilizem o Mac para trabalhar através de programas "traga o seu próprio dispositivo" (BYOD). Seja qual for o modelo de propriedade, permitir que os funcionários escolham os produtos Apple pode trazer vantagens a toda a empresa, como níveis mais elevados de produtividade, criatividade, envolvimento e satisfação dos funcionários, e a redução dos custos relacionados com valores residuais e assistência. As empresas também podem tirar partido de várias opções de financiamento e leasing para reduzir os custos iniciais. Para compensar os custos, as empresas podem permitir que os funcionários contribuam com deduções salariais durante a atualização, ou que comprem o equipamento no fim do período de leasing ou do ciclo de vida do dispositivo.

As políticas da empresa, bem como os processos de implementação, gestão e assistência descritos neste documento, podem variar de acordo com a informação recolhida pela equipa durante a fase de teste. Nem todos os utilizadores necessitam das mesmas políticas, definições e apps, uma vez que os requisitos dos diferentes grupos ou equipas de uma empresa diferem significativamente.

Passos de implementação

A implementação do macOS tem quatro passos principais: preparar o ambiente, configurar a MDM, implementar os dispositivos junto dos funcionários e efetuar tarefas de gestão contínua.

1. Preparar

O primeiro passo de qualquer implementação é considerar o ambiente existente. Esta fase implica a avaliação da rede e da infraestrutura principal, assim como a configuração dos sistemas necessários para o sucesso da implementação.

Avaliar a infraestrutura

Embora o Mac se integre na perfeição na maioria dos ambientes de TI utilizados habitualmente pelas empresas, é importante avaliar a infraestrutura existente e garantir que a empresa tira o máximo partido de tudo o que o macOS tem para oferecer. Se a empresa necessitar de ajuda nesta área, pode solicitar assistência aos Serviços profissionais da Apple, assim como às equipas técnicas do seu parceiro de canal ou revendedor.

Wi-Fi e rede

O acesso consistente e fiável a uma rede sem fios é essencial para efetuar a configuração de dispositivos macOS. Confirme se a rede Wi-Fi da empresa foi concebida de forma a considerar a posição e potência dos pontos de acesso e satisfazer as necessidades de roaming e capacidade.

Também poderá ser necessário ajustar as configurações de proxies da Web ou portas de firewall se os dispositivos não conseguirem aceder aos servidores da Apple, ao serviço de notificações em tempo real da Apple (APN), ao iCloud ou à iTunes Store. Tal como no iPad e iPhone, algumas fases do processo de implementação do Mac requerem o acesso a estes serviços, especialmente no caso de hardware Mac mais recente.

A Apple e a Cisco otimizaram a comunicação entre os computadores Mac e as redes sem fios da Cisco, adicionando compatibilidade para as funcionalidades de rede avançadas do macOS, como qualidade de serviço (QoS). Se tiver equipamento de rede da Cisco, colabore com as equipas internas para garantir que o Mac será capaz de otimizar o tráfego de dados importantes.

As empresas devem avaliar a infraestrutura de VPN para garantir que os utilizadores conseguem aceder aos recursos da empresa de forma segura e remota. Recomendamos que utilize a opção VPN On Demand do macOS para que a ligação VPN seja iniciada apenas quando necessário. Se pretender utilizar a opção VPN por app, verifique se os gateways VPN são compatíveis com estas capacidades, e compre licenças suficientes para abranger o número necessário de utilizadores e ligações.

Certifique-se de que a infraestrutura de rede está configurada para funcionar corretamente com o Bonjour (o protocolo de rede de configuração automatizada baseado em normas da Apple). O Bonjour permite aos dispositivos encontrar serviços numa rede automaticamente. O macOS utiliza o Bonjour para estabelecer ligação a impressoras compatíveis com AirPrint e a dispositivos compatíveis com AirPlay, como a Apple TV. Algumas apps e funcionalidades integradas do macOS utilizam o Bonjour para descobrir outros dispositivos para colaboração e partilha.

Saiba mais sobre o design de rede Wi-Fi:

support.apple.com/guide/deployment-reference-macos

Saiba mais sobre configurar a sua rede para MDM:

support.apple.com/HT210060

Saiba mais sobre o Bonjour:

support.apple.com/pt-pt/guide/deployment-reference-macos

Gerir identidades

O macOS consegue aceder a serviços de diretório para gestão de identidades e outros dados dos utilizadores, incluindo Active Directory, Open Directory e LDAP. Alguns fornecedores de MDM oferecem ferramentas para a integração imediata das soluções de gestão com diretórios Active Directory e LDAP. Ferramentas adicionais, como a extensão Single Sign-On Kerberos no macOS Catalina, permitem a integração com funcionalidades e políticas do Active Directory sem exigir um vínculo tradicional e uma conta móvel. A solução de MDM também gere vários tipos de certificados de autoridades de certificação (CA) internas e externas, para que seja possível confiar automaticamente nas identidades.

Saiba mais sobre a nova extensão Single Sign-on Kerberos:

support.apple.com/guide/deployment-reference-macos

Saiba mais sobre a integração do diretório:

support.apple.com/pt-pt/guide/deployment-reference-macos

Principais serviços para os funcionários

Verifique se o serviço Microsoft Exchange está atualizado e configurado para suportar todos os utilizadores na rede. Se não utilizar o Exchange, o macOS também é compatível com servidores baseados em normas, incluindo IMAP, POP, SMTP, CalDAV, CardDAV e LDAP. Teste processos de trabalho básicos para emails, contactos e calendários, bem como outro software de produtividade e colaboração da empresa que represente a maior percentagem diária de processos de trabalho importantes dos utilizadores.

Saiba mais sobre a configuração do Microsoft Exchange:

support.apple.com/guide/deployment-reference-macos

Saiba mais sobre serviços baseados em normas:

support.apple.com/guide/deployment-reference-macos

Conteúdos em cache

O serviço de cache integrado no macOS armazena uma cópia local de conteúdos dos servidores Apple solicitados com frequência, ajudando a minimizar a largura de banda necessária para descarregar conteúdos na rede. Pode colocar conteúdos em cache para acelerar o download e a transmissão de software através da Mac App Store. Pode ainda colocar atualizações de software em cache, para descarregar estes conteúdos mais rapidamente em dispositivos macOS, iOS ou iPadOS da empresa. Também é possível colocar conteúdos adicionais em cache com soluções de outras empresas (da Cisco e da Akamai).

Saiba mais sobre a colocação de conteúdos em cache:

support.apple.com/guide/deployment-reference-macos

Estabelecer uma solução de gestão

Com a MDM, as empresas podem registar o Mac no ambiente empresarial, configurar e atualizar definições sem fios, implementar apps, monitorizar a conformidade com as políticas empresariais, consultar os dispositivos e apagar todos os dados ou bloquear remotamente os dispositivos geridos de forma segura. A equipa de TI pode facilmente criar perfis para gerir as contas dos utilizadores, configurar definições do sistema, aplicar restrições e definir políticas de palavra-passe, através da mesma solução de gestão de dispositivos móveis que utiliza para o iPhone e iPad.

Em segundo plano, todas as plataformas da Apple utilizam a mesma estrutura de gestão da Apple, que permite aos clientes trabalhar com várias soluções de MDM de outras empresas. Estão disponíveis várias soluções de gestão de dispositivos, de empresas como Jamf, VMware e MobileIron. Embora o macOS partilhe muitas estruturas de gestão de dispositivos com o iOS e o iPadOS, as soluções de MDM de outras empresas diferem ligeiramente em termos de funcionalidades administrativas, compatibilidade com o sistema operativo, estruturas de preços e modelo de alojamento. Podem ainda fornecer diferentes níveis de serviços de integração, formação e assistência. Antes de escolher uma solução, avalie quais são as funcionalidades mais relevantes para a empresa.

Assim que selecionar uma solução de MDM, terá de visitar o Portal de certificados da Apple e iniciar sessão para criar um novo certificado de MDM.

Saiba mais sobre a implementação da MDM:

support.apple.com/guide/deployment-reference-macos

Visite o Portal de certificados da Apple:

identity.apple.com/pushcert/

Registo no Apple Business Manager

O Apple Business Manager é um portal baseado na internet que permite aos administradores de TI implementar o iPhone, iPad, iPod touch, Apple TV e Mac num só local. Ao trabalhar de forma integrada com a sua solução de gestão de dispositivos móveis (MDM), o Apple Business Manager faz com que seja fácil automatizar a implementação de dispositivos, comprar apps, distribuir conteúdos e criar ID Apple geridos para os funcionários.

O Programa de registo de dispositivos (DEP) e o Programa de compras em volume (VPP) estão agora totalmente integrados no Apple Business Manager, para que as empresas possam reunir tudo o que é necessário para implementar dispositivos Apple. Estes programas vão deixar de estar disponíveis a partir de 1 de dezembro de 2019.

Dispositivos

O Apple Business Manager permite efetuar o Registo automatizado de dispositivos, oferecendo às empresas uma forma rápida e otimizada de implementar dispositivos Apple que são propriedade da empresa e efetuar o registo na MDM sem necessidade de preparar ou de interagir fisicamente com cada dispositivo.

- Simplifique o processo de configuração dos utilizadores ao otimizar passos no Assistente de Configuração, garantindo que os funcionários recebem as configurações adequadas imediatamente após a ativação. Agora, as equipas de TI podem personalizar ainda mais esta experiência ao facultarem o texto

de consentimento, a marca da empresa ou um método de autenticação moderno aos funcionários.

- Proporcione um nível mais elevado de controlo para dispositivos que são propriedade da empresa utilizando a supervisão, que oferece controlos de gestão de dispositivos adicionais que não estão disponíveis para outros modelos de implementação, incluindo a MDM não removível.
- Faça a gestão de servidores de MDM predefinidos mais facilmente configurando um servidor predefinido com base no tipo de dispositivo. E agora, pode utilizar o Apple Configurator 2 para registar manualmente o iPhone, o iPad e a Apple TV, seja qual for o método de aquisição.

Conteúdos

O Apple Business Manager permite que as empresas comprem facilmente conteúdos em volume. Independentemente dos dispositivos utilizados pela sua força de trabalho (iPhone, iPad ou Mac), pode fornecer conteúdos fantásticos e preparados para funcionarem com opções de distribuição flexíveis e seguras.

- Compre apps, livros e apps personalizadas em volume, incluindo apps programadas internamente. Transfira facilmente licenças de apps entre locais e partilhe licenças entre compradores no mesmo local. Consulte uma lista unificada do histórico de compras, incluindo o número atual de licenças utilizadas com a MDM.
- Distribua diretamente apps e livros a dispositivos geridos ou utilizadores autorizados, e controle facilmente que conteúdo foi atribuído a que utilizador ou dispositivo. Com a distribuição gerida, controle o processo de distribuição completo, mantendo a propriedade total das apps. As apps que não forem necessárias para um dispositivo ou um utilizador podem ser revogadas e atribuídas novamente na empresa.
- Utilize várias opções de pagamento, incluindo cartões de crédito e notas de encomenda. As empresas podem adquirir crédito para compras em volume (onde disponível) na Apple ou num Apple Authorized Reseller em quantias específicas da moeda local, que é fornecido eletronicamente ao titular da conta na forma de crédito da loja.
- Distribua uma app por dispositivos ou utilizadores em qualquer país onde a app estiver disponível, para uma distribuição multinacional. Os programadores podem disponibilizar as apps em vários países através do processo de publicação habitual da App Store.

Nota: as compras de livros no Apple Business Manager não estão disponíveis em alguns países ou regiões. Para ver a disponibilidade das funcionalidades e métodos de compra, visite support.apple.com/HT207305.

Pessoas

Com o Apple Business Manager, as empresas podem criar e gerir contas para funcionários que são integradas na infraestrutura existente e fornecer acesso a apps e serviços da Apple, bem como ao Apple Business Manager.

- Crie ID Apple geridos para os funcionários, de forma a que possam colaborar em apps e serviços da Apple, bem como aceder a dados de trabalho em apps geridas que utilizam o iCloud Drive. Estas contas são controladas por cada empresa, de quem são propriedade.
- Tire partido da autenticação federada ao associar o Apple Business Manager ao Azure Active Directory da Microsoft. São criados ID Apple geridos

automaticamente à medida que cada funcionário inicia sessão pela primeira vez com as suas credenciais existentes num dispositivo Apple compatível.

- Utilize ID Apple geridos num dispositivo que é propriedade do funcionário em conjunto com um ID Apple pessoal com as novas funcionalidades de Registo de utilizadores do iOS 13, iPadOS e macOS Catalina. Em alternativa, os ID Apple geridos podem ser utilizados em qualquer dispositivo como o principal (e único) ID Apple. Os ID Apple geridos também podem aceder ao iCloud na internet após o início de sessão inicial num dispositivo Apple.
- Designe outras funções para as equipas de TI na sua empresa para gerir dispositivos, apps e contas com eficácia no Apple Business Manager. Utilize a função Administrador para aceitar termos e condições, se necessário, e transferir facilmente responsabilidades caso um funcionário saia da organização.

Nota: atualmente, o iCloud Drive não está disponível com Registo de utilizadores. O iCloud Drive pode ser utilizado com um ID Apple gerido se este for o único ID Apple do dispositivo.

Saiba mais sobre o Apple Business Manager: apple.com/pt/business/it

Registe-se no Apple Developer Enterprise Program

O Apple Developer Enterprise Program oferece um conjunto completo de ferramentas para programar, testar e distribuir apps aos utilizadores. Pode distribuir apps colocando-as num servidor Web ou utilizando uma solução de MDM. Pode assinar e autenticar os instaladores e apps para Mac com o seu Developer ID para Gatekeeper, que ajuda a proteger o macOS do malware.

Saiba mais sobre o Developer Enterprise Program:

developer.apple.com/programs/enterprise

2. Configurar

Durante a configuração da implementação, é necessário definir políticas da empresa e preparar a solução de gestão de dispositivos móveis para configurar o Mac para os funcionários.

Compreender a segurança do macOS

A segurança e privacidade são fundamentais para a conceção de todo o hardware, software e serviços Apple. Protegemos a privacidade dos nossos clientes com encriptação forte e políticas rigorosas que governam a forma como todos os dados são processados. O fornecimento de uma plataforma informática segura para os dispositivos Apple implica:

- Métodos de prevenção da utilização não autorizada dos dispositivos
- Proteção dos dados inativos, mesmo em caso de perda ou roubo do dispositivo
- Protocolos de rede e encriptação dos dados transmitidos
- Execução segura das apps, sem comprometer a integridade da plataforma

Todos os dispositivos Apple têm várias camadas de segurança, para garantir a proteção dos dados importantes e o acesso seguro aos serviços de rede. O macOS, o iOS e o iPadOS também fornecem proteção através de políticas de código e palavra-passe, que podem ser distribuídas e aplicadas com a MDM. Se um dispositivo Apple cair nas mãos erradas, o utilizador ou o administrador podem utilizar um comando remoto para apagar todas as informações privadas.

A equipa de TI pode utilizar a MDM para implementar várias políticas de proteção dos dispositivos. Pode, por exemplo, utilizar o FileVault e o depósito de chave de recuperação com a MDM, aplicar uma política de palavra-passe ou um bloqueio de proteção de ecrã específico e ativar a firewall integrada.

Saiba mais sobre a segurança da plataforma Apple: apple.com/security

Definir as políticas da empresa

Para desenvolver as políticas empresariais, comece por estabelecer políticas gerais, aplicáveis à maioria dos utilizadores do Mac da empresa. A solução de MDM permite personalizar aspetos específicos para cada utilizador, como contas ou o acesso a determinadas apps. Também pode definir políticas específicas para empresas ou outros grupos mais pequenos de utilizadores, como a implementação de software ou definições num determinado departamento.

Colabore com as equipas internas para atualizar as políticas empresariais existentes, de forma a incorporar a utilização de computadores Mac. Algumas políticas principais são comuns a todas as plataformas, como os requisitos de rotação e complexidade das palavras-passe, limites temporais da proteção de ecrã e utilização aceitável.

Se a política da empresa afetar uma tecnologia específica utilizada noutra plataforma, avalie o problema subjacente e procure reestruturar a política de forma a abranger as tecnologias integradas do macOS. Em vez de forçar todos os computadores a utilizar uma solução específica de outra empresa para encriptar um disco inteiro, pode criar uma política que determine que os dados empresariais devem ser encriptados quando estão inativos, através do FileVault. Se a política exigir um software específico para proteção contra malware, informe as equipas sobre as funcionalidades integradas, como o Gatekeeper, e atualize a política para aceitar a sua utilização.

Configurar definições na MDM

Para permitir a gestão de políticas empresariais e garantir o acesso dos funcionários aos recursos necessários, todos os Mac são registados de forma segura na solução de MDM. As soluções de MDM aplicam as políticas e definições utilizando perfis de configuração. Os perfis de configuração são ficheiros XML criados pela solução de MDM que permitem distribuir definições aos dispositivos. Estes perfis automatizam a configuração de definições, contas, políticas, restrições e credenciais. Podem ser assinados e encriptados para aumentar a segurança dos sistemas.

Após o registo de um dispositivo na MDM, um administrador pode iniciar um comando, consulta ou política de MDM. Com uma ligação à rede, o dispositivo recebe uma notificação enviada pelo serviço de notificações em tempo real da Apple (APN), que lhe permite comunicar diretamente com a solução de MDM através de uma ligação segura, e assim processar a ação do administrador. Uma vez que a comunicação é efetuada apenas entre a solução de MDM e o dispositivo, as APN não transmitem informações confidenciais ou sujeitas a direitos de propriedade. Caso um dispositivo seja removido da gestão, as definições e políticas controladas pelo respetivo perfil de configuração serão removidas. Se necessário, a empresa também pode apagar remotamente os dados do dispositivo.

Muitas empresas unem a solução de MDM aos serviços de diretório existentes. Durante o Registo automatizado de dispositivos, o Assistente de Configuração do macOS pode solicitar que os utilizadores iniciem sessão com as credenciais

do serviço de diretório. Com o macOS Catalina, o Assistente de Configuração pode apresentar a autenticação a partir de fornecedores de identidade na nuvem graças a novas opções de personalização do registo. Quando o dispositivo for atribuído a um utilizador específico, a MDM pode personalizar as configurações e contas para uma pessoa ou um grupo. Por exemplo, a conta individual do Microsoft Exchange de um utilizador pode ser fornecida automaticamente durante o registo. Também é possível utilizar identidades de certificados para tecnologias como 802.1x, VPN e muito mais.

Devido ao controlo proporcionado por estes sistemas, muitas vezes as empresas sentem-se confortáveis ao fornecer ao utilizador o acesso administrativo ao seu Mac, para poder personalizar definições, instalar apps e resolver problemas, tudo sob o controlo das políticas empresariais, aplicado via MDM. Este modelo segue o tipo de privilégios e controlos que os utilizadores têm para o iPhone ou iPad sob gestão.

Saiba mais sobre os perfis de configuração:

support.apple.com/guide/deployment-reference-macos

Preparar o Registo automatizado de dispositivos

O método mais simples para o registo de um dispositivo na MDM é durante a utilização do Assistente de Configuração com as funcionalidades de Registo automatizado de dispositivos do Apple Business Manager. Permite efetuar o registo sem intervenção da equipa de TI e otimizar alguns ecrãs do Assistente de Configuração para acelerar o processo.

Para configurar o Registo automatizado de dispositivos, é necessário associar a solução de MDM à conta do Apple Business Manager utilizando um token seguro. O processo de confirmação em dois passos autoriza a solução de MDM de forma segura. O fornecedor da sua solução de MDM pode fornecer documentação específica sobre a respetiva implementação.

Se os dispositivos pertencerem ou estiverem a ser usados pelos funcionários, o utilizador pode abrir e verificar um único perfil de configuração nas Preferências do Sistema para concluir o registo. Este processo é conhecido como registo na MDM aprovado pelo utilizador. O registo deve ser efetuado através do registo de dispositivos ou do registo na MDM aprovado pelo utilizador, para gerir determinadas definições relacionadas com a segurança, como a Política de extensão Kernel e o Controlo das normas das preferências de privacidade.

Saiba mais sobre o carregamento de extensões de kernel:

support.apple.com/guide/deployment-reference-macos

Saiba mais sobre o Controlo de preferências da política de privacidade:

support.apple.com/guide/mdm

Preparar a distribuição de apps e livros

A Apple oferece programas abrangentes que ajudam as empresas a tirar partido das apps e conteúdos fantásticos disponíveis para o macOS. Com estas capacidades, é possível distribuir aos funcionários apps e livros adquiridos através do Apple Business Manager, assim como apps internas, para que tenham acesso a tudo o que precisam para serem produtivos. A MDM permite também distribuir apps e instalar pacotes para software que não esteja disponível na Mac App Store.

A solução de MDM pode utilizar a distribuição gerida para distribuir apps e livros adquiridos no Apple Business Manager em qualquer país onde estas apps estejam disponíveis. Para ativar a distribuição gerida, em primeiro lugar é necessário associar a solução de MDM à conta do Apple Business Manager através de um token seguro. Após estabelecer ligação à solução de MDM, pode atribuir apps e livros aos utilizadores, mesmo se a App Store estiver desativada nesse dispositivo. Também pode atribuir apps aos dispositivos diretamente, o que torna a implementação significativamente mais simples, uma vez que qualquer utilizador do dispositivo tem acesso às apps.

Saiba mais sobre a compra de conteúdos no Apple Business Manager:
support.apple.com/guide/apple-business-manager

Saiba mais sobre a distribuição de apps e livros:
support.apple.com/guide/apple-business-manager

Preparar conteúdos adicionais

A sua solução de MDM pode ajudar a distribuir pacotes adicionais com conteúdos não provenientes da Mac App Store. Esta é uma abordagem comum para muitos pacotes de software empresariais, como apps personalizadas internas ou apps como Chrome ou Firefox. O software necessário pode ser enviado através deste método e instalado automaticamente após a conclusão do registo. Tipos de letra, scripts e outros elementos podem também ser instalados e executados através de pacotes. Certifique-se de que estes pacotes são devidamente assinados com o seu Developer ID do Developer Enterprise Program.

Saiba mais sobre a instalação de conteúdos adicionais:
support.apple.com/guide/deployment-reference-macos

3. Implementar

O macOS torna fácil implementar dispositivos para funcionários, personalizá-los consoante necessário e começar a utilizá-los sem qualquer intervenção de TI.

Utilizar o Assistente de Configuração

Os funcionários podem usar o utilitário Assistente de Configuração no macOS durante o arranque para definir as preferências de idioma e região e estabelecer ligação a uma rede. Após a ligação à internet, surgem várias janelas do Assistente de Configuração que orientam os utilizadores ao longo dos passos essenciais da configuração de um novo Mac. Os dispositivos registados no Apple Business Manager podem ser registados automaticamente na MDM durante este processo. Os sistemas Mac registados também podem ser configurados para avançar determinados ecrãs, como os Termos e condições, início de sessão com o ID Apple, serviços de localização e muito mais.

A MDM pode então ser utilizada após o Assistente de Configuração para implementar uma variedade de definições aquando da configuração inicial, incluindo definir se um utilizador terá privilégios administrativos totais sobre o computador. Tal como no iPhone e no iPad, isto permite aos utilizadores ter o controlo do dispositivo mantendo a conformidade com as políticas e definições da empresa que são geridas pela MDM. Para permitir que os utilizadores sejam produtivos imediatamente após a conclusão do Assistente de Configuração, apenas as apps e pacotes mais essenciais devem ser descarregados e instalados em segundo plano, sem impedir o funcionário de

iniciar o seu trabalho. As apps maiores podem ser agendadas para download e instalação em segundo plano ou posteriormente pelo utilizador na ferramenta de autoassistência da sua solução de MDM.

Configurar contas empresariais

A MDM pode configurar contas de email ou outras contas de utilizador de forma automática. Consoante o fornecedor da solução de MDM e a sua integração com os sistemas internos, as cargas úteis das contas podem ainda ser pré-preenchidas com um nome de utilizador, endereço de email e identidades dos certificados de autenticação e assinatura.

Permitir a personalização pelos utilizadores

Permitir que os utilizadores personalizem os dispositivos pode aumentar a produtividade, uma vez que os utilizadores podem escolher as apps e os conteúdos mais eficazes para efetuar tarefas e atingir objetivos. E agora, com os ID Apple geridos e o Registo de utilizadores no macOS Catalina, as empresas obtêm novas opções para fornecerem aos utilizadores o acesso a serviços da Apple a partir de um ID Apple pertencente à empresa ou juntamente com um ID Apple pessoal.

ID Apple e ID Apple gerido

Quando os funcionários utilizam um ID Apple para iniciar sessão em serviços da Apple, como FaceTime, iMessage, App Store e iCloud, têm acesso a um vasto conjunto de conteúdos para otimizar as tarefas empresariais, aumentar a produtividade e apoiar a colaboração. Tal como os ID Apple, os ID Apple geridos são utilizados para iniciar sessão num dispositivo pessoal. Também são utilizados para aceder a serviços da Apple, incluindo o iCloud e a colaboração com o iWork e a app Notas, e ao Apple Business Manager. Ao contrário dos ID Apple, os ID Apple geridos são geridos pela sua empresa, de quem são propriedade, para tarefas como a reposição de palavras-passe e a administração com base em funções. Os ID Apple geridos têm determinadas definições restritas.

Os dispositivos registados através do Registo de utilizadores requerem um ID Apple gerido. O Registo de utilizadores permite utilizar um ID Apple pessoal opcional; as outras opções de registo permitem utilizar um ID Apple pessoal ou um ID Apple gerido. Apenas o Registo de utilizadores permite utilizar vários ID Apple.

Para tirarem o máximo partido destes serviços, os utilizadores devem utilizar os seus próprios ID Apple ou os ID Apple geridos que são criados para eles. Os utilizadores que não têm um ID Apple podem criá-lo antes de receber o dispositivo. O Assistente de Configuração permite aos utilizadores criar um ID Apple pessoal, caso não o tenham. Não é necessário ter um cartão de crédito para criar um ID Apple.

Saiba mais sobre ID Apple geridos:

support.apple.com/guide/deployment-reference-macos

iCloud

O iCloud permite aos utilizadores sincronizar automaticamente documentos e conteúdos pessoais, como contactos, calendários, documentos e fotografias, e mantê-los atualizados em vários dispositivos. A funcionalidade Encontrar permite aos utilizadores localizar um Mac, iPhone, iPad ou iPod touch, em caso de perda ou roubo. Componentes específicos do iPhone, como o Porta-chaves iCloud e o iCloud Drive, podem ser desativados através de restrições introduzidas manualmente no dispositivo ou definidas via MDM. Esta opção oferece às empresas mais controlo sobre os dados que são armazenados em cada conta.

Saiba mais sobre a gestão do iCloud:

support.apple.com/guide/deployment-reference-macos

4. Gerir

Assim que os utilizadores começarem a usar os dispositivos, está disponível uma ampla variedade de capacidades administrativas para gerir os dispositivos e conteúdos ao longo do tempo.

Administrar os dispositivos

As soluções de MDM podem administrar um dispositivo gerido através de um conjunto de tarefas específicas. Entre outras ações, pode ser efetuada a consulta de dispositivos para obter informações e podem ser executadas tarefas que permitem gerir dispositivos perdidos, roubados ou não abrangidos pela política da instituição.

Consultas

Uma solução de MDM pode consultar dispositivos relativamente a uma variedade de informações para ajudar a garantir que os utilizadores mantêm o conjunto de apps e definições adequado. As consultas podem ser relativas a hardware, como o número de série ou modelo do dispositivo, ou a software, como a versão do macOS ou a lista de apps instaladas. Além disso, a MDM pode consultar o estado das principais funcionalidades de segurança, como o FileVault ou a firewall integrada.

Tarefas de gestão

Quando um dispositivo é gerido, a solução de MDM pode realizar uma grande variedade de tarefas administrativas, incluindo alterar definições de configuração automaticamente, sem interação do utilizador, realizar uma atualização do macOS, bloquear ou apagar um dispositivo remotamente, ou gerir palavras-passe.

Saiba mais sobre tarefas de gestão:

support.apple.com/guide/deployment-reference-macos

Gerir atualizações de software

A equipa de TI pode oferecer aos utilizadores a oportunidade de atualizarem para o sistema operativo mais recente assim que estiver disponível. Ao testar a versão de pré-lançamento do macOS, a equipa de TI pode identificar os problemas de compatibilidade das apps numa fase inicial e contactar os programadores antes do lançamento final. A equipa de TI pode participar no teste de cada lançamento através do Apple Beta Software Program ou do AppleSeed destinado a profissionais de TI. Adote uma abordagem abrangente para manter os computadores Mac atualizados de forma a proteger os utilizadores e os seus dados. Atualize frequentemente, assim que determinar que o seu processo de trabalho é compatível com uma nova versão do macOS.

A MDM pode enviar atualizações do macOS automaticamente para um Mac registado. Um Mac registado pode também ser configurado para adiar atualizações e notificações de atualizações até 90 dias caso os sistemas críticos não estejam preparados. Os utilizadores não vão poder iniciar atualizações manualmente até que a política seja removida ou a MDM envie um comando de instalação.

A Apple não recomenda nem suporta imagens monolíticas de sistema para atualizações do macOS. À semelhança do iPhone e iPad, é frequente os

computadores Mac contarem com atualizações de firmware específicas do seu modelo. Do mesmo modo, as atualizações do sistema operativo Mac obrigam a que estas atualizações de firmware sejam instaladas diretamente da Apple. A estratégia mais fiável é utilizar o macOS Installer ou comandos da MDM para atualizar.

Gerir software adicional

É frequente as empresas terem necessidade de distribuir apps adicionais aos utilizadores, além do conjunto inicial. Tal pode ser realizado automaticamente pela MDM para apps e atualizações críticas, ou a pedido permitindo que os funcionários solicitem apps através de um portal de autoassistência fornecido pela solução de MDM. Estes portais podem fazer tudo, desde instalar software adquirido na App Store até ao Apple Business Manager ou apps externas à App Store, scripts e outros utilitários.

Embora a maioria do software possa ser instalado automaticamente, determinadas instalações podem requerer a interação do utilizador. Para melhorar a segurança, as apps que requerem extensões do kernel requerem agora o consentimento do utilizador para serem carregadas. Tal é denominado Carregamento de extensões do kernel aprovadas pelo utilizador e pode ser gerido pela MDM.

Manter a segurança dos dispositivos

Além do conjunto inicial de políticas de segurança estabelecidas antes da implementação dos dispositivos, a sua equipa deve monitorizar as máquinas relativamente a conformidade e obter o máximo de comunicações possíveis através da solução de MDM. Tal pode incluir a monitorização da postura de segurança de cada dispositivo ou a recolha de informações sobre a instalação de correções de software. Embora a maioria das empresas esteja confortável com a utilização de ferramentas nativas para encriptar e proteger cada Mac, algumas podem exigir a utilização de serviços de sincronização e partilha de ficheiros ou de ferramentas de prevenção de perda de dados adicionais para evitar a fuga de dados empresariais e fornecer comunicações pormenorizadas sobre quaisquer dados importantes.

A funcionalidade Encontrar Mac do iCloud pode iniciar uma eliminação remota que remove todos os dados e desativa um Mac em caso de perda ou roubo. As equipas de TI também podem efetuar uma eliminação remota via MDM.

Reaprovisionar dispositivos

Um Mac pode facilmente ser reaprovisionado para outro utilizador quando um funcionário deixa a empresa utilizando a Recuperação da Internet e a partilha de recuperação local. Tal permite que os conteúdos do Mac sejam eliminados e que a versão mais recente do sistema operativo seja instalada. Um Mac atribuído a uma MDM específica no Apple Business Manager vai efetuar automaticamente um novo registo na MDM durante o Assistente de Configuração, configurar definições para o novo utilizador, aplicar políticas da empresa e implementar todo o software adequado. Os computadores Mac que não estejam registados podem ser eliminados e reaprovisionados seguindo o mesmo processo, e então registados manualmente.

Opções de assistência

Muitas empresas consideram que os utilizadores do Mac requerem um nível mínimo de assistência por parte da equipa de TI. Para incentivar a autoassistência e melhorar a qualidade da assistência, a maioria das equipas de TI cria ferramentas de autoassistência. Estas incluem páginas de assistência para Mac, fóruns de autoajuda e postos de assistência técnica. As soluções de MDM também podem permitir aos utilizadores realizar tarefas de assistência como instalar ou atualizar software a partir de um portal de autoassistência.

Como melhor prática, as empresas não devem forçar os utilizadores a dependerem totalmente deles próprios para assistência. Em vez disso, adote uma abordagem colaborativa para a resolução de problemas e concentre-se em permitir que os utilizadores solucionem os problemas de forma autónoma antes de contactarem a assistência. Incentive os utilizadores a participarem no processo e a investigarem as questões por eles próprios antes de pedirem ajuda.

A responsabilidade de assistência partilhada permite reduzir o tempo de inatividade dos funcionários, baixar os custos de assistência e ter uma equipa de assistência mais pequena. Para as empresas com mais necessidades, o AppleCare fornece uma variedade de programas e serviços que complementam as estruturas de assistência internas para funcionários e TI.

AppleCare for Enterprise

O AppleCare for Enterprise ajuda as empresas interessadas numa cobertura completa a reduzir a pressão sobre a sua própria assistência técnica, proporcionando uma assistência telefónica permanente para os seus funcionários, com tempos de resposta de 1 hora para assuntos prioritários. O programa fornece cenários de integração ao nível do departamento de TI, incluindo MDM e Active Directory.

AppleCare OS Support

O AppleCare OS Support fornece ao departamento de TI assistência de nível empresarial por telefone e email para a implementação do iOS, iPadOS, macOS e macOS Server. Oferece assistência até 24 horas por dia, 7 dias por semana, e um gestor de conta técnico exclusivo, conforme o nível de assistência adquirido. Com acesso direto a técnicos para obter ajuda relacionada com a integração e migração, e para colocar questões complexas relacionadas com o funcionamento de servidores, o AppleCare OS Support pode aumentar a eficácia do seu departamento de TI na implementação de dispositivos e resolução de problemas.

AppleCare Help Desk Support

O AppleCare Help Desk Support permite-lhe ter acesso telefónico prioritário à equipa de assistência técnica da Apple. Inclui ainda um conjunto de ferramentas de diagnóstico e resolução de problemas de hardware da Apple, que podem ajudar as grandes empresas a gerir os recursos de forma mais eficaz, melhorar o tempo de resposta e reduzir os custos de formação. O AppleCare Help Desk Support cobre um número ilimitado de incidentes de diagnóstico de hardware e software, bem como a deteção e resolução de problemas em dispositivos iOS e iPadOS.

AppleCare e AppleCare+ para Mac

Todos os computadores Mac incluem uma garantia limitada de 1 ano e assistência técnica gratuita por telefone durante 90 dias a partir da data de compra. Esta cobertura de serviço pode ser prolongada até 3 anos a partir da data de compra com o AppleCare+ ou AppleCare Protection Plan. Os funcionários podem contactar a Assistência Apple com questões relacionadas com o hardware ou software. A Apple também fornece cómodas opções de assistência quando os dispositivos necessitam de reparação. Além disso, o AppleCare+ para Mac oferece cobertura para um determinado número de incidentes de danos acidentais, estando cada ocorrência sujeita a uma taxa de serviço.

Saiba mais sobre as opções de assistência AppleCare:

apple.com/pt/support/professional/

Resumo

Estão disponíveis várias opções de implementação e gestão de computadores Mac para toda a empresa ou simplesmente para um grupo de utilizadores. Ao escolher as estratégias mais adequadas para a sua empresa, pode ajudar os funcionários a aumentarem a produtividade e a trabalharem de formas totalmente novas.

Saiba mais sobre as funcionalidades de implementação, gestão e segurança do macOS:

support.apple.com/guide/deployment-reference-macos

Saiba mais sobre as definições de gestão de dispositivos móveis para TI:

support.apple.com/guide/mdm

Saiba mais sobre o Apple Business Manager:

support.apple.com/guide/apple-business-manager

Saiba mais sobre ID Apple geridos para empresas:

apple.com/business/docs/site/

[Overview_of_Managed_Apple_IDs_for_Business.pdf](#)

Saiba mais sobre Apple no trabalho:

www.apple.com/pt/business/

Saiba mais sobre funcionalidades de TI:

www.apple.com/pt/business/it/

Saiba mais sobre a segurança da plataforma Apple:

www.apple.com/security/

Explore os programas AppleCare disponíveis:

www.apple.com/pt/support/professional/

Encontre Formação e Certificação Apple:

training.apple.com

Interaja com os Serviços profissionais da Apple:

consultingservices@apple.com

© 2019 Apple Inc. Todos os direitos reservados. Apple, o logótipo Apple, AirPlay, AirPrint, Apple TV, Bonjour, FaceTime, FileVault, iMessage, iPad, iPhone, iPod touch, iTunes, Mac e macOS são marcas comerciais da Apple Inc., registadas nos EUA e noutros países. Swift é uma marca comercial da Apple Inc. App Store, AppleCare, Apple Books, iCloud, iCloud Drive, iCloud Keychain e iTunes Store são marcas de serviço da Apple Inc., registadas nos EUA e noutros países. IOS é uma marca comercial ou marca comercial registada da Cisco nos EUA e noutros países, e é utilizada sob licença. Outros nomes de produtos e empresas referidos neste documento podem ser marcas comerciais das respetivas empresas. As especificações do produto estão sujeitas a alterações sem aviso prévio. Este material é fornecido apenas para fins informativos. A Apple não assume qualquer responsabilidade pela sua utilização.