Comandos

A página do dispositivo oferece um painel **Comandos** para enviar comandos remotos a um dispositivo gerenciado. Os comandos disponíveis dependem da plataforma (Android ou Apple) e do estado do dispositivo.

Os comandos só podem ser enviados a um dispositivo registrado no momento. Em um dispositivo com registro cancelado, em um dispositivo ADE que ainda não foi registrado e no histórico de um registro anterior, o painel mostra apenas o histórico de comandos.

> Se o dispositivo não estiver online no momento, o comando será entregue e executado assim que o dispositivo se conectar à Internet. Para comandos Android, você pode definir o parâmetro **Validade** para determinar por quanto tempo um comando não entregue permanece válido.

Comandos Android (AMAPI)

Para dispositivos Android, o painel Comandos inclui um campo **Validade** (valor + unidade) e um seletor **Comando**. Alguns comandos exigem parâmetros adicionais, que aparecem dinamicamente quando você seleciona o comando.

Parâmetros comuns

- **Validade**: por quanto tempo o comando é válido se não puder ser executado imediatamente.
- **Comando**: escolha qual ação enviar ao dispositivo.

Comandos sem campos adicionais

- **Bloquear dispositivo**: bloqueia o dispositivo.
- **Reiniciar dispositivo**: reinicia o dispositivo. Requer Android 7.0 ou posterior.
- **Desativar modo perdido**: tira o dispositivo do modo perdido.
- **Renunciar à propriedade**: remove o perfil de trabalho e todas as políticas de um dispositivo corporativo com Android 8.0 ou posterior e o deixa para uso pessoal. Os apps e dados do perfil pessoal são mantidos. O dispositivo é excluído do servidor depois que confirma o comando. Isso não pode ser desfeito.

Comandos com campos adicionais

- **Redefinir senha**: requer **Nova senha** e **Confirmar nova senha**. Opções opcionais incluem **Bloquear agora**, **Exigir entrada** e **Não pedir credenciais na inicialização**.
- **Limpar dados do app**: requer o **Nome do pacote** de destino.
- **Ativar modo perdido**: requer uma **Mensagem do modo perdido** e oferece suporte a campos de contato opcionais (endereço, organização, número de telefone, e-mail). Quando o dispositivo informa, seu estado passa a ser **Perdido**, a página do dispositivo mostra um banner e este comando fica oculto até o modo perdido ser desativado.
- **Apagar dispositivo**: oferece suporte a uma **Mensagem de motivo da limpeza** (exibida aos usuários em dispositivos pessoais) e a flags de limpeza opcionais, incluindo **Apagar eSIMs**.

> Os comandos de eSIM (**Adicionar eSIM**, **Remover eSIM**, **Solicitar EID**) estão disponíveis no painel dedicado **Gerenciamento de SIMs**.

Histórico de comandos

Abaixo dos controles de envio, o painel mostra uma tabela de histórico de comandos. A tabela é classificável e oferece suporte a paginação. Algumas linhas podem ser expandidas para ver parâmetros adicionais ou detalhes de execução.

Colunas do histórico Android

- **Data de criação**
- **Comando**
- **Validade**
- **Status**
- **Erro**
- **Data de execução**

Comandos Apple (MDM)

Para dispositivos Apple, o painel Comandos oferece um seletor **Comando**. Alguns comandos exigem entradas adicionais. Assim como no Android, uma tabela de histórico de comandos é exibida abaixo.

Comandos com campos adicionais

- **Instalar app**: requer o **Bundle ID** do aplicativo.
- **Enviar notificação**: requer uma **Mensagem de notificação** (comprimento máximo de 200 caracteres).

Em iPhones e iPads, **Enviar notificação** e o rastreamento ao vivo chegam ao dispositivo pelo app **Cerberus Enterprise**: eles ficam desativados até o app ser instalado e ter se registrado para notificações (consulte o campo **app Cerberus Enterprise**). Iniciar o rastreamento ao vivo mostra "Solicitação de rastreamento ao vivo enviada ao dispositivo": o rastreamento começa quando o dispositivo envia sua primeira localização. O iOS pode atrasar a solicitação ou não entregá-la, por exemplo no Modo de Baixo Consumo ou sem conexão de rede: se nenhuma localização chegar em 2 minutos, peça ao usuário para abrir o app uma vez. Quando uma solicitação falha, a mensagem informa o motivo, por exemplo o app ainda não se registrou, a chave de notificação do servidor está ausente ou o token de notificação do dispositivo não é mais válido.

Ações do dispositivo

Somente os comandos compatíveis com o dispositivo são listados: alguns exigem um iPhone ou iPad supervisionado, outros não estão disponíveis em um Mac. Os comandos disruptivos pedem confirmação.

- **Bloquear dispositivo**: bloqueia a tela, com mensagem e número de telefone opcionais. Um Mac é reiniciado e bloqueado com um PIN de seis dígitos, exibido uma vez após o envio do comando e nos detalhes do comando. O iPhone mostra o título "iPhone Perdido" acima da sua mensagem, embora este comando não ative o modo perdido.
- **Ativar modo perdido** (iPhone e iPad supervisionados): bloqueia o dispositivo e mostra sua mensagem, número de telefone e nota de rodapé na Tela Bloqueada. Enquanto o modo perdido está ativo, a página mostra um banner e os comandos **Localizar dispositivo** (a localização aparece no Mapa de localização), **Reproduzir som** e **Desativar modo perdido**.
- O dispositivo informa a quem o estiver segurando que foi localizado: após **Localizar dispositivo**, a Tela Bloqueada mostra **iPhone Localizado** com o horário e o nome do servidor que recebeu a localização, e um botão **Continuar**. O iOS mostra este aviso e ele não pode ser desativado.
- **Limpar código de acesso**: remove o código de acesso de um iPhone ou iPad, por exemplo quando o usuário o esqueceu. Se a política exigir um código de acesso, o usuário será solicitado a definir um novo.
- **Atualizar informações do dispositivo**: solicita ao dispositivo suas informações (supervisão, versão do sistema, status de segurança, certificado MDM) e seu inventário.
- **Configurações do dispositivo**: abre uma janela para alterar o nome do dispositivo, o nome do host de um Mac, Bluetooth, roaming de dados, Acesso Pessoal, fuso horário, papel de parede, se o Bloqueio de Ativação é permitido e, em um iPad Compartilhado, suas configurações (veja abaixo). Apenas as configurações que você alterar são enviadas; as que o dispositivo não oferece suporte ficam desativadas com o motivo. Um dispositivo pode confirmar o roaming de dados ou o Acesso Pessoal sem aplicá-los (por exemplo,

quando o plano do SIM não tem Acesso Pessoal), então o Cerberus Enterprise os lê novamente cerca de 30 segundos depois e grava um aviso nos logs do sistema se não tiverem mudado.
- **Reiniciar dispositivo** e **Desligar dispositivo**: reiniciam ou desligam o dispositivo imediatamente, após uma confirmação.
- **Apagar dispositivo**: apaga todo o conteúdo e as configurações e remove o dispositivo do gerenciamento. Em iPhone e iPad, você pode manter o plano de dados eSIM e ignorar a configuração por proximidade; um Mac recebe um PIN de seis dígitos.
- **Retornar ao serviço** (opção de **Apagar dispositivo**, iPhone e iPad com iOS 17 ou posterior): após a limpeza, o dispositivo se configura novamente, sem que ninguém o toque, e se registra de novo com a política, o usuário e a propriedade atuais. Escolha uma rede Wi-Fi da política do dispositivo para a configuração, a menos que o dispositivo tenha Ethernet ou dados celulares: somente redes pessoais (com senha, sem certificados) podem ser usadas, porque o dispositivo ainda não tem usuário nem certificado. O Bloqueio de Ativação deve estar desativado.
- **Atualizar planos celulares** (iPhone e iPad celular, iOS 13 ou posterior, exceto User Enrollment): insira a **URL do servidor eSIM da operadora** fornecida pela operadora (um endereço https://, um nome de host ou um código de ativação LPA, do qual apenas o servidor é usado) e o dispositivo baixa os planos eSIM que a operadora vinculou ao EID dele. O EID do dispositivo é exibido abaixo do campo para enviá-lo à operadora. Consulte a página **Gerenciamento de SIMs**.
- **Manter o plano de dados eSIM** desativado remove todos os eSIMs com a limpeza. A restrição de política **Manter o eSIM quando o dispositivo for apagado** (dispositivos supervisionados, iOS 17.2 ou posterior) se aplica a limpezas iniciadas no próprio dispositivo (muitas tentativas de código de acesso com falha, Apagar Todo o Conteúdo e Ajustes): a Apple não documenta seu efeito neste comando.
- **Sair do usuário** (iPad Compartilhado): desconecta o usuário atual e volta à tela de login. Os dados ainda não sincronizados com o iCloud permanecem no iPad.

iPad Compartilhado

Um iPad Compartilhado é usado por várias pessoas, cada uma com sua própria Conta Apple Gerenciada, ou por convidados com sessões temporárias. Ele é configurado com um perfil ADE que habilita o iPad Compartilhado (consulte a página **Apple Automated Device Enrollment**), e seu campo **Tipo de registro** mostra **iPad Compartilhado**.

- **Usuários do iPad Compartilhado**: os usuários do iPad, com o usuário conectado, o armazenamento que usam e se alguns dados ainda não foram sincronizados com o iCloud. Use **Atualizar** para solicitar a lista ao iPad novamente. Um usuário pode ser excluído com seus dados, exceto o usuário conectado (desconecte-o primeiro); **Excluir todos os usuários** requer iPadOS 14 ou posterior. Quando os dados ainda não foram sincronizados, a confirmação avisa que eles serão perdidos.
- **Configurações do dispositivo**: o armazenamento de cada usuário, o número esperado de usuários, o tempo de inatividade após o qual usuários e sessões de convidado são

desconectados, somente sessões de convidado, os domínios de Conta Apple Gerenciada sugeridos na tela de login, por quantos dias um usuário pode entrar sem verificar a senha online e a opção de ignorar a configuração de idioma e região para novos usuários. Campos vazios mantêm o valor atual; as configurações que exigem um iPadOS mais recente ficam desativadas.

Usuários do Mac

Em um Mac, o painel **Usuários do Mac** lista os usuários registrados no gerenciamento, normalmente o usuário que registrou o Mac. As contas da política são instaladas nas sessões deles. Para cada usuário, ele mostra quando foi registrado, o último relatório da sessão e o estado das contas: **Atualizado**, **Aguardando o usuário** (o Mac as instala quando o usuário está conectado), **Não aplicado** com os motivos informados pelo Mac, ou **Sem contas** quando a política não tem nenhuma. Use **Recarregar** para ler a lista novamente.

Bloqueio de Ativação

O campo **Bloqueio de Ativação** mostra se o Bloqueio de Ativação está ativado. Quando está ativado, um dispositivo apagado só pode ser configurado novamente com a Conta Apple do usuário ou com o código de desvio do dispositivo. Dispositivos supervisionados ativam o Bloqueio de Ativação somente se ele for permitido em **Configurações do dispositivo**. O Cerberus Enterprise solicita o código de desvio aos dispositivos supervisionados e o armazena: use **Mostrar código de desvio** no menu do campo para vê-lo (somente administradores podem, e cada visualização é registrada no log do sistema); depois insira-o como senha na tela de Bloqueio de Ativação do dispositivo, deixando a Conta Apple vazia.

Bloqueio de Recuperação e senha de firmware (Mac)

Um Mac com Apple silicon mostra o campo **Bloqueio de Recuperação**, e um Mac com processador Intel mostra o campo **Senha de firmware**. Ambos protegem o Mac na inicialização: com o Bloqueio de Recuperação, o recoveryOS solicita a senha; com uma senha de firmware, o Mac a solicita para iniciar de outro disco ou da recuperação. O campo mostra se o Mac informa uma senha e, na dica, quando o Cerberus Enterprise a armazenou e quando ela foi verificada pela última vez.

- **Definir ou alterar senha**: o Cerberus Enterprise gera uma senha de 20 letras que ficam nas mesmas teclas em qualquer layout de teclado, ou um administrador digita uma (8 a 64 caracteres sem acentos; outros perfis só podem gerar uma, porque não conseguem ver as senhas armazenadas). A senha é armazenada criptografada antes de ser enviada e substitui a armazenada somente quando o Mac confirma. Se o Mac já tiver uma senha

definida fora do Cerberus Enterprise, digite-a como senha atual: ela é usada uma vez e não é armazenada.
- **Verificar senha**: pergunta ao Mac se a senha armazenada está correta. O resultado fica na dica e no log do sistema.
- **Mostrar senha**: somente administradores podem ver a senha armazenada, e cada visualização é registrada no log do sistema. As senhas geradas são exibidas em grupos de quatro letras: digite-as sem espaços.
- **Limpar senha**: remove a senha do Mac.

Um Mac com processador Intel reinicia para aplicar uma alteração de senha de firmware: até lá, a senha anterior ainda é necessária (Mostrar senha a exibe), e outra alteração não pode ser enviada. A Apple também aceita apenas um comando de senha de firmware a cada 30 segundos. As senhas ficam ocultas no histórico de comandos.

Quando um Mac sai do gerenciamento (registro cancelado, removido pelo usuário ou apagado), o macOS remove o Bloqueio de Recuperação por conta própria, e o Cerberus Enterprise descarta a senha de Bloqueio de Recuperação armazenada; ele faz o mesmo quando o Mac informa que não tem Bloqueio de Recuperação, por exemplo após se registrar novamente. Quando você cancela o registro de um Mac (ou exclui a política dele), uma senha de firmware armazenada é limpa primeiro, o Mac reinicia e então sai do gerenciamento. Se a limpeza falhar, o Mac sai do gerenciamento mesmo assim, e a senha permanece armazenada para que você ainda possa vê-la. Um Mac removido do gerenciamento pelo usuário, ou apagado, mantém sua senha de firmware: o Cerberus Enterprise também a mantém. Excluir o registro do dispositivo apaga a senha armazenada, por isso você precisa confirmar antes: anote a senha, porque sem ela somente a Apple pode removê-la.

FileVault (Mac)

O campo **FileVault** mostra se o disco do Mac está criptografado e, na sua dica, se o Cerberus Enterprise armazena a chave de recuperação pessoal dele. Um Mac envia a chave quando o FileVault é ativado depois que ele recebe a configuração de FileVault da política dele (consulte a página **macOS** das políticas Apple).

- **Mostrar chave de recuperação**: somente administradores podem ver a chave, e cada visualização é registrada no log do sistema. Use-a na janela de login do Mac para redefinir a senha do usuário, ou na recuperação para desbloquear o disco. Ela permanece disponível depois que o Mac sai do gerenciamento; excluir o registro do dispositivo a apaga.
- **Alterar chave de recuperação**: o Mac substitui sua chave de recuperação pessoal e envia a nova, criptografada; a chave antiga deixa de funcionar. Isso só é possível quando a chave armazenada pode ser lida: o Mac é desbloqueado com ela, e nenhuma senha de usuário é necessária. A chave armazenada fica oculta no histórico de comandos e é removida do servidor quando o Mac responde (ou após 7 dias sem resposta).

Bootstrap Token (Mac)

Um Mac com macOS 10.15 ou posterior envia seu **Bootstrap Token** ao servidor de gerenciamento quando um usuário com um token seguro entra. O servidor o mantém e o devolve somente a esse Mac, que o usa para conceder um token seguro a novos usuários e, em um Mac com Apple silicon, para instalar atualizações de software e aprovar extensões de kernel sem pedir uma senha de administrador. Ninguém pode ver o token, no painel nem em outro lugar. O campo **Bootstrap Token** mostra o estado dele:

- **Escrowado**: o servidor tem o token; a dica mostra quando o Mac o enviou.
- **Armazenado anteriormente**: o token armazenado foi enviado antes do último registro ou da última renovação do certificado MDM do Mac. Após uma renovação, isso é esperado: o token é mantido e o Mac não o envia novamente. Após um novo registro, ele pode não ser mais válido: execute `sudo profiles install -type bootstraptoken` no Terminal do Mac.
- **Não escrowado**: o Mac ainda não enviou um token. Para enviá-lo agora, um administrador do Mac executa `sudo profiles install -type bootstraptoken` no Terminal (`sudo profiles status -type bootstraptoken` mostra se ele está escrowado).

A dica também informa se o Mac permite o token para autenticação. Macs configurados com o Automated Device Enrollment o permitem automaticamente; em outros Macs com Apple silicon, um usuário pode permiti-lo no Utilitário de Segurança de Inicialização no recoveryOS. Macs Intel não podem usar o token para autenticação (**Não suportado**), mas um token escrowado ainda concede um token seguro a novos usuários. Cada vez que um Mac envia, remove ou solicita seu token, isso é registrado no log do sistema.

Status do dispositivo e atualizações do sistema

O painel **Status do dispositivo** mostra o que o dispositivo informa sobre si mesmo: a versão e a compilação do sistema, o progresso de uma atualização de software (versão pendente, prazo, o que a iniciou, falhas), se um código de acesso está definido e em conformidade com a política, o FileVault em um Mac, a saúde da bateria e as contas configuradas no dispositivo.

A lista **Atualizações disponíveis** mostra as atualizações de SO que o dispositivo pode instalar, coletadas no registro e semanalmente. Use **Verificar atualizações** para solicitá-las agora e **Instalar** para instalar uma atualização imediatamente (o dispositivo reinicia, após uma confirmação) ou apenas baixá-la e deixar o usuário instalá-la. Isso funciona em iPhones e iPads supervisionados e em Macs, até iOS, iPadOS e macOS 26: em versões posteriores e para atualizar muitos dispositivos, use as atualizações obrigatórias da política (consulte a página **Atualizações de software** das políticas Apple).

Um Mac com Apple silicon instala uma atualização sem pedir uma senha de administrador somente quando permite seu Bootstrap Token para autenticação e o token está escrowado (consulte Bootstrap Token acima). Caso contrário, a confirmação informa que um usuário pode precisar inserir uma senha de administrador antes de a atualização ser instalada.

Aplicativos e inventário

O painel **Aplicativos** lista todos os apps do dispositivo em uma única tabela. O estado de instalação dos apps instalados pela política ou por um comando é informado ao vivo pelo dispositivo; versões, tamanhos e os apps instalados pelo usuário vêm da última lista de apps, coletada no registro e semanalmente. Use **Perguntar ao dispositivo** para solicitá-la agora.

- **Gerenciamento**: **Política** para apps instalados pela política do dispositivo, **Gerenciado** para apps instalados com um comando como **Instalar app**, **Não gerenciado** para os instalados pelo usuário. O app Cerberus Enterprise tem o selo **Instalado pelo Cerberus**.
- **Precisa de atenção**: apps que falharam na instalação, foram recusados ou removidos pelo usuário, ou aguardam o usuário. Abra uma linha para ver o erro; apps de política que falharam podem ser instalados novamente com o botão de tentar de novo. Apps integrados e apps da App Store que o dispositivo informa como não validados não são contados.
- **Remover app**: apps gerenciados podem ser removidos, com os dados deles. Para remover um app instalado pela política, remova-o da política. A política também envia este comando automaticamente quando um pacote de Mac instalado como app gerenciado é removido da política.

O painel **Perfis, certificados e segurança** mostra os perfis de configuração, os certificados e o status de segurança (código de acesso, criptografia, FileVault e firewall em um Mac) informados pelo dispositivo.

> Em dispositivos de propriedade pessoal, os apps instalados pelo usuário não são coletados, e somente os perfis e certificados gerenciados pelo Cerberus Enterprise são listados.

O painel **Alterações no inventário** mostra o que mudou entre duas listas enviadas pelo dispositivo: apps instalados, removidos ou atualizados (com a versão antiga e a nova), perfis instalados, removidos ou atualizados, e certificados adicionados ou removidos. Uma alteração é detectada quando o dispositivo envia uma nova lista, semanalmente para apps e perfis, diariamente para certificados, ou quando você usa **Perguntar ao dispositivo**: a data exibida é quando ela foi detectada, e a alteração ocorreu entre a lista anterior e essa. A primeira lista de um dispositivo, e a primeira após um novo registro ou uma mudança de propriedade, é registrada apenas como ponto de partida. Pesquise por nome ou identificador e filtre por tipo e alteração. As alterações são mantidas por 365 dias.

>

> Quando uma atualização do sistema substitui muitos apps Apple de uma vez, eles são exibidos como uma única linha (por exemplo, "23 apps Apple atualizados") que você pode expandir. A renovação do certificado MDM é exibida como **Certificado MDM renovado**. Em dispositivos de propriedade pessoal, somente as alterações dos itens gerenciados pelo Cerberus Enterprise são exibidas.

Colunas do histórico Apple

- **Data de criação**
- **Comando**
- **Status**: **Enviado** (aguardando o dispositivo; entregue assim que ele se conectar), **Sucesso**, **Respondido** (abra a linha para ver o resultado), **Aguardando o dispositivo** (o dispositivo não pode executar o comando no momento), **Falhou** (abra a linha para ver o motivo) ou **Cancelado** (a fila de comandos do dispositivo foi limpa, por exemplo quando ele se registrou novamente).
- **Data de execução**

Atualizar

Use a ação de atualização no painel Comandos para recarregar o histórico de comandos.

Revision #58
Created 2025-12-17 09:34:44 UTC by Admin
Updated 2026-11-12 09:57:13 UTC by Admin