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.

Revision #6
Created 2026-11-10 15:17:44 UTC by Admin
Updated 2026-11-12 09:57:21 UTC by Admin