Registro orientado por conta da Apple

Com o registro orientado por conta, os usuários registram o iPhone, iPad ou Mac entrando com a conta de trabalho (uma **Managed Apple Account**, por exemplo *name@company.com*) nas configurações do dispositivo. Nenhum perfil para baixar e nenhum QR code: o Cerberus Enterprise encontra o usuário, aplica a política e define a propriedade sozinho.

Dois modos

- **User Enrollment** (dispositivos pessoais): apenas os apps, contas e dados de trabalho são gerenciados, em uma área separada do dispositivo. O Cerberus não pode ver dados pessoais, apagar o dispositivo, localizá-lo ou ler o número de série dele. O dispositivo é definido como pessoal. Requer iOS e iPadOS 15 ou macOS 14 ou posterior.
- **Device Enrollment** (dispositivos da empresa que não estão no Apple Business): o dispositivo inteiro é gerenciado, como em um registro manual. Um Mac registrado dessa forma é supervisionado; um iPhone ou iPad não é. O dispositivo é definido como da empresa. Requer iOS e iPadOS 17.1 ou macOS 14.1 ou posterior.

> Você escolhe o modo para iPhone e iPad e, separadamente, para Mac: por exemplo, User Enrollment para iPhones pessoais e Device Enrollment para Macs. Você pode alterar a propriedade de um dispositivo mais tarde na página do dispositivo.

> O registro orientado por conta fica disponível quando o Apple Management (APNs) está configurado. Se você ainda não concluiu a configuração do APNs, leia **Configuração do Apple Management (APNs)**.

Configurar o Apple Business

Os usuários entram com Managed Apple Accounts, que são criadas no Apple Business. Antes de começar:

1. **Verifique seu domínio** (por exemplo *company.com*) no Apple Business, nos domínios da sua organização.
2. **Crie as Managed Apple Accounts** dos seus usuários, ou conecte o Apple Business ao Google Workspace ou ao Microsoft Entra ID: assim, a conta de cada usuário é o endereço de e-mail corporativo dele e ele entra com a senha dela.
3. Para o User Enrollment, verifique nas configurações de gerenciamento de acesso se as Managed Apple Accounts podem entrar em **dispositivos pessoais**: quando elas só podem entrar em dispositivos supervisionados, o User Enrollment falha.
4. Apenas para a opção **Apple Business** abaixo: abra **Dispositivos → Serviços de gerenciamento → Atribuição de dispositivo padrão** (Editar) e escolha o serviço de gerenciamento de dispositivos Cerberus Enterprise para iPhone, iPad e Mac.

> Mantenha o serviço de gerenciamento de dispositivos Cerberus Enterprise e o token dele no Apple Business enquanto os dispositivos estiverem registrados com Managed Apple Accounts: removê-los pode impedir que as contas funcionem nos dispositivos.

Configurar o Cerberus Enterprise

Abra a seção **Registro** do painel e selecione a aba **Entrada com conta Apple**. Uma lista de verificação na parte superior mostra o que ainda falta. Somente administradores podem alterar as configurações.

- **Permitir registro entrando com uma conta de trabalho**: ativa ou desativa o registro orientado por conta para toda a organização.
- **Domínios**: os domínios das contas dos seus usuários (por exemplo *company.com*), até 20. Apenas contas desses domínios podem se registrar, e somente depois que o domínio for verificado (veja abaixo).
- **iPhone e iPad** e **Mac**: Desativado, User Enrollment ou Device Enrollment para cada família de dispositivos.
- **Política** de cada modo: aplicada aos dispositivos assim que eles se registram. Sem uma política, os dispositivos se registram sem uma. Uma política alterada se aplica aos próximos registros.
- **Usuários**: *Somente usuários existentes* (o endereço de e-mail de um usuário no Cerberus Enterprise deve corresponder à conta digitada no dispositivo) ou *Criar um usuário para contas dos domínios que não têm um*.

> A conta digitada no dispositivo é correspondida com o campo **Managed Apple Account** dos usuários e, depois, com o endereço de e-mail deles. O código é sempre enviado ao endereço de e-mail do usuário. Uma Managed Apple Account definida em um usuário pode se registrar mesmo quando o domínio dela não está verificado no Cerberus, por exemplo uma conta do domínio reservado *org.appleid.com* do Apple Business. Com a descoberta de

serviço do Apple Business, os usuários sempre digitam a Managed Apple Account.

Verificar os domínios

Depois de salvar as configurações, a seção **Verificação de domínio** mostra um registro TXT para cada domínio. Adicione-o ao DNS do domínio e clique em **Verificar**. As alterações de DNS podem levar algum tempo para ficarem visíveis. Um domínio verificado permanece verificado: você pode remover o registro depois. Usuários de um domínio que não foi verificado não podem se registrar.

Descoberta de serviço: como os dispositivos encontram o Cerberus Enterprise

Quando um usuário entra, o dispositivo pergunta ao domínio da conta (por exemplo *https://company.com*) qual servidor o gerencia. Configure pelo menos uma destas três opções. A seção **Descoberta de serviço** da aba mostra a URL de descoberta da sua organização e o texto exato para copiar em cada opção.

Opção 1: Apple Business (recomendado)

Clique em **Registrar no Apple Business**: o Cerberus Enterprise armazena a URL de descoberta dele na sua organização do Apple Business e nada precisa ser publicado nos seus domínios. **Verificar no Apple Business** mostra a URL que o Apple Business tem agora, e **Remover do Apple Business** a remove.

- Requer iOS e iPadOS 18.2 ou macOS 15.2 ou posterior. Dispositivos mais antigos precisam da opção 2 ou 3.
- Requer o Apple Business conectado no Cerberus Enterprise (token do serviço Automated Device Enrollment) e a atribuição de dispositivo padrão descrita acima.
- O dispositivo pergunta ao Apple Business somente quando o seu domínio não responde: o endereço *https://company.com/.well-known/com.apple.remotemanagement* não deve existir (um erro como "not found"). Se o seu site responder com uma página da web, os dispositivos param ali. Use **Verificar configuração** para ver o que ele responde.

O Apple Business mantém uma URL de descoberta por organização: registrá-la envia todas as Managed Apple Accounts da organização para esta organização do Cerberus Enterprise.

> Não a registre a partir de duas organizações do Cerberus Enterprise que usam a mesma organização do Apple Business.

Opção 2: Redirecionar do seu site

No servidor web de cada domínio, redirecione */.well-known/com.apple.remotemanagement* para a URL de descoberta da sua organização, **mantendo a string de consulta** (ela carrega a conta digitada pelo usuário). Isso funciona com todas as versões de SO compatíveis com o registro orientado por conta, e o modo pode ser diferente para iPhone e Mac. Copie o texto para Apache ou nginx da aba; ele se parece com isto, com a chave da sua organização:

Apache (.htaccess ou host virtual):

```
RewriteEngine On
RewriteRule ^\.well-known/com\.apple\.remotemanagement$
https://enterprise.cerberusapp.com/account-enroll/YOUR-KEY/discovery [R=302,L,QSA]
```

nginx:

```
location = /.well-known/com.apple.remotemanagement {
    return 302 https://enterprise.cerberusapp.com/account-enroll/YOUR-
KEY/discovery$is_args$args;
}
```

Em outros servidores ou serviços web (IIS, Cloudflare, painéis de controle de hospedagem), crie uma regra de redirecionamento (302) do mesmo caminho para a URL de descoberta com a opção que mantém ou encaminha a string de consulta.

Opção 3: Arquivo estático no seu site

Se você não puder adicionar um redirecionamento, publique um arquivo em *https://company.com/.well-known/com.apple.remotemanagement* (sem extensão de arquivo), servido com *Content-Type: application/json*. Copie o conteúdo dele da aba. Um arquivo estático não pode escolher o modo por dispositivo: ele usa o mesmo modo para iPhone, iPad e Mac. Para o User Enrollment, ele se parece com isto:

```
{"Servers":[{"Version":"mdm-byod","BaseURL":"https://enterprise.cerberusapp.com/account-
enroll/YOUR-KEY/byod"}]}
```

e para o Device Enrollment:

```
{"Servers":[{"Version":"mdm-adde","BaseURL":"https://enterprise.cerberusapp.com/account-enroll/YOUR-KEY/adde"}]}
```

> O modo do arquivo também deve ser o modo definido na aba para a família de dispositivos; caso contrário, o registro é recusado.

Verificar configuração

Em **Verificar configuração**, escolha um domínio e um dispositivo (iPhone ou Mac) e clique em **Verificar**: o Cerberus Enterprise pergunta ao domínio o que um dispositivo perguntaria e mostra a resposta, cada redirecionamento e um veredito. O domínio apontando para o Cerberus Enterprise significa que as opções 2 ou 3 funcionam; uma resposta de erro (como "not found") está tudo bem para a opção 1; uma página da web ou um arquivo apontando para outro lugar interrompe os dispositivos. A verificação também avisa quando um redirecionamento descarta a string de consulta ou o arquivo não é servido como *application/json*.

Chave de registro

As URLs de descoberta e registro contêm uma chave da sua organização. Se as URLs foram publicadas por engano, clique em **Regenerar chave**: as URLs antigas param de funcionar imediatamente, então atualize os redirecionamentos e arquivos estáticos nos seus sites. O Cerberus Enterprise registra a nova URL no Apple Business sozinho quando a opção 1 é usada.

Como os usuários se registram

1. iPhone e iPad: abra *Configurações → Geral → VPN & Gerenciamento de Dispositivos → Entrar na Conta de Trabalho ou Escola*. Mac: *Ajustes do Sistema → Geral → Gerenciamento de Dispositivos → Entrar* (no macOS 14: *Privacidade e Segurança → Perfis → Entrar*).
2. Digite a Managed Apple Account, ou o endereço de e-mail de trabalho do usuário no Cerberus (por exemplo *name@company.com*). Quando a Managed Apple Account do usuário é diferente do que foi digitado, o dispositivo então pede para entrar com essa conta.
3. Uma página do Cerberus Enterprise é aberta: toque em *Enviar o código* e insira o código de 6 dígitos recebido por e-mail. O código expira após 10 minutos; após 5 códigos errados, o usuário precisa fechar a página e entrar novamente.
4. Entre com a senha da Managed Apple Account (ou com a página de entrada da empresa quando o Apple Business está conectado ao Google Workspace ou ao Microsoft Entra ID) e permita o gerenciamento do dispositivo.

> Contas que não podem se registrar (domínio não verificado, nenhum usuário correspondente quando os usuários não são criados automaticamente, vários usuários com o mesmo endereço de e-mail) veem "Esta conta não está configurada para registro. Contate o administrador de TI." Os eventos ficam nos registros do sistema do painel.

Após o registro

- A página do dispositivo mostra a **Managed Apple Account** usada para se registrar e o tipo de registro (User Enrollment ou Account-driven Device Enrollment). Na lista de dispositivos, os dispositivos com User Enrollment mostram "User Enrollment".
- Nos dispositivos com User Enrollment, os comandos e configurações de política que a Apple não permite (apagar, localização, modo perdido, atualizações de SO, muitas restrições) não são oferecidos ou não são enviados. Os apps da App Store da política usam uma licença de usuário em vez de uma licença de dispositivo (veja **Apps em dispositivos pessoais** abaixo).
- Nos dispositivos com User Enrollment, os clipes da web aparecem na Tela de Início, mas não são listados em *Ajustes → Geral → VPN e Gerenciamento de Dispositivo*.
- O certificado MDM desses dispositivos não é renovado automaticamente e **Return to Service** não está disponível: antes de o certificado MDM expirar (um ano após o registro, veja a página do dispositivo), peça ao usuário para registrar o dispositivo novamente.
- Para sair do gerenciamento, o usuário sai da conta de trabalho no mesmo lugar das configurações, ou você cancela o registro do dispositivo no Cerberus Enterprise. Com o User Enrollment, apenas os apps, contas e dados de trabalho são removidos; os dados pessoais permanecem. Um dispositivo que se registra novamente aparece como um novo dispositivo.

> Logo após o registro, alguns perfis da política (certificados, redes Wi-Fi, web clips) podem ser informados como com falha com um erro desconhecido, e o dispositivo pode aparecer como **Não conforme** por um tempo. O dispositivo tenta novamente por conta própria e eles são instalados depois de um tempo, sem necessidade de ação. Não salve a política novamente nem registre o dispositivo novamente por causa disso.

Apps em dispositivos pessoais

iPhones e iPads registrados com User Enrollment não têm número de série, então o Apps and Books não pode dar a eles uma licença de dispositivo. O Cerberus Enterprise dá aos apps da App Store da política deles uma **licença de usuário**: a licença vai para a Managed Apple Account conectada no dispositivo. Nada muda na política: a mesma política atende dispositivos da empresa e pessoais, e o Cerberus escolhe o tipo de licença para cada dispositivo.

- **Automático**: no primeiro registro, o Cerberus registra a Managed Apple Account no Apps and Books e então pede à Apple uma licença de cada app da App Store da política. Apps gratuitos também precisam de uma licença; a Apple dá licenças ilimitadas para eles. Um app pago usa uma licença por Managed Apple Account, compartilhada por todos os dispositivos pessoais dessa conta.
- **Mesma organização**: as Managed Apple Accounts e o token do Apps and Books do Cerberus Enterprise devem pertencer à mesma organização do Apple Business, e os apps devem estar na biblioteca do local do token.
- **Licença primeiro**: um app só é enviado ao dispositivo depois que a Apple confirma a licença dele, geralmente em alguns minutos. Até lá, o painel **Aplicativos** do dispositivo o mostra como **Aguardando uma licença de usuário**, com o motivo.
- **Aviso de instalação**: dispositivos pessoais nunca são supervisionados, então o iOS pergunta ao usuário antes de instalar cada app, incluindo o app **Cerberus Enterprise**, que o Cerberus também instala nesses dispositivos (**Instalar** ou **Cancelar**); não é necessário entrar com uma Conta Apple. Se o usuário cancelar, o app mostra **Aguardando a aprovação do usuário para a instalação**: use **Solicitar novamente** na página do dispositivo para mostrar o aviso outra vez. Apps instalados como **Obrigatório** não podem ser excluídos pelo usuário.
- **Apps instalados antes do registro**: a Apple não permite que a organização assuma um app que o usuário instalou pessoalmente em um dispositivo registrado com User Enrollment. Peça ao usuário para excluir a cópia dele antes de se registrar, ou exclua-a e use **Solicitar novamente** na página do dispositivo: a organização então instala a cópia gerenciada.
- **Sair do gerenciamento**: quando o dispositivo tem o registro cancelado, o iOS remove os apps gerenciados e os dados deles. Uma licença é liberada quando nenhum outro dispositivo registrado da mesma Managed Apple Account precisa dela, por exemplo quando o app sai da política ou o último dispositivo tem o registro cancelado; as licenças que ninguém mais precisa são liberadas pela verificação diária dentro de um dia.

> Quando a Apple não consegue atribuir uma licença, por exemplo porque um app pago não tem mais licenças, o app mostra **Falha na licença de usuário** com a mensagem da Apple. Adicione licenças no Apple Business e use **Solicitar novamente** na página do dispositivo; o Cerberus também tenta novamente sozinho na verificação diária. A linha acima da lista de apps mostra a Managed Apple Account e o status do usuário do Apps and Books dela; o mesmo status fica na página do usuário.

> As licenças de usuário são usadas somente em iPhones e iPads: em Macs registrados com o Registro de Usuário, os apps da App Store da política não são instalados. Livros e Contas Apple pessoais não são compatíveis.

Revision #6
Created 2026-11-10 15:17:37 UTC by Admin
Updated 2026-11-12 09:57:15 UTC by Admin