

Manual do Usuário

Documentação do Cerberus Enterprise MDM

- [Introdução](#)
- [Configuração](#)
 - [Configuração do Android Management](#)
 - [Configuração do Apple Management \(APNs\)](#)
- [Visão geral do provisionamento de dispositivos](#)
- [Provisionamento de Dispositivos - Android](#)
 - [Dispositivos compatíveis](#)
 - [Tokens de inscrição](#)
 - [Dispositivos de propriedade pessoal](#)
 - [Dispositivos de propriedade da empresa para uso profissional e pessoal](#)
 - [Dispositivos de propriedade da empresa para uso exclusivo de trabalho](#)
 - [Zero-touch](#)
 - [Autenticação via Inscrição do Google](#)
- [Provisionamento de Dispositivos - Apple](#)
 - [Visão geral do provisionamento Apple](#)
 - [Apple manual enrollment \(Perfil de Registro\)](#)
 - [Apple Automated Device Enrollment \(ADE\)](#)
- [Visão geral das políticas](#)
- [Políticas - Android](#)
 - [Resumo](#)
 - [Gerenciamento de apps](#)
 - [Modo quiosque](#)
 - [Segurança](#)

- [Multimídia](#)
- [Celular](#)
- [Rede](#)
- [Sistema](#)
- [Localização e cercas virtuais](#)
- [Gerenciamento de usuários](#)
- [Uso pessoal](#)
- [Políticas entre perfis](#)
- [Relatório de status](#)
- [Diversos](#)
- [Regras de aplicação de política](#)
- [Políticas - Apple](#)
 - [Políticas da Apple](#)
 - [Política da Apple: Código de acesso](#)
 - [Política da Apple: Restrições](#)
 - [Política da Apple: Aplicativos e perfis](#)
- [Status do Dispositivo](#)
 - [Visão geral do dispositivo](#)
 - [Gerenciamento de SIMs](#)
 - [Comandos](#)
 - [Mapa de localização](#)
- [Mapa de localização do dashboard](#)
- [Aplicativos privados](#)
- [Gerenciamento de certificados](#)
- [Regras de eventos](#)
- [Dispositivos](#)
 - [Dispositivos](#)
- [Usuários](#)
 - [Usuários](#)
 - [Editor de usuário](#)

- [Conta](#)
 - [Configurações](#)
- [Multitenância](#)
 - [Visão geral do multi-tenant](#)
 - [Empresas gerenciadas](#)
 - [Troca de empresa \(Enterprise switching\)](#)
 - [Subcontas](#)
- [Insights](#)

Introdução

O Cerberus Enterprise é uma solução de EMM abrangente, projetada para ajudar você a proteger e gerenciar seus dispositivos Android e Apple. Ele possui todos os recursos necessários para o gerenciamento eficaz de dispositivos BYOD e de propriedade da empresa em um painel limpo e intuitivo, e você pode começar a usá-lo em minutos.

Para usar o Cerberus Enterprise de forma eficaz, você precisa entender alguns conceitos fundamentais sobre como o sistema funciona.

O sistema suporta o gerenciamento de dispositivos Android e Apple:

No Android, o Cerberus Enterprise usa a oficial [Android Management API](#) do Google para gerenciar dispositivos por meio do aplicativo [Android Device Policy](#) (ADP). A maioria das configurações é aplicada diretamente pelo ADP. Alguns recursos opcionais também podem exigir o aplicativo complementar do Cerberus Enterprise, que amplia as possibilidades além do ADP.

Em dispositivos Apple, o Cerberus Enterprise gerencia os aparelhos por meio do MDM (Mobile Device Management) da Apple. O gerenciamento da Apple exige um certificado APNs e pode, opcionalmente, integrar-se ao Apple Business Manager para registro automático e licenciamento de aplicativos.

Cada dispositivo pode ser **registrado** no sistema usando um [token de registro](#) ou um [perfil de registro](#) (registro manual da Apple). O método de registro é associado a uma [Política](#) que contém as regras que devem ser aplicadas aos dispositivos.

Os administradores de TI podem alterar a política associada a um dispositivo após o registro. No entanto, cada dispositivo pode estar associado a apenas uma política por vez.

Durante o processo de registro (provisionamento), os componentes de gerenciamento necessários são instalados e configurados automaticamente. No Android, isso normalmente inclui o aplicativo Android Device Policy (e, dependendo da sua configuração, o aplicativo complementar do Cerberus Enterprise). Em dispositivos Apple, o gerenciamento é aplicado por meio de MDM assim que o dispositivo é registrado. Consequentemente, a política correspondente é aplicada automaticamente ao dispositivo, e todas as regras associadas são aplicadas pelo sistema de gerenciamento da plataforma.

Uma política pode ser aplicada a muitos dispositivos. Nesse caso, ao modificar a política, todos os dispositivos associados receberão as alterações.

Configuração

Configuração do Android Management

Para gerenciar dispositivos Android com o Cerberus Enterprise, você deve primeiro conectar sua organização ao Google Android Enterprise.

O processo de configuração geralmente leva alguns minutos e requer um **e-mail corporativo** (por exemplo, *nome@empresa.com*) ou, alternativamente, um **e-mail pessoal do Google**.

O que acontece durante a configuração

- Você será redirecionado para o Google Android Enterprise.
- Você faz o login com seu e-mail corporativo (ou um e-mail pessoal do Google).
- O Google cria a conta do Android Management para sua organização.
- Você é redirecionado de volta ao Cerberus Enterprise para concluir a configuração.

Informações importantes

Recomendamos o cadastro com um e-mail corporativo, não com uma conta pessoal do Gmail. Se o endereço de e-mail já estiver associado a uma conta de Administrador do Google, essa conta existente será reutilizada e vinculada ao Cerberus Enterprise; caso contrário, uma nova conta gratuita de Administrador do Google será criada. Uma conta de Administrador do Google desbloqueia o conjunto completo de recursos — por exemplo, a inscrição de dispositivos usando a autenticação do Google com contas gerenciadas pelo seu domínio de Administrador do Google.

Não tem um e-mail corporativo?

Você ainda pode se cadastrar com um e-mail pessoal do Google (por exemplo, uma conta Gmail). Neste caso, o Google cria uma conta gratuita do Google Play gerenciada que é vinculada ao Cerberus Enterprise.

Próximos passos

Após concluir a configuração, crie um [token de registro](#) e escolha o método de provisionamento apropriado para o dispositivo.

Configuração do Apple Management (APNs)

Para gerenciar dispositivos Apple, o Cerberus Enterprise requer o certificado do serviço Apple Push Notification (APNs).

Use o ID Apple associado à sua organização. O certificado APNs é válido por um ano e deve ser renovado anualmente para continuar o gerenciamento dos dispositivos.

Passo 1: Baixar o arquivo CSR

No dashboard, inicie a configuração do Apple Management e baixe o arquivo de Solicitação de Assinatura de Certificado (CSR) assinada pelo fornecedor, gerado pelo Cerberus Enterprise.

Passo 2: Criar o certificado de push no portal da Apple

- Faça login no Portal de Certificados de Push da Apple com seu ID Apple.
- Clique em "*Criar um certificado*".
- Faça o upload do arquivo CSR do Passo 1.
- Baixe o certificado de push criado.

Link do portal: <https://identity.apple.com/>

Passo 3: Fazer o upload do certificado de push

Faça o upload do certificado de push que você baixou da Apple no Cerberus Enterprise para concluir a configuração.

Se o certificado APNs expirar, o gerenciamento de dispositivos Apple parará de funcionar até que o certificado seja renovado.

Próximos passos

Após a configuração do APNs, você pode prosseguir com o registro de dispositivos Apple. Continue com [Visão geral do provisionamento Apple](#).

Visão geral do provisionamento de dispositivos

A Cerberus Enterprise oferece suporte ao gerenciamento de dispositivos para as plataformas Android e Apple. Você pode configurar cada plataforma de forma independente, dependendo dos dispositivos que precisa inscrever.

1. Conclua a configuração da plataforma no painel

Antes de inscrever os dispositivos, conclua a configuração da plataforma no painel do Cerberus Enterprise. Se a sua conta ainda não estiver configurada, o painel irá guiá-lo através das etapas necessárias.

Configuração do Android (Google Android Enterprise)

Para o procedimento completo de configuração do Android, leia [Configuração do Android Management](#).

- Vá para o fluxo de inscrição no painel e selecione **Configurar o Android Management**.
- Você será redirecionado para o Google para fazer login com uma **conta de trabalho** e autorizar o Android Enterprise.
- Após a autorização, você será redirecionado de volta ao Cerberus Enterprise para concluir a configuração.

Configuração da Apple (certificado de push APNs)

Para o procedimento completo de configuração da Apple, leia [Configuração do Apple Management \(APNs\)](#).

- Vá para o fluxo de inscrição no painel e selecione **Configurar o Apple Management**.
- Baixe o arquivo CSR do Cerberus Enterprise.
- Crie o certificado APNs no Portal de Certificados de Push da Apple e baixe o certificado resultante.
- Faça o upload do certificado baixado de volta no Cerberus Enterprise para habilitar o gerenciamento de dispositivos Apple.

2. Inscrever dispositivos

Após concluir a configuração da plataforma, escolha o método de inscrição que corresponda ao seu modelo de propriedade de dispositivos e ao sistema operacional.

Inscrição Android

Para o Android, a inscrição é orientada por [tokens de inscrição](#). Selecione o método apropriado dependendo se o dispositivo é de propriedade pessoal ou da empresa.

- Propriedade pessoal (BYOD / perfil de trabalho): [siga este guia](#).
- Propriedade da empresa (uso pessoal e de trabalho / perfil de trabalho): [siga este guia](#).
- Propriedade da empresa (uso exclusivo de trabalho / gerenciamento total ou dispositivos dedicados): [siga este guia](#).
- Zero-touch: [siga este guia](#).

Inscrição Apple

Para a Apple, comece concluindo a configuração do APNs descrita acima e, em seguida, siga os guias de provisionamento da Apple: [Visão geral do provisionamento da Apple](#).

Provisionamento de Dispositivos - Android

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 o uso de dispositivos que atendam aos requisitos [Android Enterprise Recommended](#).

Alguns recursos são limitados a versões específicas do Android ou podem se comportar de maneira diferente entre as versões do sistema operacional. Para mais informações sobre um recurso específico, consulte a seção [Políticas](#) da documentação.

O Cerberus Enterprise suporta tanto dispositivos de propriedade da empresa quanto dispositivos pessoais, e dois modos de gerenciamento: proprietário do dispositivo (device owner) e proprietário do perfil (profile owner).

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

Dispositivos de **propriedade 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 de propriedade da empresa com perfil de trabalho são adequados quando você fornece dispositivos corporativos aos funcionários para o trabalho, permitindo ainda o uso pessoal. Dispositivos totalmente gerenciados são mais adequados para dispositivos que devem ser usados apenas para o trabalho ou para **dispositivos dedicados** (COSU, dispositivos de uso único de propriedade corporativa), como quiosques.

Para mais informações sobre o provisionamento de dispositivos, consulte a página [Visão geral do provisionamento de dispositivos](#).

Tokens de inscrição

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

A guia de tokens de inscrição do Android está disponível apenas após a conclusão da **Configuração do Android Management**.

Onde encontrar os tokens de inscrição

No painel, abra **Tokens de inscrição**. Dependendo da configuração da sua conta, a página pode exibir várias guias (Tokens Android, Inscrição via login do Google, Inscrição manual da Apple e Inscrição Automatizada de Dispositivos da Apple).

Se a sua empresa Android for baseada em um domínio gerenciado pelo Google (Google Workspace), o painel também pode exibir uma guia de **Autenticação via Inscrição do Google**. Para detalhes sobre como ativá-la e utilizá-la, consulte **Autenticação via Inscrição do Google**.

Lista de tokens de inscrição (Android)

A guia de tokens Android mostra uma tabela com todos os tokens. Ao clicar em uma linha, a página de detalhes do token será aberta.

Colunas

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

Ações

- Cada linha possui uma ação de exclusão (**Excluir token de inscrição**). A exclusão é desativada quando a licença estiver expirada.
- A tabela suporta 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 atualizar para recarregar a lista. A tabela é paginada (10/25/50 itens por página).

Criar um novo token de inscrição

Na guia de tokens Android, clique em **Novo token de inscrição** para abrir a página de criação de token. Se a sua licença estiver expirada, o botão de criação estará desativado.

Opções do token

1. Política

Obrigatório. A política aplicada automaticamente a todos os dispositivos inscritos usando este token. Selecione uma de suas [políticas Android](#). Se você ainda não tiver nenhuma política, crie uma primeiro.

2. Usuário

Opcional. Se definido, os novos dispositivos inscritos serão associados automaticamente 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 de propriedade pessoal (perfil de trabalho) e dispositivos de propriedade da empresa para uso pessoal e de trabalho.
- **Não permitido:** adequado para dispositivos de propriedade da empresa para uso exclusivo de trabalho (totalmente gerenciados).
- **Dispositivo dedicado:** adequado para dispositivos de quiosque/dedicados (o dispositivo não está associado a um único usuário).

4. Usos permitidos

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

5. Expiração

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

6. Autenticação do Google

Controla se o usuário deve se autenticar com uma conta do Google durante a inscrição 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 a inscrição.
- **Opcional:** o usuário pode optar por pular a autenticação do Google durante a inscrição.
- **Obrigatório:** o usuário deve se autenticar com uma conta do Google para prosseguir com a inscrição.

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

Opções de provisionamento (apenas código QR)

Essas opções adicionais são incorporadas ao 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 isso para permitir que um dispositivo se conecte automaticamente ao Wi-Fi durante o provisionamento, para que possa baixar e inicializar o aplicativo de gerenciamento. Os campos disponíveis incluem **SSID**, **SSID oculto**, **Segurança** e (quando necessário) **Senha de rede**.

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

Outras opções

As opções adicionais incluem **Localidade**, **Fuso horário** e **Pular criptografia**.

Detalhes do token de inscrição

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

- **Status**, **Expiração**, **Uso**, **Uso pessoal**, **Usos permitidos** e (quando definido) **Autenticação do Google** com o opcional **E-mail da conta obrigatória**.
- **Token**: o valor bruto do token de inscrição (copiável).
- **URL de inscrição**: uma 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 provisionamento passo a passo, siga os guias de inscrição do Android: [**Dispositivos de propriedade pessoal**](#), [**Dispositivos de propriedade da empresa para uso pessoal e de trabalho**](#), [**Dispositivos de propriedade da empresa para uso exclusivo de trabalho**](#), 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 aplicativos e dados de trabalho, separado dos aplicativos e dados pessoais. A maioria das políticas de aplicativos, dados e outras gestões 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, use um dos seguintes métodos de provisionamento (certifique-se de que o [token de inscrição](#) tenha o **Uso pessoal** definido como **Permitido**):

Link do token de inscrição

Versão do Android
6.0+

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

Adicionar perfil de trabalho a partir das "Configurações"

Versão do Android
6.0+

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

Se a pesquisa não obtiver sucesso, 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 e restaurar -> Configurar seu perfil de trabalho.*

Essas 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. Após a instalação do aplicativo, o usuário será solicitado a escanear um código QR ou inserir manualmente um token de registro para concluir a configuração do perfil de trabalho.

Dispositivos de propriedade da empresa para uso profissional e pessoal

A configuração de um dispositivo de propriedade da empresa com um **perfil de trabalho** habilita o dispositivo para uso profissional e pessoal. Em dispositivos de propriedade da empresa com perfis de trabalho:

- A maioria das políticas de aplicativos, dados e outros gerenciamentos 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 o *Escopo de bloqueio* para aplicar ações de conformidade em todo o dispositivo ou apenas no seu perfil de trabalho.
- A remoção de registro do dispositivo e os comandos do dispositivo aplicam-se ao dispositivo como um todo.

Para configurar um dispositivo de propriedade da empresa com um perfil de trabalho, use um dos seguintes métodos de provisionamento (certifique-se de que o [token de inscrição](#) tenha o **Uso pessoal** definido como **Permitido**):

Método de código QR

Versão do Android
8.0+

Em um dispositivo novo ou com restauração de fábrica, o usuário (geralmente um administrador de TI) toca na tela seis vezes no mesmo local. Isso fará com que o dispositivo solicite ao usuário a leitura de um código QR.

Dispositivos de propriedade da empresa para uso exclusivo de trabalho

O **gerenciamento total do dispositivo** é adequado para dispositivos de propriedade da empresa destinados exclusivamente a fins de trabalho. As empresas podem gerenciar todos os aplicativos no dispositivo e aplicar todo o espectro de políticas e comandos da Android Management API.

Também é possível bloquear um dispositivo (via política) para um único aplicativo ou um pequeno conjunto de aplicativos para atender a um propósito ou caso de uso dedicado. Este subconjunto de dispositivos totalmente gerenciados é chamado de **dispositivos dedicados**.

Para configurar o gerenciamento total em um dispositivo de propriedade da empresa, use um dos seguintes métodos de provisionamento (certifique-se de que o [token de inscrição](#) tenha o **Uso pessoal** definido como **Não permitido**):

Método de código QR

Versão do Android
7.0+

Em um dispositivo novo ou com restauração de fábrica, o usuário (geralmente um administrador de TI) toca na tela seis vezes no mesmo local. Isso fará com que o dispositivo solicite ao usuário a leitura de um código QR.

Método de identificador DPC

Versão do Android
5.1+

Se o Android Device Policy não puder ser adicionado via 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 com restauração de fábrica.
2. Insira os detalhes de login do Wi-Fi para conectar o dispositivo à internet.

3. Quando for solicitado o login, insira **afw#setup**, o que fará o download do Android Device Policy.
4. Escaneie um código QR ou insira manualmente um token de inscrição para provisionar o dispositivo.

Zero-touch

Os administradores de TI podem provisionar dispositivos de propriedade 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 para as configurações definidas pelo administrador de TI.

Os administradores de TI podem pré-configurar dispositivos adquiridos 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 via Inscrição do Google

A Autenticação via Inscrição do Google (também chamada de **Autenticação do Google para Inscrição**) permite que os usuários se autenticem com sua conta do Google Workspace durante a inscrição de dispositivos Android.

Este recurso está disponível apenas para empresas Android baseadas em um domínio gerenciado pelo Google (Google Workspace).

Onde encontrá-la

No painel, abra **Tokens de inscrição** e selecione a guia **Autenticação via 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.

Ativar (ou desativar) a Autenticação do Google

A Autenticação do Google é ativada a partir do **Console de administração do Google**. Após alterar a configuração, retorne 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 Android EMM** para o Cerberus Enterprise e abra-a.
5. Clique em **Gerenciar provedores de EMM**.

6. Ative ou desative **Autenticação via Inscrição do Google** para habilitar ou desabilitar a autenticação do Google para inscrição.
7. Clique em **Salvar**.
8. Retorne ao painel do Cerberus Enterprise e clique em **Atualizar status** na guia **Autenticação via Inscrição do Google**.

Token de Inscrição via Autenticação do Google

Quando a Autenticação do Google está ativada, o painel mostra um token de inscrição dedicado usado para este modo de inscrição. A página pode exibir um **código QR**, um valor de **Token de inscrição** e uma **URL de inscrição** (copiável e enviável por e-mail).

Opções principais

- **Permitir uso pessoal**: controla se o token pode inscrever dispositivos para uso pessoal e de trabalho (cenários de perfil de trabalho) ou apenas para uso de trabalho (cenários de gerenciamento total / dispositivos dedicados).
- **Política Padrão de Contingência**: a política aplicada quando o usuário que realiza a inscrição não possui uma política padrão de Autenticação do Google específica atribuída.

Interação com a política

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

Para dispositivos já inscritos, esta política só se aplica se o dispositivo for gerenciado por uma conta do Google Play gerenciada (ou seja, inscrito sem a **Autenticação via Inscrição do Google**).

Algumas ações (por exemplo, alterar as opções do token) podem ser desativadas quando a licença estiver expirada.

Inscriver um dispositivo

Durante a inscrição, o usuário será solicitado a se autenticar com sua conta do Google Workspace. Após uma inscrição bem-sucedida, o dispositivo será associado ao usuário autenticado.

Perfil de trabalho (dispositivos de propriedade pessoal)

- Compartilhe a **URL de inscrição** com o usuário. Quando o usuário a abrir em seu dispositivo Android, ele será guiado pela configuração do perfil de trabalho e pela autenticação do Google.
- Como alternativa, o usuário pode iniciar a partir das Configurações do Android e escolher o fluxo de configuração do perfil de trabalho, então escanear o código QR ou inserir o token de inscrição quando solicitado.

Dispositivos de propriedade da empresa

- **Método de código QR:** em um dispositivo novo ou com restauração de fábrica, toque na tela várias vezes no mesmo local até que o comando para ler o código QR apareça e, em seguida, escaneie o código QR exibido no painel.
- **Método de identificador DPC** (quando a leitura de código QR não estiver disponível): siga o assistente de configuração, conecte-se ao Wi-Fi e, quando for solicitado o 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 provisionamento Android (perfil de trabalho vs. gerenciamento total), consulte as páginas padrão de inscrição do Android neste manual.

Provisionamento de Dispositivos - Apple

Visão geral do provisionamento Apple

O Cerberus Enterprise suporta o registro e o gerenciamento de dispositivos Apple. O provisionamento da Apple requer um certificado APNs e pode ser realizado usando diferentes métodos de registro.

Pré-requisito: configurar o Apple Management (APNs)

Antes de registrar qualquer dispositivo Apple, conclua a [configuração do Apple Management \(APNs\)](#).

Escolha um método de registro

Registro manual (Perfil de Registro)

Este método fornece uma URL de registro e um arquivo de perfil de configuração (mobileconfig) que você instala no dispositivo. Leia [Registro manual da Apple](#).

Automated Device Enrollment (ADE)

Este método integra-se ao Apple Business Manager para automatizar o registro de dispositivos de propriedade da empresa. Leia [Apple Automated Device Enrollment \(ADE\)](#).

Você pode usar o registro manual e o ADE em paralelo, dependendo da sua frota de dispositivos e do seu processo de compra.

Apple manual enrollment (Perfil de Registro)

O Cerberus Enterprise suporta o registro manual de dispositivos Apple usando uma URL de registro e um arquivo de perfil de registro.

O registro manual está disponível quando o Apple Management (APNs) está configurado. Se você ainda não concluiu a configuração do APNs, leia [Configuração do Apple Management \(APNs\)](#).

Obtenha a URL e o perfil de registro

- Abra a seção **Inscrição** no dashboard e selecione a aba **Apple manual enrollment (Enrollment Profile)**.
- Copie a **URL de registro** ou use a ação de enviar por e-mail.
- Baixe o **Perfil de Registro** (arquivo mobileconfig).

Como registrar um iPhone ou iPad

iOS/iPadOS 15.0+

1. Envie o arquivo do perfil de registro (*enroll.mobileconfig*) para o dispositivo ou abra a URL de registro no Safari do dispositivo.
2. No dispositivo, abra *Ajustes* → *Perfil Baixado* → *Instalar* e siga as instruções.
3. Após o registro, você pode verificar o status em *Ajustes* → *Geral* → *VPN e Gerenciamento de Dispositivos* (ou *Perfis e Gerenciamento de Dispositivos*).

Instale apenas perfis de registro que você obteve no seu dashboard do Cerberus Enterprise.

Apple Automated Device Enrollment (ADE)

O Automated Device Enrollment (ADE) integra-se ao Apple Business Manager (ABM) para registrar automaticamente dispositivos de propriedade da empresa quando são ligados pela primeira vez (ou após uma restauração de fábrica).

O ADE exige que o Apple Management (APNs) seja configurado primeiro. Se necessário, leia [Configuração do Apple Management \(APNs\)](#).

Como registrar dispositivos automaticamente

1. Adicione dispositivos à sua conta do Apple Business Manager.
2. Após adicionar novos dispositivos à sua conta do ABM, sincronize-os no Cerberus Enterprise na seção **Dispositivos** usando a ação **Sincronizar do ABM**.
3. Crie um perfil ADE no dashboard em **Inscrição** → **Apple Automated Device Enrollment (ADE)** → **Novo perfil ADE**.
4. Atribua um perfil ADE a um dispositivo na página de detalhes do dispositivo usando o campo **Perfil ADE**.

Configurações do perfil ADE (visão geral)

Um perfil ADE controla como o dispositivo é registrado e como o Assistente de Configuração se comporta. No Cerberus Enterprise, um perfil ADE inclui um nome, uma política inicial opcional e algumas opções de registro.

Nome do perfil

Um nome legível para o perfil (por exemplo, *Perfil ADE padrão*).

Política

A política aplicada inicialmente aos dispositivos registrados. Você pode atribuir uma política ao criar um novo perfil ADE.

Opções de registro

- **MDM removível:** controla se o payload de MDM pode ser removido do dispositivo.
- **Permitir emparelhamento:** controla se o emparelhamento é permitido (descontinuado pela Apple no iOS 13).
- **Avanço automático da configuração:** avança automaticamente o Assistente de Configuração por suas telas.
- **Aguardar dispositivo configurado:** bloqueia o Assistente de Configuração até que o servidor marque o dispositivo como configurado.
- **Obrigatório:** impede que a aplicação do perfil seja pulada durante a configuração.
- **Multiusuário (iPad compartilhado):** configura o dispositivo para o modo iPad compartilhado.
- **Supervisionado:** solicita a supervisão para o dispositivo.

Depois que um dispositivo tem um perfil ADE atribuído, ele está pronto para ser registrado automaticamente.

Visão geral das políticas

A seção de **Políticas** do painel (*Painel* → *Políticas*) lista todas as políticas em sua conta e permite que você as crie, copie, edite e exclua.

Lista de políticas

As políticas são exibidas em uma tabela. Ao clicar em uma linha, o editor de política correspondente será aberto.

Colunas

- **ID**: identificador interno da política.
- **MDM**: a plataforma da política (Android ou Apple).
- **Nome**: nome da política.
- **Descrição**: descrição da política.
- **Dispositivos**: número de dispositivos inscritos atualmente atribuídos à política.

Filtros e pesquisa

- Se o Android Management e o Apple Management estiverem configurados, você poderá filtrar a lista por **Todos**, **Android** ou **Apple**.
- Você pode ativar a **Pesquisa** e pesquisar pelo nome ou descrição da política.

Atualização e paginação

- Use a ação de atualizar para recarregar a lista.
- A tabela é paginada (10/25/50 itens por página).

Criar uma nova política

Na parte inferior da página de Políticas, você pode criar uma nova política. Dependendo de qual plataforma estiver configurada em sua conta, você poderá ver uma ou ambas as ações:

- Criar nova política Android
- Criar nova política da Apple

Se a sua licença estiver expirada, a criação de políticas (e outras ações de escrita) estarão desativadas.

Copiar e excluir políticas

Cada linha de política possui um menu de ações que inclui **Copiar política** e **Excluir política**.

Avisos de exclusão de política

Ao excluir uma política, o painel pode exibir avisos adicionais dependendo de como a política é utilizada.

- Se a política estiver atribuída a dispositivos inscritos, excluí-la removerá a inscrição dos dispositivos associados e apagará seus aplicativos e dados.
- Se a política estiver atribuída a tokens de inscrição, esses tokens podem não ser mais capazes de concluir a inscrição.
- Se a política estiver definida como padrão para a inscrição por Autenticação do Google (globalmente ou para alguns usuários), excluí-la pode fazer com que as inscrições falhem.

Excluir várias políticas

A lista de Políticas suporta a seleção de várias linhas para exclusão em massa. No modo de seleção múltipla, você pode selecionar várias políticas e excluí-las em uma única ação.

A exclusão em massa só é habilitada quando todas as políticas selecionadas pertencem à mesma plataforma (todas Android ou todas Apple).

Próximo: editar configurações de política

A lista de Políticas é o ponto de entrada. Para configurar as definições de política, utilize a documentação do editor apropriada: [Políticas → Android](#) e [Políticas → Apple](#).

As políticas referenciadas por tokens de inscrição são aplicadas automaticamente durante a inscrição do dispositivo.

Políticas - Android

Resumo

As políticas do Android são as entidades centrais do sistema: elas definem as regras que são aplicadas e aplicadas aos dispositivos gerenciados.

Você pode navegar por suas políticas e criar novas na seção **Políticas** do painel. Para abrir uma política do Android, clique na linha da política na tabela: o sistema abrirá a página do **Editor de Políticas**.

Uma política pode ser associada a um [token de inscrição](#), portanto ela será aplicada automaticamente aos dispositivos durante o processo de provisionamento. Você também pode alterar a política atribuída a um dispositivo após o provisionamento.

Cada dispositivo pode ser associado a apenas uma política por vez.

Muitas opções de política aplicam-se apenas a tipos específicos de dispositivos (totalmente gerenciados, dedicados, perfil de trabalho) e versões do Android. Configurações não suportadas podem ser ignoradas pelo dispositivo ou relatadas como não conformes.

Layout do Editor de Políticas

O Editor de Políticas é organizado como um conjunto de seções expansíveis. No topo da página, você sempre poderá editar:

- **Nome** (obrigatório)
- **ID** (somente leitura)
- **Descrição** (opcional)

As seções abaixo correspondem aos painéis do Editor de Políticas (por exemplo: Gerenciamento de aplicativos, Segurança, Rede, Sistema, Uso pessoal, Políticas entre perfis e muito mais). Use as páginas dos capítulos deste manual para entender cada painel em detalhes.

Salvar, excluir e dispositivos associados

Use **Salvar política** para aplicar suas alterações. O botão é desativado quando não há edições pendentes ou quando a licença expirou.

Se você abriu uma política existente (que possui um ID), a página mostrará uma ação de **Excluir política** e uma lista de **Dispositivos associados** na parte inferior, para que você possa ver quantos dispositivos estão usando a política no momento.

Gerenciamento de apps

Nesta seção, você pode definir políticas relacionadas à disponibilidade de aplicativos, instalação, atualizações e gerenciamento de permissões.

As Contas do Google Play Gerenciado são criadas automaticamente quando os dispositivos são provisionados.

1. Modo da Play Store

Este modo controla quais aplicativos estão disponíveis para o usuário na Play Store e o comportamento no dispositivo quando os aplicativos são removidos da política.

Lista de permissões (padrão): Apenas os aplicativos que estão na política estarão disponíveis, e qualquer aplicativo que não esteja na política será desinstalado automaticamente do dispositivo. A Play Store mostrará apenas os aplicativos disponíveis.

Lista de bloqueio: Todos os aplicativos estão disponíveis, e qualquer aplicativo que não deva estar no dispositivo deve ser explicitamente marcado como **bloqueado** na política de aplicativos. A Play Store mostrará todos os aplicativos, exceto os bloqueados.

2. Política de aplicativos não confiáveis

A política para aplicativos não confiáveis (aplicativos de fontes desconhecidas) aplicada ao dispositivo. Esta opção controla a configuração do sistema Android que determina se um usuário pode instalar aplicativos de fora da Play Store (sideloading).

Não permitir (padrão): Não permitir a instalação de aplicativos não confiáveis em todo o dispositivo.

Apenas no perfil pessoal: Para dispositivos com perfis de trabalho, permite a instalação de aplicativos não confiáveis apenas no perfil pessoal do dispositivo.

Permitir: Permitir a instalação de aplicativos não confiáveis em todo o dispositivo.

3. Google Play Protect

Se a verificação de aplicativos do Google Play Protect é aplicada.

Aplicada (padrão): Força a verificação de aplicativos.

Escolha do usuário: Permite que o usuário escolha se deseja ativar a verificação de aplicativos.

4. Política de permissão padrão

A política para conceder solicitações de permissão em tempo de execução aos aplicativos.

Solicitar (padrão): Solicita que o usuário conceda uma permissão.

Conceder: Concede uma permissão automaticamente.

Negar: Nega uma permissão automaticamente.

5. Funções de aplicativos

Controla se os aplicativos em dispositivos totalmente gerenciados ou em perfis de trabalho têm permissão para expor funções do aplicativo. Requer Android 16 ou superior.

Permitido (padrão): Aplicativos em dispositivos totalmente gerenciados ou em perfis de trabalho podem expor funções do aplicativo.

Não permitido: Aplicativos em dispositivos totalmente gerenciados ou em perfis de trabalho não podem expor funções do aplicativo.

6. Instalação de aplicativos desativada

Se a instalação de aplicativos pelo usuário está desativada.

7. Desinstalação de aplicativos desativada

Se a desinstalação de aplicativos pelo usuário está desativada.

8. Políticas de permissão

Concessões ou negações explícitas de permissão individual ou em grupo para todos os aplicativos. Esses valores substituem a configuração de **Política de permissão padrão**.

Use **Adicionar política de permissão** para criar entradas e remova-as com a ação de excluir.

Cada entrada inclui:

Permissão/grupo Android: A permissão ou grupo Android (obrigatório), por exemplo **android.permission.READ_CALENDAR** ou **android.permission_group.CALENDAR**.

Política: Conceder / Negar / Solicitar (usa as mesmas opções de política da **Política de permissão padrão**).

9. Aplicativos

Lista de aplicativos que devem ser incluídos na política. O comportamento do conteúdo da lista depende do valor definido em **Modo da Play Store**.

Se o **Modo da Play Store** estiver definido como **lista de permissões**, apenas os aplicativos que estão na política estarão disponíveis e qualquer aplicativo que não esteja na política será desinstalado automaticamente do dispositivo.

Se o **Modo da Play Store** estiver definido como **lista de bloqueio**, todos os aplicativos estarão disponíveis e qualquer aplicativo que não deva estar no dispositivo deve ser explicitamente marcado como **bloqueado** na política de aplicativos.

Para adicionar um novo aplicativo, clique no botão **Adicionar aplicativos** (ou no ícone **Adicionar aplicativos**), selecione **Do Managed Google Play**, escolha o aplicativo na Play Store e clique no botão **Selecionar** no cartão do aplicativo.

Para adicionar um aplicativo que não está publicado no Google Play, mas já está presente no dispositivo (por exemplo, um aplicativo de sistema ou do fabricante), clique em **Adicionar aplicativos**, selecione **Por nome do pacote (aplicativos pré-instalados)**, digite o nome do pacote do aplicativo (ex: **com.example.app**) e clique em **Adicionar**. O aplicativo é adicionado com o tipo de instalação **Forçar instalação**. Para exibir o aplicativo no launcher personalizado do modo quiosque, o seu **Tipo de instalação** deve ser **Pré-instalado** ou **Forçar instalação**: com **Disponível** o aplicativo não é exibido.

Aplicativos que não estão disponíveis no Managed Google Play são marcados com um ícone do Android na lista de aplicativos. Eles não podem ser instalados a partir do Google Play, portanto, já devem estar presentes no dispositivo: dispositivos que não possuem o aplicativo

não conseguirão instalá-lo.

Todos os aplicativos publicados na Play Store em seu país estão disponíveis para seleção por padrão. Para selecionar seus próprios aplicativos privados ou da web, você deve primeiro carregá-los no sistema. Para mais informações, leia a página de [Aplicativos privados](#).

Cada aplicativo pode ser configurado com suas próprias definições, que estão contidas visualmente em um card:

9.1. Tipo de instalação

O tipo de instalação a ser realizada para um aplicativo.

Disponível: O aplicativo está disponível para instalação.

Pré-instalado: O aplicativo é instalado automaticamente e pode ser removido pelo usuário.

Instalação forçada: O aplicativo é instalado automaticamente e não pode ser removido pelo usuário.

Bloqueado: O aplicativo está bloqueado e não pode ser instalado. Se o aplicativo foi instalado sob uma política anterior, ele será desinstalado.

Obrigatório para configuração: O aplicativo é instalado automaticamente, não pode ser removido pelo usuário e impedirá a conclusão da configuração até que a instalação seja concluída.

Quiosque: O aplicativo é instalado automaticamente no modo quiosque: ele é definido como a intenção de tela inicial preferencial e incluído na lista de permissões para o modo de tarefa bloqueada. A configuração do dispositivo não será concluída até que o aplicativo seja instalado. Após a instalação, os usuários não poderão remover o aplicativo. Você só pode definir este **tipo de instalação** para um aplicativo por política. Quando isso estiver presente na política, a barra de status será desativada automaticamente. Para mais informações, leia a página dedicada ao [Modo quiosque](#).

9.2. Restrições de instalação

Define um conjunto de restrições para a instalação do aplicativo. Quando várias restrições são selecionadas, todas elas devem ser atendidas para que o aplicativo seja instalado.

Esta opção é exibida apenas quando o **Tipo de instalação** for **Pré-instalado** ou **Instalação forçada**.

Rede sem limite de dados: Instale o aplicativo apenas quando o dispositivo estiver conectado a uma rede sem limite de dados (ex: Wi-Fi).

Carregando: Instale o aplicativo apenas quando o dispositivo estiver carregando.

Inativo: Instale o aplicativo apenas quando o dispositivo estiver inativo.

9.3. Modo de atualização automática

Controla o modo de atualização automática do aplicativo.

Padrão: O aplicativo é atualizado automaticamente com baixa prioridade para minimizar o impacto no usuário. O aplicativo é atualizado quando todas as seguintes restrições forem atendidas: (1) o dispositivo não estiver sendo usado ativamente, (2) o dispositivo estiver conectado a uma rede sem limite de dados, (3) o dispositivo estiver carregando. O dispositivo é notificado sobre uma nova atualização em até 24 horas após ser publicada pelo desenvolvedor, após o que o aplicativo será atualizado na próxima vez que as restrições acima forem atendidas.

Adiado: O aplicativo não é atualizado automaticamente por um período máximo de 90 dias após o aplicativo ficar desatualizado. Após 90 dias do aplicativo ficar desatualizado, a versão mais recente disponível é instalada automaticamente com baixa prioridade (veja o modo de **Atualização automática Padrão**). Após a atualização do aplicativo, ele não será atualizado automaticamente de novo até que se passem 90 dias após ficar desatualizado novamente. O usuário ainda pode atualizar o aplicativo manualmente pela Play Store a qualquer momento.

Prioridade alta: O aplicativo é atualizado o mais rápido possível. Nenhuma restrição é aplicada. O dispositivo é notificado imediatamente sobre uma nova atualização assim que ela estiver disponível.

9.4. Código de versão mínimo

A versão mínima do aplicativo que é executada no dispositivo. Se definida, o dispositivo tentará atualizar o aplicativo para pelo menos este código de versão. Se o aplicativo não estiver atualizado, o dispositivo exibirá um **detalhe de não conformidade** com o **motivo de não conformidade** definido como **APP_NOT_UPDATED**. O aplicativo já deve estar publicado no Google Play com um código de versão maior ou igual a este valor. No máximo 20 aplicativos podem especificar um código de versão mínimo por política.

9.5. Escopos delegados

Os escopos delegados ao aplicativo a partir do Android Device Policy. Você pode conceder a outros aplicativos uma seleção de permissões especiais do Android:

Instalação de certificados: Concede acesso à instalação e ao gerenciamento de certificados.

Configurações gerenciadas: Concede acesso ao gerenciamento de configurações gerenciadas.

Bloquear desinstalação: Concede acesso ao bloqueio de desinstalação.

Permissões: Concede acesso à política de permissões e ao estado de concessão de permissões.

Acesso a pacotes: Concede acesso ao estado de acesso a pacotes.

App do sistema: Concede acesso para habilitar aplicativos do sistema.

9.6. Rede preferencial

O serviço de rede preferencial a ser usado para este aplicativo. Se definido, o aplicativo usará o fatiamento de rede empresarial especificado para suas conexões quando disponível. Isso deve corresponder a um fatiamento de rede configurado na seção **Configuração de Fatiamento de Rede 5G** do painel **Celular**.

9.7. Política de permissão padrão

A política padrão para todas as permissões solicitadas pelo aplicativo. Se especificada, esta substitui a **Política de permissão padrão** de nível de política, que se aplica a todos os aplicativos. Ela não substitui as **Políticas de permissão** que se aplicam a todos os aplicativos.

Solicitar (padrão): Solicita que o usuário conceda uma permissão.

Conceder: Concede uma permissão automaticamente.

Negar: Nega uma permissão automaticamente.

9.8. App de trabalho e pessoal conectados

Controla se o aplicativo pode se comunicar entre os perfis de trabalho e pessoal do dispositivo, sujeito ao consentimento do usuário (Android 11+).

Não permitido (padrão): Impede que o aplicativo se comunique entre perfis.

Permitido: Permite que o aplicativo se comunique entre perfis após receber o consentimento do usuário.

9.9. Isenção de bloqueio do Always On VPN

Especifica se o aplicativo tem permissão para usar a rede quando a VPN não estiver conectada e o **bloqueio ativado** estiver ativo. Suportado apenas em dispositivos com Android 10 ou superior.

Aplicada (padrão): O aplicativo respeita a configuração de bloqueio do Always On VPN.

Isento: O aplicativo está isento da configuração de bloqueio do Always On VPN.

9.10. Widgets do perfil de trabalho

Especifica se o aplicativo instalado no perfil de trabalho tem permissão para adicionar widgets à tela inicial.

Permitido: O aplicativo pode adicionar widgets à tela inicial.

Não permitido: O aplicativo não pode adicionar widgets à tela inicial.

9.11. Configurações de controle do usuário

Especifica se o controle do usuário é permitido para um determinado aplicativo. O controle do usuário inclui ações como forçar a parada e limpar os dados do aplicativo (Android 11+). Se o **extensionConfig** estiver ativado para um aplicativo, o controle do usuário será desativado, independentemente desta configuração. Para aplicativos de quiosque, você pode usar **Permitido** para permitir o controle do usuário.

Não especificado: Usa o comportamento padrão do aplicativo para determinar se o controle do usuário é permitido ou não.

Permitido: O controle do usuário é permitido para o aplicativo.

Não permitido: O controle do usuário não é permitido para o aplicativo.

9.12. Desativado

Se o aplicativo está desativado. Quando desativado, os dados do aplicativo ainda são preservados.

9.13. Permitir Provedor de Credenciais

Se o aplicativo tem permissão para atuar como um provedor de credenciais no Android 14 ou superior.

9.14. Configuração gerenciada

Para configurar as definições gerenciadas do aplicativo, clique no botão **Ativar configuração gerenciada**. Se uma configuração gerenciada já estiver definida para o aplicativo, você pode modificá-la com o botão **Configuração gerenciada** ou excluí-la com o botão **Remover configuração**.

A opção de **Configuração gerenciada** está disponível apenas para aplicativos que suportam essa funcionalidade.

9.15. Políticas de permissão

Concessões ou negações explícitas de permissão para o aplicativo. Esses valores substituem a **Política de permissão padrão** e as **Políticas de permissão** que se aplicam a todos os aplicativos.

Use **Adicionar política de permissão** para adicionar uma ou mais regras de permissão ao card do aplicativo e remova-as com a ação de excluir.

9.16. IDs de trilha

Lista dos IDs de trilha de teste fechado do aplicativo que um dispositivo pode acessar. Se vários IDs de trilha forem selecionados, os dispositivos receberão a versão mais recente entre todas as trilhas acessíveis. Se nenhum ID de trilha for selecionado, os dispositivos terão acesso apenas à trilha de produção do aplicativo.

A opção de **IDs de trilha** está disponível apenas para aplicativos que possuem pelo menos um ID de trilha disponível para sua organização. Para mais detalhes sobre como adicionar sua organização a uma trilha de teste fechado para um aplicativo específico, leia [aqui](#).

10. Configurações de aplicativos padrão

Defina aplicativos padrão para os tipos suportados. Quando um aplicativo padrão é definido para pelo menos um tipo, os usuários são impedidos de alterar os aplicativos padrão naquele perfil.

Apenas uma configuração de aplicativo padrão é permitida por **Tipo de aplicativo padrão**. A lista de aplicativos padrão não deve conter duplicatas.

10.1. Tipo de aplicativo padrão

Selecione a categoria de aplicativo para configurar (por exemplo, Navegador, Discador, SMS, Carteira ou Assistente). A disponibilidade depende da versão do Android e do modo de gerenciamento.

10.2. Escopos de aplicativo padrão

Selecione onde o aplicativo padrão deve ser aplicado (Totalmente gerenciado, Perfil de trabalho ou Perfil pessoal). Apenas os escopos suportados pelo tipo selecionado podem ser escolhidos.

Se nenhum dos escopos selecionados for aplicável ao modo de gerenciamento do dispositivo, o dispositivo reportará um detalhe de não conformidade.

10.3. Aplicativos padrão

Lista de aplicativos que podem ser definidos como padrão para o tipo selecionado. O primeiro aplicativo instalado e elegível é definido como o padrão.

Se os escopos incluírem **Totalmente gerenciado** ou **Perfil de trabalho**, cada aplicativo também deve existir na lista de **Aplicativos** com o **Tipo de instalação** não definido como **Bloqueado**.

11. Seleção de chave privada

Permite a exibição da interface no dispositivo para que o usuário escolha um alias de chave privada caso não haja regras correspondentes em **Escolher regras de chave privada**.

Para dispositivos com versão inferior ao Android P, a definição desta opção pode deixar as chaves empresariais vulneráveis.

12. Escolher regras de chave privada

Controla o acesso dos aplicativos às chaves privadas. A regra determina qual chave privada, se houver, o Android Device Policy concede ao aplicativo especificado. O acesso é concedido quando o aplicativo chama `KeyChain.choosePrivateKeyAlias`` (ou qualquer sobrecarga) para solicitar um alias de chave privada para uma determinada URL, ou para regras que não são específicas de URL (ou seja, se `urlPattern`` não estiver definido, ou estiver definido como string vazia ou ``.``) no Android 11 e superior, diretamente para que o aplicativo possa chamar `KeyChain.getPrivateKey``, sem ter que chamar primeiro `KeyChain.choosePrivateKeyAlias``. Quando um aplicativo chama `KeyChain.choosePrivateKeyAlias`` e mais de uma regra de `choosePrivateKeyRules`` coincide, a última regra correspondente define qual alias de chave será retornado.

Use **Adicionar regra de chave privada** para criar entradas e remova-as com a ação de excluir.

12.1. Alias de chave privada

O alias da chave privada a ser utilizada.

12.2. Padrão de URL

O padrão de URL para correspondência com a URL da solicitação. Se não for definido ou estiver vazio, corresponderá a todas as URLs. Isso utiliza a sintaxe de expressão regular de `java.util.regex.Pattern`.

12.3. Nomes de pacotes

Os nomes de pacotes aos quais esta regra se aplica. O hash do certificado de assinatura de cada aplicativo é verificado em relação ao hash fornecido pelo Play. Se nenhum nome de pacote for especificado, o alias será fornecido a todos os aplicativos que chamarem

``KeyChain.choosePrivateKeyAlias`` ou qualquer sobrecarga (mas não sem chamar ``KeyChain.choosePrivateKeyAlias``, mesmo no Android 11 ou superior). Qualquer aplicativo com o mesmo UID do Android de um pacote especificado aqui terá acesso ao chamar ``KeyChain.choosePrivateKeyAlias``.

Use **Adicionar nome de pacote** para adicionar entradas e remova-as com a ação de excluir.

Para excluir um aplicativo, clique no ícone de **lixeira** na parte inferior do card do aplicativo.

Modo quiosque

Com o modo quiosque, você pode restringir a funcionalidade de um dispositivo a um único aplicativo ou a vários aplicativos. A escolha entre o modo quiosque de aplicativo único ou de múltiplos aplicativos depende dos seus objetivos de negócio.

No **modo quiosque de aplicativo único**, o dispositivo é configurado para um único aplicativo e não permite que os usuários finais acessem outros apps no dispositivo. Eles também não podem sair do aplicativo, tornando-o um dispositivo dedicado para aquele app específico. Para ativar este modo, especifique um aplicativo na seção [Gerenciamento de aplicativos](#) com o **Tipo de instalação** definido como **Quiosque**.

No **modo quiosque de múltiplos aplicativos**, os dispositivos têm permissão para acessar vários aplicativos. Os usuários finais podem navegar entre múltiplos apps por meio de um launcher personalizado. Para ativar este modo, ative a opção **Launcher de quiosque personalizado**.

Quando o modo quiosque está ativado, você também pode configurar se os usuários finais podem acessar certos recursos do sistema, como as configurações do sistema e a barra de status.

Launcher de quiosque personalizado

Define se o launcher de quiosque personalizado está ativado. Isso substitui a tela inicial por um launcher que restringe o dispositivo aos aplicativos instalados por meio da configuração de [Gerenciamento de aplicativos](#). Os aplicativos aparecem em uma única página em ordem alfabética.

Ações do botão de energia

Define o comportamento de um dispositivo no modo quiosque quando um usuário pressiona e mantém (pressionamento longo) o botão de energia.

Disponível (padrão): O menu de energia (ex: Desligar, Reiniciar) é exibido quando um usuário pressiona e mantém o botão de energia de um dispositivo no modo quiosque.

Bloqueado: O menu de energia (ex: Desligar, Reiniciar) não é exibido quando um usuário pressiona e mantém o botão de energia de um dispositivo no modo quiosque. Observação: isso pode impedir que os usuários desliguem o dispositivo.

Avisos de erro do sistema

Especifica se os diálogos de erro do sistema para aplicativos que travaram ou não respondem são bloqueados no modo quiosque. Quando bloqueados, o sistema encerrará o aplicativo compulsoriamente como se o usuário tivesse escolhido a opção "fechar aplicativo" na interface.

Bloqueado (padrão): Todos os diálogos de erro do sistema, como falhas e o aplicativo não respondendo (ANR), são bloqueados. Quando bloqueados, o sistema encerra o aplicativo compulsoriamente como se o usuário fechasse o aplicativo pela interface.

Ativado: Todos os diálogos de erro do sistema, como falhas e o aplicativo não respondendo (ANR), são exibidos.

Navegação do sistema

Especifica quais recursos de navegação são ativados (ex: botões Início e Visão geral) no modo quiosque.

Desativado (padrão): Os botões Início e Visão geral não estão acessíveis.

Apenas Início: Apenas o botão Início é ativado.

Ativado: Os botões Início e Visão geral estão ativados.

Barra de status

Especifica se as informações do sistema e as notificações são desativadas no modo quiosque.

Desativado (padrão): As informações do sistema e as notificações são desativadas no modo quiosque.

Apenas sistema: Apenas as informações do sistema são exibidas na barra de status.

Ativado: As informações do sistema e as notificações são exibidas na barra de status no modo quiosque. Observação: para que esta política surta efeito, o botão Início do dispositivo deve estar ativado usando `kioskCustomization.systemNavigation`.

Configurações do dispositivo

Especifica se o aplicativo de Configurações é permitido no modo quiosque.

Permitido (padrão): O acesso ao aplicativo de Configurações é permitido no modo quiosque.

Bloqueado: O acesso ao aplicativo de Configurações não é permitido no modo quiosque.

Segurança

Nesta seção, você pode configurar políticas relacionadas à segurança.

Ações de risco de segurança

Escolha o que fazer quando um dispositivo reportar um SecurityRisk nos relatórios de status.

Tipos de SecurityRisk suportados:

SO desconhecido: A Play Integrity API detecta que o dispositivo está executando um SO desconhecido (a verificação basicIntegrity é bem-sucedida, mas a ctsProfileMatch falha).

SO comprometido: A Play Integrity API detecta que o dispositivo está executando um SO comprometido (a verificação basicIntegrity falha).

Falha na avaliação baseada em hardware: A Play Integrity API detecta que o dispositivo não possui uma garantia forte de integridade do sistema, caso o rótulo MEETS_STRONG_INTEGRITY não apareça no campo de integridade do dispositivo.

Ações disponíveis:

Limpar dados corporativos (padrão): Desvincular e limpar os dados de trabalho (dispositivo inteiro se totalmente gerenciado, ou apenas o perfil de trabalho para perfis proprietários).

Nenhuma ação: Manter o dispositivo vinculado e não fazer nada automaticamente.

Ao selecionar **Limpar dados corporativos**, você também pode configurar as opções de limpeza:

Preservar a proteção de restauração de fábrica: Preservar os dados de Proteção de Restauração de Fábrica (FRP) ao limpar o dispositivo.

Limpar armazenamento externo: Limpar adicionalmente o armazenamento externo do dispositivo (como cartões SD) ao realizar a limpeza.

Limpar eSIMs: Para dispositivos de propriedade da empresa, isso remove todos os eSIMs do dispositivo quando o dispositivo é limpo. Em dispositivos de propriedade pessoal, isso removerá os eSIMs gerenciados (eSIMs que foram adicionados via comando ADD_ESIM) nos dispositivos, e nenhum eSIM de propriedade pessoal será removido.

1. Tempo máximo para bloqueio

Tempo máximo (em segundos) de atividade do usuário até que o dispositivo seja bloqueado. Um valor de 0 significa que não há restrição.

2. Permanecer ligado ao carregar

Os modos de bateria conectada para os quais o dispositivo permanece ligado. Ao usar esta configuração, recomenda-se limpar **Tempo máximo para bloqueio** para que o dispositivo não se bloqueie enquanto estiver ligado.

Carregador AC: A fonte de alimentação é um carregador AC.

Porta USB: A fonte de alimentação é uma porta USB.

Carregador sem fio: A fonte de alimentação é sem fio.

3. Keyguard desativado

Se verdadeiro, isso desativa a tela de bloqueio para telas primárias e/ou secundárias. Esta política é suportada apenas no modo de gerenciamento de dispositivo dedicado.

4. Requisitos de senha

Políticas de requisitos de senha.

Use **Configurar requisitos de senha** para adicionar um ou mais blocos de requisitos de senha. Use **Limpar tudo** para remover todos os requisitos de senha configurados.

Os requisitos de senha podem usar o escopo **Auto** (requisito único) ou escopos separados de **Dispositivo/Perfil de trabalho**. Requisitos baseados em complexidade devem ser combinados

com requisitos baseados em qualidade para o mesmo escopo.

4.1. Escopo

O escopo ao qual o requisito de senha se aplica.

Auto: O escopo não é especificado. Os requisitos de senha são aplicados ao perfil de trabalho para dispositivos com perfil de trabalho e a todo o dispositivo para dispositivos totalmente gerenciados ou dedicados.

Dispositivo: Os requisitos de senha são aplicados apenas ao dispositivo.

Perfil de trabalho: Os requisitos de senha são aplicados apenas ao perfil de trabalho.

4.2. Tamanho do histórico de senhas

O tamanho do histórico de senhas. Após definir este campo, o usuário não poderá inserir uma nova senha que seja igual a qualquer senha no histórico. Um valor de 0 significa que não há restrição.

4.3. Máximo de tentativas de senha incorretas para limpeza de dados

Número de senhas incorretas para desbloqueio do dispositivo que podem ser inseridas antes que o dispositivo seja limpo. Um valor de 0 significa que não há restrição.

4.4. Tempo de expiração da senha (dias)

Esta configuração força o usuário a atualizar periodicamente sua senha após o número de dias especificado.

4.5. Exigir desbloqueio por senha

O período de tempo após um dispositivo ou perfil de trabalho ser desbloqueado por meio de uma forma de autenticação forte (senha, PIN, padrão) durante o qual ele pode ser desbloqueado usando qualquer outro método de autenticação (ex: impressão digital, agentes de confiança, rosto). Após o término do período especificado, apenas formas de autenticação forte poderão ser usadas para desbloquear o dispositivo ou perfil de trabalho.

Padrão do dispositivo: O período de tempo limite é definido como o padrão do dispositivo.

Todos os dias: O período de tempo limite é definido para 24 horas.

4.6. Qualidade da senha

A qualidade de senha exigida.

Complexidade alta: Define a faixa de alta complexidade de senha como: No Android 12 ou superior: PIN sem sequências repetitivas (4444) ou ordenadas (1234, 4321, 2468),

comprimento de pelo menos 8 caracteres; alfabética, comprimento de pelo menos 6 caracteres; alfanumérica, comprimento de pelo menos 6 caracteres.

Complexidade média: Define a faixa de complexidade média de senha como: PIN sem sequências repetitivas (4444) ou ordenadas (1234, 4321, 2468), comprimento de pelo menos 4 caracteres; alfabética, comprimento de pelo menos 4 caracteres; alfanumérica, comprimento de pelo menos 4 caracteres.

Complexidade baixa: Define a faixa de baixa complexidade de senha como: padrão; PIN com sequências repetitivas (4444) ou ordenadas (1234, 4321, 2468).

Nenhum: Não há requisitos de senha.

Fraca: O dispositivo deve ser protegido, no mínimo, com uma tecnologia de reconhecimento biométrico de baixa segurança. Isso inclui tecnologias que podem reconhecer a identidade de um indivíduo e que são aproximadamente equivalentes a um PIN de 3 dígitos (detecção falsa inferior a 1 em 1.000).

Qualquer uma: Uma senha é necessária, mas não há restrições sobre o que a senha deve conter.

Numérica: A senha deve conter caracteres numéricos.

Numérica complexa: A senha deve conter caracteres numéricos sem sequências repetitivas (4444) ou ordenadas (1234, 4321, 2468).

Alfabética: A senha deve conter caracteres alfabéticos (ou símbolos).

Alfanumérica: A senha deve conter caracteres numéricos e alfabéticos (ou símbolos).

Complexa: A senha deve atender aos requisitos mínimos especificados em `passwordMinimumLength`, `passwordMinimumLetters`, `passwordMinimumSymbols`, etc. Por exemplo, se `passwordMinimumSymbols` for 2, a senha deve conter pelo menos dois símbolos.

4.7. Comprimento mínimo

O comprimento mínimo permitido para a senha. Um valor de 0 significa que não há restrição.

4.8. Mínimo de letras

Número mínimo de letras exigido na senha.

4.9. Mínimo de letras minúsculas

Número mínimo de letras minúsculas exigido na senha.

4.10. Mínimo de letras maiúsculas

Número mínimo de letras maiúsculas exigido na senha.

4.11. Mínimo de caracteres não alfabéticos

Número mínimo de caracteres não alfabéticos (dígitos numéricos ou símbolos) exigido na senha.

4.12. Mínimo de dígitos numéricos

Número mínimo de dígitos numéricos exigido na senha.

4.13. Mínimo de símbolos

Número mínimo de símbolos exigido na senha.

4.14. Bloqueio unificado

Controla se um bloqueio unificado é permitido para o dispositivo e o perfil de trabalho em dispositivos com Android 9 ou superior que possuam um perfil de trabalho. Isso não tem efeito em outros dispositivos.

Permitir bloqueio unificado: Um bloqueio comum para o dispositivo e o perfil de trabalho é permitido.

Exigir bloqueio de trabalho separado: Um bloqueio separado para o perfil de trabalho é exigido.

5. Restauração de fábrica desativada

Se a restauração de fábrica pelas configurações está desativada. Aplica-se apenas a dispositivos totalmente gerenciados.

6. Proteção de restauração de fábrica

Endereços de e-mail dos administradores do dispositivo para a proteção de restauração de fábrica. Quando o dispositivo sofrer uma restauração de fábrica não autorizada, será necessário que um desses administradores faça login com o e-mail e a senha da conta do Google para desbloquear o dispositivo. Se nenhum administrador for especificado, o dispositivo não oferecerá proteção de restauração de fábrica. Aplica-se apenas a dispositivos totalmente gerenciados.

E-mails de administradores: use **Ativar Proteção de Restauração de Fábrica** para começar a configurar os administradores. Em seguida, use **Adicionar e-mail de administrador** para adicionar endereços e remova-os com a ação de excluir.

7. Recursos do bloqueio de tela

Recursos de bloqueio de tela que podem ser desativados.

7.1. Desativar tudo

Desativa todas as personalizações atuais e futuras do bloqueio de tela.

7.2. Desativar câmera

Desativa a câmera em telas de bloqueio seguras (ex: PIN).

7.3. Desativar notificações

Desativa a exibição de todas as notificações em telas de bloqueio seguras.

7.4. Desativar notificações não ocultas

Desativa a exibição de notificações não ocultas em telas de bloqueio seguras.

7.5. Ignorar estado do agente de confiança

Ignorar o estado do agente de confiança em telas de bloqueio seguras.

7.6. Desativar impressão digital

Desativa o sensor de impressão digital em telas de bloqueio seguras.

7.7. Desativar entrada de texto em notificações

Desativa a entrada de texto em notificações em telas de bloqueio seguras.

7.8. Desativar autenticação facial

Desativa a autenticação facial em telas de bloqueio seguras.

7.9. Desativar autenticação de íris

Desativa a autenticação de íris em telas de bloqueio seguras.

7.10. Desativar toda a autenticação biométrica

Desativa toda a autenticação biométrica em telas de bloqueio seguras.

7.11. Desativar todos os atalhos

Desativa todos os atalhos na tela de bloqueio segura no Android 14 ou superior.

Multimídia

Nesta seção, você pode configurar o comportamento da câmera/microfone, o acesso a dados via USB, impressão e restrições relacionadas à tela.

1. Acesso à câmera

Controla o uso da câmera e se o usuário pode acessar a opção de alternância de acesso à câmera (Android 12+). Em geral, desativar a câmera aplica-se a todo o dispositivo em dispositivos totalmente gerenciados e apenas dentro do perfil de trabalho em dispositivos com perfil de trabalho.

Escolha do usuário (padrão): Comportamento padrão do dispositivo. As câmeras estão disponíveis e (Android 12+) o usuário pode alternar o acesso à câmera.

Desativado: Todas as câmeras são desativadas (totalmente gerenciado: em todo o dispositivo; perfil de trabalho: apenas para aplicativos do perfil de trabalho). A opção de alternância de acesso à câmera não tem efeito no escopo gerenciado.

Imposto: As câmeras estão disponíveis. Em dispositivos totalmente gerenciados com Android 12+, o usuário não pode alternar o acesso à câmera. Em outros dispositivos/versões, isso funciona como a Escolha do usuário.

2. Acesso ao microfone

Em dispositivos totalmente gerenciados, controla o uso do microfone e se o usuário pode acessar a opção de alternância de acesso ao microfone (Android 12+). Esta configuração não tem efeito em dispositivos que não são totalmente gerenciados.

Escolha do usuário (padrão): Comportamento padrão. O microfone está disponível e (Android 12+) o usuário pode alternar o acesso ao microfone.

Desativado: O microfone é desativado (em todo o dispositivo). A opção de alternância de acesso ao microfone não tem efeito.

Imposto: O microfone está disponível. No Android 12+, o usuário não pode alternar o acesso ao microfone. No Android 11 ou inferior, isso funciona como a Escolha do usuário.

3. Acesso a dados via USB

Controla quais arquivos e/ou dados podem ser transferidos via USB. Suportado apenas em dispositivos de propriedade da empresa.

Não permitir transferência de arquivos (padrão): As transferências de arquivos não são permitidas, mas outras conexões de dados USB (ex: mouse/teclado) são permitidas.

Não permitir transferência de dados: Todos os tipos de transferências de dados via USB são proibidos (Android 12+ com USB HAL 1.3+). Se não for suportado, o dispositivo retornará para Não permitir transferência de arquivos.

Permitir transferência de dados: Todos os tipos de transferências de dados via USB são permitidos.

4. Impressão

Controla se a impressão é permitida (Android 9+).

Permitido (padrão): A impressão é permitida.

Não permitido: A impressão não é permitida (Android 9+).

5. Configurações de brilho da tela

Controla o modo de brilho da tela e (opcionalmente) o valor do brilho.

Modo de brilho da tela:

Escolha do usuário (padrão): O usuário tem permissão para configurar o brilho da tela.

Automático: O brilho é automático e o usuário não pode alterá-lo. Você ainda pode definir um valor de brilho, que é usado como parte do ajuste automático (Android 9+ totalmente gerenciado; perfis de trabalho em Android 15+ de propriedade da empresa).

Fixo: O brilho é definido para o valor configurado e o usuário não pode alterá-lo. O valor de brilho é obrigatório (Android 9+ totalmente gerenciado; perfis de trabalho em Android 15+ de propriedade da empresa).

Brilho da tela:

Valor de 1 a 255 (1 = mínimo, 255 = máximo). Um valor de 0 significa que nenhum valor de brilho foi definido.

6. Configurações de tempo limite da tela

Controla se o usuário pode configurar o tempo limite da tela e, quando aplicado, o valor do tempo limite.

O campo **Modo de tempo limite da tela** permite escolher entre o comportamento controlado pelo usuário e o aplicado.

Escolha do usuário (padrão): O usuário tem permissão para configurar o tempo limite da tela.

Aplicado: O tempo limite da tela é definido para o valor configurado e o usuário não pode alterá-lo (Android 9+ totalmente gerenciado; perfis de trabalho em Android 15+ de propriedade da empresa).

Tempo limite da tela:

Duração do tempo limite em segundos. O valor deve ser maior que 0. Se for maior que **Tempo máximo para bloqueio**, o sistema pode ajustá-lo e reportar não conformidade.

7. Captura de tela desativada

Se a captura de tela está desativada.

8. Ajuste de volume desativado

Se o ajuste do volume principal está desativado.

9. Montagem de mídia física desativada

Se a montagem de mídia física externa está desativada.

Celular

Nesta seção, você pode configurar políticas relacionadas ao celular.

1. Modo avião

Controla se o modo avião pode ser ativado ou desativado pelo usuário.

Escolha do usuário (padrão): O usuário tem permissão para ativar ou desativar o modo avião.

Desativado: O modo avião está desativado. O usuário não tem permissão para ativar o modo avião. Suportado no Android 9 ou superior.

2. Celular 2G

Controla se a configuração de celular 2G pode ser ativada ou desativada pelo usuário.

Escolha do usuário (padrão): O usuário tem permissão para ativar ou desativar o celular 2G.

Desativado: O celular 2G está desativado. O usuário não tem permissão para ativar o celular 2G via configurações. Suportado no Android 14 ou superior.

3. Substituir APNs

Controla se a substituição de APNs está ativada ou desativada. Quando ativada, apenas os APNs de substituição configurados são usados e todos os outros APNs no dispositivo são ignorados.

Desativado (padrão): Todas as configurações de APN configuradas são salvas no dispositivo, mas estão desativadas e não têm efeito. Todos os outros APNs no dispositivo permanecem em uso.

Ativado: Apenas os APNs de substituição são usados, e todos os outros APNs são ignorados. Esta configuração só pode ser configurada em dispositivos totalmente gerenciados com Android 10 ou superior.

4. Configurações de APN

Configure uma ou mais entradas de APN. Use **Adicionar APN** para criar uma entrada e **Remover APN** para excluí-la.

Cada APN possui campos obrigatórios:

Tipos de APN: Selecione um ou mais tipos de tráfego para esta APN (a disponibilidade depende do modo de gerenciamento e da versão do Android).

Nome da APN: O identificador da APN fornecido pela sua operadora.

Nome de exibição: Nome amigável exibido na interface.

Campos de APN opcionais:

Tipo de autenticação, Nome de usuário, Senha: Configure a autenticação da operadora (se necessário).

Protocolo e Protocolo de Roaming: Configuração do protocolo IP.

Tipos de rede: Restrinja as tecnologias celulares que a APN pode usar (por exemplo, LTE/5G NR).

Endereço do proxy e Porta do proxy: Proxy HTTP para tráfego de dados (se aplicável).

Endereço do proxy MMS, Porta do proxy MMS, MMSC (URI do Centro MMS): Configurações relacionadas a MMS.

ID do Operador Numérico (MCC+MNC) e ID da Operadora: Campos de identificação da operadora.

Configuração Always On: Se a sessão PDU ativada por esta APN deve ser sempre ativa (always-on). Suportado no Android 15 ou superior.

Tipo de MVNO: Tipo de identificador do operador de rede móvel virtual.

MTU IPv4 e MTU IPv6: Unidade Máxima de Transmissão para rotas IPv4/IPv6. Suportado no Android 13 ou superior.

5. Configuração de transmissão celular desativada

Se a configuração de transmissão celular está desativada.

6. Configuração de redes móveis desativada

Se a configuração de redes móveis está desativada.

7. Dados de roaming desativados

Se os serviços de dados de roaming estão desativados.

8. Chamadas de saída desativadas

Se as chamadas de saída estão desativadas.

9. SMS desativado

Se o envio e recebimento de mensagens SMS está desativado.

10. Configuração de Fatiamento de Rede 5G

Configure as definições de serviço de rede preferencial para habilitar o fatiamento de rede 5G empresarial. Você pode configurar até 5 fatias empresariais e atribuir aplicativos a redes específicas para o roteamento otimizado de tráfego.

10.1. Rede Preferencial Padrão

ID da rede preferencial padrão para aplicativos que não estão na lista de aplicativos, ou se a **Rede Preferencial** de um aplicativo não estiver definida. Deve haver uma configuração para o ID de rede especificado (a menos que esteja definido como **Sem Rede Preferencial**).

Observação: Aplicativos críticos como **com.google.android.apps.work.clouddpc** e **com.google.android.gms** estão excluídos desta configuração padrão.

10.2. Configurações de Serviço de Rede

Use **Adicionar Configuração de Rede** para criar uma configuração de fatia. Você pode adicionar até 5 configurações. Cada configuração possui:

ID da Rede Preferencial (Atribuído Automaticamente): O ID da rede é atribuído automaticamente e não pode ser alterado.

Fallback para Conexão Padrão: Se o retorno para a rede padrão de todo o dispositivo é permitido. Se não for permitido, os aplicativos não poderão acessar a internet caso a fatia 5G esteja indisponível.

Redes não correspondentes: Se os aplicativos sujeitos a esta configuração podem usar redes que não sejam o serviço preferencial. Se definido como **Não permitido**, o **Fallback para Conexão Padrão** também deve ser **Não permitido**. Requer Android 14 ou superior.

Rede

Nesta seção, você pode configurar políticas relacionadas à rede.

As configurações de Wi-Fi podem ser provisionadas e gerenciadas pelo sistema por meio das **configurações de Wi-Fi**. Dependendo do valor definido em **Configurar Wi-Fi**, os usuários podem ter controle limitado ou nenhum sobre a adição/modificação de redes.

Estado do rádio do dispositivo

1. Estado do Wi-Fi

Controla o estado atual do Wi-Fi e se o usuário pode alterar seu estado.

Escolha do usuário (padrão): O usuário tem permissão para ativar/desativar o Wi-Fi.

Ativado: O Wi-Fi está ligado e o usuário não tem permissão para desligá-lo (Android 13+).

Desativado: O Wi-Fi está desligado e o usuário não tem permissão para ligá-lo (Android 13+).

2. Nível mínimo de segurança do Wi-Fi

O nível mínimo de segurança exigido para redes Wi-Fi às quais o dispositivo pode se conectar. Suportado no Android 13 ou superior, para dispositivos totalmente gerenciados e perfis de trabalho em dispositivos de propriedade da empresa.

Rede aberta (padrão): O dispositivo pode se conectar a todos os tipos de redes Wi-Fi.

Rede pessoal: Não permite redes Wi-Fi abertas; exige pelo menos segurança pessoal (por exemplo, WPA2-PSK).

Rede corporativa: Exige redes EAP corporativas; não permite redes Wi-Fi abaixo deste nível de segurança.

Rede corporativa de 192 bits: Exige redes corporativas de 192 bits; opção mais rigorosa.

3. Estado de banda ultralarga (UWB)

Controla o estado da configuração de banda ultralarga e se o usuário pode ativá-la ou desativá-la.

Escolha do usuário (padrão): O usuário tem permissão para ativar ou desativar o UWB.

Desativado: O UWB está desativado e o usuário não tem permissão para ativá-lo via configurações (Android 14+).

Gerenciamento de conectividade do dispositivo

4. Compartilhamento via Bluetooth

Controla se o compartilhamento via Bluetooth é permitido.

Permitido: O compartilhamento via Bluetooth é permitido (padrão em dispositivos totalmente gerenciados, Android 8+).

Não permitido: O compartilhamento via Bluetooth não é permitido (padrão em perfis de trabalho, Android 8+).

5. Configurar Wi-Fi

Controla os privilégios de configuração do Wi-Fi. Dependendo da opção selecionada, o usuário terá controle total, limitado ou nenhum sobre a configuração de redes Wi-Fi.

Permitir configuração de Wi-Fi (padrão): O usuário tem permissão para configurar o Wi-Fi.

Não permitir adição de configuração de Wi-Fi: A adição de novas configurações de Wi-Fi não é permitida. O usuário pode alternar entre redes já configuradas (Android 13+; dispositivos totalmente gerenciados e perfis de trabalho em dispositivos de propriedade da empresa).

Não permitir configuração de Wi-Fi: Não permite a configuração de redes Wi-Fi. Para dispositivos totalmente gerenciados, isso remove as redes configuradas pelo usuário e mantém apenas as redes configuradas via **configurações de Wi-Fi**. Para perfis de trabalho em dispositivos de propriedade da empresa, as redes existentes não são afetadas, mas os usuários não podem adicionar/remover/modificar redes Wi-Fi.

Quando a configuração de Wi-Fi está desativada e o dispositivo não consegue se conectar no momento da inicialização, o sistema pode exibir a **válvula de escape de rede** para permitir que o usuário se conecte temporariamente e atualize a política.

6. Configurações de Wi-Fi Direct

Controla a configuração e o uso das definições de Wi-Fi Direct. Suportado em dispositivos de propriedade da empresa com Android 13 ou superior.

Permitir (padrão): O usuário tem permissão para usar o Wi-Fi Direct.

Não permitir: O usuário não tem permissão para usar o Wi-Fi Direct.

7. Configurações de roteamento (tethering)

Controla as configurações de roteamento (tethering). Dependendo do valor definido, o usuário pode ter o uso de diferentes formas de roteamento parcialmente ou totalmente proibido.

Permitir todo o roteamento (padrão): Permite a configuração e o uso de todas as formas de roteamento.

Não permitir roteamento via Wi-Fi: Impede que o usuário utilize o roteamento via Wi-Fi (Android 13+ de propriedade da empresa).

Não permitir todo o roteamento: Impede todas as formas de roteamento (dispositivos totalmente gerenciados + perfis de trabalho em dispositivos de propriedade da empresa).

8. Política de SSID do Wi-Fi

Restrições sobre a quais SSIDs de Wi-Fi o dispositivo pode se conectar (isso não afeta quais redes podem ser configuradas no dispositivo). Suportado em dispositivos de propriedade da empresa com Android 13 ou superior.

Lista de bloqueio de SSID (padrão): O dispositivo não pode se conectar a nenhuma rede Wi-Fi cujo SSID esteja listado, mas pode se conectar a outras redes.

Lista de permissão de SSID: O dispositivo pode se conectar apenas aos SSIDs listados. A lista de SSID não deve estar vazia.

Use **Adicionar SSID** para adicionar entradas. Dependendo do tipo de política selecionada, a lista é interpretada como SSIDs permitidos ou negados.

Na interface do Editor de Políticas, a lista de SSID é rotulada como **SSIDs de Wi-Fi permitidos** para listas de permissão e **SSIDs de Wi-Fi negados** para listas de bloqueio.

9. Configurações de roaming de Wi-Fi

Configure o modo de roaming de Wi-Fi por SSID. Use **Adicionar configuração de roaming de Wi-Fi** para criar entradas.

Cada entrada inclui:

SSID: O SSID ao qual a configuração de roaming se aplica (obrigatório).

Modo de roaming de Wi-Fi: Padrão / Desativado / Agressivo. As opções Desativado e Agressivo exigem Android 15+ e são suportadas apenas em dispositivos totalmente gerenciados e perfis de trabalho em dispositivos de propriedade da empresa.

Restrições de rede

10. Bluetooth desativado

Se o Bluetooth está desativado. Prefira esta configuração em vez de "Configuração de Bluetooth desativada", pois a configuração de Bluetooth desativada pode ser contornada pelo usuário.

11. Compartilhamento de contatos via Bluetooth desativado

Se o compartilhamento de contatos via Bluetooth está desativado.

12. Configuração de Bluetooth desativada

Se a configuração de Bluetooth está desativada.

13. Redefinição de rede desativada

Se a redefinição das configurações de rede está desativada.

14. Beam de saída desativado

Se o uso de NFC para transmitir dados de aplicativos está desativado.

VPN

15. Aplicativo de VPN sempre ativa (Always On VPN)

Especifique o nome do pacote de um aplicativo de VPN sempre ativa para garantir que os dados dos aplicativos gerenciados especificados passem sempre por uma VPN configurada.

Nota: Este recurso exige a implantação de um cliente VPN que suporte os recursos de "Sempre Ativa" (Always On) e de VPN por aplicativo.

16. Bloqueio de rede via VPN (VPN lockdown)

Impede o uso de rede quando a VPN não estiver conectada.

17. Configuração de VPN desativada

Se a configuração de VPN está desativada.

Proxy e serviços de rede

18. Serviço de rede preferencial

Controla se o serviço de rede preferencial está ativado no perfil de trabalho. Por exemplo, uma organização pode ter um acordo com uma operadora para que os dados de trabalho sejam enviados por meio de um serviço de rede da operadora dedicado ao uso corporativo (por exemplo, um slice corporativo em redes 5G). Isso não tem efeito em dispositivos totalmente gerenciados.

Desativado: O serviço de rede preferencial está desativado no perfil de trabalho.

Ativado: O serviço de rede preferencial está ativado no perfil de trabalho.

Se você usa o fatiamento de rede corporativa (network slicing), configure também a **Configuração de fatiamento de rede 5G** no painel de política **Celular** e atribua os aplicativos a um slice usando a configuração de **Rede preferencial**.

19. Proxy global recomendado

O proxy HTTP global independente de rede. Normalmente, os proxies devem ser configurados por rede nas configurações de Wi-Fi. Um proxy global pode ser útil para configurações incomuns, como filtragem interna geral. O proxy global é apenas uma recomendação e alguns aplicativos podem ignorá-lo.

Desativado

Proxy direto

Proxy de autoconfiguração (PAC)

19.1. Host

O host do proxy direto.

19.2. Porta

A porta do proxy direto.

19.3. URI do PAC

A URI do script PAC usado para configurar o proxy.

19.4. Hosts excluídos

Para um proxy direto, os hosts pelos quais o proxy é ignorado. Os nomes de host podem conter caracteres curinga como ***.example.com**.

Use **Adicionar host excluído** para adicionar entradas (disponível apenas para proxy direto).

Configurações de Wi-Fi

Defina as configurações de rede Wi-Fi que o sistema aplicará nos dispositivos. Use **Adicionar configuração de Wi-Fi** para criar uma entrada e remova-a com a ação de excluir.

20. Campos de configuração de Wi-Fi

Cada configuração inclui:

Nome da configuração: Obrigatório.

SSID: Obrigatório.

Conectar automaticamente: Se a rede deve ser conectada automaticamente quando estiver ao alcance.

Transição Rápida: Se o cliente deve tentar usar a Transição Rápida (IEEE 802.11r-2008) com a rede.

SSID oculto: Se o SSID será transmitido.

Modo de randomização de MAC: Hardware ou Automático (Android 13+).

20.1. Segurança

Opções de segurança de Wi-Fi:

WEP-PSK: WEP (Chave Pré-Compartilhada).

WPA-PSK: WPA/WPA2/WPA3-Personal (Chave Pré-Compartilhada).

WPA-EAP: WPA/WPA2/WPA3-Enterprise (Extensible Authentication Protocol).

Modo WPA3 de 192 bits: Rede WPA-EAP que permite apenas o modo WPA3 de 192 bits.

20.2. Passphrase (Chave Pré-Compartilhada)

Exibido quando a Segurança é **WEP-PSK** ou **WPA-PSK**. A frase de passagem é obrigatória.

20.3. Método EAP (Enterprise)

Exibido quando a Segurança é **WPA-EAP** ou **Modo WPA3 de 192 bits**. Selecione um método EAP externo:

EAP-TLS

EAP-TTLS

PEAP

EAP-SIM

EAP-AKA

20.4. Autenticação de fase 2

Exibido para métodos externos de tunelamento (**EAP-TTLS** e **PEAP**).

MSCHAPv2

PAP

20.5. Credenciais EAP dos usuários

Quando ativado, o sistema aplica automaticamente as credenciais EAP nos dispositivos com base em cada usuário. Você pode configurar as credenciais do usuário na seção **Usuários**.

20.6. Certificado do cliente

Para **EAP-TLS**, você pode atribuir um certificado de cliente usado para a autenticação Wi-Fi. Para mais informações, leia a página [Gerenciamento de certificados](#).

Se um certificado já estiver atribuído, você pode usar **Abrir certificado** para visualizá-lo ou **Alterar certificado** para selecionar um diferente.

Como alternativa, você pode especificar o **Alias do par de chaves do certificado do cliente**, que faz referência a um certificado de cliente armazenado no chaveiro do Android e permitido para autenticação Wi-Fi.

Se tanto o **Certificado do cliente** quanto o **Alias do par de chaves do certificado do cliente** estiverem configurados, o alias do par de chaves será ignorado.

20.7. Identidade

Identidade do usuário. Para protocolos externos de tunelamento (PEAP, EAP-TTLS), esta é usada para autenticar dentro do túnel, e a **Identidade anônima** é usada para a identidade EAP fora do túnel. Para protocolos externos que não utilizam tunelamento, esta é usada para a identidade EAP.

20.8. Identidade anônima

Apenas para protocolos de tunelamento, isso indica a identidade do usuário apresentada ao protocolo externo.

20.9. Senha

Senha do usuário. Se não for especificada, o padrão será solicitar ao usuário.

20.10. Certificados CA do servidor

Lista de certificados CA a serem usados para verificar a cadeia de certificados do host. Pelo menos um certificado CA deve corresponder. Para mais informações, leia a página [Gerenciamento de certificados](#).

Use **Adicionar certificado CA do servidor** para adicionar entradas e remova-as com a ação de excluir.

20.11. Correspondências de sufixo de domínio

Uma lista de restrições para o nome de domínio do servidor. As entradas são usadas como requisitos de correspondência de sufixo em relação ao(s) nome(s) DNS do nome alternativo do assunto de um certificado de servidor de autenticação.

Sistema

Nesta seção, você pode configurar políticas relacionadas ao sistema.

1. Nível de API mínimo

O nível de API do Android mínimo permitido.

2. Política de criptografia

Se a criptografia está ativada.

Padrão: Este valor é ignorado, ou seja, nenhuma criptografia é exigida.

Ativado sem senha: A criptografia é exigida, mas não é necessária uma senha para a inicialização.

Ativado com senha: A criptografia é exigida, com senha necessária para a inicialização.

3. Data e hora automáticas

Se a data, hora e fuso horário automáticos estão ativados em um dispositivo de propriedade da empresa.

Escolha do usuário (padrão): A data, hora e fuso horário automáticos ficam a critério do usuário.

Imposto: Força a configuração de data, hora e fuso horário automáticos no dispositivo.

4. Configurações do desenvolvedor

Controla o acesso às configurações do desenvolvedor: opções do desenvolvedor e inicialização segura.

Desativado (padrão): Desativa todas as configurações do desenvolvedor e impede que o usuário acesse essas opções.

Permitido: Permite todas as configurações do desenvolvedor. O usuário pode acessar e, opcionalmente, configurar as definições.

5. Modo Common Criteria

Controla o Modo Common Criteria — padrões de segurança definidos no Common Criteria for Information Technology Security Evaluation (CC). A ativação do Modo Common Criteria aumenta certos componentes de segurança no dispositivo (por exemplo: criptografia AES-GCM de chaves de longo prazo do Bluetooth, validação adicional para alguns certificados de rede e verificações de integridade da política criptográfica). O Modo Common Criteria é suportado apenas em dispositivos de propriedade da empresa com Android 11 ou superior. Aviso: O Modo Common Criteria impõe um modelo de segurança rigoroso, normalmente exigido apenas para organizações altamente sensíveis. O uso padrão do dispositivo pode ser afetado; ative-o apenas se for necessário.

Desativado (padrão): Desativa o Modo Common Criteria.

Ativado: Ativa o Modo Common Criteria.

6. Memory Tagging Extension (MTE)

Controla a Memory Tagging Extension (MTE) no dispositivo.

Escolha do usuário (padrão): O usuário pode optar por ativar ou desativar o MTE no dispositivo (se suportado pelo dispositivo).

Imposto: O MTE é ativado e o usuário não tem permissão para alterá-lo (Android 14+; suportado em dispositivos totalmente gerenciados e perfis de trabalho em dispositivos de propriedade da empresa).

Desativado: O MTE é desativado e o usuário não tem permissão para alterá-lo (Android 14+; suportado apenas em dispositivos totalmente gerenciados).

7. Proteção de conteúdo

Controla se a proteção de conteúdo (que verifica aplicativos enganosos) está ativada. Isso é suportado no Android 15 ou superior.

Desativado (padrão): A proteção de conteúdo está desativada e o usuário não pode alterar isso.

Imposto: A proteção de conteúdo está ativada e o usuário não pode alterar isso (Android 15+).

Escolha do usuário: A proteção de conteúdo não é controlada pela política; o usuário pode escolher (Android 15+).

8. Conteúdo de assistência

Controla se o AssistContent pode ser enviado para um aplicativo privilegiado, como um aplicativo de assistência (por exemplo, o Circle to Search). O AssistContent inclui capturas de tela e informações sobre um aplicativo, como o nome do pacote. Isso é suportado no Android 15 ou superior.

Permitido (padrão): O conteúdo de assistência pode ser enviado para um aplicativo privilegiado (Android 15+).

Não permitido: O envio de conteúdo de assistência para um aplicativo privilegiado é bloqueado (Android 15+).

9. Desativação de janelas de criação

Se a criação de janelas além das janelas de aplicativos está desativada. Esta opção impede a exibição das seguintes interfaces do sistema: toasts e snackbars, atividades de telefone (como chamadas recebidas) e atividades de telefone prioritárias (como chamadas em andamento), alertas do sistema, erros do sistema e sobreposições do sistema.

10. Saída de emergência de rede

Se a saída de emergência de rede está ativada. Se uma conexão de rede não puder ser estabelecida no momento da inicialização, a saída de emergência solicitará que o usuário se conecte temporariamente a uma rede para atualizar a política do dispositivo. Após a aplicação da política, a rede temporária será esquecida e o dispositivo continuará a inicialização. Isso evita que o usuário fique impossibilitado de se conectar a uma rede caso não haja uma rede adequada na última política aplicada e o dispositivo inicie diretamente em um aplicativo no modo de tarefa bloqueada (lock task mode), ou se o usuário estiver impossibilitado de acessar as configurações do dispositivo por outros motivos.

11. Atividades padrão

Uma lista de atividades padrão para lidar com intents que correspondam a um filtro de intent específico. Por exemplo, este recurso permitiria aos administradores de TI escolher qual aplicativo de navegador abre links da web automaticamente ou qual aplicativo de inicialização (launcher) é usado ao tocar no botão de início.

Use **Adicionar atividade padrão** para criar entradas. Dentro de uma entrada, use **Adicionar ação** e **Adicionar categoria** para construir o filtro de intent.

11.1. Atividade de receptor

A atividade que deve ser o manipulador de intent padrão. Deve ser um nome de componente Android, por exemplo: `com.android.enterprise.app/.MainActivity`. Alternativamente, o valor pode ser o nome do pacote de um aplicativo, o que faz com que a Política de Dispositivo Android escolha uma atividade apropriada do aplicativo para lidar com a intent.

11.2. Ação

As ações de intent para correspondência no filtro. Se houver ações incluídas no filtro, a ação da intent deve ser um desses valores para que ocorra a correspondência. Se nenhuma ação for incluída, a ação da intent será ignorada.

11.3. Categoria

As categorias de intent para correspondência no filtro. Uma intent inclui as categorias que ela exige, e todas elas devem estar incluídas no filtro para que ocorra a correspondência. Em outras palavras, adicionar uma categoria ao filtro não tem impacto na correspondência, a menos que essa categoria seja especificada na intent.

12. Métodos de entrada permitidos

Especifica os métodos de entrada permitidos.

Todos permitidos: Nenhuma restrição aplicada. Todos os métodos de entrada são permitidos.

Apenas do sistema: Apenas os métodos de entrada integrados do sistema são permitidos.

Apenas do sistema e fornecidos: Apenas os métodos de entrada fornecidos e os integrados do sistema são permitidos.

12.1. Métodos de entrada permitidos

Nomes de pacotes de métodos de entrada que são permitidos. Aplica-se apenas quando **Métodos de entrada permitidos** estiver definido como **Apenas do sistema e fornecidos**.

Use **Adicionar método de entrada** para adicionar entradas e remova-as com a ação de excluir.

13. Serviços de acessibilidade permitidos

Especifica os serviços de acessibilidade permitidos.

Todos permitidos: Qualquer serviço de acessibilidade pode ser usado.

Apenas do sistema: Apenas os serviços de acessibilidade integrados do sistema podem ser usados.

Apenas do sistema e fornecidos: Apenas os serviços de acessibilidade fornecidos e os integrados do sistema podem ser usados.

13.1. Serviços de acessibilidade permitidos

Serviços de acessibilidade permitidos. Aplica-se apenas quando **Serviços de acessibilidade permitidos** estiver definido como **Apenas do sistema e fornecidos**.

Use **Adicionar serviço de acessibilidade** para adicionar entradas e remova-as com a ação de excluir.

14. Política de atualização do sistema

Configuração para o gerenciamento de atualizações do sistema.

Padrão: Segue o comportamento de atualização padrão do dispositivo, que normalmente exige que o usuário aceite as atualizações do sistema.

Automático: Instala automaticamente assim que uma atualização estiver disponível.

Janela de manutenção: Instala automaticamente dentro de uma janela de manutenção diária. Isso também configura os aplicativos do Play para serem atualizados dentro da janela. Isso é altamente recomendado para dispositivos de quiosque, pois é a única maneira de atualizar aplicativos fixados permanentemente em primeiro plano pelo Play.

Adiar: Adia a instalação automática por até um máximo de 30 dias.

14.1. Janela de manutenção (Apenas para o modo Janela)

Quando a **Política de atualização do sistema** estiver definida como **Janela de manutenção**, você poderá definir a janela de manutenção diária usando os campos **de** e **até**.

14.2. Períodos de congelamento de atualização do sistema

Um período de tempo que se repete anualmente, no qual as atualizações do sistema via rede (OTA) são adiadas para congelar a versão do SO em execução no dispositivo. Para evitar o congelamento indefinido do dispositivo, cada período de congelamento deve ser separado por pelo menos 60 dias. Cada período de congelamento não deve exceder 90 dias.

Use **Adicionar período de congelamento de atualização do sistema** para criar entradas.

15. Provedores de credenciais padrão

Controla quais aplicativos têm permissão para atuar como provedores de credenciais no Android 14 ou superior.

Não permitido (padrão): Aplicativos com a política credentialProviderPolicy não especificada não têm permissão para atuar como um provedor de credenciais.

Não permitido, exceto sistema: Aplicativos com a política credentialProviderPolicy não especificada não têm permissão para atuar como um provedor de credenciais, exceto os provedores de credenciais padrão do fabricante (OEM).

Localização e cercas virtuais

Este painel agrupa as configurações de política do Android que controlam o relatório de localização do dispositivo, a imposição de localização e as definições de cercas virtuais. Use-o quando quiser que o Cerberus Enterprise colete as localizações dos dispositivos ou detecte quando os dispositivos entram ou saem de áreas configuradas.

Relatório de localização

Relatar localização

Ativa o relatório de geolocalização do dispositivo. Os dados de localização coletados por meio desta configuração são usados pelo [mapa de localização do dashboard](#), o histórico de localização na visão geral do dispositivo e o processamento de cercas virtuais.

Em dispositivos que não são totalmente gerenciados, os dados de localização ainda podem depender do aplicativo Cerberus Enterprise possuir as permissões de localização necessárias e dos serviços de localização estarem ativados no dispositivo.

Modo de localização

Controla a configuração de localização do dispositivo em dispositivos de propriedade da empresa.

- **Escolha do usuário:** os serviços de localização não são restringidos pela política.
- **Imposto:** os serviços de localização são ativados no dispositivo.
- **Desativado:** os serviços de localização são desativados no dispositivo.

Compartilhamento de localização desativado

Desativa o compartilhamento de localização para aplicativos de trabalho. Em dispositivos com proprietário de perfil, isso afeta o perfil de trabalho. Em dispositivos totalmente gerenciados, desativa a localização para todo o dispositivo e substitui o modo de localização do dispositivo.

Comportamento automático com cercas virtuais ativas

As cercas virtuais ativas exigem o relatório de localização para funcionar. Quando pelo menos uma cerca virtual estiver ativa, o Cerberus Enterprise mantém automaticamente as configurações de localização relacionadas consistentes.

- **Relatar localização** é forçado enquanto existirem cercas virtuais ativas.
- **Modo de localização** é forçado para **Imposto**.
- **Compartilhamento de localização desativado** é forçado para desativado.

Se você tentar desativar **Relatar localização** enquanto uma ou mais cercas virtuais estiverem ativas, o Cerberus Enterprise exibirá um diálogo de confirmação. Se você continuar, todas as cercas virtuais ativas na política serão desativadas.

Lista de cercas virtuais

Uma política pode conter até **10 cercas virtuais**. Os nomes das cercas virtuais devem ser exclusivos dentro da política.

Use **Adicionar cerca virtual** para criar uma nova entrada. Cada cerca virtual contém estes campos principais:

- **Nome**: obrigatório e exclusivo.
- **Latitude** e **Longitude**: o centro da área.
- **Raio (m)**: obrigatório, de **100** a **10000** metros.
- **Descrição**: notas opcionais para administradores.
- **Relatar entrada** e **Relatar saída**: escolha quais eventos de transição devem ser gerados.
- **Ativa**: ativa ou desativa a cerca virtual sem excluí-la.

Pelo menos uma das opções **Relatar entrada** ou **Relatar saída** deve permanecer ativada para cada cerca virtual.

Ferramentas de edição do mapa

Cada cartão de cerca virtual inclui uma visualização do mapa da área. Você pode editar a geometria pelo mapa ou pelos campos numéricos.

- Clique no mapa para mover o centro da cerca virtual quando a edição de área estiver desbloqueada.
- Use o botão **Localização atual** para centralizar o mapa na sua posição atual no navegador.
- Use o botão **Recentralizar mapa** para restaurar a visualização preferida para essa cerca virtual.
- Use o botão de bloqueio para evitar alterações acidentais na geometria da cerca virtual.

Onde os dados da cerca virtual aparecem

As transições de cercas virtuais podem ser revisadas na página [Visão geral do dispositivo](#) do Android, dentro da aba **Cerca virtual** do painel de localização. Essa aba mostra as transições em um mapa dedicado, juntamente com ferramentas de filtragem e a lista de transições.

Gerenciamento de usuários

Desativação de adição de usuário

Se a adição de novos usuários e perfis está desativada. Para dispositivos onde o `managementMode` é **DEVICE_OWNER**, este campo é ignorado e o usuário nunca tem permissão para adicionar ou remover usuários.

Desativação de modificação de contas

Se a adição ou remoção de contas está desativada.

Desativação de configuração de credenciais do usuário

Se a configuração de credenciais do usuário está desativada.

Desativação de remoção de usuário

Se a remoção de outros usuários está desativada.

Desativação de definição de ícone do usuário

Se a alteração do ícone do usuário está desativada.

Desativação de definição de papel de parede

Se a alteração do papel de parede está desativada.

Autenticação de configuração de conta de trabalho

Controla como os usuários se autenticam durante a configuração da conta de trabalho. Esta opção está disponível apenas para empresas Android com suporte de um domínio gerenciado pelo Google (Google Workspace).

Durante a configuração/registro do dispositivo, esta política influencia se o login em uma conta de trabalho é obrigatório, mas a configuração **Autenticar usando o Google** no Console de Administração do Google e o tipo de token de registro ainda podem exigir autenticação.

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

Para mais detalhes e solução de problemas, consulte [Registro de Autenticação usando o Google](#).

Tipos de conta bloqueados

Tipos de conta que não podem ser gerenciados pelo usuário. Esta opção impede que os usuários do dispositivo adicionem contas não aprovadas.

Use **Adicionar tipo de conta bloqueada** para adicionar um ou mais tipos de conta.

Cada entrada possui um campo **Tipo de conta** (obrigatório). Insira uma string como **com.google**. Remova uma entrada usando a ação de excluir.

Uso pessoal

Ao [provisionar um dispositivo de propriedade da empresa para uso profissional e pessoal](#), você pode especificar algumas regras para limitar como o usuário pode operar o dispositivo para uso pessoal, fora do perfil de trabalho.

Esta seção se aplica apenas a dispositivos de propriedade da empresa com perfil de trabalho. Ela não terá efeito em dispositivos totalmente gerenciados ou de propriedade pessoal.

1. Câmera desativada

Se a câmera será desativada.

2. Captura de tela desativada

Se a captura de tela será desativada.

3. Máximo de dias com o trabalho desativado

Controla por quanto tempo o perfil de trabalho pode permanecer desativado.

4. Compartilhamento via Bluetooth

Controla se o compartilhamento via Bluetooth é permitido no perfil pessoal de um dispositivo de propriedade da empresa com perfil de trabalho.

5. Espaço privado

Controla se um espaço privado é permitido no dispositivo.

6. Modo da Play Store

Este modo controla quais aplicativos são permitidos ou bloqueados para o usuário na Play Store do perfil pessoal.

Lista de bloqueio (padrão): Todos os aplicativos estão disponíveis e qualquer aplicativo que não deva estar no dispositivo deve ser explicitamente marcado como **Bloqueado** na seção **Aplicativos**.

Lista de permissão: Apenas os aplicativos explicitamente especificados na seção **Aplicativos** com o **Tipo de instalação** definido como **Disponível** podem ser instalados no perfil pessoal.

7. Aplicativos

Lista de aplicativos que devem ser permitidos ou bloqueados no perfil pessoal. O comportamento do conteúdo da lista depende do valor definido em **Modo da Play Store**.

Para adicionar um novo aplicativo da Play Store, clique no ícone +.

7.1. Tipo de instalação

Tipos de comportamentos de instalação que um aplicativo do perfil pessoal pode ter.

Bloqueado: O aplicativo é bloqueado e não pode ser instalado no perfil pessoal.

Disponível: O aplicativo está disponível para instalação no perfil pessoal.

8. Tipos de contas bloqueadas

Tipos de contas que não podem ser gerenciados pelo usuário. Esta opção impede que os usuários do dispositivo adicionem contas não aprovadas em seu perfil pessoal.

Políticas entre perfis

Aplica-se apenas a dispositivos com perfis pessoal e de trabalho.

Copiar/colar entre perfis

Se o texto copiado de um perfil (pessoal ou de trabalho) pode ser colado no outro perfil.

Não permitido (padrão): Impede que os usuários colem no perfil pessoal textos copiados do perfil de trabalho. Textos copiados do perfil pessoal podem ser colados no perfil de trabalho.

Permitido: O texto copiado em qualquer um dos perfis pode ser colado no outro perfil.

Compartilhamento de dados entre perfis

Se os dados de um perfil (pessoal ou de trabalho) podem ser compartilhados com aplicativos no outro perfil. Controla especificamente o compartilhamento simples de dados via intents. O gerenciamento de outros canais de comunicação entre perfis, como pesquisa de contatos, copiar/colar, ou aplicativos de trabalho e pessoais conectados, é configurado separadamente.

Não permitido: Impede o compartilhamento de dados tanto do perfil pessoal para o perfil de trabalho quanto do perfil de trabalho para o perfil pessoal.

Bloqueio de trabalho para pessoal (padrão): Impede que os usuários compartilhem dados do perfil de trabalho com aplicativos no perfil pessoal. Dados pessoais podem ser compartilhados com aplicativos de trabalho.

Permitido: Os dados de qualquer um dos perfis podem ser compartilhados com o outro perfil.

Padrão de widgets do perfil de trabalho

Comportamento padrão para os widgets do perfil de trabalho. Se um aplicativo específico não definir uma política de widgets, ele seguirá o padrão definido aqui.

Funções de aplicativos entre perfis

Controla se os aplicativos do perfil pessoal podem invocar funções de aplicativos do perfil de trabalho. Isso requer o Android 16 ou superior.

Esta configuração depende da opção de **Funções de aplicativos** de nível de política (na seção de Gerenciamento de apps). Se as Funções de aplicativos estiverem definidas como **Não permitido**, a API rejeitará as Funções de aplicativos entre perfis definidas como **Permitido**.

Contatos de trabalho no perfil pessoal

Se os contatos armazenados no perfil de trabalho podem ser exibidos em pesquisas de contatos e chamadas recebidas no perfil pessoal.

Permitido (padrão): Permite que os contatos do perfil de trabalho apareçam no perfil pessoal.

Não permitido: Impede que aplicativos do perfil pessoal acessem os contatos do perfil de trabalho e pesquisem por contatos de trabalho.

Não permitido, exceto sistema: Impede que a maioria dos aplicativos do perfil pessoal acesse os contatos do perfil de trabalho, exceto para os aplicativos padrão do fabricante (OEM), como Discador, Mensagens e Contatos (Android 14+).

Quando a opção Contatos de trabalho no perfil pessoal estiver configurada, você pode definir opcionalmente uma lista de entradas de **Nomes de pacotes isentos**. Dependendo do modo selecionado, essas isenções funcionam como uma lista de permissões ou uma lista de bloqueio para os aplicativos pessoais.

Relatório de status

Nesta seção, você pode configurar quais dados devem ser recuperados do dispositivo. Os dados de status podem ser visualizados na página do painel [Status do dispositivo](#).

Relatórios de aplicativos

Se os relatórios de aplicativos estão ativados. (Informações relatadas sobre um aplicativo instalado.)

Esta opção é exigida pelo sistema (para integração com aplicativos complementares) e está sempre ativada; ela não pode ser desativada.

Incluir aplicativos removidos

Se os aplicativos removidos são incluídos nos relatórios de aplicativos.

Configurações do dispositivo

Se o relatório de configurações do dispositivo está ativado. (Informações sobre as configurações de segurança no dispositivo.)

Informações de software

Se o relatório de informações de software está ativado. (Informações sobre o software do dispositivo.)

Informações de memória

Se o relatório de memória está ativado. (Um evento relacionado a medições de memória e armazenamento.)

Informações de rede

Se o relatório de informações de rede está ativado. (Informações de rede do dispositivo.)

Informações de tela

Se o relatório de telas está ativado. Os dados do relatório não estão disponíveis para dispositivos de propriedade pessoal com perfis de trabalho. (Informações de tela do dispositivo.)

Eventos de gerenciamento de energia

Se o relatório de eventos de gerenciamento de energia está ativado. Os dados do relatório não estão disponíveis para dispositivos de propriedade pessoal com perfis de trabalho.

Status do hardware

Se o relatório de status do hardware está ativado. Os dados do relatório não estão disponíveis para dispositivos de propriedade pessoal com perfis de trabalho.

Propriedades do sistema

Se o relatório de propriedades do sistema está ativado.

Modo de Critérios Comuns

Se o relatório do Modo de Critérios Comuns está ativado.

Diversos

1. Jogo easter egg desativado

Define se o jogo easter egg nas Configurações está desativado.

2. Pular dicas de primeiro uso

Sinalizador para pular as dicas no primeiro uso. O administrador da empresa pode ativar a recomendação do sistema para que os aplicativos pulem seus tutoriais de usuário e outras dicas introdutórias na inicialização.

3. Mensagem de suporte curta

Uma mensagem exibida ao usuário na tela de configurações sempre que uma funcionalidade for desativada pelo administrador. Se a mensagem tiver mais de 200 caracteres, ela poderá ser truncada.

4. Mensagem de suporte longa

Uma mensagem exibida ao usuário na tela de configurações de administradores do dispositivo.

5. Informações da tela de bloqueio do proprietário

As informações do proprietário do dispositivo que serão exibidas na tela de bloqueio.

6. Ações de configuração

Ações a serem realizadas durante o processo de configuração. Durante o registro, você pode exigir que o usuário abra um ou mais aplicativos necessários para a configuração do dispositivo.

Use **Adicionar ação de configuração** para criar entradas e remova-as com a ação de excluir.

6.1. Iniciar aplicativo

Nome do pacote do aplicativo a ser iniciado

6.2. Título

Fornece uma mensagem para o usuário, para explicar por que é necessário iniciar o aplicativo.

6.3. Descrição

Fornece uma mensagem para o usuário, para explicar por que é necessário iniciar o aplicativo.

7. Visibilidade do nome de exibição da empresa

Controla se o nome de exibição da empresa é visível no dispositivo (por exemplo, como uma mensagem na tela de bloqueio em dispositivos de propriedade da empresa).

Visível (padrão): O nome de exibição da empresa é visível no dispositivo (suportado em perfis de trabalho no Android 7+ e dispositivos totalmente gerenciados no Android 8+).

Oculto: O nome de exibição da empresa é ocultado no dispositivo.

Regras de aplicação de política

Se um dispositivo ou perfil de trabalho deixar de cumprir qualquer uma das configurações de política listadas abaixo, o Android Device Policy bloqueará imediatamente o uso do dispositivo ou perfil de trabalho por padrão:

- **Requisitos de senha**
- **Política de criptografia**
- **Keyguard desativado**
- **Métodos de entrada permitidos**
- **Serviços de acessibilidade permitidos**

Se o dispositivo ou perfil de trabalho permanecer em não conformidade após 10 dias, o Android Device Policy fará a restauração de fábrica do dispositivo ou excluirá o perfil de trabalho.

Nesta seção, você pode substituir as regras de aplicação de conformidade padrão ou adicionar novas.

Regras

Lista de regras que definem o comportamento quando uma política específica não pode ser aplicada a um dispositivo.

Use **Adicionar regra** para criar uma nova regra. Cada cartão de regra pode ser removido usando a ação de excluir.

Nome da configuração

A política de nível superior a ser aplicada. Por exemplo, **Aplicativos** ou **Requisitos de senha**.

Obrigatório. O valor deve corresponder a um nome de política de nível superior compatível; caso contrário, o campo será marcado como inválido.

Bloquear após dias

Número de dias em que a política está em não conformidade antes que o dispositivo ou perfil de trabalho seja bloqueado. Para bloquear o acesso imediatamente, defina como 0. **Bloquear após dias** deve ser menor que **Limpar após dias**. Aplicável apenas a dispositivos de propriedade da

empresa.

Intervalo permitido: 0-300.

Escopo do bloqueio

Especifica o escopo da ação de bloqueio. Aplicável apenas a dispositivos de propriedade da empresa.

Padrão (nova regra): **Perfil de trabalho**.

Perfil de trabalho: A ação de bloqueio é aplicada apenas aos aplicativos no perfil de trabalho. Os aplicativos no perfil pessoal não são afetados.

Dispositivo inteiro: A ação de bloqueio é aplicada a todo o dispositivo, incluindo os aplicativos no perfil pessoal.

Limpar após dias

Número de dias em que a política está em não conformidade antes que o dispositivo ou perfil de trabalho seja limpo.

Limpar após dias deve ser maior que **Bloquear após dias**. Aplicável apenas a dispositivos de propriedade da empresa.

Obrigatório. Padrão (nova regra): **1**.

Intervalo permitido: 1-300.

Preservar a proteção de restauração de fábrica

Se os dados de proteção de restauração de fábrica serão preservados no dispositivo. Esta configuração não se aplica a perfis de trabalho.

Padrão (nova regra): ativado.

Políticas - Apple

Políticas da Apple

As políticas da Apple definem as configurações de gerenciamento que o Cerberus Enterprise aplica aos dispositivos Apple via MDM. Essas configurações são configuradas a partir do dashboard no editor de política da Apple.

Antes de começar

O gerenciamento de dispositivos Apple exige que o Apple Management (APNs) seja configurado. Se necessário, leia a página de [Configuração do Apple Management \(APNs\)](#).

Abra o Editor de Política da Apple

No painel, abra **Políticas** e clique em **Criar nova política da Apple**. Para editar uma política da Apple existente, clique na linha correspondente na tabela de políticas.

Layout do editor

O Editor de Política da Apple é organizado como um conjunto de seções expansíveis. No topo da página, você sempre poderá editar:

- **Nome** (obrigatório)
- **ID** (somente leitura)
- **Descrição** (opcional)

Seções de política

As seções abaixo correspondem aos painéis atualmente disponíveis no Editor de Política da Apple:

- **Gerenciamento de apps:** configure restrições relacionadas a aplicativos e apps gerenciados.

- **Configurações de código de acesso:** configure os requisitos de código de acesso e regras relacionadas.
- **Segurança:** controle recursos como o Desbloqueio Automático e desbloqueio biométrico.
- **iCloud:** permita ou bloqueie serviços específicos do iCloud (backup, sincronização de chaveiro, private relay, etc.).
- **Multimídia:** permita ou bloqueie a câmera e recursos relacionados.
- **Celular:** controle as configurações relacionadas ao celular (configurações de dados celulares de apps, eSIM, alterações de plano).
- **Rede:** controle o AirDrop/AirPrint/AirPlay e outras configurações de conectividade.
- **Contas:** restrinja a modificação de contas e (opcionalmente) configure contas do Google e de E-mail.

Muitas opções no Editor de Política da Apple incluem uma dica de ferramenta que documenta os requisitos e as versões de SO compatíveis.

Salvar, excluir e dispositivos associados

Use **Salvar política** para aplicar suas alterações. O botão fica desativado quando não há edições pendentes ou quando a licença expirou.

Ao editar uma política existente, a página também mostra a ação **Excluir política**. O editor pode exibir uma lista de **Dispositivos associados** na parte inferior, para que você possa ver quantos dispositivos estão usando a política no momento.

Próximas páginas

- **Passcode:** configure os requisitos de código de acesso e opções de segurança relacionadas.
- **Restrições:** defina os recursos permitidos e as limitações no nível do SO.
- **Apps e perfis:** configure aplicativos instalados e perfis de configuração.

Política da Apple: Código de acesso

A seção de **Configurações de código de acesso** controla os requisitos de código de acesso do dispositivo e as regras de segurança relacionadas (por exemplo, comprimento mínimo e complexidade).

Opções

No Editor de Política da Apple, as opções de código de acesso são configuradas por meio de uma combinação de chaves e campos numéricos. Muitos campos incluem dicas de ferramenta que indicam as versões de SO compatíveis e os requisitos de supervisão.

Chaves de código de acesso

- **ChangeAtNextAuth:** força a redefinição de senha na próxima vez que o usuário se autenticar.
- **RequireAlphanumericPasscode:** exige pelo menos um caractere alfabético e um número.
- **RequireComplexPasscode:** exige um código de acesso "complexo" (sem padrões repetitivos/sequenciais e com pelo menos um caractere não alfanumérico).
- **RequirePasscode:** exige um código de acesso sem requisitos adicionais de comprimento/qualidade. Observação: configurar outras chaves de código de acesso exige implicitamente um código de acesso.

Campos numéricos

- **FailedAttemptsResetInMinutes:** minutos antes de o contador de tentativas falhas ser redefinido (requer MaximumFailedAttempts).
- **MaximumFailedAttempts:** tentativas falhas permitidas antes que o dispositivo seja apagado/bloqueado (intervalo: 2–11).
- **MaximumGracePeriodInMinutes:** quanto tempo o dispositivo pode permanecer desbloqueado sem exigir o código de acesso (0 = nenhum).

- **MaximumInactivityInMinutes:** tempo de inatividade antes que o dispositivo bloqueie (intervalo: 0-15).
- **MaximumPasscodeAgeInDays:** idade máxima do código de acesso antes de uma alteração forçada (intervalo: 0-730).
- **MinimumComplexCharacters:** número mínimo de caracteres "complexos" (intervalo: 0-4).
- **MinimumLength:** comprimento mínimo do código de acesso (intervalo: 0-16).
- **PasscodeReuseLimit:** tamanho do histórico de códigos de acesso para evitar a reutilização de códigos antigos (intervalo: 1-50).

Política da Apple: Restrições

As seções de Restrições controlam quais recursos do SO são permitidos em dispositivos Apple gerenciados. No Editor de Política da Apple, essas opções são exibidas como painéis agrupados com múltiplas chaves.

Muitas restrições são suportadas apenas em versões específicas do SO e podem exigir dispositivos supervisionados. Use as dicas de ferramenta no dashboard para requisitos oficiais.

Segurança

- **Permitir desbloqueio automático**
- **Permitir impressão digital para desbloqueio**
- **Permitir modificação de impressão digital**

iCloud

- **Permitir agenda do iCloud**
- **Permitir backup do iCloud**
- **Permitir favoritos do iCloud**
- **Permitir calendário do iCloud**
- **Permitir Mesa e Documentos do iCloud**
- **Permitir sincronização de documentos do iCloud**
- **Permitir Freeform do iCloud**
- **Permitir sincronização do chaveiro do iCloud**
- **Permitir Mail do iCloud**
- **Permitir Notas do iCloud**
- **Permitir Biblioteca de Fotos do iCloud**
- **Permitir Retransmissão Privada do iCloud**
- **Permitir Lembretes do iCloud**

Multimídia

- **Permitir câmera**
- **Permitir modificação de compartilhamento de arquivos**
- **Permitir acesso de arquivos a unidades USB**

Celular

- **Permitir modificação de dados celulares por aplicativo**
- **Permitir modificação de plano celular**
- **Permitir modificação de eSIM**
- **Permitir transferências de saída de eSIM**

Rede

- **Permitir AirDrop**
- **Permitir solicitações de entrada do AirPlay**
- **Permitir AirPrint**
- **Permitir armazenamento de credenciais do AirPrint**
- **Permitir descoberta iBeacon para AirPrint**
- **Permitir modificação de Bluetooth**
- **Permitir modificação de compartilhamento via Bluetooth**
- **Permitir acesso de arquivos a unidades de rede**
- **Permitir modificação de compartilhamento de Internet**

Contas (restrição)

O painel de Contas contém tanto uma restrição quanto (opcionalmente) a configuração da conta. A chave de restrição controla se o usuário pode modificar as contas do sistema.

- **Permitir modificação de conta**

Política da Apple: Aplicativos e perfis

Esta seção documenta como configurar aplicativos gerenciados e payloads de conta para dispositivos Apple.

Gerenciamento de aplicativos

O painel de **Gerenciamento de aplicativos** contém tanto restrições gerais relacionadas a aplicativos quanto uma lista de aplicativos gerenciados.

Restrições gerais de aplicativos

- **Permitir App Clips**
- **Permitir instalação de aplicativos**
- **Permitir remoção de aplicativos**
- **Permitir downloads automáticos de aplicativos**
- **Permitir que aplicativos sejam ocultados**
- **Permitir que aplicativos sejam bloqueados**
- **Permitir compras no aplicativo**

Aplicativos gerenciados

Use **Adicionar aplicativo** para adicionar um aplicativo à política. Cada aplicativo gerenciado é exibido como um card. Você pode expandir o card para editar suas configurações e remover o aplicativo usando a ação de excluir.

- **ID da App Store:** o identificador da App Store do aplicativo gerenciado.
- **Bundle ID:** o identificador do pacote do aplicativo.
- **Comportamento de instalação:** controla se o aplicativo deve permanecer instalado ou se pode ser instalado/removido pelo usuário.
- **Atribuição:** tipo de atribuição de licença.
- **Licença VPP:** tipo de licença VPP usada para instalação através da App Store.

Contas

O painel de **Contas** permite configurar contas que são aplicadas a dispositivos gerenciados. Ele também inclui uma opção de restrição para modificação de conta.

Restrição

- **Permitir modificação de conta:** quando desativado, os usuários não podem modificar contas como Contas Apple e contas de internet.

Adicionar contas

Use **Adicionar conta do Google** ou **Adicionar conta de e-mail** para adicionar payloads de conta à política. Cada conta aparece como um card com seus campos de configuração.

Credenciais de conta dos usuários

Tanto os cards de conta do Google quanto os de e-mail oferecem uma opção de **Credenciais de conta dos usuários**. Quando ativado, o sistema aplica as credenciais da conta individualmente por usuário. Quando desativado, você insere a identidade da conta na política.

Campos da conta do Google

- **Nome visível:** o nome exibido ao usuário para a conta.
- **Endereço de e-mail do Google:** o endereço de e-mail do usuário.
- **Nome completo:** o nome completo do usuário.

Campos da conta de e-mail

As contas de e-mail incluem campos de identidade, além da configuração de servidores de entrada/saída. Os nomes de host são obrigatórios.

- **Nome visível:** o nome exibido ao usuário para a conta de e-mail.
- **Endereço de e-mail:** o endereço de e-mail do usuário.
- **Nome completo:** o nome completo do usuário.

Servidor de entrada

- **Tipo de servidor:** protocolo de e-mail (por exemplo, IMAP ou POP).
- **Método de autenticação:** método de autenticação para o servidor.
- **Prefixo do caminho IMAP:** exibido apenas quando o Tipo de servidor for IMAP.
- **Nome do host:** obrigatório.
- **Porta:** porta do servidor (1-65535).

Servidor de saída

- **Método de autenticação**
- **Nome do host:** obrigatório.
- **Porta:** porta do servidor (1-65535).

Opções de S/MIME

Para contas de e-mail, você também pode configurar o comportamento de criptografia e assinatura S/MIME.

Criptografia

- **Criptografia S/MIME**
- **Identidade substituível pelo usuário**
- **Alternância por mensagem ativada**
- **Substituível pelo usuário**

Assinatura

- **Assinatura S/MIME**
- **Identidade substituível pelo usuário**
- **Substituível pelo usuário**

As opções de conta e restrição incluem dicas de ferramenta no dashboard que documentam os pré-requisitos e as versões de SO compatíveis.

Status do Dispositivo

Visão geral do dispositivo

Abra um dispositivo em **Dashboard** → **Dispositivos** clicando na linha do dispositivo. O título da página mostra o **Modelo** do dispositivo (quando disponível) e o **ID** interno.

Dados históricos vs. registro atual

Quando um dispositivo possui múltiplos registros, o Cerberus Enterprise pode exibir um registro histórico de apenas leitura. Nesse caso, a página exibe um banner de **Dados históricos** e um botão para retornar aos dados do registro atual.

Campos principais

A seção superior resume a identidade, atribuição e o estado de gerenciamento do dispositivo. Alguns campos são específicos de cada plataforma e aparecem apenas para dispositivos Android ou Apple.

- **ID** e **Modelo**: identificadores de apenas leitura.
- **Usuário**: mostra o usuário atribuído atualmente (se houver). No menu de usuário, você pode **Abrir usuário** ou **Alterar usuário**, ou atribuir um usuário quando nenhum estiver definido.
- **Modo de gerenciamento** e **Propriedade**: exibidos com dicas de ferramenta na interface do usuário.
- **Estado**: estado atual do dispositivo (com ícone e detalhes de dica de ferramenta).
- **Perfil ADE** (apenas Apple): mostra o perfil de Inscrição Automática de Dispositivos atribuído (se houver) e permite abri-lo ou alterá-lo.
- **Política**: mostra a política atribuída e permite abri-la ou alterá-la, ou atribuir uma quando nenhuma estiver definida.
- **Status de conformidade da política** (quando uma política está atribuída): indica se o dispositivo está em conformidade.
- **Versão da política** (quando uma política está atribuída): indica se a versão mais recente da política foi aplicada ao dispositivo.
- **Registrado em** e **Último relatório de status**: carimbos de data/hora do registro e do último status relatado.
- **Removido em**: exibido quando o dispositivo foi removido.

Alguns dados e painéis estão disponíveis apenas quando a categoria correspondente está ativada na política do dispositivo. Para mais informações, leia as páginas de [Relatório de status](#) e [Localização e geofence](#).

Painéis

O editor de Dispositivos é organizado em seções expansíveis. Dependendo da plataforma e do estado, você poderá ver um ou mais dos seguintes painéis:

- **Mapa de localização:** um painel com abas contendo o histórico de **Localização** do dispositivo atual e, em dispositivos Android, uma aba de **Geofence** para transições de geofence quando os dados de geofence estiverem disponíveis.
- **Gerenciamento de SIMs** (apenas Android): EID do dispositivo, SIMs e eSIMs instalados e histórico de comandos de eSIM. Consulte a página dedicada de [Gerenciamento de SIMs](#).
- **Comandos:** envie comandos para o dispositivo e visualize o histórico de comandos (específico por plataforma).
- **Postura de segurança** (apenas Android): postura, veredito de Integridade do Play e riscos de segurança.
- **Relatórios de aplicativos** (apenas Android): aplicativos instalados e relatórios de feedback/erro.
- **Aplicativos gerenciados** (apenas Apple): estado dos aplicativos gerenciados e detalhes de instalação.
- **Detalhes de não conformidade:** exibido quando um dispositivo não está em conformidade; lista as configurações de política que estão fora de conformidade.
- **Relatórios de status:** dados adicionais relatados pelo dispositivo, exibidos como uma árvore de categorias e valores.
- **Histórico de registro:** registros anteriores para este mesmo dispositivo físico, exibidos como uma lista.

Abas do painel de localização

O painel de **Mapa de localização** agora usa abas para que o histórico de localização e as transições de geofence permaneçam separados.

- **Localização:** mostra filtros de histórico, uma pesquisa por intervalo de datas, marcadores de localização, o círculo de precisão e controles de rastreamento ao vivo para o dispositivo atual.
- **Geofence** (apenas Android): mostra o histórico de transições de geofence em um mapa dedicado, com filtros de período, uma opção para alternar entre geofences arquivadas e

uma lista lateral de transições.

Para o comportamento completo dessas abas, consulte [Mapa de localização](#).

Ações

Na parte inferior da página, você pode atualizar os dados e realizar ações dependendo da plataforma, do estado do dispositivo e do status da licença.

- **Atualizar dados:** recarrega o registro do dispositivo.
- **Desativar dispositivo / Ativar dispositivo** (apenas Android): disponível em estados compatíveis.
- **Remover registro do dispositivo:** remove o gerenciamento do dispositivo. O comportamento exato depende da plataforma e da propriedade (por exemplo, no Android pode apagar um perfil de trabalho ou realizar uma restauração de fábrica).
- **Excluir dispositivo:** disponível quando o dispositivo já foi removido e seu registro pode ser excluído.

Gerenciamento de SIMs

Em dispositivos Android, o editor de Dispositivo oferece um painel de **Gerenciamento de SIMs** para gerenciar os perfis de SIM e eSIM instalados no dispositivo, adicionar ou remover perfis de eSIM e visualizar o histórico de comandos de eSIM enviados ao dispositivo. Este painel está disponível apenas para dispositivos Android.

As informações do SIM são relatadas por dispositivos totalmente gerenciados quando o relatório de **Informações de rede** está ativado na política do dispositivo (esta opção é sempre ativada pelo Cerberus Enterprise). Consulte a página de [Relatório de status](#).

EID do Dispositivo

O EID (Identificador eUICC) identifica o hardware do eSIM do dispositivo. As operadoras o utilizam para vincular perfis de eSIM ao dispositivo, portanto, recuperá-lo é geralmente a primeira etapa de um fluxo de trabalho de provisionamento de eSIM.

- **Dispositivos de propriedade da empresa** (Android 13 e superior): o EID é relatado automaticamente com o status do dispositivo e não é necessária nenhuma interação do usuário.
- **Dispositivos de propriedade pessoal** (Android 13 e superior): use o botão **Solicitar EID**. O usuário verá uma notificação no dispositivo solicitando o compartilhamento do EID e poderá aprovar ou recusar a solicitação. O EID é exibido apenas se o usuário aprovar. Enquanto a solicitação estiver pendente, o botão permanecerá desativado.

Ao enviar uma solicitação de EID, um diálogo de confirmação é exibido primeiro, pois o usuário verá uma notificação no dispositivo.

SIMs instalados

A tabela de **SIMs instalados** lista os SIMs atualmente conhecidos para o dispositivo, incluindo SIMs físicos e perfis de eSIM. Em dispositivos de propriedade pessoal, os perfis de eSIM instalados com o comando **Adicionar eSIM** são exibidos mesmo quando o dispositivo não relata informações de SIM.

- **Operadora:** o nome da operadora associado ao SIM (quando relatado).
- **Número de telefone:** o número de telefone associado ao SIM (quando relatado).
- **ICCID:** o Identificador de Cartão de Circuito Integrado do SIM.
- **Estado de ativação:** se o eSIM está ativado ou não. Relatado apenas para eSIMs no Android 15 e superior.
- **Modo de configuração:** se o eSIM foi configurado por um administrador ou pelo usuário. Relatado apenas para eSIMs no Android 15 e superior.
- **Tipo de SIM:** mostra se o dispositivo relata a entrada como um eSIM.

eSIMs com um comando de remoção em andamento ou executado (não falho) mostram um estado de ativação temporário de **Removendo**. A entrada desaparece da lista quando o dispositivo relata a lista de SIMs atualizada. Enquanto uma remoção estiver em andamento, o botão remover não estará disponível para evitar o envio do mesmo comando duas vezes.

Remover eSIM

Use o botão remover ao lado de um eSIM instalado para remover seu perfil do dispositivo. Um diálogo de confirmação solicitará que você confirme o ICCID do eSIM a ser removido antes que o comando seja enviado. A remoção de um eSIM é suportada no Android 15 e superior.

Adicionar eSIM

A seção **Adicionar eSIM** instala um novo perfil de eSIM no dispositivo (suportado no Android 15 e superior). Ela requer:

- **Validade:** por quanto tempo o comando é válido caso não possa ser executado imediatamente.
- **Código de ativação:** o código de ativação para o perfil do eSIM, fornecido pela operadora. Você pode inserir o código completo ou apenas o endereço SM-DP+ para permitir que o dispositivo descubra um perfil que a operadora já vinculou ao seu EID.
- **Estado de ativação:** se o perfil do eSIM deve ser ativado automaticamente após o download ou se deve permanecer não ativado para ativação manual pelo usuário.

Histórico de comandos

Abaixo da seção Adicionar eSIM, o painel mostra o histórico de comandos de eSIM enviados ao dispositivo: **Adicionar eSIM**, **Remover eSIM** e **Solicitar EID**. A tabela é classificável e suporta paginação. Algumas linhas podem ser expandidas para visualizar os parâmetros do comando (por exemplo, o código de ativação ou o ICCID) e o status de execução, incluindo os detalhes de erro do

eSIM quando uma operação falha no dispositivo.

- **Data de criação**
- **Comando**
- **Validade**
- **Status**
- **Erro:** mostra o status de erro do eSIM (por exemplo *Usuário negou*, *Código de ativação inválido*, ou *ICCID não encontrado*) quando a execução do comando o relata.
- **Data de execução**

Limpar eSIMs ao limpar e desinscrever

Quando você limpa o dispositivo a partir do painel de Comandos, o sinalizador **Limpar eSIMs** controla se os perfis de eSIM serão removidos com a limpeza. Em dispositivos de propriedade pessoal com um perfil de trabalho, este sinalizador está ativado por padrão (eSIMs gerenciados são removidos, eSIMs de propriedade pessoal não são afetados). O mesmo sinalizador está disponível no diálogo de confirmação **Desinscrever dispositivo**.

Comandos

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

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

Parâmetros comuns

- **Validade:** por quanto tempo o comando é válido caso não possa ser executado imediatamente.
- **Comando:** escolha qual ação enviar para o dispositivo.

Comandos com campos adicionais

- **Redefinir senha:** requer **Nova senha** e **Confirmar nova senha**. As chaves opcionais incluem **Bloquear agora**, **Exigir entrada** e **Não solicitar credenciais na inicialização**.
- **Limpar dados do aplicativo:** requer o **nome do pacote** de destino.
- **Iniciar modo perdido:** requer uma **Mensagem de perda** e suporta campos de contato opcionais (endereço, organização, número de telefone, e-mail).
- **Limpar:** suporta uma **mensagem de motivo da limpeza** (exibida aos usuários em dispositivos pessoais) e sinalizadores de limpeza opcionais, incluindo **Limpar eSIMs**.

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

Histórico de comandos

Abaixo dos controles de envio, o dashboard exibe uma tabela de histórico de comandos. A tabela é classificável e suporta paginação. Algumas linhas podem ser expandidas para visualizar 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 de Comandos fornece um seletor de **Comando**. Alguns comandos exigem entradas adicionais. Assim como no Android, uma tabela de histórico de comandos é exibida abaixo.

Comandos com campos adicionais

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

Colunas do histórico Apple

- **Data de criação**
- **Comando**
- **Status**
- **Hora do status**

Atualizar

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

Mapa de localização

Esta página documenta as ferramentas de localização específicas para dispositivos disponíveis na [Visão geral do dispositivo](#). O painel contém uma aba de **Localização** para o histórico de posição e, em dispositivos Android, uma aba de **Cerca virtual** para transições de cercas virtuais.

Pré-requisitos

Os dados de localização do dispositivo são exibidos apenas quando o relatório de localização estiver ativado na política do dispositivo. Para ativá-lo, abra a política e ligue **Localização e cercas virtuais** → **Relatar localização**. Para mais detalhes, consulte [Localização e cercas virtuais](#).

Em dispositivos que não são totalmente gerenciados, os dados de localização ainda podem depender do aplicativo Cerberus Enterprise possuir as permissões de localização necessárias e dos serviços de localização estarem ativados no dispositivo.

Para o mapa global de múltiplos dispositivos disponível a partir do dashboard, consulte [Mapa de localização do dashboard](#).

Estado de carregamento e sem dados

- Enquanto os dados de localização estão sendo carregados, o painel exibe uma sobreposição de carregamento no mapa.
- Se o dispositivo não tiver dados de localização disponíveis, o painel exibirá uma mensagem informando **Nenhum dado de localização disponível**, juntamente com um lembrete para ativar o relatório de localização na política atribuída.
- Se um filtro de data estiver ativo e nenhum dado corresponder a ele, o painel exibirá **Nenhum dado disponível no intervalo de datas selecionado**.

Aba de Localização

Abra a aba de **Localização** para inspecionar o histórico de um único dispositivo. Os filtros disponíveis incluem a última localização conhecida, intervalos de histórico recente, um intervalo de datas personalizado e rastreamento ao vivo.

- **Última**: mostra a última localização conhecida.
- **Hoje, Últimos 7 dias e Últimos 30 dias**: mostram as localizações registradas para o período selecionado.
- **Pesquisar**: permite escolher um intervalo de datas personalizado.
- **Ao vivo**: inicia ou interrompe o rastreamento ao vivo para o dispositivo atual.

Detalhes do marcador

Ao clicar em um marcador de localização, uma janela de informações é aberta com:

- O registro de data e hora do registro de localização.
- A **precisão** relatada (em metros).
- A **velocidade** relatada, quando o dispositivo a fornece.
- O **rumo** ou direção relatada, quando o dispositivo a fornece.

Círculo de precisão

Quando a janela de informações está aberta, um círculo de precisão é exibido ao redor do marcador. O raio do círculo corresponde à precisão relatada (em metros). Ao fechar a janela de informações, o círculo é ocultado.

Rastreamento ao vivo

Na visualização de histórico do dispositivo, selecionar o filtro **Ao vivo** inicia uma solicitação de rastreamento em tempo real para aquele dispositivo específico. O Cerberus Enterprise solicita confirmação antes de iniciar a solicitação.

- O rastreamento ao vivo dura até **15 minutos**.
- O dispositivo exibe uma notificação enquanto o rastreamento ao vivo estiver ativo.
- Enquanto o rastreamento ao vivo estiver ativo, o painel continuará atualizando a localização mais recente e o indicador de live permanecerá visível.

- Selecionar o filtro ao vivo novamente permite interromper o rastreamento ao vivo antes que o tempo limite termine.

Aba de Cerca virtual

Em dispositivos Android, a segunda aba mostra as transições de cercas virtuais geradas pelas cercas definidas na política atribuída. Esta aba está disponível quando existem dados de cerca virtual para o dispositivo.

- O mapa mostra as áreas de cerca virtual atuais juntamente com os pontos de transição registrados.
- A lista de transições à direita permite inspecionar os eventos de **entrada** e **saída**.
- Os filtros disponíveis são **Hoje**, **Últimos 7 dias**, **Últimos 30 dias** e uma pesquisa por intervalo de datas personalizado.
- **Incluir arquivados** também mostra transições relacionadas a definições de geofence antigas que não estão mais presentes na política atual.

Detalhes da transição de geofence

Ao selecionar uma transição, os detalhes dela são abertos no mapa e a entrada correspondente na lista é destacada. Quando disponível, o Cerberus Enterprise também mostra as coordenadas do dispositivo e a precisão relatada para essa transição.

Mapa de localização do dashboard

O mapa de localização do dashboard fornece uma visão global da última posição conhecida dos dispositivos que estão reportando dados de localização. Abra-o a partir do **Dashboard** para revisar vários dispositivos no mesmo mapa do Google.

Pré-requisitos

Um dispositivo aparece neste mapa apenas quando o relatório de localização estiver ativado em sua política atribuída. Para ativá-lo, abra a política e ligue **Localização e cercas virtuais** →

Relatar localização. Para mais detalhes, consulte [Localização e cercas virtuais](#).

Em dispositivos que não são totalmente gerenciados, os dados de localização ainda podem depender do aplicativo Cerberus Enterprise possuir as permissões de localização necessárias e dos serviços de localização estarem ativados no dispositivo.

Para o histórico por dispositivo e as transições de cerca virtual disponíveis no editor de dispositivos, consulte [Mapa de localização](#).

Estado de carregamento e sem dados

- Enquanto os dados de localização estão sendo carregados, o mapa exibe uma sobreposição de carregamento.
- Se nenhum dispositivo tiver dados de localização disponíveis no momento, a página exibirá uma mensagem de **Nenhum dado de localização disponível**.

Marcadores e agrupamentos

Cada dispositivo com dados de localização disponíveis é exibido como um marcador. Quando muitos dispositivos estão próximos uns dos outros, os marcadores são agrupados automaticamente para manter o mapa legível.

Dispositivos que estão em rastreamento ao vivo são destacados com um marcador animado para que sejam mais fáceis de localizar no mapa.

Controles do mapa

Quando o mapa contém localizações de dispositivos, o Cerberus Enterprise exibe botões de ação no canto superior direito do mapa.

- **Localização atual:** usa a localização do seu navegador para mover o mapa para sua posição atual e ajustar a área de precisão relatada.
- **Centralizar mapa:** ajusta o mapa novamente em torno dos marcadores de dispositivos exibidos no momento.
- Selo de rastreamento ao vivo **Rastreando:** aparece quando um ou mais dispositivos estão sendo rastreados ao vivo e mostra quantos estão ativos no momento.
- **Parar todo o rastreamento ao vivo:** o botão de ícone dentro do selo de rastreamento ao vivo interrompe o rastreamento ao vivo de todos os dispositivos rastreados no momento após a confirmação.

Detalhes do marcador

Ao clicar em um marcador, uma janela de informações é aberta com:

- O **Modelo** do dispositivo e o **ID** interno.
- O registro de data e hora da última localização relatada.
- A **precisão** relatada em metros.
- A **velocidade** relatada, quando disponível.
- O **rumo** ou direção relatada, quando disponível.

O identificador do dispositivo na janela de informações é um link que abre a respectiva página de

[Visão geral do dispositivo](#).

Ações da janela de informações

Cada janela de informações também inclui botões de ação para o dispositivo selecionado.

- **Link do dispositivo:** o nome e o ID do dispositivo no topo da janela de informações abrem a respectiva página de visão geral do dispositivo.
- **Aproximar zoom:** centraliza o mapa no dispositivo selecionado e ajusta o círculo de precisão relatada mais próximo a ele.
- **Ao vivo:** inicia o rastreamento ao vivo para esse dispositivo. Se o rastreamento ao vivo já estiver ativo, o mesmo botão o interrompe após a confirmação.
- **Rastreamento ao vivo ativo:** quando presente, esta linha de status indica que o dispositivo selecionado já está sendo rastreado em tempo real.

Círculo de precisão

Quando um marcador é selecionado, o mapa exibe um círculo de precisão ao redor da localização. O raio do círculo corresponde à precisão relatada.

Comportamento do rastreamento ao vivo

Iniciar o rastreamento ao vivo a partir de uma janela de informações envia uma solicitação de rastreamento em tempo real para o dispositivo. O Cerberus Enterprise, então, atualiza o mapa automaticamente enquanto a sessão estiver ativa.

- Cada sessão de rastreamento ao vivo dura até **15 minutos**.
- O dispositivo exibe uma notificação enquanto o rastreamento ao vivo estiver ativo.
- O rastreamento ao vivo pode ser interrompido tanto na janela de informações do dispositivo selecionado quanto pelo botão global de **Parar todo o rastreamento ao vivo** no mapa.

Aplicativos privados

Nesta seção do painel, você pode carregar seus próprios aplicativos Android privados ou criar aplicativos web para distribuir em seus dispositivos.

Os únicos detalhes que você precisa fornecer são o título e o APK do aplicativo. Aplicativos privados são aprovados automaticamente para sua organização e normalmente ficam prontos para distribuição em até 10 minutos. Você pode carregar um total de 15 aplicativos privados por dia. Observe que os aplicativos web também contam para esse total.

Na primeira vez que você publicar um aplicativo privado, precisará fornecer um endereço de e-mail para receber notificações do Play Console sobre seus aplicativos e sua conta de desenvolvedor do Google Play. Além disso, o Managed Play cria automaticamente uma conta de Desenvolvedor do Play em nome da sua organização. Você não precisa pagar uma taxa de registro para esta conta.

Aplicativos privados publicados a partir do iframe:

- Não estão sujeitos às mesmas verificações que outros aplicativos. Como resultado, não podem ser convertidos em aplicativos públicos.
- Não são transferíveis. Você não pode transferir a propriedade de um aplicativo para uma conta de desenvolvedor do Play diferente.

Para mais detalhes, visite a [Ajuda do Managed Google Play](#)

Gerenciamento de certificados

O dashboard inclui uma seção de **Certificados** para importar, visualizar e excluir certificados. Clicar em uma linha de certificado abre o editor de certificados.

Lista de certificados

Os certificados são exibidos em uma tabela paginada e classificável. A lista inclui tanto certificados de cliente quanto Autoridades Certificadoras (CA).

Filtros

No topo da página, você pode ativar filtros usando a lista de chips. Alguns filtros são mutuamente exclusivos.

- **Todos:** mostra todos os certificados.
- **Cliente:** mostra apenas certificados de cliente.
- **Autoridade Certificadora (CA):** mostra apenas certificados de CA.
- **Pesquisar:** mostra um campo de texto (rótulo **Nome ou nome do arquivo**) para pesquisar pelo nome do certificado ou nome do arquivo importado.
- **Sem usuário:** mostra certificados de cliente não associados a nenhum usuário.

Colunas da tabela

- **Nome**
- **Tipo**
- **Expiração**
- **Usuário** (exibido para certificados de cliente)
- **Nome do arquivo importado**
- **Data de importação**

Ações

- **Abrir certificado:** clique em uma linha para abrir o editor de certificados.
- **Excluir certificado:** disponível apenas quando o certificado não estiver associado a usuários/políticas e não for usado por dispositivos. A ação também pode ser desativada quando a licença estiver expirada.
- **Seleção de múltiplas linhas:** você pode ativar a seleção de múltiplas linhas para excluir vários certificados de uma só vez. Apenas certificados que podem ser excluídos podem ser selecionados.
- **Atualizar:** recarrega a lista de certificados.

Importar certificados

Para importar certificados, clique em **Importar certificado** e selecione um ou mais arquivos. Os formatos suportados são exibidos na dica de ferramenta do botão de importação.

Clientes

Formato suportado: PKCS#12 codificado em Base64 (.p12 / .pfx).

Certificados de cliente identificam um usuário ou um dispositivo na rede da empresa. Certificados de cliente podem ser associados a um usuário específico.

Cada certificado de cliente pode ser opcionalmente atribuído a um usuário específico: isso permite implantar a mesma configuração de Wi-Fi EAP em vários dispositivos. Você pode fazer isso na seção de [configuração de rede](#) da política, usando a opção de **credenciais EAP dos usuários**.

Como alternativa, você pode atribuir um certificado a um usuário na página de **Usuários**.

Autoridades Certificadoras (CA)

Formatos suportados: X.509 codificado em Base64 (.crt / .pem / .cer / .der).

Certificados de CA identificam uma Autoridade Certificadora e indicam ao dispositivo que quaisquer certificados emitidos pela CA devem ser confiáveis. O dashboard valida se um certificado X.509 importado é uma CA.

Editor de certificados

Quando você abre um certificado, o editor mostra seus campos principais e um painel de **Informações do certificado** apenas para leitura.

Campos principais

- **Nome** (obrigatório)
- **ID** (apenas leitura)
- **Tipo** (apenas leitura)
- **Expiração** (apenas leitura)
- **Data de importação** (apenas leitura)
- **Nome do arquivo importado** (apenas leitura)

Associação de usuário (certificados de cliente)

Para certificados de **Cliente**, o editor mostra um campo de **Usuário**. Se um usuário estiver atribuído, um menu permite **Abrir usuário**, **Alterar usuário** ou **Desvincular usuário**. Se nenhum usuário estiver atribuído, você pode atribuir um usando o botão de ação de usuário.

Excluir certificado

A ação de exclusão é desativada quando o certificado estiver associado a um usuário ou sendo usado em políticas. Ela também pode ser desativada quando a licença estiver expirada.

Regras de eventos

As regras de eventos permitem automatizar reações a eventos de dispositivos compatíveis. Abra **Painel** → **Regras de eventos** para criar regras que monitorem eventos de registro, remoção de registro, não conformidade e cercas virtuais (geofence) no Android, disparando uma ou mais ações automaticamente.

O que uma regra de evento pode fazer

Cada regra combina um **assunto**, um **evento** e uma ou duas **ações**. Os assuntos compatíveis são **Todos os dispositivos**, **Dispositivo específico** e **Política**.

- **Eventos:** dispositivo registrado, dispositivo removido do registro, dispositivo torna-se não conforme, entrada em cerca virtual (geofence), saída de cerca virtual (geofence).
- **Ações do dispositivo:** desativar dispositivo, ativar dispositivo, bloquear dispositivo.
- **Ação de e-mail:** envia um e-mail de notificação para os administradores e, quando ativado, para os gestores delegados.

Uma regra pode conter apenas uma ação de e-mail, apenas uma ação de dispositivo ou uma ação de dispositivo mais uma ação de e-mail. Se ambas as ações forem configuradas, o Cerberus Enterprise executará primeiro a ação de dispositivo e, em seguida, a ação de e-mail.

Regras de plataforma e compatibilidade

Os eventos e ações disponíveis dependem do assunto selecionado e da plataforma que se aplica a esse assunto.

- **Android** suporta eventos de registro, remoção de registro, não conformidade e cercas virtuais (geofence).
- **Apple** suporta eventos de registro, remoção de registro e não conformidade.

- **Desativar dispositivo** e **Ativar dispositivo** são ações exclusivas para Android.
- **Bloquear dispositivo** e **Enviar e-mail** estão disponíveis tanto para Android quanto para Apple, quando o evento selecionado os suporta.
- **Remoção de registro do dispositivo** suporta apenas ações de e-mail.

Lista de regras

A lista de Regras de eventos é a página principal de gerenciamento para este recurso. Ela inclui uma tabela pesquisável com nome da regra, assunto, evento, ações, plataforma, estado de ativação e hora de atualização.

- Use os chips de filtro para alternar entre todas as regras, regras ativadas, regras desativadas e pesquisa de texto.
- Use o botão **Atualizar** para recarregar a visualização atual da tabela.
- Use o interruptor de ativação em cada linha para ativar ou desativar temporariamente uma regra.
- Use o modo de seleção de múltiplas linhas para excluir várias regras ao mesmo tempo.
- Use **Criar regra de evento** para abrir o editor de uma nova regra.

Editor de regras

O editor é dividido nas seções **Geral**, **Escopo**, **Gatilho** e **Ações**. Na parte inferior da página, uma barra de ações fixa mantém os botões principais visíveis enquanto você rola a página.

Geral

- **Nome:** obrigatório, até 150 caracteres.
- **Descrição:** opcional, até 2000 caracteres.
- **Regra ativada:** salva a regra no estado ativado ou desativado.

Escopo

O escopo define quais dispositivos a regra pode corresponder. O editor também mostra a plataforma resolvida e, quando disponível, o contexto de política efetivo.

- **Todos os dispositivos:** a regra pode corresponder a todos os dispositivos compatíveis na empresa.
- **Dispositivo específico:** selecione um dispositivo gerenciado na caixa de diálogo de seleção.

- **Política:** selecione um modelo de política na caixa de diálogo de seleção.

Gatilho

A seção de gatilho filtra os eventos disponíveis automaticamente com base no escopo e na plataforma selecionados.

Gatilhos de cerca virtual (geofence)

As regras de entrada e saída de cerca virtual (geofence) são suportadas apenas para Android e exigem um contexto de política Android válido. Para informações sobre relatórios de localização e definições de cercas virtuais, consulte [Localização e cerca virtual \(geofence\)](#).

- Se o assunto for **Todos os dispositivos**, a regra sempre será aplicada a **Qualquer cerca virtual (geofence)**.
- Se o assunto for um dispositivo ou política, você pode escolher **Qualquer cerca virtual (geofence)** ou uma **Cerca virtual (geofence) específica**.
- A lista de cercas virtuais (geofence) específicas é carregada a partir do contexto de política efetivo do dispositivo ou política selecionados.

Ações

A seção de ações permite que você escolha uma ação de dispositivo opcional e uma notificação por e-mail opcional. A interface oculta automaticamente as combinações não suportadas.

- Se não houver uma ação de dispositivo disponível para o evento e escopo selecionados, você ainda poderá salvar uma regra apenas de e-mail.
- Se o e-mail estiver desativado para o evento e a plataforma selecionados, o interruptor de e-mail não estará disponível.
- Uma regra sem nenhuma ação é inválida e não pode ser salva.

Destinatários do e-mail

As ações de e-mail sempre incluem os usuários da empresa com a função **ADMIN**. Se a empresa for gerenciada por meio de multi-tenancy, você pode expandir os destinatários para incluir os gestores de MT.

- **Apenas gestores principais:** inclui os administradores da empresa e os contatos principais dos gestores de MT.

- **Gestores principais e gestores de subconta:** adiciona também os gestores de subconta atribuídos.
- A lista de visualização mostra os endereços de e-mail reais que serão usados quando a regra for executada.
- Apenas os gestores delegados com acesso concedido à empresa são incluídos na lista final de destinatários.

Comportamento de execução

As regras de eventos são executadas imediatamente quando o Cerberus Enterprise recebe um evento compatível das integrações de backend. As regras desativadas são ignoradas automaticamente.

As execuções bem-sucedidas e as que falharam são registradas no log do sistema com mensagens legíveis para humanos.

Dispositivos

Dispositivos

A seção **Dispositivos** do painel (*Painel* → *Dispositivos*) lista todos os dispositivos registrados em sua conta. A partir desta página, você pode filtrar a lista, abrir o registro de um dispositivo e realizar ações no dispositivo, como desativar ou remover o registro.

Filtros

No topo da página, você pode ativar um ou mais filtros usando a lista de chips. Os chips selecionados representam os filtros ativos no momento.

Filtros disponíveis

- **Todos:** mostra todos os dispositivos.
- **Android:** mostra apenas dispositivos Android.
- **Apple:** mostra apenas dispositivos Apple.
- **Propriedade da empresa:** mostra apenas dispositivos de propriedade da empresa.
- **Propriedade pessoal:** mostra apenas dispositivos de propriedade pessoal.
- **Proprietário do perfil:** mostra apenas dispositivos com perfil de trabalho Android.
- **Proprietário do dispositivo:** mostra apenas dispositivos Android totalmente gerenciados.
- **Ativo:** mostra dispositivos em estado ativo.
- **Em conformidade:** mostra dispositivos que estão em conformidade com as políticas.
- **Não em conformidade:** mostra dispositivos que não estão em conformidade com as políticas.
- **Seguro:** mostra dispositivos com postura de segurança.
- **Não seguro:** mostra dispositivos com postura de segurança não segura.
- **Política não atualizada:** mostra dispositivos que possuem alterações de política pendentes.
- **Status não atualizado:** mostra dispositivos que não reportaram o status nas últimas 72 horas.
- **Erro de aplicativos:** mostra dispositivos cujos aplicativos enviaram feedback de erro.
- **Pesquisa:** ativa um campo de pesquisa de texto.

Pesquisa

Quando você ativa o filtro **Pesquisa**, um campo de texto aparece com o rótulo **ID, Modelo ou Usuário**. A lista é atualizada automaticamente após você parar de digitar.

Tabela de dispositivos

Os dispositivos são exibidos em uma tabela paginada e classificável. Ao clicar em uma linha, o editor de dispositivos é aberto.

Colunas

- **ID**: identificador interno do dispositivo.
- **MDM**: plataforma (Android ou Apple).
- **Modelo**: modelo do dispositivo.
- **Propriedade**: propriedade da empresa ou pessoal (com detalhes no tooltip).
- **Modo de gerenciamento**: modo de gerenciamento (com detalhes no tooltip).
- **Política**: política atribuída no momento.
- **Usuário**: usuário associado (nome, e-mail ou ID, dependendo da disponibilidade).
- **Último relatório de status**: carimbo de data/hora do relatório de status mais recente (quando disponível).
- **Estado**: estado do dispositivo (com detalhes no tooltip).
- **Conformidade**: indicador de status de conformidade.
- **Segurança**: postura de segurança (com detalhes no tooltip).
- **Erro de aplicativos**: indicador de erro de aplicativos.

Atualização e paginação

- Use a ação de atualizar para recarregar a lista.
- A tabela é paginada (10/25/50 itens por página).

Ações do dispositivo

Cada linha de dispositivo pode oferecer ações, dependendo da plataforma e do estado do dispositivo. Algumas ações são desativadas quando sua licença expira ou é encerrada.

Ações por dispositivo

- **Desativar dispositivo / Ativar dispositivo:** disponível para dispositivos Android em estados compatíveis.
- **Remover registro do dispositivo:** remove o gerenciamento. No Android, isso pode apagar o perfil de trabalho ou realizar a restauração de fábrica (dependendo da propriedade); no Apple, isso remove as configurações de política.
- **Excluir dispositivo:** disponível para dispositivos que já foram removidos do registro (remove o registro do sistema).

Seleção de múltiplas linhas

Você pode ativar a seleção de múltiplas linhas na barra de ações abaixo da tabela. Quando ativada, você pode selecionar várias linhas e aplicar ações em massa (desativar, ativar, remover registro ou excluir), dependendo de quais dispositivos forem selecionados.

Sincronização com o Apple Business Manager

Se o Gerenciamento Apple estiver configurado e um token de Registro Automático de Dispositivos estiver presente, a página poderá exibir a ação **Sincronizar do ABM** para importar dispositivos do Apple Business Manager.

Registrar um dispositivo

Use **Registrar um dispositivo** para abrir a seção de tokens de registro e iniciar o registro de um novo dispositivo.

Usuários

Usuários

A seção **Usuários** do painel (*Painel* → *Usuários*) lista todos os usuários configurados em sua conta. Nesta página, você pode pesquisar usuários, abrir o editor de usuário, criar novos usuários e excluir usuários que não estejam associados a dispositivos no momento.

Pesquisar

No topo da página, há um campo de pesquisa com o rótulo **Pesquisar** e o marcador de posição **Nome, nome de usuário ou e-mail**. A lista é atualizada automaticamente após você parar de digitar.

Tabela de usuários

Os usuários são exibidos em uma tabela paginada e classificável. Clicar em uma linha abre o editor de usuário.

Colunas

- **ID**: identificador interno do usuário.
- **Nome**: nome do usuário.
- **Sobrenome**: sobrenome do usuário.
- **Nome de usuário**: nome de usuário (frequentemente o nome de usuário do diretório).
- **E-mail**: endereço de e-mail do usuário.
- **Dispositivos**: número de dispositivos associados atualmente ao usuário.
- **Certificado Wi-Fi**: indicador que mostra se um certificado Wi-Fi está atribuído ao usuário.

Atualização e paginação

- A ação de atualizar recarrega a lista.
- A tabela é paginada (10/25/50 itens por página).

Ações do usuário

Criar novo usuário

Use **Criar novo usuário** para abrir a caixa de diálogo de criação de usuário. Esta ação é desativada quando sua licença estiver expirada.

Sincronizar do Google Workspace

Se a sincronização de diretório do Google Workspace estiver disponível para sua conta, a página exibirá **Sincronizar do Google Workspace**. Quando você iniciar uma sincronização, um indicador de progresso será exibido enquanto a solicitação estiver em execução.

Excluir um usuário

Você só pode excluir um usuário quando ele não estiver associado a nenhum dispositivo (a coluna **Dispositivos** deve ser 0). A ação de excluir é desativada quando sua licença estiver expirada ou encerrada.

Seleção de múltiplas linhas e exclusão em massa

Na barra de ações abaixo da tabela, você pode ativar a seleção de múltiplas linhas. Neste modo, você pode selecionar vários usuários e excluí-los em massa.

- **Elegibilidade:** apenas usuários com **Dispositivos** = 0 podem ser selecionados para exclusão.
- **Selecionar tudo:** a caixa de seleção **Tudo** seleciona todas as linhas elegíveis na página atual.
- **Exclusão em massa:** **Excluir usuários selecionados** é desativado quando nenhuma linha está selecionada, ou quando sua licença estiver expirada ou encerrada.

Certificados Wi-Fi e EAP

A coluna **Certificado Wi-Fi** mostra se um certificado está atribuído atualmente a um usuário. Certificados de usuário são normalmente usados para configurações de Wi-Fi EAP (por exemplo,

EAP-TLS). Para atribuição e gerenciamento de certificados, consulte [**Gerenciamento de certificados**](#).

Editor de usuário

O editor de usuário está disponível em *Painel* → *Usuários* ao clicar em uma linha de usuário. Ele permite editar os detalhes do usuário, configurar credenciais Wi-Fi EAP por usuário e visualizar os dispositivos associados ao usuário.

Detalhes do usuário

A seção superior contém os campos principais do usuário. Alguns campos são obrigatórios e o editor exibe erros de validação quando eles estão ausentes ou são inválidos.

- **ID:** identificador de apenas leitura.
- **Nome:** obrigatório.
- **Sobrenome:** obrigatório.
- **Nome de usuário:** obrigatório.
- **E-mail:** obrigatório e deve ser um endereço de e-mail válido.
- **Número de telefone:** opcional.
- **Conta do Google:** opcional e deve ser um endereço de e-mail válido quando fornecido.

Política Padrão de Autenticação do Google

Em ambientes do Google Workspace com a Autenticação do Google ativada, o editor pode exibir a **Política Padrão de Autenticação do Google**. Esta é a política aplicada aos dispositivos registrados usando a Autenticação do Google por este usuário.

- **Alterar política:** abre a caixa de diálogo de seleção de política.
- **Abrir política:** abre a política selecionada no editor de políticas (quando uma política estiver definida).
- Após selecionar uma nova política padrão, você deve salvar o usuário para aplicar a alteração. O editor exibirá uma notificação lembrando-o de salvar.

Credenciais Wi-Fi EAP

A seção **Credenciais Wi-Fi EAP** é usada para configurar credenciais por usuário que são instaladas automaticamente nos dispositivos do usuário quando a política atribuída contém uma configuração de Wi-Fi EAP que as exige. A configuração de Wi-Fi EAP faz parte da [configuração de rede](#) da política Android.

Certificado do cliente

Você pode, opcionalmente, atribuir um certificado de cliente a um usuário. Quando um certificado é atribuído, ele é exibido no campo **Certificado do cliente** e um menu fornece ações. Quando nenhum certificado é atribuído, o campo exibe **Nenhum certificado atribuído** e você pode atribuir um.

- **Atribuir certificado:** abre a caixa de diálogo de seleção de certificado.
- **Abrir certificado:** abre o editor de certificados.
- **Alterar certificado:** seleciona um certificado de cliente diferente.
- **Desassociar certificado:** remove o certificado do usuário. O sistema também remove o certificado de todos os dispositivos associados a este usuário.

Para importação e gerenciamento de certificados, consulte [Gerenciamento de certificados](#).

Identidade, identidade anônima e senha

- **Identidade:** identidade do usuário. Para protocolos de tunelamento externos (PEAP, EAP-TTLS), esta é usada dentro do túnel.
- **Identidade anônima:** usada para protocolos de tunelamento como a identidade apresentada fora do túnel. Quando não especificada, o padrão é uma string vazia.
- **Senha:** a senha do usuário para métodos EAP que a exigem. Se não for especificada, o dispositivo pode solicitar ao usuário. Uma ação de mostrar/ocultar alterna a visibilidade da senha.

Dispositivos associados

A seção **Dispositivos associados** mostra a lista de dispositivos vinculados atualmente ao usuário. Se o usuário tiver um ou mais dispositivos associados, ele não poderá ser excluído.

Salvar e excluir

- **Salvar usuário:** habilitado apenas quando o formulário é válido, há alterações pendentes e a licença está ativa. Um indicador de progresso é exibido durante o salvamento.
- **Excluir usuário:** desativado quando o usuário estiver associado a dispositivos ou quando a licença estiver expirada/encerrada. Quando a exclusão for permitida, uma caixa de diálogo de confirmação será exibida. Se o usuário estiver atribuído a tokens de registro, a caixa de diálogo avisará que os dispositivos registrados com esses tokens não estarão mais atribuídos a um usuário.

Aviso de alterações não salvas

Se você tiver alterações não salvas e tentar sair da página, o painel perguntará se você deseja descartar as alterações.

Conta

Configurações

A página de **Configurações** (*Dashboard* → *Configurações*) resume as informações de conta e licença, e fornece ações para gerenciar o faturamento, a configuração da plataforma (Android Management e Apple Management) e integrações opcionais de diretório/token.

Banner de licença (expirando / expirada)

Quando sua licença estiver **expirando**, **expirada** ou **encerrada**, um banner de destaque será exibido no topo da página. Dependendo do estado da sua assinatura, ele fornecerá uma ação de **Gerenciar faturamento** (portal do cliente Stripe) ou uma ação de **Comprar licença**.

Quando a licença estiver expirada, a conta passará a ser limitada apenas ao desvinculo de dispositivos. Após o período de carência, a conta poderá ser cancelada e os dispositivos poderão ser desvinculados automaticamente.

Acesso do gerente da empresa

O cartão **Acesso do gerente da empresa** é exibido apenas para empresas gerenciadas por uma conta multi-tenancy (por exemplo, um provedor de serviços gerenciados). Ele permite ver quais contas de gerente podem operar na sua empresa e controlar o acesso delas.

O cartão mostra:

- O **proprietário** da empresa. O proprietário sempre tem acesso e esse acesso não pode ser revogado.
- Cada conta de gerente da conta multi-tenancy, identificada como **Gerente principal** ou **Subconta**, com nome, nome de usuário e status de acesso (**Concedido**, **Revogado** ou **Não concedido**).

Conceder e revogar o acesso

Use **Conceder** para permitir que uma conta de gerente acesse e gerencie sua empresa e **Revogar** para remover esse acesso. Cada ação solicita confirmação. Um gerente cujo acesso foi revogado não pode mais operar na empresa, mesmo que esteja trabalhando nela no momento.

- Como administrador da empresa, você pode conceder ou revogar o acesso de qualquer conta de gerente listada.
- O gerente principal pode conceder ou revogar o acesso das próprias subcontas, mas somente enquanto o próprio acesso estiver concedido. Ele não pode conceder acesso a si mesmo nem revogar o próprio acesso.

Revogar o acesso do **Gerente principal** também revoga o acesso de todas as suas subcontas. Nesse caso, a caixa de diálogo de confirmação lista as subcontas que perderão o acesso.

Informações da conta

O cartão de **Informações da Conta** exibe campos apenas para leitura:

- **Nome de usuário**
- **Nome da empresa**
- **ID da empresa**

Alterar senha

Se você não estiver conectado com Google, Apple ou Microsoft, o cartão também exibirá uma ação de **Alterar senha**. Isso abrirá um diálogo para continuar com o fluxo de alteração de senha.

Você também pode alterar sua senha a qualquer momento no menu do usuário na barra superior, com **Alterar senha**. Isso é útil para contas multi-tenancy, que podem alterar a senha sem entrar em uma empresa.

Se um administrador criou sua conta ou redefiniu sua senha, você entra com uma senha temporária e precisa escolher uma nova senha antes de continuar.

Informações da licença

O cartão de **Informações da Licença** mostra o estado atual da licença e o limite de seus dispositivos. Ele também fornece ações para entrar em contato com vendas, gerenciar o

faturamento ou comprar uma licença.

- **Status da licença:** exibido como **Ativa** ou **Expirada** (com um selo de ícone e dica de ferramenta).
- **Teste gratuito:** exibido quando a conta está atualmente em modo de teste.
- **Dispositivos licenciados:** número máximo de dispositivos permitidos pela licença. O link *precisa de mais dispositivos?* abre uma mensagem para entrar em contato com o suporte.
- **Próxima renovação agendada:** exibido para assinaturas ativas que renovam automaticamente. Caso contrário, o cartão mostra a **Data de expiração**.

Android Management

O cartão de **Android Management** mostra o status do Android Management para sua empresa. Se o Android Management ainda não estiver configurado, o cartão fornecerá uma ação de **Configurar Android Management** que abre o fluxo de configuração.

Estado configurado

Quando o Android Management estiver configurado, o cartão pode exibir:

- **ID de gerenciamento**
- **Tipo de vínculo:** identifica se a empresa utiliza uma **conta do Managed Google Play** ou um **domínio do Managed Google**.
- **Sincronizado com o Google Workspace** (selo exibido quando a sincronização de diretório está ativa)
- **Sincronizar com o Google Workspace** (exibido quando a sincronização de diretório não estiver configurada; abre o painel de instruções na parte inferior da página)

Vínculo do Android Enterprise

O Android Management pode ser associado a uma **conta do Managed Google Play** ou a um **domínio do Managed Google**. O campo **Tipo de vínculo** mostra qual opção está associada atualmente à sua empresa.

Uma **conta do Managed Google Play** é uma conta Android Enterprise simplificada. Ela é adequada para gerenciar dispositivos e aplicativos Android por meio do Cerberus Enterprise, mas é separada de uma organização Google Workspace ou Cloud Identity. Ela não oferece a experiência de administração central do Google disponível com um domínio gerenciado pelo Google.

Um **domínio do Managed Google** associa o Android Enterprise à identidade do Google da sua organização. Os administradores de TI podem gerenciar produtos do Google, como Google Workspace, Cloud Identity e Gemini, a partir do console de administração do Google, enquanto

continuam a gerenciar aplicativos e políticas do Android no Cerberus Enterprise. Isso oferece uma abordagem mais ágil e integrada ao gerenciamento do Android e permite fluxos de trabalho de inscrição e gerenciamento de usuários baseados no Google Workspace.

Quando a empresa utiliza uma conta do Managed Google Play, o cartão de Configurações oferece as opções **Atualizar para um domínio gerenciado pelo Google** e uma ação de informação. A atualização abre o processo guiado do Google para migrar o Android Enterprise existente para um domínio gerenciado.

Durante a atualização, o Google pode vincular uma conta de administrador do Google existente associada ao seu endereço de e-mail corporativo ou criar automaticamente uma nova conta gratuita de administrador do Google. Use um endereço de e-mail corporativo como *name@enterprise.com* para continuar a configuração guiada do Google.

Apple Device Management

O cartão de **Apple Device Management** mostra o status do gerenciamento de dispositivos Apple (MDM) para sua empresa. Se o gerenciamento da Apple ainda não estiver configurado, o cartão fornecerá uma ação de **Configurar Apple Management** que abre o fluxo de configuração.

Estado configurado

Quando o gerenciamento da Apple estiver configurado, o cartão pode exibir:

- **ID Apple**
- **Expiração do Apple Push Certificate:** mostra a data de expiração e um selo de ícone. Se o certificado estiver expirando/expirado, o selo será clicável e abrirá as instruções de renovação.
- **Expiração do token ABM:** mostra a expiração do token do Apple Business Manager (com um selo clicável quando uma ação for necessária).
- **Token VPP:** mostra o nome da organização e a expiração do token do Apple Volume Purchase Program (com um selo clicável quando uma ação for necessária).
- **Portal do Apple Business Manager:** link exibido quando um token ABM está presente.
- **Sincronizar com o Apple Business Manager** e **Sincronizar com o Apple Volume Purchase Program:** exibidos quando os tokens estão ausentes.

O gerenciamento da Apple requer a configuração do certificado APNs. Se necessário, consulte [Configuração do Apple Management \(APNs\)](#).

Preferências e Privacidade

O cartão de **Preferências e Privacidade** contém uma chave de preferência de marketing e links para os Termos de Serviço e Política de Privacidade. Use **Salvar preferências** para aplicar as alterações (um indicador de progresso é exibido durante o salvamento).

Enviar feedback

Quando as assinaturas estiverem ativadas para a conta, a página pode exibir um cartão de **Enviar feedback** com links para: **Fazer uma solicitação de recurso** e plataformas de avaliação externas.

Instruções de configuração e renovação integradas

Na parte inferior da página, o dashboard pode exibir painéis de instruções expansíveis dependendo do estado atual (por exemplo, quando um certificado/token está ausente ou expirando).

Renovar o Apple Push Certificate (APNs)

Quando o certificado APNs estiver expirando ou já tiver expirado, a página exibirá um painel com as etapas para baixar um CSR, renovar o certificado no portal da Apple e carregar o novo certificado no Cerberus Enterprise.

Sincronizar com o Apple Business Manager (ABM)

Quando o token ABM estiver ausente, expirado ou expirando, a página exibirá um painel com as etapas para baixar um token do Apple Business Manager e carregá-lo no Cerberus Enterprise.

Sincronizar com o Apple Volume Purchase Program (VPP)

Quando o token VPP estiver ausente, expirado ou expirando, a página exibirá um painel com as etapas para baixar um token de conteúdo do Apple Business Manager e carregá-lo no Cerberus Enterprise.

Sincronizar com o Google Workspace

Quando a sincronização de diretório do Google Workspace não estiver configurada, a página exibirá um painel que explica a integração e fornece um botão de autorização. Ela também lista o escopo do Google OAuth necessário:

<https://www.googleapis.com/auth/admin.directory.user.readonly>.

Para a configuração inicial do Android, consulte [Configuração do Android Management](#).

Multitenância

Visão geral do multi-tenant

A seção de **Multi-tenancy** está disponível para contas de MSP e de gerenciadores de empresas que gerenciam múltiplas empresas de clientes a partir de um único login. Este capítulo explica o modelo de escopo de empresa, a alternância de empresas, a administração de empresas gerenciadas e as subcontas.

Para solicitar uma conta multi-tenant, entre em contato com enterprise@cerberusapp.com.

Conceitos fundamentais

- **Conta multi-tenant principal:** a conta gerenciadora primária que pode acessar o espaço de trabalho global multi-tenant.
- **Subconta:** uma conta de gerenciador delegado criada pela conta principal, com atribuições de empresas selecionáveis.
- **Contexto da empresa selecionada:** a empresa ativa que está aberta no dashboard para as operações do dia a dia.
- **Delegação:** permissão concedida por um proprietário de empresa que permite a uma conta de gerenciador entrar e gerenciar aquela empresa.

Modelo de navegação

Quando nenhum contexto de empresa estiver selecionado, a navegação lateral mostra áreas de multi-tenant como **Empresas** e, para contas principais, **Subcontas**. Após entrar em uma empresa, o dashboard muda para a navegação padrão de empresa única (Início, Usuários, Dispositivos, Registro, Políticas e mais).

Propriedade e delegação

Cada empresa gerenciada tem um proprietário. O proprietário pode sempre acessar essa empresa. Contas de gerenciador que não são proprietárias podem acessar uma empresa apenas quando a delegação é concedida.

- Quando uma empresa tem o próprio usuário administrador, esse administrador é o proprietário e decide quais contas de gerente podem acessar a empresa.
- Quando uma empresa não tem o próprio usuário administrador, o proprietário é a conta multi-tenancy principal.
- Em empresas cujo proprietário é um administrador do cliente, a conta principal pode conceder ou revogar o acesso das próprias subcontas enquanto o próprio acesso estiver concedido, mas não pode conceder acesso a si mesma.
- Se o administrador da empresa revogar o acesso da conta principal, o acesso das subcontas dela também é revogado.
- Remover uma empresa das atribuições de uma subconta também remove o acesso dessa subconta à empresa. Se você atribuí-la novamente mais tarde, o acesso precisará ser concedido de novo.

Os administradores da empresa gerenciam o acesso no cartão **Acesso do gerente da empresa** da página **Configurações**.

O estado de proprietário e de delegação é exibido diretamente nos cards de empresa para tornar o escopo de acesso explícito antes de entrar em uma empresa.

Ações de licença e faturamento

As visualizações de multi-tenant expõem o status da licença, limites de dispositivos e ações de faturamento da empresa. Dependendo do estado da assinatura da empresa e de suas permissões, o card pode mostrar **Gerenciar faturamento** ou **Comprar licença**.

Para empresas criadas por uma conta multi-tenant, o licenciamento é gerenciado pelos usuários da conta multi-tenant. A conta principal pode sempre gerenciar o licenciamento, enquanto as subcontas podem gerenciar o licenciamento apenas quando a conta principal ativa a opção **Pode gerenciar licença** para aquela subconta.

Páginas deste capítulo

- [Empresas gerenciadas](#): busca, filtros, detalhes do card e criação de empresas.
- [Alternância de empresas](#): comportamento do alternador superior e transições de escopo.
- [Subcontas](#): operadores delegados, atribuições e gerenciamento de credenciais.

Empresas gerenciadas

A página de **Empresas** (*Dashboard* → *Empresas*) é o centro de controle para o acesso gerenciado de empresas. Ela lista todas as empresas visíveis para sua conta multi-tenant e permite filtrar, inspecionar propriedade/delegação, entrar no contexto de uma empresa e criar novas empresas gerenciadas (apenas para contas principais).

Busca e filtros

- **Buscar empresa:** filtra por nome da empresa ou ID da empresa.
- **Delegação:** **Todas**, **Delegadas** ou **Não delegadas**.
- **Status da licença:** **Todas**, **Válida**, **A vencer**, **Expirada** ou **Encerrada**.

Cards de empresas

Cada card de empresa mostra metadados de gerenciamento essenciais:

- **Status da licença** com selo de ícone e dica de ferramenta contextual.
- **Dispositivos licenciados** (limite de dispositivos da empresa).
- **Próxima renovação agendada** ou **Data de expiração**, dependendo do estado da assinatura.
- Estado de **delegação** (**Proprietário**, **Concedida** ou **Não concedida**).
- Nome de exibição e nome de usuário do **Proprietário**.

Empresas selecionadas recentemente

As empresas que você acessou recentemente estão fixadas em uma seção de **Selecionadas recentemente** para agilizar a alternância repetida de contexto.

Ações da empresa

- **Entrar na empresa:** abre o contexto da empresa selecionada quando a delegação/propriedade permite o acesso.

- **Gerenciar faturamento:** abre o gerenciamento de faturamento da empresa quando disponível e permitido.
- **Comprar licença:** abre o fluxo de compra da empresa quando o faturamento não estiver ativo.

Quem pode gerenciar licenças

Para empresas criadas por uma conta multi-tenant, o gerenciamento de licenças é controlado pelos usuários da conta multi-tenant. A conta principal pode sempre gerenciar o faturamento e as ações de licença para essas empresas.

Subcontas podem gerenciar faturamento e ações de licença apenas se a conta principal conceder a permissão **Pode gerenciar licença** na página de [Subcontas](#).

Criar empresa gerenciada

Contas multi-tenant principais podem expandir **Criar empresa gerenciada** a partir da área de ações na parte inferior.

- **O nome da empresa** é obrigatório.
- **Criar usuário administrador por empresa** controla o modo de propriedade.
- Quando ativado, **Nome de usuário do administrador** (formato de e-mail) e **Nome do administrador** são obrigatórios.
- Antes da criação, uma caixa de diálogo de confirmação resume a operação e, quando aplicável, avisa que credenciais temporárias são enviadas por e-mail para o novo usuário administrador.

O novo usuário administrador deve escolher uma nova senha na primeira vez que entrar com a senha temporária.

Modo de propriedade

- **Administrador por empresa ativado:** o novo usuário administrador é o proprietário da empresa e pode delegar o gerenciamento para sua conta multi-tenant.
- **Administrador por empresa desativado:** a empresa é de propriedade direta da sua conta multi-tenant.

Cota de empresa

Se a conta atingir a cota de empresas configurada, a criação será bloqueada e o formulário exibirá uma mensagem de contato de suporte com a contagem atual e máxima de empresas.

Quando a cota de empresas for atingida, você não poderá criar novas empresas gerenciadas até que seu limite seja aumentado.

Troca de empresa (Enterprise switching)

O alternador de empresa na barra de ferramentas superior permite que usuários de multi-tenancy alternem entre empresas delegadas sem precisar encerrar a sessão. Ele está disponível quando pelo menos um contexto de empresa pode ser selecionado.

Comportamento do alternador

- O gatilho mostra o nome da empresa atual (ou o ID da empresa, caso não haja um nome disponível).
- O menu lista as empresas delegadas/acessíveis e marca a empresa atual como já selecionada.
- Durante a troca, as ações do alternador são desativadas temporariamente para evitar mudanças de escopo simultâneas.

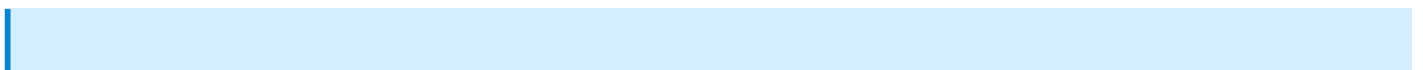
Sair da empresa

O menu do alternador inclui **Sair da empresa**, que limpa o contexto da empresa atual e retorna você para a área de trabalho global de multi-tenancy.

Regras de redefinição de contexto

A troca de empresa ou a saída da empresa redefine o escopo do painel. As páginas específicas da empresa e os dados são atualizados para o novo contexto selecionado, e a visibilidade do menu se adapta ao fato de uma empresa estar ou não selecionada no momento.

A empresa selecionada se aplica a todas as abas abertas do navegador. Se você trocar de empresa ou sair dela em uma aba, as outras abas recarregam o painel na próxima ação, para nunca operarem em uma empresa diferente da exibida.



Use o alternador para mudanças rápidas de contexto operacional, mas verifique o nome da empresa selecionada antes de executar ações sensíveis, como atualizações de política ou comandos de dispositivos.

Subcontas

A página de **Subcontas** (*Dashboard* → *Subcontas*) está disponível para contas multi-tenant principais. Ela permite criar usuários gerenciadores delegados, atribuir empresas gerenciadas, controlar permissões de faturamento e manter as credenciais das subcontas.

Lista de subcontas

Cada card de subconta mostra controles de identidade e gerenciamento:

- **Nome** e **nome de usuário/e-mail**.
- **Atribuição de múltiplas empresas gerenciadas**.
- Alternância de permissão **Pode gerenciar licença**.
- Ações de **Redefinir senha** e **Excluir**.

Atribuição de empresas gerenciadas

As atribuições de empresas são editadas por meio do campo de seleção múltipla **Empresas gerenciadas**. Quando você fecha o seletor após as alterações, o dashboard solicita confirmação antes de salvar as atualizações.

Atribuir uma empresa a disponibiliza para a subconta, mas a subconta só pode entrar nela depois que o acesso for concedido. Remover uma empresa das atribuições também remove o acesso da subconta a ela.

Permissão de gerenciamento de licença

A alternância **Pode gerenciar licença** controla se uma subconta pode acessar as ações de faturamento/gerenciamento de licenças da empresa.

Para empresas criadas pela conta multi-tenant, a conta principal sempre possui direitos de gerenciamento de licenças. As subcontas recebem direitos de gerenciamento de licenças apenas quando esta opção é ativada pela conta principal.

Redefinição de senha

Redefinir senha gera uma nova senha temporária e a envia para a subconta por e-mail após a confirmação.

Ao entrar com uma senha temporária, seja após uma redefinição ou em uma subconta recém-criada, o usuário deve escolher uma nova senha antes de continuar.

Excluir subconta

A exclusão de uma subconta requer confirmação e remove permanentemente o acesso delegado para essa conta.

Criar subconta

Use o painel de ações inferior **Criar subconta** para adicionar um novo gerenciador delegado.

- **E-mail:** obrigatório e validado no formato de e-mail.
- **Nome:** nome de exibição obrigatório.
- **Pode gerenciar licença:** permissão de faturamento inicial opcional.
- Antes da criação, uma caixa de diálogo de confirmação avisa que um e-mail com a senha temporária será enviado para o endereço fornecido.

Insights

Aqui estão alguns artigos que detalham como o MDM pode ajudar sua empresa:

[O que é o Modo Quiosque? Um guia para bloquear dispositivos Android e Apple para negócios](#)

O modo quiosque transforma telefones e tablets comuns em ferramentas de negócios focadas. O Cerberus Enterprise ajuda as organizações a bloquear dispositivos em um único aplicativo ou em um pequeno conjunto de aplicativos aprovados para casos de uso como PDV de varejo, check-in para clientes e navegação de frotas, mantendo esses dispositivos especializados mais fáceis de proteger, suportar e gerenciar em escala.

[Como Escolher a Solução de MDM Certa: Um Checklist de 7 Pontos para Pequenas Empresas](#)

Escolher um MDM tarde no processo de compra é mais fácil quando a comparação permanece prática. Este checklist ajuda pequenas empresas a avaliar fornecedores com base nos sete critérios que geralmente são mais importantes em implementações reais: segurança, suporte a Android e Apple, facilidade de uso para equipes enxutas, escalabilidade, limites de privacidade, custo total de propriedade e suporte operacional diário.

Criando uma Sala de Aula Digital

Segura e Focada: Um Guia de MDM para Escolas K-12

Dispositivos gerenciados pela escola funcionam melhor quando permanecem centrados no aprendizado. O Cerberus Enterprise ajuda as organizações de ensino fundamental e médio a manter os dispositivos dos alunos focados por meio de aplicativos gerenciados, restrições no estilo quiosque, configurações padronizadas para dispositivos compartilhados ou emprestados e ações de recuperação remota que reduzem perdas, desvios de uso e interrupções em sala de aula.

Equipando seus Técnicos de

Campo: Como o MDM Impulsiona a

Eficiência e a Segurança no Local

Técnicos de campo dependem de dispositivos móveis para cronogramas, notas de serviço, referências técnicas, histórico de clientes e atualizações de tarefas enquanto trabalham no local. O Cerberus Enterprise ajuda a manter esses dispositivos prontos por meio de aplicativos gerenciados, modelos de dispositivos padronizados, comandos de suporte remoto e visibilidade baseada em localização, o que pode melhorar a coordenação de despacho ao mesmo tempo que reforça a segurança no campo.

Além do Mapa: Usando MDM para uma Gestão de Frota e Segurança

do Motorista Mais Inteligentes

As operações de frota dependem de dispositivos móveis para navegação, despacho, mensagens, registros e execução em campo. O Cerberus Enterprise ajuda a manter esses dispositivos focados em fluxos de trabalho aprovados por meio de aplicativos gerenciados, controles de quiosque e dispositivos dedicados, políticas de comunicação segura, solução remota de problemas e supervisão baseada em localização, o que pode reduzir o tempo de inatividade e apoiar operações de direção mais seguras.

Como Cercas Virtuais (Geofences),

Rastreamento ao Vivo e Mapas de

Localização Melhoram as

Operações Empresariais

Recursos baseados em localização no Cerberus Enterprise ajudam as organizações a passar de uma simples visibilidade de dispositivos para um controle operacional mais prático. Relatórios periódicos de localização, rastreamento ao vivo, transições de cercas virtuais (geofence) e mapas interativos podem dar suporte à logística, serviços de campo, saúde, varejo, construção e outras equipes distribuídas que precisam de uma melhor percepção sobre onde o trabalho está ocorrendo e quando os dispositivos entram ou saem de áreas importantes.

Como o Multi-tenancy Ajuda os

MSPs a Escalar Serviços de MDM e

Criar Novas Fontes de Receita

O multi-tenancy permite que MSPs, revendedores e organizações multieempresas gerenciem várias empresas a partir de uma única conta do Cerberus Enterprise, mantendo cada ambiente separado. Este modelo reduz o atrito operacional, melhora a escalabilidade do serviço e suporta o acesso delegado por meio de subcontas e administração explícita controlada pelo cliente. Também cria oportunidades de negócios mais fortes para provedores que desejam combinar o licenciamento de software com serviços de integração (onboarding), suporte, conformidade e mobilidade gerenciada.

Aprimorando a Operatividade

Empresarial com Soluções de MDM

O Gerenciamento de Dispositivos Móveis (MDM) centraliza o controle dos dispositivos da empresa, simplificando o registro, a configuração e a manutenção. O provisionamento automatizado e as operações em massa reduzem o trabalho manual de TI e garantem políticas consistentes em todos os dispositivos. Recursos de segurança, como criptografia, monitoramento de conformidade e limpeza remota, protegem os dados corporativos. No geral, o MDM aumenta a produtividade ao mesmo tempo que reduz os custos de suporte e a complexidade operacional.

Segurança Avançada no

Gerenciamento Android Enterprise

O Android Enterprise usa um perfil de trabalho para isolar os aplicativos e dados corporativos do conteúdo pessoal no mesmo dispositivo. Essa containerização cria ambientes criptografados separados, gerenciados de forma independente pelos administradores de TI. As políticas de segurança podem controlar o compartilhamento de dados corporativos sem afetar os aplicativos pessoais. A arquitetura protege os dados empresariais mesmo que os aplicativos pessoais sejam comprometidos.

MDM para Apple iPhone e Registro

Automático

A estrutura de MDM da Apple permite o gerenciamento centralizado de iPhones em ambientes empresariais. Combinado com o Apple Business Manager, os dispositivos podem se registrar e configurar automaticamente ao serem ativados pela primeira vez. Os administradores podem implantar e configurar aplicativos corporativos de forma silenciosa, aplicar configurações de segurança e monitorar a conformidade. Essa automação garante uma configuração consistente dos dispositivos e reduz erros de configuração.

Entendendo o Gerenciamento de

Dispositivos Móveis

O Gerenciamento de Dispositivos Móveis (MDM) oferece uma plataforma centralizada para monitorar, proteger e controlar dispositivos móveis que acessam sistemas corporativos. As capacidades principais incluem a aplicação de políticas de segurança, o gerenciamento de aplicativos e o bloqueio ou limpeza remota de dispositivos perdidos. O MDM ajuda a proteger os dados corporativos enquanto mantém a conformidade dos dispositivos. Ele permite que organizações de qualquer tamanho gerenciem com segurança equipes de trabalho móveis em crescimento.

Modelos de Implantação de

Dispositivos Empresariais

As organizações podem adotar múltiplos modelos de propriedade de dispositivos, como BYOD, CYOD, COPE, COBO e COSU. Cada modelo equilibra custo, flexibilidade do usuário e controle de segurança de forma diferente. O BYOD prioriza a conveniência do usuário, enquanto o COBO e o COSU maximizam o controle corporativo e a segurança. A escolha do modelo correto depende de

requisitos regulatórios, necessidades da força de trabalho e capacidade de gerenciamento de TI.

MDM vs. EMM vs. UEM

O MDM foca no gerenciamento e na segurança de dispositivos móveis por meio da aplicação de políticas, controle de configuração e gerenciamento remoto. O EMM expande esse escopo para incluir o gerenciamento de aplicativos e conteúdo, enquanto o UEM tenta gerenciar todos os endpoints, incluindo laptops e desktops. Para muitas PMEs, suítes completas de EMM ou UEM adicionam uma complexidade desnecessária. Na prática, recursos robustos de MDM geralmente atendem à maioria dos requisitos de gerenciamento móvel.

MDM em Telefones Pessoais e

Privacidade do Funcionário

Os sistemas modernos de MDM usam a containerização para separar os dados de trabalho dos dados pessoais em dispositivos de propriedade do funcionário. Os empregadores podem apenas gerenciar e monitorar o ambiente de trabalho, incluindo aplicativos corporativos e informações de conformidade do dispositivo. Dados pessoais, como fotos, mensagens e histórico de navegação, permanecem inacessíveis para a empresa. Essa separação técnica permite programas BYOD seguros, preservando ao mesmo tempo a privacidade do funcionário.

ROI de MDM e Valor de Negócio

O MDM deve ser avaliado como um investimento estratégico, e não apenas como uma despesa de segurança. Ele gera retornos financeiros por meio da redução de perdas de dispositivos, menores custos de suporte de TI e melhoria na eficiência operacional. O gerenciamento automatizado também aumenta a produtividade dos funcionários e reduz o tempo de inatividade. Além disso, uma segurança mais robusta reduz o risco e o impacto financeiro de violações de dados.

Gerenciamento de Dispositivos em

Conformidade com a HIPAA

As organizações de saúde devem proteger os dados eletrônicos dos pacientes de acordo com os requisitos de segurança da HIPAA. O MDM ajuda a aplicar criptografia, controles de autenticação, transmissão segura de dados e logs de auditoria detalhados. Ele também permite a limpeza remota e a aplicação centralizada de políticas para dispositivos que acessam sistemas médicos. Esses controles reduzem os riscos de conformidade, ao mesmo tempo que permitem fluxos de trabalho móveis em ambientes de saúde.

MDM para Operações de Varejo e

Segurança

As organizações de varejo dependem de dispositivos móveis para sistemas de PDV, gerenciamento de estoque e operações em loja. O MDM garante que esses dispositivos permaneçam seguros, atualizados e em conformidade com padrões como o PCI-DSS. O gerenciamento centralizado reduz o tempo de inatividade e simplifica a implantação de dispositivos em múltiplos locais. O resultado é uma melhor eficiência operacional e a redução do risco de incidentes de segurança relacionados a pagamentos.