Políticas - Apple

- Políticas da Apple
- Apps e perfis
- Quiosque e Tela de Início
- Código de acesso
- Restrições
- Rede
- Atualizações de software
- macOS
- Localização e geocercas
- Contas
- Regras de conformidade

Políticas da Apple

As políticas da Apple definem configurações de gerenciamento que o Cerberus Enterprise aplica aos dispositivos Apple via MDM. Essas configurações são definidas no painel, no editor de políticas da Apple.

Antes de começar

O gerenciamento de dispositivos Apple exige que o Apple Management (APNs) esteja configurado. Se necessário, leia a página Configuração do Apple Management (APNs).

Abrir o Editor de Políticas da Apple

No painel, abra **Políticas** e clique em **Criar nova política da Apple**. Para editar uma política da Apple existente, clique na linha dela na tabela de políticas.

Layout do editor

O Editor de Políticas da Apple é organizado como um conjunto de seções expansíveis. No topo da página, você sempre pode editar:

- **Nome** (obrigatório)
- **Id** (somente leitura)
- **Descrição** (opcional)

Seções da política

As seções abaixo correspondem aos painéis disponíveis no momento no Editor de Política da Apple. Quando você abre uma política salva, as seções com configurações alteradas já estão abertas e as demais permanecem fechadas:

- **Gerenciamento de apps**: configure restrições relacionadas a apps, apps gerenciados e as configurações do app Cerberus Enterprise.

- **Quiosque e Tela de Início**: Modo de App Único, apps permitidos e bloqueados, layout da Tela de Início, web clips, configurações de notificação e mensagem da Tela de Bloqueio.
- **Segurança**: controle recursos como Desbloqueio Automático e desbloqueio biométrico.
- **Configurações de senha**: configure requisitos de senha e regras relacionadas.
- **Multimídia**: permitir/não permitir a câmera e recursos relacionados.
- **Celular**: controla configurações relacionadas a celular (configurações de dados celulares dos apps, eSIM, mudanças de plano) e o APN celular.
- **Rede**: redes Wi-Fi (também 802.1X empresarial), VPNs, certificados, proxy global, DNS criptografado e filtro de conteúdo da web, e restrições de conectividade como AirDrop e Bluetooth.
- **Sistema e interface do usuário**: restringe recursos do sistema como Handoff, o nome do dispositivo e o protetor de tela.
- **Atualizações de software**: exigir uma versão do SO até um prazo e controlar como as atualizações são baixadas e instaladas.
- **macOS**: firewall, Gatekeeper, protetor de tela e bloqueio, armazenamento externo e de rede, Compartilhamento de Tela, permissões de privacidade e itens de login dos Macs.
- **Apps e serviços da Apple**: restringe apps e serviços da Apple como iMessage, Game Center e Buscar.
- **Siri e Apple Intelligence**: restringe Siri, ditado e os recursos do Apple Intelligence.
- **iCloud**: permitir ou não serviços específicos do iCloud (backup, sincronização do chaveiro, retransmissão privada etc.).
- **Localização e geocercas**: áreas onde iPhones e iPads com o app Cerberus Enterprise informam quando entram ou saem, para regras de evento.
- **Contas**: restringir a modificação de contas e configurar contas de Mail, Exchange, Google, calendário, contatos e diretório.
- **Regras de conformidade**: requisitos (senha, versão mínima do SO, supervisão, FileVault) que tornam os dispositivos não conformes, com bloqueio opcional.

> Muitas opções no Editor de Políticas da Apple incluem uma dica que documenta os requisitos e as versões de SO compatíveis.

Salvar, excluir e dispositivos associados

Use **Salvar política** para aplicar suas alterações. O botão fica desativado quando não há edições pendentes ou quando a licença está expirada.

Ao editar uma política existente, a página também mostra a ação **Excluir política**. O editor pode mostrar uma lista de **Dispositivos associados** na parte inferior, para que você veja quantos dispositivos estão usando a política no momento.

Próximas páginas

- Apps & perfis: configure apps instalados e perfis de configuração.
- Quiosque e Tela de Início: Modo de App Único, apps permitidos, layout da Tela de Início e web clips.
- Senha: configure requisitos de senha e opções de segurança relacionadas.
- Restrições: defina recursos permitidos e limitações no nível do SO.
- Rede: redes Wi-Fi, VPNs, certificados e restrições de conectividade.
- Atualizações de software: atualizações de SO obrigatórias e configurações de atualização de software.
- macOS: firewall, Gatekeeper, bloqueio de tela, armazenamento, permissões de privacidade e itens de login dos Macs.
- Localização e geocercas: áreas que iPhones e iPads informam ao entrar e sair, e o que elas precisam para funcionar.
- Contas: contas de mail, Exchange, Google, calendário, contatos e diretório.
- Regras de conformidade: requisitos para os dispositivos e bloqueio de dispositivos não conformes.

Apps e perfis

Esta seção documenta como configurar aplicativos gerenciados e payloads de conta para dispositivos Apple.

Gerenciamento de apps

O painel **Gerenciamento de apps** contém tanto restrições gerais relacionadas a apps quanto uma lista de apps gerenciados.

Restrições gerais de apps

- **Permitir App Clips**
- **Permitir instalação de apps**
- **Permitir remoção de apps**
- **Permitir downloads automáticos de apps**
- **Permitir que apps sejam ocultados**
- **Permitir que apps sejam bloqueados**
- **Permitir compras dentro do app**
- **Permitir alteração do navegador padrão**
- **Permitir confiança em apps empresariais**

Apps gerenciados

Use **Adicionar aplicativo** para adicionar um app à política. Cada app gerenciado é exibido como um cartão. Você pode expandir o cartão para editar suas configurações e remover o app usando a ação de exclusão.

- **App Store ID**: o identificador na App Store do app gerenciado.
- **Bundle ID**: o identificador do bundle do app.
- **Comportamento de instalação**: controla se o app deve permanecer instalado ou se pode ser instalado/removido pelo usuário.
- **Atribuição**: o tipo de licença, escolhido pelo Cerberus para cada dispositivo: uma licença de dispositivo em dispositivos da empresa, uma licença de usuário da Conta Apple Gerenciada em iPhones e iPads pessoais (Registro de Usuário). O campo não pode ser alterado.
- **Licença VPP**: tipo de licença VPP usado para instalação pela App Store.

A lista de seleção de apps mostra as licenças disponíveis e totais de cada app. Apps gratuitos mostram **Ilimitadas**: a Apple concede licenças ilimitadas para eles. Um app pode ser adicionado a uma política apenas uma vez: um app com o mesmo App Store ID ou bundle ID de um app que já está na política é recusado, assim como uma política que lista o mesmo app duas vezes ao ser salva.

A lista de seleção de apps mostra os apps da sua biblioteca do Apple Business. Para adicionar um app, no Apple Business, abra **Apps & Services → Apps & Books → App Store**, pesquise o app e clique em **View**. Para um app gratuito, clique em **Add**, selecione **All current and future** (ou a unidade organizacional do seu token do Apps and Books) em **Organizational Units**, clique em **Add**, depois **Review** e confirme. Para um app pago, clique no preço, escolha **Managed Licenses** como **License Type** (códigos de resgate não podem ser usados pelo Cerberus Enterprise), selecione a **Organizational Unit** do seu token do Apps and Books, informe o número de **Licenses** (até 1.000 por pedido), depois **Review** e compre. Um método de pagamento deve ser configurado primeiro em **Settings → Payments & Billing → Apps & Services → Payment Methods**. Os apps então aparecem na lista de seleção de apps.

Apps em dispositivos pessoais (Registro de Usuário)

iPhones e iPads pessoais registrados com o Registro de Usuário não têm número de série, então recebem os apps da App Store da política com uma **licença de usuário** da Conta Apple Gerenciada conectada no dispositivo. O Cerberus registra a conta no Apps and Books e atribui as licenças por conta própria, incluindo apps gratuitos. As Contas Apple Gerenciadas e o token do Apps and Books devem pertencer à mesma organização do Apple Business. Um app pago usa uma licença por conta, compartilhada por todos os dispositivos pessoais dessa conta.

- **Aguardando uma licença de usuário**: o app só é enviado ao dispositivo depois que a Apple confirma a licença, geralmente em poucos minutos. O painel **Aplicativos** do dispositivo mostra o motivo.
- **Falha na licença de usuário**: a Apple não conseguiu atribuir a licença, por exemplo porque um app pago não tem mais licenças disponíveis. Adicione licenças no Apple Business e use **Solicitar novamente**; o Cerberus também tenta novamente sozinho todos os dias.
- **Solicitação de instalação**: o iOS pergunta ao usuário antes de instalar cada app. Se o usuário cancelar, o app mostra **Aguardando o usuário aprovar a instalação**; **Solicitar novamente** exibe a solicitação de novo.
- **Liberação**: remover o app da política, ou cancelar o registro do último dispositivo pessoal da conta, remove o app e libera sua licença, a menos que outro dispositivo registrado da mesma conta ainda precise dele.

Para os detalhes, consulte **Registro orientado por conta da Apple**.

Configuração gerenciada

Uma configuração gerenciada fornece a um app suas configurações (por exemplo, um endereço de servidor ou um nome de conta), da forma como o fornecedor do app as documenta. Abra o app na política e clique em **Adicionar configuração gerenciada**. Ela é enviada a iPhones e iPads com **iOS ou iPadOS 18.4 ou posterior** e a Macs com **macOS 27 ou posterior**; ainda não é enviada ao Apple Vision Pro. O app precisa oferecer suporte a configuração gerenciada: um app que não a lê a ignora. O painel do app mostra o número de chaves ao lado do nome do app.

- **Chaves**: cada linha tem uma chave, um tipo e um valor. Os tipos são Texto, Inteiro, Número decimal, Booleano, Data, Lista de texto e Lista de inteiros. As chaves diferenciam maiúsculas de minúsculas e devem ser exclusivas. **Adicionar chave** adiciona uma linha; **Remover configuração** remove todas as chaves.
- **Variáveis**: valores de Texto e Lista de texto podem conter $EMAIL$, $USERNAME$, $FULLNAME$, $SERIAL$ e $UDID$, substituídos pelos valores de cada dispositivo e do seu usuário. Uma variável sem valor (por exemplo, $EMAIL$ em um dispositivo sem usuário) é deixada vazia, e os logs do sistema registram isso. Quando os dados de um usuário mudam, os dispositivos recebem os novos valores; para usuários sincronizados do Google Directory, os valores são atualizados na próxima alteração da política ou do dispositivo.
- **Importar uma configuração**: abra ou cole o arquivo que o fornecedor do app publica para MDM e clique em **Ler**. Um **specfile do AppConfig** (specfile.xml) lista todas as chaves compatíveis com o app, com descrição, tipo, valor padrão e valores permitidos: selecione as chaves a importar (aquelas com valor padrão já vêm selecionadas) e preencha as demais após a importação. Um aviso aparece quando o specfile é de outro app. Uma **property list** (uma property list inteira ou apenas seu <dict>) é importada como está. Depois, escolha se deseja substituir as chaves atuais ou adicionar a elas. Dicionários aninhados, valores de dados e listas com tipos mistos ou desconhecidos não são suportados e são listados como ignorados. A Apple não publica as chaves de configuração dos apps, então peça o arquivo ao fornecedor quando ele não estiver na documentação. **Copiar como plist** copia a configuração conforme o dispositivo a recebe, antes da substituição das variáveis.
- **Limites**: até 200 chaves por app; chaves de até 255 caracteres; valores de texto de até 4.096 caracteres; listas de até 200 itens de até 1.024 caracteres cada; datas entre 1970 e 9999; 64 KB por app no total.
- **Não use para senhas**: a configuração é enviada apenas ao dispositivo para o qual foi criada e os logs mostram apenas nomes e tipos de chaves, mas os administradores do painel podem ler os valores, e o endereço do qual o dispositivo a baixa muda com os valores, então um valor fácil de adivinhar (um booleano ou um número pequeno) pode ser inferido a partir dele. Não coloque senhas ou outros segredos em uma configuração gerenciada.
- **Status**: quando o dispositivo informa que o app não aceitou sua configuração, o painel Aplicativos do dispositivo mostra **Configuração não aceita** ao lado do app. Isso não torna o dispositivo não conforme. Uma configuração que o dispositivo não consegue baixar torna o dispositivo não conforme.

Opções de apps

Cada app da política (da App Store e apps personalizados) tem estas opções. **Padrão do dispositivo** deixa a escolha para o dispositivo. Dispositivos que não suportam uma opção não a recebem; o app ainda é instalado.

- **Atualizações automáticas**: configuração da App Store, Sempre ou Nunca. iOS, iPadOS, macOS e visionOS 26 ou posterior. Para apps personalizados, a configuração da App Store se comporta como Nunca.
- **Downloads via celular**: configuração da App Store, Sempre ou Nunca, para instalações e atualizações automáticas. Somente iPhones e iPads supervisionados com iOS ou iPadOS 26 ou posterior.
- **Fazer backup dos dados do app**: se os dados do app são incluídos nos backups do dispositivo. Não no Mac.
- **O usuário pode ocultar o app** e **O usuário pode bloquear o app**: iOS e iPadOS 18.1 ou posterior, aplicado em dispositivos supervisionados. Não permitir o bloqueio também impede o ocultamento. As restrições **Permitir que apps sejam ocultados** e **Permitir que apps sejam bloqueados** se aplicam a todos os apps.
- **Bloquear o dispositivo após transações Tap to Pay que exigem o PIN do cliente**: somente iPhone.
- **Domínios associados**: os domínios aos quais o app está associado (por exemplo, para links universais ou preenchimento automático de senhas), até 50. Informe nomes de host simples como www.example.com, sem applinks:, curingas ou ?mode=. Não no Mac.
- **Verificar os domínios diretamente**: o dispositivo verifica o arquivo de associação de site dos domínios diretamente, em vez de pelos servidores da Apple. Ative apenas para domínios internos que não podem ser acessados pela internet.
- **Remoção**: apps instalados como **Obrigatório** não podem ser removidos pelo usuário.

Apps da Mac App Store

A lista de seleção de apps mostra as plataformas de cada app (iPhone/iPad, Mac, Apple TV, Vision); um app que existe apenas para Mac mostra seu ícone de Mac. Um app que existe apenas para Mac se aplica a Macs quando você o adiciona. Um app da App Store sem versão para Mac não é enviado a Macs: a política mostra "Este app não tem versão para Mac: ele não é enviado a Macs" em **Aplica-se a**. Os Macs recebem apps da App Store pelo App Store ID, então apps com um bundle ID diferente no Mac são instalados corretamente.

App Cerberus Enterprise

O Cerberus instala seu app **Cerberus Enterprise** em todos os iPhones e iPads com **iOS ou iPadOS 18.4 ou posterior**, com ou sem política. O app compartilha a localização do dispositivo e recebe notificações e solicitações de rastreamento ao vivo. Ele é instalado como **Obrigatório**, com

uma licença de dispositivo do Apps and Books (uma licença de usuário em dispositivos pessoais), então o usuário não pode excluí-lo.

- **Configuração única**: adicione o app gratuito à sua biblioteca uma vez. No Apple Business, abra **Apps & Services** → **Apps & Books** → **App Store**, pesquise por "Cerberus Enterprise", clique em **View**, depois **Add**, selecione **All current and future** em **Organizational Units**, clique em **Add**, depois **Review** e confirme. Se o app mostrar **Manage**, ele já está na sua biblioteca: abra-o e verifique se suas unidades organizacionais são **All current and future units**. Até lá, o painel mostra um banner e os dispositivos mostram o app como não instalado. Consulte **Account settings**.
- **Não disponível em políticas**: o app não pode ser adicionado a uma política. Ele fica desativado na lista de seleção de apps e é recusado como app personalizado (mesmo bundle ID). Uma política que já o lista tem a entrada removida quando você a abre: salve a política para confirmar.
- **Não instalado em**: dispositivos com iOS ou iPadOS anterior ao 18.4. O iPad Compartilhado é compatível com a instalação, mas os recursos do app não são verificados nele.
- **Dispositivos pessoais**: em iPhones e iPads registrados com User Enrollment, o app também é instalado, com um aviso de instalação e uma licença de usuário da Conta Apple Gerenciada. Ele recebe mensagens da sua organização e não acessa a localização, a menos que a política ative **Localização e geocercas em dispositivos pessoais** e o usuário permita.
- **Mantido instalado**: se o token do Apps and Books expirar ou o app sair da sua biblioteca, o app permanece nos dispositivos e a página do dispositivo informa que o Apps and Books precisa de atenção. Ele só é removido se o app ainda estiver ausente da sua biblioteca 24 horas depois.

Apps personalizados

Apps personalizados são os seus próprios apps para iPhone e iPad (arquivos .ipa), distribuídos sem a App Store. No Xcode, exporte o app para distribuição **Enterprise** (Apple Developer Enterprise Program: ele é instalado em todos os dispositivos) ou distribuição **Ad Hoc** (ele é instalado apenas nos dispositivos registrados no seu perfil de provisionamento). Builds da App Store não podem ser enviados.

Clique em **Adicionar app personalizado** para abrir os apps personalizados da sua organização. **Enviar app** adiciona um arquivo .ipa (até 2 GB). Selecione um app e clique em **Adicionar à política**. A lista mostra a versão, o tipo de assinatura, o número de dispositivos no perfil de apps ad hoc e a data de expiração do perfil de provisionamento.

- **Nova versão**: envie um app com o mesmo bundle ID. Ele substitui a versão anterior, e os dispositivos das políticas que o usam atualizam o app.
- **Requisitos**: iPhone e iPad com iOS 17.2 ou posterior. Dispositivos que não podem instalar o app não o recebem: um app exclusivo para iPad em um iPhone, um iOS mais antigo do que o app exige, um dispositivo que não está no perfil de um app ad hoc ou um perfil de

provisionamento expirado.
- **Expiração**: quando o perfil de provisionamento expira, o app deixa de abrir. Envie uma versão assinada com um novo perfil antes da data de expiração.
- **Bundle ID reservado**: um app personalizado com o bundle ID do app Cerberus Enterprise (com.lsdroid.Cerberus.Enterprise) não pode ser adicionado a uma política, porque o Cerberus instala esse app por conta própria.
- **Excluir**: remova o app das políticas dele primeiro; depois, os dispositivos o removem.

Pacotes do Mac

Os apps personalizados também aceitam pacotes de instalação do Mac (arquivos .pkg). O pacote deve ser um pacote de distribuição criado com **productbuild** (um pacote de componente criado apenas com pkgbuild é recusado) e assinado com um certificado **Developer ID Installer**. Recomenda-se notarizá-lo e grampear o tíquete (**notarytool** e **stapler**). Pacotes não assinados, pacotes alterados depois da assinatura e pacotes assinados com outros certificados são recusados.

Envie o arquivo .pkg com **Upload app** e adicione-o à política: ele aparece em **Pacotes do Mac**. iPhones e iPads o ignoram.

Macs com **macOS 26 ou posterior** (supervisionados, o que inclui Macs registrados manualmente, mas não o Registro do Usuário) recebem o pacote como uma **declaração**: o Mac baixa, instala, tenta novamente e atualiza o pacote sozinho e informa o estado. Macs mais antigos, e pacotes instalados como apps gerenciados, o recebem com um **comando MDM**, em qualquer versão do macOS. Um Mac atualizado para o macOS 26 passa para a declaração sozinho; ele pode instalar cada pacote mais uma vez. O mesmo pode acontecer quando um Mac passa para outra política que tem o mesmo pacote.

- **Nova versão**: envie um pacote com o mesmo identificador de pacote. Ela substitui a versão anterior, e os Macs das políticas que a usam instalam a nova.
- **Macs ignorados**: Macs com um macOS mais antigo do que o permitido pelo pacote, e Macs Intel para pacotes criados apenas para Apple silicon. A página do dispositivo mostra o pacote como Ignorado, com o motivo; a versão instalada antes permanece no Mac.
- **Instalação**: **Obrigatório** (padrão) instala o pacote no Mac; **Opcional** deixa o pacote disponível no Mac sem instalá-lo. O macOS 26 não mostra pacotes opcionais ao usuário em Ajustes do Sistema nem na App Store (testado no macOS 26.3), então um app ou um script no Mac precisa instalá-los; escolha Opcional apenas se você tiver um. A opção se aplica a Macs com macOS 26 ou posterior; Macs mais antigos sempre instalam o pacote. A escolha não está disponível para pacotes instalados como apps gerenciados.
- **Remover os arquivos do pacote quando ele sai da política (macOS 27 ou posterior)**: quando o pacote é removido da política, Macs com macOS 27 ou posterior excluem os arquivos que ele instalou. Fica desativado por padrão. Em Macs mais antigos, os arquivos permanecem. Não disponível para pacotes instalados como apps gerenciados.
- **Instalar como app gerenciado**: ative esta opção para um pacote da política instalar o app dele como app gerenciado (macOS 11 ou posterior, não com registro do usuário). O

macOS então informa quando a instalação falha, e o MDM pode remover o app. O app deve ser instalado diretamente na pasta Aplicativos, assinado com um certificado **Developer ID Application** e notarizado; no macOS 11 a 13, o pacote deve conter apenas esse app (nenhum outro arquivo ou script). Os apps personalizados mostram quais pacotes são elegíveis. Quando a opção não pode ser aplicada em um Mac, o pacote é instalado lá como de costume e a página do dispositivo explica o motivo.

- **Opções de remoção** de um app gerenciado: **Remover o app quando o pacote for removido da política** (ativado por padrão) e **Remover o app quando o Mac sair do gerenciamento**. Remover um app também exclui os dados dele. Se o usuário já tiver instalado o mesmo app, essa cópia passa a ser gerenciada e também é removida.
- **Remoção**: o comando MDM não pode desinstalar um pacote. Para um pacote instalado como app gerenciado, removê-lo da política remove o app (quando a opção está ativada); os outros arquivos dele e o recibo do pacote permanecem. Pacotes com **Remover os arquivos do pacote** ativado são removidos de Macs com macOS 27 ou posterior. Outros pacotes: removê-los da política apenas interrompe novas instalações, os arquivos permanecem nos Macs. Um Mac ignorado (por exemplo, após uma nova versão que exige um macOS mais recente) mantém o app enquanto o pacote estiver na política; remover o pacote da política então também o remove. Remova os arquivos restantes no Mac (por exemplo, com o próprio desinstalador do pacote) e execute `sudo pkgutil --forget <identifier>` para esquecer o recibo do pacote.
- **Estado no dispositivo**: o painel Aplicativos do Mac mostra cada pacote da política como Na fila, Aceito (o Mac aceitou o comando), Baixado, Instalado (somente para pacotes que contêm apps, quando os apps são encontrados no Mac) ou Falhou (com o erro). O macOS não informa a instalação de um pacote enviado com o comando, então Baixado é o último estado para pacotes sem apps. Um pacote instalado como app gerenciado também passa a Falhou quando o macOS informa que o app não pôde ser instalado ou foi removido do Mac. **Instalar novamente** envia o pacote ao Mac outra vez.
- **Estado com a declaração**: pacotes entregues como uma declaração mostram o chip **Declaração** e o estado informado pelo Mac: Na fila, Disponível (um pacote opcional que o usuário não instalou), Aguardando o usuário, Baixando, Instalando, Instalado ou Falhou (com o motivo, por exemplo um download ou uma instalação com falha, ou uma declaração que o Mac rejeitou). O chip **Arquivos removidos com a política** marca os pacotes cujos arquivos um Mac com macOS 27 remove quando eles saem da política. **Instalar novamente** aparece apenas após uma falha e pede que o Mac tente de novo; ele não é oferecido quando o Mac rejeitou a declaração.

Contas

O painel **Contas** permite configurar contas que são aplicadas a dispositivos gerenciados. Ele também inclui um alternador de restrição para modificação de contas.

Restrição

- **Permitir modificação de contas**: quando desativado, os usuários não podem modificar contas como Contas Apple e contas de internet.

Adicionar contas

Use **Adicionar conta do Google** ou **Adicionar conta de e-mail** para adicionar payloads de conta à política. Cada conta aparece como um cartão com os campos de configuração.

Credenciais de conta dos usuários

Os cartões de conta do Google e de e-mail oferecem um alternador **Credenciais de conta dos usuários**. Quando ativado, o sistema aplica as credenciais de conta por usuário. Quando desativado, você insere a identidade da conta na política.

Campos da conta do Google

- **Nome visível**: o nome mostrado ao usuário para a conta.
- **Endereço de e-mail do Google**: o endereço de e-mail do usuário.
- **Nome completo**: o nome completo do usuário.

Campos da conta de e-mail

As contas de e-mail incluem campos de identidade e a configuração dos servidores de entrada e saída. Os nomes de host são obrigatórios.

- **Nome visível**: o nome mostrado ao usuário para a conta de e-mail.
- **Endereço de e-mail**: o endereço de e-mail do usuário.
- **Nome completo**: o nome completo do usuário.

Servidor de entrada

- **Tipo de servidor**: protocolo de e-mail (por exemplo, IMAP ou POP).
- **Método de autenticação**: método de autenticação do servidor.
- **Prefixo de caminho IMAP**: mostrado somente quando o Tipo de servidor é IMAP.
- **Nome do host**: obrigatório.
- **Porta**: porta do servidor (1–65535).

Servidor de saída

- **Método de autenticação**
- **Nome do host**: obrigatório.

- **Porta**: porta do servidor (1–65535).

Opções de S/MIME

Para contas de e-mail, você também pode configurar o comportamento de criptografia e assinatura S/MIME.

Criptografia

- **Criptografia S/MIME**
- **Identidade substituível pelo usuário**
- **Alternador por mensagem ativado**
- **Substituível pelo usuário**

Assinatura

- **Assinatura S/MIME**
- **Identidade substituível pelo usuário**
- **Substituível pelo usuário**

> As opções de conta e restrição incluem dicas no painel que documentam os pré-requisitos e as versões de sistema operacional suportadas.

Quiosque e Tela de Início

A seção **Quiosque e Tela de Início** do Editor de Política da Apple bloqueia os dispositivos em um app, escolhe quais apps podem ser abertos, organiza a Tela de Início e adiciona ícones de sites. Cada configuração é instalada nos dispositivos como um perfil de configuração.

> A Apple aplica a maioria dessas configurações somente a iPhone e iPad supervisionados (dispositivos registrados com Automated Device Enrollment ou preparados com o Apple Configurator). Outros dispositivos não as recebem. Os clipes da web também funcionam em iPhone e iPad não supervisionados. Macs não recebem nenhuma dessas configurações.

Escolher apps

Os apps são identificados pelo ID do pacote. Digite o nome de um app para escolhê-lo entre os apps integrados da Apple e os apps da política, ou digite qualquer ID de pacote, por exemplo `com.example.app`.

Modo de App Único

O dispositivo executa somente o app escolhido: os usuários não podem voltar à Tela de Início nem abrir outros apps. Instale o app com a política primeiro. O dispositivo sai do Modo de App Único quando você desativa a configuração ou remove o app.

- **Opções**: desative a tela de toque, a rotação, os botões de volume, a chave Silencioso/Toque, o botão lateral ou o Bloqueio Automático, e ative recursos de acessibilidade como VoiceOver ou Zoom.
- **Recursos de acessibilidade que o usuário pode ativar**: recursos que o usuário pode ativar com um clique triplo no botão lateral.

Apps permitidos e bloqueados

- **Apps bloqueados**: os dispositivos ocultam esses apps e não os abrem. `com.apple.webapp` bloqueia todos os web clips. Ajustes e, no iPhone, Telefone não podem ser bloqueados.
- **Permitir somente alguns apps**: os dispositivos mostram somente esses apps. Deixe a lista vazia para permitir todos os apps. **Apps da política** adiciona os apps instalados pela

política; `com.apple.webapp` permite todos os clipes da web.
- **Apps que podem iniciar o Modo de App Único**: apps que podem bloquear o dispositivo neles mesmos enquanto precisam, por exemplo durante uma prova.

> Com **Permitir apenas alguns apps**, todo app que não estiver na lista desaparece dos dispositivos, incluindo os apps da política. Ajustes e, no iPhone, Telefone sempre permanecem.

Layout da Tela de Início

Organize o Dock e as páginas da Tela de Início. Adicione apps, pastas de apps e os clipes da web da política, escolhendo onde com **Adicionar a**, e arraste os ícones para movê-los entre o Dock e as páginas. Clique em uma pasta para alterar o nome e os apps dela.

Os usuários não podem mover os ícones nem remover apps da Tela de Início. Apps que não estão no layout vão para as páginas após as que você definiu. Um iPhone mostra quatro ícones no Dock. Os usuários ainda podem excluir apps que não sejam Obrigatórios na tela de armazenamento dos Ajustes. Para impedir isso, desative **Permitir remoção de apps** em Gerenciamento de apps.

Clipes da web

Um clipe da web é um ícone na Tela de Início que abre um site. Defina o rótulo e a URL, e opcionalmente uma imagem (PNG ou JPEG, cortada em um quadrado).

- **Os usuários podem removê-lo**: desative para manter o ícone nos dispositivos.
- **Tela cheia**: o site abre como um web app, sem a barra de endereço do Safari. **Permanecer em tela cheia em outros sites** também abre os links para outros sites no web app.
- **Abrir com este app**: um app que abre a URL em vez do Safari.

Configurações de notificações

Escolha como os dispositivos mostram as notificações de alguns apps: se são permitidas, onde aparecem (Tela Bloqueada, Central de Notificações, CarPlay), badges, sons, alertas críticos, estilo de banner, agrupamento e prévias. Os usuários não podem alterar essas configurações.

Mensagem da Tela Bloqueada

Uma mensagem mostrada na parte inferior da Tela Bloqueada, por exemplo quem chamar se o dispositivo for encontrado, e uma etiqueta de patrimônio. Ambas podem conter as variáveis $EMAIL$, $USERNAME$, $FULLNAME$, $SERIAL$ e $UDID$: uma variável sem valor para o dispositivo fica vazia.

Código de acesso

A seção **Configurações de código de acesso** controla os requisitos de código de acesso do dispositivo e as regras de segurança relacionadas (por exemplo, comprimento mínimo e complexidade). Em um Mac (macOS 13 ou posterior, não com o Registro de Usuário), as regras se aplicam à senha de login dos usuários.

Opções

No Editor de Política da Apple, as opções de código de acesso são configuradas com uma combinação de alternadores e campos numéricos. Muitos campos incluem dicas que indicam as versões de SO suportadas e os requisitos de supervisão.

Alternadores de código de acesso

- **Alterar na próxima autenticação**: força a redefinição do código de acesso na próxima vez que o usuário se autenticar.
- **Exigir código de acesso alfanumérico**: exige pelo menos um caractere alfabético e um número.
- **Exigir código de acesso complexo**: exige um código de acesso “complexo” (sem padrões repetidos/sequenciais e pelo menos um caractere não alfanumérico).
- **Exigir código de acesso**: exige um código de acesso sem requisitos adicionais de comprimento/qualidade. Observação: definir outras chaves de código de acesso implicitamente exige um código de acesso.

Campos numéricos

- **Redefinição de tentativas com falha (minutos)**: minutos antes de o contador de tentativas com falha ser redefinido (requer Máximo de tentativas com falha).
- **Máximo de tentativas com falha**: tentativas com falha permitidas antes de um iPhone ou iPad ser apagado, ou um Mac ser bloqueado (intervalo: 2–11).
- **Período de carência máximo (minutos)**: por quanto tempo o dispositivo pode ficar desbloqueado sem exigir o código de acesso (0 = nenhum).
- **Inatividade máxima (minutos)**: tempo ocioso antes de o dispositivo ser bloqueado (intervalo: 0–15).
- **Idade máxima do código de acesso (dias)**: idade máxima do código de acesso antes de uma alteração forçada (intervalo: 0–730).

- **Mínimo de caracteres complexos**: número mínimo de caracteres “complexos” (intervalo: 0–4).
- **Comprimento mínimo**: comprimento mínimo do código de acesso (intervalo: 0–16).
- **Limite de reutilização de código de acesso**: tamanho do histórico de códigos de acesso para impedir a reutilização de códigos antigos (intervalo: 1–50).

Restrições

As seções Restrições controlam quais recursos do SO são permitidos em dispositivos Apple gerenciados. No Editor de Política da Apple, essas opções são exibidas como painéis agrupados com vários alternadores.

Os alternadores dos painéis **Gerenciamento de apps** e **Rede** são descritos nas páginas Apps e perfis e Rede das políticas Apple.

> Muitas restrições são suportadas somente em versões específicas do SO e podem exigir dispositivos supervisionados. Use as dicas no painel para obter os requisitos oficiais.

> Em dispositivos com Registro do Usuário (dispositivos pessoais registrados ao entrar com uma conta de trabalho), as restrições que a Apple não permite neles não são enviadas. Se nenhuma das restrições da política se aplicar, esses dispositivos não recebem perfil de restrições. O editor de política mostra quantas restrições não se aplicam a dispositivos com Registro do Usuário.

Segurança

- **Permitir desbloqueio automático**
- **Permitir impressão digital para desbloquear**
- **Permitir modificação da impressão digital**
- **Permitir apagar conteúdo e ajustes**
- **Permitir ativação de restrições**
- **Permitir instalação de perfis pelos usuários**
- **Permitir emparelhamento com host**
- **Permitir envio de diagnósticos**
- **Permitir alteração do envio de diagnósticos**
- **Permitir publicidade personalizada da Apple**
- **Permitir alteração do Gerenciamento Remoto**

Multimídia

- **Permitir câmera**
- **Permitir modificação do Compartilhamento de Arquivos**
- **Permitir acesso a unidades USB no app Arquivos**
- **Permitir gravação de chamadas**
- **Permitir AirPrint**
- **Permitir armazenamento de credenciais do AirPrint**
- **Permitir descoberta de iBeacon para AirPrint**

Celular

- **Permitir modificação de dados celulares por app**
- **Permitir modificação de plano celular**
- **Permitir modificação do eSIM**
- **Permitir transferências de saída do eSIM**
- **Manter o eSIM quando o dispositivo for apagado**
- **Permitir busca em segundo plano durante roaming**

APN de celular

APN de celular define o nome do ponto de acesso (APN) que sua operadora forneceu, por exemplo para uma rede móvel privada ou corporativa. Defina o **nome do ponto de acesso** e, se a operadora pedir, a autenticação (PAP ou CHAP), o nome de usuário (variáveis como $EMAIL$ são permitidas), a senha, as versões de IP (também em roaming), um servidor proxy com a porta e o XLAT464. Ative **APN de conexão** somente se a operadora fornecer um APN separado para conectar à rede.

- Somente iPhone e iPad com celular o recebem, também sem supervisão. Dispositivos registrados com o Registro do Usuário (dispositivos pessoais) não o recebem.
- Ele se aplica somente ao SIM usado para dados celulares. Um dispositivo que já tem um perfil de APN instalado de outra forma não o instala.
- A senha é protegida como as outras senhas de rede: o perfil é enviado somente ao dispositivo para o qual foi criado e a senha não é gravada nos registros.

> Um APN errado deixa os dispositivos sem dados celulares: teste as configurações em um dispositivo de teste com um SIM da operadora primeiro.

Sistema e interface do usuário

- **Permitir Handoff**
- **Permitir correção automática**
- **Permitir escurecimento automático**
- **Permitir protetor de tela automático**
- **Permitir teclado QuickPath**
- **Permitir consulta de definições**
- **Permitir alteração do nome do dispositivo**
- **Permitir repouso do dispositivo**
- **Permitir Espelhamento do iPhone**
- **Permitir widgets do iPhone no Mac**
- **Permitir atalhos de teclado**

Apps e serviços da Apple

- **Permitir iMessage**
- **Permitir Game Center**
- **Permitir adicionar amigos no Game Center**
- **Permitir Buscar dispositivo**
- **Permitir Buscar amigos**
- **Permitir alteração de Buscar amigos**
- **Permitir Livraria**
- **Permitir conteúdo erótico da Livraria**
- **Permitir backup de livros corporativos**
- **Permitir sincronização de metadados de livros corporativos**
- **Permitir iTunes Store**
- **Permitir conteúdo explícito**

Siri e Apple Intelligence

- **Permitir Siri**
- **Permitir conteúdo gerado pelo usuário no Siri**
- **Permitir Siri com o dispositivo bloqueado**
- **Permitir ditado**
- **Permitir integrações de inteligência externas**
- **Permitir login em inteligência externa**
- **Permitir Genmoji**
- **Permitir Image Playground**
- **Permitir Image Wand**

iCloud

- **Permitir catálogo de endereços do iCloud**
- **Permitir backup do iCloud**
- **Permitir favoritos do iCloud**
- **Permitir calendário do iCloud**
- **Permitir Área de Trabalho e Documentos do iCloud**
- **Permitir sincronização de documentos do iCloud**
- **Permitir Freeform do iCloud**
- **Permitir sincronização do chaveiro do iCloud**
- **Permitir Mail do iCloud**
- **Permitir Notas do iCloud**
- **Permitir Biblioteca de Fotos do iCloud**
- **Permitir Retransmissão Privada do iCloud**
- **Permitir Lembretes do iCloud**

Contas (restrição)

O painel Contas contém tanto uma restrição quanto (opcionalmente) a configuração de contas. O botão de restrição controla se o usuário pode modificar as contas do sistema.

- **Permitir modificação de conta**

Rede

A seção **Rede** do Editor de Política da Apple configura redes Wi-Fi e VPNs nos dispositivos, instala certificados e restringe recursos de conectividade como AirDrop e Bluetooth. Cada rede Wi-Fi, VPN e certificado é instalado como seu próprio perfil de configuração, que você pode ver no dispositivo em **Configurações > Geral > VPN & Gerenciamento de Dispositivos** (Mac: **Ajustes do Sistema > Geral > Gerenciamento de Dispositivos**, ou **Privacidade e Segurança > Perfis** no macOS 13 e 14) e no painel **Perfis, certificados e segurança** da página do dispositivo.

> Os certificados são obtidos na página **Certificados**: importe-os lá primeiro. A política apenas se refere a eles, então um certificado nunca é copiado na política.

Restrições

- **Permitir AirDrop**
- **Permitir solicitações recebidas do AirPlay**
- **Permitir modificação do Bluetooth**
- **Permitir modificação do Compartilhamento Bluetooth**
- **Permitir acesso a unidades de rede no app Arquivos**
- **Permitir modificação do Compartilhamento de Internet**
- **Permitir cache de conteúdo**
- **Permitir compartilhamento de arquivos do iTunes**

Redes Wi-Fi

Clique em **Adicionar rede Wi-Fi** e preencha:

- **Nome da rede (SSID)**: o nome da rede, com até 32 caracteres.
- **Segurança**: nenhuma (rede aberta), WEP, WPA ou WPA2, WPA2 ou WPA3, somente WPA3, ou qualquer uma.
- **Senha**: a senha de uma rede pessoal.
- **Entrar automaticamente** e **Rede oculta** (para redes que não transmitem o nome).
- **Proxy**: nenhum, manual (servidor e porta) ou automático (uma URL de arquivo PAC, ou vazio para encontrar as configurações na rede com WPAD).
- **Nome do perfil** (opcional) e **Aplica-se a**, para limitar a rede a alguns tipos de dispositivo.

Redes corporativas (802.1X)

Ative **Corporativa (802.1X)** quando os usuários se autenticam com as próprias credenciais ou um certificado em vez de uma senha compartilhada.

- **Autenticação**: PEAP, TTLS (com a autenticação interna dele, por exemplo MSCHAPv2) ou TLS (somente certificado).
- **Credenciais do usuário do dispositivo**: cada dispositivo usa a identidade EAP, a identidade anônima e a senha do usuário dele, definidas na página Usuários. Dispositivos sem um usuário não recebem a rede.
- **Identidade**, **Identidade anônima** e **Senha**: iguais para todos os dispositivos. A identidade pode conter as variáveis $EMAIL$, $USERNAME$, $FULLNAME$, $SERIAL$ e $UDID$. Deixe a senha vazia para permitir que o usuário a digite no dispositivo.
- **Certificado de identidade**: o certificado de cliente que o dispositivo apresenta (obrigatório para TLS). Consulte as opções de certificado abaixo.
- **Certificados confiáveis**: os certificados da CA que emitiram o certificado do seu servidor RADIUS. Eles são instalados com a rede.
- **Nomes de servidor confiáveis**: os nomes dos certificados do servidor RADIUS que os dispositivos aceitam, por exemplo radius.example.com ou *.example.com.

VPN

Clique em **Adicionar VPN** para configurar uma VPN IKEv2 ou Cisco IPSec, integrada ao iOS, iPadOS e macOS (não é necessário um app de VPN).

- **Tipo** e **Servidor**. Para IKEv2, também o **Identificador remoto** (a identidade do servidor, vazio significa o endereço do servidor) e o **Identificador local**, que pode conter as variáveis $EMAIL$, $USERNAME$, $FULLNAME$, $SERIAL$ e $UDID$.
- **Autenticação** do dispositivo: um certificado (da página Certificados, o certificado do usuário do dispositivo, ou solicitado a um servidor SCEP), um segredo compartilhado (com o nome do grupo opcional para IPSec), ou nenhuma para servidores IKEv2 que verificam apenas o nome de usuário e a senha.
- **Certificados confiáveis**: os certificados da CA do seu servidor VPN, instalados com a VPN. Para IKEv2, você também pode definir o emissor e o nome esperados do certificado do servidor.
- **Nome de usuário e senha**: o usuário também se autentica com um nome de usuário (variáveis permitidas) e uma senha (EAP para IKEv2, XAuth para IPSec). Deixe a senha vazia para permitir que o usuário a digite no dispositivo.
- **Nome da VPN** (mostrado em Ajustes) e **Aplica-se a**.

Conexão

- **O usuário se conecta em Ajustes**: a VPN é instalada e o usuário a ativa quando precisar.
- **Sob demanda**: o dispositivo conecta a VPN automaticamente. Com **exceto em Wi-Fi confiável**, a VPN não é usada nas redes Wi-Fi que você listar, por exemplo a rede do escritório.
- **Sempre ativa** (IKEv2, somente iPhone e iPad supervisionados): todo o tráfego passa pela VPN em celular e Wi-Fi e o usuário não pode desativá-la. Outros dispositivos não recebem esta VPN. Se a VPN usar um nome de usuário, a senha deve ser definida na política.
- **VPN por app**: somente alguns apps usam a VPN. Escolha a VPN de cada app na seção **Gerenciamento de apps** (campo **VPN** do app, não disponível no Mac), e opcionalmente liste domínios do Safari que a usam.

> Teste uma VPN sempre ativa ou sob demanda em um dispositivo de teste primeiro: se o servidor não puder ser alcançado, o dispositivo pode ficar sem conexão.

Proxy global, DNS criptografado e filtro de conteúdo da web

Essas configurações se aplicam a todo o tráfego do dispositivo. Ative-as com o alternador correspondente.

- **Proxy HTTP global** (iPhone e iPad supervisionados, Mac): todo o tráfego HTTP passa pelo proxy, em todas as redes. Defina o servidor e a porta (com um nome de usuário e senha opcionais) ou uma configuração automática (URL de arquivo PAC, ou vazio para encontrá-la na rede). **Permitir páginas de login de Wi-Fi** permite que o usuário entre em redes Wi-Fi públicas sem o proxy.
- **DNS criptografado**: o dispositivo resolve nomes com o seu servidor DNS por DNS over HTTPS (URL do servidor) ou DNS over TLS (nome do servidor), opcionalmente somente para alguns domínios. Em dispositivos supervisionados, você pode impedir que o usuário o desative.
- **Filtro de conteúdo da web** (iPhone e iPad supervisionados): o filtro integrado ao iOS limita sites adultos, com listas de sites sempre permitidos ou sempre bloqueados, ou permite somente uma lista de sites, mostrada como favoritos no Safari.

> Um proxy ou servidor DNS errado pode deixar os dispositivos sem conexão: teste as configurações em um dispositivo de teste primeiro.

Certificados

Clique em **Adicionar certificado** para instalar um certificado de forma independente: uma autoridade de certificação em que o Safari e os apps devem confiar, ou uma identidade usada por apps. Os certificados de uma rede Wi-Fi ou de uma VPN não precisam ser adicionados aqui.

Opções de certificado

- **Um certificado da página Certificados**: o mesmo certificado em todos os dispositivos. Clique em **Escolher um certificado** para escolhê-lo.
- **O certificado do usuário do dispositivo**: cada dispositivo recebe o certificado de cliente vinculado ao usuário dele. Dispositivos cujo usuário não tem um certificado não o recebem. Quando você vincula outro certificado ao usuário, os dispositivos são atualizados.
- **Solicitado a um servidor SCEP**: cada dispositivo solicita o próprio certificado ao seu servidor SCEP (por exemplo Microsoft NDES), então a chave privada nunca sai do dispositivo. Defina a URL do servidor, o desafio se o servidor exigir, o assunto (por exemplo CN=$EMAIL$), os nomes alternativos, o tamanho da chave e o uso da chave.

> Certificados de cliente (.p12) protegidos com a antiga criptografia RC2 não podem ser instalados em dispositivos Apple. Exporte-os novamente com criptografia 3DES ou AES antes de importá-los.

Segurança

Perfis que contêm senhas ou chaves privadas são enviados somente ao dispositivo para o qual foram criados: o dispositivo deve assinar a solicitação com o certificado de gerenciamento dele. Senhas e certificados não são gravados nos registros.

Atualizações de software

A seção **Atualizações de software** do Editor de Políticas da Apple mantém os dispositivos atualizados: ela pode exigir uma versão específica do sistema operacional até um prazo e controlar como os dispositivos baixam e instalam atualizações.

Atualizações de SO obrigatórias

Clique em **Adicionar atualização obrigatória** para exigir uma versão do SO. O dispositivo baixa a atualização, informa o usuário sobre o prazo e a instala no prazo se o usuário ainda não a tiver feito. Dispositivos que já executam essa versão ou uma posterior a ignoram. Requer iOS e iPadOS 17 ou macOS 14.

- **Aplica-se a** (obrigatório): iPhone e iPad, ou Mac. Cada SO tem seus próprios números de versão, então adicione uma atualização obrigatória para cada um.
- **Versão do SO**: a versão a instalar, por exemplo 18.5 ou 15.4.1.
- **Build** (opcional): uma build específica, por exemplo um beta ou uma Melhoria de Segurança em Segundo Plano.
- **Instalar até**: o prazo, no horário local de cada dispositivo. Uma data no passado faz os dispositivos instalarem a atualização o quanto antes.
- **URL de detalhes** (opcional): uma página da web sobre a atualização, exibida ao usuário.

> O dispositivo relata o progresso da atualização (download, instalação, falhas) no painel **Status do dispositivo** da página do dispositivo.

Configurações de atualização de software

Ative **Configurações de atualização de software para iPhone e iPad** ou **Configurações de atualização de software para Mac** para controlar as atualizações nesses dispositivos. Quando um botão está desativado, os dispositivos mantêm suas próprias configurações. Requer iOS e iPadOS 18 ou macOS 15: dispositivos mais antigos ignoram essas configurações.

- **Adiar atualizações**: as novas atualizações são mostradas ao usuário somente após o número de dias informado (1 a 90). Em um Mac, você pode definir períodos diferentes para atualizações principais, secundárias e outras atualizações do sistema.
- **Atualizações mostradas ao usuário** (iPhone e iPad): quando mais de uma atualização estiver disponível, mostrar todas, somente a atualização secundária mais antiga ou somente a mais recente.
- **Usuários padrão podem instalar atualizações** (Mac): usuários sem direitos de administrador podem instalar atualizações do macOS.
- **Notificar o usuário sobre atualizações obrigatórias**: mostrar as notificações sobre as atualizações obrigatórias e seu prazo.
- **Download automático**, **Instalação automática** e **Atualizações de segurança automáticas**: deixe o usuário decidir (padrão da Apple) ou mantenha-as sempre ativadas ou sempre desativadas.
- **Melhorias de Segurança em Segundo Plano**: ofereça as correções de segurança rápidas da Apple ao usuário e escolha se ele pode removê-las.
- **Programas beta**: permita que o usuário participe dos programas beta da Apple ou remova o dispositivo deles e os bloqueie (no iPhone e iPad, somente dispositivos supervisionados).

Instalar uma atualização na página do dispositivo

O painel **Status do dispositivo** de um dispositivo lista as atualizações disponíveis para ele. Use **Verificar atualizações** para solicitar a lista ao dispositivo e **Instalar** para instalar uma agora ou baixá-la e deixar o usuário instalá-la. Isso funciona em iPhones e iPads supervisionados e em Macs. A Apple remove esses comandos no iOS, iPadOS e macOS 27: nessas versões, use as atualizações obrigatórias da política.

macOS

A seção **macOS** do Editor de Política da Apple gerencia as configurações de segurança, privacidade e login dos Macs: FileVault, firewall, Gatekeeper, protetor de tela e bloqueio, armazenamento externo e de rede, Compartilhamento de Tela, permissões de privacidade, itens de login e as extensões de sistema e de kernel permitidas para carregar. Ela também instala arquivos de configuração de serviços do sistema e tarefas em segundo plano. Os outros dispositivos da política não recebem essas configurações. Ative uma configuração para gerenciá-la; enquanto estiver desativada, os usuários mantêm as próprias escolhas.

> A maioria das configurações é instalada no Mac como perfis de configuração, visíveis em Ajustes do Sistema > Geral > Gerenciamento de Dispositivos. FileVault, permissões de privacidade, itens de login e as configurações de extensões precisam de MDM aprovado pelo usuário: em um Mac registrado com a URL de registro ou o código QR, o usuário aprova o perfil de registro em Ajustes do Sistema. A página do dispositivo mostra isso no campo **MDM aprovado pelo usuário**. Quando o usuário aprova depois, o Mac recebe essas configurações automaticamente.

FileVault

O FileVault criptografa o disco do Mac. Com esta configuração ativada, os usuários são solicitados a ativar o FileVault com a senha deles, e o Mac envia a chave de recuperação pessoal ao Cerberus Enterprise, criptografada com uma chave que pertence somente à sua organização. A chave é mostrada e alterada no campo **FileVault** da página do dispositivo (consulte Comandos do dispositivo). A configuração precisa do macOS 13 ou posterior e de MDM aprovado pelo usuário; sem MDM aprovado pelo usuário, o Mac não é solicitado a ativar o FileVault, mas, se um usuário o ativar, a chave dele é armazenada.

- **Obrigatório no login**: no próximo login, após um número de pulos (o usuário é solicitado de novo a cada login e no logout), ou somente quando o usuário faz logout.
- **Não perguntar no logout**: o usuário é solicitado somente no login. Não pode ser combinado com "Solicitado somente no logout".
- **Mostrar a chave de recuperação ao usuário**: desativado por padrão, então somente os administradores conhecem a chave, na página do dispositivo.
- **Impedir a desativação do FileVault**: ativado por padrão.
- **Remover a chave da memória em espera**: o usuário digita a senha de novo quando o Mac desperta da espera.
- **Onde a chave é mantida**: texto mostrado ao usuário na janela de login, por exemplo quem chamar para recuperar o Mac (padrão "Cerberus Enterprise").

>

> Um Mac que já estava criptografado quando recebeu a configuração mantém a chave atual, que o Cerberus Enterprise não recebe: a chave é armazenada somente depois que o usuário desativa e ativa o FileVault de novo (com "Impedir a desativação do FileVault" desativado). Desativar a configuração, ou remover o Mac do gerenciamento, não desativa o FileVault, e a chave armazenada continua funcionando. A configuração não pode ser salva quando o servidor não está configurado para armazenar chaves de recuperação.

Firewall

- **Ativar o firewall**: quando está desativado, o firewall permanece desativado e os usuários não podem ativá-lo.
- **Bloquear todas as conexões de entrada**: somente os serviços de rede básicos (DHCP, Bonjour, IPSec) podem receber conexões.
- **Modo furtivo**: o Mac não responde a solicitações de ping nem a conexões para portas fechadas.
- **Permitir software integrado** e **Permitir apps assinados baixados** para receber conexões sem perguntar ao usuário (macOS 12.3 ou posterior).
- **Regras para apps específicos**: permita ou bloqueie as conexões de entrada de um app, pelo ID do pacote.

Gatekeeper

O Gatekeeper verifica os apps antes de abri-los. Escolha se os Macs abrem somente apps da App Store, ou também os apps de desenvolvedores identificados. Com o Gatekeeper desativado, qualquer app pode ser aberto, inclusive apps não assinados ou danificados. No macOS 15 ou posterior, você também pode escolher se os usuários são solicitados a enviar malware bloqueado à Apple.

Protetor de tela e bloqueio

Inicie o protetor de tela após um tempo de inatividade e peça a senha quando o protetor de tela iniciar ou a tela entrar em repouso, imediatamente ou após um atraso. Uma configuração deixada como **Não gerenciada** permanece a escolha do usuário.

Armazenamento externo e de rede

Permita, torne somente leitura ou bloqueie o armazenamento externo (unidades USB, cartões SD, discos externos) e o armazenamento de rede (compartilhamentos de arquivos) dos Macs. Precisa do macOS 15 ou posterior.

Compartilhamento de Tela

Limites das pessoas que se conectam a esses Macs com o Compartilhamento de Tela: copiar arquivos de ou para o Mac, conexões de alto desempenho e o número de telas virtuais. Ativar o Compartilhamento de Tela continua sendo uma escolha do usuário. Precisa do macOS 14 ou posterior.

Permissões de privacidade

Conceda ou negue aos apps o acesso que os usuários normalmente permitiriam em Ajustes do Sistema > Privacidade e Segurança, por exemplo Acesso Total ao Disco para um app de backup, ou negue a câmera a um app. Para cada permissão, escolha:

- **Permissão**: Acesso Total ao Disco, Acessibilidade, Automação, as pastas, contatos, calendários, fotos, câmera, microfone, gravação de tela e as outras de Privacidade e Segurança.
- **Acesso**: permitir ou negar. A câmera, o microfone, a gravação de tela e o monitoramento de entrada não podem ser permitidos por um perfil, apenas negados; para gravação de tela e monitoramento de entrada, você pode permitir que os usuários os autorizem também sem direitos de administrador.
- **App**: o ID do pacote de um app, ou o caminho de um programa (por exemplo, uma ferramenta de linha de comando).
- **Requisito de código**: identifica o app pela assinatura. Obtenha-o no Terminal com `codesign -dr - /Applications/Example.app` e copie o texto após `designated =>`.
- **Automação** também precisa do app controlado (por exemplo, o Finder) e do requisito de código dele.

Itens de login e em segundo plano

Os itens de login e itens em segundo plano que correspondem às regras são gerenciados: eles são executados sem perguntar, e os usuários não podem desativá-los em Ajustes do Sistema > Geral > Itens de Login. Uma regra corresponde ao ID da equipe de desenvolvedor de um app, ao ID do pacote dele ou ao rótulo de um daemon ou agente de inicialização (também pela primeira parte deles). Precisa do macOS 13 ou posterior.

Extensões do sistema

As extensões do sistema são a forma moderna de os apps estenderem o macOS: filtros de rede e VPNs, agentes e drivers de segurança de endpoint. Com esta configuração ativada, as extensões do sistema das equipes de desenvolvedor listadas carregam sem perguntar ao usuário. Precisa do macOS 10.15 ou posterior e de MDM aprovado pelo usuário.

- **ID da equipe**: o ID de equipe de 10 caracteres do desenvolvedor (por exemplo, nos detalhes "Assinado por" do app, ou com `codesign -dv`). Cada equipe pode aparecer somente uma vez.
- **Permitir**: todas as extensões da equipe, ou somente as extensões com os IDs de pacote listados.
- **Tipos**: limita a equipe a extensões de driver, de rede ou de segurança de endpoint. Sem nenhum selecionado, todos os tipos são permitidos.
- **Remoção** (somente para extensões listadas): o app pode remover a extensão dele sem um administrador (macOS 12 ou posterior), a extensão não pode ser desativada nem removida enquanto a Proteção de Integridade do Sistema estiver ativada, ou ela não pode ser removida em Ajustes do Sistema e no Finder (macOS 15 ou posterior). Macs com um macOS mais antigo ainda permitem a extensão, sem a opção de remoção.
- **Os usuários podem aprovar outras extensões do sistema**: ativado por padrão. Quando desativado, somente as extensões permitidas por um perfil podem carregar; se qualquer perfil no Mac o desativar, ele fica desativado.

> No macOS 11.3 ou posterior, remover esta configuração desativa as extensões do sistema que ela permitia, por exemplo um agente de segurança ou um filtro de rede. Isso acontece quando a configuração é desativada, quando a política é excluída e quando o Mac passa para uma política sem ela. O editor pede confirmação antes de desativar a configuração.

Extensões de kernel (legado)

As extensões de kernel são a forma mais antiga e obsoleta de estender o macOS: prefira as extensões do sistema quando o fornecedor as oferecer. As extensões de kernel das equipes listadas (todas as extensões de uma equipe, ou somente os IDs de pacote listados) carregam sem perguntar ao usuário, após uma reinicialização. Precisa do macOS 10.13.2 ou posterior e de MDM aprovado pelo usuário.

- **Os usuários podem aprovar outras extensões de kernel**: desativado por padrão, então somente as equipes listadas podem carregar extensões de kernel.
- **Usuários padrão também podem aprová-las**: com as aprovações do usuário ativadas, os usuários sem direitos de administrador também podem aprová-las (macOS 11 ou posterior).

> Em Macs com Apple silicon, um perfil sozinho não basta: alguém precisa iniciar o Mac no recoveryOS, escolher Segurança Reduzida no Utilitário de Segurança de Inicialização e permitir o gerenciamento de extensões de kernel pelo usuário a partir de desenvolvedores identificados. O Mac também pode precisar de um Bootstrap Token guardado no Cerberus Enterprise para aprová-las (consulte o campo Bootstrap Token da página do dispositivo).

Arquivos do Mac

Os arquivos de configuração de serviço e as tarefas em segundo plano usam arquivos que você envia para os **Arquivos do Mac** da sua organização: arquivos zip e listas de propriedades (.plist) de até 20 MB. Envie, verifique onde são usados ou exclua-os com o botão **Arquivos do Mac** da seção macOS, ou com **Escolher arquivo** em uma configuração. Um arquivo usado por uma política não pode ser excluído. Para alterar um arquivo, envie a nova versão e escolha-a na política: os Macs a baixam novamente.

Arquivos de configuração de serviço

Instala os arquivos de configuração de um serviço do sistema a partir de um arquivo zip. Os serviços integrados são o servidor SSH (sshd), o sudo, o PAM, a impressão (CUPS), o servidor web Apache, o bash, o zsh, o login com cartão inteligente e a autorização. Você também pode usar seu próprio serviço, com um identificador de DNS reverso como `com.example.service`: ele encontra os arquivos com a biblioteca de arquivos de configuração gerenciados do macOS. Cada serviço pode ter uma configuração. Precisa do macOS 14 ou posterior.

> Um serviço integrado usa somente os arquivos do arquivo zip e ignora os próprios arquivos dele, por exemplo /etc/ssh para o sshd: coloque toda a configuração no arquivo zip, em pastas que começam na raiz do disco (por exemplo `etc/ssh/sshd_config`). Os arquivos são somente leitura no Mac, e são removidos com a configuração. Teste o arquivo zip em um Mac primeiro: uma configuração errada de sudo ou PAM pode impedir os usuários de entrar ou de usar direitos de administrador.

Tarefas em segundo plano

Programas e scripts que são executados em segundo plano, iniciados pelo launchd. Os usuários não podem desativá-los, e eles são removidos com a configuração. Precisa do macOS 15 ou

posterior. Para cada tarefa, escolha:

- **Identificador da tarefa**: um identificador de DNS reverso, como `com.example.task`, diferente para cada tarefa.
- **Programas e scripts** (opcional): um arquivo zip que o Mac descompacta em `/var/db/ManagedConfigurationFiles/BackgroundTaskServices/Services/` seguido do identificador da tarefa. Mantenha a permissão de execução dos arquivos e não coloque listas de propriedades nele.
- **Listas de propriedades do launchd**: os trabalhos que iniciam os programas, carregados como um daemon (para todo o sistema, como root) ou como um agente (em cada sessão do usuário). Refira-se aos programas pelo caminho deles na pasta acima.

Uma tarefa precisa dos programas ou de pelo menos uma lista de propriedades. Quando os arquivos mudam, os Macs reiniciam a tarefa.

Localização e geocercas

A seção **Localização e geocercas** do Editor de Política da Apple define áreas, por exemplo um local ou um depósito. iPhones e iPads com o app Cerberus Enterprise informam quando entram ou saem de uma dessas áreas, e as regras de evento podem reagir a isso: enviar um e-mail, bloquear ou desativar o dispositivo, ou ativá-lo novamente. Macs não usam geocercas.

Campos da geocerca

Use **Adicionar geocerca** para criar uma nova entrada. Uma política pode conter até **10 geocercas**, e os nomes delas devem ser exclusivos dentro da política. Cada geocerca contém estes campos:

- **Nome**: obrigatório e exclusivo.
- **Latitude** e **Longitude**: o centro da área. Você também pode clicar no mapa para defini-lo.
- **Raio (m)**: obrigatório, de **200** a **10000** metros.
- **Descrição**: notas opcionais para administradores.
- **Informar entrada** e **Informar saída**: escolha quais eventos são gerados. Pelo menos um deve permanecer ativado.
- **Ativa**: ativa ou desativa a geocerca sem excluí-la.

Cada geocerca tem uma prévia no mapa. O centro e o raio de uma geocerca salva ficam bloqueados: use o botão de cadeado no mapa para alterá-los. Os outros botões centralizam o mapa na área ou na sua localização atual.

Quando você salva a política, o Cerberus Enterprise pede que os iPhones e iPads da política obtenham as novas geocercas. Isso geralmente leva alguns minutos, mas o iOS pode atrasar, por exemplo no Modo de Pouca Energia ou sem conexão de rede. A página do dispositivo mostra quando o app ainda não aplicou as geocercas mais recentes.

Requisitos

As geocercas funcionam em iPhones e iPads com o app Cerberus Enterprise. Macs as ignoram. No dispositivo:

- o app Cerberus Enterprise está instalado (o Cerberus o instala) e o usuário o abriu pelo menos uma vez;

- o acesso à localização do app está definido como **Sempre**;
- **Localização Precisa** está ativada para o app;
- **Atualização em Segundo Plano** está ativada.

> **Localização e geocercas em dispositivos pessoais**, no topo da seção, fica desativado por padrão. Enquanto estiver desativado, o Cerberus não coleta a localização de dispositivos pessoais (Registro do Usuário), os eventos de geocerca deles não são gerados e a página do dispositivo deles não oferece Localizar nem rastreamento ao vivo. Quando você o ativa, os dispositivos pessoais da política compartilham a localização e os eventos de geocerca como os dispositivos da empresa, mas somente se o usuário permitir a localização para o app Cerberus Enterprise; o app explica isso ao usuário antes de o iOS perguntar. Sua organização é responsável por informar os usuários e por seguir as regras locais sobre a localização de funcionários. O Modo Perdido e a solicitação de localização do MDM nunca estão disponíveis em dispositivos pessoais (a Apple não os permite).

No **Modo de Pouca Energia**, as geocercas continuam funcionando, mas o iOS informa a saída de uma área mais tarde e com uma localização menos precisa, e pode atrasar em horas a obtenção de novas geocercas depois de uma alteração na política, até o app ser executado novamente (por exemplo, na próxima travessia ou quando o usuário o abre).

Como os eventos chegam

O iOS monitora as áreas para o app e o desperta quando o dispositivo cruza uma fronteira, também quando o app não está aberto. Os eventos podem chegar alguns minutos depois da travessia, e uma área pequena ou uma visita curta podem passar despercebidas: o iOS precisa que o dispositivo se afaste da fronteira e permaneça lá por algum tempo.

Se o app não puder ser executado, por exemplo após uma reinicialização antes de o dispositivo ser desbloqueado, o servidor também detecta a travessia a partir das localizações que o app envia, mais tarde. Cada travessia dispara as regras de evento uma vez, seja o app ou o servidor a detectar.

Quando o app não entra em contato com o servidor por várias horas, o servidor pede ao iOS que o desperte para que ele possa verificar as geocercas novamente. O iOS não garante essas solicitações.

Página do dispositivo

Na página do dispositivo, a aba **Geocerca** do painel **Mapa de localização** mostra as transições do dispositivo. Quando a política tem geocercas ativas, uma linha de status informa se a geocerca funciona no dispositivo, ou por que não funciona: o app não entrou em contato com o servidor ou

precisa ser atualizado, o acesso à localização não é **Sempre**, **Localização Precisa** ou **Atualização em Segundo Plano** está desativada, o **Modo de Pouca Energia** estava ativado quando o app informou suas configurações pela última vez, ou o app ainda não aplicou as geocercas mais recentes.

> As transições de geocerca e as localizações são mantidas por **90 dias** e os dados mais antigos são excluídos automaticamente todas as noites. A última localização de cada dispositivo registrado é sempre mantida, então ele continua nos mapas.

Limitações

- Copiar uma política não copia as geocercas dela: adicione-as novamente na cópia.
- Os eventos de geocerca em iPhones e iPads dependem do melhor esforço: o iOS decide quando o app pode ser executado.

> Para reagir a eventos de geocerca, crie uma regra de evento para **Dispositivo entra em uma geocerca** ou **Dispositivo sai de uma geocerca**. Consulte **Regras de evento**.

Contas

A seção **Contas** do Editor de políticas da Apple adiciona contas de e-mail, Exchange, Google, calendário, contatos e diretório ao iPhone, iPad e Mac. Clique em **Adicionar conta** e escolha o tipo. A seção também contém a restrição **Permitir modificação da conta** (dispositivos supervisionados).

> Em um Mac (macOS 13 ou posterior), as contas são instaladas na sessão dos usuários registrados no gerenciamento, geralmente o usuário que registrou o Mac, quando ele está conectado. A página do dispositivo lista esses usuários em **Usuários do Mac**, com o estado das contas deles. As contas que usam o endereço de e-mail do usuário do dispositivo usam o usuário atribuído ao Mac no Cerberus Enterprise.

Configurações comuns

- **Nome e e-mail do usuário do dispositivo** (Mail, Exchange, Google): cada dispositivo usa o nome e o endereço de e-mail do seu usuário, definidos na página Usuários (para Google, a conta Google do usuário). Dispositivos sem usuário, ou cujo usuário não tem endereço de e-mail, não recebem a conta. Caso contrário, defina um endereço de e-mail e um nome completo fixos.
- **Nome da conta** (opcional): o nome da conta em Configurações e nos apps.
- **Nome de usuário** e **Senha** (opcional): o nome de usuário pode conter as variáveis $EMAIL$, $USERNAME$, $FULLNAME$, $SERIAL$ e $UDID$. Deixe a senha vazia para o usuário digitá-la no dispositivo, ou deixe ambos vazios para o usuário digitá-los.
- **Aplica-se a**: limita a conta a alguns tipos de dispositivo.

Tipos de conta

- **Conta de e-mail**: servidor de entrada IMAP ou POP e servidor de saída, com suas portas e autenticação. O servidor de saída pode usar o mesmo nome de usuário e senha do servidor de entrada.
- **Conta Exchange** (Exchange ActiveSync): o servidor, ou vazio para encontrá-lo a partir do endereço de e-mail. Escolha os serviços (e-mail, contatos, calendários, lembretes, notas) e se o usuário pode alterá-los. Com **Autenticação moderna (OAuth)**, o usuário entra pela página do seu provedor de identidade, por exemplo Microsoft 365. Um **Certificado de autenticação** (iOS 17 ou posterior) autentica o dispositivo com um certificado.

- **Conta Google**: o usuário entra na conta Google com o endereço de e-mail informado.
- **Conta de calendário (CalDAV)** e **Conta de contatos (CardDAV)**: o servidor, a porta e o caminho.
- **Diretório (LDAP)**: o servidor e a porta, e as pesquisas (base de pesquisa, escopo e descrição) usadas para procurar contatos.
- **Calendário assinado**: a URL do calendário (https, http ou webcal).

S/MIME

As contas Mail e Exchange podem assinar e criptografar mensagens com S/MIME (iOS 17 ou posterior). Para cada uma, escolha o certificado: um da página Certificados, o certificado do usuário do dispositivo ou solicitado a um servidor SCEP. Você pode permitir que o usuário o desative, escolha outro certificado e, para criptografia, exiba um interruptor para cada mensagem.

Segurança

Senhas e certificados não fazem parte das configurações enviadas aos dispositivos: cada dispositivo baixa suas próprias credenciais do Cerberus Enterprise, assinando a solicitação com seu certificado de gerenciamento. Eles não são gravados nos logs.

Regras de conformidade

A seção **Regras de conformidade** do Editor de Política da Apple define requisitos para os dispositivos da política. Um dispositivo que viola uma regra fica sem conformidade imediatamente: a página do dispositivo mostra o motivo, em **Por que o dispositivo está sem conformidade**, e a lista de dispositivos o mostra como sem conformidade. Um dispositivo também fica sem conformidade quando uma configuração da política não pode ser aplicada nele.

Regras

- **Código de acesso**: o dispositivo tem um código de acesso e ele atende às configurações de código de acesso da política.
- **Versão mínima do SO**: para iPhone e iPad, ou para Mac. Para atualizar os dispositivos, adicione uma atualização obrigatória em Atualizações de software.
- **Dispositivo supervisionado**: dispositivos registrados com o perfil de registro ou com o Registro do Usuário não são supervisionados.
- **FileVault ativado (Mac)**: o disco do Mac está criptografado com FileVault. Outros dispositivos não são afetados.

Uma regra é verificada quando o dispositivo envia seu status, quando a política é salva e a cada hora. Um dispositivo cujo status é desconhecido (por exemplo, um Mac que ainda não informou o FileVault) não viola a regra.

Bloquear o dispositivo

Ative **Bloquear o dispositivo se ele continuar sem conformidade** e defina depois de quantos dias (0 bloqueia imediatamente). iPhones e iPads supervisionados entram no modo perdido com a mensagem que você definir. Os outros dispositivos são bloqueados uma vez; um Mac reinicia e pede um PIN, mostrado nos detalhes do comando no histórico de comandos.

- **Desbloquear**: quando o dispositivo volta a estar em conformidade, o modo perdido é desativado automaticamente.
- **Desativar o modo perdido por conta própria**: o dispositivo não é bloqueado novamente até voltar a estar em conformidade e violar uma regra de novo. Use isso para permitir que o usuário corrija o dispositivo.

> Para ser notificado, ou reagir de outras maneiras, crie uma regra de evento para **Dispositivo fica sem conformidade**: ela também recebe os motivos.