# 设备配置 - Android

- 支持的设备
- 注册令牌
- 个人拥有的设备
- 用于工作和个人用途的公司设备
- 仅用于工作的公司设备
- Zero-touch
- Authenticate Using Google enrollment

支持的设备
通常，任何运行 Android 6 或更高版本并带有 Google Play 服务的设备都与 Cerberus Enterprise 兼容。

为了获得更好的用户体验，我们建议使用符合 Android Enterprise Recommended要求的设备。

某些功能仅限于特定的 Android

版本，或者在不同操作系统版本中的行为可能有所不同。有关特定功能的详细信息，请参阅文档的 政策
部分。

Cerberus Enterprise 同时支持公司拥有和个人拥有的设备，以及两种管理模式：设备所有者和资料所有者。

个人拥有 的设备可以通过 工作资料
进行管理。这样可以将员工的工作数据和应用与个人数据和应用分开，从而同时提高安全性和隐私性，实现
BYOD 解决方案。此选项适用于员工已拥有、且你希望将其注册到组织中用于工作的设备。

公司拥有 的设备也可以通过工作资料进行管理，但你还可以选择 完全受管理
选项，从而对设备进行更严格的控制。当你向员工提供公司设备用于工作但仍允许个人使用时，带工作资料的
公司设备非常合适。完全受管理的设备更适合必须仅用于工作的设备，或用于 专用设备 （COSU ，公司拥有单用途），例如自助服务终端。

有关设备配置的详细信息，请参阅 设备配置概览 页面。

注册令牌
Cerberus Enterprise 使用注册令牌来启动 Android
设备注册（配置）流程。你选择的令牌会定义应用于已注册设备的初始政策，并影响允许使用的配置模式。

只有在完成 Android Management 设置 后，才会显示 Android 注册令牌标签页。

在哪里查找注册令牌
在仪表板中，打开 注册令牌 。根据你的账户配置，该页面可能会显示多个标签页（ Android 令牌、 Google 登录注册、 Apple 手动注册和 Apple Automated Device Enrollment）。

如果你的 Android 企业由受管理的 Google 域（ Google Workspace）提供支持，仪表板还可能会显示
Authenticate Using Google Enrollment标签页。有关启用和使用它的详细信息，请参阅

Authenticate Using Google enrollment。

注册令牌列表（ Android）
Android 令牌标签页会显示所有令牌的表格。点击某一行会打开令牌详细信息页面。

列

状态 ：有效 （设备可使用该令牌注册）、 已过期 （过期日期已过）或 已用完
（已使用的一次性令牌）。
政策 ：分配给该令牌的政策（工具提示会显示政策 ID）。 已删除的政策
表示该政策在令牌创建后被删除。
用户 ：预先分配给使用该令牌注册的设备的可选用户。 已删除的用户
表示该用户在令牌创建后被删除。
注册数 ：使用该令牌注册的设备数量；对于一次性令牌，显示为 n / 1。
个人使用 ：允许 / 不允许 / 专用设备。
创建时间 ：令牌的创建时间。表格将最新的令牌显示在最前面。
过期时间 ：过期日期 /时间，或 从不 。
注册代码 ：令牌的代码，即在不使用二维码注册设备时在设备上输入的代码。

操作

每一行都有一个删除操作（ 删除注册令牌 ）。许可证过期时，删除操作会被禁用。
该表格支持多行选择：你可以启用选择模式，选择多个令牌，然后使用 删除所选令牌 将其删除。
使用刷新操作重新加载列表。表格已分页（每页 10/25/50 项）。

创建新的注册令牌
在 Android 令牌标签页上，点击 新建注册令牌
以打开令牌创建页面。如果你的许可证已过期，创建按钮会被禁用。

令牌选项

1. 政策

必需。 此政策会自动应用于使用该令牌注册的所有设备。请选择你的 Android 政策之一。如果你还没有任何政策，请先创建一个。

2. 用户

可选。如果设置，新注册的设备会自动关联到此用户。

3. 个人使用

控制使用此注册令牌配置的设备是否允许个人使用：
允许 ：适用于个人拥有的设备（工作资料）以及用于工作和个人用途的公司设备。
不允许 ：适用于仅用于工作的公司设备（完全受管理）。
专用设备 ：适用于自助服务终端 /专用设备（设备不与单个用户关联）。

4. 允许的使用次数

选择该令牌可以多次使用（ 多次 ）还是仅使用一次（ 仅一次 ）。

5. 过期时间

选择过期单位（ 分钟 、小时 、天 或从不
）。如果未设置为从不，请输入过期值。允许的范围取决于所选单位，最大可达 10,000 天。

6. Google 身份验证

控制用户在设备注册期间是否必须使用 Google 账户进行身份验证：

- 未指定 ：将使用企业级 Google 身份验证设置来确定用户在注册期间是否需要使用 Google 进行身份验证。
- 可选：用户可以选择在注册期间跳过 Google 身份验证。
- 必需：用户必须使用 Google 账户进行身份验证才能继续注册。

当选择 必需 时，会出现可选的 必需账户电子邮件 字段。如果设置，用户必须在注册期间使用该特定 Google 账户进行身份验证。

## 配置选项（仅限二维码）

这些附加选项会嵌入二维码中，并在通过扫描二维码注册完全受管理设备的配置过程中应用。它们不适用于工作资料或使用注册 URL 或令牌注册的设备。

## Wi-Fi 配置

使用此项可让设备在配置期间自动连接 Wi-Fi，以便下载并初始化管理应用。可用字段包括 **SSID**、隐藏 **SSID**、安全性 ，以及（需要时） 密码短语 。

你还可以配置 HTTP 代理（ 代理），并根据模式设置 主机 /端口、 **PAC URI**和 代理绕过主机 。

### 其他选项

附加选项包括 区域设置 、时区 和 跳过加密 。

## 注册令牌详细信息

打开令牌后，详细信息页面会显示令牌配置和使用信息：

- 状态、过期时间 、使用情况 、个人使用 、允许的使用次数 ，以及（设置时） **Google** 身份验证和可选的 必需账户电子邮件 。
- 令牌：原始注册令牌值（可复制）。
- 注册 **URL**：Google Android Enterprise 注册 URL（可复制并可通过电子邮件发送）。
- 二维码 ：显示在页面右侧，用于注册完全受管理的设备。

> 有关分步配置流程，请参阅 Android 注册指南：个人拥有的设备、用于工作和个人用途的公司设备、仅用于工作的公司设备，以及 **Zero-touch**。

# 个人拥有的设备

员工拥有的设备可以设置 工作资料

。工作资料为工作应用和数据提供一个独立的空间，与个人应用和数据分开。大多数应用、数据和其他管理政

策仅适用于工作资料，而员工的个人应用和数据保持私密。

要在个人拥有的设备上设置工作资料，请使用以下配置方法之一（确保 注册令牌 的 个人使用 设置为 允许 ）：

## 注册令牌链接

| Android 版本 |
| --- |
| 6.0+ |

你可以将注册 URL 提供给最终用户。当最终用户从设备上打开该链接时，系统会引导他们完成工作资料设置。

## 从 "设置 "添加工作资料

| Android 版本 |
| --- |
| 6.0+ |

要在其设备上设置工作资料，用户可以打开设备的 设置 应用，然后使用搜索栏查找并点按 设置工作资料 选项。

如果搜索不成功，此选项的位置可能会有所不同。以下是几种可能：

- 设置 -> *Google* 服务和偏好设置 -> 所有服务 -> 设置工作资料 .
- 设置 -> *Google* -> 设置 & 恢复 -> 设置工作资料 .

这些步骤会启动一个设置向导，在设备上下载 *Android Device Policy*

。接下来，系统会提示用户扫描二维码或手动输入注册令牌，以完成工作资料设置。

## 下载 Android Device Policy

| Android 版本 |
| --- |
| 6.0+ |

要在其设备上设置工作资料，用户可以从 Google Play 商店下载 Android Device Policy

。应用安装后，系统会提示用户扫描二维码或手动输入注册令牌，以完成工作资料设置。

## 个人 iPhone 和 iPad

个人 iPhone 和 iPad（以及 Mac）使用 Apple 用户注册 ：用户在设备设置中使用其 Managed Apple Account 登录，只有工作应用、账户和数据受到管理。在 iPhone 和 iPad 上，政策中的 App Store 应用和 Cerberus Enterprise应用会使用该账户的用户许可证安装。仅当个人设备的政策开启

个人设备上的位置和地理围栏 且用户允许时，才会收集其位置。请阅读 Apple 账户驱动注册 。

用于工作和个人用途的公司设备
通过设置带 工作资料 的公司设备，可使该设备同时用于工作和个人用途。在带工作资料的公司设备上：
大多数应用、数据和其他管理政策仅适用于工作资料。
员工的个人资料保持私密。不过，企业可以强制执行某些设备级政策和个人使用政策。
企业可以使用 屏蔽范围 在整个设备或其工作资料上强制执行合规性操作。
设备取消注册和设备命令会应用于整个设备。

要设置带工作资料的公司设备，请使用以下配置方法之一（确保 注册令牌 的个人使用 设置为 允许 ）：

二维码方法

Android 版本

8.0+

在全新或恢复出厂设置的设备上，用户（通常是 IT
管理员）在同一位置点按屏幕六次。这会触发设备提示用户扫描二维码。

仅用于工作的公司设备
完全设备管理 适用于专用于工作目的的公司设备。企业可以管理设备上的所有应用，并可以强制执行 Android Management API 的全套政策和命令。
还可以（通过政策）将设备锁定到单个应用或一小组应用，以满足特定目的或使用场景。这类完全受管理的设
备子集称为 专用设备 。
要在公司设备上设置完全管理，请使用以下配置方法之一（确保 注册令牌 的个人使用 设置为 不允许 ）：

二维码方法

Android 版本

7.0+

在全新或恢复出厂设置的设备上，用户（通常是 IT
管理员）在同一位置点按屏幕六次。这会触发设备提示用户扫描二维码。

DPC 标识符方法

Android 版本

5.1+

如果无法通过二维码添加 Android Device Policy，用户或 IT
管理员可以按照以下步骤配置完全受管理或专用设备：

1. 在全新或恢复出厂设置的设备上按照设置向导操作。
2. 输入 Wi-Fi 登录详细信息，将设备连接到互联网。
3. 当系统提示登录时，输入 afw#setup，这会下载 Android Device Policy。
4. 扫描二维码或手动输入注册令牌以配置设备。

# Zero-touch

IT 管理员可以使用 Zero-touch 注册方法配置公司拥有的设备，具体步骤见 Zero-touch enrollment for IT admins。设备首次开机时，会自动强制应用 IT 管理员定义的设置。

IT 管理员可以预配置从 授权经销商 购买的设备，并使用 Cerberus Enterprise 仪表板进行管理。要关联你的 Zero-touch 账户，请转到仪表板中的 **Zero-touch**部分，然后按照说明操作。

| Android 版本 | 工作资料 | 完全受管理的设备 | 专用设备 |
| --- | --- | --- | --- |
| 8.0+ (Pixel 7.1+) | ✓ | ✓ | ✓ |

Authenticate Using Google

enrollment

Authenticate Using Google enrollment（也称为 Google Authentication for Enrollment ）允许用户在 Android 设备注册期间使用其 Google Workspace 账户进行身份验证。

此功能仅适用于由受管理的 Google 域（ Google Workspace）提供支持的 Android 企业。

在哪里找到它
在仪表板中，打开 注册令牌 并选择 Authenticate Using Google Enrollment标签页。仅当已配置
Android Management 且你的企业可以使用 Google Workspace 集成时，才会显示该标签页。

启用（或禁用） Google 身份验证
Google 身份验证可在 Google Admin 控制台 中启用。更改设置后，请返回 Cerberus Enterprise 并使用刷新状态 重新加载当前配置。

1. 使用管理员账户登录你的 Google Admin 控制台 。
2. 打开 设备 。
3. 转到 移动设备与端点 → 设置 → 第三方集成 。
4. 找到 Cerberus Enterprise 的Android EMM 集成 并将其打开。
5. 点击 管理 EMM 提供商 。
6. 切换 Authenticate Using Google以启用或禁用注册时的 Google 身份验证。
7. 点击 保存 。
8. 返回 Cerberus Enterprise 仪表板，并在 Authenticate Using Google Enrollment 标签页上点击 刷新状态 。

Google 身份验证注册令牌

启用 Google 身份验证后，仪表板会显示一个专用于此注册模式的注册令牌。该页面可能会显示 二维码 、注册令牌 值和 注册 URL（可复制并可通过电子邮件发送）。

关键选项

允许个人使用
：控制该令牌是否可以注册用于工作和个人用途的设备（工作资料场景）或仅用于工作的设备（完全
受管理 /专用场景）。
回退默认政策 ：当注册用户未分配特定的 Google 身份验证默认政策时应用的政策。

政策交互

政策设置 工作账户设置身份验证 （workAccountSetupConfig.authenticationType
）控制用户在工作账户设置期间进行身份验证的方式，但 Google Admin Console 设置 Authenticate Using Google和注册令牌类型仍可能要求进行身份验证。

对于已注册的设备，此政策仅在设备由受管理的 Google Play 账户管理时适用（即未使用 Authenticate Using Google Enrollment注册）。

许可证过期时，某些操作（例如更改令牌选项）可能会被禁用。

注册设备
在注册期间，系统会提示用户使用其 Google Workspace
账户进行身份验证。注册成功后，设备会与通过身份验证的用户关联。

工作资料（个人拥有的设备）

将注册 URL分享给用户。当用户在 Android 设备上打开它时，会引导他们完成工作资料设置和 Google 身份验证。
或者，用户可以从 Android
设置开始，选择工作资料设置流程，然后在系统提示时扫描二维码或输入注册令牌。

公司拥有的设备

二维码方法
：在全新或恢复出厂设置的设备上，在同一位置多次点按屏幕，直到出现二维码提示，然后扫描仪表
板中显示的二维码。

DPC 标识符方法 （无法进行二维码扫描时）：按照设置向导操作，连接 Wi‑Fi
，然后在提示登录时输入 afw#setup，并通过扫描二维码或输入注册令牌继续。出现提示时，使用
Google Workspace 账户进行身份验证。

有关通用的 Android 配置流程（工作资料与完全受管理），请参阅本手册中的标准 Android 注册页面。