Provisionamento de Dispositivos - Android

- Dispositivos compatíveis
- Tokens de registro
- Dispositivos de propriedade pessoal
- Dispositivos da empresa para uso profissional e pessoal
- Dispositivos da empresa somente para uso profissional
- Zero-touch
- Autenticação do Google no registro

Dispositivos compatíveis

Em geral, qualquer dispositivo com Android 6 ou superior e Google Play Services é compatível com o Cerberus Enterprise.

Para uma melhor experiência do usuário, sugerimos usar dispositivos que atendam aos requisitos do Android Enterprise Recommended.

> Alguns recursos são limitados a versões específicas do Android ou podem se comportar de forma diferente entre versões do sistema operacional. Para obter mais informações sobre um recurso específico, consulte a seção Políticas da documentação.

O Cerberus Enterprise oferece suporte a dispositivos da empresa e de propriedade pessoal, além de dois modos de gerenciamento: proprietário do dispositivo e proprietário do perfil.

Dispositivos de propriedade pessoal podem ser gerenciados por meio de um **perfil de trabalho**. Isso possibilita uma solução BYOD ao manter os dados e apps de trabalho dos funcionários separados dos dados e apps pessoais, melhorando a segurança e a privacidade. Esta opção é adequada para dispositivos já pertencentes aos funcionários que você deseja registrar na sua organização para uso profissional.

Dispositivos da empresa também podem ser gerenciados por meio de um perfil de trabalho, mas você também pode escolher a opção **totalmente gerenciado**, que permite um controle mais rigoroso sobre o dispositivo. Dispositivos da empresa com perfil de trabalho são adequados quando você fornece dispositivos corporativos aos funcionários para uso profissional, permitindo ainda o uso pessoal. Dispositivos totalmente gerenciados são mais adequados para dispositivos que devem ser usados apenas para trabalho ou para **dispositivos dedicados** (COSU, corporate-owned single-use), como quiosques.

Para obter mais informações sobre o provisionamento de dispositivos, consulte a página Visão geral do provisionamento de dispositivos.

Tokens de registro

O Cerberus Enterprise usa tokens de registro para iniciar o processo de registro (provisionamento) de dispositivos Android. O token selecionado define a política inicial aplicada aos dispositivos registrados e influencia quais modos de provisionamento são permitidos.

> A aba de tokens de registro do Android só fica disponível após concluir **Configuração do Android Management**.

Onde encontrar tokens de registro

No painel, abra **Tokens de registro**. Dependendo da configuração da sua conta, a página pode mostrar várias abas (tokens do Android, registro com login do Google, registro manual da Apple e Registro Automatizado de Dispositivos da Apple).

> Se o seu ambiente corporativo Android for respaldado por um domínio Google gerenciado (Google Workspace), o painel também pode mostrar uma aba **Autenticar usando o Google Enrollment**. Para detalhes sobre como habilitá-la e usá-la, consulte **Autenticar usando o Google Enrollment**.

Lista de tokens de registro (Android)

A aba de tokens do Android mostra uma tabela com todos os tokens. Clicar em uma linha abre a página de detalhes do token.

Colunas

- **Status**: **Ativo** (os dispositivos podem se registrar com o token), **Expirado** (a data de expiração já passou) ou **Esgotado** (um token de uso único que já foi usado).

- **Política**: a política atribuída ao token (a dica de ferramenta mostra o id da política). **Política excluída** significa que a política foi excluída após a criação do token.
- **Usuário**: usuário opcional pré-atribuído aos dispositivos registrados com o token. **Usuário excluído** significa que o usuário foi excluído após a criação do token.
- **Registros**: quantos dispositivos se registraram com o token, exibido como **n / 1** para um token de uso único.
- **Uso pessoal**: Permitido / Não permitido / Dispositivo dedicado.
- **Criação**: quando o token foi criado. A tabela mostra os tokens mais recentes primeiro.
- **Expiração**: data/hora de expiração ou **Nunca**.
- **Código de registro**: o código do token, aquele que você digita no dispositivo quando o registra sem um código QR.

Ações

- Cada linha tem uma ação de exclusão (**Excluir token de registro**). A exclusão fica desabilitada quando a licença está expirada.
- A tabela oferece suporte à seleção de várias linhas: você pode ativar o modo de seleção, selecionar vários tokens e excluí-los com **Excluir tokens selecionados**.
- Use a ação de atualização para recarregar a lista. A tabela é paginada (10/25/50 itens por página).

Criar um novo token de registro

Na aba de tokens do Android, clique em **Novo token de registro** para abrir a página de criação de token. Se sua licença estiver expirada, o botão de criação fica desabilitado.

Opções do token

1. Política

Obrigatório. A política aplicada automaticamente a todos os dispositivos registrados com este token. Selecione uma das suas **políticas do Android**. Se você ainda não tiver nenhuma política, crie uma primeiro.

2. Usuário

Opcional. Se definido, os dispositivos recém-registrados são associados automaticamente a este usuário.

3. Uso pessoal

Controla se o uso pessoal é permitido em um dispositivo provisionado com este token de registro:

- **Permitido**: adequado para dispositivos de propriedade pessoal (perfil de trabalho) e dispositivos da empresa para uso profissional e pessoal.
- **Não permitido**: adequado para dispositivos da empresa somente para uso profissional (totalmente gerenciados).
- **Dispositivo dedicado**: adequado para dispositivos de quiosque/dedicados (o dispositivo não é associado a um único usuário).

4. Usos permitidos

Selecione se o token pode ser usado várias vezes (**Várias vezes**) ou apenas uma vez (**Apenas uma vez**).

5. Expiração

Selecione a unidade de expiração (**Minutos**, **Horas**, **Dias** ou **Nunca**). Quando não definida como Nunca, informe o valor de expiração. O intervalo permitido depende da unidade selecionada e pode chegar a 10.000 dias.

6. Autenticação do Google

Controla se o usuário deve se autenticar com uma conta Google durante o registro do dispositivo:

- **Não especificado**: a configuração de autenticação do Google no nível da empresa é usada para determinar se o usuário precisa se autenticar com o Google durante o registro.
- **Opcional**: o usuário pode optar por ignorar a autenticação do Google durante o registro.
- **Obrigatório**: o usuário deve se autenticar com uma conta Google para prosseguir com o registro.

Quando **Obrigatório** está selecionado, um campo opcional **E-mail da conta obrigatória** aparece. Se definido, o usuário deve se autenticar com essa conta Google específica durante o registro.

Opções de provisionamento (somente código QR)

Essas opções adicionais são incorporadas ao código QR e aplicadas durante o provisionamento de dispositivos totalmente gerenciados registrados pela leitura do código QR. Elas não se aplicam a perfis de trabalho nem a dispositivos registrados usando a URL de registro ou o Token.

Configuração de Wi-Fi

Use isto para permitir que um dispositivo se conecte automaticamente ao Wi-Fi durante o provisionamento, para que ele possa baixar e inicializar o app de gerenciamento. Os campos disponíveis incluem **SSID**, **SSID oculto**, **Segurança** e (quando necessário) **Frase secreta**.

Você também pode configurar um proxy HTTP (**Proxy**) e, dependendo do modo, definir **Host**/**Porta**, **URI PAC** e **Host de exceção do proxy**.

Outras opções

As opções adicionais incluem **Idioma**, **Fuso horário** e **Ignorar criptografia**.

Detalhes do token de registro

Ao abrir um token, a página de detalhes mostra a configuração do token e as informações de uso:

- **Status**, **Expiração**, **Uso**, **Uso pessoal**, **Usos permitidos** e (quando definido) **Autenticação do Google** com o campo opcional **E-mail da conta obrigatória**.
- **Token**: o valor bruto do token de registro (copiável).
- **URL de registro**: uma URL de registro do Google Android Enterprise (copiável e enviável por e-mail).
- **Código QR**: exibido no lado direito da página, usado para registrar dispositivos totalmente gerenciados.

> Para procedimentos de provisionamento passo a passo, siga os guias de registro do Android: **Dispositivos de propriedade pessoal**, **Dispositivos da empresa para uso profissional e pessoal**, **Dispositivos da empresa somente para uso profissional** e **Zero-touch**.

Dispositivos de propriedade pessoal

Dispositivos de propriedade dos funcionários podem ser configurados com um **perfil de trabalho**. Um perfil de trabalho oferece um espaço independente para apps e dados de trabalho, separado dos apps e dados pessoais. A maioria das políticas de apps, dados e outras políticas de gerenciamento se aplica apenas ao perfil de trabalho, enquanto os apps e dados pessoais dos funcionários permanecem privados.
Para configurar um perfil de trabalho em um dispositivo de propriedade pessoal, use um dos seguintes métodos de provisionamento (verifique se o token de registro tem ***Uso pessoal*** definido como **Permitido**):

Link do token de registro

Versão do Android
6.0+

Você pode fornecer a URL de registro aos usuários finais. Quando um usuário final abre o link no dispositivo, ele é guiado pela configuração do perfil de trabalho.

Adicionar perfil de trabalho em "*Configurações*"

Versão do Android
6.0+

Para configurar um perfil de trabalho no dispositivo, o usuário pode abrir o app ***Configurações*** e usar a barra de pesquisa para encontrar e tocar na opção ***Configurar seu perfil de trabalho***.

Se a pesquisa não funcionar, o local desta opção pode variar. Aqui estão algumas possibilidades:

- *Configurações -> Serviços e preferências do Google -> Todos os serviços -> Configurar seu perfil de trabalho*.
- *Configurações -> Google -> Configurar & restaurar -> Configurar seu perfil de trabalho*.

Estas etapas iniciam um assistente de configuração que baixa o *Android Device Policy* no dispositivo. Em seguida, o usuário será solicitado a escanear um código QR ou inserir manualmente um token de registro para concluir a configuração do perfil de trabalho.

Baixar o Android Device Policy

Versão do Android
6.0+

Para configurar um perfil de trabalho no dispositivo, o usuário pode baixar o Android Device Policy na Google Play Store. Depois que o app for instalado, o usuário será solicitado a escanear um código QR ou inserir manualmente um token de registro para concluir a configuração do perfil de trabalho.

iPhones e iPads pessoais

iPhones e iPads pessoais (e Macs) são registrados com o **User Enrollment** da Apple: o usuário entra com sua Conta Apple Gerenciada nos ajustes do dispositivo, e apenas os apps, contas e dados de trabalho são gerenciados. Em iPhones e iPads, os apps da App Store da política e o app **Cerberus Enterprise** são instalados com uma licença de usuário dessa conta. A localização de dispositivos pessoais é coletada somente se a política deles ativar **Localização e geocercas em dispositivos pessoais** e o usuário permitir. Leia **Registro orientado pela conta Apple**.

Dispositivos da empresa para uso profissional e pessoal

Configurar um dispositivo da empresa com um **perfil de trabalho** permite usar o dispositivo tanto para fins profissionais quanto pessoais. Em dispositivos da empresa com perfis de trabalho:

- A maioria das políticas de apps, dados e outras políticas de gerenciamento se aplica apenas ao perfil de trabalho.
- Os perfis pessoais dos funcionários permanecem privados. No entanto, as empresas podem aplicar certas políticas para todo o dispositivo e políticas de uso pessoal.
- As empresas podem usar *Escopo de bloqueio* para aplicar ações de conformidade em um dispositivo inteiro ou apenas no perfil de trabalho.
- O cancelamento de registro e os comandos de dispositivo se aplicam ao dispositivo inteiro.

Para configurar um dispositivo da empresa com um perfil de trabalho, use um dos seguintes métodos de provisionamento (verifique se o token de registro tem **Uso pessoal** definido como **Permitido**):

Método de código QR

Versão do Android
8.0+

Em um dispositivo novo ou redefinido de fábrica, o usuário (normalmente um administrador de TI) toca a tela seis vezes no mesmo ponto. Isso faz com que o dispositivo solicite ao usuário que escaneie um código QR.

Dispositivos da empresa somente para uso profissional

Gerenciamento completo do dispositivo é adequado para dispositivos da empresa destinados exclusivamente a fins profissionais. As empresas podem gerenciar todos os apps do dispositivo e aplicar toda a gama de políticas e comandos da API Android Management.
Também é possível bloquear um dispositivo (por meio de política) em um único app ou em um pequeno conjunto de apps para atender a uma finalidade ou caso de uso específico. Esse subconjunto de dispositivos totalmente gerenciados é chamado de **dispositivos dedicados**.
Para configurar o gerenciamento completo em um dispositivo da empresa, use um dos seguintes métodos de provisionamento (verifique se o token de registro tem **Uso pessoal** definido como **Não permitido**):

Método de código QR

Versão do Android
7.0+

Em um dispositivo novo ou redefinido de fábrica, o usuário (normalmente um administrador de TI) toca a tela seis vezes no mesmo ponto. Isso faz com que o dispositivo solicite ao usuário que escaneie um código QR.

Método do identificador DPC

Versão do Android
5.1+

Se o Android Device Policy não puder ser adicionado por código QR, um usuário ou administrador de TI pode seguir estas etapas para provisionar um dispositivo totalmente gerenciado ou dedicado:

1. Siga o assistente de configuração em um dispositivo novo ou redefinido de fábrica.
2. Insira os dados de login do Wi-Fi para conectar o dispositivo à internet.
3. Quando solicitado a entrar, insira **afw#setup**, o que baixa o Android Device Policy.
4. Escaneie um código QR ou insira manualmente um token de registro para provisionar o dispositivo.

Zero-touch

Os administradores de TI podem provisionar dispositivos da empresa usando o método de registro Zero-touch, descrito em Registro Zero-touch para administradores de TI. Quando um dispositivo é ligado pela primeira vez, ele é automaticamente forçado a usar as configurações definidas pelo administrador de TI.

Os administradores de TI podem pré-configurar dispositivos comprados de revendedores autorizados e gerenciá-los usando o painel do Cerberus Enterprise. Para vincular sua conta Zero-touch, vá para a seção **Zero-touch** no painel e siga as instruções.

Versão do Android	Perfil de trabalho	Dispositivo totalmente gerenciado	Dispositivo dedicado
8.0+ (Pixel 7.1+)	✓	✓	✓

Autenticação do Google no registro

A autenticação do Google no registro (também chamada de **Autenticação do Google para Registro**) permite que os usuários se autentiquem com a conta do Google Workspace durante o registro de dispositivos Android.

> Este recurso está disponível apenas para ambientes corporativos Android respaldados por um domínio Google gerenciado (Google Workspace).

Onde encontrá-lo

No painel, abra **Tokens de registro** e selecione a aba **Autenticar usando o Google Enrollment** . A aba só é exibida quando o Android Management está configurado e a integração com o Google Workspace está disponível para sua empresa.

Ativar (ou desativar) a autenticação do Google

A autenticação do Google é ativada no **Console do Google Admin**. Depois de alterar a configuração, volte ao Cerberus Enterprise e use **Atualizar status** para recarregar a configuração atual.

1. Entre no seu **Console do Google Admin** com uma conta de administrador.
2. Abra **Dispositivos**.
3. Vá para **Dispositivos móveis & endpoints** → **Configurações** → **Integrações de terceiros**.
4. Localize a **integração Android EMM** do Cerberus Enterprise e abra-a.
5. Clique em **Gerenciar provedores EMM**.
6. Ative ou desative **Autenticar usando o Google** para habilitar ou desabilitar a autenticação do Google no registro.

7. Clique em **Salvar**.
8. Volte ao painel do Cerberus Enterprise e clique em **Atualizar status** na aba **Autenticar usando o Google Enrollment**.

Token de registro para autenticação do Google

Quando a autenticação do Google está habilitada, o painel mostra um token de registro dedicado usado para esse modo de registro. A página pode mostrar um **código QR**, um valor de **Token de registro** e uma **URL de registro** (copiável e enviável por e-mail).

Opções principais

- **Permitir uso pessoal**: controla se o token pode registrar dispositivos para uso profissional e pessoal (cenários de perfil de trabalho) ou somente para uso profissional (cenários totalmente gerenciados/dedicados).
- **Política padrão de fallback**: a política aplicada quando o usuário que está registrando não tem uma política padrão de autenticação do Google específica atribuída.

Interação com políticas

A configuração de política **Autenticação de configuração da conta corporativa** (workAccountSetupConfig.authenticationType) controla como os usuários se autenticam durante a configuração da conta corporativa, mas a configuração **Autenticar usando o Google** do Console do Google Admin e o tipo de token de registro ainda podem exigir autenticação.

Para dispositivos já registrados, esta política se aplica apenas se o dispositivo for gerenciado por uma conta gerenciada do Google Play (ou seja, registrado sem **Autenticar usando o Google Enrollment**).

> Algumas ações (por exemplo, alterar as opções do token) podem ficar desabilitadas quando a licença está expirada.

Registrar um dispositivo

Durante o registro, o usuário é solicitado a se autenticar com a conta do Google Workspace. Após um registro bem-sucedido, o dispositivo é associado ao usuário autenticado.

Perfil de trabalho (dispositivos de propriedade pessoal)

- Compartilhe a **URL de registro** com o usuário. Quando o usuário a abrir no dispositivo Android, ele será guiado pela configuração do perfil de trabalho e pela autenticação do Google.
- Como alternativa, o usuário pode começar nas Configurações do Android e escolher o fluxo de configuração do perfil de trabalho, depois escanear o código QR ou inserir o token de registro quando solicitado.

Dispositivos da empresa

- **Método de código QR**: em um dispositivo novo ou redefinido de fábrica, toque a tela várias vezes no mesmo ponto até que o aviso de código QR apareça, depois escaneie o código QR exibido no painel.
- **Método do identificador DPC** (quando a leitura de QR não estiver disponível): siga o assistente de configuração, conecte-se ao Wi-Fi e, quando solicitado a entrar, insira **afw#setup** e prossiga escaneando o código QR ou inserindo o token de registro. Quando solicitado, autentique-se com a conta do Google Workspace.

Para procedimentos gerais de provisionamento do Android (perfil de trabalho versus totalmente gerenciado), consulte as páginas padrão de registro do Android neste manual.