Provisionamento de Dispositivos - Android

- Dispositivos compatíveis
- Tokens de inscrição
- Dispositivos de propriedade pessoal
- Dispositivos corporativos para uso no trabalho e pessoal
- Dispositivos de propriedade da empresa, destinados apenas para uso profissional
- Configuração simplificada
- Autentique-se usando o cadastro do Google

Dispositivos compatíveis

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

Para uma melhor experiência do usuário, recomendamos o uso de dispositivos que atendam aos requisitos do Android Enterprise Recommended.

> Algumas funcionalidades são limitadas a versões específicas do Android ou podem ter um comportamento diferente em diferentes versões do sistema operacional. Para mais informações sobre uma funcionalidade específica, consulte a seção Políticas da documentação.

O Cerberus Enterprise suporta tanto dispositivos pertencentes à empresa quanto dispositivos pessoais, e dois modos de gerenciamento: proprietário do dispositivo e proprietário do perfil.

Dispositivos pertencentes a funcionários podem ser gerenciados através de um **perfil de trabalho**. Isso possibilita uma solução BYOD (Bring Your Own Device), mantendo os dados e aplicativos de trabalho dos funcionários separados dos dados e aplicativos pessoais, melhorando tanto a segurança quanto a privacidade. Essa opção é adequada para dispositivos já pertencentes a funcionários que você deseja inscrever em sua organização para uso profissional.

Dispositivos corporativos também podem ser gerenciados por meio de um perfil de trabalho, mas você também pode optar pela opção de **gerenciamento completo**, que permite um controle mais rígido sobre o dispositivo. Dispositivos corporativos com um perfil de trabalho são adequados quando você fornece dispositivos corporativos aos funcionários para uso profissional, permitindo, ao mesmo tempo, o uso pessoal. Dispositivos com gerenciamento completo são mais adequados para dispositivos que devem ser usados apenas para trabalho, ou para **dispositivos dedicados** (COSU, dispositivos corporativos de uso único), como quiosques.

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

Tokens de inscrição

O Cerberus Enterprise utiliza tokens de inscrição para iniciar o processo de inscrição (provisionamento) de dispositivos Android. O token que você seleciona define a política inicial aplicada aos dispositivos inscritos e influencia quais modos de provisionamento são permitidos.

> A guia de tokens de inscrição para Android está disponível somente após a conclusão da **Configuração do gerenciamento Android**.

Onde encontrar os tokens de inscrição

No painel, abra **Tokens de inscrição**. Dependendo da configuração da sua conta, a página pode exibir várias abas (tokens Android, inscrição com o Google, inscrição manual da Apple e inscrição automatizada de dispositivos da Apple).

> Se seu ambiente Android Enterprise for gerenciado por um domínio Google (Google Workspace), o painel também pode exibir uma aba de **Autenticação via Inscrição com o Google**. Para obter detalhes sobre como habilitar e usar essa opção, consulte **Autenticação via Inscrição com o Google**.

Lista de tokens de inscrição (Android)

A aba "Tokens Android" exibe uma tabela com todos os tokens. Clicar em uma linha abre a página com os detalhes do token.

Colunas

- **Id**: identificador de token interno.
- **Status**: **Disponível**, **Utilizado** (token de uso único já utilizado) ou **Expirado**.
- **Validade**: data e hora de expiração, ou **Nunca**.
- **Política**: a política atribuída ao token (a dica de ferramenta da interface do usuário também mostra o ID da política).
- **Uso pessoal**: Permitido / Não permitido / Dispositivo dedicado.
- **Usos permitidos**: Uso único ou múltiplo.
- **Usuário**: usuário opcional, pré-atribuído aos dispositivos registrados com o token.

Ações

- Cada linha possui uma ação de exclusão (**Excluir token de inscrição**). A exclusão é desabilitada quando a licença expirou.
- A tabela suporta a seleção de múltiplas linhas: você pode ativar o modo de seleção, selecionar vários tokens e excluí-los com **Excluir tokens selecionados**.
- Use a ação "atualizar" para recarregar a lista. A tabela possui paginação (10/25/50 itens por página).

Criar um novo token de inscrição

Na guia "Tokens Android", clique em **Novo token de inscrição**. para abrir a página de criação do token. Se sua licença expirou, o botão de criação fica desabilitado.

Opções de token

1. Política

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

2. Usuário

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

3. Uso pessoal

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

- **Permitido**: adequado para dispositivos pessoais (perfil de trabalho) e dispositivos corporativos para uso profissional e pessoal.
- **Não permitido**: adequado para dispositivos corporativos, destinados apenas para uso profissional (gerenciamento total).
- **Dispositivo dedicado**: adequado para dispositivos tipo quiosque ou dedicados (o dispositivo não está 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. Validade

Selecione a unidade de validade (**Minutos**, **Horas**, **Dias**, ou **Nunca**. Quando não definido como Nunca, insira o valor da validade. A faixa permitida depende da unidade selecionada e pode chegar a 10.000 dias.

Opções de provisionamento (apenas código QR)

Essas opções adicionais estão embutidas no código QR e são aplicadas durante o provisionamento de dispositivos totalmente gerenciados, inscritos por meio da leitura do código QR. Elas não se aplicam a perfis de trabalho ou dispositivos inscritos usando a URL de inscrição ou o token.

Configuração de Wi-Fi

Use this to let a device automatically connect to Wi-Fi during provisioning, so it can download and initialize the management app. Available fields include **SSID**, **SSID oculto**, **Segurança**, and (when needed) **Frase de segurança**.

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

Outras opções

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

Detalhes do token de inscrição

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

- **Status**, **Validade**, **Uso**, **Uso pessoal**, e **Usos permitidos**.
- **Token**: o valor bruto do token de inscrição (copiável).
- **URL de inscrição**: um URL de inscrição do Google Android Enterprise (copiável e enviável por e-mail).
- **Código QR**: exibido no lado direito da página, usado para inscrever dispositivos totalmente gerenciados.

> Para procedimentos de configuração passo a passo, siga os guias de inscrição para Android: **Dispositivos de propriedade pessoal**, **Dispositivos de propriedade da empresa para uso profissional e pessoal**, **Dispositivos de propriedade da empresa para uso profissional exclusivo** e **Inscrição automática**.

Dispositivos de propriedade pessoal

Dispositivos pertencentes a funcionários podem ser configurados com um **perfil de trabalho**. Um perfil de trabalho oferece um espaço isolado para aplicativos e dados corporativos, separado de aplicativos e dados pessoais. A maioria das políticas de gerenciamento de aplicativos, dados e outros recursos se aplica apenas ao perfil de trabalho, enquanto os aplicativos e dados pessoais dos funcionários permanecem privados.
Para configurar um perfil de trabalho em um dispositivo de propriedade pessoal, utilize um dos seguintes métodos de provisionamento (certifique-se de que o token de inscrição tenha a opção ***Uso pessoal*** definida como **Permitido**):

Link do token de inscrição

Versão Android
6.0+

Você pode fornecer a URL de inscrição para os usuários finais. Quando um usuário final abrir o link em seu dispositivo, ele será guiado pela configuração do perfil de trabalho.

Adicione o perfil de trabalho a partir de "*Configurações*

Versão Android
6.0+

Para configurar um perfil de trabalho em seu dispositivo, o usuário pode abrir o aplicativo ***Configurações*** do dispositivo, depois usar a barra de pesquisa para encontrar e tocar na opção ***Configurar seu perfil de trabalho***.

Se a busca não for bem-sucedida, a localização desta opção pode variar. Aqui estão algumas possibilidades:

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

Esses passos iniciam um assistente de configuração que baixa *Política de Dispositivo Android* no dispositivo. Em seguida, o usuário será solicitado a digitalizar um código QR ou inserir manualmente um token de inscrição para concluir a configuração do perfil de trabalho.

Baixar Android Device Policy

Versão Android
6.0+

Para configurar um perfil de trabalho no dispositivo, o usuário pode baixar a <x id="START_EMPHASISED_TEXT" ctype="x-em" equiv-text=""/>Política de Dispositivo Android<x id="CLOSE_EMPHASISED_TEXT" ctype="x-em" equiv-text=""/> da Google Play Store. Após a instalação do aplicativo, o usuário será solicitado a digitalizar um código QR ou inserir manualmente um token de inscrição para concluir a configuração do perfil de trabalho.

Dispositivos corporativos para uso no trabalho e pessoal

Configurar um dispositivo corporativo com um **perfil de trabalho** permite que o dispositivo seja usado tanto para fins profissionais quanto pessoais. Em dispositivos corporativos com perfis de trabalho:

- A maioria das políticas de gerenciamento de aplicativos, dados e outros recursos se aplica apenas ao perfil de trabalho.
- Os perfis pessoais dos funcionários permanecem privados. No entanto, as empresas podem impor certas políticas de dispositivo e políticas de uso pessoal.
- As empresas podem usar o *Escopo de bloqueio* para aplicar ações de conformidade em todo o dispositivo ou apenas no perfil de trabalho.
- A desativação do dispositivo e os comandos do dispositivo se aplicam a todo o dispositivo.

Para configurar um dispositivo corporativo com um perfil de trabalho, use um dos seguintes métodos de provisionamento (certifique-se de que o token de inscrição tenha **uso pessoal** definido como **Permitido**):

Método de leitura de código QR

Versão Android
8.0+

Em um dispositivo novo ou com as configurações de fábrica restauradas, o usuário (geralmente um administrador de TI) toca na tela seis vezes no mesmo local. Isso faz com que o dispositivo solicite ao usuário que escaneie um código QR.

Dispositivos de propriedade da empresa, destinados apenas para uso profissional

O gerenciamento completo do dispositivo é adequado para dispositivos de propriedade da empresa, destinados exclusivamente para fins de trabalho. As empresas podem gerenciar todos os aplicativos no dispositivo e podem aplicar todo o conjunto de políticas e comandos da Android Management API.
Também é possível restringir um dispositivo (por meio de políticas) a um único aplicativo ou a um pequeno conjunto de aplicativos para atender a um propósito ou caso de uso específico. Este subconjunto de dispositivos totalmente gerenciados é chamado de **dispositivos dedicados**.
Para configurar o gerenciamento completo em um dispositivo de propriedade da empresa, use um dos seguintes métodos de provisionamento (certifique-se de que o token de inscrição tenha a opção **Uso pessoal** definida como **Não permitido**):

Método de leitura de código QR

Versão Android
7.0+

Em um dispositivo novo ou com as configurações de fábrica restauradas, o usuário (geralmente um administrador de TI) toca na tela seis vezes no mesmo local. Isso faz com que o dispositivo solicite ao usuário que escaneie um código QR.

Método de identificação do DPC

Versão Android
5.1+

Se a política de dispositivo Android não puder ser adicionada por meio de código QR, um usuário ou administrador de TI pode seguir estas etapas para configurar um dispositivo totalmente gerenciado ou dedicado:

1. Siga o assistente de configuração em um dispositivo novo ou com as configurações de fábrica restauradas.
2. Insira as credenciais de login do Wi-Fi para conectar o dispositivo à internet.
3. Ao ser solicitado a fazer login, insira **afw#setup**, que baixa a política do dispositivo Android.
4. Escaneie um código QR ou insira manualmente um token de inscrição para configurar o dispositivo.

Configuração simplificada

Administradores de TI podem configurar dispositivos corporativos usando o método de inscrição simplificada, conforme descrito em Inscrição simplificada para administradores de TI. Quando um dispositivo é ligado pela primeira vez, ele é automaticamente configurado de acordo com as configurações definidas pelo administrador de TI.

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

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

Autentique-se usando o cadastro do Google

Autentique-se usando o cadastro do Google (também conhecido como **Autenticação do Google para Cadastro**), que permite que os usuários autentiquem-se com sua conta do Google Workspace durante o cadastro do dispositivo Android.

> Este recurso está disponível apenas para empresas Android que utilizam um domínio gerenciado do Google (Google Workspace).

Onde encontrar

No painel, abra **Tokens de inscrição** e selecione a guia **Autenticar usando inscrição do Google**. A guia é exibida apenas quando o Android Management está configurado e a integração com o Google Workspace está disponível para sua empresa.

Habilite (ou desabilite) a autenticação usando a conta do Google

A autenticação via Google está habilitada no console de administração do **Google**. Após alterar essa configuração, volte ao Cerberus Enterprise e use **Atualizar Status** para recarregar a configuração atual.

1. Faça login no seu **console de administração do Google** com uma conta de administrador.
2. Abra **Dispositivos**.
3. Vá para **Dispositivos móveis e endpoints → Configurações → Integrações de terceiros**.
4. Encontre a **integração com o EMM para Android** do Cerberus Enterprise e abra-a.
5. Clique em **Gerenciar provedores EMM**.
6. Ative ou desative **a autenticação usando o Google** para configurar a autenticação com o Google para o processo de inscrição.
7. Clique em **Salvar**.
8. Retorne ao painel do Cerberus Enterprise e clique em **Atualizar Status** na guia **Autenticar com Inscrição do Google**.

Token de inscrição para autenticação com o Google

Quando a autenticação com o Google está habilitada, o painel exibe um token de inscrição dedicado, usado para este modo de inscrição. A página pode mostrar um **código QR**, um **valor do token de inscrição** e uma **URL de inscrição** (que pode ser copiada e enviada por e-mail).

Opções principais

- **Permitir uso pessoal**: controla se o dispositivo pode ser cadastrado para uso profissional e pessoal (cenários de perfil de trabalho) ou apenas para uso profissional (cenários totalmente gerenciados/dedicados).
- **Política Padrão Alternativa**: a política aplicada quando o usuário que está sendo cadastrado não possui uma política padrão do Google Authentication atribuída.

Interação com a política

A configuração de política "**Autenticação na configuração da conta de trabalho**" (workAccountSetupConfig.authenticationType) controla como os usuários autenticam durante a configuração da conta de trabalho, mas a configuração do console de administração do Google "**Autenticar com o Google**" e o tipo de token de inscrição ainda podem exigir autenticação.

Para dispositivos já inscritos, esta política se aplica apenas se o dispositivo for gerenciado por uma conta do Google Play corporativa (ou seja, inscrito sem **autenticação via Google**).

> Algumas ações (por exemplo, alterar as opções de token) podem ser desabilitadas quando a licença estiver expirada.

Cadastrar um dispositivo

Durante o processo de cadastro, o usuário é solicitado a autenticar com sua conta do Google Workspace. Após o cadastro bem-sucedido, o dispositivo é associado ao usuário autenticado.

Perfil de trabalho (dispositivos de propriedade pessoal)

- Compartilhe o **link de inscrição** com o usuário. Quando o usuário abrir o link em seu dispositivo Android, ele será guiado pelo processo de configuração do perfil de trabalho e

pela autenticação do Google.
- Alternativamente, o usuário pode iniciar pelo menu de Configurações do Android e escolher o fluxo de configuração do perfil de trabalho, e então escanear o código QR ou inserir o token de inscrição quando solicitado.

Dispositivos pertencentes à empresa

- **Método de código QR**: em um dispositivo novo ou redefinido para as configurações de fábrica, toque na tela várias vezes no mesmo local até que o prompt do código QR apareça, e então escaneie o código QR exibido no painel.
- **Método de identificação DPC** (quando a leitura de QR Code não está disponível): siga o assistente de configuração, conecte-se ao Wi-Fi e, quando solicitado a fazer login, insira **afw#setup** e prossiga escaneando o código QR ou inserindo o token de inscrição. Quando solicitado, autentique-se com a conta do Google Workspace.

Para procedimentos gerais de configuração do Android (perfil de trabalho versus gerenciamento completo), consulte as páginas de inscrição padrão do Android neste manual.