AppTec360 企业移动管理器和 ContentBox

管理手册 5.0 版 (202110)

目录

- 关机装置
- 重启设备
- 警报和丢失模式 | 禁用丢失模式
- 删除设备
- 擦拭设备
- 企业擦除 | 删除 MDM
- 发送信息
- TeamViewer 远程控制
- 发送注册申请

安卓

- 编辑设备
- 清除密码
- 锁定装置
- 删除设备
- 擦拭设备
- 移除 MDM
- 发送信息
- 转换为 COPE 模式
- 发送注册申请
- 迁移传统设备

视窗

- 编辑设备
- 删除设备
- 企业擦除 | 删除 MDM
- TeamViewer 远程控制
- 发送注册申请

内容管理

- 组文件
- 文件资源管理器
- 审计跟踪
- 垃圾
- 外部存储

审计日志

iOS 配置

- SecurePIM 安全
- SecurePIM 浏览器
- 交流

连接管理

- 无线网络
  - 代理设置
  - 安全类型
- 虚拟专用网
  - VPN 类型
    - 虚拟专用网
    - 每个应用程序的 VPN
  - 代理设置
- APN
- 细胞
- HTTP 代理服务器
- AirPrint
- AirPlay

PIM 管理

- Exchange Active Sync
- 电子邮件
  - 来信
  - 外寄邮件
- CalDav
- 订阅日历
- LDAP

网络管理

- 网络剪辑
- 网页内容过滤器

应用程序管理

- 企业应用管理器
  - 已安装的应用程序（仅限设备级别）
  - 必须使用的应用程序
    - 安装-选项
  - 网络应用程序

- 限制和设置
  - 黑名单/白名单应用程序
  - 系统应用程序限制
  - App-VPN
  - 应用程序设置
- 企业应用商店
  - iTunes 应用程序
  - 内部
- 信息亭模式
  - 应用类型
    - 包装
    - 网址
  - 信息亭模式设置

安卓企业 – 全面管理设备配置

一般情况

- 组概况概览（仅适用于组级）
- 设备概述（仅限设备级别）
- 配置修订（仅限设备级）
- 设备日志（仅限设备级）
  - 命令日志
  - 可能的命令状态
- 设备设置
  - 客户端配置
  - 壁纸

资产管理（仅限设备级）

- 设备信息
  - 无线网络
- 细胞
- 蓝牙

安全管理

- 防盗（仅限设备级）
  - GPS 信息（仅限设备级别）
  - 擦除和锁定（仅限设备级别）
  - 信息（仅限设备级别）

- 安全配置
  - 设备密码
  - 防病毒
- 报废（仅限设备级）
  - 擦除（仅限设备级）
- 限制设置
  - 限制条件
- 证书管理

连接管理

- 无线网络
  - 安全类型
    - WEP
    - WPA/WPA2
    - 802.1x EAP
- 虚拟专用网
  - VPN 类型
    - 虚拟专用网
    - 每个应用程序的 VPN
- 限制条件

PIM 管理

- Gmail Exchange

应用程序管理

- 企业应用管理器
  - 已安装的应用程序（仅限设备级别）
  - 系统应用程序（仅限设备级）
  - 必须使用的应用程序
  - 黑名单和白名单
  - AE 系统应用程序
- 限制和设置
  - 应用程序管理设置
- 企业应用商店
  - 内部
- 企业 Play 商店
  - AE Play 商店
- 信息亭模式和启动器

- 资产管理（仅限设备级）
  - 设备信息
    - 无线网络
  - 细胞
  - 蓝牙
- 安全管理
  - 防盗（仅限设备级）
    - GPS 信息（仅限设备级别）
    - 擦除和锁定（仅限设备级别）
    - 信息（仅限设备级别）
  - 安全配置
    - 设备密码
    - 集装箱密码
    - 防病毒
  - 报废（仅限设备级）
    - 擦除（仅限设备级）
  - 限制设置
    - 限制条件
  - 证书管理
- 连接管理
  - 无线网络
    - 安全类型
      - WEP
      - WPA/WPA2
      - 802.1x EAP
  - 虚拟专用网
    - VPN 类型
      - 虚拟专用网
      - 每个应用程序的 VPN
  - 限制条件
- PIM 管理
  - Gmail Exchange
- 应用程序管理
  - 企业应用管理器
    - 已安装的应用程序（仅限设备级别）

- 安全配置
  - 密码
  - 加密
  - 防病毒
- 报废（仅限设备级）
  - 擦除（仅限设备级）
- 限制设置
  - 限制条件
  - AE 设备所有者

BYOD 容器

- 安卓企业
  - 安卓企业
  - Gmail Exchange
  - AE 系统应用程序
  - 集装箱密码
- 三星 KNOX
  - 激活
  - 诺克斯密码
  - 诺克斯安全系统
  - 诺克斯交流中心
  - 诺克斯电子邮件
  - 诺克斯应用程序

连接管理

- 无线网络
  - 安全类型
    - WEP
    - WPA/WPA2
    - 802.1x EAP
- 虚拟专用网
- 限制条件
- APN
- 蓝牙

PIM 管理

- 交流
- 电子邮件

- AE Gmail Exchange
- 应用程序管理
  - 企业应用管理器
    - 已安装的应用程序（仅限设备级别）
    - 系统应用程序（仅限设备级）
    - 必须使用的应用程序
    - AE 系统应用程序
  - 限制和设置
    - 黑名单和白名单
    - 系统应用程序限制
      - 三星应用程序
      - 华为应用程序
    - 应用程序管理设置
  - 企业应用商店
    - Playstore
    - 内部
  - 企业 Play 商店
  - 信息亭模式和启动器
    - 信息亭模式
    - AppTec360 启动器
    - AppTec360 设置
- 遥控器
  - 泼水节
  - Teamviewer
- 内容管理
  - 内容框
  - 安全浏览器

配置 Windows 10 电脑

- 一般情况
  - 组概况概览（仅适用于组级）
  - 设备概述（仅限设备级别）
  - 设置
  - 配置修订（仅限设备级）
  - 设备日志（仅限设备级）

- 命令日志
- 可能的命令状态

资产管理（仅限设备级）

- 设备信息
- 细胞
- 同步信息

安全管理

- 防盗（仅限设备级）
  - GPS 信息（仅限设备级别）
  - GPS 设置
- 安全配置
  - 密码
  - 杀毒软件
  - 安全中心
  - 防火墙配置
  - 防火墙规则
- 限制设置
  - 设备功能
- 比特锁
  - BitLocker 配置
  - BitLocker 状态
- 证书管理
  - 证书列表
  - 证书配置
  - SCEP

连接管理

- 无线网络
  - 安全类型
  - 使用代理服务器
- 无线网络限制
- 虚拟专用网
  - 连接类型
  - 通用 VPN 配置
- VPN 限制
- 蓝牙

PIM 管理

- Exchange Active Sync

- 电子邮件
- 应用程序管理
  - 企业应用管理器
    - 已安装的应用程序
    - 必须使用的应用程序
    - 系统应用程序限制
    - 黑名单和白名单

MacOS 配置

一般情况

- 组概况概览（仅适用于组级）
- 设备概述（仅限设备级别）
- 配置修订（仅限设备级）
- 设备日志（仅限设备级）
  - 命令日志
  - 可能的命令状态

资产管理（仅限设备级）

- 设备信息
- 无线网络
- 细胞
- 蓝牙

更新管理（仅限设备级）

- 更新信息

安全管理

- 防盗
  - 擦拭和锁定
- 安全配置
  - 密码
  - 证书
- 限制设置
  - 设备功能
  - iCloud
  - 媒体管理

连接管理

- 无线网络

- 企业 Wi-Fi 配置
- 虚拟专用网
- HTTP 代理服务器
- AirPrint
- AirPlay

PIM 管理

- Exchange Active Sync
- 电子邮件
- CalDav
- 卡达维
- LDAP

仪表板和报告

仪表板设置

仪表板视图

扩展报告

- 合规报告
  - 扎根设备
  - 漫游设备
  - 支持漫游的设备
  - 受监控设备
  - 非活动设备
- 设备报告
  - 按所有权划分的设备
  - 所有设备
  - 设备载体
  - 安全设备
  - Windows BitLocker 设备
- 应用程序报告
  - 已安装的应用程序
  - 安装最多的应用程序
  - 必须使用的应用程序
  - 黑名单应用程序
- 用户报告
  - 关税

概况

AppTec360 简介

AppTec 的企业移动管理解决方案可通过其直观的管理控制台管理和配置所有移动设备。 在这种情况下，EMM 服务器既可以在您自己的环境中运行，也可以利用我们的云解决方案。

即使是关于在智能手机上集中安装企业应用程序的话题，您也找对了地方。 通过企业移动管理器，您可以在几秒钟内将企业应用程序和文档分发到设备上，或通过白名单/黑名单阻止不受欢迎的应用程序。

公司使用私人设备给智能手机和平板电脑的安全带来了新的挑战。 由于员工希望越来越多地使用智能手机，IT 管理员必须保护大量不同类型的设备。 我们将帮助您保护所有设备及其存储的敏感数据，并通过直观的控制台对其进行管理。

支持的设备操作系统

AppTec360 支持 iOS、Android 和 Windows 设备。 请注意，上述平台的功能容量可能因操作系统而异。

- 苹果 iOS 11.0 或更高版本*
- 苹果 macOS 10.11 或更高版本
- 云版本的谷歌 Android 4.4 或更高版本**
- 企业内部版本的谷歌 Android 4.1 或更高版本**
- MS Windows 10 或更高版本***（台式电脑、笔记本电脑和平板电脑）

**请注意，由于苹果公司对注册过程进行了大幅修改，iOS 10 或更早版本的设备无法注册。*

***即使设备使用的版本不再受制造商支持，也可以连接和配置。 请注意，有些功能可能需要特定的 Android 版本。 在支持案例中，我们遵循制造商的官方支持。 如果是由制造商不再支持的过时版本引起的问题或错误，我们保留仅提供有限支持的权利。*

****由于操作系统的限制，不支持 Windows 家庭版。 我们强烈建议使用仍受制造商支持的操作系统版本。 这不仅是出于兼容性考虑，也是出于安全考虑。 因此，我们推荐使用 iOS 12 或更高版本和 Android 9 或更高版本。*

支持的 LDAP 目录

- 微软活动目录
- 打开 LDAP

有关 "支持的设备操作系统 "和 "支持的 LDAP 目录 "的最新信息，请点击此处：

https://www.apptec360.com/products/systemrequirements/

苹果设备的 “监管模式 “解析

监管模式是 iOS 设备的扩展界面。

在分别配置的设备上，还可以应用与最终用户设备功能相关的其他限制。 这些内容也包含在管理手册中，并用横幅标出。

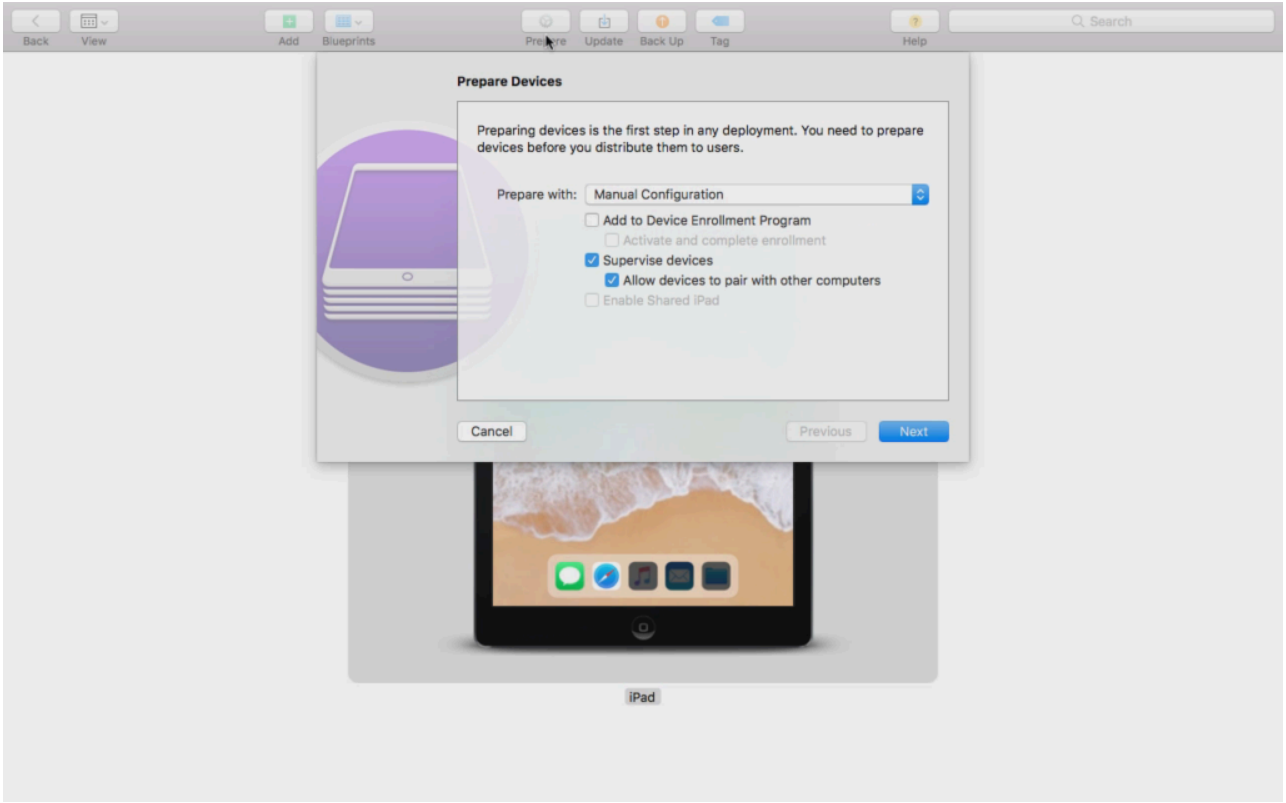
在监控模式下可用

监控模式 "可通过 "Apple 配置器 "程序激活。 作为一种配置工具（通过 USB 接口），Apple Configurator 可以设置新 iOS 设备的默认设置。

该工具不仅可以安装配置文件，还可以安装应用程序。 它是免费的，但需要一台 Mac 电脑。

激活监控模式

1. 打开苹果配置器



2. 点击设备并选择 "准备
3. 选择 "手动配置 "和 "监控设备"。
4. 点击 "下一步
5. 可选 现在可以添加一个 MDM 服务器，设备将在此注册。 相关链接可在 "常规设置 - iOS 配置 - 配置器和 URL "中找到 选择您的组织或创建一个新组织
6. 选择您的组织或创建一个新组织
7. 选择初始设置中应跳过的步骤，然后点击 "下一步"（注意：继续将删除您的设备！）。

现在设备将进入监管模式。 这可能需要几分钟时间。 完成后，设备将重新启动。

现在，您的设备已受到监控！

向 DEP 添加设备

如果你的设备使用的是 iOS 11 或更高版本，你还可以使用 Apple 配置器将设备添加到 DEP（设备注册程序）中。

有关 DEP 的更多信息： https://www.apple.com/business/dep/

按照监管设备的相同步骤操作，并勾选 "添加到设备注册程序"。如果您从未使用 Apple 配置器登录过 DEP，系统会要求您提供 DEP 登录数据。

过程完成后，设备将出现在 DEP 服务器 "Apple Configurator 2 添加的设备 "中。现在，您可以使用该服务器并将其连接到管理控制台，或将设备转移到已有的服务器上。

现在您已成功将设备添加到 DEP！

安卓企业解释

什么是安卓企业版?

安卓企业版可以更好地控制使用 MDM 管理的工作设备。这样，管理员既可以完全控制安卓设备，也可以将公司数据与容器设备上的私人数据分开。此外，Android Enterprise 还能更轻松地注册设备和分发应用程序。

使用 Android Enterprise 有哪些要求?

每个人都可以免费使用安卓企业版。只需将谷歌账户连接到 MDM，即可启用所有安卓企业版功能。有关这方面的更多信息，请参阅 "安卓企业版 "部分。

安卓企业版可在安卓 5.1 或更高版本的设备上使用，但 "增强工作配置文件"（见下文）除外。我们建议至少使用安卓 7 或更高版本，以方便注册；或使用安卓 11，以使用所有可用功能。

安卓企业版有哪些可用模式?

使用安卓企业版时，有 3 种不同的模式可供选择。

AE 全面管理设备（工作管理）：只用于工作的完全托管设备。这允许管理员完全控制设备。这不允许私人使用设备。要在此模式下注册设备，必须重置设备并使用 QR 码注册（请参阅AE 注册）或通过 Knox 注册或 Zero Touch 注册。

AE BYOD 容器：BYOD（自带设备）容器允许用户在单独的容器中通过私人手机访问公司数据。在这种模式下，私人应用程序无法查看公司数据和应用程序，反之亦然。要在此模式下注册设备，必须下载 AppTec 应用程序并扫描 QR 码。在控制台中创建设备，并选择 "AE Container (BYOD & Enahnced Work Profile) "作为设备类型。点击新生成设备上的二维码获取二维码，并将第一个开关设置为 "传统和 BYOD"。

AE 增强工作配置文件：（需要 Android 11 或更高版本）上面提到的 BYOD 容器可将公司数据导入私人设备，而增强工作配置文件也可将公司数据导入公司所有的设备。它创建了相同的容器，但赋予管理员对设备更多的控制权，因此用户不能简单地从设备上删除 MDM。在控制台中创建设备，选择 "AE 容器（BYOD 和 Enahnced Work Profile）"作为设备类型。点击新生成设备上的二维码获取二维码，并将第一个开关设置为 "增强工作配置文件"。按照AE 注册中方法 1 的说明，重置设备并在屏幕上点击 6 次后，即可扫描此二维码。

如何为 Android 企业设备分配应用程序?

首先，您必须在常规设置 → 应用程序管理 → AE Play Store → Play Store 应用程序中批准要使用的应用程序。批准应用程序后，您可以通过点击 "+"并从 "AE Play Store "选项卡中选择应用程序，将其分配

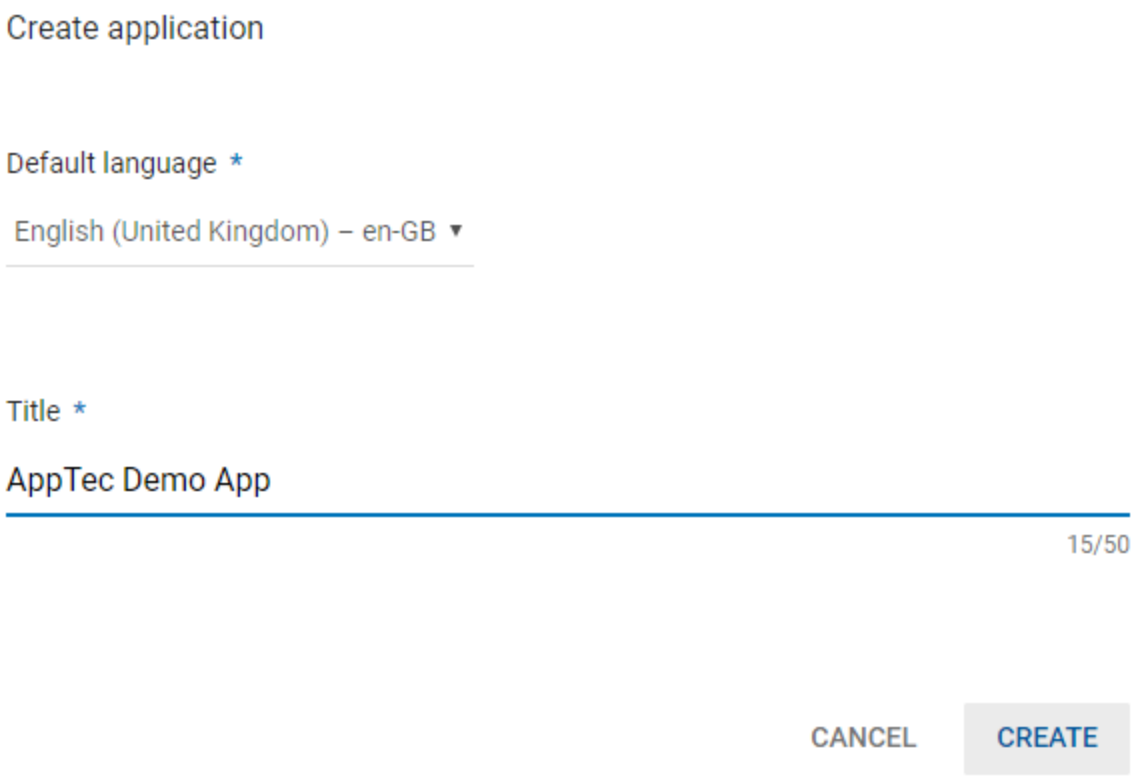
到您个人档案的必选应用程序列表 → 中。这将自动下载并安装应用程序。设备上无需谷歌账户，用户也无需确认或允许。

将自己的应用程序上传到 Google Play 商店

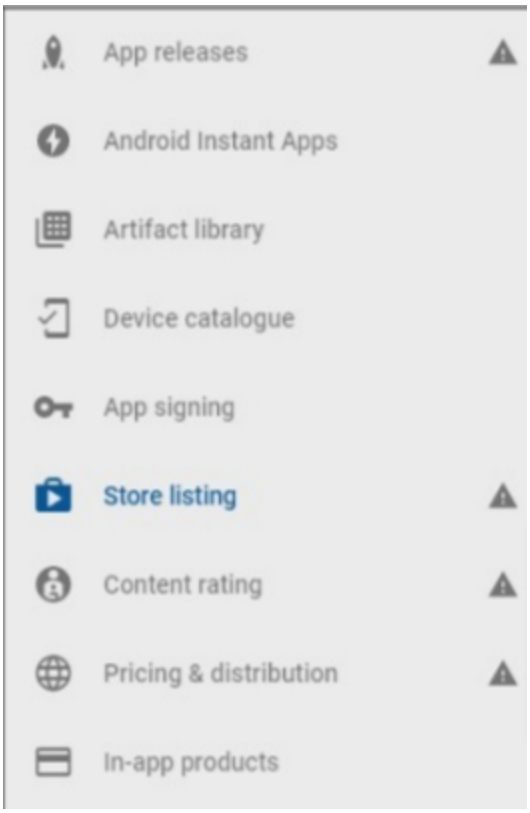
您可以将内部应用程序上传到 Google Play 商店。这样，您就可以从 Play Store 的更新机制等不同优势中获益。

为此，您需要一个 Google Developer 帐户。使用 Google Play 控制台登录 (https://play.google.com/apps/publish)

点击 "创建应用程序"。选择默认语言和应用程序标题。



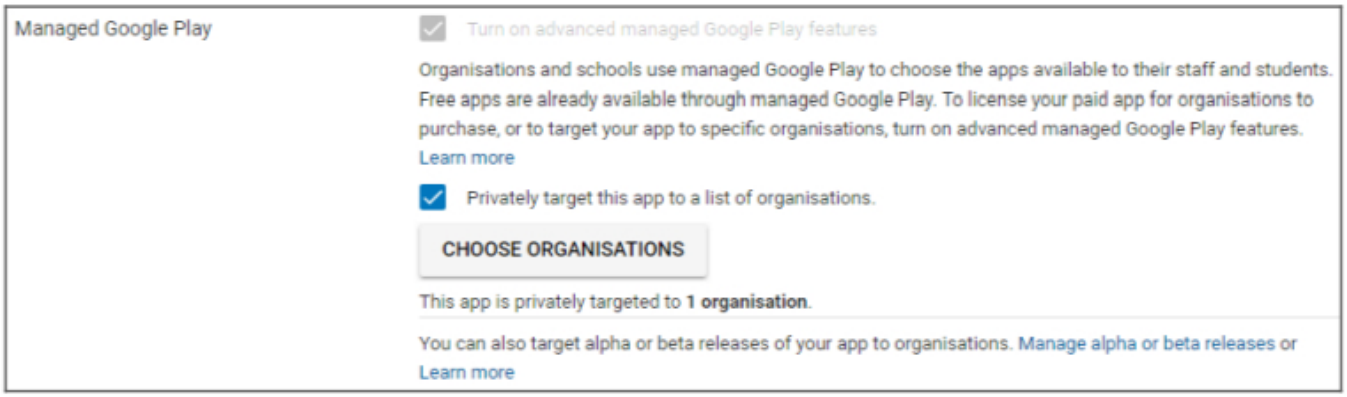
在接下来的页面中，您需要输入有关应用程序的各种详细信息。



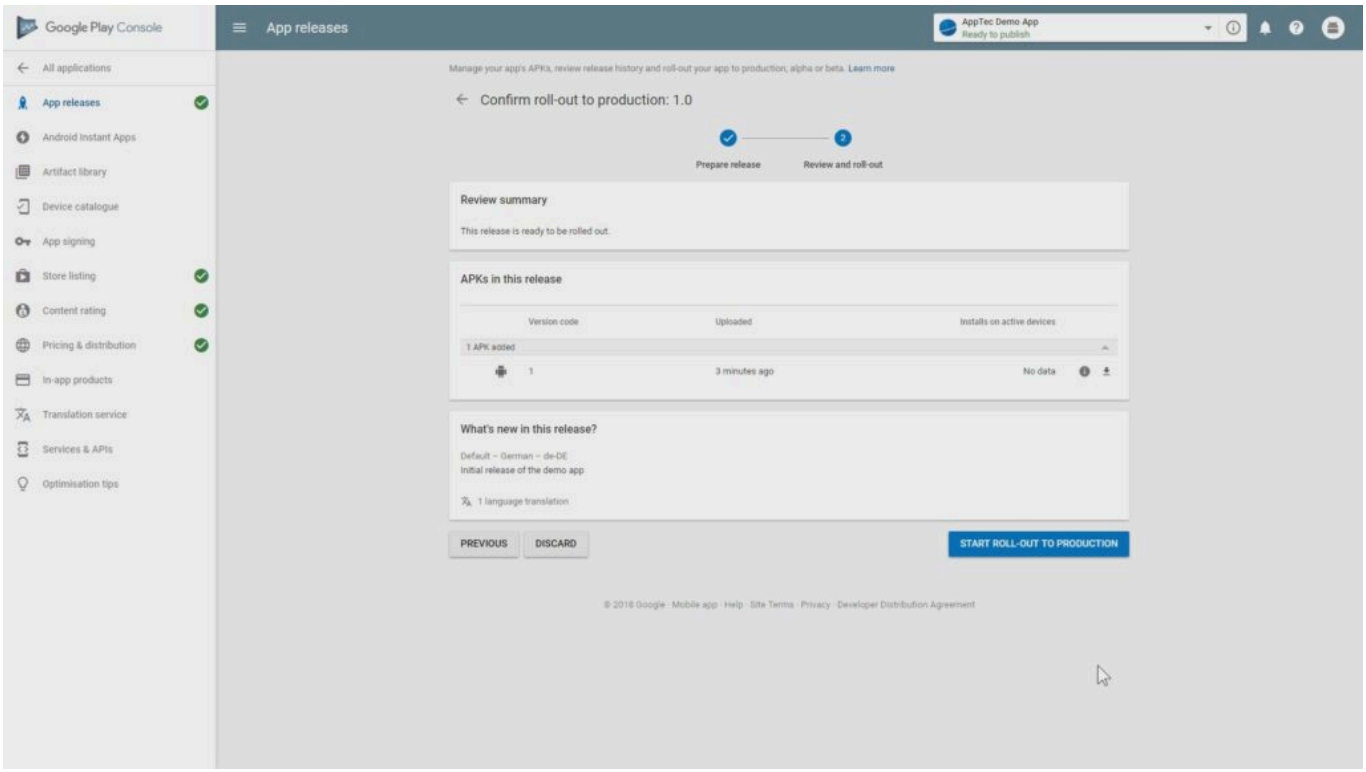
输入所有详细信息后，您会在左侧看到不同的提示符号。

将鼠标悬停在这些步骤上，查看还剩下哪些步骤，然后按照自己喜欢的顺序进行操作。

注意：请务必勾选 "定价与分发 "下 "管理 Google Play "的两个复选框。否则，应用程序将被公开，所有人都可以访问。此外，请务必选择发布的国家/地区。



完成每个步骤后，您就可以进入 "应用程序发布"。点击 "审核 "和 "开始推出到生产"，完成草稿并发布应用程序。



应用程序在 Play Store 上架需要一些时间。程序完成后，您可以在 Play for Work 商店搜索您的应用程序并批准它。之后，您就可以使用 EMM 控制台将应用程序分配给设备，就像使用其他应用程序一样。

要求和安装

要求

系统要求

虚拟设备有开放虚拟化格式（VMWare、VirtualBox、Citrix Xen Server）和压缩 .vhdx (Hyper-V) 文件*。

*注意：使用 Hyper-V 时，必须使用第 1 代创建机器。

虚拟磁盘的目标大小为 20GB，机器需要 4GB 内存。

设备基于 Debian 9 64 位操作系统

将导入的机器升级到最新的兼容性（如在 VMWare 中），并确保在管理程序中正确设置了机器操作系统类型。

许可证密钥

为了成功激活和安装服务器，您需要一个有效的许可证文件。您可以直接从 AppTec360 和/或各自的经销商处获取。

IP 地址和 DNS 解析

设备必须可以通过使用许可证发放的主机名访问 AppTec360 设备。

要注册 Windows 10 设备，还需要以 "enterpriseenrollment. "的形式设置一个指向设备的附加子域。

SSL 证书

由于与设备之间的所有连接都必须使用 SSL 才能确保安全，因此您需要设备信任的证书颁发机构为主机名颁发的有效证书。证书的私钥必须在无密码保护的情况下上传。在大多数情况下，设备需要 CA 的中间证书才能识别服务器证书。

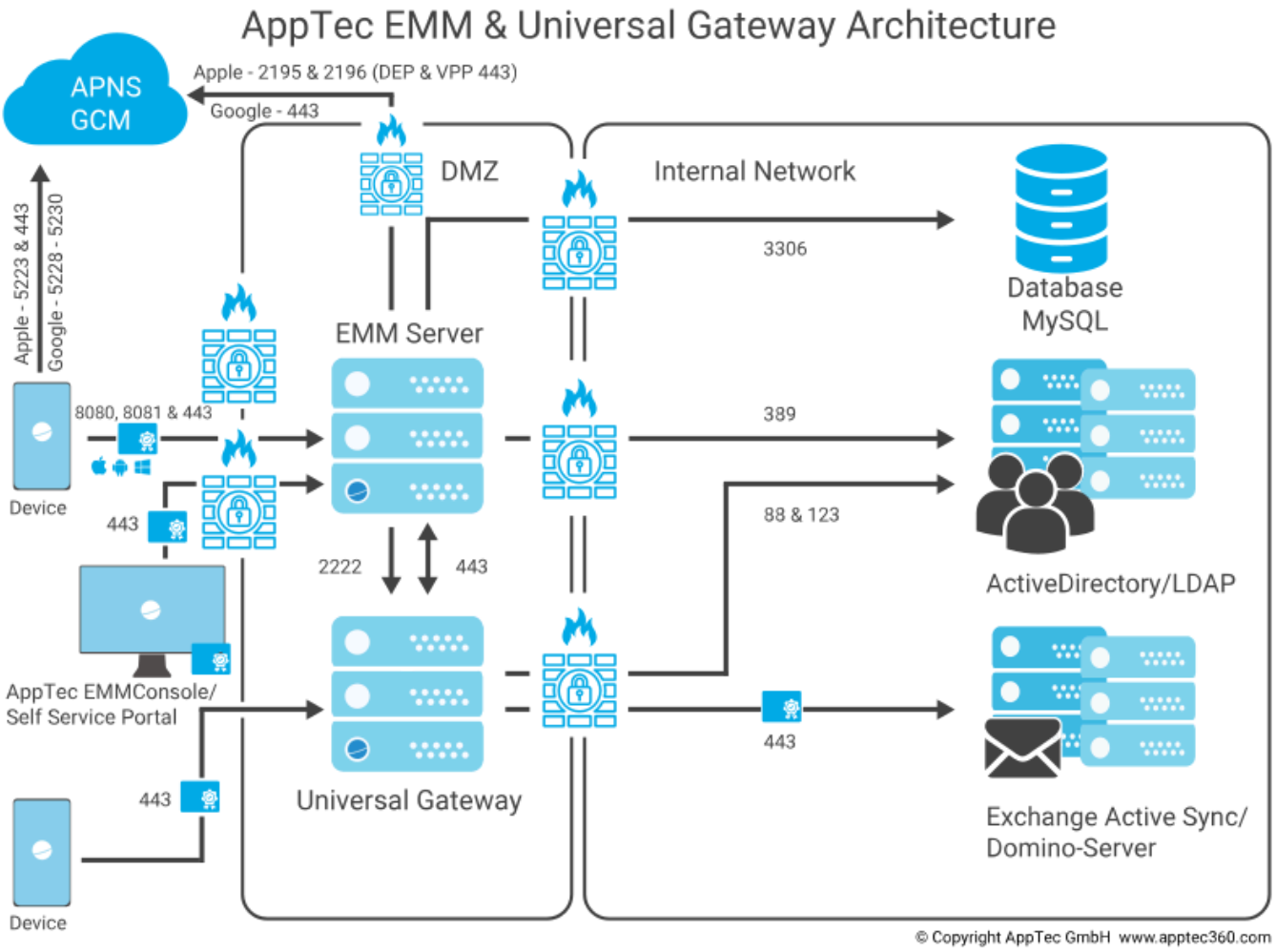
Windows 10 设备需要企业注册子域的特定证书。

从设备版本 202104 开始，您还可以使用自动生成的 Let's Encrypt 证书（在第二步 - SSL 证书中进行了描述）。

SMTP 服务器

需要电子邮件服务器和/或电子邮件中继器，以便 AppTec360 EMM 发送电子邮件（例如用于设备注册和账户验证）。

防火墙规则



该图显示了根据您要使用的服务，需要使用哪种连接。

更详细的说明请参见下一页的表格。

任何（外部/设备）	→	**AppTec360 Appliance / emmconsole.com**
港口	443	管理、企业应用商店和 Windows Phone 通信
	8080	安卓和 iOS 通信
	80	首次设置 Let´s Encrypt。之后使用 443。
任何（设备）	→	**任何（外部）**
港口	5223, 443	苹果推送服务，无需代理即可访问，443 作为回退，请参阅 https://support.apple.com/en-us/HT203609
	5228-5230	Android 推送服务 (FCM)，必须无需代理即可访问
AppTec360 设备	→	**域控制器**
港口	389，（LDAPS 636）	与 LDAP 的用户同步
AppTec360 设备	→	**任何**
港口	443	用于 Android 推送服务 (GCM) AppStore / Play Store 搜索
AppTec360 设备	→	**emmconsole.com**
港口	443	AppTec360 设备更新、APNS 证书生成
AppTec360 设备	→	**苹果网络（17.0.0.0/8）**
港口	2195, 2196	苹果推送服务和反馈服务
	443	DEP 和 VPP

安全更新

Debian 操作系统应定期更新，以获得最新的安全修复。不过，请确保不要手动升级到较新的 Debian 主版本。当 AppTec360 EMM 兼容较新的主要版本时，我们将在设备更新中添加升级方法。

虚拟设备的默认密码

登录用户（禁用 Root 登录。 使用 "sudo "执行管理任务）

apptec

登录密码

apptec

MySQL 根用户

根基

MySQL 根密码

apptec

MySQL 默认用户

AppTec

MySQL 默认用户密码

AppTec

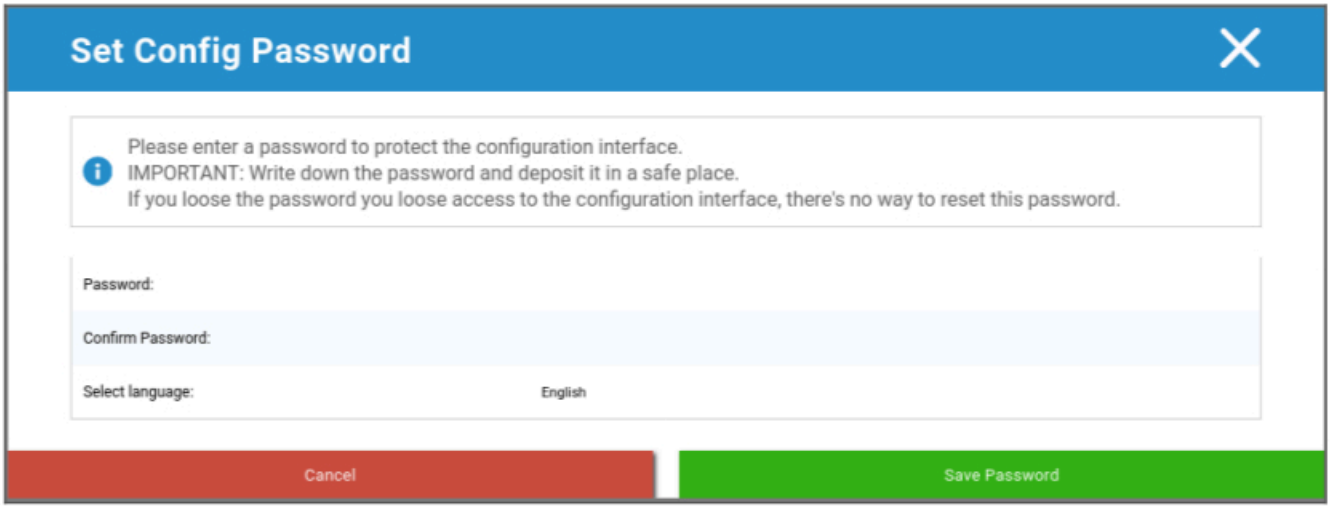
虚拟设备的配置

重要：在开始配置虚拟设备之前，显示器分辨率至少应设置为 1280 x 800 像素。

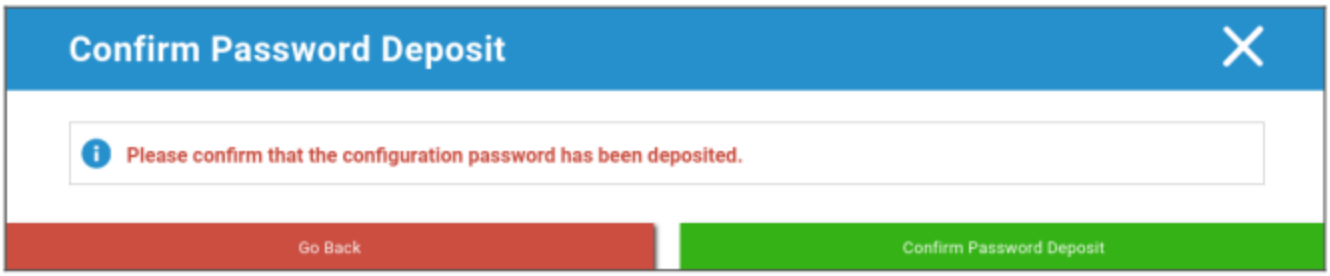
登录设备后，Firefox 会自动启动并显示配置界面。

准备工作

首先，您需要为配置界面提供一个密码。该密码用于加密在配置界面输入的所有信息和文件。您还可以在此设置界面显示语言（可稍后更改）。

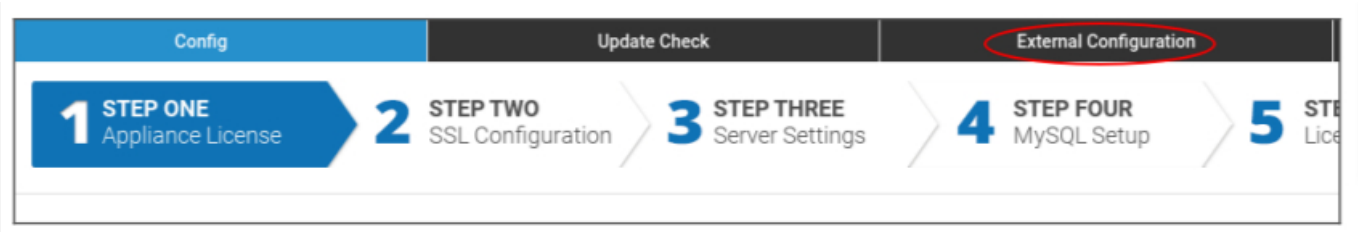


密码只能由 AppTec360 支持人员重置，因此请确保将密码存放在安全的地方，并确认即将弹出的提示。



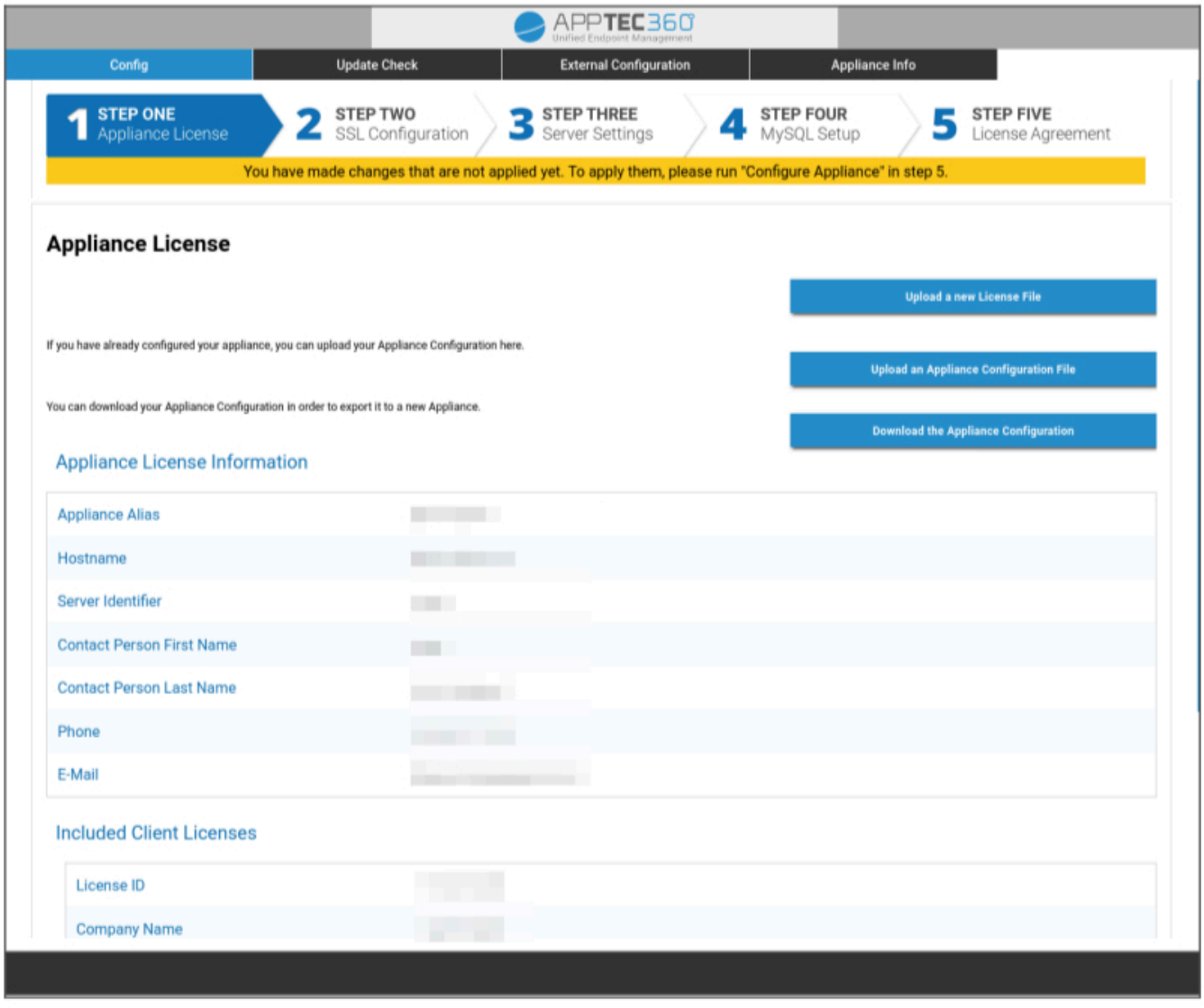
从外部主机进行配置

为了简化设置过程，可以从远程访问配置页面。为此，请按照 "从外部主机配置 "中的步骤操作。



第一步 – 设备许可证

1. 请上传从 AppTec 收到的许可证文件。
2. 如果许可证文件上传成功，则可以看到设备许可证信息，如下图所示。



第二步 – SSL 证书

你可以使用 Let's Encrypt 自动设置证书，也可以自己提供证书（更多信息请参阅 SSL-Certificate）。

自动

证书将使用Let's Encrypt 服务自动生成。

AppTec360 EMM 使用HTTP-01 挑战来验证域，这意味着首次请求证书时，HTTP 端口必须从互联网打开。随后的更新请求可通过 HTTPS 验证。

将单选按钮切换到 "自动（Let's Encrypt）"，然后按 "保存值"。在应用步骤五--许可协议中的配置时，将自动申请证书。如有必要，证书将自动续期，如果证书即将过期（这意味着续期可能失败），你将收到一封电子邮件。

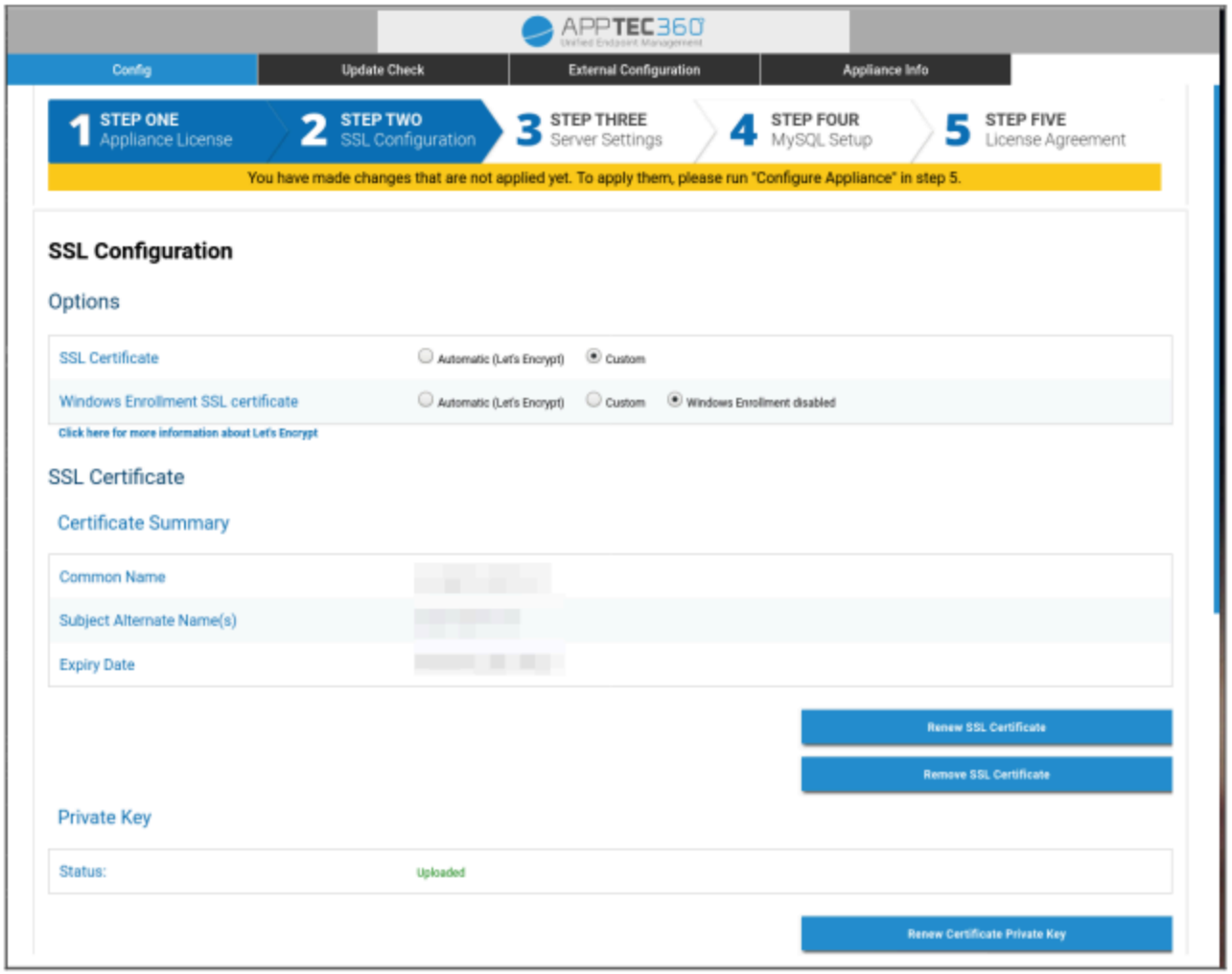
定制

1.上传许可主机名的 SSL 证书。您可以在步骤 1 - 设备许可证中看到主机名。

2.还请上传证书的私钥，必要时上传中间证书。

重要：密钥不得受密码保护。如果有，请在上传前删除密码。

提示：如果还想使用 Windows 10 设备，则必须启用 "Windows 注册 SSL 证书"，并上传子域的证书、私钥和中间证书（参见页面底部的 IP 地址和 DNS 解析）。



第三步 – 服务器设置

1. 请输入全球支持电子邮件地址。该地址将用于向用户发送电子邮件，以便他们在设备出现任何问题时知道与谁联系。
2. 提供系统用于发送电子邮件的电子邮件设置。这些设置将用于向用户发送电子邮件，以及向"support@apptec360.com "发送错误报告和功能请求。保存电子邮件设置后，您需要点击 "测试电子邮件配置 "并按照说明进行验证。

第四步：MySQL 设置

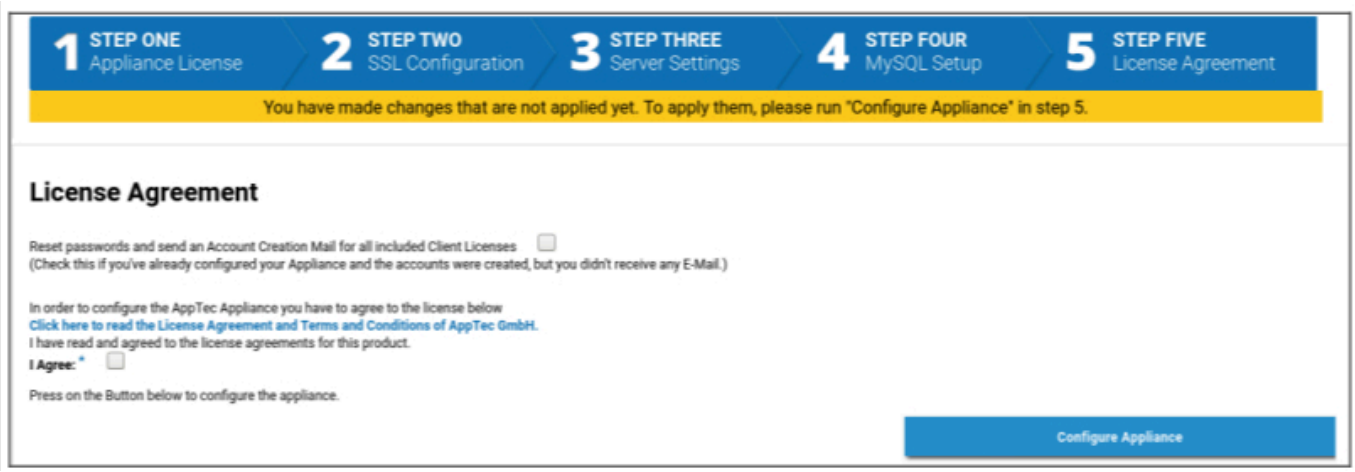
1. 如果想使用内部数据库，可以跳过这一步。否则，您可以输入外部数据库服务器的连接信息。


1 STEP ONE
Appliance License
2 STEP TWO
SSL Configuration
3 STEP THREE
Server Settings
4 STEP FOUR
MySQL Setup
5 STEP FIVE
License Agreement
You have made changes that are not applied yet. To apply them, please run "Configure Appliance" in step 5.
MySQL Setup
The MySQL connection has been successfully tested at April 7, 2021, 8:45 am.
If you change the settings after the initial configuration, you have to reconfigure your appliance by clicking on "Configure now" in step 5.
IP Address or Hostname
127.0.0.1
(Default: 127.0.0.1)
Username
AppTec
(Default: AppTec)
Password
(Default: AppTec)
Port
3306
(Default: 3306)

第五步 – 许可协议

1. 请阅读许可协议。
2. 选中 "我同意 "并按下 "配置设备 "按钮，应用设置。

提示：每次更改 5 个步骤中的设置时，都需要运行 "配置设备 "以应用这些设置。



祝贺你

您已完成虚拟设备的配置。

包含密码的电子邮件将发送到您为许可证提供的地址（在步骤一 - 设备许可证中的 "包含的客户端许可证 "中可见）。

现在，您可以使用该密码和收到密码的电子邮件地址登录控制台。

要登录控制台，请在浏览器地址栏中输入控制台的主机名。

您可以在步骤一 - 设备许可证中找到设备的主机名。

故障排除

1.在步骤五 - 许可协议中配置设备时，您没有收到电子邮件：

确保 "步骤三 - 服务器设置 "中的电子邮件设置正确无误。要重新发送密码，请在再次运行 "配置设备 "之前，检查 "步骤五 - 许可证协议 "中的 "重置密码并为所有包含的客户端许可证发送账户创建邮件"。

2.在步骤五 "许可协议 "的配置过程中，您收到了有关 Let's Encrypt 的错误信息：

确保可通过域名在 80 端口连接到设备。Let's encrypt 还会将日志写入"/var/log/letsencrypt"，这可能有助于进一步排除故障。

安全建议

建议执行以下步骤确保 AppTec360 设备的安全。

这不是一套完整的说明，只是对基本配置的建议。

- 更改 AppTec360 用户密码
- 更改 MySQL 用户 "root "和 "AppTec "的密码，并相应更新步骤四 - MySQL 设置
- 更改 SSH 服务器默认端口
- 在控制台中屏蔽 80 端口，禁止 HTTP 流量，只使用 HTTPS。配置完成后，也可以通过 HTTPS 进行外部配置。
- 在 "步骤三 - 服务器设置 "的底部，限制只有特定 Ips 才能访问管理界面
- 配置防火墙

常规设置

账户概览

账户信息

概述

在这里，您可以看到您的 AppTec360 账户概览。

公司名称	您的公司名称
创建日期	账户创建日期
许可证类型	付费 = 付费许可证 免费 = 无偿许可 注：由于技术原因，预置设备上的账户将始终显示为已付费账户。
客户标识符	您账户的标识符（这不是您的客户编号）
许可证到期日	您的 AppTec360 许可证到期日期
内容盒许可证	免费 = 25 台设备的免费许可证 付费 = x 台设备的付费许可证
发射器	显示是否可以使用 Android 的自定义启动器
设备	当前使用的许可证数量/许可证总数
联系人	提供联系人
电话	提供的电话号码
电子邮件*	提供的电子邮件地址
根用户	可以登录的根用户
软件版本	当前软件版本

**注：此处显示的电子邮件地址是您注册账户时输入的地址。在此基础上，将在用户/设备树中创建一个用户，并可对其进行修改。编辑该用户将更改登录时必须使用的电子邮件地址，但不会更改账户概览中的信息。 .*

错误报告

错误报告可直接发送给支持人员，以报告问题或错误，其中包括有关账户和设置的信息和日志。

主题	错误报告的主题。如果要将此添加到现有的支持票单中，请包含票单编号。
预期行为	详细描述你所做的事情以及你预期会发生的事情
实际行为	详细描述具体发生了什么。请准确引用错误信息。在附件中添加截图也会有所帮助。
您是什么时候遇到这个问题的?	请提供您收到具体错误信息/问题的确切时间。 最好也包括秒数，例如：18:55:27
能否复制该问题？如果可以，如何复制（详细说明）？	详细描述如何重现问题。
该功能之前是否按照您的预期运行？如果是，直到什么时候?	如果不知道，请留空。
在出现此问题之前，是否对系统进行了任何具体更改？如果有，是哪些更改（详细）？	一定要提及在问题出现之前，你最后的改变或行动是什么，即使你认为它无关紧要。
如果适用：哪些设备型号和操作系统版本受到影响?	请务必准确命名操作系统版本（例如 iOS 14.7.1 或 Android 11）
如果适用：设备的公共 IP 地址或/和序列号是什么?	即使所有设备都受到影响，也至少命名一个。
包括日志文件	选中此项可将日志文件与错误报告一起发送。建议这样做。
从 Apple 获取当前 VPP 状态，并将其纳入错误报告	包括有关 VPP 许可证分配的信息。只有当支持人员要求您这样做或您的问题与 VPP 有关时，才能激活此功能。
附件	附加任何有用的文件（如错误信息的屏幕截图）

功能请求

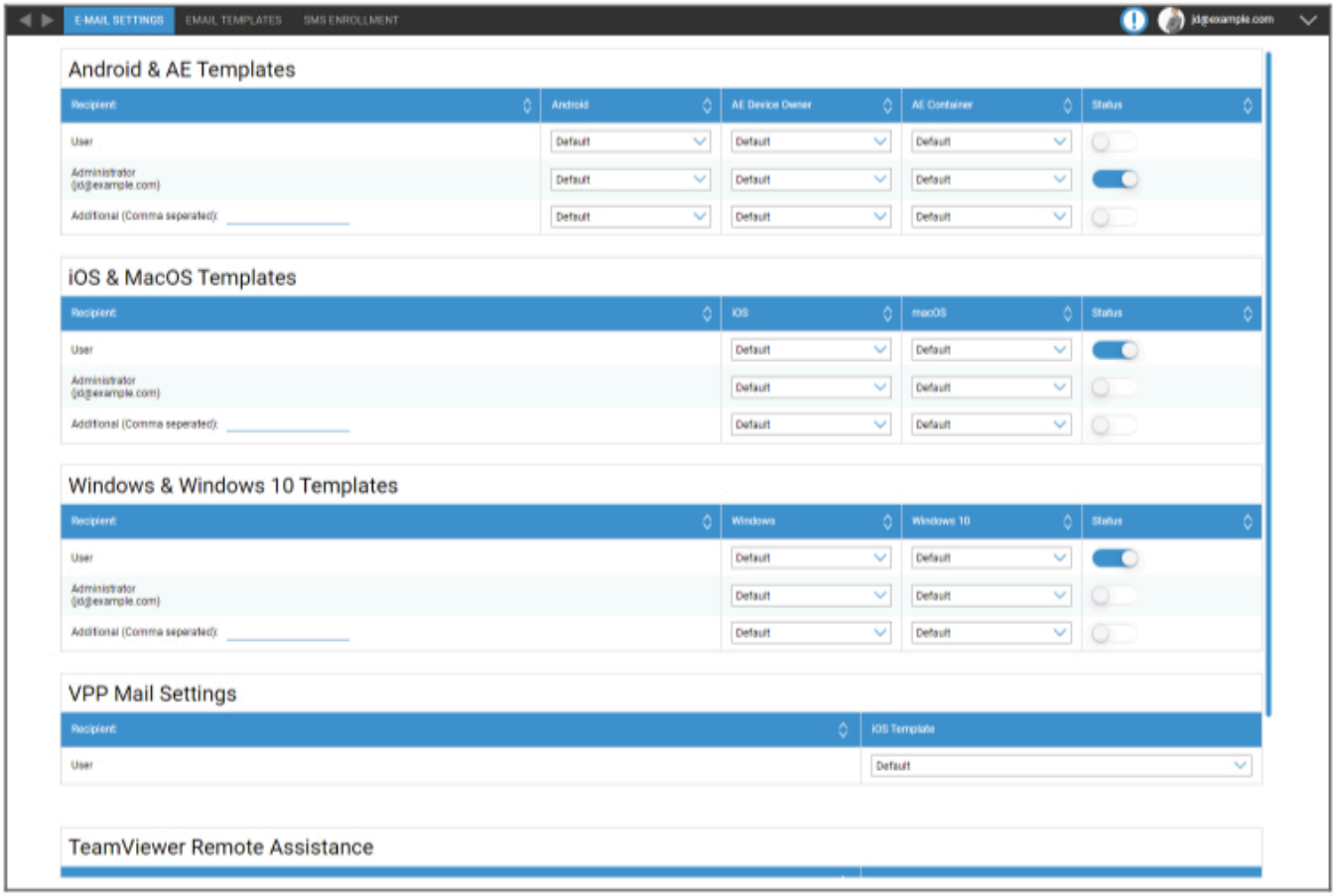
可直接向支持部门发送功能请求。其中可以包含对特定功能的请求，也可以包含对以下功能的改进请求

摘要	问题概述
说明	详细描述您的问题，请尽可能具体
附件	在错误报告中附加文件

全局配置

电子邮件设置

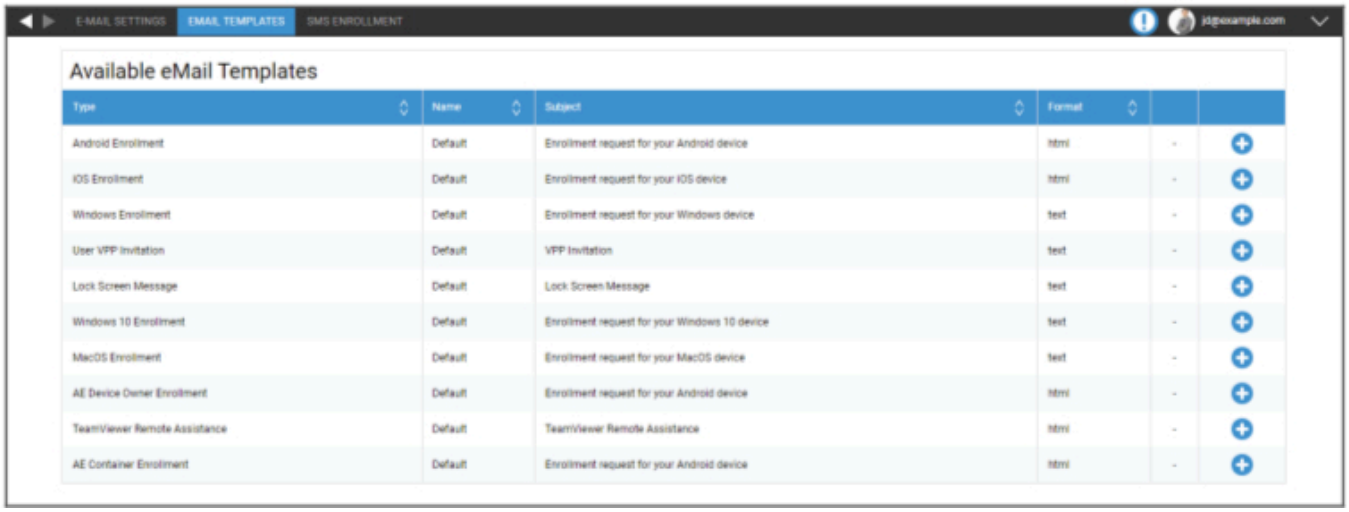
在这里，您可以定义在生成注册申请时谁会收到邮件，以及该邮件使用的文本模板。



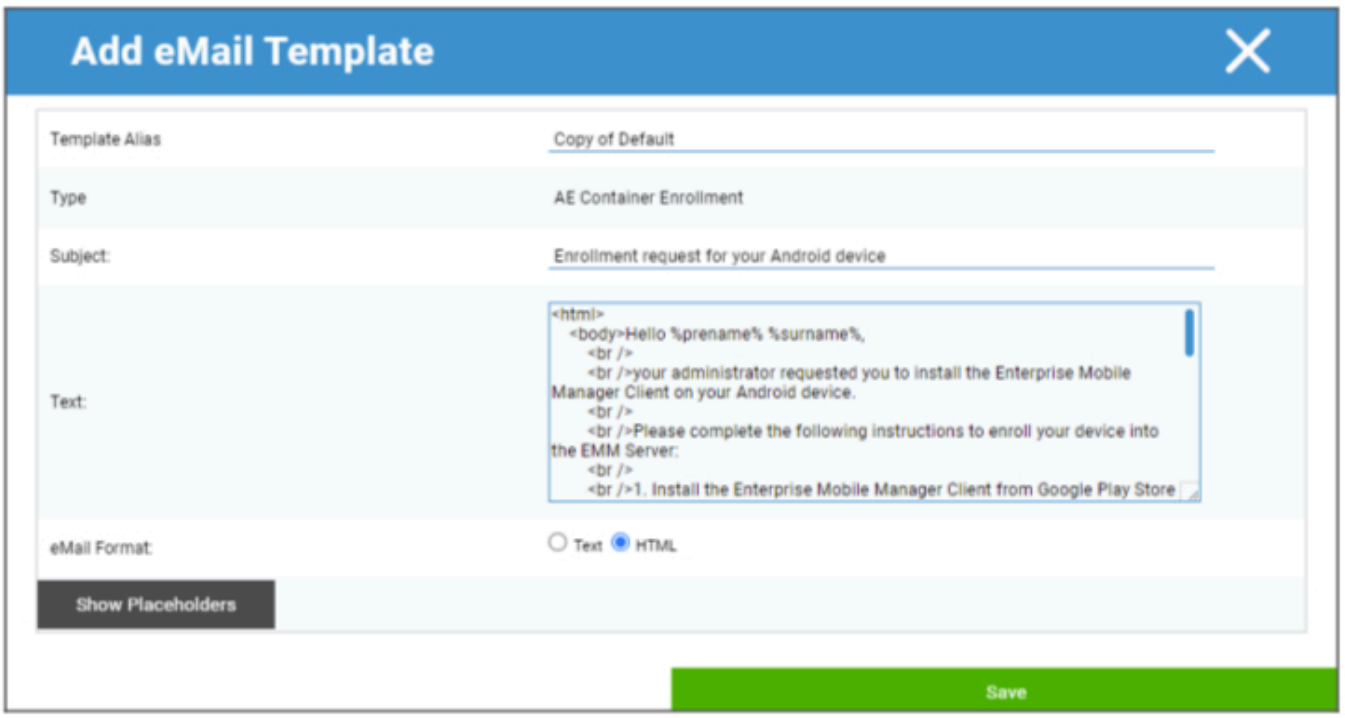
电子邮件模板

在这里，您可以为不同场景生成和编辑模板。这些模板可以是普通文本形式，也可以是 HTML 形式。使用 HTML，您可以更好地控制文本格式。

默认模板不可编辑或删除。



您也可以使用占位符作为变量，它会自动替换。编辑时点击 "显示占位符"，即可看到可用的占位符。不同类别有不同的占位符。



短信注册

您可以在此执行/激活短信注册程序。

(默认：停用)

您还会看到显示屏，显示还有多少短信积分可用。

短信积分需单独购买。

隐私权

GPS 接入

在这里，您可以使用 1 或 2 个密码（四眼原则）保护每个设备的 GPS 视图。每次尝试访问设备的位置时，系统都会提示您输入密码。

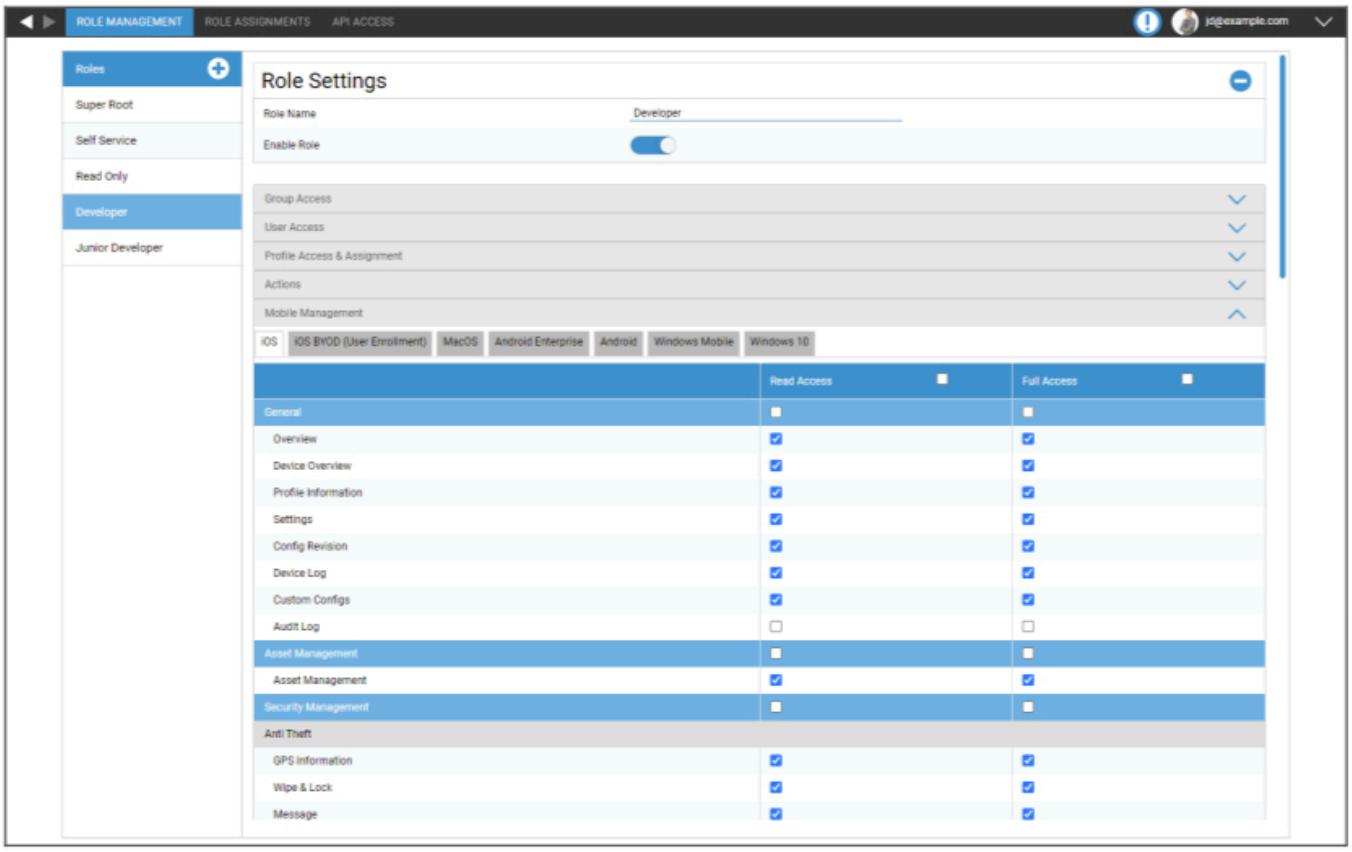
限制访问 GPS 设置	关 = 关闭功能，本地化无需密码
	打开 = 功能已打开，本地化需要密码
保护方法	使用一个密码 = 本地化时使用一个密码
	使用两个密码 = 使用两个密码进行本地化
输入密码 (1)	输入所选密码
重复密码 (1)	重新输入所选密码
可选：输入密码 2	输入第二个密码
可选：重复密码 2	重新输入第二个密码

注意：设置密码后，必须再输入一次才能完全启用。

基于角色的访问

角色管理

角色定义了用户登录管理控制台后可以查看和执行的操作。这样就可以创建可以登录但功能有限的用户。



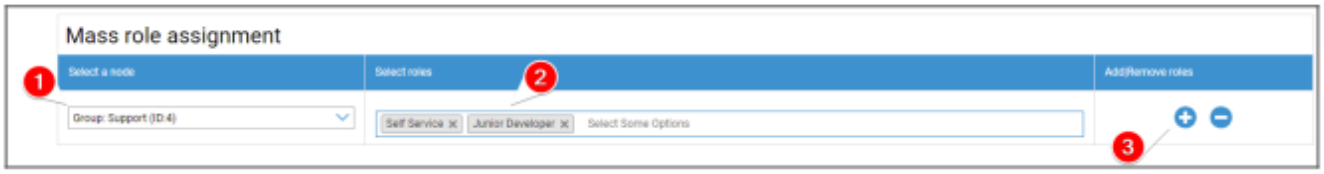
超级根角色是一个默认角色，可以查看和更改所有内容。该角色不可更改或删除。自助服务角色只能查看自己的用户和设备。你可以将自助服务和自定义角色结合起来，例如，允许用户自己登录和注册设备，而且只能为自己的用户登录和注册。

自定义角色可以手动启用或禁用。新角色默认为禁用。禁用角色的用户在工作时就像没有该角色一样。这样就可以暂时限制某个角色的操作。

所有权限都分为 "读取访问 "和 "完全访问 "两种。给予角色 "读取访问 "权限，允许他们查看控制台的特定部分。授予角色 "完全访问 "权限，允许其查看和更改控制面板的特定部分。

角色分配

在这里，您可以概览所有拥有角色的用户，并查看他们拥有的角色。您还可以在这里为用户或整个组分配角色：

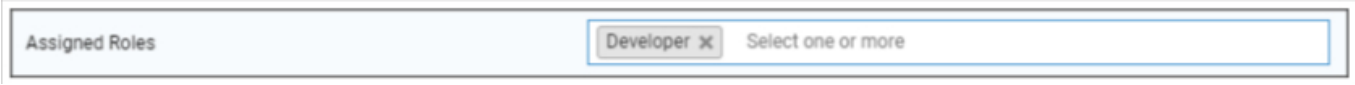


1. 选择要添加或删除角色的组或用户。您可以选择一个用户，也可以选择一个组。选择组时，您的更改将影响该组内的所有用户以及所选组中子组的所有用户。
2. 选择要添加或删除的角色。您可以选择一个或多个角色。
3. . Select what operation you want to perform. Clicking the “+” adds the selected roles if the user(s) did not have them already. Clicking the “-” removes the selected roles from the user(s). If you add roles to a user which did not yet have any role, it will automatically enable “Can Login” for the user.
4. 保存以完成程序。之前没有角色并禁用了 "可以登录 "的用户将自动收到一封带有设置密码链接的邮件。

在 "批量角色分配 "下方，您可以找到已分配角色的概览。您还可以在这里为特定用户手动更改角色。

角色分配

要为用户分配角色，必须进入 "移动管理"，在这里可以找到组、用户和设备树。编辑用户以分配角色。或者，你也可以只对单个用户使用上述方法。



API 访问

访问 AppTec360 REST API

AppTec360 REST API 需要在管理控制台中生成一个身份验证令牌（API 密钥）和一个私人密钥。

为此，请登录 AppTec360 EMM 并转至

常规设置 → 基于角色的访问 → API 访问并添加新密钥。

您必须选择一个用户，其权限将适用于 API 密钥。

私人密钥只能下载一次。下载开始后，密钥将被删除，"下载 "按钮也将消失。

如果您丢失了私人密钥，则必须生成一个新的 API 密钥。

一般规则

- REST API 位于基本 URL 下方：

/public/external/api

- 所有请求都必须通过 POST 发送。
- REST API 仅支持通过 HTTPS 提出的请求。
- 请求必须包含以下标题：

标题名称	标题值	说明
内容类型	应用程序/json	固定的
授权	123...xyz	API 访问 "选项卡中的 API 密钥
签字	Base64 编码签名	生成的有效载荷的签名。 API 访问 "选项卡中的私人密钥

- 请求正文必须是一个 json 编码对象，其中必须包含以下值：

现场	字段示例值	说明
应用程序接口	v2/device/listdevices	应用程序接口名称
时间	1529662725	客户机的 Unix 时间戳（UTC）。 允许的最大时差 客户端和服务器之间的 分钟。

- 成功后，API 会返回所请求的数据（见下面的查询）和 HTTP 状态代码 200。
- 如果出现错误，HTTP 状态代码将根据错误的不同在 4xx 和 5xx 之间变化，响应对象将包含一个以 "errors "为关键字的数组，其中包含一系列人类可读的错误信息。
- 如果没有设备的匹配数据，将返回一个空数组。
- 如果设备 Id 不存在，返回的数据将为空。

申请示例

POST /public/external/api HTTP/1.1
Host: myapptecemm.com
Accept: /
Content-Type: application/jsonauth: 1234567890abcdefghijklmnopqrstuvwxyz
signature: a/bnOV466a0SiyVfsbpspZ+NxiTpmeF18NkfnOIq+OrEZDu9+VW7ESKziPXvw
kTM5B9j/t1WGN1mRcIKe80m8fDKPj+lr3BqoMJe7wGXift+uy6iS7Chpdz2iZA4KPxxU9Z
GU2cdQ/SQceX57pi+ch7ApxBeVX2+lJapTwA6CfB0mJFaf4MPcg/
7LZWkzKxKF7LNzNJHiy/vSpZcqjbXjpC4HWrX6j2uZG5eSP8kYcTR
9VQfGtkX9pcyaNAwguR7zOOwMu/8L0oKq21/19rkabE4ZgUjtKS2+
+q+rh6mrP1g4BCZ7Xq/wvgZkaP
b0CStBdMRvj46i3enxCXcLQQ==
Content-Length: 74
{"api":"v2/device/listposition","time":1529665112,"params":{"ids": [10]}}

查询

列出所有设备

功能：返回包含设备 ID、IMEI 和序列号的所有设备列表
API URI：v2/device/listdevices
必选参数：无
可选参数：无

请求正文示例

{
"api": "v2/device/listdevices",
"time": 1529662725
}

响应正文示例

{
"errors": [],
"list":[
{ "id":"10","serial":"987612345","imei":"899938455454"},
{ "id":"11","serial":"619723118","imei":"713032378599"}
]
}

获取 (GPS) 位置列表

功能：返回设备 ID 的所有存储位置日志条目列表
API URI：v2/device/listposition
必选参数："ids" - 设备 ID 数组
可选参数：无

请求正文示例

{
"api": "device/listposition",
"params": {
"ids": [10, 11]
},
"time": 1529662725
}

响应正文示例

{
"errors": [],
"list":[
"10":[
{"time":"1529632725","pos":"47.5572,7.5967"},
{"time":"1529642725","pos":"47.5572,7.5968"},
{"time":"1529652725","pos":"47.5573,7.5969"},
],
"88":[],
]
}

获取资产地图

功能：
返回使用 "获取任何资产数据 "请求的所有已存储可能资产的列表。
您可以使用人可读表单或资产标签来请求数据。
API URI：v2/device/getassetmap
必选参数：无
可选参数：无

请求正文示例

{
"api": "v2/device/getassetmap",
"time": 1529662725
}

响应正文示例

为便于阅读，本答复被缩短。

{
"AssetKeys": {
"UDID": "AT001",
"Device Alias": "AT002",
"OS Version WinMobile iOS MacOS": "AT003",
"Model Name": "AT004",
"Serial Number": "AT005",
"Total Storage": "AT006",
"Free Storage": "AT007",
"IMEI": "AT008",
…
"apptecID": "APPTECID"
},
"errors": []
}

获取任何资产数据

功能：返回设备 ID 请求的资产数据列表
API URI: v2/device/getassetdata
必选参数："ids" - 设备 ID 数组
可选参数：
"assetkeys" - 要返回的资产数据键。如果未指定，
。您可以使用 Get asset map 获取资产键列表。

请求正文示例


```
{
"api": "v2/device/getassetdata",
"time": 1529662725,
"params": {
"ids": [
26
],
"assetkeys": [
"imei"
]
}
}
```


响应正文示例


```
{
"result": {
"26": {
"imei": "349157642516427”
}
},
"errors": []
}
```

Python3 示例代码

```
! /usr/bin/python
import base64
from Crypto.Hash import SHA512
from Crypto.Signature import PKCS1_v1_5
from Crypto.PublicKey import RSA
import os
import time
import json
import urllib.request
import urllib.parse
import urllib.error
import http.client
applianceDomain = "YOURAPPLIANCE.COM"
apiURL = "https://"+applianceDomain+"/public/external/api"
privateKeyPath = "/path/to/PrivateKey-XXXXXXXXXXX.pem"
apptecAPIAuthToken = "7eXXXXXXXXXXXXXXXXXXXXXXXXXXX20"
currentTimestamp = int(time.time())
# Get Devices
#requestData = {"api": "v2/device/listdevices", "time": currentTimestamp}
# Get Positions
#requestData = {"api": "v2/device/listposition", "time": currentTimestamp,
"params":{"ids":[26]}}
# Get AssetData
requestData = {"api": "v2/device/getassetdata", "time": currentTimestamp,
"params":{"ids":[26], "assetkeys": ["imei"]}}
# encode the request data to json
print(json.dumps(requestData, indent=1))
jsonEncodedRequestData = json.dumps(requestData)
# Sign the request data json with the API private key
message = jsonEncodedRequestData.encode('utf-8')
print("Body:", message)
digest = SHA512.new()
digest.update(message)
```

```
# Read private key from file
with open(privateKeyPath, "r") as myKeyFile:
private_key = RSA.importKey(myKeyFile.read())
```

```
# Load private key and sign message
signer = PKCS1_v1_5.new(private_key)
signatureOfRequestData = signer.sign(digest)
Base64EncodedSignature = base64.b64encode(
signatureOfRequestData).decode("utf-8")

headers = {"Content-type": "application/json",
"auth": apptecAPIAuthToken, "signature": Base64EncodedSignature}
print("Headers:", headers, "\n")

# Send request to Server
httpsClient = http.client.HTTPSConnection(applianceDomain, 443, timeout=10)
httpsClient.request("POST", apiURL, jsonEncodedRequestData, headers)

# Get answer
response = httpsClient.getresponse()
status = response.status
data = response.read()

if data == False:
print("Invalid answer from the server")
else:
print("Answer:")
print(json.dumps(json.loads(data), indent=1))
if status != 200:
print("http error: lastReceivedHttpCode")
print(status)
```

苹果配置

APNS 证书

您可以在此上传 APNS 证书。管理 iOS 和 MacOS 设备需要此证书。

注意：APNS 证书的有效期只有一年。过期前必须更新。续期过程与创建过程相同（见下文），只需短短几分钟。

如果您忘记及时更新，则无法更改已注册的设备 **您必须重新注册所有设备。** .

步骤 1

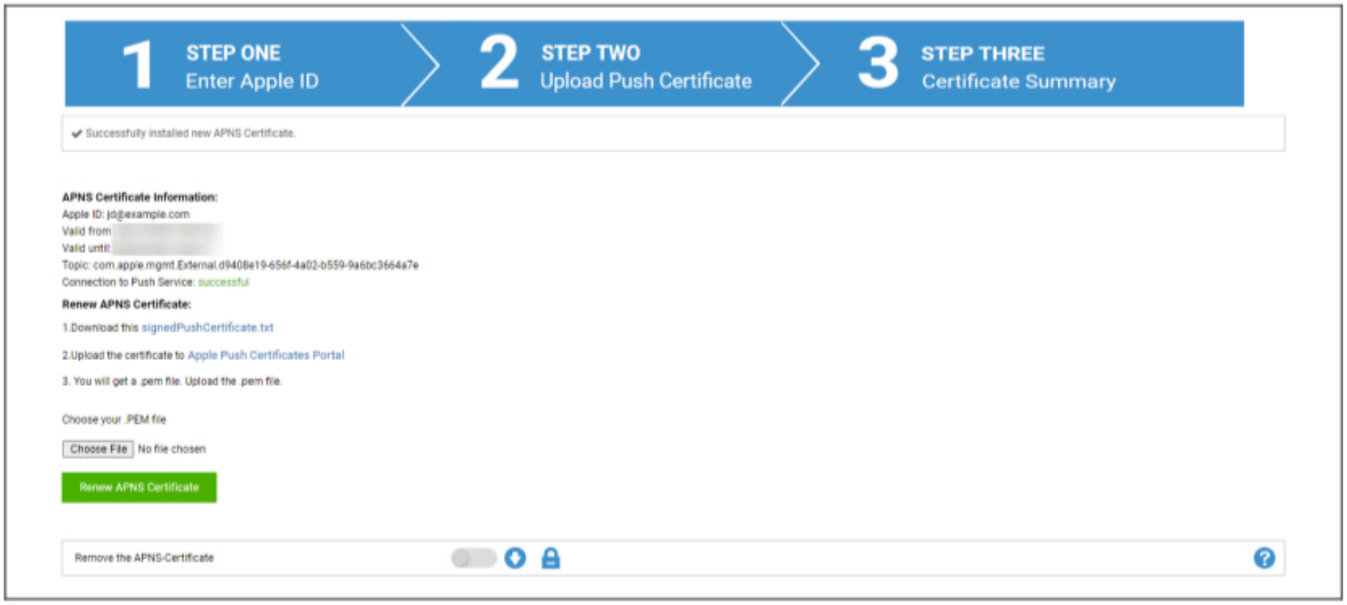
- 首先，输入要用来创建 APNS 证书的 Apple ID。

注意： 此 Apple ID 仅用于创建 APNS 证书。此 Apple ID 与设备无关，设备也不会知道此 Apple ID。此外，您还需要访问此 Apple ID 才能更新 APNS 证书。因此，建议使用一些通用的 Apple ID 并记录登录数据。在 APNS 证书过期前，会向 Apple ID 使用的邮件地址发送提醒。

- 点击 "下一步 "继续。
- (可选）如果您不小心删除了先前删除的 APNS 证书，您还可以恢复它

步骤 2

- 下载 signedPushCertificate.txt
- 访问https://identity.apple.com/pushcert/并使用步骤 1 中的 Apple ID 登录
- 点击 "创建证书
- (可选）输入备注。如果您管理多个租户，这将有助于轻松识别他们。
- 点击 "选择文件"，选择之前下载的 signedPushCertificate.txt 文件
- 点击 "上传"。
- 现在您将看到创建 APNS 证书的确认信息。
- 点击 "下载 "并保存。
- 返回管理控制台。
- 点击 "选择文件"，选择要上传的 APNS 证书。
- 点击 "上传



步骤 3

现在您已成功设置了 APNS 证书，可以管理 iOS 和 MacOS 设备了。

在步骤 3 中，您将看到当前使用的 APNS 证书概览。

此外，您还可以按照屏幕上显示的步骤更新 APNS 证书。请注意在过期前进行续订。

更新 APNS 证书时，请记住使用步骤 3 中显示的 Apple ID 登录，同时更新以前使用过的证书，而不是创建新的证书。在步骤 3 和点击 Apple Push Certificate Portal 中的 "i "时，您将看到 APNS 证书的 "主题"。这是识别证书的唯一 ID。这将帮助您识别正确的证书并更新正确的证书。

当您在更新时收到 "错误：错误：推送的证书有不同的主题！"时，这意味着您已经更新了另一个证书或创建了一个新证书。

如果要上传新证书，例如无法再访问以前使用过的 Apple ID，则必须先删除当前上传的证书。

无论如何，删除 APNS 证书意味着您无法再对当前注册的设备进行更改，直到您再次注册它们。因此，请务必为此做好准备，只有在别无他法的情况下才删除证书。

托管访问

在这里可以启用 iOS 设备的用户注册和 iOS 设备的共享 iPad。

用户注册

用户注册 "可为 BYOD 设备启用特殊模式。

必须在 Apple Business Portal 中为每个用户创建一个受管理的 AppleID。

在注册过程中，用户会被要求提供 Apple-ID 凭据。

由于 "用户注册 "只允许 MDM 配置有限的设置和限制，因此能最大限度地保证用户的安全。

管理域：

用于将用户电子邮件地址映射到其管理的 Apple-ID 的域（格式必须为：'@appleid.company.com'）。例如，john.doe@example.com 将被映射到 john.doe@appleid.company.com。

查看 Apple Business Manager，查看您的托管域

共享 iPad

共享 iPad 是配置了特殊 DEP 配置文件的 DEP 设备。

这样，多个用户就可以使用自己管理的 AppleID 登录设备。

管理的 Apple-ID 必须在 Apple Business Portal 或 Apple School Manager 中创建。

登录共享 iPad 的用户会被要求提供他们管理的 Apple-ID 凭据。

管理域：

用于将用户电子邮件地址映射到其管理的 Apple-ID 的域（格式必须为：'@appleid.company.com'）。例如，john.doe@example.com 将被映射到 john.doe@appleid.company.com。

查看 Apple Business Manager，查看您的托管域

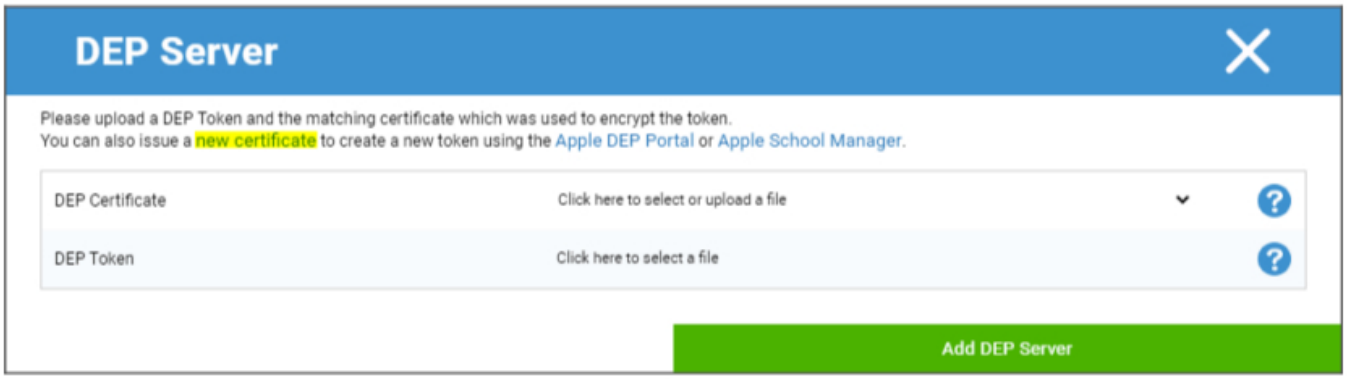
环境保护部

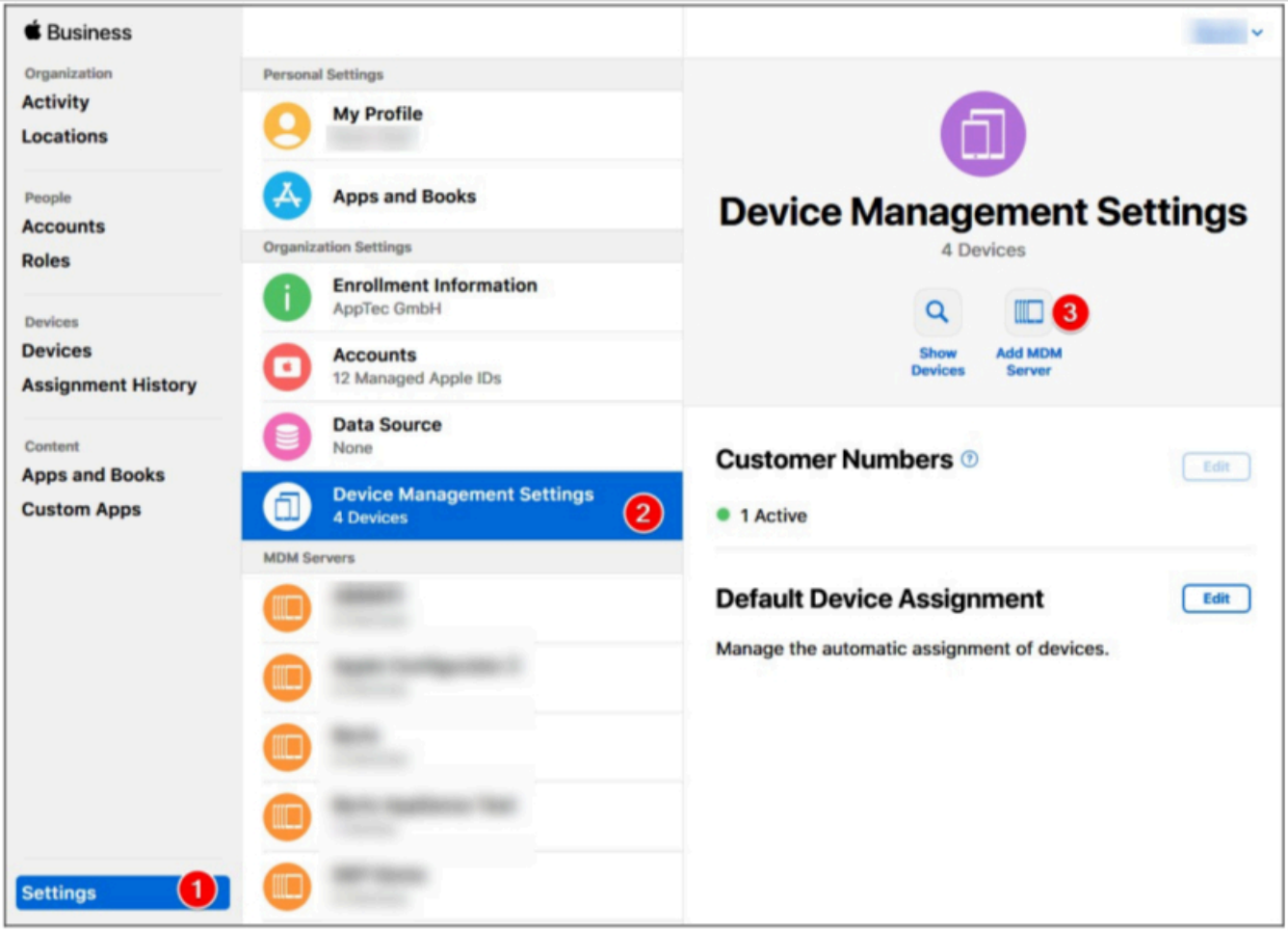
通过 DEP（设备注册程序），您可以轻松地将设备注册到 MDM。使用 DEP 时，设备将在设置时自动连接到 MDM。您还可以跳过几乎所有的设置步骤，而这些步骤在 iOS 上通常都是强制性的。

请记住，您需要从支持 DEP 的经销商处购买设备。有关详细信息，请联系您的经销商或 Apple。

有关 DEP 的更多信息： https://www.apple.com/business/dep/

点击 "+"添加 DEP 令牌。在弹出窗口中，点击文本中的 "新证书"（下图中标为黄色）。这将生成并下载 DEP 证书。然后访问 Apple Business Manager(https://business.apple.com/) 或 Apple School Manager(https://school.apple.com/)。

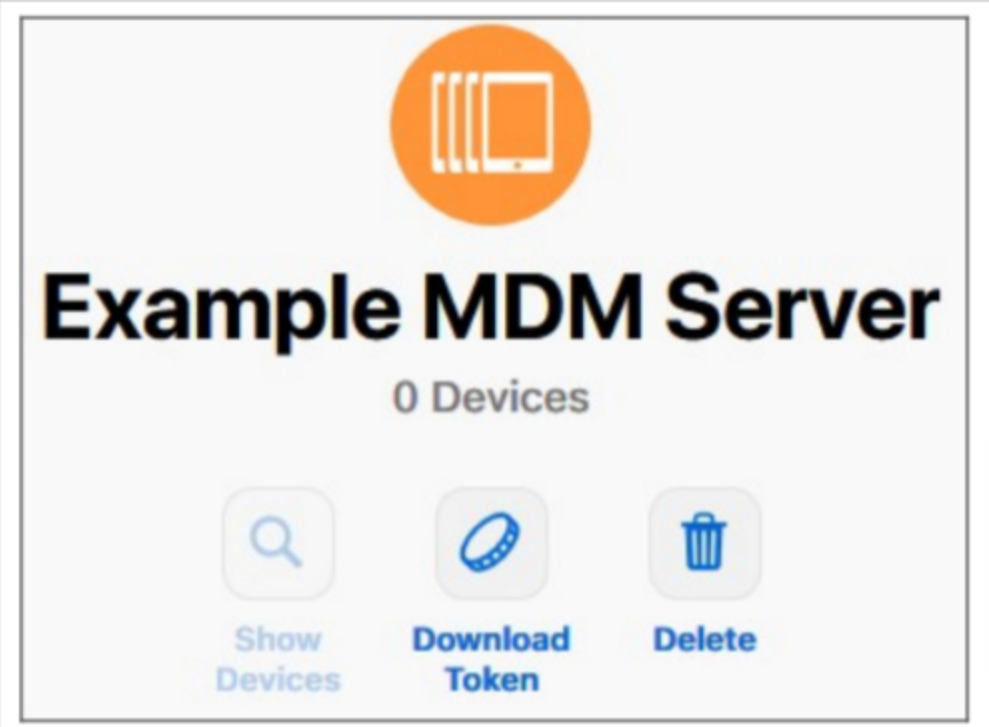




在 Apple Business Manager 中，按照上图所示步骤操作。设置 → 设备管理设置 → 添加 MDM 服务器。

在 MDM 服务器设置 → 上传公钥下上传之前下载的 DEP 证书，然后点击 "保存"。

现在您将看到 "下载令牌 "选项。点击并保存。令牌的有效期只有一年。但只要再次点击 "下载令牌"，就会获得一个新的令牌，这样令牌的续期就非常容易了。



现在您可以回到先前下载 DEP 证书的 MDM。如果您没有关闭标签页，添加 DEP 服务器的弹出窗口应该仍然打开，并且 DEP 证书应该已经选中。现在可以在 "DEP 令牌 "字段上传令牌，然后点击 DEP 服务器。

在 "**设备**"栏中，您将看到分配给此 DEP 服务器的设备数量。添加到此 DEP 服务器的设备将自动在移动管理中的 DEP 池中创建。

您可以点击该号码，查看所有 DEP 设备及其状态。

注意：根据您在业务管理器中的工作流程或配置，您可能需要手动将这些设备分配给 DEP 服务器。您也可以在 Apple Business Manager 中为新设备设置默认 DEP 服务器。

在 "**预案**"一栏中，您可以看到您拥有的 DEP 预案数量。您还可以点击该数字查看 DEP 预案的详细信息，并在此删除旧的/未使用的预案。目前无法更改这些配置文件。如果要更改，必须创建一个新配置文件。

在 "**上次同步**"栏中，您可以手动同步 DEP 服务器（例如，如果您刚向 DEP 添加了新设备），并查看上次成功同步的日期。

在 "**自动配置文件**"栏中，您可以将 DEP 配置文件设置为自动默认设置。该预案将自动分配给新设备。如果不设置自动预案，则每次都必须手动为新设备分配预案。

在 "**添加配置文件**"栏中，您可以添加新的 DEP 配置文件。设备将在开始设置时收到该配置文件。DEP 配置文件定义了设备的设置方式以及跳过的设置步骤。

注意：设备注册后，这些设置只能通过执行出厂重置和使用新配置文件注册设备来更改。这与 "**可移动**"和 "**允许配对**"尤其相关。如果是 "**允许配对**"，建议将其打开，因为可以通过 MDM 限制将其禁用，但如果在 DEP 配置文件中禁用，则无法再次启用。

在 "**编辑**"栏中，您可以上传新的令牌，例如在更新令牌时。

配置器和 URL

游泳池注册 URL

在这里，您可以创建一个注册 URL 和注册 QR 码，其有效期为设定的注册数量和日期。这样，您只需使用一个链接或 QR 码就可以注册多个设备。

使用此 URL 或 QR 码注册的设备将出现在移动管理中的设备库中，之后您必须手动将其分配给组或用户。

注意：这仅用于手动注册。如果通过 Apple Configurator 注册设备，请勿使用此 URL

MDM 配置文件 – Apple 配置器

您可以在此获得通过 Apple Configurator 注册设备时所需的 URL。使用 Apple Configurator 准备设备时，可以在同一流程中将设备添加到 MDM。为此，Apple Configurator 需要此 URL。

通过 Apple Configurator 添加的设备会出现在 "移动管理 "的 "设备池 "中，之后你必须手动将它们分配给某个组或用户。

你还可以在这里找到一个 .mobileconfig 文件，用于通过 Apple Configurator 注册设备。无论如何，建议使用该 URL。

安卓配置

安卓配置

卸载保护	如果激活了该功能，用户在不输入 MDM 管理员设置的密码的情况下，就无法停用设备管理员。密码是在注册时设置的，因此必须重新注册设备才能更新密码。 删除设备管理员有两种选择： 1. 在设备上手动操作 ○ 打开设备上的 EMM 应用程序 ○ 切换到状态选项卡 ○ 点击 "卸载保护 ○ 输入密码 您可以使用修订版从控制台的 "密码历史记录 "中获取正确密码。 ○ 向下滚动并点击新添加的点，"点击卸载 AppTec360 MDM 应用程序"（您有 20 秒时间执行此任务） ○ 在对话 "卸载 AppTec360 MDM 应用程序 "中确认 "确定"。这将从控制台中取消设备注册。 ○ 要从设备上删除应用程序，请在对话框 "AppTec360 MDM 将被卸载 "中确认 "UNINSTALL"。 2. 自动（控制台） ○ 在控制台中选择设备 ○ 点击蓝色齿轮图标，选择 "企业擦除 注：仅适用于 Android 4.x 及更低版本或配备 KNOX API 的设备（三星设备）
卸载密码（第 x 版）	建立的密码，用户可以用它删除设备管理员 重要的是用户需要哪个密码，因为设备有可能尚未与 AppTec360 服务器通信，因此最新密码尚未传输
密码历史	点击蓝色按钮（"显示历史记录"）后，您可以查看以前设置的密码
扩展卸载保护	该选件可提供针对非安全设备的保护 只要激活此设置，就无法轻松停用设备管理员

提示用户卸载被阻止的应用程序?	如果可能，被阻止的应用程序不仅会被阻止，还会被自动卸载。如果无法自动卸载，则会提示用户卸载被阻止的应用程序。
智能系统应用程序封堵	如果启用白名单，Android MDM 客户端会阻止所有用户安装的应用程序。启用此设置可在白名单模式下阻止所有可启动的系统应用程序。

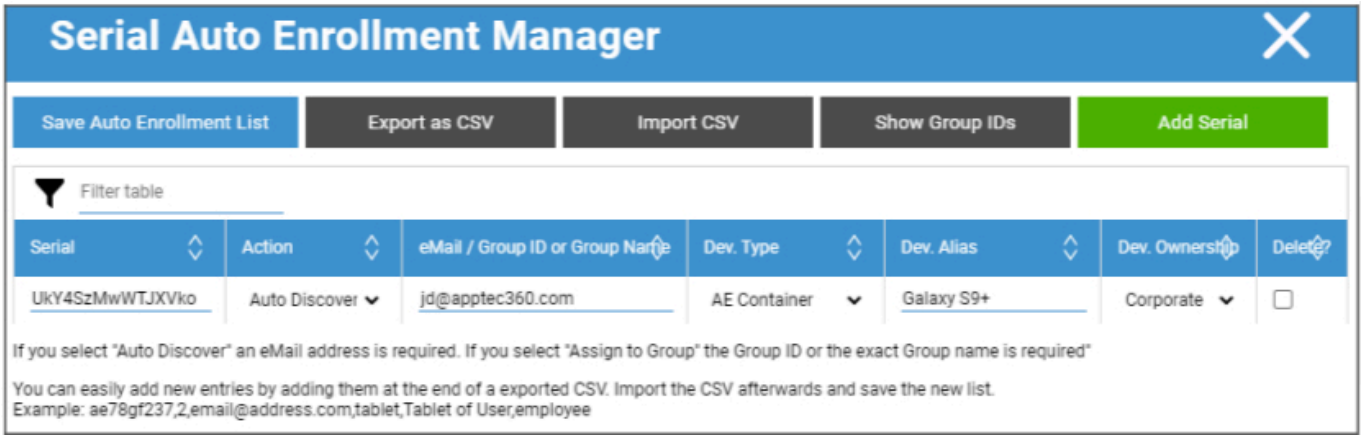
自动注册

您可以在此启用自动注册功能，以便在设备上打开 AppTec360 MDM 客户端时自动注册设备。

重要：此注册方法已被弃用，不再适用于 Android 10 或更高版本。无论如何，在使用 Android 7 或更高版本时，您都应该将设备注册为 Android 企业完全托管。如果您想使用安卓企业版 BYOD 容器，并且使用的是安卓 10 或更高版本，则必须通过凭据、二维码或短信手动注册设备。无论如何，自动注册列表仍可用于自动注册流程，如 AE 注册、Knox 注册等。

无论如何，自动注册列表仍可用于自动注册 AE 注册、Knox 注册等流程。

点击 "序列号管理器 "或 "IMEI 管理器"，即可分别添加设备的序列号或 IMEI。无需同时为设备添加序列号和 IMEI，只需添加一个即可。



操作 定义设备是注册到池、用户还是组。

您还可以导出和导入 .csv 文件，并按关键字过滤条目。

安卓企业

您可以在此设置 Android 企业版。要使用 Android 企业版的所有功能，这一点必不可少。

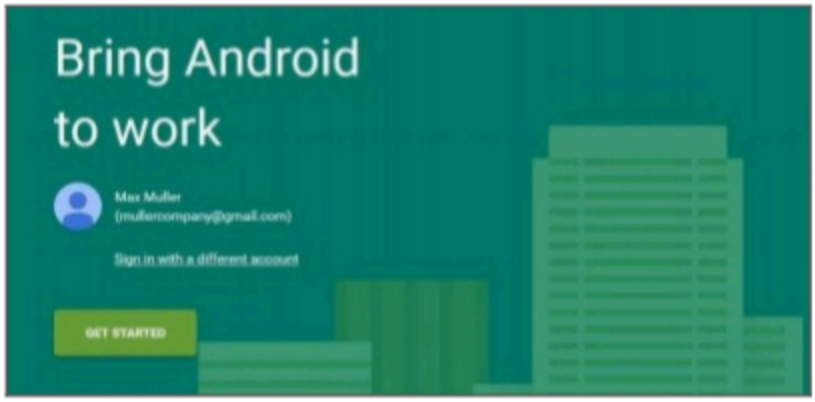
第一种方法：安卓企业账户（谷歌账户）

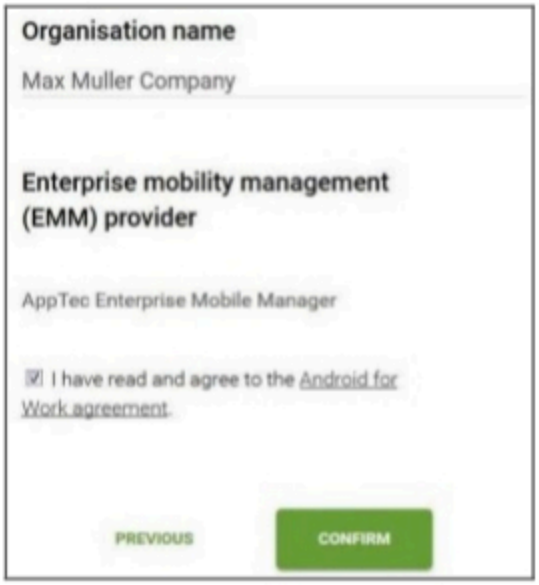
首先按下 "Prepare Setup（准备设置）"，稍等片刻后，就会出现 "Start Setup（开始设置）"按钮。

这将带您进入 Google 的 Android 企业设置页面。

如果尚未登录，请使用您要使用的 Google 账户登录，然后按 "开始"。

现在您可以输入公司名称。输入完成后，选中复选框并按 "确认"。





最后一步，您可以完成注册并返回控制台。如果一切正常，应该是这样的

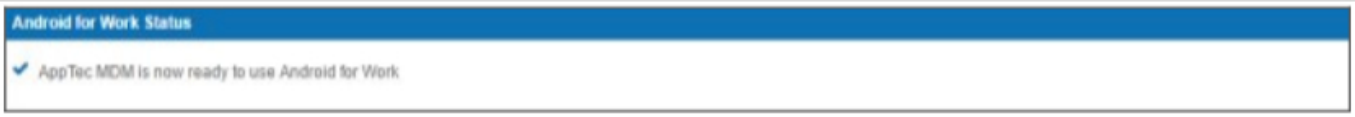
现在，你可以开始配置 Android 企业容器了。

第二种方法：G-Suite 账户

按 "Use G-Suite"（使用 G-Suite）并登录 Google 管理账户。进入 "安全"->"显示更多"->"管理安卓的 EMM 提供商 "并生成令牌。注意：如果你在 G-Suite 账户中没有看到安卓企业设置，你必须进入 "获取更多应用程序和服务 "并添加安卓设备管理。现在在我们的控制台中输入令牌和你的主域，然后点击 "保存更改"。完成后，点击 "使用安卓企业账户"。

现在，您应该可以看到 "创建服务账户 "按钮。点击它。这个过程可能需要一些时间。

如果一切正常，应该是这样的：



现在，你可以开始配置 Android 企业容器了。

出厂重置保护

通过 "出厂重置保护"，您可以将设备绑定到您选择的谷歌账户，这也会覆盖任何现有的谷歌账户绑定。要使用 "出厂重置保护"，您必须先在这里进行设置，然后在您的配置文件中激活它。

要设置 "出厂重置保护"，请单击 "FRP 设置 "并按照屏幕上的说明操作。

注意：仔细阅读并执行步骤。我们建议在新的隐身浏览器窗口中执行此操作，以避免自动登录到错误的谷歌账户。如果输入了错误的 ID 或失去了使用 Google 账户的权限，你可以将自己完全锁定在设备之外！

AE 注册

在此，您可以激活 Android Enterprise Ernollment。使用此方法可将设备注册为Android 企业设备所有者模式。在此模式下，您将拥有对设备的完全控制权。

启用 AE 注册	激活 AE 注册 注意：如果禁用 AE 注册，现有 QR 码和已配置的 NFC 编程器设备将停止工作。如果再次启用 AE 注册，则必须重新发送 NFC 推送配置/生成新的 QR 代码。
启用自动发现	当设备通过 "AE 注册 "进行注册时，系统会尝试根据序列号/IMEI 白名单（"常规设置">"安卓配置">"自动注册"）中设置的信息将其分配给用户。
阻止未知设备	只有在序列号/IMEI 白名单（"常规设置">"Android 配置">"自动注册"）中被列入白名单的设备才能注册。

方法 1 和 2 的注意事项："欢迎屏幕 "是指重置出厂设置后看到的第一个屏幕。根据您使用的安卓版本和/或设备型号的不同，欢迎界面也会有所不同。

方法 1：二维码注册

(需要 Android 7.0 或更高版本）如果您运行的是 Android 7 或更高版本，我们建议您始终使用此方法。

1. 出厂重置设备
2. 使用以下两种方法之一为注册生成 QR 码：
   - 在 "常规设置 -> Android 配置 -> AE 注册 "中点击 "生成 QR 码"。选择是否要跳过存储加密和/或删除所有系统应用程序。
   - (或者）选择一个现有设备。在 "设备概述 "中点击显示的 QR 码。选择是否要跳过存储加密和/或删除所有系统应用程序。
3. 现在在设备的欢迎屏幕上点击 6 次。这将启动 QR 注册模式。
4. 现在连接到无线网络，稍等片刻，直到二维码阅读器安装完毕
5. 现在扫描二维码
6. 就是这样。现在，您的设备已注册为 Android 企业设备模式。
   - a.如果您在 "常规设置 "中使用了 QR 码，则可以在 "池 -> AE 设备所有者设备 "中找到您的设备。(提示：您可能需要重新加载网站才能看到设备)。如果您选中了 "启用自动发现"，您可以在自动发现用户中找到它。
   - 如果您使用的是现有设备配置文件的 QR 码，则设备将注册到此配置文件中。

方法 2：NFC 注册

(需要 NFC 和 Android 6.0 或更高版本)。

准备工作在 "常规设置 -> Android 配置 -> AE 注册 -> NFC 配置数据 "中输入 WiFi 信息。现在使用 "NFC 设备 "搜索将成为编程器的设备。该设备将用于通过 NFC 向其他设备发送注册信息。

1. 重置设备
2. 在编程器上打开 AppTec360 的 NFC 配对应用程序
3. 选择是否要跳过存储加密和/或删除所有系统应用程序。
4. 背靠背握住两个设备
5. 现在，安卓企业注册应鲜明地体现出
6. 现在您可以在控制台中找到您的设备
    - a.在池中，如果没有配置自动发现
    - b.在为自动发现配置的用户中
    - c.提示：有可能需要重新加载网站才能看到设备

方法 3：谷歌账户

(需要安卓 5.1 或更高版本)

(注意：如果使用此方法，设备不会自动注册。您必须手动注册，或使用自动注册来自动完成注册过程)。

1. 重置设备
2. 完成设置步骤，直到可以使用谷歌账户登录为止
3. 输入 "afw#apptec "作为用户名/电子邮件
4. 点击 "下一步
5. 您的设备现在是安卓企业设备

KNOX 注册

在这里您可以激活 KNOX 注册并找到在 KNOX 部署门户中创建 KNOX 注册档案所需的信息。您需要一个 KNOX 部署门户的账户来配置和使用该功能。

(https://www.samsungknox.com/en/knox-deployment-program)

启用 KNOX 注册	激活 KNOX 注册。 注意如果禁用 KNOX 注册，现有的 MDM 配置文件将停止工作。如果再次启用 KNOX 注册，则必须更新 MDM 配置文件的 "自定义 JSON 数据 "字段
启用自动发现	当设备通过 "KNOX 注册 "进行注册时，系统会尝试根据序列号/IMEI 白名单（"常规设置">"Android 配置">"自动注册"）中设置的信息将其分配给用户。

1. 登录三星 KNOX 移动注册门户https://eukme.samsungknox.com/itadmin
2. 转到 "MDM 配置文件
3. 点击 "添加
4. 选择 "我的 MDM 不需要服务器 URI"，然后点击 "下一步"。
5. 现在使用管理控制台中显示的信息创建一个配置文件

现在，如果您直接从三星购买设备，三星可以直接将此 KNOX 注册配置文件安装到设备上。

您也可以下载 KNOX 部署应用程序，使用 KNOX 部署账户登录，并通过 NFC 向其他设备发送 KNOX 注册信息。

如果设备已经安装了 KNOX 注册配置文件，那么它将下载我们的应用程序并注册设备，前提是它有正常的网络连接。

通过 KNOX 注册的设备可在 "池 -> KNOX 注册 "中找到，或在自动发现中指定的用户内找到。

零接触

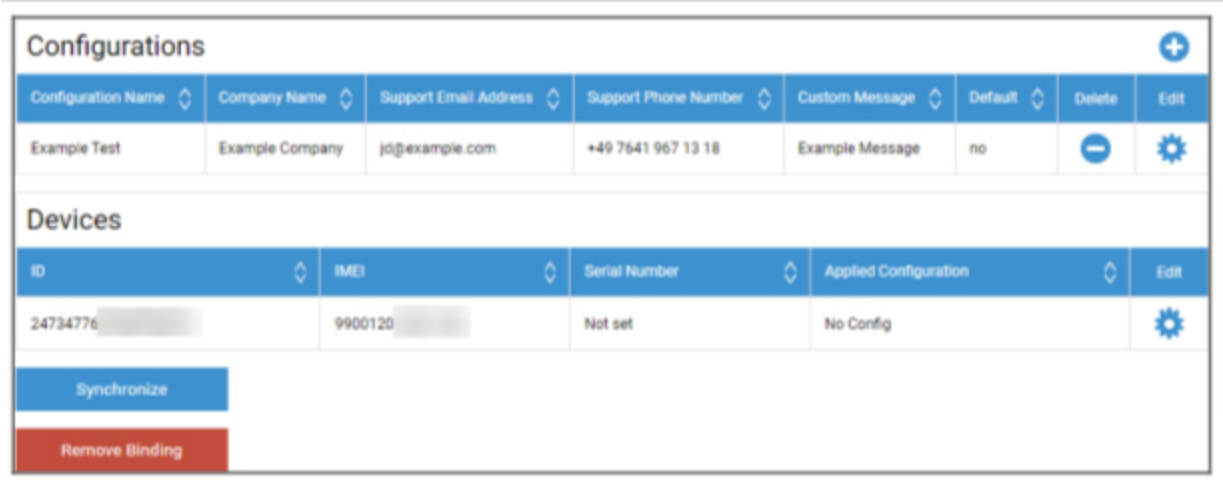
利用零接触技术，您无需接触设备或在设备上进行任何配置，就能轻松注册设备。您只需打开设备，像平常一样进行配置，设备就会自动接收所有关于如何设置和连接到 MDM 的信息。

要使用 Zero-Touch，您必须从支持 Zero-Touch 的经销商处购买设备。同一家经销商还要在 Zero-Touch 门户网站上为您创建一个帐户。如果您在访问 Zero-Touch 门户网站时遇到问题，请联系您的经销商以获取更多有关程序的信息。

点击 "开始设置 "开始设置。您将被重定向到一个登录页面，在这里您必须选择可以访问 Zero-Touch 门户的 Google 账户。

注意：可以选择任何账户。因此，请务必在此步骤中选择正确的账户。如果你看不到你的设备/配置，你很可能用错了账户。

完成登录后，界面如下：



单击 "+"添加配置并填写屏幕上显示的字段。如果将 "配置 "启用为默认 "配置"，它将自动分配给新设备。创建或设置默认配置不会将其分配给现有设备。

如果设备未指定 "配置"，则会设置为普通设备，无法连接到 MDM。因此，请确保为设备分配了 "配置"。

连接账户、设备可见并为其分配配置后，就可以开始设置设备了。

您可以将设备添加到自动注册列表，这样它们就会自动注册到指定的组或用户中。如果您没有在自动注册列表中配置任何内容，设备将注册到设备池中。

Windows 配置

Windows 配置

在这里，您可以选择在 Windows 10 PC 上启用以下配置：

即时 DM 连接	
初始重试时间	建立与设备的首次连接尝试，该值呈指数增长
连接重试	表示在出现连接错误时，DM-客户端应执行多少次连接尝试。
最长睡眠时间	表示连接错误后的最长休眠时间
首次同步重试	设备在首次连接后与服务器通信的时间间隔
首次重试间隔	与 "首次同步重试 "有关 这里的时间以分钟为单位 例如，在 "首次同步重试 "下列出值 "2"，在 "首次重试间隔 "下列出值 "4 分钟"，这样设备在首次连接后每 4 分钟进行 2 次通信。
第二次同步重试	设备在完成 "首次同步重试 "后与服务器通信的时间间隔
第二次重试间隔	与 "第一次重试间隔 "的原理相同，只是这里适用于 "第二次同步重试"。
常规同步重试	间隔，设备今后与服务器通信的频率 默认值："无限 建议不要更改此值，因为如果输入 "10"，设备将与服务器通信 10 次，然后停止通信！
常规重试间隔	与 "第一次/第二次重试间隔 "的原理相同，只是在这里会将设置应用于未来
常规重试间隔	与 "第一次/第二次重试间隔 "的原理相同，只是在这里会将设置应用于未来

内容框

配置

您可以在此配置内容盒。您可以在 ContentBox 中为群组放置文件，这些文件可以通过设备上的 ContentBox 应用程序访问。

启用内容框	启用 ContentBox。如果不使用 ContentBox，禁用此功能可以节省内部部署机器上的资源。
使用外部 ContentBox 安装	ContentBox 也可以与您自己的 Nextcloud 一起运行。
网址	Nextcloud 实体的完整 URL
根用户	Nextcloud 账户的根用户
根密码	Nextcloud 账户的根密码
默认组文件夹权限	默认组文件夹权限，可按组单独修改（在 "移动管理 "中）
与子组共享组文件夹	如果激活，每个子组可读取主组的所有文件夹，也可为每个组单独配置（移动管理）
分组权限	分组权限 可为每个组单独配置（移动管理）
允许共享	允许用户通过链接共享内容，可为每个组单独配置
最大文件上传大小（MB	文件的最大大小 标准：512 MB 最大配置：2048
WebDAV 证书	
WebDAV URL	您还可以使用 WebDAV 打开 ContentBox。 在任何情况下，请勿删除以下文件夹：/apptecgroups /apptecgroups/AppTecGroup-X
根用户	根用户名称
密码	根用户密码

与 ContentBox 的同步会自动进行。不过，您也可以使用 "同步 ContentBox "进行手动同步。

此外，您还可以在每个设备上激活/禁用 ContentBox。

如果您没有获得额外的 ContentBox 许可，那么您仍然可以使用 25 台设备来测试 ContentBox - 在这里您可以为相应的设备激活此功能。

LDAP 配置

LDAP 概述

在这里，您可以通过 LDAP 与活动目录建立连接，批量导入用户和组。同步必须手动执行。您可以将多个 LDAP 连接配置到不同的系统或使用不同的配置/过滤器。

服务器名称	服务器的显示名称
类型	目前只支持支持 LDAP 的 Active Directories
LDAP 域	主 LDAP 域（如 example.com）
LDAP 主机	只有在给定的 LDAP 域下无法访问 LDAP 主机时才需要使用。
港口	留空表示使用标准端口（389 或 636 用于 SSL）
用户名	例如：CN=John,OU=Users,DC=EXAMPLE,DC=COM 注意：大多数系统要求使用这种格式的用户名，不接受 "John "作为用户名。
密码	
确认密码	
连接安全	注意：使用 SSL 或 TLS 时，将检查 Active Directory 的证书。如果是自签名，则必须将根 CA 添加到本地计算机的信任存储中。如果是云计算，则活动目录必须提供受信任的证书，否则连接只能在无加密的情况下工作。
自动同步。	在常规 LDAP 设置中指定的时间间隔内启用 LDAP 目录自动同步。
基准 DN	如果不想同步整个目录，可以在此指定一个 OU，例如：OU=AndroidUsers,OU=Users,DC=EXAMPLE,DC=COM
成员	所有导入的用户都将添加到选定的组中
只有激活的用户?	启用后，将考虑 userAccountControl 属性，没有该属性的用户将不会被导入。
LDAP 过滤器	您可以使用 LDAP 过滤器来过滤哪些用户会被导入
Regex 过滤器	您可以使用 Regex 过滤器过滤哪些用户会被导入
测试连接	保存配置时测试连接
同步时重置目录结构?	如果为 "true"，所有 LDAP 条目都将移回其在 LDAP 树中的原始位置。建议启用。

重新导入已删除的用户和组?	启用后，已删除的用户和组将重新创建。建议启用。
同步删除?	启用后，组和用户在 LDAP 服务器上删除时将被删除。被删除用户的设备也将被删除。

在 LDAP 配置列表下方，您可以定义系统自动同步的时间段。只有激活了相应选项的 LDAP 配置才能进行自动同步。

应用程序管理

内部应用程序 DB

安卓

在这里，您可以上传公司开发的 Android 应用程序，然后在移动管理的设备或组配置文件中进行分发。

请注意，我们建议仅以这种方式发布 Google Play 商店中没有的应用程序。

点击 "+"上传您要上传的应用程序的 APK。目前只支持 APK 格式。

内部部署设备的上传限制可在设备配置步骤 3 中增加。如果您想增加云设备的上传限制，请联系支持部门获取更多信息。

请注意，APK 通常比其内容小一些。由于 APK 会在过程中解压缩，因此上传可能会因此失败。例如，在上传限制为 100MB 的情况下，95MB 的 APK 有可能上传失败。在这种情况下，请按照上述方法提高上传限制。

我们还建议首先将 APK 手动移动到一个测试设备上（例如通过 USB），然后尝试使用该设备的 "文件 "应用程序手动安装。如果因故无法安装，通过 MDM 安装也会失败。

更新目标

使用 "更新目标 "功能，您可以选择应安装哪个版本的应用程序，或者如果激活了某个应用程序的 "保持更新 "功能，则应将其更新到哪个版本。

如果未选择更新目标，则将使用最高版本。

请记住，安卓系统不能降级应用程序。此外，请注意 "版本代码 "决定了一个版本是更高、更低还是相同。因此，在创建更新时，请确保在应用程序中正确增加此版本。

iOS

在这里，您可以上传您开发的 iOS 应用程序，然后在设备或群组配置文件的移动管理中发布它们。

点击 "+"上传您要上传的应用程序的 IPA。目前只支持 IPA 格式。

内部部署设备的上传限制可在设备配置步骤 3 中增加。如果您想增加云设备的上传限制，请联系支持部门获取更多信息。

更新目标

使用 "更新目标 "功能，您可以选择应安装哪个版本的应用程序，或者如果激活了某个应用程序的 "保持更新 "功能，则应将其更新到哪个版本。

如果未选择更新目标，则将使用最高版本。

MacOS

您可以在这里上传您开发的 MacOS 应用程序，然后在设备或群组配置文件中的移动管理中发布它们。

点击 "+"上传您要上传的应用程序的 PKG。目前只支持 PKG 格式。

内部部署设备的上传限制可在设备配置步骤 3 中增加。如果您想增加云设备的上传限制，请联系支持部门获取更多信息。

更新目标

通过 "更新目标 "功能，您可以选择应安装哪个版本的应用程序，或者如果激活了某个应用程序的 "保持更新 "功能，则应将其更新到哪个版本。

如果未选择更新目标，则将使用最高版本。

Windows 10

在这里，您可以上传 Windows 10 应用程序，然后在设备或群组配置文件的 "移动管理 "中进行分发。

点击 "+"上传您要上传的应用程序的 APPX、APPXBUNDLE 或 MSI。目前仅支持 APPX、APPXBUNDLE 或 MSI 格式。

您还可以上传和定义应用程序的依赖项，这些依赖项将在安装所需应用程序之前自动分发和安装。

内部部署设备的上传限制可在设备配置步骤 3 中增加。如果您想增加云设备的上传限制，请联系支持部门获取更多信息。

更新目标

通过 "更新目标 "功能，您可以选择应安装哪个版本的应用程序，或者如果激活了某个应用程序的 "保持更新 "功能，则应将其更新到哪个版本。

如果未选择更新目标，则将使用最高版本。

Win32 软件包 (.exe)

您还可以向设备分发 .exe 文件/安装程序。

软件包名称	将显示在 MDM 中的名称
说明	MDM 中显示的说明
软件包文件	只允许使用 .zip 文件。将要部署的文件放入此压缩文件中。
部署环境	**系统**：安装命令以系统权限运行，高于 "用户 "权限。此外，使用 "System "时，进程没有用户界面，因此会保持沉默，用户配置文件（如%AppDat% 等环境变量）也无法访问。**用户**：安装命令可以访问用户配置文件，必要时可以显示用户界面。注意：某些进程可能只在一种情况下工作。例如，如果一个软件将自己安装到 AppData 中，那么它只能在选择 "用户 "时工作。
安装命令	用于安装程序的命令。例如，对于根目录中包含 "setup.exe "的压缩文件，如果支持参数"/s "以进行静默安装，则安装命令为 "setup.exe /s"。请注意，不同的软件可能有不同的参数。
卸载命令	通过 MDM 卸载软件时要运行的命令。通常指向卸载程序。例如 "C:\Program Files\ExampleSoftware\uninstall.exe".
要求	
注意：必须满足所有设置要求才能安装软件。否则将无法安装。某些字段可能是强制性的。如果未为某个要求设置值，该要求将被忽略。	
操作系统架构	操作系统架构
最低操作系统版本	最低操作系统版本
最小可用磁盘空间（MB）	最小可用磁盘空间（MB）
最小物理内存（MB）	最小物理内存（MB）
最小逻辑处理器数量	最小逻辑处理器数量
最低 CPU 速度（兆赫）	最低 CPU 速度（兆赫）

额外要求	如果需要，您还可以在此手动定义规则或上传脚本，以执行额外的要求检查。
检测规则	
检测方法	您可以在此定义如何检测设备上是否安装了应用程序。只有当这些规则检测到应用程序未安装时，才会运行安装命令。只有当这些规则检测到应用程序未安装时，才会运行卸载命令。**手动定义规则**：允许您手动定义一个或多个规则，以检查是否存在特定文件、文件夹、MSI 或注册表键值。如果所有给定的检测规则都为真，应用程序将被视为存在。**使用脚本**：上传您自己的脚本，其中包含您自己的检查规则。如果脚本返回"$TRUE"，则认为应用程序存在。
检测规则	

应用程序设置

iOS 应用程序设置

在这里，您可以定义将应用程序添加到强制应用程序或企业应用程序商店的默认设置。

注意：这只能设置添加应用程序时默认选择的内容。这不会更改已添加到强制应用程序或企业应用程序商店中的应用程序的现有设置。

保持更新	自动更新应用程序。请注意，更新发布后可能需要 7 天才能更新应用程序。
无人管理时超车	如果（用户）已经安装了一个未受管理的应用程序，则该应用程序将由 MDM 接管和管理。
删除 MDM 配置文件时移除应用程序	移除 MDM 时卸载应用程序。
防止备份应用程序数据	防止备份应用程序数据。

安卓应用程序设置

在这里，您可以定义将应用程序添加到强制应用程序或企业应用程序商店的默认设置。

注意：这只是设置添加时默认选择的内容。这不会更改已添加到强制应用程序或企业应用程序商店中的应用程序的设置。

保持更新	自动更新应用程序。仅适用于 InHouse 应用程序。
受控 AppTec360 EMM 客户端更新	如果启用，管理员可以指定 AppTec360 EMM 客户端的更新目标。AppTec360 EMM 客户端所有可用版本的列表将显示在 "常规设置"→"应用程序管理"→"内部应用程序数据库"→"Android "中。

第三方应用程序

安卓

您可以在此设置 Ikarus 激活码。

将其设置为 "使用激活代码"，然后在此处输入激活代码。

注意：输入代码并保存后，代码尚未添加到发送到设备的配置文件中。您必须对配置文件进行任何更改，代码才能添加到配置文件中。例如，将配置文件中的任何开关从关 → 开 → 关 - 保存 → 立即分配。

iOS

在此输入 SecurePIM 许可证。输入许可证后，按 "保存更改"，即可使用 SecurePIM 选项。

VPP / KNOX Premium

苹果批量购买计划（VPP）允许您在设备上轻松发布付费和免费应用程序。我们强烈建议您这样做，因为您无需在设备上安装 Apple ID，用户无需确认安装（监督），用户无需输入 Apple ID 密码，而且您可以轻松分发付费应用程序，无需在每台设备上重复购买。

要使用 VPP，您必须在 Apple Business Manager 中注册。

VPP 许可证

在这里，您可以全面了解 VPP 应用程序、已使用的许可证数量以及可用许可证数量。

单击 "滚轮 "可查看哪些设备已分配了许可证，以及该分配的状态如何。

单击 "刷新 VPP 缓存"，该缓存会将 MDM 中分配的许可证与 Apples 端分配的许可证进行比较。在某些情况下，这可以解决许可证问题。

VPP 令牌

您可以在此上传 VPP 令牌，令牌可在设置 → 应用程序和书籍中的 Apple 业务管理器中找到。你可以上传多个 VPP 令牌。

只需在 Apple 业务管理器中下载一个新的令牌，点击 "编辑 "轮并上传新令牌，即可更新令牌。

VPP 模式 "决定许可证分配的处理方式。根据具体情况，您必须使用不同的模式：

通过 QR 码、链接、Apple 配置器或 DEP 注册设备时，必须使用 "基于设备"。

如果设备是通过用户注册或作为共享 iPad 注册的，则必须使用 "基于用户"。

如果启用 "自动许可证管理"，从一个组移动到另一个组的用户将自动根据移动到的组配置文件分配 Apple VPP 许可证。

他们迁出的组别中现有的 Apple VPP 许可证不会被撤销。

添加到组的新用户将根据各自的组配置文件自动分配 Apple VPP 许可证。

KNOX 高级密钥

在这里您可以输入您的 KNOX Premium 密钥来使用三星 KNOX 容器。

请注意，自 Android 10 起，该功能已不再受支持。请使用安卓企业级容器。

应用程序商店设置

地区和语言

在此，您可以为应用程序管理中的应用程序搜索设置默认语言和地区。

请注意，iTunes 的设置也定义了系统抓取某些应用程序信息的方式。如果你在列表中遇到以奇怪方式显示的应用程序（例如图标丢失），你可能设置了一个特定应用程序不可用的区域。

AE Play 商店

在此，您可以找到用于安卓企业设备的 Play Store 的所有选项，以批准应用程序、将自己的应用程序上传到 Play Store 或创建自己的 Web 应用程序。

批准的应用程序

在这里，您可以概览您已批准的所有应用程序。

Play 商店应用程序

这将加载一个显示 Play Store 的 iFrame。搜索任何你想要的应用程序，点击并批准它。在批准应用程序时，你还可以定义，如果所需权限发生变化，批准将被撤销。我们建议在批准应用程序时将这些设置设为默认。

应用程序通过审核后，您可以将其添加到您的个人资料中。

批准后，"批准 "按钮将变为 "撤销批准"，因此如果您不再需要这些应用程序，可以随时将其删除。

私人应用程序

在这里，您可以将自己的应用程序作为私人应用程序上传到 Google Play 商店。这样，您就可以通过 Googles 服务发布应用程序，并通过它们进行更新。这样做的另一个好处是，您自己的应用程序无需用户确认即可安装，而用户确认通常是必要的。

网络应用程序

您可以在这里创建网络应用程序，它是指向某些网页的链接，可以像应用程序一样进行分配。

您还可以自定义图标，并进一步定义显示方式。

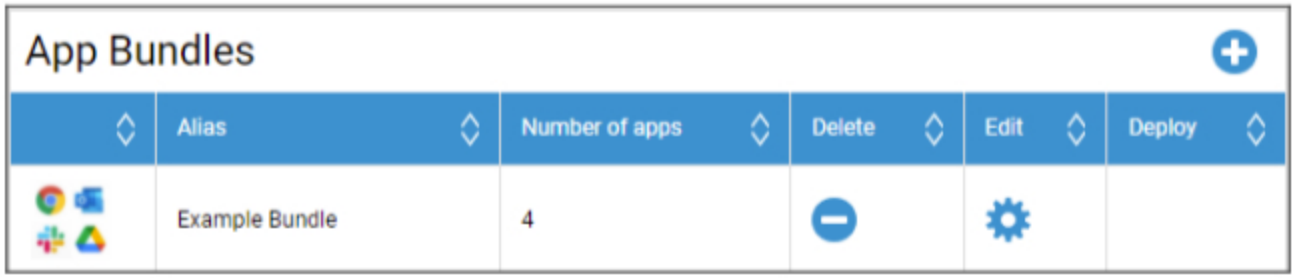
商店布局

商店布局定义应用程序在 Play 商店中的显示方式，或者是否显示。

请记住，如果要显示 Play Store 中的应用程序供用户手动安装，就必须在布局中添加这些应用程序 **和** 中添加到企业 Play 商店。如果只在其中之一添加应用程序，则不会显示。

应用程序捆绑包

通过应用程序捆绑包，您可以定义一组应用程序，只需单击一下即可将其分配给设备或组配置文件。



点击 "+"创建新的应用程序捆绑包。创建应用程序捆绑包后，您可以点击 "编辑"，将不同来源的应用程序添加到捆绑包中。

捆绑包可以像其他应用程序一样添加到配置文件中。添加应用程序时，您会看到一个名为 "应用程序捆绑包 "的额外选项卡，捆绑包就在其中。

如果您对应用程序捆绑包做了任何更改，"部署 "一栏中将出现一个按钮。这样，您就可以将这些更改推送到包含此软件包的所有配置文件中。因此请记住，在添加或删除软件捆绑包中的应用程序后，必须手动执行此操作。

遥控器

TeamViewer

TeamViewer 连接器

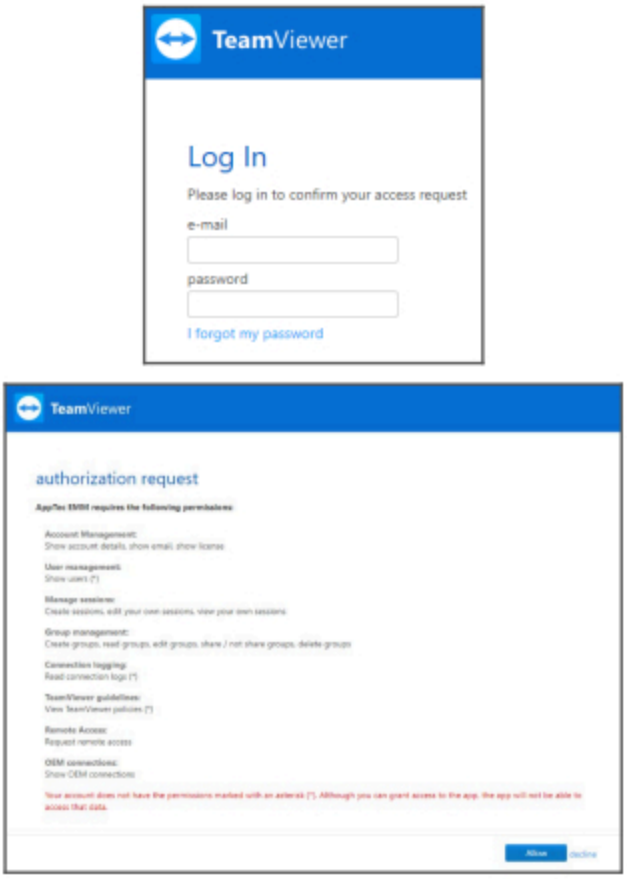
注意：在云版本的免费试用中，您无法连接 TeamViewer 帐户。您将自动连接一个免费演示账户。

转到常规设置 -> 远程控制 -> TeamViewer。在这里，您可以将 TeamViewer 账户与控制台链接，或查看当前连接账户的信息。此外，如果进入 "Active Sessions（活动会话）"，您还可以查看当前所有活动会话。

要链接账户，请单击 "开始设置"。

这样做会将您转到一个新页面，您必须使用 TeamViewer 帐户登录。

登录后，您必须授权 AppTec360 MDM 使用此帐户。确认后，您需要等待几秒钟，然后账户就连接好了。


TeamViewer
Log In
Please log in to confirm your access request
e-mail
password
I forgot my password
TeamViewer
authorization request

安装 TeamViewer QuickSupport

将应用程序 "TeamViewer QuickSupport "添加到设备配置文件或群组配置文件的必选应用程序中，然后点击 "立即分配"。等待应用程序安装到设备上。

如果尝试访问未安装应用程序的设备，则会根据设备配置安装或要求安装。

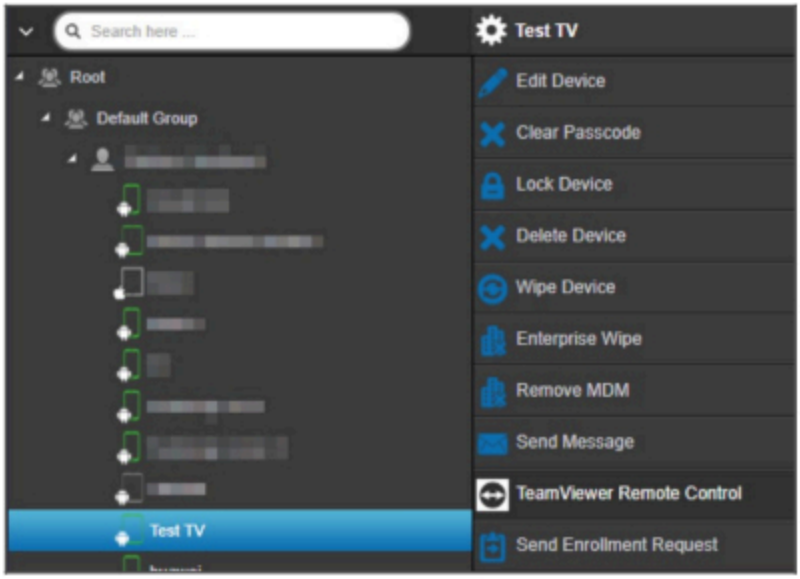
远程控制设备

要远程控制设备，请选择设备，点击滚轮并选择 "TeamViewer 远程控制"。

如果已经有一个活动会话，则可以使用旧会话或创建一个新会话。

确认要创建新的 TeamViewer 会话。

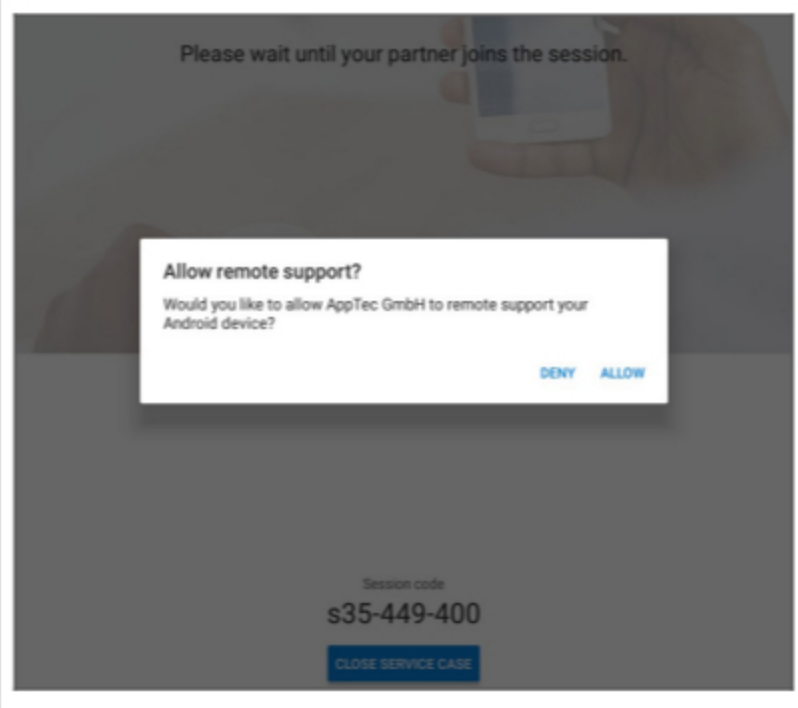
几秒钟后，您将获得一个 TeamViewer 会话链接。您可以点击 "开始 "在新窗口中打开该链接。


Search here ...
Root
Default Group
Test TV
Test TV
Edit Device
Clear Passcode
Lock Device
Delete Device
Wipe Device
Enterprise Wipe
Remove MDM
Send Message
TeamViewer Remote Control
Send Enrollment Request


Remote Control
Supporter URL: https://get.teamviewer.com/v13/
Click on "Start" to open the TeamViewer Remote Control in a new window.
Cancel
Start

该链接将打开已安装的 TeamViewer 并将您连接到设备。

现在，您必须在设备上确认连接，才能对其进行远程控制。

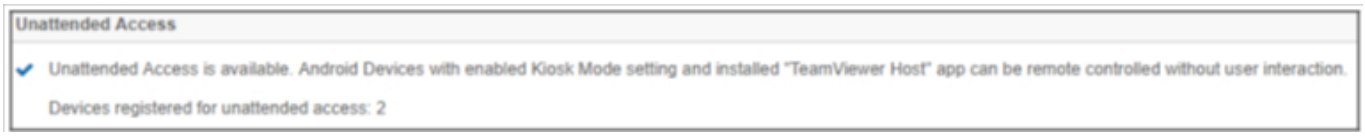


如果您使用的是 iOS，您将在 AppTec360 MDM 客户端中收到一条信息。通过该链接，设备将加入远程会话。根据设备的通知设置，您可能不会收到通知，而必须手动打开 AppTec360 MDM 客户端。

在某些安卓设备（如三星）上，需要安装额外的附加应用程序。如果您的设备需要，设备上的 TeamViewer 应用程序会通知您。

无人值守访问

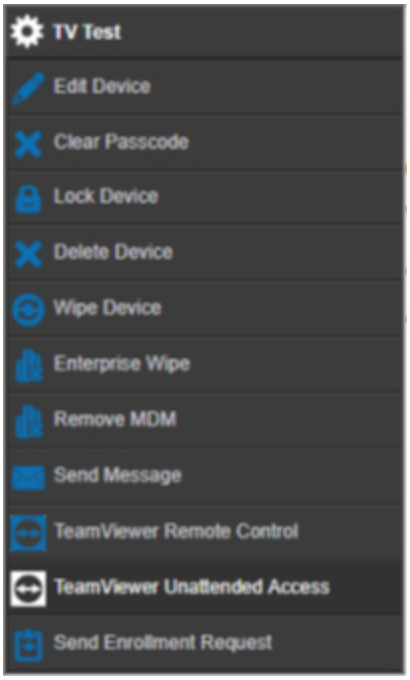
注意：无人值守访问仅适用于安卓设备。



只有当您的 TeamViewer 帐户使用 "Tensor "或 "Corporate "许可证时，您才能在不接受设备连接的情况下连接设备。

您可以在链接账户后，在 "常规设置 "中进行检查

要使用无人值守访问，您必须安装应用程序 "TeamViewer Host"，并激活个人档案中 "Kiosk Mode & Launcher "下的 "启用无人值守访问"。请注意，这只有在您使用 "Kiosk 模式 "时才能实现。



现在，只要选择设备并点击滚轮，就可以选择 "无人值守访问"。这将连接到您的设备，无需在设备上进行任何确认。请注意，在获得访问设备的链接之前可能需要一些时间。

泼水节

如果启用了 Splashtop 选项，就会在配置文件中看到 Splashtop 配置选项。

要使用 Splashtop，您必须在个人配置文件中将 Splashtop Streamer (com.splashtop.streamer.csrs) 设置为必选应用程序。然后，您可以在配置文件的 "远程控制 "中启用 Splashtop 配置。启用后将配置 Splashtop Streamer 应用程序。如果您正在使用 Splashtop Streamer，但没有与 MDM 结合使用，则应关闭此选项。

您还必须在 "远程控制 "下的个人资料中设置部署代码。访问 https://my.splashtop.com 并登录您的 Splashtop 账户。单击 "Add Computer（添加计算机）"，然后从生成的页面中复制 12 位部署代码。

没有部署代码，就无法进行远程控制。

之后，您可以右键单击设备，然后单击 "Splashtop Remote Control（Splashtop 远程控制）"启动远程会话。

Sim 卡管理

CSV 批量导入

这将显示已分配 Sim 卡的概览和所有相关信息。这有助于您在一个系统中掌握所有信息，不仅包括设备信息，还包括 Sim 卡信息。

注意： 这是手动管理/记录。由于操作系统的隐私/安全机制，无法从设备中自动获取这些数据。

您还可以将此列表导出为 CSV 格式。

承运商和关税

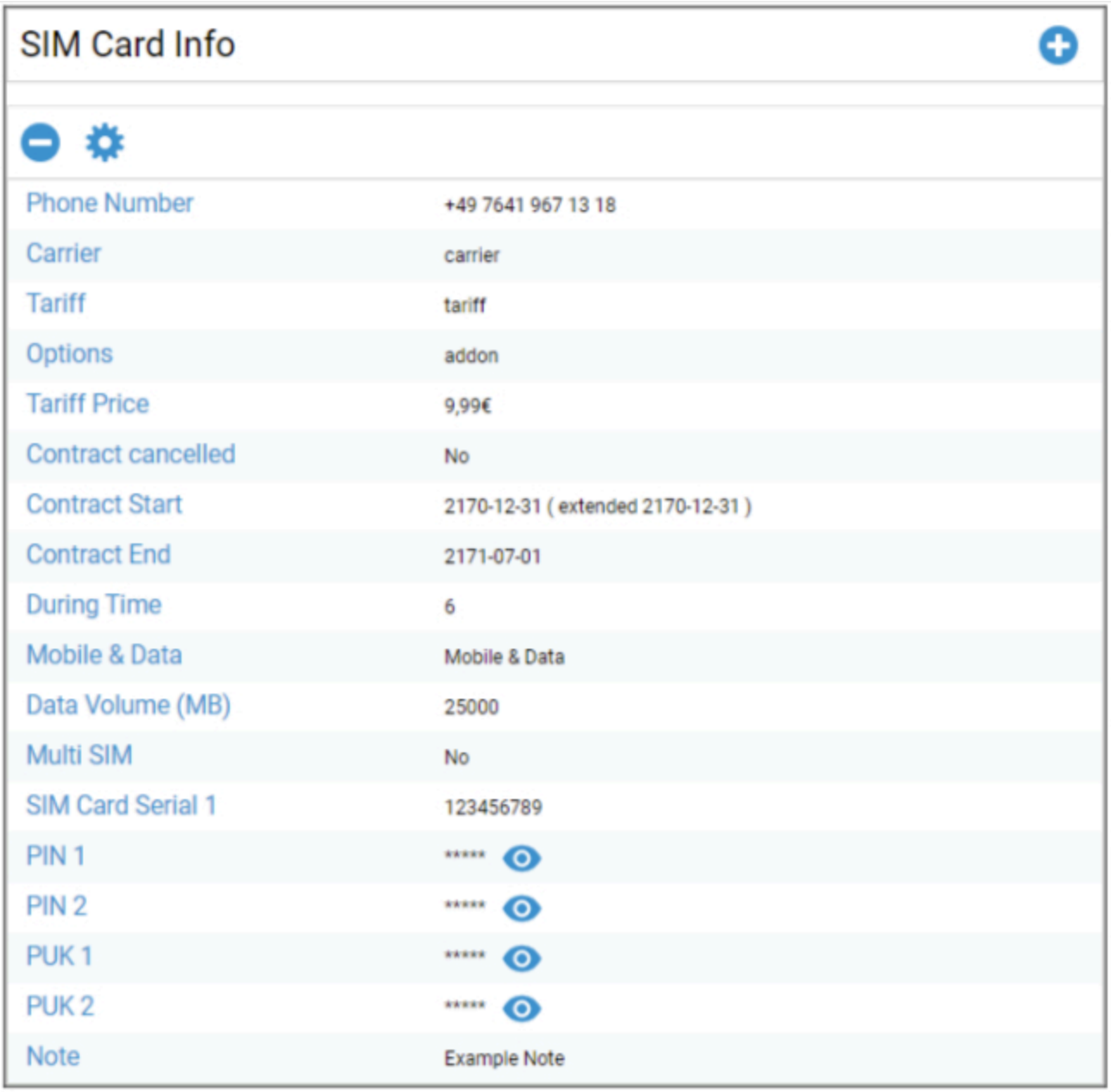
要添加 Sim 卡，首先点击按钮添加一个或多个运营商。

然后点击 "关税信息 "上的 "+"，为运营商添加关税。

如果您有类似功能，还可以在下面添加可选附加功能。

这准备了添加实际 Sim 卡所需的一切。Sim 卡目前分配给一个用户。因此，请进入 "移动管理"，选择用户并进入 "Sim 卡概览"。

在这里，您可以看到该用户的 SIM 卡。如果有，您可以编辑或删除。用户可以拥有多张 SIM 卡。

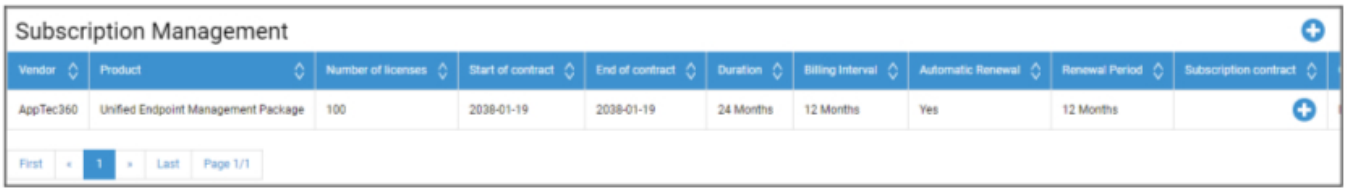


点击 "+"添加 Sim 卡，并添加所需的全部信息。这些 SIM 卡也会列在常规设置 → SIM 卡管理中的所有 SIM 卡列表中。

订阅管理

订阅管理

在这里，您可以记录正在运行的订阅及其详细信息，还可以存储不同的文件，如已签署的合同、终止信等。您还可以设置提醒功能，在订阅结束前通过邮件提醒您，或者自动延长订阅期限。



点击顶部的 "+"添加订阅。您可以添加任意数量的订阅。

点击不同字段中的 "+"，上传有关此订阅的文件。从技术上讲，您可以上传任何文件类型，但请注意，并非所有文件类型都能在浏览器中预览。

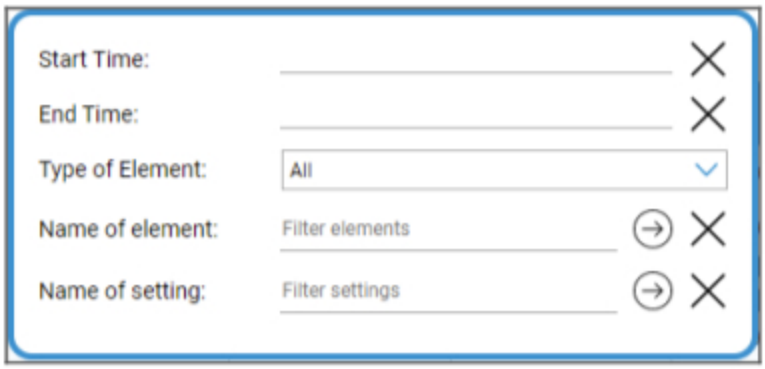
一般审计日志

审计日志

这里有一个通用的审计日志，可以显示所有更改。用户或组的审计日志只显示该用户或组所做的更改，而这里则显示控制台中任何地方所做的所有更改。

您可以查看哪些内容被更改、更改人、更改时间和更改地点。在某些情况下，您还可以扩展条目，查看更多细节。

可以点击用户或 "路径/类型 "中的条目，进入进行更改的位置。



在右上角，您还可以定义一个过滤器，这有助于在发生许多变化的环境中找到某些变化。

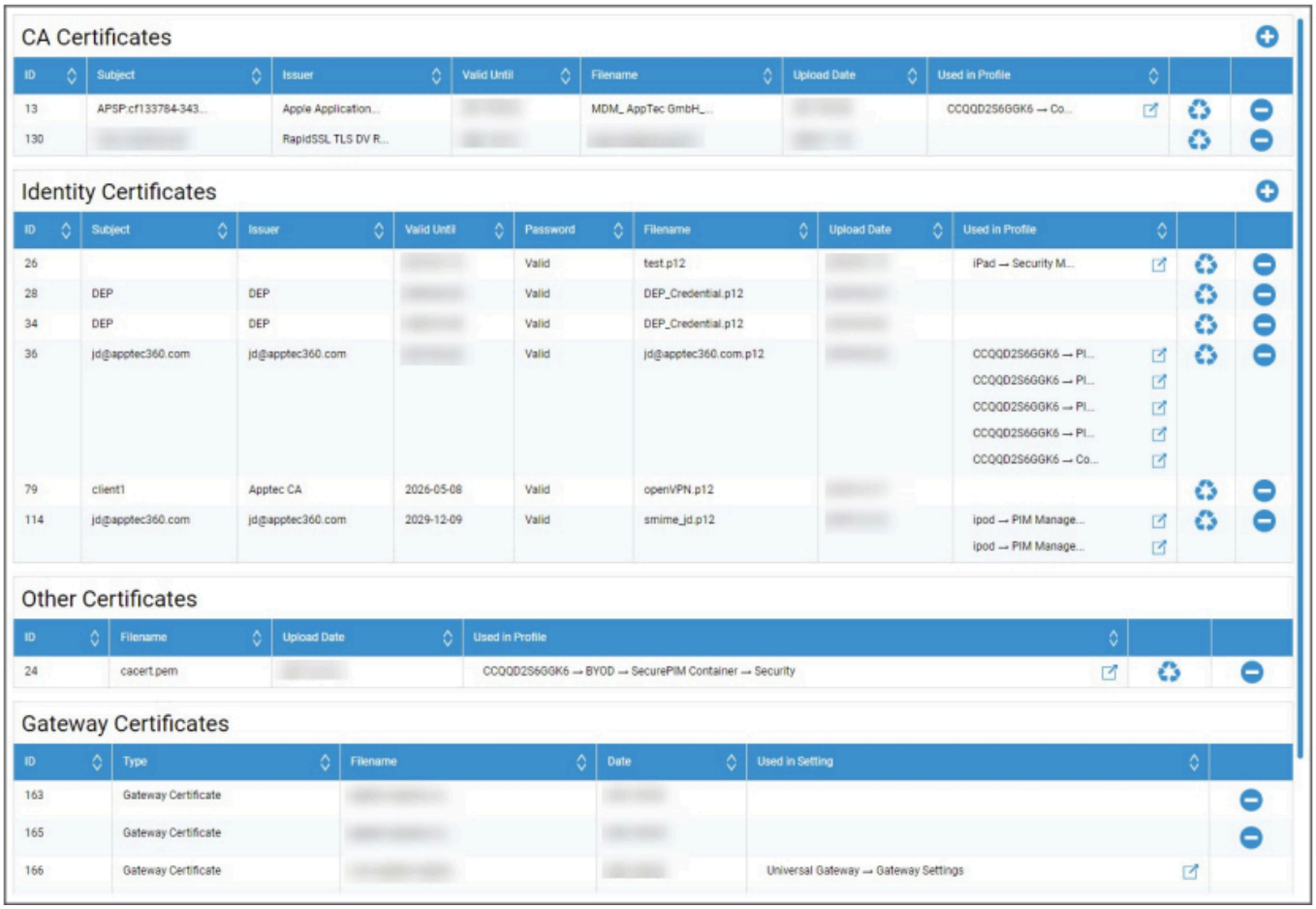
审计日志设置

"审计日志保留期 "定义审计日志在删除前应保留多长时间。

证书管理

在这里，您将看到控制台上传和使用的所有证书的概览。这只是一个概览。Wi-Fi 证书等的实际配置仍在相应位置的配置文件中完成。

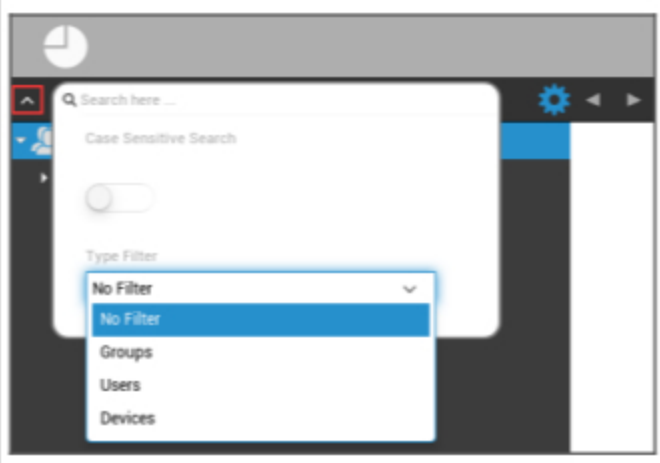
您还可以在此删除或更新证书，受影响的配置文件中将自动反映这些信息。点击 "已在配置文件中使用 "中的信息，可查看仍然分配证书的具体位置。



移动管理

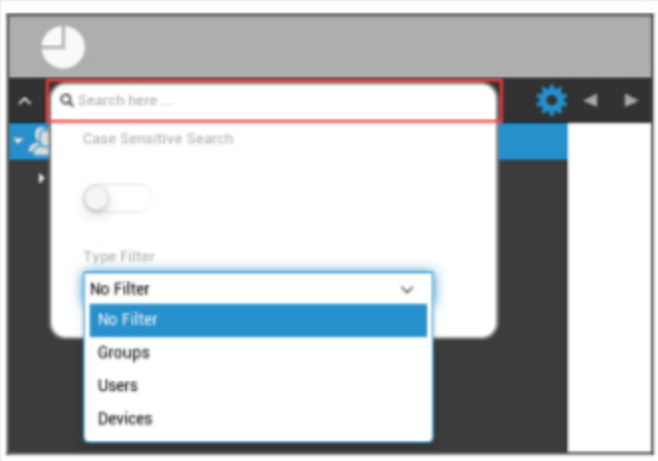
移动管理屏幕

设备过滤器



点击屏幕左上角，就可以找到用于显示设备的各种筛选器。

搜索窗口



搜索窗口允许您使用特定关键词搜索所有设备和/或用户。

选项齿轮

点击相应符号后，将显示可供选择的选项列表。

这些功能随当前窗口的变化而变化，并在相应章节中进行了说明。

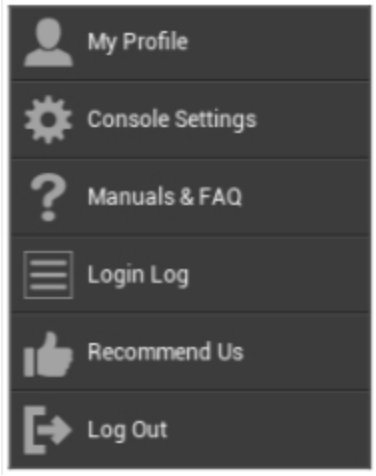
导航箭头

点击左箭头，您将进入上一页。

然后，点击右箭头，就会跳转到刚才离开的页面。

管理帐户设置

点击上面的电子邮件地址，会显示以下菜单：



我的简介	编辑管理员账户详细信息
控制台设置	配置管理员账户的控制台设置
手册和常见问题	查看 "常规设置 "中的 "手册和常见问题 "页面
登录日志	访问 "登录日志
推荐我们	查看 "常规设置 "中的 "推荐我们 "页面
退出登录	退出 MDM 控制台

用户信息

在这里，您可以编辑当前登录管理员的账户详情。

用户名	账户的用户名和/或电子邮件地址
名称	管理员姓名
姓氏	管理员姓氏
登录名	管理员登录名
电子邮件地址	管理员电子邮件地址
备用电子邮件地址	管理员备用电子邮件地址
图片	简介图片
电话号码	管理员电话号码
手机号码	管理员手机号码
电话分机	电话分机
地点	地点
职位	在公司的职位
用户组	选择要将管理员账户分配给哪个用户组
评论	输入评论
输入新密码	输入密码以更改密码
重复新密码	重复新密码以确认

请注意，管理访问权限也可以作为本地用户账户在层次结构中归档。在没有建立额外管理员的情况下，不应删除此管理员！

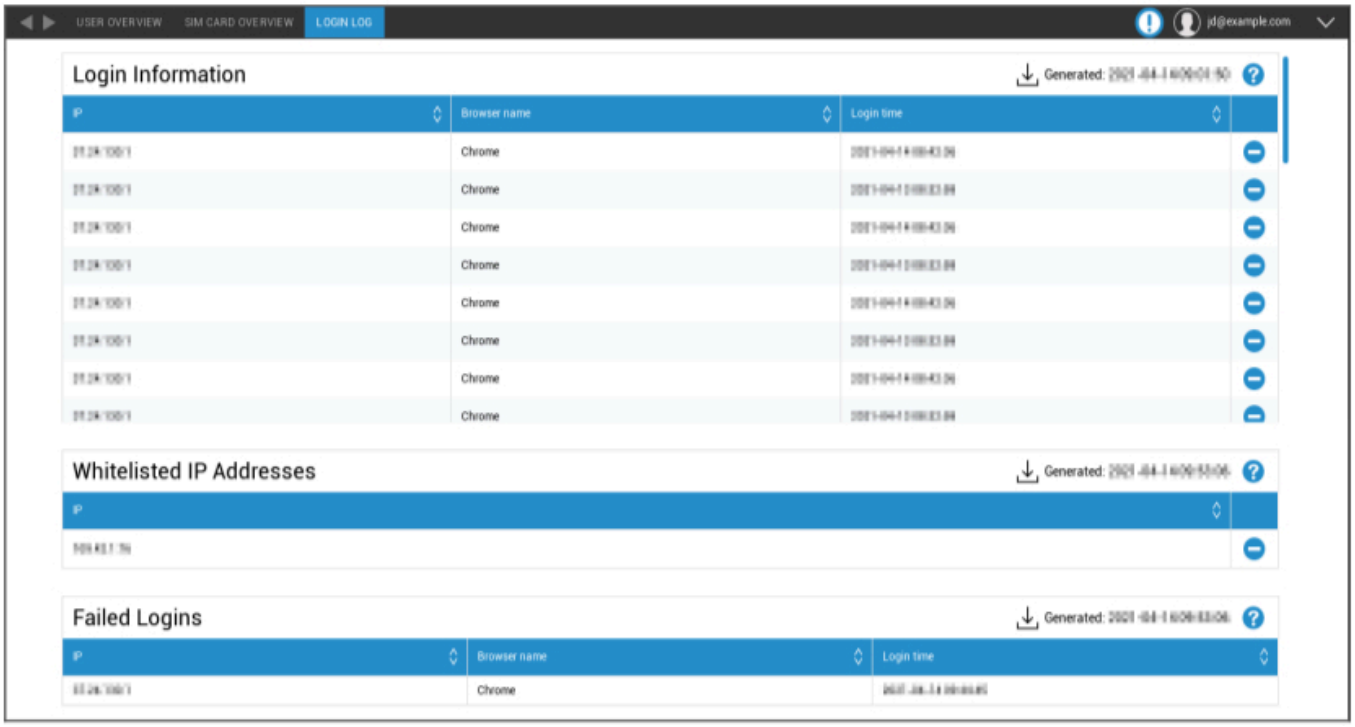
控制台设置

在这里，您可以为管理员账户配置以下控制台设置：

目录用户显示选项	定义用户在树中的标记方式
目录设备显示选项	定义设备在树中的标记方式
会话超时	如果用户在指定时间内没有任何操作，则会被注销。默认值为 60 分钟。更改此设置后，请注销并重新登录。
时区	选择使用的时区
时间格式	选择显示时间戳的方式
控制台语言	选择控制台的显示语言。可选择英语和德语。
主色调	您可以设置一种颜色，作为控制台配色方案的基色。 您可以使用颜色选择器，也可以用 HTML HEX 符号输入颜色。 粉红"、"黄色 "等 RGB 格式也可以使用。
保存命令	在不按 "保存 "按钮的情况下触发保存的组合键。
使用双因素身份验证	登录时启用双因素身份验证。 登录后，您将收到一封电子邮件，其中包含一个代码，您必须输入该代码才能登录。
双因素身份验证超时	设置一个时间段，在该时间段内，如果已经成功进行了身份验证，则不会要求您进行双因素身份验证。
通过以下方式发送验证码	验证码将发送到所选选项。设备信息将显示在属于您的所有 Android 和 iOS 设备上的 AppTec360 MDM 应用程序中。
登录后发送登录信息	如果启用，每次从未列在白名单上的 IP 地址登录时，系统都会发送一封电子邮件。电子邮件包含登录信息（如 IP、浏览器）。

登录日志

在这里可以看到当前登录的管理员账户的登录信息。



登录信息	控制台记录的当前登录的管理员账户的登录列表。 该列表显示您在过去 30 天内成功登录的所有信息。
白名单 IP 地址	这是所有白名单 IP 地址的列表。 如果您从此处列出的 IP 地址登录，则不会收到登录信息。 点击 "登录信息 "列表中某条目旁边的按钮，即可将 IP 地址添加到该列表中。 您可以点击该列表或上面 "登录信息 "列表中某条目旁边的按钮，将 IP 地址从该列表中删除。
登录失败	这是过去 30 天内所有登录失败尝试的列表。 如果您在 20 分钟内至少 3 次未输入正确密码，则该列表中将出现一个条目。 如果登录失败，您还会收到电子邮件通知。

移动管理中的企业管理（根节点

到达根节点（第一组）后，您可以为公司执行有关移动管理的各种设置。

创建分组	创建分组
重命名根节点	重新命名根节点（例如您的公司名称）
大规模招生	同时注册多个设备/用户
大规模分配	为各组指定一个简介，一目了然
快速应用程序管理	向各组设备发送应用程序的（未）安装请求
CSV 用户导入	将 CSV 中的用户导入到相应的组中

创建分组

通过 "创建子组"，您可以创建一个额外的子组。

您可以确定子组应该分配给哪个组。

(默认情况下，创建的新组被指定为根节点中的子组)

重命名根节点

您可以在此重命名根名称。在这种情况下，通常使用公司名称。

大规模招生

通过 "批量注册"，您可以注册多个设备和用户。

您可以直接选择用户接收注册的方式（电子邮件、替代电子邮件、短信）

根据用户要接收的设备（iOS、Android、Windows Phone），您可以直接在此处标记。

您还可以在这里配置是智能手机还是平板电脑，您必须正确选择，并打上对勾。

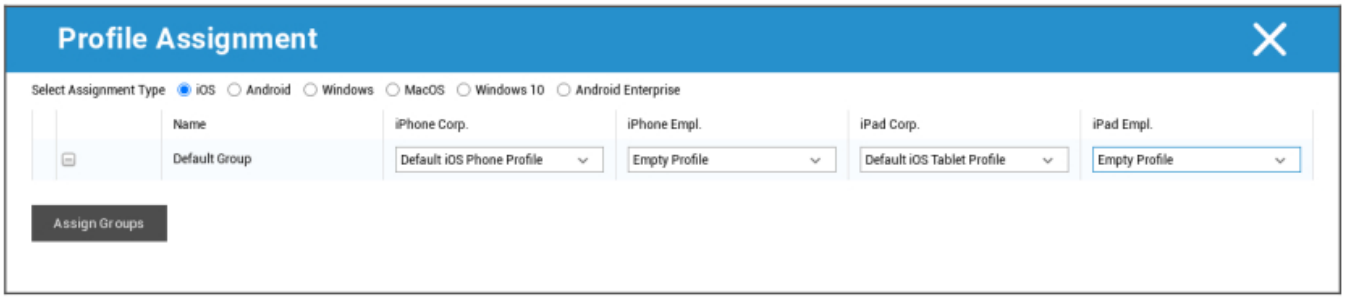
最后，您可以确定相关设备是企业设备还是私人设备（BYOD）。

使用 "导出为 CSV"，可以将信息导出为 CSV 数据文件。反过来，您也可以用 "导入 CSV "导入 CSV 数据文件，文件应如下所示：

Philipp Reiss；philipp.reis@apptec360.com；pr@apptec360.com；+41 61 511 3210；

大规模分配

在 "批量分配 "下，您可以将配置文件分配给所有组，其中分为 iOS - Android - Windows - MacOS - Windows 10 - Android 企业版

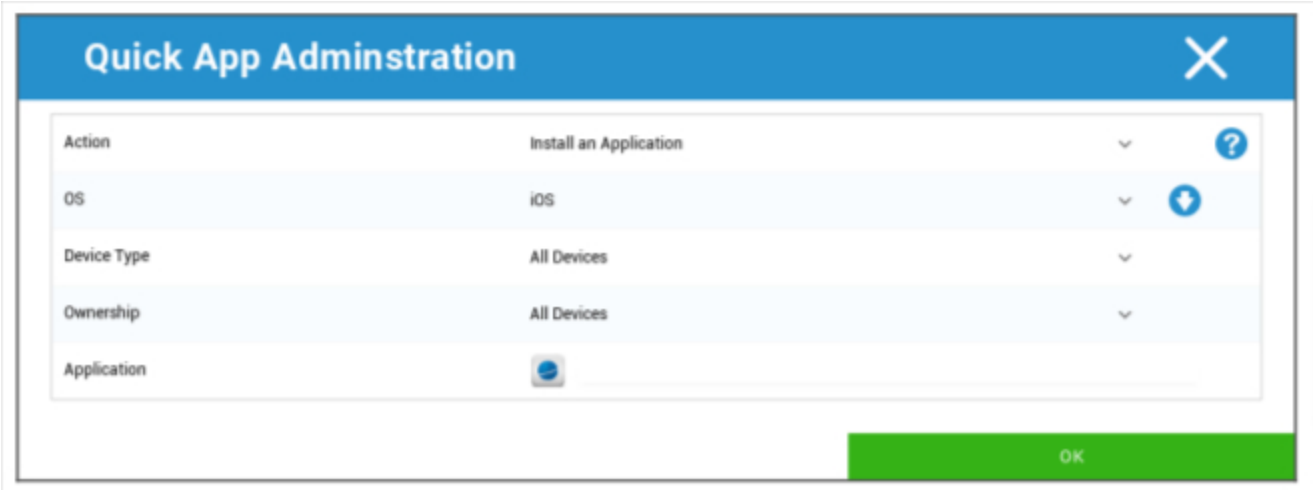


Windows - MacOS - Windows 10 - 安卓企业版

快速应用程序管理

在 "快速应用程序管理 "下，您可以向所选操作系统发送指定应用程序的安装或卸载请求。

您还可以定义是向所选操作系统的所有设备类型发送请求，还是只向特定设备类型发送请求。



CSV 用户导入

将 CSV 中的用户导入相应的组。

通过 "下载 CSV 模板"，您可以导出一个 CSV 模板文件，供填写（或用作参考）。

您也可以使用 "显示角色编号 "和 "显示组编号 "选项作为参考，创建自己的 CSV 文件。

CSV 文件可通过 "上传 CSV "上传到 MDM。

最后一步，点击 "开始导入 "即可开始导入。

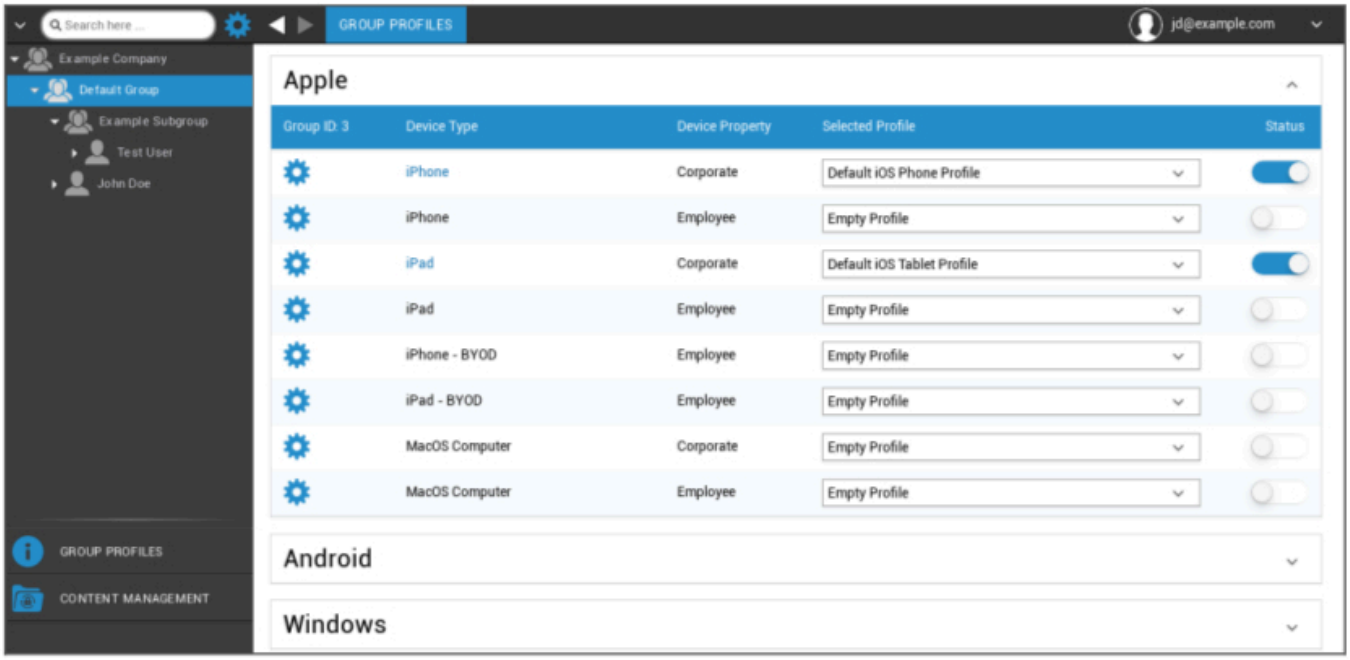
移动管理中的小组管理

只需单击概览，即可显示相应平台的不同配置文件。

一个配置文件包含所有可通过 AppTec360 提前在最终用户设备上建立的设置选项。在每个平台上，您都可以为公司设备（企业）或自带设备（员工）创建配置文件。

为了区分设备组的配置，例如根据位置或功能，建议创建几个子组。

请注意移动管理中的配置文件管理



通过档位菜单，您可以为相应的（子）组别进行各种设置。

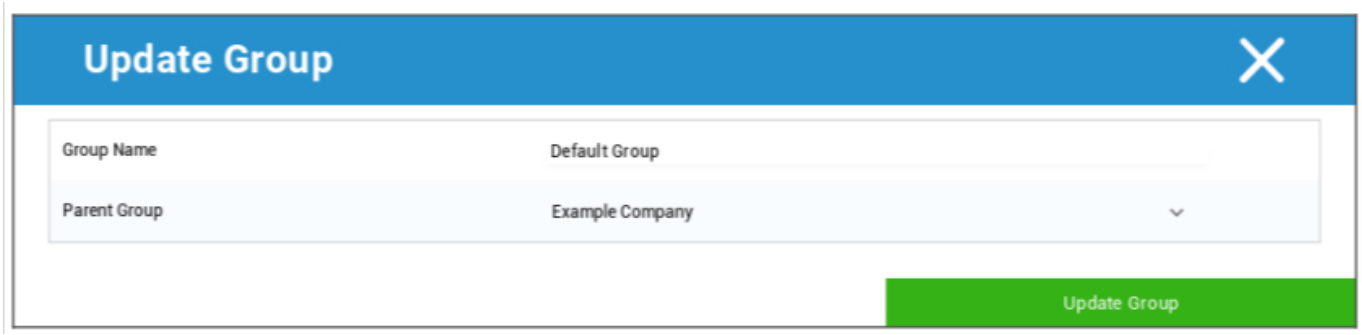
创建分组	为相应（子）组创建子组
编辑所选组	编辑所选组
删除所选组	删除所选组
大规模招生	为所选配置文件同时注册多个设备/用户
大规模分配	将配置文件分配给当前选定的组
创建分组	为相应（子）组创建子组
创建用户	为相应（子）组创建用户

创建分组

通过 "创建子组"，您可以创建一个额外的子组。

您可以确定将分组分配给哪个组（默认情况下，分组分配给当前选择的组）。

编辑所选组



在这里您可以编辑配置文件 - 在这里可以进行以下设置：

- 可更改组名
- 可更改父组

删除所选组

在 "删除所选组 "下，会列出相应组中的所有用户和设备。在这里，你可以选择删除它们。

对于一个用户，您可以执行以下删除命令：

删除用户	用户已删除
将用户移至组：	您可以将用户移动到另一个组（下面一栏，例如 "管理员）

对于一个设备，您可以执行以下删除命令：

擦除和删除	擦除和删除设备
从系统中删除	仅从 AppTec 移除设备

参考资料大众入学

参考资料质量分配

创建用户

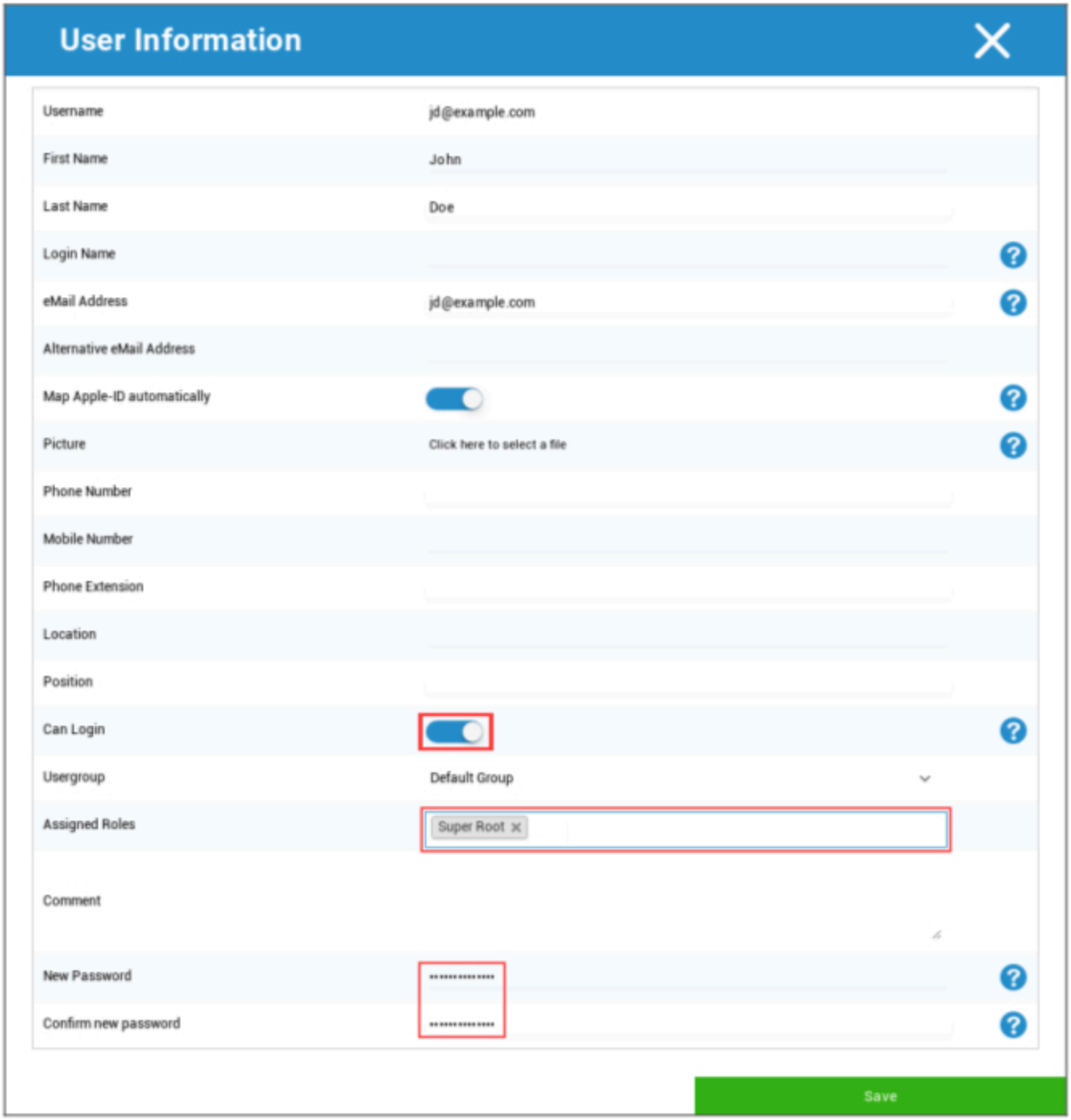
通过 "创建用户"，您可以添加一个新用户。

创建新的管理员用户

您可以将用户设置为管理员用户。这样他就有权限登录控制台并更改用户/组/设备。

创建一个普通用户或使用现有用户。选择要授予管理权限的用户，点击滚轮并选择 "编辑用户"：

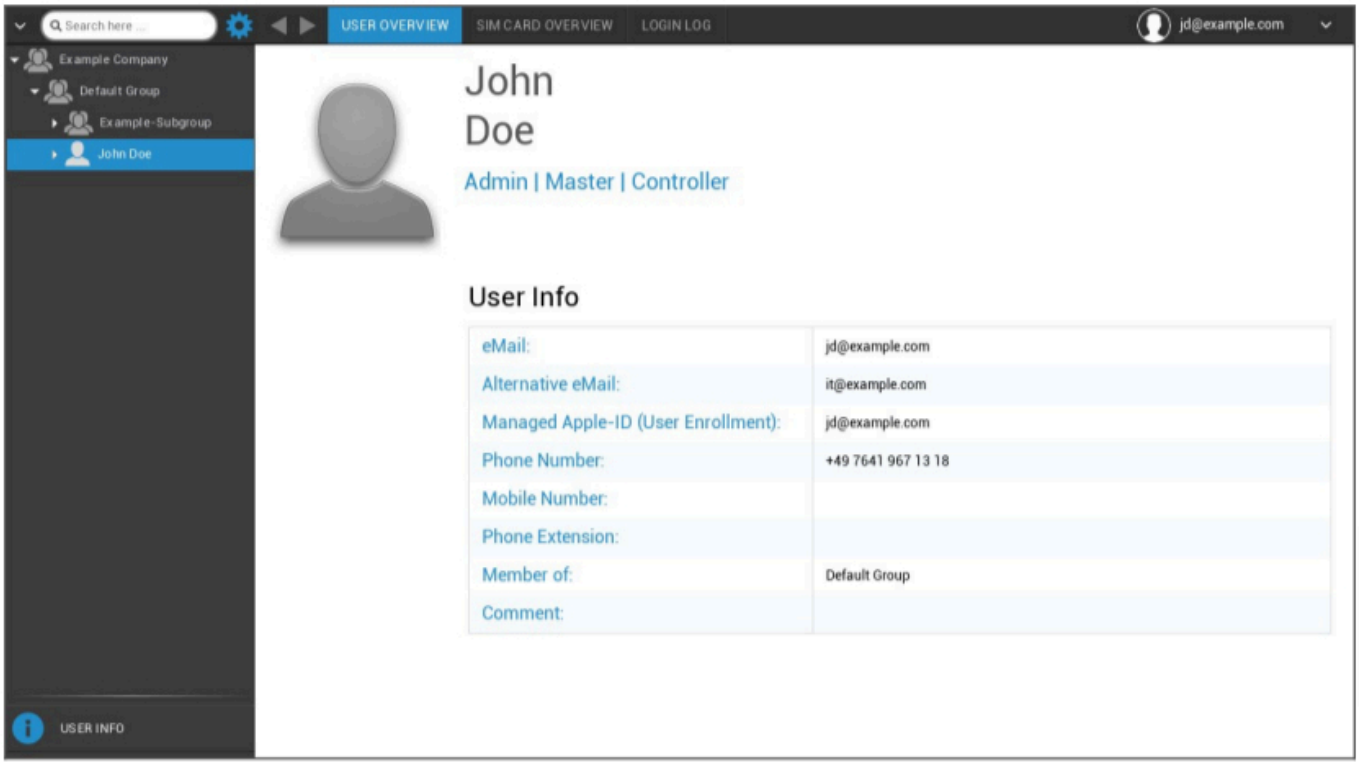
激活 "可以登录 "开关，为用户分配 "超级根 "角色并设置密码。



保存后，用户就可以使用用户名和密码登录了。

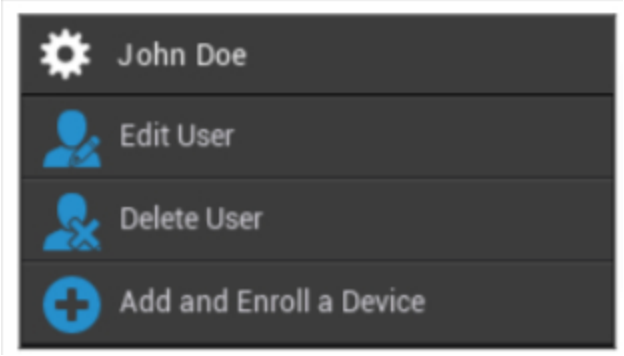
移动管理中的用户管理

选择某个用户后，您将看到以下概览：



您将看到之前在 "创建用户 "中输入的所有信息的概览。

使用安装在顶部的齿轮，可以进行以下配置：



用户名	所选用户的用户名
编辑用户	编辑用户信息
删除用户	删除用户 • 从系统中删除 = 设备将从 AppTec 中删除

	• 擦除和删除 = 设备将恢复出厂设置并从 AppTec 中删除
添加和注册设备	为所选用户注册设备

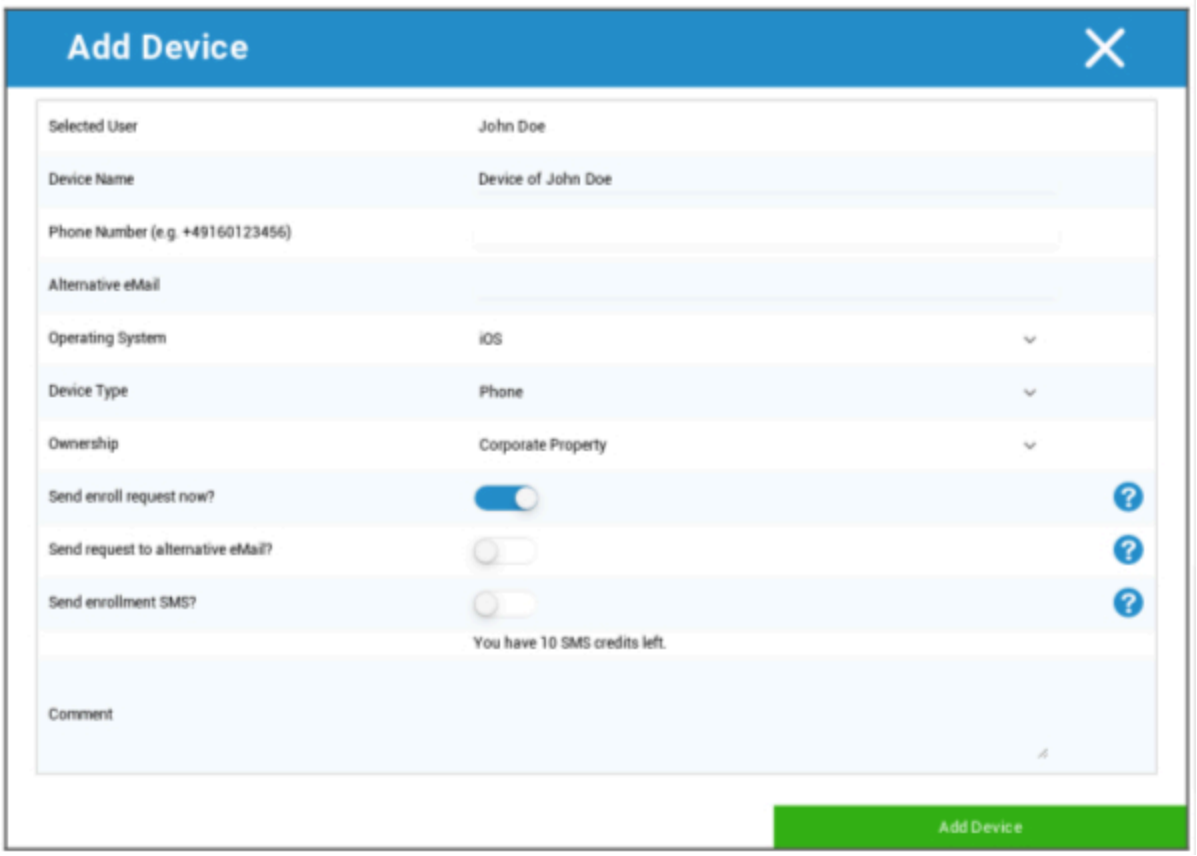
请注意，管理访问权限也可以作为本地用户账户在层次结构中归档。在没有建立额外管理员的情况下，不应删除此管理员！

添加和注册设备

在这里，您可以为所选用途选择一个设备。

您也可以直接将设备注册到组中。为此，请单击组，单击滚轮并选择 "添加并注册设备"。

您将看到以下概览：



根据要注册的设备类型，您必须执行以下配置：

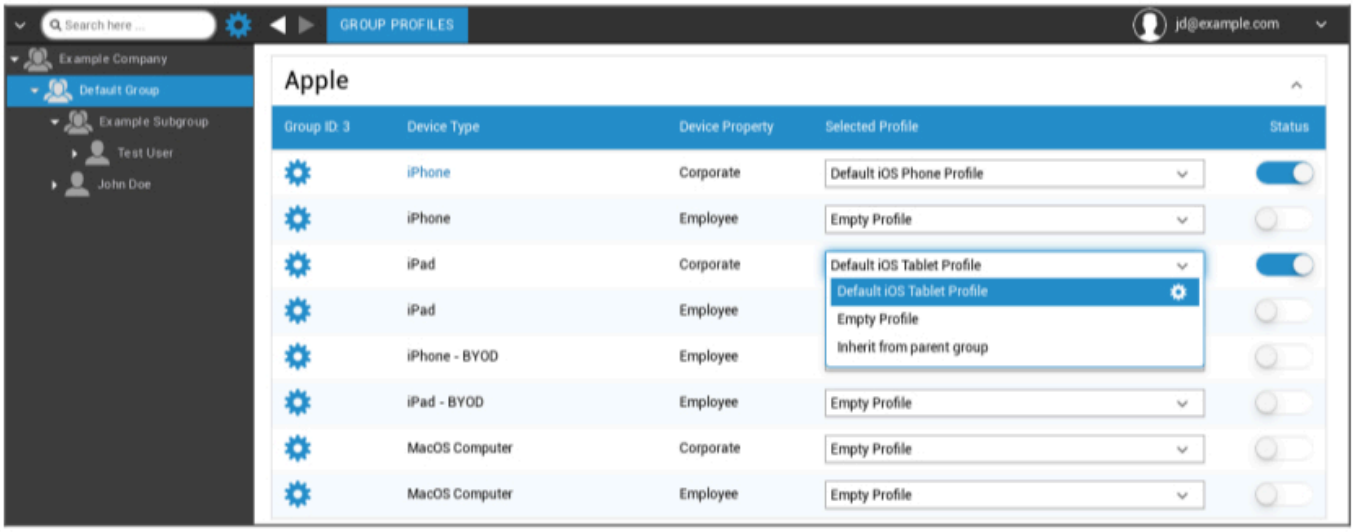
选定用户	所选用户（将自动填写）
设备名称	将自动填写（设备为 "用户名"）--但可以更改
电话号码	电话号码，将自动填写（只要用户提供了电话号码）--但在此处可以添加或更改电话号码
替代电子邮件	备用电子邮件，将自动填写（只要用户提供了备用电子邮件）--但可以在此添加或更改
设备所有者	公司财产 = 公司设备 员工财产 = BYOD 设备
选择操作系统	在这里，您可以选择以下操作系统： • iOS • iOS BYOD（用户注册） • MacOS • 安卓企业 • 安卓 • Windows 移动 • Windows 10
发送注册请求？	电子邮件会立即发送到主电子邮件地址，并提示用户连接设备
向其他电子邮件发送请求？	向备用电子邮件地址（电子邮件与 "正常 "注册请求电子邮件不同）额外或专门发送电子邮件（如果 "发送注册请求？）
发送注册短信？	通过 SMS 发送注册请求（必须输入 "电话号码"）。

注册请求发送后，设备将立即显示（红色标记）。

一旦设备连接成功，设备很快就会被标记为绿色，从而可以接收限制、应用程序等。

移动管理中的配置文件管理

单击组后，您将看到要配置的所有设备平台和分别分配的配置文件的概览。



	为所选配置文件执行配置
设备类型	设备类型和/或型号
设备属性	设备所有者（公司 = 公司财产，员工 = 员工私人设备）
精选简介	所选配置文件（齿轮打开配置文件的配置对话框）
现状	开/关（激活/禁用配置文件）

选择齿轮后，您将收到以下选项：

创建个人资料

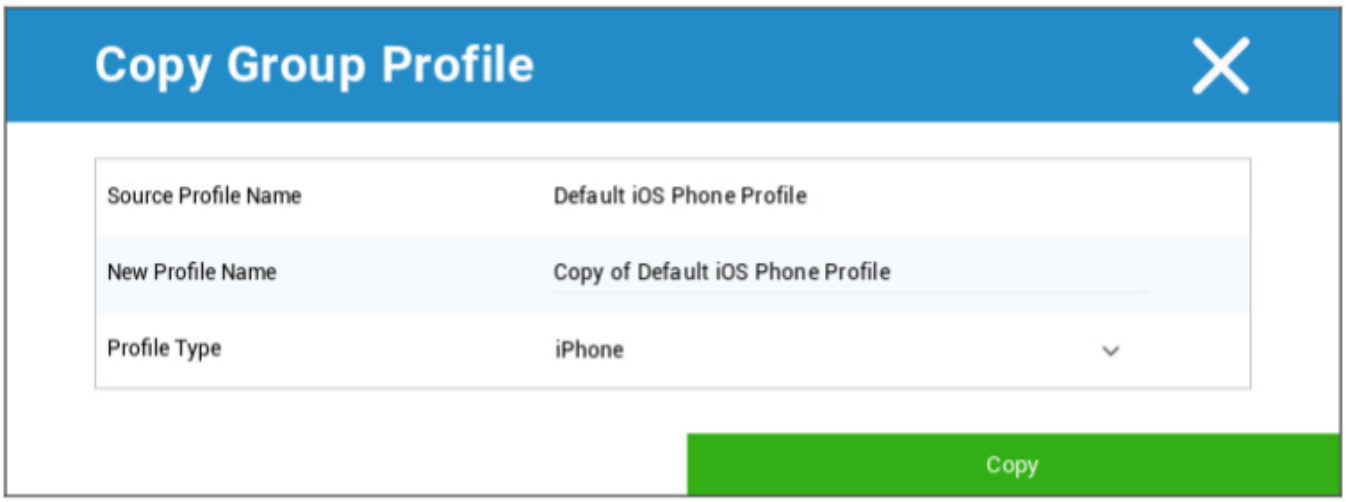
您可以为每个条目和/或平台创建和配置新的配置文件。点击该子点后，将立即创建配置文件，您可以立即开始配置 iOS、Android 和 Windows Phone。

编辑简介

点击 "编辑配置文件 "后，您将看到相应配置文件的配置显示，您可以在此设置配置。

复制简介

借助 "复制预案 "功能，您可以从已有的预案中复制设置/配置，并将其添加到新的预案中。

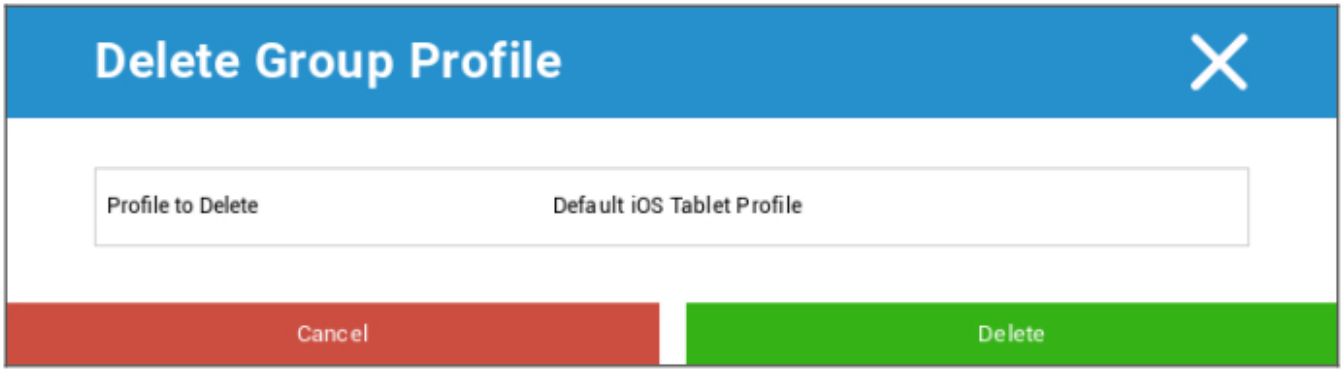


来源简介名称	要复制的配置文件的名称
新简介名称	新配置文件的名称
简介类型	配置文件类型（手机/平板电脑）

点击 "复制 "后，就会创建个人资料，现在就可以将其分配给小组了

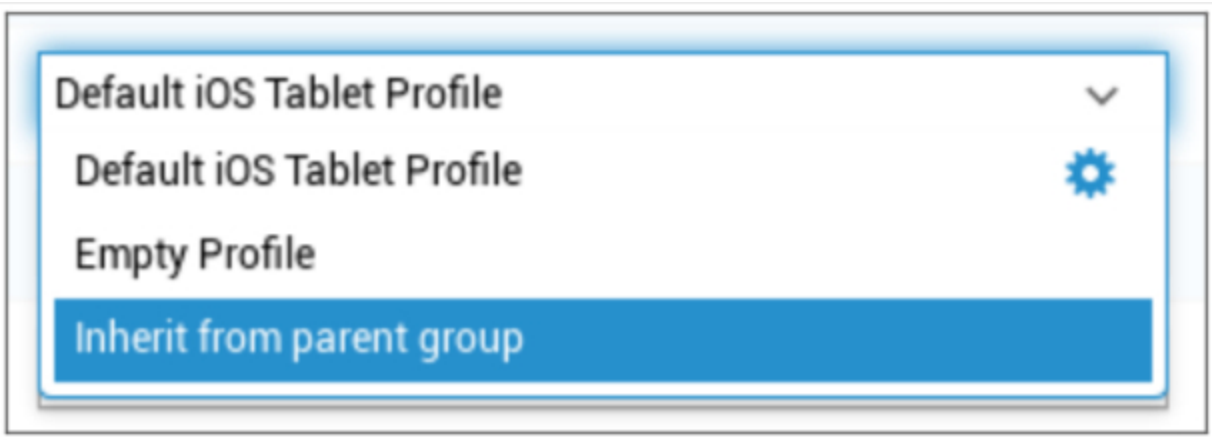
删除简介

您可以在此永久删除配置文件。请注意，在删除过程和随后的 "立即分配 "过程中，配置文件的配置将在受影响组的相应设备上消失，且无法恢复！


Delete Group Profile
Profile to Delete
Default iOS Tablet Profile
Cancel
Delete

档案继承

在选择配置文件时，可以选择 "从父组中继承"。



激活预案后，父组的预案将用于各自选定的设备（和各自的设备类型）。还请注意，对该预案的更改可能会影响多个组。

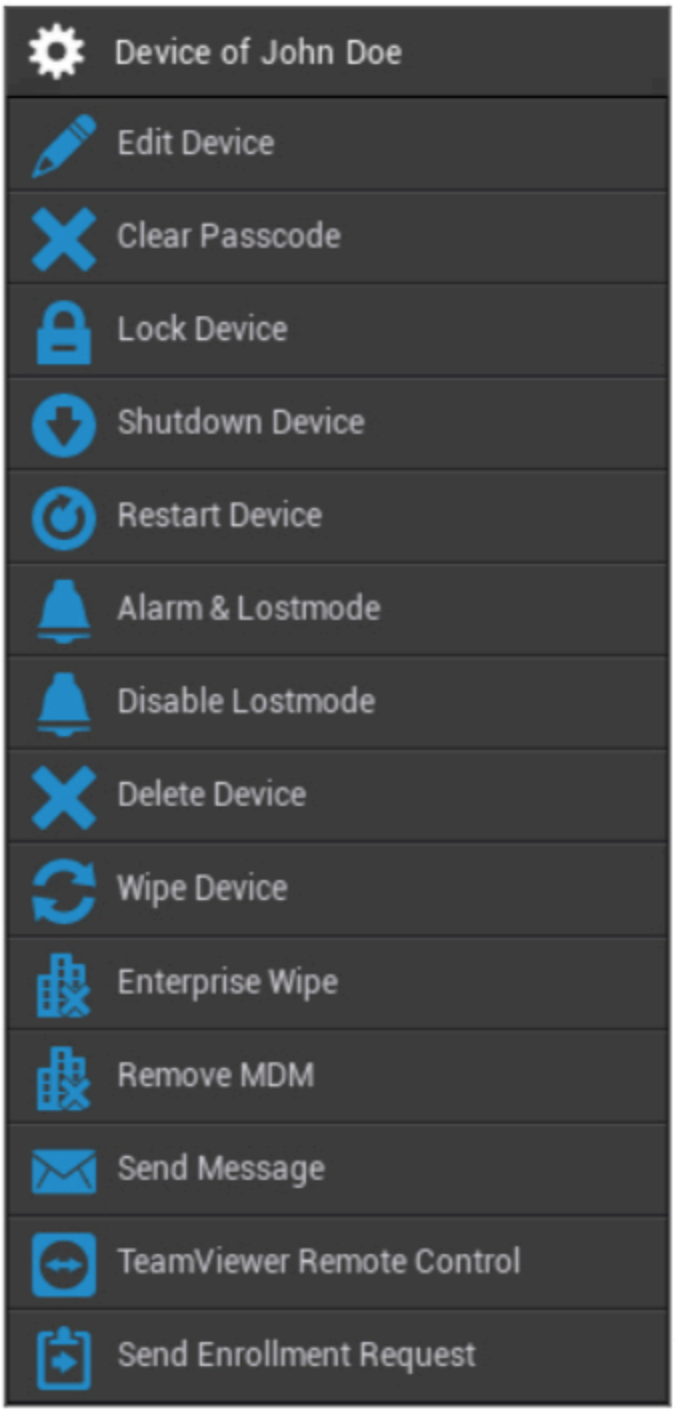
创建新分组时，该配置将设为默认值。

还可使用 "空配置文件 "配置，该配置相当于一个空配置文件，意味着最终不会在最终用户设备上执行任何新配置。

移动管理中的设备管理

选择设备后，可以通过 "齿轮 "执行各种任务。根据操作系统平台（iOS、安卓企业版、安卓、Windows Mobile、Windows 10）的不同，这些任务也有所不同。

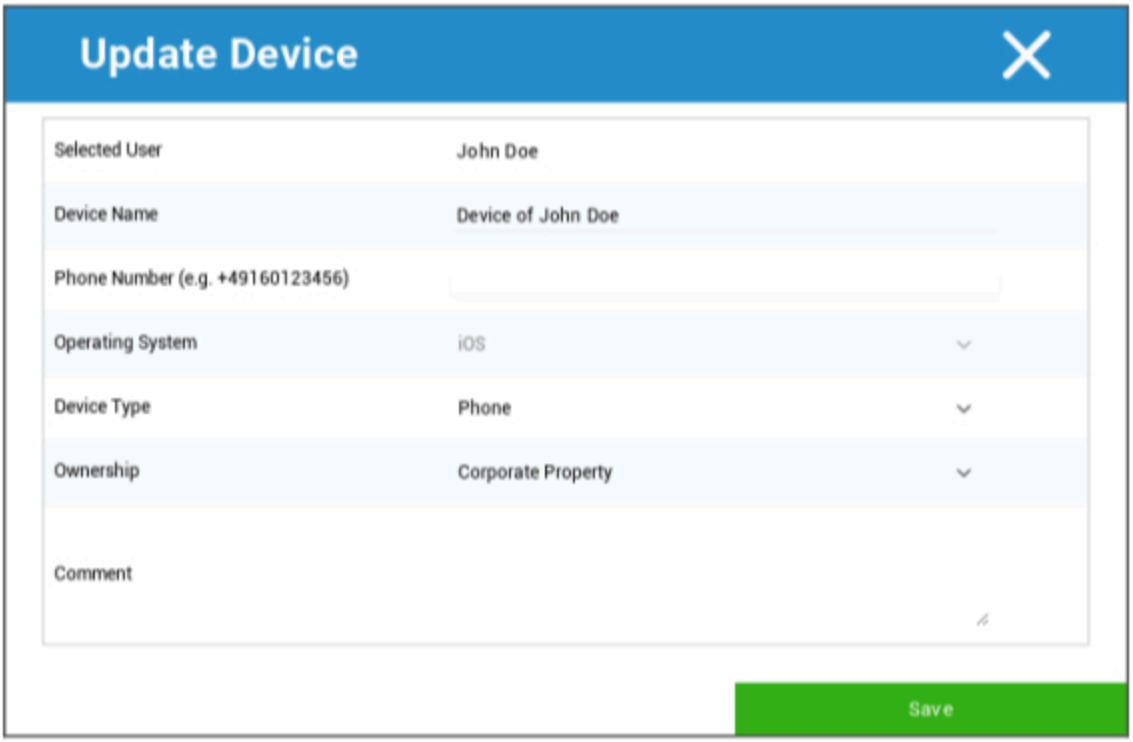
IOS



编辑设备	编辑设备
清除密码	设备密码已清除
锁定装置	锁定设备（锁定屏幕）
关机装置	关机装置

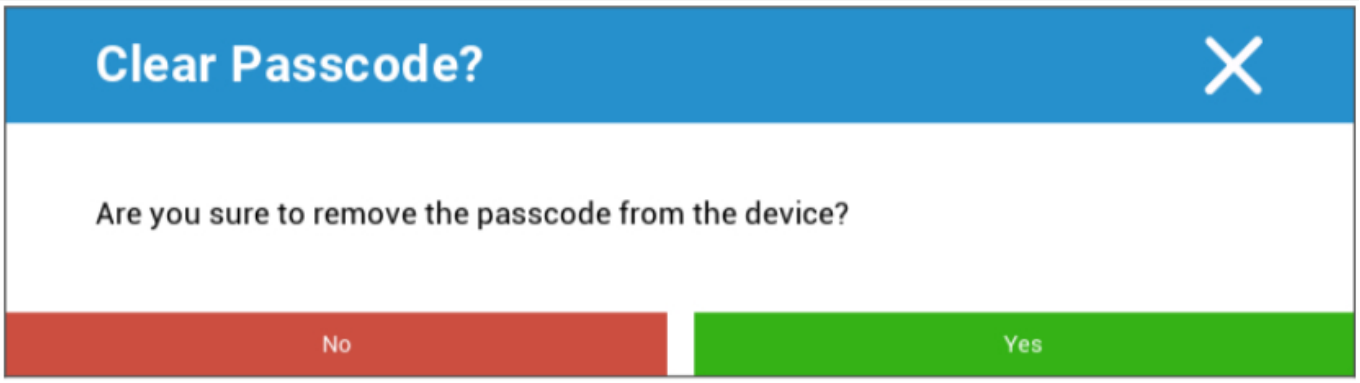
重启设备	重启设备
警报和丢失模式	启动警报和丢失模式
禁用丢失模式	禁用丢失模式
删除设备	从 AppTec 移除设备
擦拭设备	将设备恢复出厂设置
企业擦拭	删除 AppTec360 提供的信息、应用程序和配置文件（设备与 MDM 分离）
移除 MDM	
发送信息	向设备发送推送通知 信息将显示在 AppTec360 应用程序中（信息选项卡）
TeamViewer 远程控制	使用 TeamViewer 启动远程控制会话
发送注册申请	发送（重复）注册请求

编辑设备



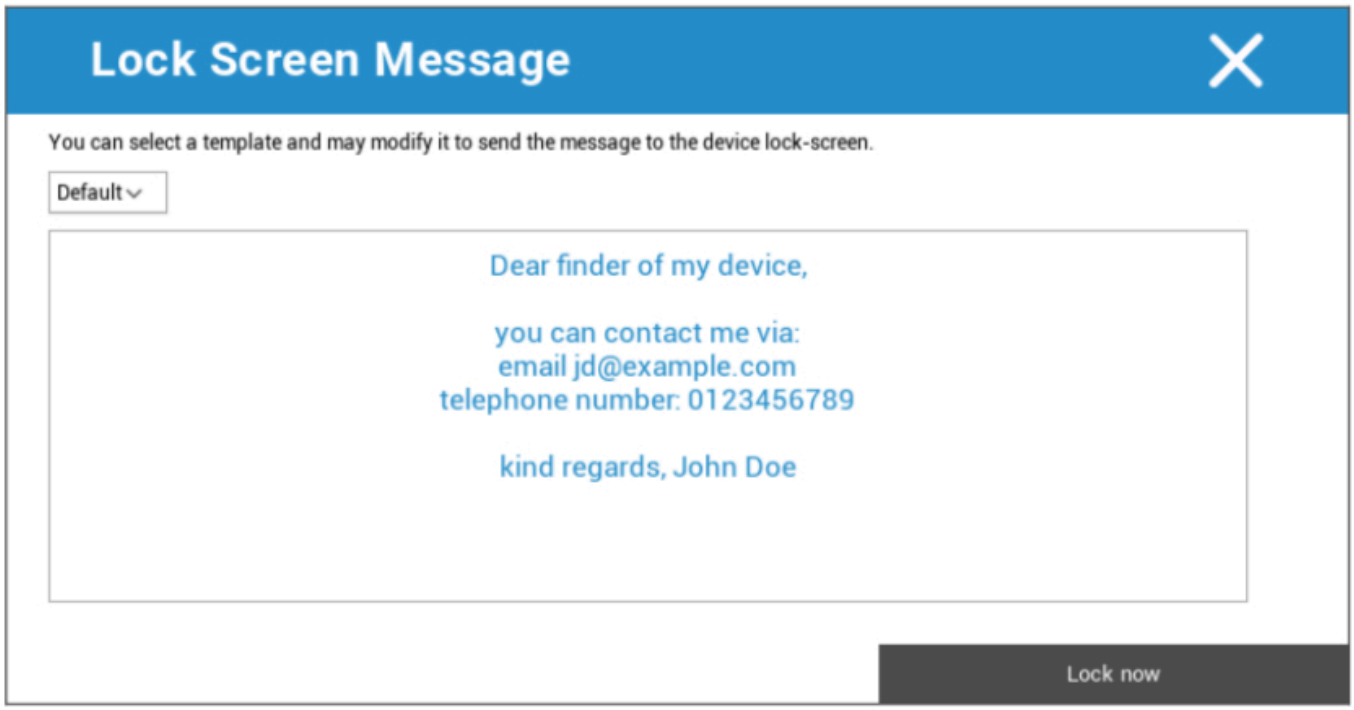
您可以在此更新设备的各种信息。

清除密码



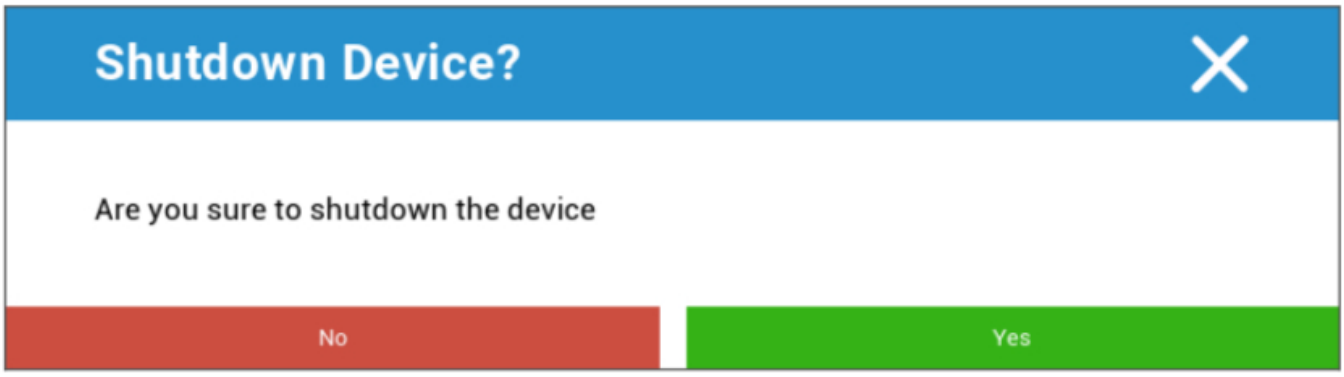
在 "清除密码 "下，您可以远程删除设备上的密码。随后，系统会提示用户输入新密码（取决于密码准则）。

锁定装置



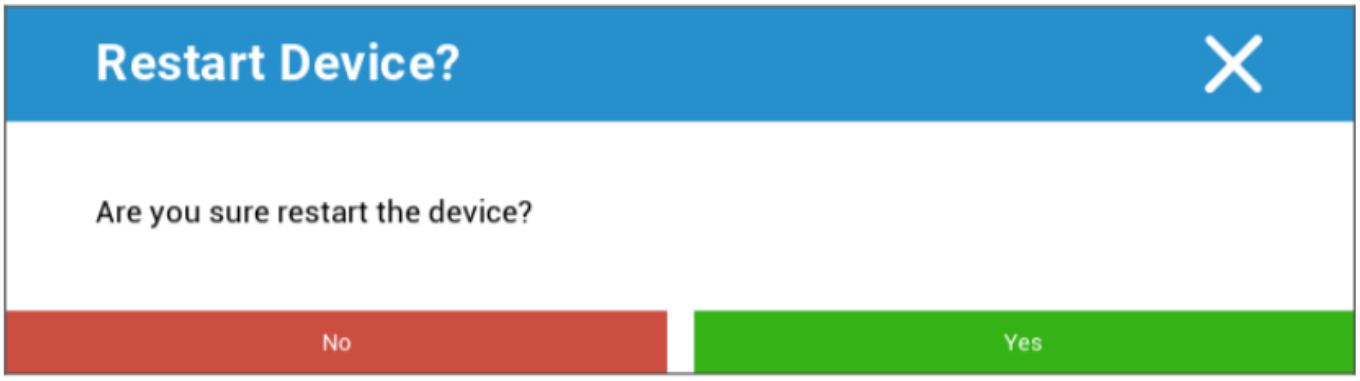
这里会向终端用户设备发送锁定命令（锁定屏幕）。

关机装置



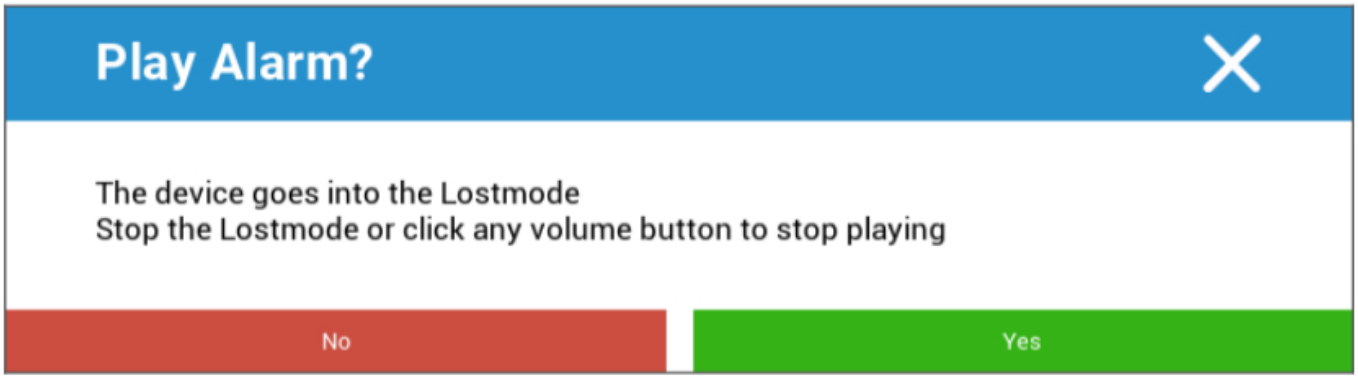
这里会向终端用户设备发送关机命令。

重启设备

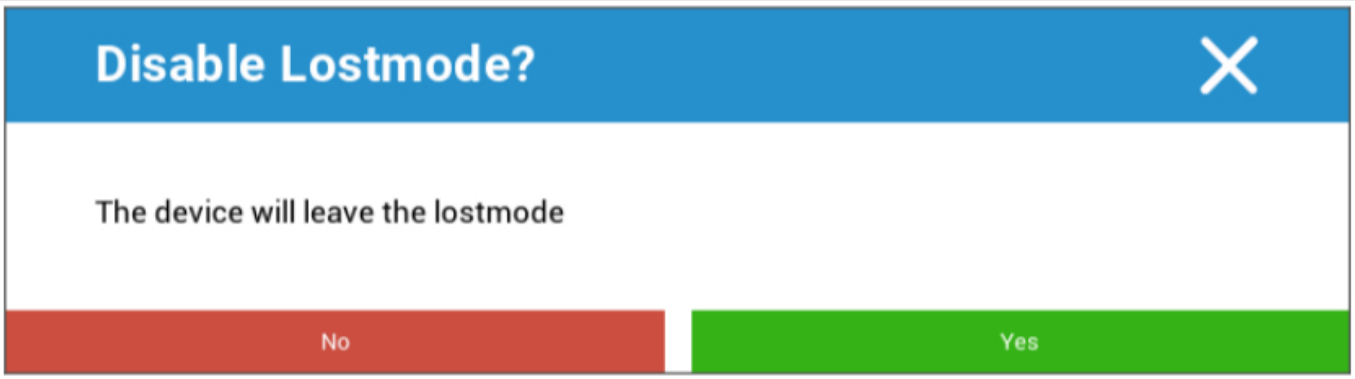


这里会向终端用户设备发送重启命令。

警报和丢失模式 | 禁用丢失模式



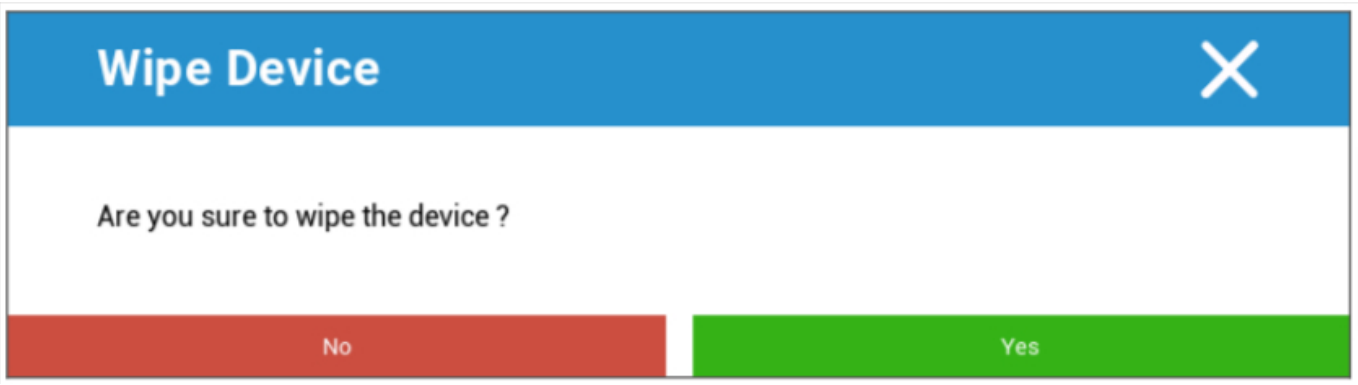
在这里可以将设备设置为 Lostmode（丢失模式），该模式将设备设置为持续播放闹钟声音。按下设备的任何音量按钮或远程点击 "禁用 Lostmode"，即可停止 Lostmode：



删除设备

在此可执行删除命令。您可以再次决定是只从 AppTec360 中删除设备（"从系统中删除"），还是从 AppTec360 中删除设备并将其恢复到出厂设置（"擦除并删除"）。

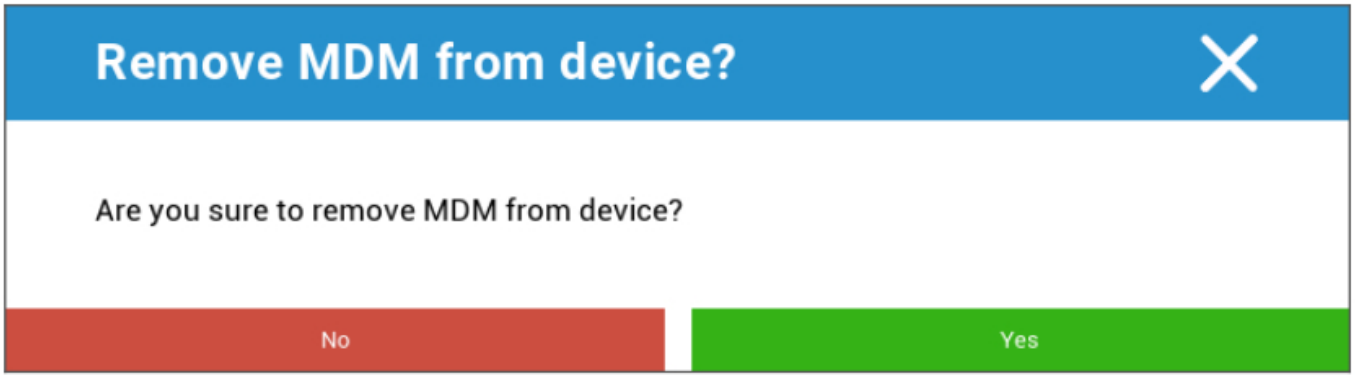
擦拭设备



在 "擦除设备 "下，您可以对设备进行彻底擦除。设备将恢复出厂设置。

企业擦除 | 删除 MDM

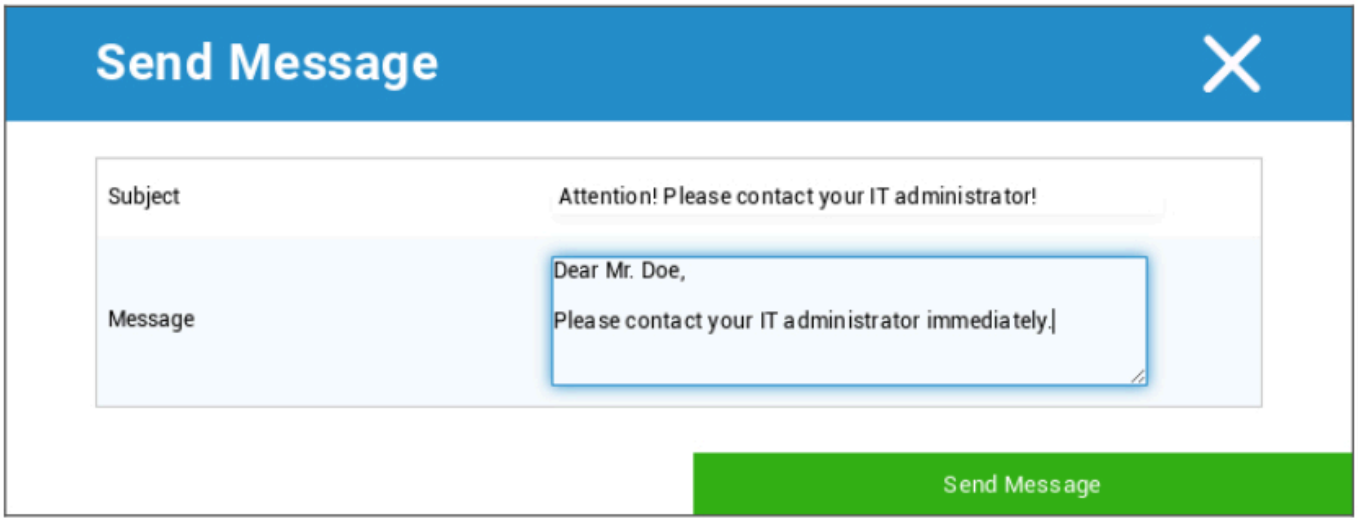
只有 AppTec360 提供的信息、应用程序和配置文件会被删除。这样，最终用户设备上就不再有公司数据。私人区域不受影响，继续保留在最终用户设备上。



通过 "删除 MDM"，您可以删除最终用户设备上的 MDM 配置文件以及 AppTec 提供的所有其他项目。

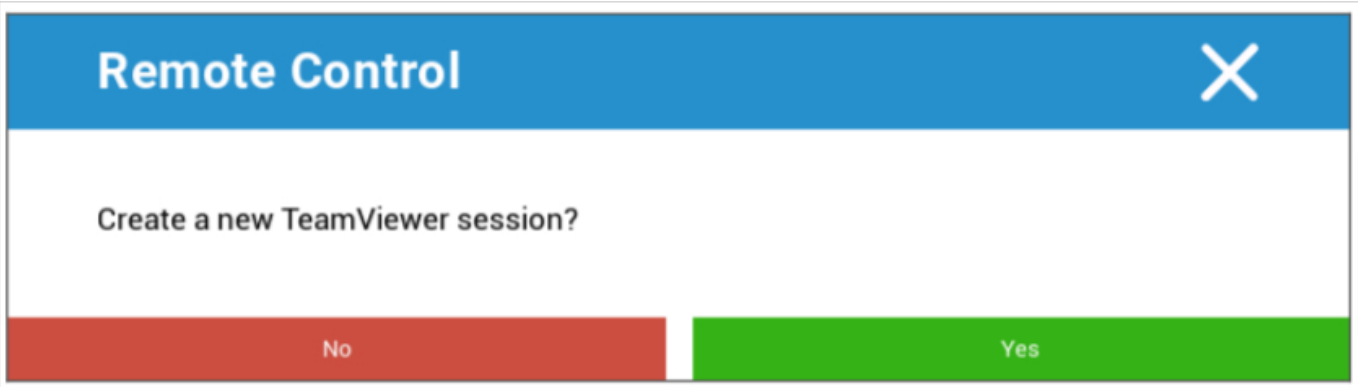
该命令执行与 "企业擦除 "相同的操作。

发送信息



您可以在此向相应设备发送推送通知。

TeamViewer 远程控制



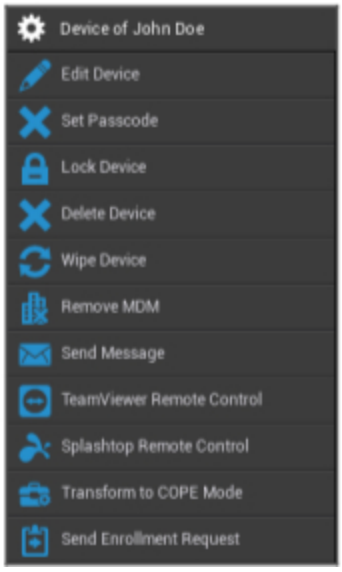
在这里可以启动 Teamviewer 远程控制会话。

发送注册申请

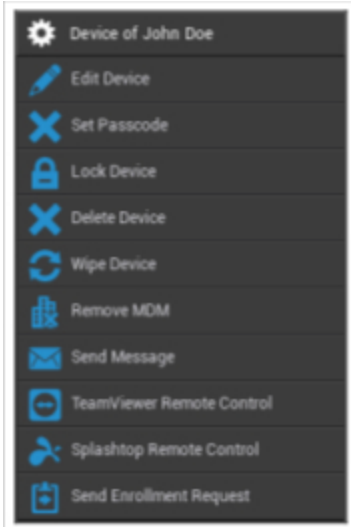
通过 "发送注册请求"，您可以向相应用户发送（再次）注册请求。

安卓

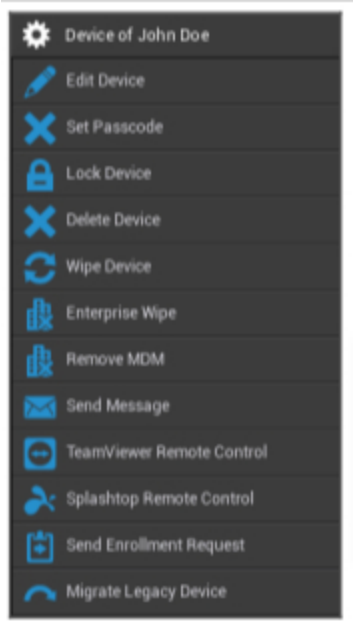
AE 全面管理设备（工作管理）



AE 工作简介（集装箱）



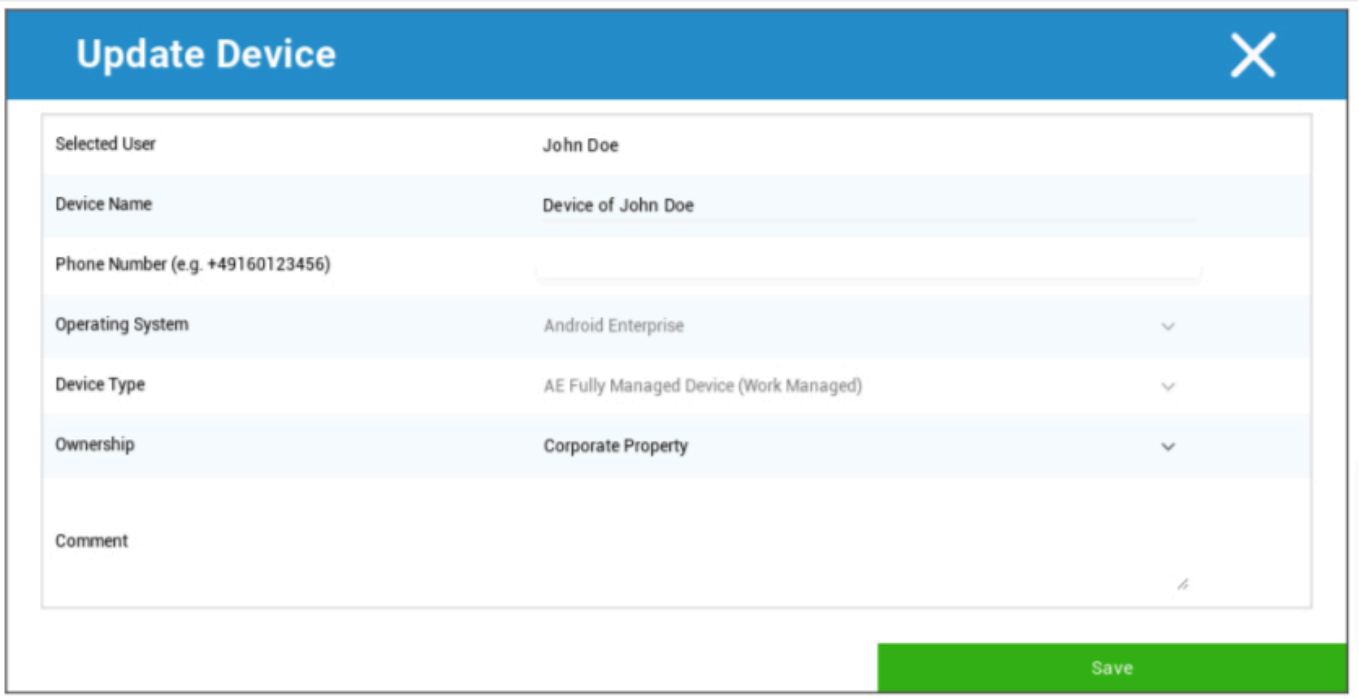
安卓手机 | 平板电脑



编辑设备	编辑设备信息
设置密码	设置设备密码
锁定装置	锁定设备（锁定屏幕）
删除设备	从 AppTec 中删除设备
擦拭设备	将设备恢复出厂设置
企业擦拭	删除由 AppTec360 提供的信息、应用程序和配置文件（设备将与 MDM 分离）
移除 MDM	
发送信息	向设备发送推送通知 信息将显示在 AppTec360 应用程序中（信息选项卡）
TeamViewer 远程控制	使用 TeamViewer 为该设备启动远程控制会话
Splashtop 遥控器	使用 Splashtop 为该设备启动远程控制会话
转换为 COPE 模式（仅适用于 AE 完全托管设备（工作托管））。	在此 AE 完全管理（工作管理）设备上创建工作配置文件
发送注册申请	发送（重复）注册请求
迁移旧设备（仅适用于使用设备所有者模式供应注册的安卓手机/平板电脑）	将 Android 手机/平板电脑配置文件迁移到 AE 完全托管设备（工作托管）配置文件

编辑设备

您可以在此更新各种设备信息。



选定用户	设备用户
设备名称	设备名称
电话号码	设备电话号码
操作系统	安卓企业 安卓
设备类型	安卓企业： • AE 全面管理设备（工作管理） • AE 工作剖面模式（仅限集装箱） • 带工作配置文件的 AE 完全托管设备 (COPE) 安卓 • 电话 • 平板电脑
所有权	公司 = 公司财产

	雇员 = 雇员属性
评论	设备的其他说明

清除密码

在此可以删除所选设备上的设备密码。默认情况下，Android 设备的密码将设置为 "123456"--用户可以也应该在之后进行更改。

锁定装置

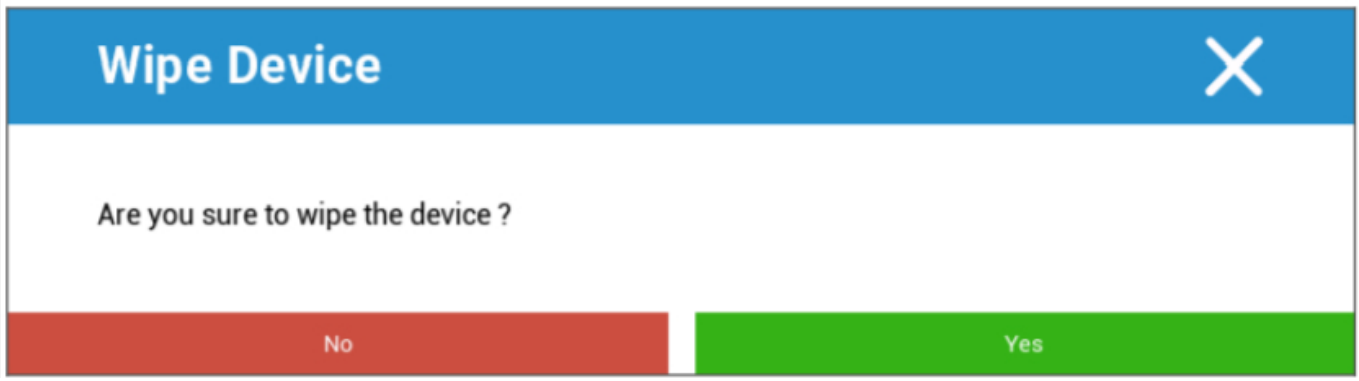
这里将向设备发送锁定设备命令（锁定屏幕）。

删除设备

在此可执行删除命令。您可以再次决定是只从 AppTec360 中删除设备（"从系统中删除"），还是从 AppTec360 中删除设备并恢复出厂设置（"擦除并删除"）。

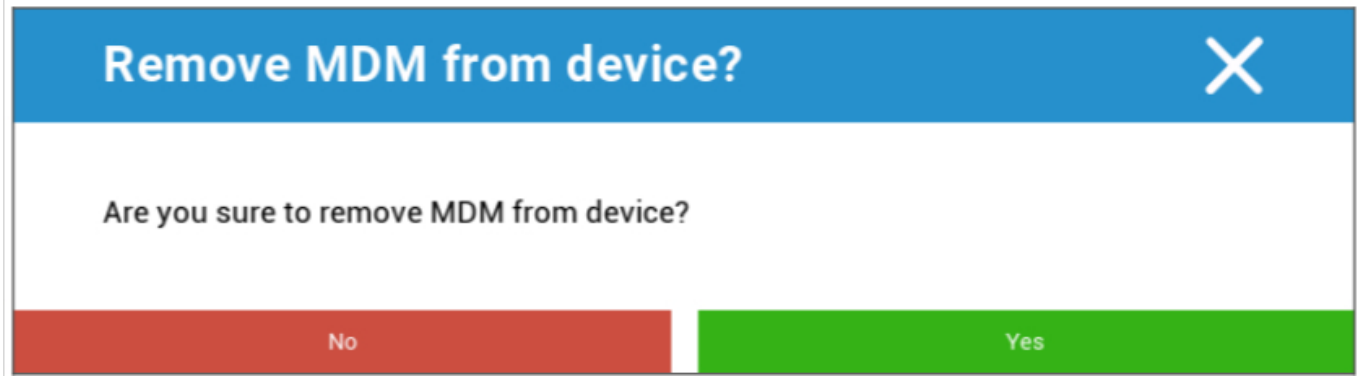
擦拭设备

在 "擦除设备 "下，您可以对设备进行彻底擦除。然后设备将恢复出厂设置。



此外，如果设备包含 SD 卡，则可以擦除 SD 卡。将 "也擦除 SD 卡？"设置为 "开启"。

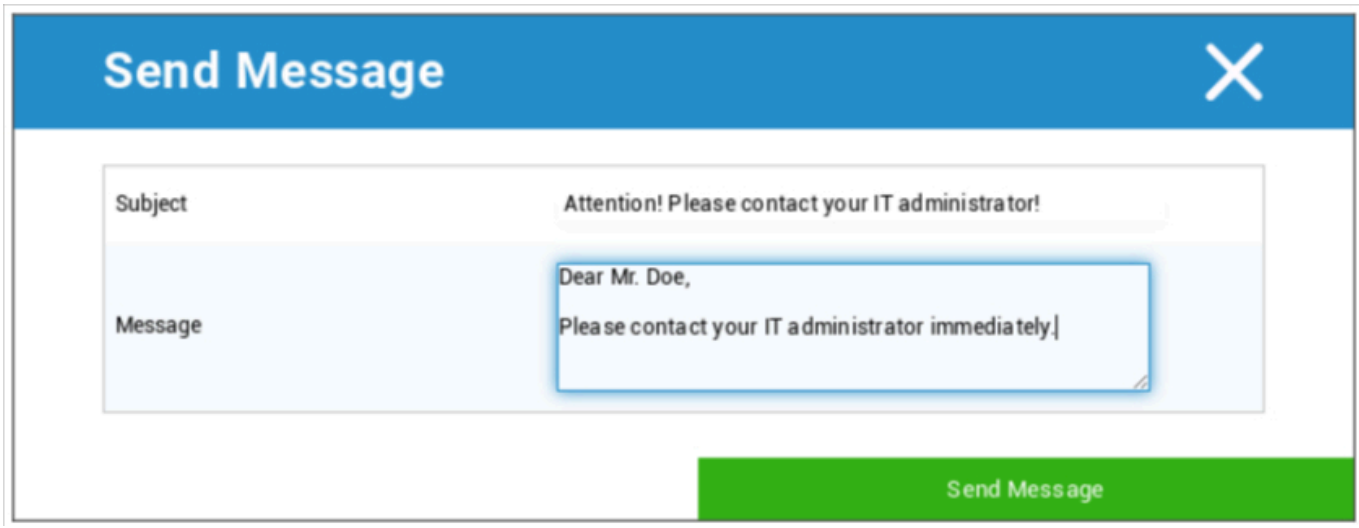
移除 MDM



这是建议采用的方法，用于创建与 MDM 的分离。

只有 AppTec360 提供的信息、应用程序和配置文件会被删除，这意味着最终用户设备上将不再有所有企业数据。但是，私人领域不受影响，将继续保留在最终用户设备上。

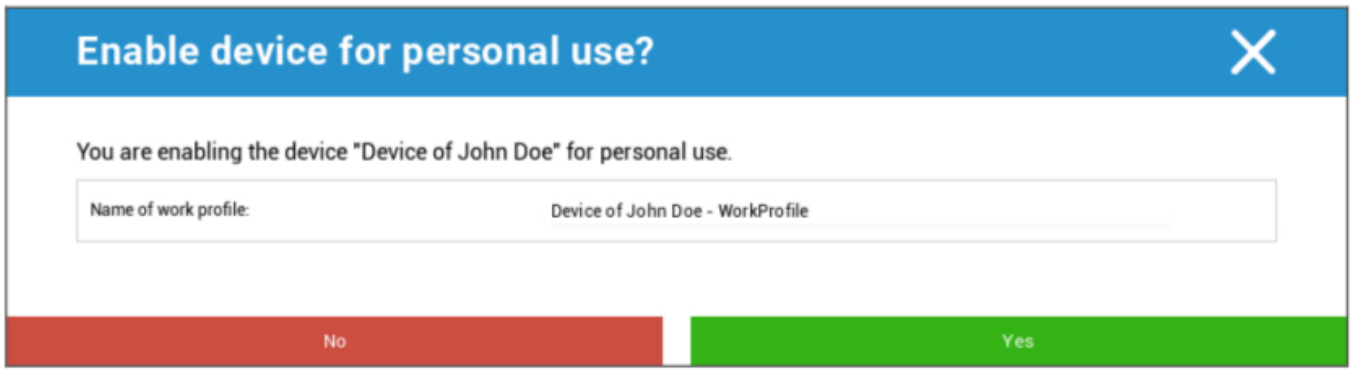
发送信息



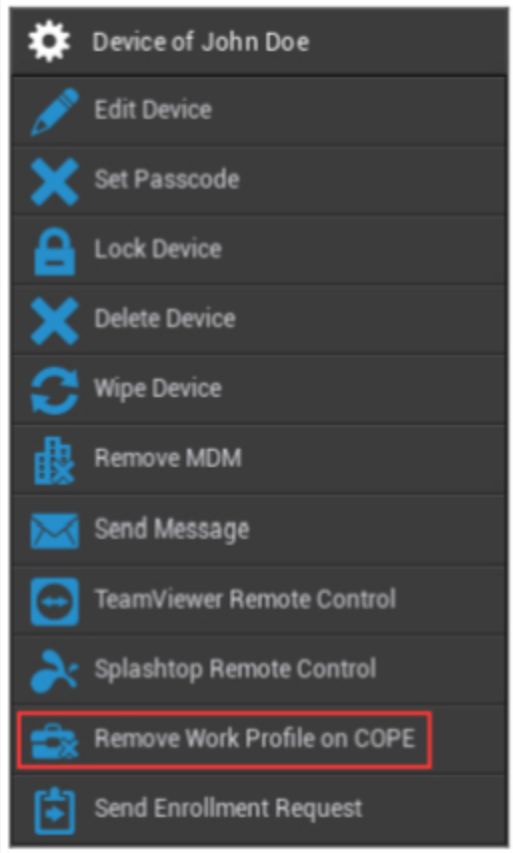
在这里，您可以向相应的终端用户设备发送推送通知。

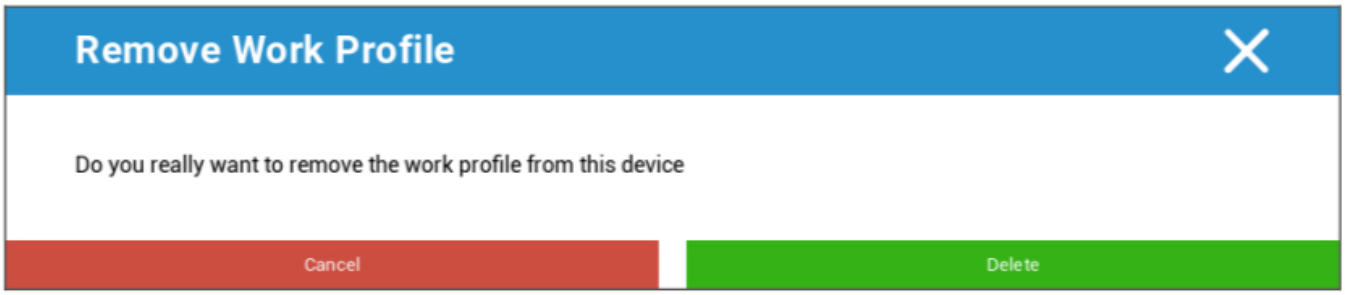
转换为 COPE 模式

在此 AE 完全管理（工作管理）设备上创建工作配置文件



将设备转换为 COPE 模式后，您可以单击齿轮选项**Remove Work Profile on COPE（删除 COPE 上的**工作配置文件）来删除**工作配置文件：**




Remove Work Profile
Do you really want to remove the work profile from this device
Cancel
Delete

发送注册申请

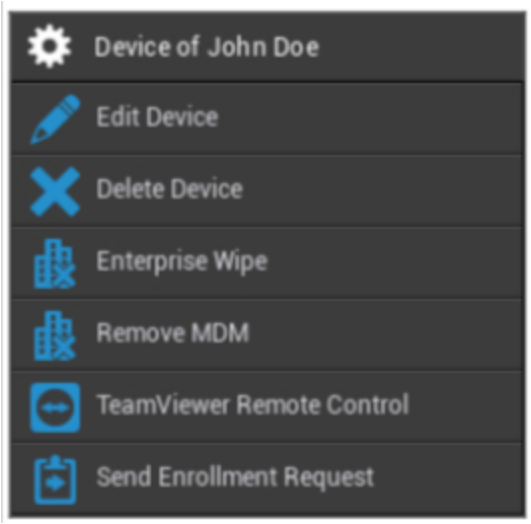
通过 "发送注册请求"，您可以（再次）向相应用户发送注册请求。

请注意，只有最新的注册申请才有效。

迁移传统设备

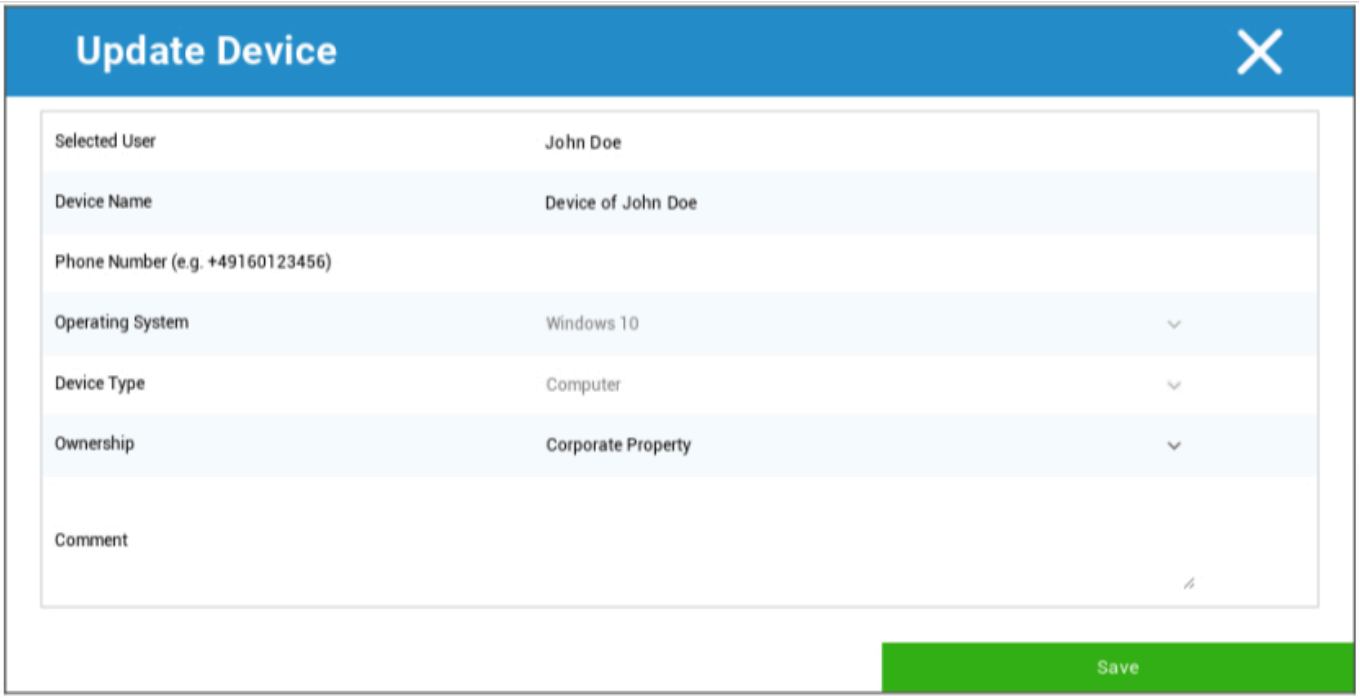
将 Android 手机/平板电脑配置文件迁移到 AE 完全托管设备（工作托管）配置文件

视窗



设备名称	所选设备的名称
编辑设备	编辑设备
删除设备	从 AppTec 移除设备
企业擦拭	AppTec360提供的信息、应用程序和个人资料将被删除
移除 MDM	
TeamViewer 远程控制	使用 TeamViewer 远程控制设备
发送注册申请	发送注册请求（再次）

编辑设备

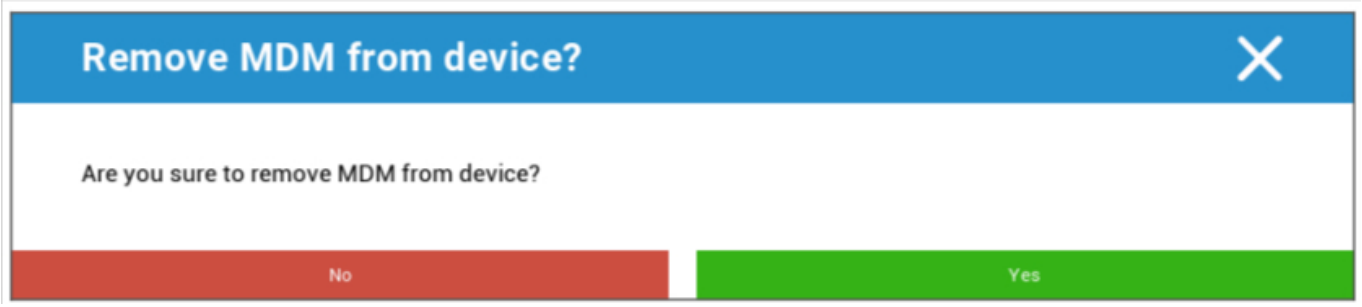


您可以在此更新设备的各种信息。

删除设备

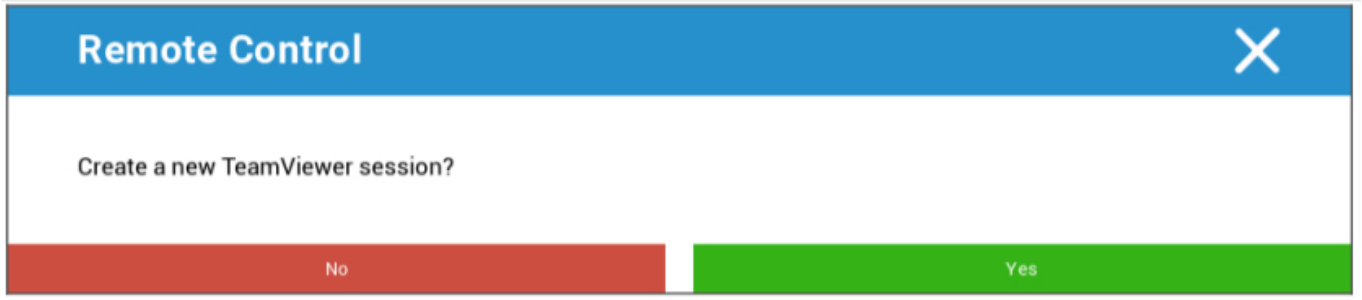
在这里可以执行删除命令，该命令只从 AppTec360 中删除设备。

企业擦除 | 删除 MDM



只有 AppTec360 提供的信息、应用程序和配置文件会被删除。这样，最终用户设备上就不再有公司数据。私人区域不受影响，继续保留在最终用户设备上。

TeamViewer 远程控制



您可以在此为该设备启动 TeamViewer 远程控制会话。

发送注册申请

通过 "发送注册请求"，您可以向相应用户发送（再次）注册请求。

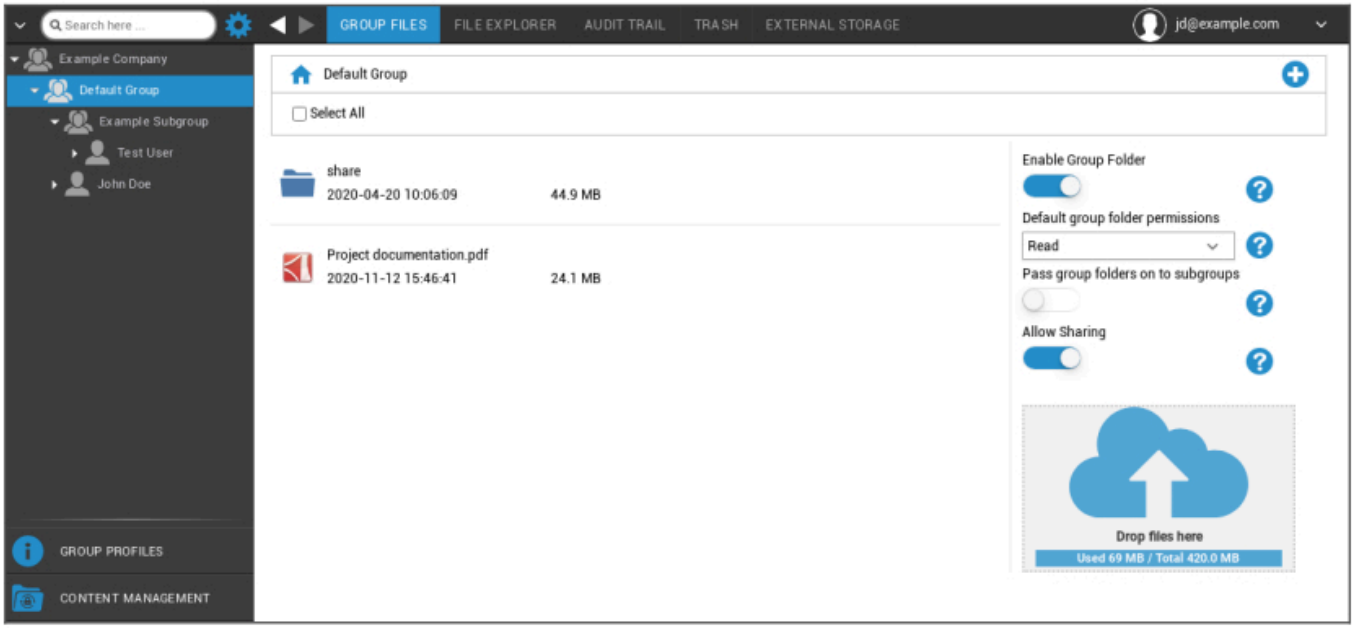
内容管理

当您在群组中时，您可以通过 "内容管理 "管理 AppTec 的 ContentBox。

有了内容盒，您就可以安全地将文档和其他企业数据分发到终端用户设备上。

组文件

"组文件 "是 ContentBox 的基本组成部分。您可以在这里进行设置、上传文件、创建新文件夹等。



通过右上角的符号，您可以创建新文件夹，并通过 "添加文件夹 "将其指定到相应的组中。

通过右上角的符号，您可以通过 "添加文件夹 "创建一个新文件夹，并将其分配给相应的组。

你可以给文件夹起任何你想要的名字。

通过 "上传文件"，您可以上传数据。这里将打开您的标准资源管理器。当然，您也可以在每个（子）文件夹中执行这两项操作。

通过左上角的符号，您可以返回主菜单。

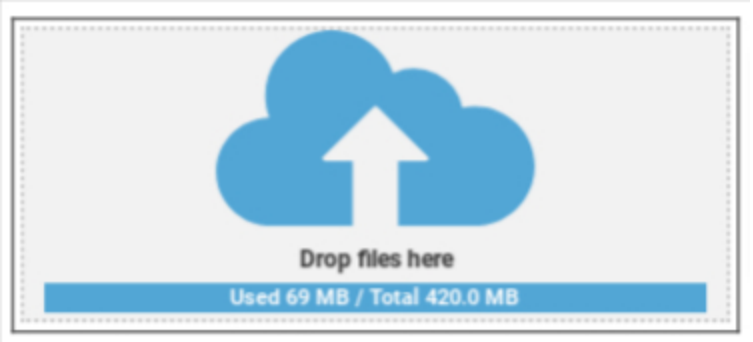
您可以选择多个文件夹和文件，然后点击 "下载 "将其下载，或者点击 "删除 "将其删除。

您还可以选择所有文件和文件夹，并执行 "下载 "和 "删除 "命令。

将鼠标移至文件夹或文件上时，会看到以下概览：

- 使用 "重命名"，可以重命名文件夹/文件
- 使用 "下载"，您可以下载文件夹/文件
- 使用 "删除 "可以删除文件夹/文件

启用组文件夹	如果激活，组内所有成员都可以访问相应文件夹
默认组文件夹权限	选定组中用户的权限： 读取 = 只读权限 更新 = 更新权限 创建 = 创建权限 删除 = 删除权限
将组文件夹传递给子组	如果激活，各分组可访问父数据文件
分组权限	所选子组中用户的权限： 读取 = 只读权限 更新 = 更新权限 创建 = 创建权限 删除 = 删除权限
允许共享	如果激活，用户可通过链接共享文件



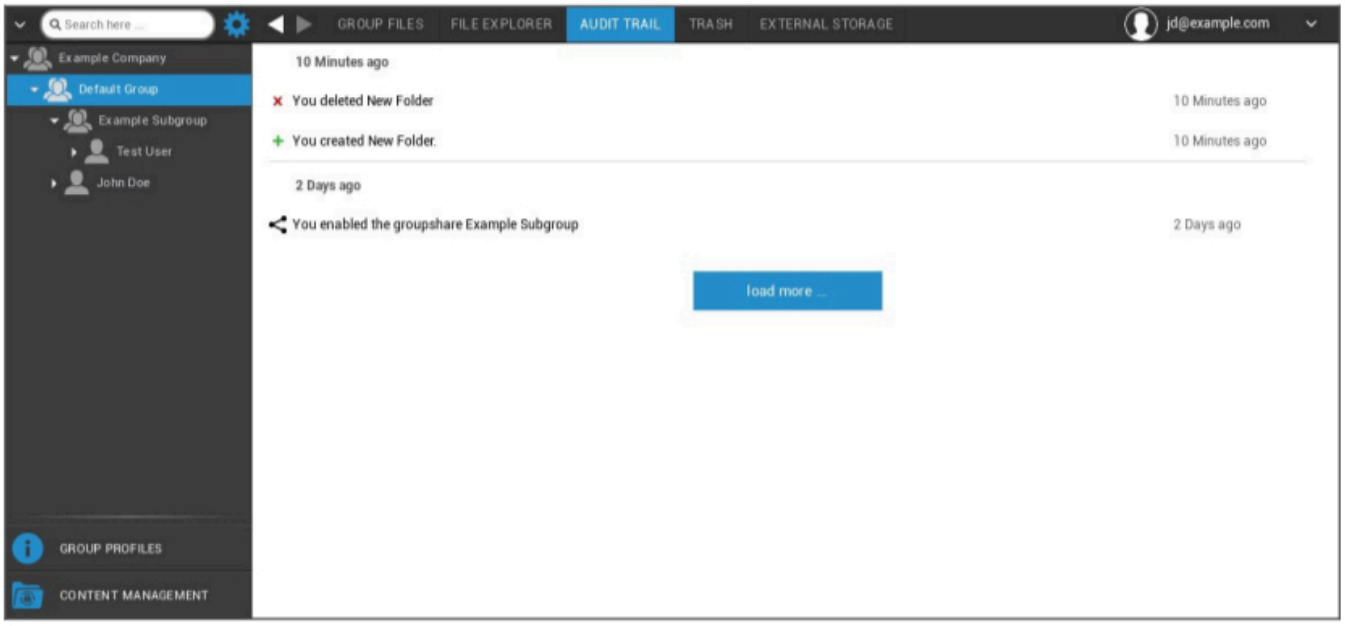
为了上传文件，您可以使用此字段，通过拖放方式将文件拉到此窗口。您也可以点击该字段，在 Internet Explorer 的帮助下选择并上传文件。

文件资源管理器

使用 "文件资源管理器"，你可以管理所有文件夹和文件，无论它们存放在哪个组。

您还可以找到在 "组文件 "中学到的设置和按钮。

审计跟踪



在 "审计跟踪 "中，你可以从历史记录中看到哪个用户创建、删除或共享了什么。这样就可以随时确定公司数据的使用情况。

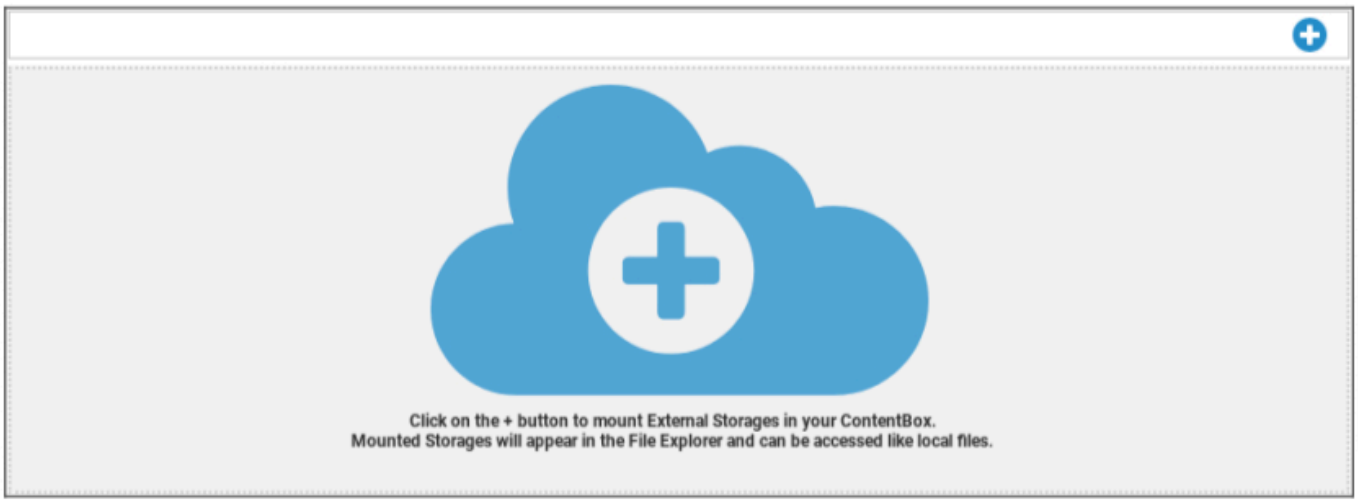
垃圾

如果你（不小心）删除了某些内容，你可以查看 "垃圾桶 "中的文件夹和文件，并根据自己的意愿恢复它们。

- 使用 "Undelete "可以恢复数据/文件夹。
- 使用 "删除 "可以永久删除数据/文件夹，但必须再次确认删除命令。

请注意，垃圾中正在使用的存储容量会减少可用的 "总空间"，这是 ownCloud 的要求。

外部存储



在 "外部存储 "标题下，您可以连接外部存储。

有了这个符号，就可以增加（额外的）存储空间。

类型	亚马逊 S3、FTP、SFTP、ownCloud、WebDAV、Windows Share、SharePoint

亚马逊 S3	
显示名称	显示名称
访问键	访问键
秘钥	安全密钥
水桶	已分配给您的子文件夹的明确标识
主机名（可选）	主机名（可选）
端口（可选）	端口（可选）
地区	地区（可选）
启用 SSL	启用 SSL
启用路径样式	清除分配给您的路径地址

文件传输协议	
显示名称	显示名称
主持人	主机地址
用户名	用户名
密码	密码
根	主菜单
安全 ftps://	

SFTP	
显示名称	显示名称
主持人	主机地址
用户名	用户名
密码	密码
根	主菜单

自有云	
显示名称	显示名称
网址	ownCloud URL
用户名	用户名
密码	密码
远程子文件夹	标准文件夹
安全 https://	

WebDAV	
显示名称	显示名称
网址	WebDAV URL
用户名	用户名
密码	密码
根	主菜单
安全 https://	
窗口共享	即将支持 Windows Share
SharePoint	即将支持 Microsoft SharePoint

审计日志

这里有一个日志，记录在 MDM 控制台中执行的操作信息。

通过筛选器图标，您可以对显示的列表进行筛选。

通过下拉菜单 "**每页**显示的项目"：您可以选择列表中每页显示的项目数量。

采取的行动/更改的设置	采取的行动/更改的设置
价值	已采取的行动/已更改的设置的值
用户	执行操作/更改设置的用户名
日期	执行此操作/更改此设置的时间戳
路径/类型	执行该操作/更改该设置的路径

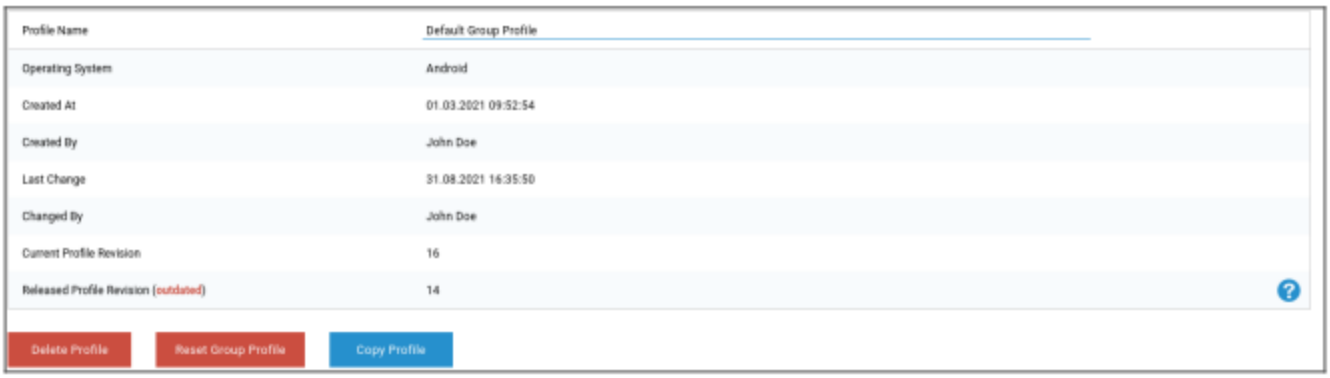
iOS 配置

一般情况

根据您当前选择的是组还是设备，显示屏及其子点有所不同，请仔细留意！

组概况概览（仅适用于组级）

打开群组简介时，您将看到简介的快速概览



简介名称	个人资料名称（可在此处更改）
操作系统	配置文件适用的操作系统
创建于	创建时间
创建者	个人资料创建者
最后的变化	最后一次更改配置文件的时间
已更改	最后更改的账户
当前的简介修订	修订已保存的配置文件状态
已发布的简介修订版	已分配的配置文件修订版（"立即分配"）。如果标签文字后面显示"（已过期）"，则表示您已经保存了配置文件，但尚未分配，因此设备仍将获得旧版本。

一般信息

如果您直接使用设备，您将收到所选设备的简要概述。

设备名称	设备名称
电话号码	设备电话号码
模型	型号
操作系统	操作系统
序列号	设备序列号
设备所有权	公司或私人设备 企业 = 企业设备 员工 = 私人设备
设备类型	设备类型（平板电脑或手机）
越狱	如果设备已越狱
监督	指示该设备是否为受监控设备
符合要求	如果违反了任何准则
最后查看	设备上次与 AppTec360 服务器通信的状态

设置

这些设置包括设备名称和预定义背景。

将设备命名为系统名称	AppTec360 控制台（左侧层次结构）中发布的名称将与相应最终用户设备上的名称相同（可在设备设置中查看）。
使用自定义壁纸（仅限受监控设备）	在这里，您可以预先定义应在终端用户设备上显示的背景（例如，用于设备的企业品牌类型）。 仅在监控模式下可用！
自动更新操作系统	强制更新操作系统（如果有）。仅适用于处于监控模式的 DEP 设备。
自定义字体	您可以在此添加自定义字体。
名称	可选项。字体的用户可见名称。安装后，该字段将被字体的实际名称取代。
字体	上传字体文件（.otf 或 .ttf）。

配置修订

在此，您将看到设备指定了哪个组配置文件。

如果点击群组配置文件，就可以直接进入配置文件并进行设置。

使用该符号，可以将已分配的应用程序还原为群组配置文件的设置。

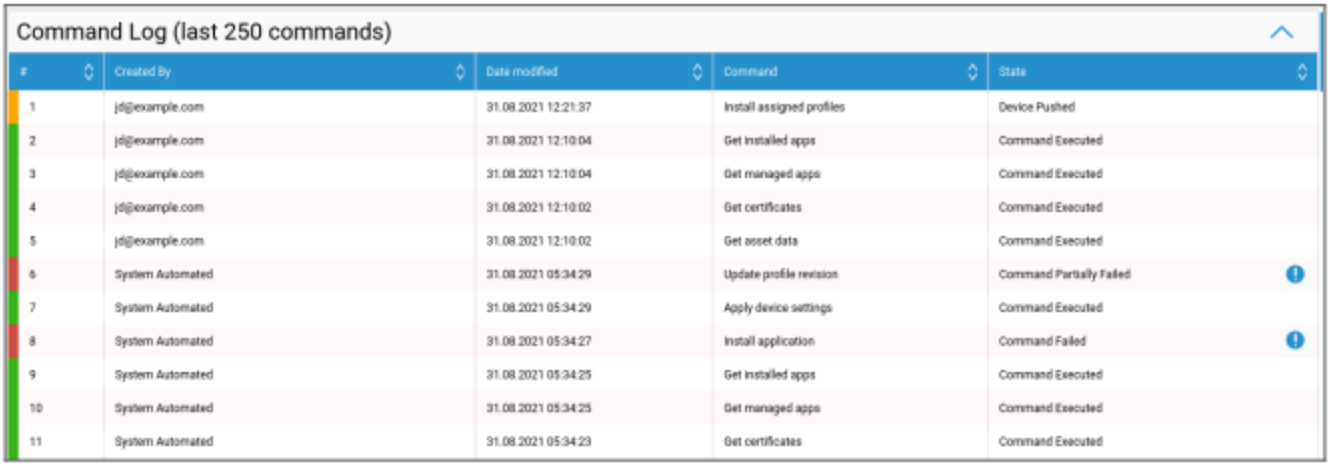
通过该符号，您可以重置设备配置文件，使其没有任何设置。

"最新版本可用 "表示组配置文件已更改并保存，但尚未分配。必须在组级别上使用 "立即分配 "来分配组配置文件，才能将更改应用到设备上。

设备日志（仅限设备级）

命令日志

在这里，您可以查看为设备发出的命令及其状态。



系统自动 "创建的命令由系统自动创建。

可能的命令状态

设备已推送	推送请求已发送至推送服务（如 APNS），以通知设备连接回 EMM 服务器。
创建命令	该命令已在系统中创建。
发送命令	设备与服务器连接后，命令被发送到设备。
命令已执行	命令已成功执行。
命令失败	命令失败。*
命令部分失败	根据设备操作系统的不同，有些命令可能会被组合在一起。 其中，该命令组的某些部分出现故障。*
命令已执行，但最终失败	命令已执行，但也可能没有执行。
命令重发	命令被用户重新推送。
弃用	命令被丢弃。例如，该命令被其他命令取代，或设备重新注册，旧命令被删除。

如果信息后面有感叹号，则可以用光标悬停在图标上获取更多信息。

资产管理（仅限设备级）

资产管理（仅限设备级）

设备信息

模型	设备型号
操作系统	操作系统
操作系统版本	操作系统版本
序列号	序列号
UDID	设备 UDID
设备名称	设备名称
监督	显示设备是否受监控
电池状态	电池状态

无线网络

IP 地址	设备 IP 地址
WiFi MAC	WiFi MAC 地址

细胞

现状	状态（存在 SIM 卡）
电话号码	电话号码
漫游状态	当前漫游状态
漫游（语音/数据）	语音/数据漫游状态
IP 地址	IP 地址
IMEI	IMEI 号码
运营商/承运商	手机服务提供商
SIM 卡运营商网络	SIM 卡运营商网络
载体版本	载体版本
调制解调器固件	调制解调器固件
目前的 MCC/MNC	参见 "SIM MCC/MNC
SIM MCC/MNC	移动国家代码是国际电联根据 E.212 标准确定的国家标识，与移动网络代码 (MNC) 一起用于识别蜂窝网络（= 国家代码）。 因此，当您进入另一个蜂窝网络时，"当前 MCC/MNC "和 "SIM MCC/MNC "是不同的。

蓝牙

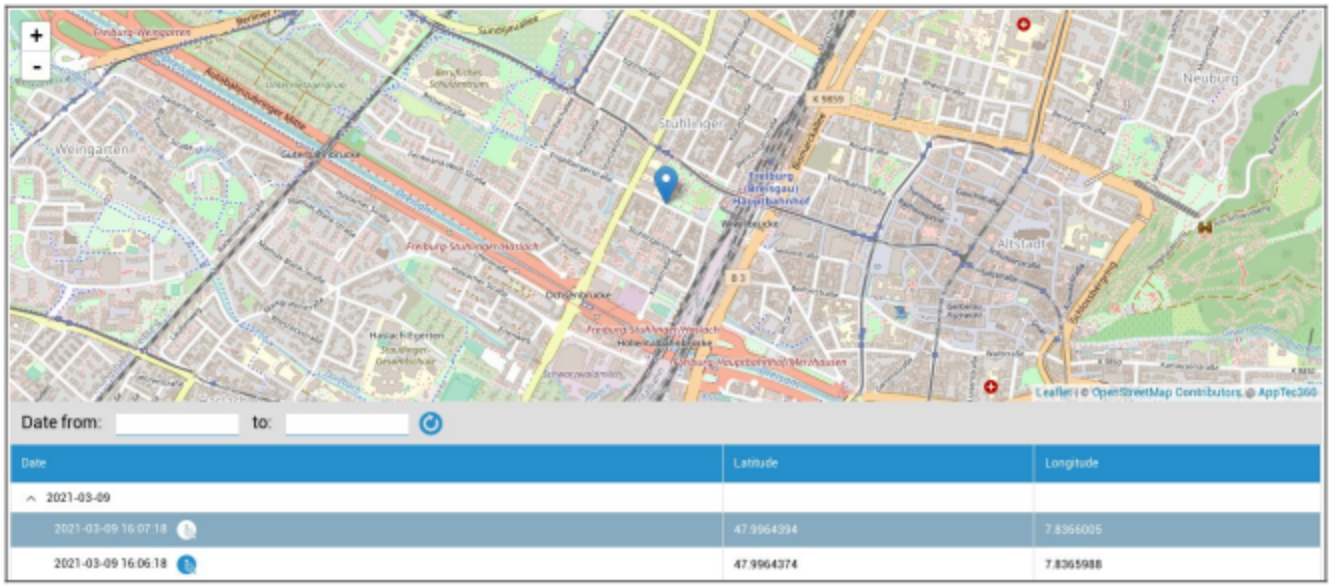
蓝牙 MAC	蓝牙 MAC 地址

安全管理

防盗（仅限设备级）

GPS 信息（仅限设备级别）

在这里可以评估设备当前/最后的位置。本地化可以使用一个或两个密码进行保护 - 请参阅 "常规设置" - "隐私" - "GPS 访问"：常规设置 - 隐私 - GPS 访问



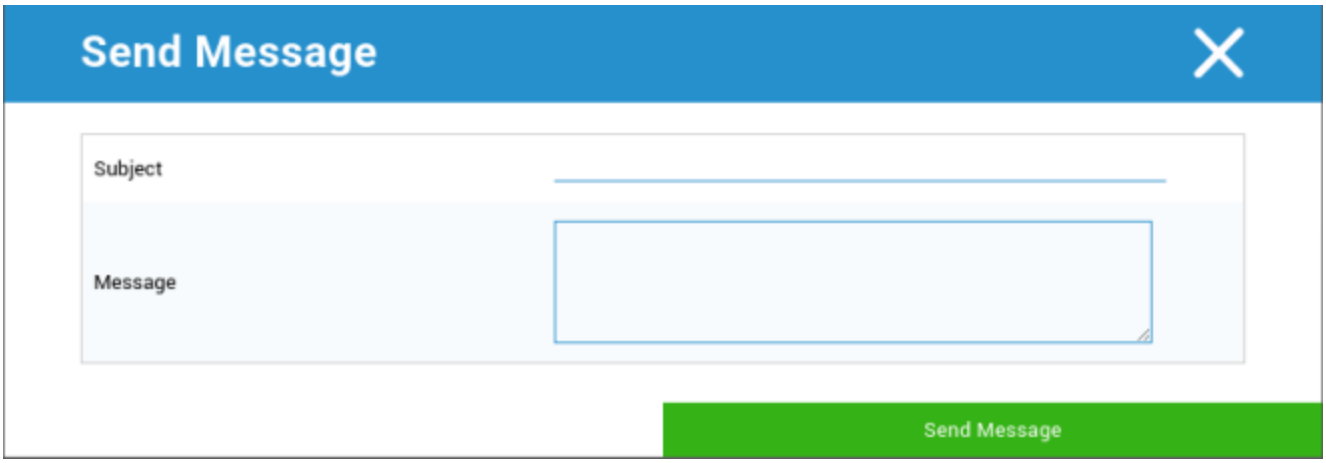
擦除和锁定（仅限设备级别）

在 "擦除和锁定 "下，您可以执行以下三项操作：

全面擦拭	设备恢复出厂设置（删除公司和个人数据）
企业擦拭	只从最终用户设备中删除企业数据（由 AppTec 提供的所有应用程序、数据等）
锁定屏幕	屏幕锁已激活，只需使用设备密码/PIN 解锁设备即可
取证锁定（仅限受监控设备）	如果使用  符号激活该功能，则设备将被锁定，并显示一条无法关闭的信息。员工也无法解锁设备。 只有管理员才能在控制台中使用  符号解锁设备。
允许激活锁（仅限受监控设备）	如果激活了该功能，只要在 iCloud 设置中激活 "查找我的 iPhone"，设备就会被锁定。

信息（仅限设备级别）

通过以下窗口，您可以填写主题和信息，并将其发送到最终用户设备：



安全配置

密码

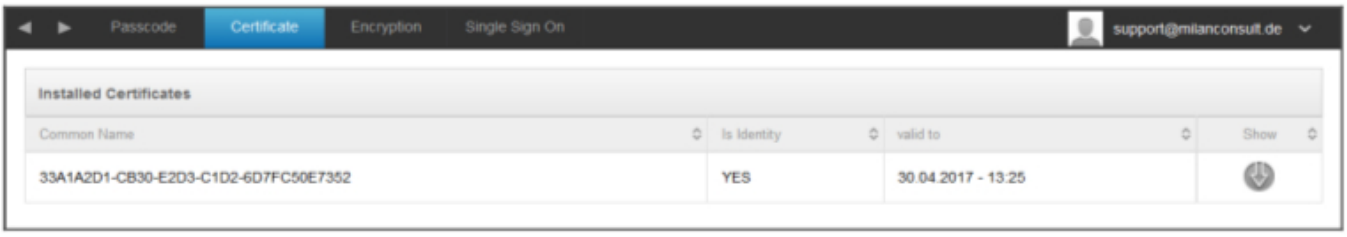
您可以在此设置设备密码

允许停用代码	激活此设置后，不会提示输入密码 密码一经设置，就不能取消
允许简单值	允许用户使用相同、递增和递减的数字字符串（如 1234、1111）
要求字母数字值	密码必须至少包含一个字母
最小密码长度	最小密码长度
最少复合字符数	密码中字母数字符号的最少数量
密码最长有效期	必须更改密码的天数
最大自动锁定	锁定设备的最长时间
设备锁定的最长宽限期	时间，之后设备进入锁定的待机状态。
最多失败尝试次数	规定在执行完全设备擦除之前，错误输入密码的频率
密码最大有效期（1-730 天）	密码最大有效期
密码历史记录（1-50 个密码）	该数字之后允许使用旧密码

点击 "垃圾桶"，打开 "密码重置 "对话框，通过该对话框可以删除遗忘的设备密码。

证书（仅限设备级）

显示设备上可用的证书



加密

要求存储加密	激活已安装的设备加密功能

单点登录

在 "单点登录 "点下，可以配置 Kerberos 身份验证。

在这里，您可以建立访问凭证和允许使用 Kerberos 标记的相应 URL/应用程序。

可在监控模式下使用	
账户名称	账户名称
校长姓名	可以分发 Kerberos 门票的唯一标识
境界	要使用的 Kerberos 领域（例如您的域）

通过符号，您可以建立更多的 URL。

用于限制此帐户的 URL 模式	可分发 Kerberos 门票的待定 URL

有了符号，您还可以建立其他应用程序。

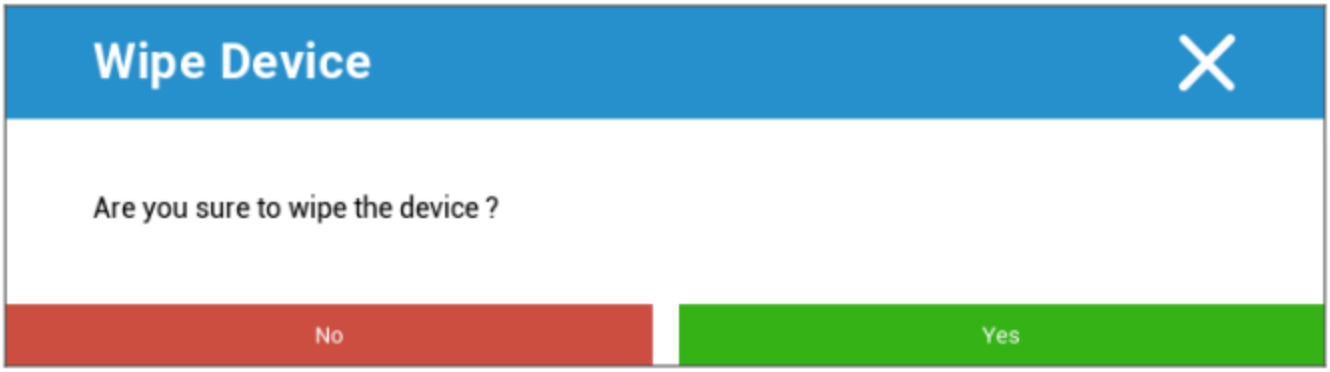
限制此帐户的应用程序	可向其分发 Kerberos 门票的应用程序待定

报废（仅限设备级）

擦除（仅限设备级）

在 "擦除 "下，可以将设备恢复出厂设置。在这里，最终用户设备上的公司和私人数据都将被删除。

点击 "减号 "后，您将收到以下信息



如果选择 "是"，则可以执行擦除操作。

在 "擦除报告 "下可显示以下项目

擦拭	进行擦拭的历史
日期	日期
现状	状态（例如擦除是否成功执行）

限制设置

设备功能

在这里，您可以阻止个别终端用户设备的功能

允许安装应用程序	允许安装应用程序
允许摄像机	允许使用摄像机
允许 FaceTime	允许 FaceTime
允许屏幕截图	允许屏幕截图
允许漫游时自动同步	允许漫游时自动同步
允许 Siri	允许 Siri
允许语音拨号	允许语音拨号
允许应用内购买	允许应用内购买
所有购买都需要 iTunes Store 密码	所有购买都需要 iTunes Store 密码
允许多人游戏	允许多人游戏
允许添加游戏中心好友	允许添加游戏中心好友
允许从托管向非托管开放	允许在非托管应用程序中打开托管应用程序中的内容
允许从非托管向托管开放	允许在托管应用程序中打开非托管应用程序中的内容
允许在锁屏中查看今日视图	激活此设置后，"今日 "视图将显示在锁定屏幕的通知中心中。
允许在锁屏中使用控制中心	允许在锁屏上使用控制中心
允许 TouchID	允许 TouchID
允许空中 PKI 更新	允许空中 PKI 更新
锁定时允许使用存折	锁定设备时允许使用存折
限制广告跟踪	这些功能会停用广告跟踪功能（例如，广告商无法使用广告跟踪功能发布个性化广告）
允许切换	允许切换
允许在聚光灯下显示互联网结果	允许在聚光灯下显示互联网结果（例如必应或维基百科）
首次配对 AirPlay 时要求输入密码	首次配对 AirPlay 时要求输入密码
Force Watch 护腕	如果激活，Apple Watch 将被迫使用 "手腕保护"（手腕识别）

允许使用 iCloud 照片库	允许使用 iCloud 照片库。如果不允许，则所有未完全从 iCloud 下载的图片都将在本地存储中删除
在监控模式下可用	
允许账户修改	允许修改 "邮件、联系人、日历
允许 AirDrop	允许 AirDrop
允许修改应用程序蜂窝	此设置阻止了允许哪些应用程序使用移动数据的设置 例如，可以在终端用户设备上手动设置该设置，然后激活该限制。
允许 Siri 从网络上查询用户生成的内容	禁止在某些网站（如维基百科）上进行网络搜索，因为每个人都可以随心所欲地进行修改
启用 Siri 亵渎过滤器	针对 Siri 的亵渎语言将受到审查
允许使用 iBook Store	允许使用 iBook Store
允许在 iBook Store 电子书商店下载情色书籍	允许在 iBook Store 电子书商店下载情色书籍
允许修改 "查找我的朋友 "设置	允许修改 "查找我的朋友 "设置
允许游戏中心	允许游戏中心
允许主机配对	控制计算机配对
允许安装配置文件	允许安装配置文件
允许移除应用程序	删除控制应用程序
允许 iMessage	允许 iMessage
允许清除所有内容和设置	允许删除所有内容和设置
允许配置限制	允许配置限制
允许播客	允许播客
允许定义查询	允许定义查询
允许使用预测键盘	允许使用预测键盘
允许自动修正	允许自动修正
允许 UI 应用程序安装	如果停用，则无法从公共 AppStore 安装应用程序（图标将不再显示）。但仍可通过 iTunes 和配置器安装应用程序
允许键盘快捷方式	如果设备连接有物理键盘，则允许使用键盘快捷方式
允许 Apple Watch 配对	禁止设备与 Apple Watch 配对，现有连接将被终止
允许修改密码	如果不允许，则无法添加、更改或删除设备密码
允许修改设备名称	确定是否可以更改设备名称的指导原则

允许修改壁纸	确定是否可以更换壁纸的指导原则
允许自动下载应用程序	如果停用，已购买的应用程序将不会自动安装到其他设备上。不适用于现有应用程序的更新
允许新闻	允许在 iOS 设备上发布新闻
允许企业应用程序信任	如果设置为 false，则防止信任企业应用程序

iCloud

在配对 iCloud 时阻止某些功能

允许备份	允许备份
允许文件同步	允许文件同步
允许照片流	允许照片流
允许共享照片流	允许共享照片流
允许云钥匙串同步	允许云钥匙串同步
允许受管应用程序存储数据	允许受管应用程序存储数据
允许同步企业图书的笔记和摘要	允许同步企业图书的笔记和摘要
允许备份企业账簿	允许备份企业账簿

安全与隐私

阻止这些与诊断数据相关的功能

允许向 Apple 发送诊断数据	允许向 Apple 发送诊断数据
允许用户接受不受信任的 TLS 证书	允许用户接受不受信任的 TLS 证书
强制加密备份	强制加密备份

自带设备

内置 iOS 安全系统（容器）

iOS 总是能够区分受管（商业）和非受管（私人）。来自 MDM 系统的一切都被视为受管。例如，如果您通过 MDM 安装应用程序或配置 Exchange 帐户，iOS 就会将其视为受管。

设备上手动配置/安装的其他所有内容都将被视为非托管。例如，用户自行安装 WhatsApp 或添加 Exchange 账户。不过，这种分离从未影响过通讯录。但从 iOS 11.3（及更高版本）开始，通讯录也加入了这一功能。

由于这是操作系统的基本功能，因此您无需安装任何东西或设置一个特殊的容器。

激活内置功能，将私人和业务应用程序/信息/文件分开。此设置还将禁用一些其他功能，否则可能会误关部分功能。

激活

激活 AppTec360 支持的容器解决方案

启用谷歌分割容器	启用谷歌分割容器
启用 SecurePIM 容器	启用 SecurePIM 容器

如果您已激活 SecurePIM Container，还可在 "激活 "下找到以下内容。此外，还会立即打开四个标签页，具体如下。

支持电子邮件地址	支持电子邮件地址，用户可通过该地址解决问题

SecurePIM 密码

在 "SecurePIM 密码 "下，可以建立密码安全强度准则。

会话超时	在此，您可以设定 SecurePIM 在后台运行多少分钟后必须再次输入新密码。
密码长度	访问 SecurePIM 容器的密码长度
大写字符	最少大写字符
小写字符	最小小写字符
特殊字符	最少特殊字符
数字	最小位数
擦拭应用	在 SecurePIM 内容被删除之前，错误输入密码的次数 (但应用程序仍保留在最终用户设备上)

SecurePIM 安全

在 "SecurePIM 安全性 "下，您可以建立各种安全设置。

检测越狱设备	如果激活此设置，一旦检测到设备已越狱，将阻止访问 SecurePIM 容器
安全文本字段	提交字段的内容将被加密，不会有任何信息到达操作系统（iOS）。 注意：只要该设置处于活动状态，自动更正功能就不再可用
将联系人数据导出到设备	如果激活此设置，则允许用户将 Exchange 联系人导出到本地设备上 注意：只导出姓名和电话号码
展示活动地点	如果激活此设置，即将发生事件的位置将显示在通知栏中
显示活动标题	如果激活此设置，即将发生的事件标题的位置将显示在通知栏中

SecurePIM 浏览器

您可以在此配置 SecurePIM 的浏览器。

使用该符号，您可以定义一个新的 URL。

使用该符号，您可以再次删除已定义的 URL。

"白名单 URL "是可以加载的 URL。

"黑名单 URL "是指无法加载并因此被阻止的 URL。

请注意，白名单条目比黑名单条目具有更高的优先级。在 "书签标题 "下，您可以发布一个标题。通过 "书签 URL"，可以将 URL 地址与书签标题相关联--这样就可以向相应用户分发个性化书签。

交流

在 "Exchange "下，您可以配置 Exchange 帐户。

ActiveSync 电子邮件地址	交换电子邮件地址（注意 "占位符）
ActiveSync Exchange 登录	交换用户名（注意 "占位符）
ActiveSync Exchange 服务器	Exchange 服务器地址（FQDN）
ActiveSync Exchange 域	交换域名地址
用户证书	用户证书
基于证书的身份验证	用户使用证书进行身份验证
允许 S/MIME 加密	允许用户加密邮件
允许 S/MIME 签名	允许用户在邮件上签名
CRL 检查	如果激活，私人证书将与 CRL（证书吊销列表）进行比较

连接管理

无线网络

服务集标识符（SSID）	要连接的网络的 SSID
自动加入	加入网络时激活自动加入
隐藏的网络	激活，以防接入点不广播 SSID

代理设置

为每个接入点配置代理

无		不设立代理
手册		建立手动代理
	代理服务器 URL	访问代理设置的地址
	港口	为代理建立端口
	认证	代理验证的用户名
	密码	代理验证密码
自动		自动建立代理
代理服务器 URL		访问代理设置的 URL

安全类型

为 AP 建立安全类型

WEP	
密码	AP 密码

WPA/WPA2	
密码	AP 密码

WEP 企业 - WPA / WPA2 企业 - 任何企业			
	协议		
	TLS	激活/禁用	
	TTLS	激活/禁用	
	LEAP	激活/禁用	
	PEAP	激活/禁用	
	EAP-FAST	激活/禁用	
	EAP-SIM	激活/禁用	
	使用 PAC		使用 PAC（受保护访问控制器）
	PAC	配置供应 PAC	
	匿名提供 PAC	匿名提供 PAC	
	内部认证	应使用的身份验证协议： PAP、CHAP、MSCHAP、MSCHAPv2	
	用户名	认证用户名	
	不要使用每次连接密码	不要使用每次连接密码	
	身份证明	上传/选择验证证书	
	外部特征	可以从外部看到的身份	
	信任		
	可信证书 1	上传第一个可信证书	
	可信证书 2	上传第二个可信证书	
	可信证书 3	上传第三个可信证书	
	受信任服务器证书名称	预期服务器证书的名称 (以逗号分隔的列表)	

无	不建立安全保障

虚拟专用网

连接名称	VPN 配置文件名称

VPN 类型

虚拟专用网

所有设备网络流量都将通过 VPN 连接传输。

连接类型	建立 VPN 连接类型
IPsec（思科）	思科的 IPsec 协议
PPTP	PPTP 协议
L2TP	L2TP 协议
思科 AnyConnect	AnyConnect 协议
瞻博网络 SSL	瞻博网络 SSL 协议
F5 SSL	F5 SSL 协议
SonicWall mConnect	SonicWall 移动连接
阿鲁巴 VIA	Aruba VIA 协议
自定义 SSL	通过自定义 SSL 连接
OpenVPN	OpenVPN 协议

每个应用程序的 VPN

打开某个应用程序时，将建立 VPN 连接

自动启动每应用程序 VPN 连接		自动启动每应用程序 VPN 连接
连接类型		建立 VPN 连接类型
	思科 AnyConnect	AnyConnect 协议
	瞻博网络 SSL	瞻博网络 SSL 协议
	F5 SSL	F5 SSL 协议
	SonicWall mConnect	SonicWall 移动连接
	阿鲁巴 VIA	Aruba VIA 协议
	自定义 SSL	通过自定义 SSL 连接
	OpenVPN	OpenVPN 协议

代理设置

为 VPN 连接配置代理服务器

无	不设立代理
手册	手动建立代理
代理服务器 URL	访问代理设置的地址
港口	为代理建立端口
认证	用于在代理处进行身份验证的用户名
密码	代理认证密码
自动	自动建立代理
代理服务器 URL	访问代理设置的 URL

显示占位符	显示 AppTec360 可以使用的所有可用用户变量

APN

接入点名称	接入点名称
接入点用户名	接入点用户名
接入点密码	接入点密码
代理服务器	代理服务器地址
港口	相应的代理端口

细胞

启用数据漫游	启用数据漫游
启用语音漫游	启用语音漫游
启用热点	启用热点

HTTP 代理服务器

代理类型	
手册	手动建立代理
代理服务器 URL	访问代理设置的地址
港口	建立代理端口
认证	用于在代理处进行身份验证的用户名
密码	代理认证密码
自动	自动建立代理
代理 PAC URL	代理 PAC URL
如果 PAC 无法连接，允许直接连接	如果 PAC 无法访问，允许直接连接（不使用 VPN
允许绕过代理访问专用网络	允许绕过代理访问专用内部网络

AirPrint

IP 地址	打印机 IP 地址
资源路径	通往 AirPrint 设备的明确路径

AirPlay

设备名称	设备名称
密码	配对密码
白名单	定义设备列表，设备可专门与之配对

PIM 管理

Exchange Active Sync

账户名称	电子邮件帐户名
Exchange ActiveSync 主机	服务器地址/FQDN
允许移动	允许移动电子邮件
仅在邮件中使用	交互只能在本地邮件应用程序上进行
使用 SSL	使用 SSL 加密
域名	服务器域
用户	用户名
电子邮件地址	电子邮件地址（仅限设备级）
密码（仅限设备级）	用户密码
身份证明	选择相应证书，以便在服务器上进行身份验证
邮件同步的过去	天数，直至电子邮件同步返回。 无限制 = 无限
启用 S/MIME	启用 S/MIME 加密
签名证书	上传相应的签名证书
加密证书	上传相应的加密证书

电子邮件

在终端用户设备上设置 POP3 / IMAP 账户

账户说明	姓名 电子邮件账户		
账户类型	IMAP	路径前缀	特殊文件夹的路径前缀
	持久性有机污染物		
用户显示名称	用户显示名称		
电子邮件地址	用户电子邮件地址		
允许移动	允许移动电子邮件		
启用 S/MIME	启用 S/MIME 加密		
签名证书	上传相应的签名证书		
加密证书	上传相应的加密证书		

来信

传入服务器设置

邮件服务器地址	邮件服务器地址
邮件服务器端口	邮件服务器端口
用户名	各自的用户名
认证类型	认证类型
无	无验证类型
密码（仅限设备级）	密码提示
MDM 挑战-回应	
NTLM	NTLM 身份验证
HTTP MD5 摘要	
使用 SSL	必要时使用 SSL

外寄邮件

外发服务器设置

邮件服务器地址	邮件服务器地址
邮件服务器端口	邮件服务器端口
用户名	用户名
认证类型	
无	无验证方法
密码（仅限设备级）	密码提示
MDM 挑战-回应	
NTLM	NTLM 身份验证
HTTP MD5 摘要	
使用 SSL	必要时使用 SSL
传出密码与传入密码相同	传出密码与传入密码相同
仅用于邮件	如果所有外发邮件都通过邮件应用程序发送，则激活

CalDav

配置 CalDav 帐户的设置和分配

账户说明	账户显示名称
主机名	主机名和/或 IP 地址
港口	CalDav 账户的端口
主要网址	账户的主要 URL
用户名	各自的 CalDav 用户名
密码（仅限设备级）	各自的 CalDav 密码
使用 SSL	必要时使用 SSL

订阅日历

设置和分发订阅日历

说明	账户显示名称
网址	日历数据库的 URL
用户名	订阅日历的用户名
密码（仅限设备级）	订阅日历的密码
使用 SSL	必要时使用 SSL

LDAP

在此区域，设置 LDAP 连接，以便在最终用户设备和 Active Directory 之间进行动态证书交换。

请注意，所选用户需要相应的读取权限。

账户说明	账户说明
账户用户名	访问 LDAP 的用户
账户密码	LDAP 访问密码
账户主机名	LDAP 服务器主机名/IP 地址
使用 SSL	必要时使用 SSL

在第二部分，您可以定义用于在 LDAP 注册表中搜索的单个筛选器。

说明	范围	搜索基地
过滤器说明	LDAP 注册表中的搜索级别	定义单个过滤器

网络管理

网络剪辑

在此位置定义书签，其中包含指向网页、内联网门户等的链接，这些链接将作为应用程序在终端用户设备上显示。

标签	终端用户设备上的连接名称
网址	相关网站链接
可拆卸	如果激活，用户可以移除网络剪辑
图标	通过此对话框上传连接徽标：尺寸为 180x180，png 格式
预制图标	如果激活，图标上将不会显示其他效果（阴影、倒影）。
全屏	打开网络剪辑时，浏览器以全屏模式打开

网页内容过滤器

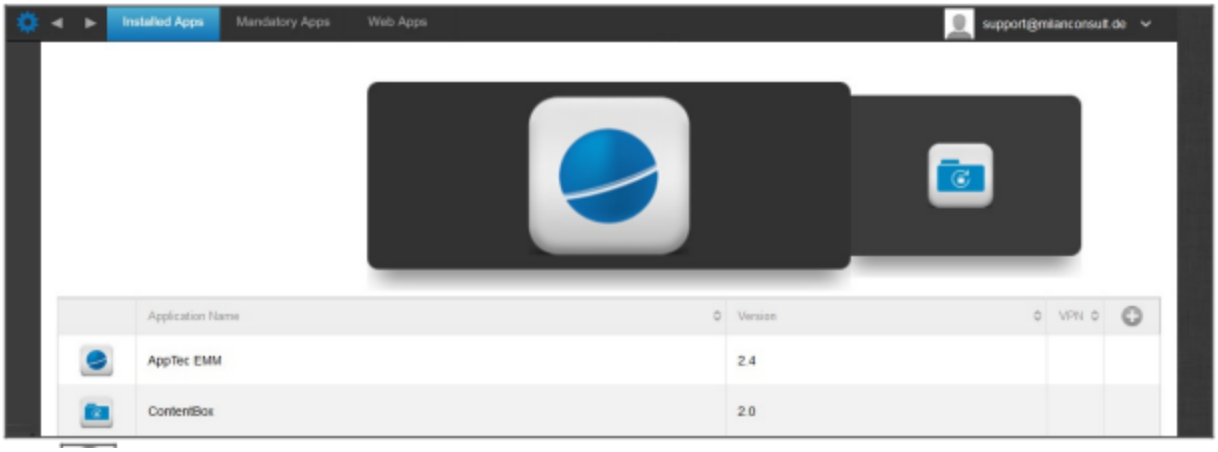
网络内容过滤器可以限制对特定网页的访问。

允许的网站	
限制成人内容	对成人内容自动应用网络过滤器
允许的 URL	使用 + 符号添加允许的页面
黑名单 URL	使用 "+"符号添加被阻止的页面
仅限特定网站	只能显示特定内容，您可以使用 + 符号添加这些内容。

应用程序管理

企业应用管理器

已安装的应用程序（仅限设备级别）



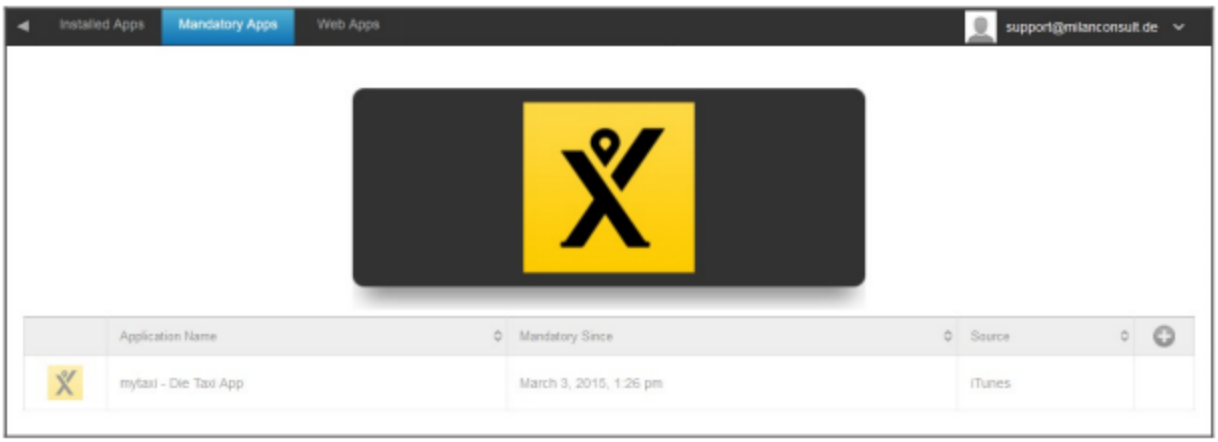
在这里，您可以看到设备上当前安装的应用程序。

必须使用的应用程序

在 "强制应用程序 "下，您可以强制使用必要的应用程序。

用户将不断被提醒安装上述应用程序。

通过 ，可以定义授权应用程序。



这可以是 Apple App Store 应用程序，也可以是内部应用程序。

如果涉及受监控设备，则会自动安装应用程序。

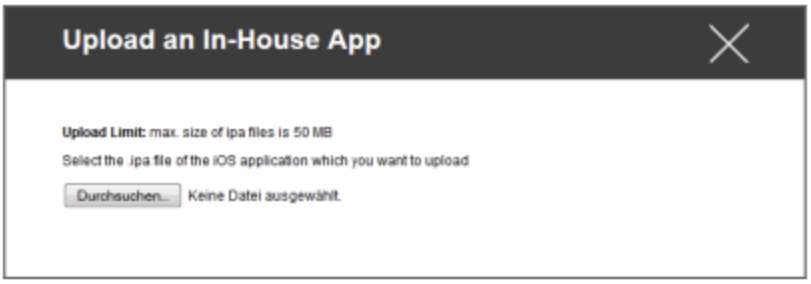
您可以将公共 AppStore 中的 "Apple AppStore "应用程序以及内部开发的内部应用程序推送到设备上。

或者，你也可以从 "iOS 内部应用程序 "类别中选择你在常规设置下上传的内部应用程序。

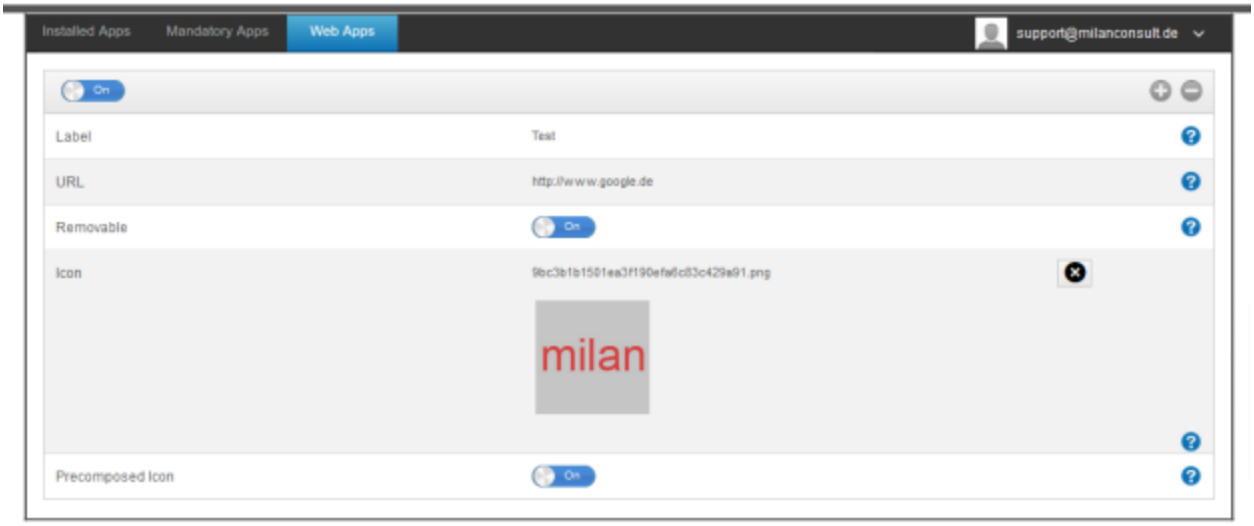
安装-选项

保持更新（仅支持每个设备的 VPP）	每周将确定应用程序是否有更新。如果有，将安装该更新 对于内部应用程序，您在常规设置中配置的更新目标将用于更新过程。
无人管理时超车	如果已安装应用程序，MDM 将接管应用程序并对其进行管理
删除 MDM 配置文件时移除应用程序	在删除设备管理的情况下，应用程序将被卸载
防止备份应用程序数据	不会创建应用程序特定数据的备份
应用程序设置	在 "应用程序设置 "下，您可以将应用程序的某些值分配到前台（只要应用程序支持，如有必要，请咨询应用程序的开发人员）。

您也可以通过 "上传内部应用程序 "直接选择并上传一个 ipa 文件。



网络应用程序



在 "Web Apps "点下，您可以像使用 "Web Clips "一样，在 Web 管理区域将互联网页面或内网门户网站作为应用程序推送到最终用户设备上。默认情况下，网络应用程序将以全屏模式显示，可在网络剪辑下进行配置。

标签	终端用户设备上的连接名称
网址	相关网站链接
可拆卸	如果激活，用户可以移除 Webclip
图标	通过此对话框上传连接徽标：尺寸为 180x180，png 格式
预制图标	如果激活，图标上将不会显示其他效果（阴影、倒影）。

限制和设置

黑名单/白名单应用程序

在这里，您可以根据 "常规设置 "中的设置来设置被阻止（或允许）的应用程序。点击后将弹出 "已知应用搜索"。您可以在此搜索想要添加的应用程序。

请注意，此功能需要一个受监控设备

系统应用程序限制

阻止设备的特定应用程序或功能

允许使用 YouTube	允许使用 YouTube
允许使用 iTunes Store	允许使用 iTunes Store
允许使用 Safari	允许使用 Safari
启用自动填充	允许自动填写
部队欺诈警告	强制执行欺诈警告
启用 JavScript	允许使用 JavaScript
阻止弹出式窗口	阻挡各种幼虫
允许 Cookie	选择 Safari 接受 cookies 的时间

App-VPN

通过该符号，您可以定义在启动时自动启动所选 VPN 连接的应用程序。

应用程序设置

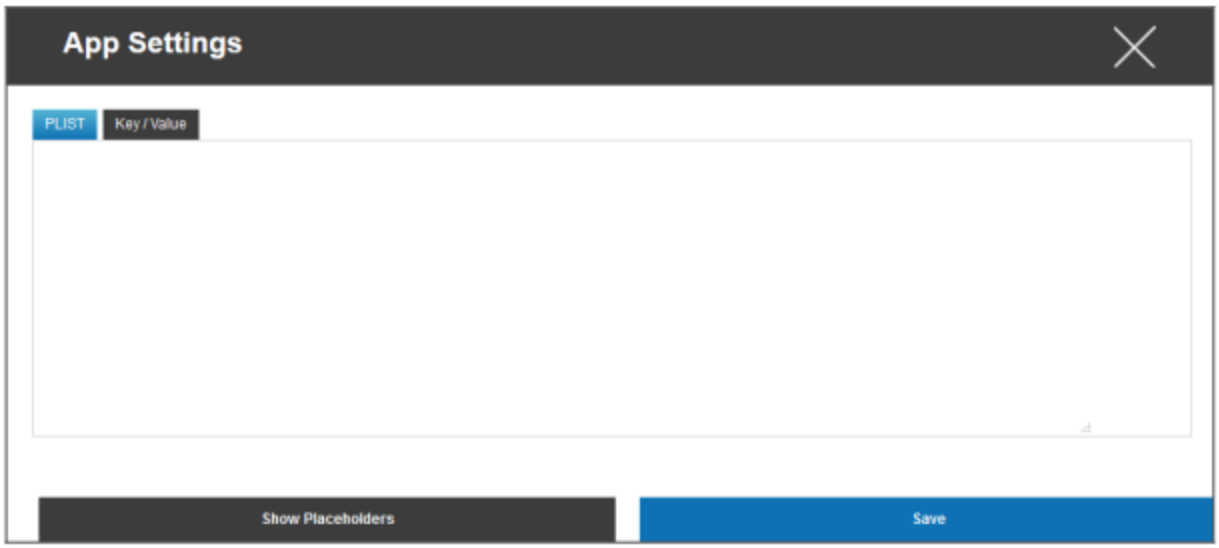
在 "应用程序设置 "下，您可以将应用程序的某些值分配到前台（只要应用程序支持，如有必要，请咨询应用程序的开发人员）。

通过该符号，您可以添加一个（额外的）应用程序。您将再次看到熟悉的 AppTec360 应用程序导入表示法。

在此搜索要配置的应用程序并选择。设置仅适用于受管理的应用程序。

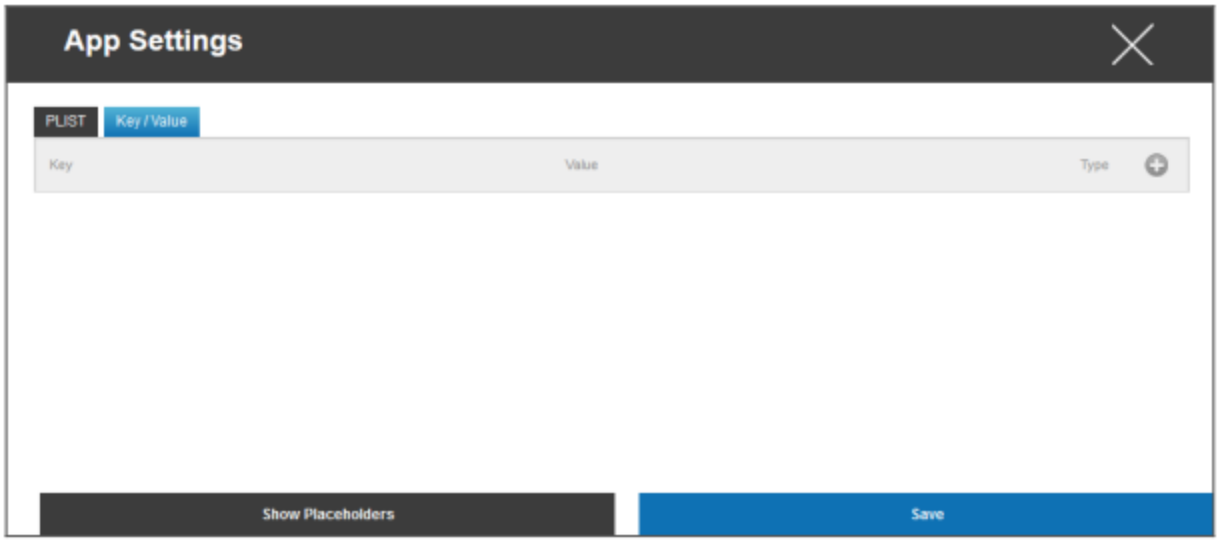
如果导入成功，您将看到以下显示：

现在，只需点击 ，就可以执行各种配置。然后，您将看到以下概览：

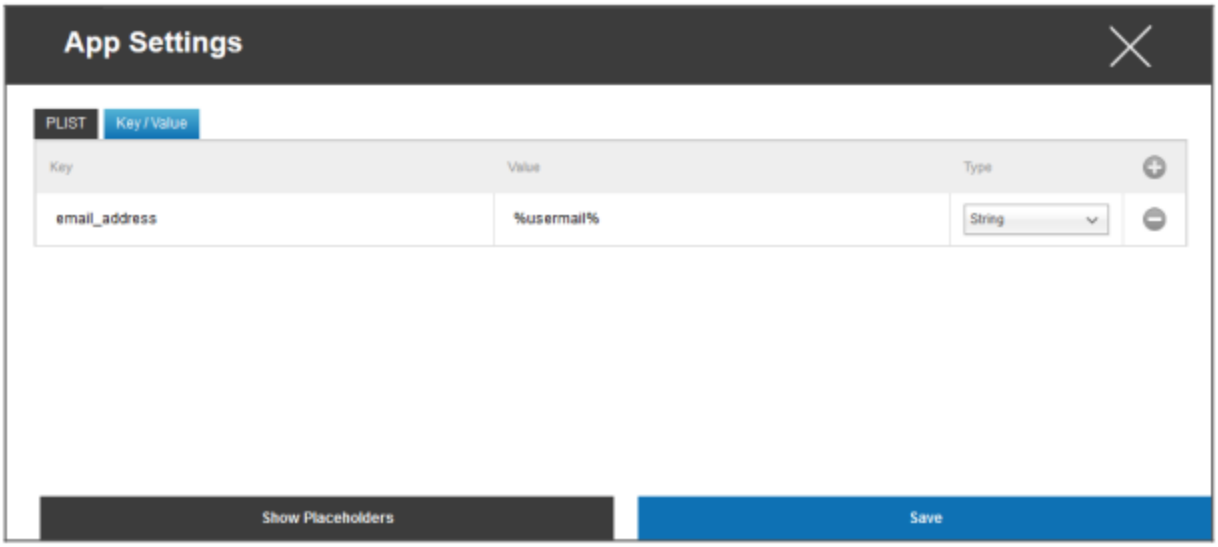


如果您已经有一个 PLIST（配置源文本），可以将其添加到这里，然后用 "保存 "将其全部保存。

在 "键/值 "下，您可以为应用程序附加特定配置



在这里，您可以用符号建立一个新键及其值。



当然，您可以使用 AppTec 的所有占位符

"类型 "解释：

字符串	文本
布尔型	真/假
数量	数量

有了这个符号，您就可以再次删除应用程序。

企业应用商店

iTunes 应用程序

在这一点上，您可以为用户分发可选应用程序。

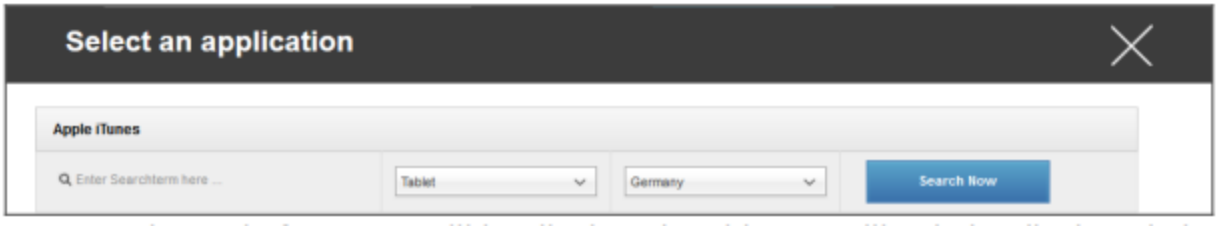
如果这里有一个应用程序，它将自动安装到 AppTec360 商店的最终用户设备上。

这些只是苹果官方应用商店的链接。因此，每个最终用户的设备都必须安装 Apple ID。

此时，我们建议每个用户都拥有自己的 Apple ID。

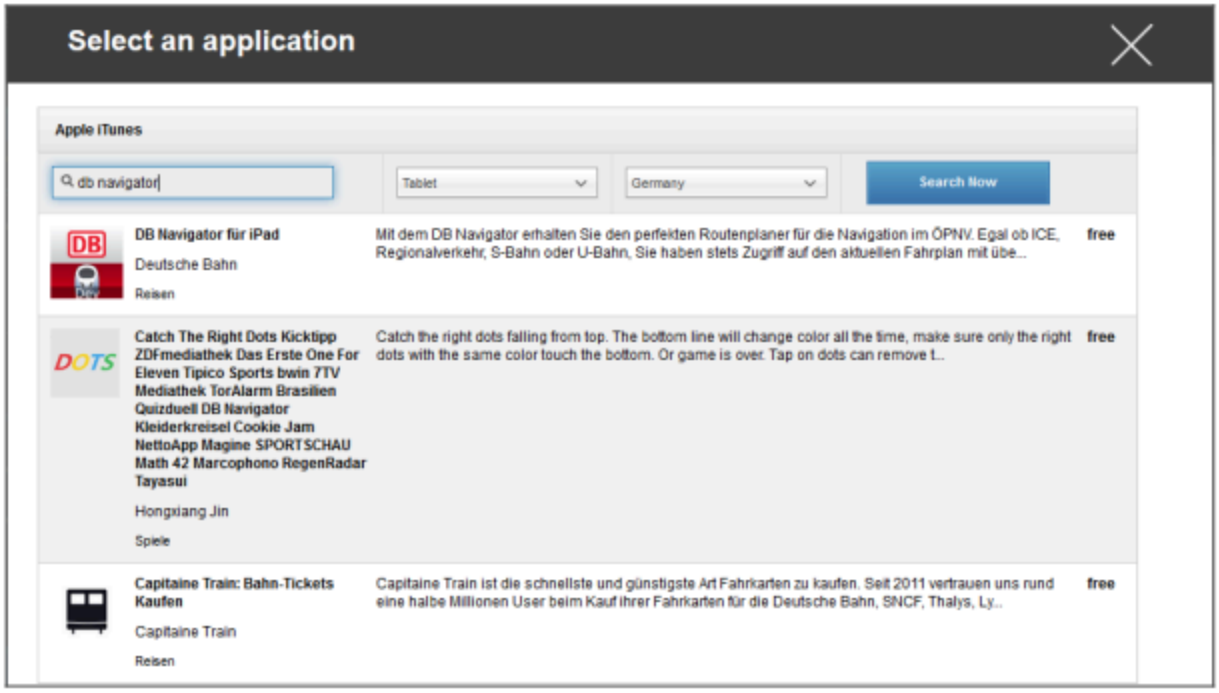
通过该符号，您可以添加其他应用程序。

然后，会打开一个窗口，显示以下概览。



请注意，只会显示免费应用程序，付费应用程序只能通过 VPN 显示。

在 "在此输入搜索词... "下，您可以搜索 Apple App Store 中的应用程序。



点击图标或应用程序名称后，系统会再次要求您执行其他配置。

保持更新	每周将确定应用程序是否有更新。如果有，将安装该更新
删除 MDM 配置文件时移除应用程序	在删除设备管理的情况下，应用程序将被卸载
防止备份应用程序数据	不会创建应用程序特定数据的备份
App-VPN	选择 VPN 连接，它将在打开应用程序时启动

点击 "安装 "后，应用程序将被添加到企业应用程序商店，然后可通过 AppTec360 AppStore 安装到最终用户设备上。

如果 App-Store 导入成功，您将收到以下概览：

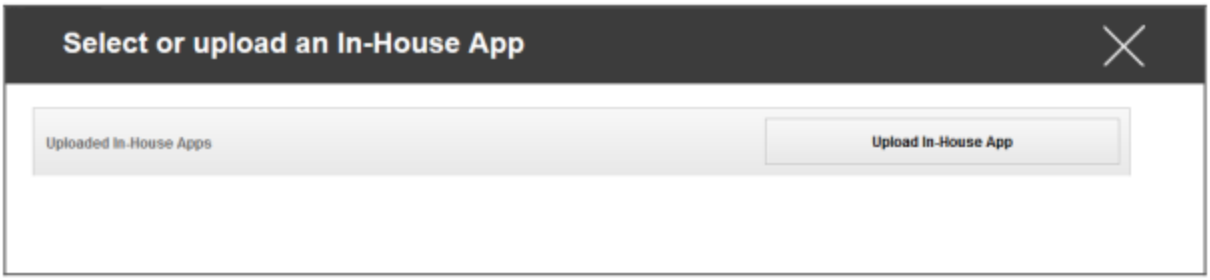

iTunes Apps
In-house
support@milanconsult.de
Application Name
Version
WordPress
4.9

内部

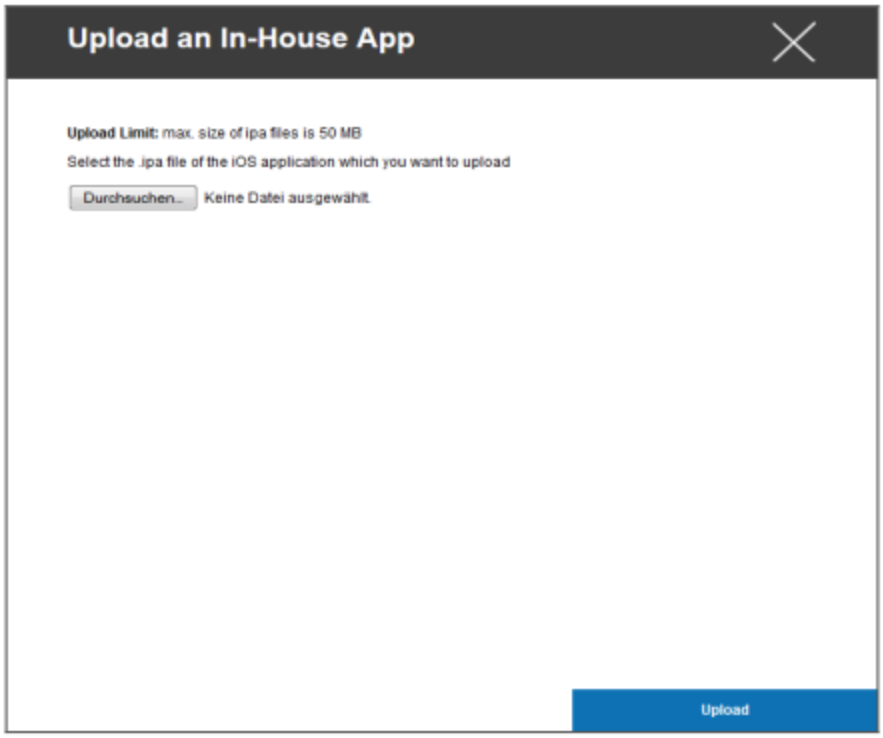
在 "内部 "点下，您可以上传内部开发的应用程序并进行分发。

有了这个符号，您就可以分发更多的内部应用程序。

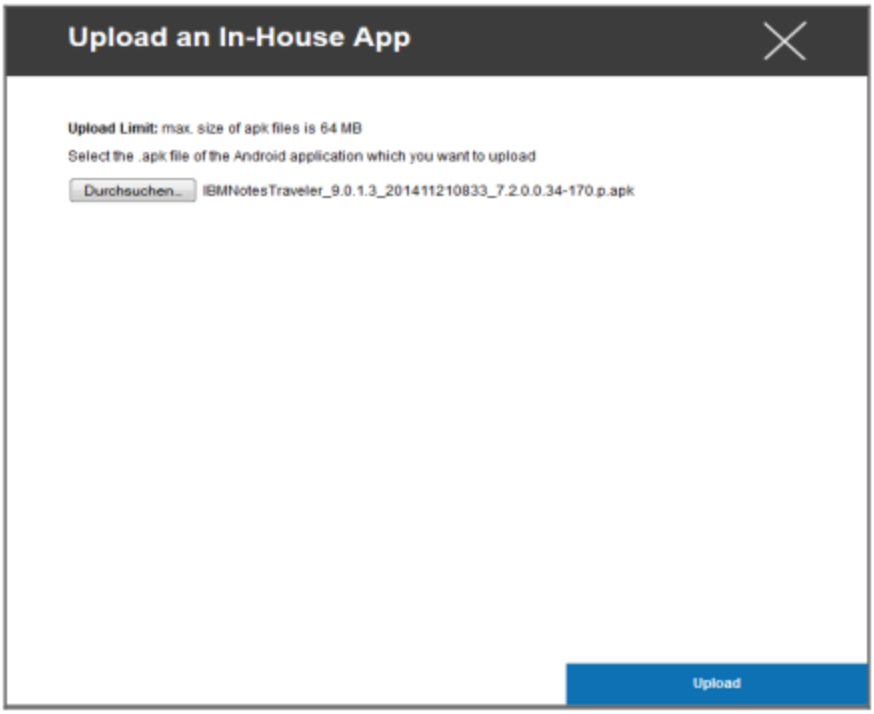
如果您从未分发过 In-House App，您将收到以下概述：



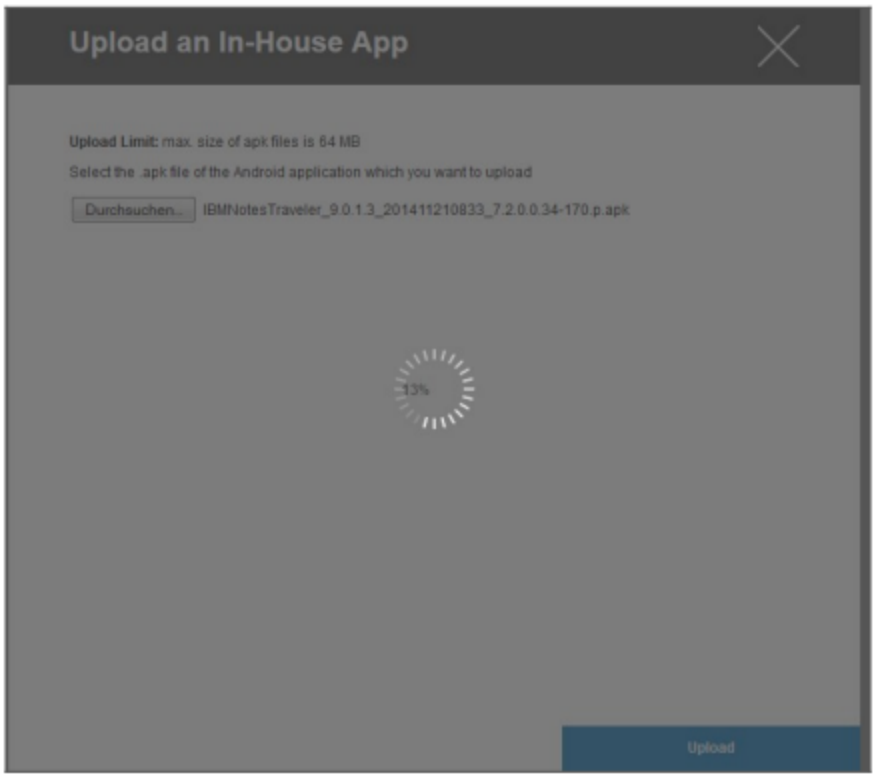
为此，请单击 "上传内部应用程序"，然后您将收到以下概览：



现在，用 "搜索... "选择一个 .ipa 文件，然后点击 "上传"。



现在，您的应用程序将被上传。在圆圈中间，您可以看到已上传应用程序的百分比。



如果已成功上传内部应用程序，您将在应用程序目录中看到新上传的应用程序。

现在，用户可以选择在终端用户设备上的 AppTec360 商店 "内部 "类别下查看并安装该应用程序。

由于这不涉及公共的苹果 AppStore 应用程序，用户不需要在最终用户设备上存储 Apple ID。

信息亭模式

iOS 信息亭模式仅在受监控模式下可用

通过 Kiosk 模式，您可以预先定义一个应用程序或 URL，这样就可以专门运行/访问该应用程序/URL。

此外，您还可以在 Kiosk 模式中停用各种硬件按钮。

应用类型

包装

如果要以 Kiosk 模式启动应用程序，请选择 "应用程序类型 " 下的 "软件包"。

信息亭应用	单击此处，选择应在 Kiosk 模式下启动的应用程序 您将看到应用程序管理的当前概览 您可以在 "苹果 iTunes 应用程序 "和 "iOS 内部应用程序 "之间进行选择

网址

如果要在 Kiosk 模式下启动 URL，请在 "应用程序类型 " 下选择 "URL"。

网址	现在，定义所需的 URL 地址
同源政策	如果激活该功能，用户只能浏览预定义 URL 的子页面 例如，如果您定义了以下 URL： www.mypage.com，那么用户就可以在 www.mypage.com/subpage 上浏览
白名单 URL	在这里您可以维护一个白名单，所有这些 URL 都是允许的 每行最多 1 个 URL URL 必须以 http:/ 或 https:// 开头
黑名单 URL	您可以在此维护一个黑名单，所有这些 URL 都将被禁止访问 每行最多 1 个 URL URL 必须以 http:/ 或 https:// 开头
闲置后清除浏览器	不活动后，浏览器缓存将被清空
启用退出密码	如果激活该功能，用户可以选择使用预先设置的密码结束自助服务终端模式。
退出密码	这是您预先定义的密码

信息亭模式设置

预定的信息亭模式	根据一天中的时间，您可以设置信息亭模式，以便在预先确定的时间自动启动和结束该模式。
开始时间	开始时间
时间（分钟	以分钟为单位，之后应再次结束信息亭模式
禁用触摸	如果激活，则停用触摸屏
禁用设备旋转	如果激活，则停用屏幕自动适应功能
禁用铃声开关	如果激活，振铃开关将被停用。从那时起，其行为取决于先前设置的功能
禁用音量按钮	如果激活，音量按钮将被禁用
禁用睡眠唤醒按钮	如果激活，开/关开关将被停用
禁用自动锁定	如果激活，设备将不会切换到待机状态
启用语音播报	如果激活，语音助理将被激活
启用缩放	如果激活，变焦将被激活
启用反转颜色	如果激活，将激活倒置显示模式
启用辅助触控	如果激活，将启动 AssistiveTouch
启用说话选择	如果激活，将激活发言选择
启用单声道音频	如果激活，单声道音频将被激活
语音	如果激活，用户可以启用 VoiceOver
放大	如果激活，用户可以启用缩放功能
反转颜色	如果激活，用户可以启用倒置颜色
辅助触控	如果激活，用户可以启用辅助触控功能

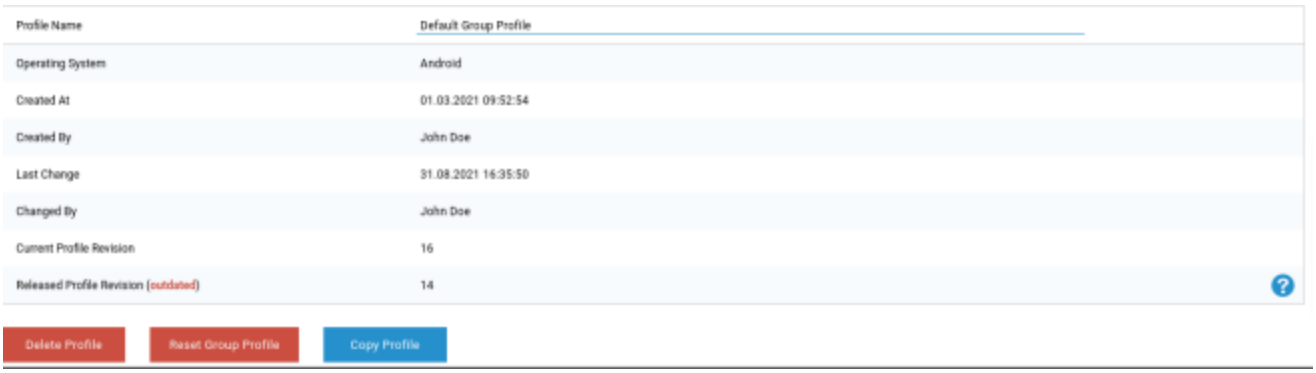
安卓企业 – 全面管理设备配置

根据您当前选择的是组配置文件还是设备，概览及其子点有所不同，请仔细考虑！

一般情况

组概况概览（仅适用于组级）

打开群组资料时，您将快速浏览该资料。



简介名称	个人资料名称（可在此处更改）
操作系统	配置文件适用的操作系统
创建于	创建时间
创建者	个人资料创建者
最后的变化	最后一次更改配置文件的时间
已更改	最后更改的账户
当前的简介修订	修订已保存的配置文件状态
已发布的简介修订版	已分配的配置文件修订版（"立即分配"）。如果标签文字后面显示"（已过期）"，则表示您已经保存了配置文件，但尚未分配，因此设备仍将获得旧版本。

设备概述（仅限设备级别）

如果您正在使用一个设备，您将收到所选设备的概述，其中包含以下内容：

设备名称	设备名称
地点	位置坐标
电话号码	电话号码
指定的强制性应用程序	分配的强制性应用程序数量
操作系统版本	设备的操作系统版本
操作系统	操作系统（安卓企业版）
序列号	设备序列号
设备所有权	公司或私人设备
设备类型	AE 工作管理设备
扎根	状态，显示设备是否已被 root
符合要求	符合准则要求
IP 地址	设备的 IP 地址
最后查看	设备最后一次连接 AppTec 的时间点
最后一搏	最后一次向设备发送推送的时间点
AE 设备所有者模式	是
用户分配	分配给该设备的用户或组

配置修订（仅限设备级）

在这里，您可以看到为设备分配的组配置文件的概览。

如果点击组配置文件，就可以直接进入该配置文件并进行设置。

使用此符号，可以将已分发的应用程序还原为群组配置文件的设置。

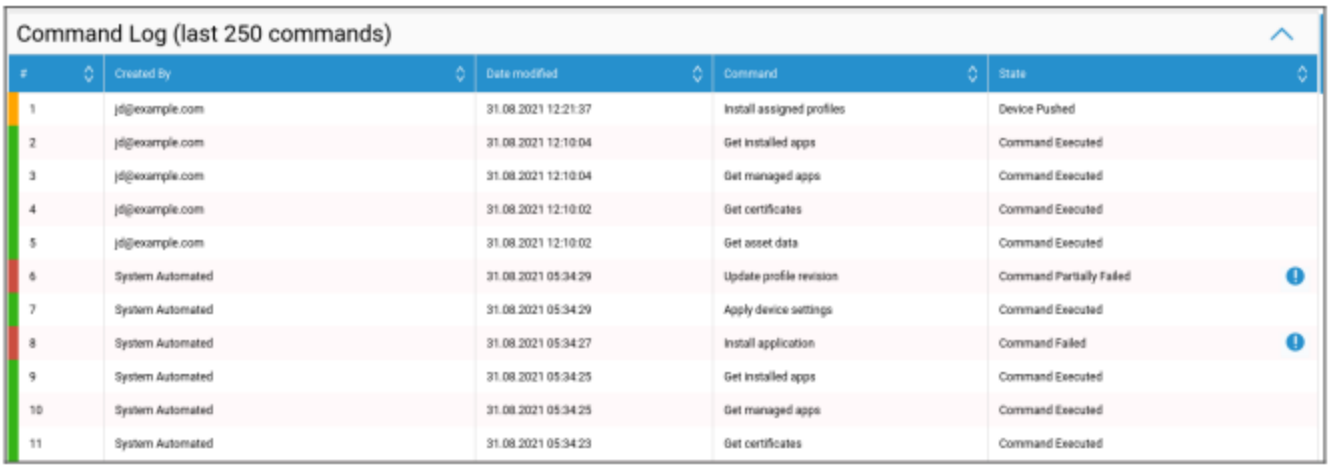
使用此符号，可以将所有使用过的应用程序还原为群组配置文件的设置。

"最新版本可用 "表示组配置文件已更改并保存，但尚未分配。必须在组级别上使用 "立即分配 "来分配组配置文件，才能将更改应用到设备上。

设备日志（仅限设备级）

命令日志

在这里，您可以查看为设备发出的命令及其状态。



系统自动 "创建的命令由系统自动创建。

可能的命令状态

设备已推送	推送请求已发送至推送服务（如 APNS），以通知设备连接回 EMM 服务器。
创建命令	该命令已在系统中创建。
发送命令	设备与服务器连接后，命令被发送到设备。
命令已执行	命令已成功执行。
命令失败	命令失败。*
命令部分失败	根据设备操作系统的不同，有些命令可能会被组合在一起。 其中，该命令组的某些部分出现故障。*
命令已执行，但最终失败	命令已执行，但也可能没有执行。
命令重发	命令被用户重新推送。
弃用	命令被丢弃。例如，该命令被其他命令取代，或设备重新注册，旧命令被删除。

如果信息后面有感叹号，则可以用光标悬停在图标上获取更多信息。

设备设置

客户端配置

在这里，您可以对安卓设备进行以下配置：

违规时间	用户响应超时限制，超时后将执行强制措施。
合规超时后的执法行动	当用户未执行导致设备状态合规的操作时采取强制措施
数据收集频率	收集设备/GPS 信息的频率
设备心跳频率	设备联系 AppTec360 服务器的时间间隔 分钟1 分钟 最长24 小时
启用位置更新	如果激活，设备会向 AppTec360 服务器发送位置更新
地点更新时间	确定设备向 AppTec360 发送位置更新的时间间隔
使用 Google 定位精度进行位置更新	如果激活，位置更新将使用网络位置（如果在 "限制 "下停用，则此设置不会产生任何影响）。
使用 GPS 定位进行位置更新	如果激活，将使用 GPS 进行位置更新
允许模拟（伪造）位置	允许通过第三方应用程序伪造位置信息
失去连接行动	如果启用，则可以为设备在心跳时间间隔内未与 MDM 服务器建立连接的情况指定操作。例如，如果设备的心跳时间为 5 分钟，它就会在上午 10:35 连接到服务器。之后，设备离开 Wi-Fi 范围。上午 10:40 时的下一次心跳将失败，指定的操作将被执行。
行动	一旦设备不符合要求，应立即采取的行动。 • 锁定设备 = 锁定设备 • 擦除设备 = 设备将恢复出厂设置 • 擦除设备和 SD 卡 = 设备将恢复出厂设置，SD 卡存储将被删除
阈值	您可以指定触发指定操作所需的失败心跳阈值。

政策执行模式	默认值：	将定期提示用户执行未执行的操作

	懒惰的政策执行	永远不会提示用户执行未执行的操作。所有未执行的操作都将显示在 AppTec360 客户端中
	积极执行政策：	会不停地提示用户执行未完成的操作
AppTec360 版本锁定	如果启用，可以指定 AppTec360 MDM 客户端的版本代码。AppTec360 客户端只会更新到指定的版本。较新版本将被忽略。不可能降级。	
版本代码	要锁定的 AppTec360 MDM 客户端的版本代码。	
禁用 AppTec360 通知	如果禁用，AppTec360 客户端将不会在通知栏中显示通知。因此用户可以通过任务管理器关闭 AppTec360 客户端。如果关闭 AppTec360 客户端，包括 Kiosk 模式和应用程序黑名单/白名单在内的多项功能将无法正常工作。 三星设备为 AppTec360 客户端提供保护机制。支持 KNOX API 的三星设备默认禁用通知功能。 使用 Android 8.0 或更高版本的设备不应禁用该通知。	

壁纸

设置自定义壁纸	启用/禁用自定义壁纸
壁纸	将壁纸模式设置为使用颜色代码或图像
指定颜色	以十六进制值指定背景色，例如 #000000 表示黑色，#ffffff 表示白色
将图像设为壁纸	上传要用作壁纸的图像文件

资产管理（仅限设备级）

设备信息

模型	设备型号
操作系统	操作系统
操作系统版本	操作系统版本
序列号	序列号
设备名称	设备名称
电池状态	电池状态
可用/总内存	可用/总内存
三星保险箱	三星 SAFE 界面，各种设置选项所需的界面
可用 SD 卡	可使用 SD 卡
模拟 SD 卡	模拟 SD 卡
可移动 SD 卡	可移动 SD 卡
SD 可用/总内存	SD 可用/SD 卡总内存

无线网络

IP 地址	设备 IP 地址
WiFi MAC	WiFi MAC 地址

细胞

现状	状态（已安装 SIM 卡）
电话号码	电话号码
漫游（语音/数据）	语音/数据漫游
漫游状态	当前漫游状态
IP 地址	IP 地址
运营商/承运商	运营商/承运商
蜂窝技术	蜂窝技术
IMEI	IMEI 号码
ICCID	这是 SIM 卡的 ID，通常也是智能卡或集成电路卡 (ICC)
IMSI	在 GSM 和 UMTS 移动网络中，国际移动用户标识（IMSI）提供了网络用户的明确标识 IMSI 最多由 15 位数字组成，配置方式如下： • 移动国家代码(MCC)，3 位数 • 移动网络代码(MNC)，2 或 3 位数 • 移动用户识别码 (MSIN)，1-10 位数
目前的 MCC/MNC	参见 "SIM MCC/MNC
SIM MCC/MNC	移动国家代码是国际电联根据 E.212 标准制定的国家标识符。它与移动网络代码（MNC）一起用于识别移动网络。 指 SIM 卡的国家/移动网络代码。 如果您漫游到另一个移动网络，那么从逻辑上讲，"当前 MCC/MNC "和 "SIM MCC/MNC "将是不同的。

蓝牙

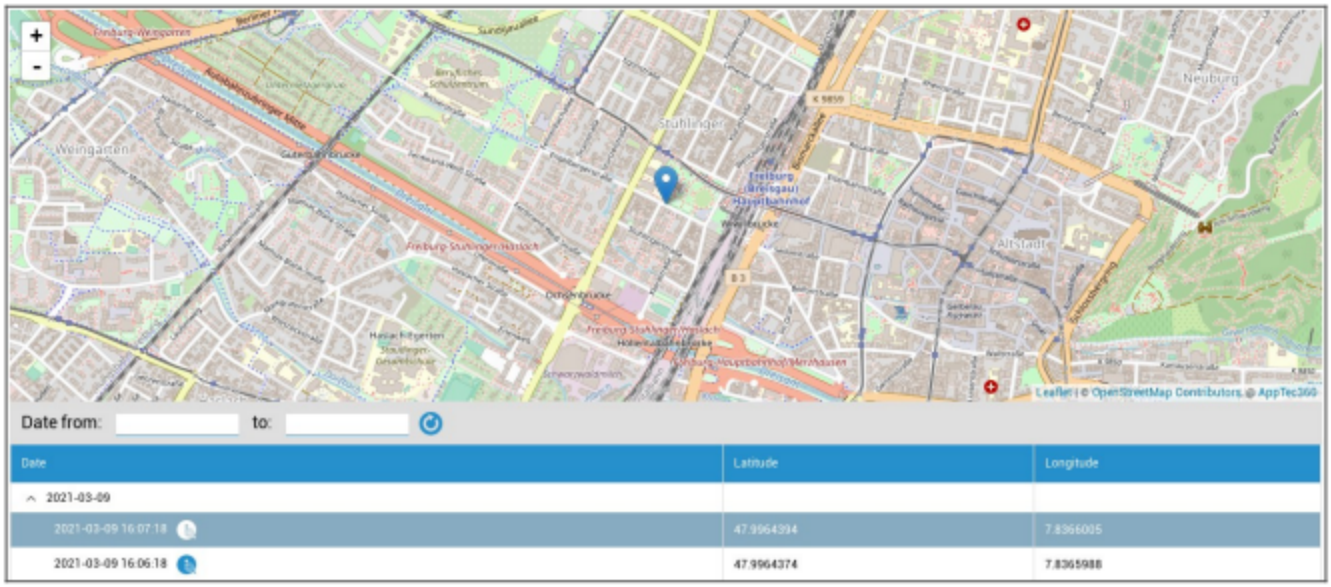
蓝牙 MAC	蓝牙 MAC 地址

安全管理

防盗（仅限设备级）

GPS 信息（仅限设备级别）

您可以在此确定当前/最后的设备位置。可以使用一个甚至两个密码来保护定位功能 - 请参阅 "常规设置"-"隐私"-"GPS 访问"：常规设置 - 隐私 - GPS 访问



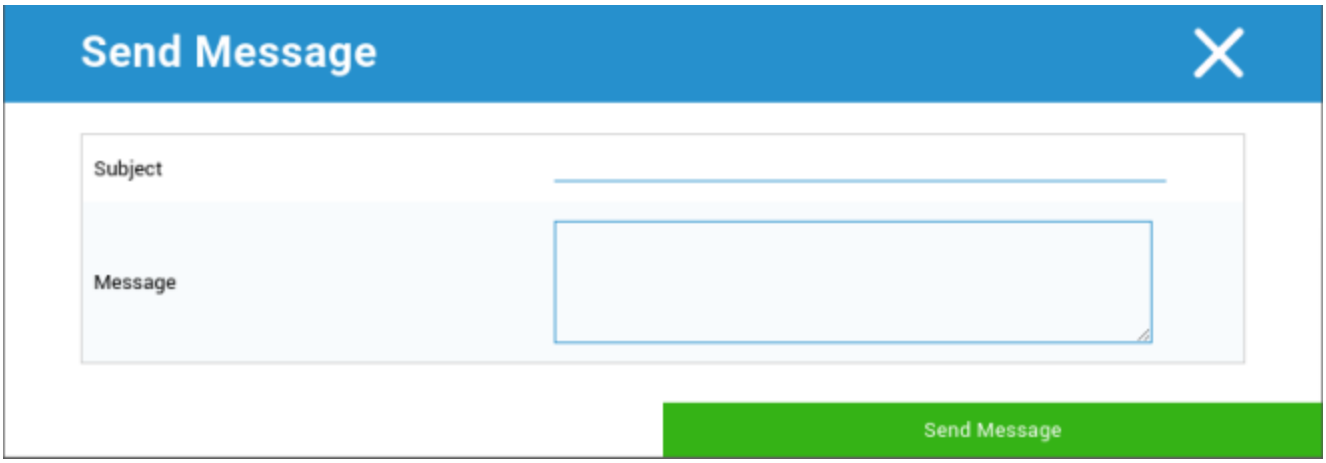
擦除和锁定（仅限设备级别）

在 "擦除和锁定 "下，您可以执行以下三项操作：

全面擦拭	设备恢复出厂设置（删除公司和个人数据）
企业擦拭	只从最终用户设备中删除企业数据（由 AppTec360 提供的所有应用程序、数据等）
锁定屏幕	屏幕锁已激活，只需使用设备密码/PIN 解锁设备即可

信息（仅限设备级别）

您可以在这里填写主题和信息，然后将其发送到最终用户设备。



安全配置

设备密码

在 "密码 "下，您可以设置设备密码，有以下设置选项供您选择

最小密码长度	规定密码必须包含的最少符号数	
密码质量	未说明	该政策对密码没有要求。
	生物特征弱	这项政策允许使用低安全性的生物识别技术。这意味着可以识别个人身份的技术，其识别率约为 3 位数的 PIN 码（错误检测率低于千分之一）。
	一些东西	该策略要求设置某种密码或模式，但不执行任何具体规则。
	字母	用户输入的密码必须至少包含字母（或其他符号）字符。
	字母数字	用户输入的密码必须至少包含数字和字母（或其他符号）字符。
	复杂	默认情况下，用户输入的密码必须至少包含一个字母、一个数字和一个特殊符号。利用这种密码质量，可以限制密码包含各种字符集，如至少包含一个大写字母等。
最小密码长度	设置密码所需的字符数。例如，可以要求 PIN 或密码至少有六个字符。	
密码所需的最小数字位数	密码所需的最小数字位数	
密码中至少需要小写字母	密码中至少需要小写字母	
密码中至少需要大写字母	密码中至少需要大写字母	
密码中需要的最少非字母字符	密码中需要的最少非字母字符	
密码所需的最少符号	密码所需的最少符号	

最长闲置时间锁定	时间锁定前用户最长不活动时间
密码过期超时	建立，在此时间间隔后密码失效，必须发布新密码

密码历史限制	不允许使用的密码数量
密码尝试失败次数上限	规定在执行完全设备擦除之前，错误输入密码的频率
允许生物识别身份验证	可通过指纹或虹膜扫描进行身份验证。仅适用于三星 KNOX 2.1 及更高版本

防病毒

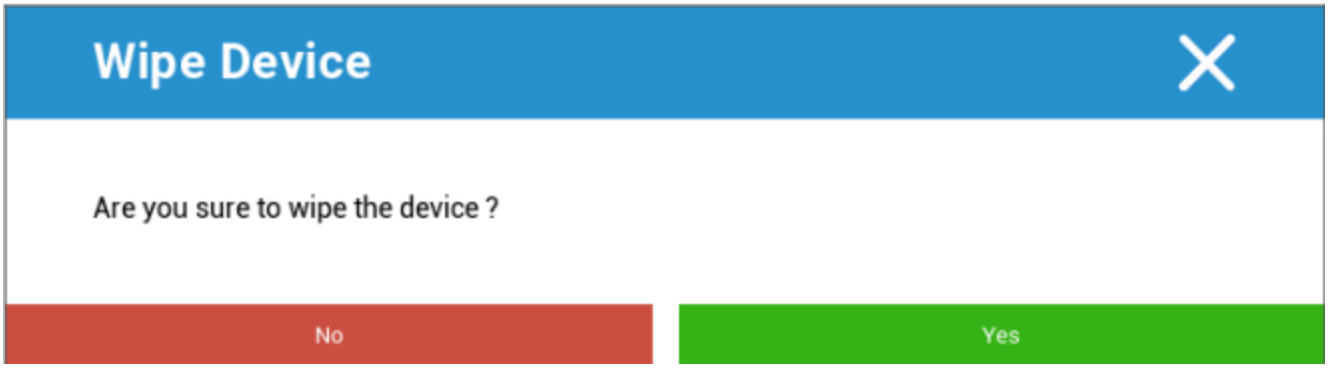
自动扫描	启用定期自动扫描
扫描时间间隔	检查间隔（快速/全面）
全自动扫描	启用全自动扫描
自动更新	启用自动更新
更新检查间隔	多久更新一次应用程序及其数据库（病毒/损坏的代码）
应用程序保护	启用应用程序自动扫描
SD 卡保护	启用自动 SD 卡扫描
仅 Wi-Fi 更新	启用后，只有当设备成功连接到 Wi-Fi 网络时才会应用更新

报废（仅限设备级）

擦除（仅限设备级）

在 "擦除 "下，可以将设备恢复出厂设置。在这里，最终用户设备上的公司和私人数据都将被删除。

点击 "减号 "后，您将收到以下信息：



如果选择 "是"，则可以执行擦除操作。

在 "擦除报告 "下可显示以下项目

擦拭	进行擦拭的历史
日期	日期
现状	状态（例如擦除是否成功执行）

限制设置

限制条件

在这里，可以限制和阻止各种事物。

启用摄像头	允许使用照相机	
强制自动同步	关于	同步永久激活
	关闭	同步永久停用
	用户选择	由用户选择
强制蓝牙	关于	蓝牙已永久激活
	关闭	蓝牙永久停用
	用户选择	由用户选择
Force GPS	关于	GPS 永久激活
	关闭	GPS 永久停用
	用户选择	由用户选择
部队网络位置	关于	永久性互联网本地化
	关闭	永久停用互联网定位功能
	用户选择	由用户选择

安全		
禁止共享位置	指定是否禁止用户开启位置共享。	
禁止安全启动	指定是否不允许用户将设备重新启动到安全启动模式。	
禁止网络重置	指定是否禁止用户从 "设置 "中重置网络设置。	
禁止出厂重置	指定是否禁止用户重置设备。	
启用 ADB	允许通过 ADB 与电脑连接	
禁用键盘防护	禁用键盘防护	
设备所有者锁屏信息	设置要在锁屏上显示的设备所有者信息。	
合规执行	模式 提示 用户	系统会提示用户执行必要的操作。
	模式锁定容器	隐藏所有应用程序，直至满足所有要求

应用程序管理	
允许跨配置文件应用程序链接	允许父配置文件中的应用程序处理来自受管配置文件的网络链接。
禁止应用程序控制	指定是否禁止用户修改设置或启动器中的应用程序。
禁止安装应用程序	指定是否禁止用户安装应用程序。
禁止卸载应用程序	指定是否禁止用户卸载应用程序。
运行时权限政策	指定如何处理来自应用程序的新权限请求。
允许未知来源	如果启用，用户可以通过安装 .apk 文件来侧载应用程序。

连接性	
禁止移动网络配置	指定是否禁止用户配置移动网络。
禁止 Tethering 配置	指定是否禁止用户配置 Tethering 和便携式热点。
禁止 VPN 配置	指定是否禁止用户配置 VPN。
禁止 Wifi 配置	指定是否禁止用户更改 WiFi 接入点。
禁止发出 NFC 光束	指定是否不允许用户使用 NFC 从应用程序传送数据。
锁定 WiFi 配置	此设置可控制由设备所有者应用程序创建的 WiFi 配置是否应被锁定（即只能由设备所有者应用程序编辑或删除，甚至不能由设置应用程序编辑或删除）。
启用数据漫游	激活数据漫游

蓝牙	
禁止蓝牙	指定设备是否禁止蓝牙。要求安卓 8.0
禁止蓝牙共享	指定设备是否禁止外发蓝牙共享。需要安卓 8.0
禁止蓝牙配置	指定是否禁止用户配置蓝牙。

账户管理	
禁止添加受管配置文件	指定是否禁止用户添加受管配置文件。需要安卓 8.0
禁止添加用户	指定是否禁止用户添加新用户。
禁止移除受管配置文件	指定除用户配置文件所有者外，是否可以删除该用户的受管配置文件。需要安卓 8.0
禁止修改账户	指定是否禁止用户添加和删除账户，除非 Authenticator 以编程方式添加了账户。

电话	
禁止拨出电话	指定不允许用户拨打外线电话。
禁止短信	指定不允许用户收发短信。

系统	
禁止创建窗口	指定不创建应用程序窗口以外的窗口。
禁止设置用户图标	指定是否不允许用户更改自己的图标。
禁止设置壁纸	禁止设置壁纸的用户限制。
禁用状态栏	禁用状态栏会阻止通知、快速设置和其他屏幕叠加功能，使用户无法从单一使用设备中逃脱。
启用自动计时	自动设置时间。
启用自动时区	自动设置时区。
插电时保持开机状态	当连接到电源时，设备将保持激活状态。

存储	
禁止禁用应用程序验证	指定是否禁止用户禁用应用程序验证。
禁止安装物理介质	指定是否禁止用户挂载物理外部介质。
启用备份服务	备份服务管理设备上的所有备份和还原机制。将此设置为假将阻止数据备份或还原。备份服务默认为关闭。需要安卓 8.0
启用 USB 大容量存储器	启用 USB 大容量存储器。

键盘	
禁止自动填写	指定是否不允许用户使用自动填充服务。要求安卓 8.0
禁止在预案之间复制和粘贴	指定复制到该预案剪贴板中的内容是否可以粘贴到相关预案中。

声音	
不允许音量调整	指定是否禁止用户调整主音量。
禁止麦克风静音	指定是否禁止用户调节麦克风音量。
静音装置	静音装置。

证书管理

您可以在此向设备分发可信证书和身份证书。

分发信任证书需要安卓 8 或更高版本，分发身份证书需要安卓 9 或更高版本。

使用 "+"可以添加多个证书。

受信任证书必须是 PEM 格式。

身份证书需采用 PKCS12 格式

连接管理

无线网络

为此，请对终端用户设备进行预配置，以便访问内部访问点

服务集标识符（SSID）	要连接的网络的 SSID
隐藏的网络	激活，以防接入点不广播 SSID

安全类型

建立 AP 的安全类型

WEP

密码	AP 密码

WPA/WPA2

密码	AP 密码

802.1x EAP

EAP 方法

工务司	身份	身份
	密码	密码

PEAP	第 2 阶段身份验证协议	无	无附加协议
		MSCHAPV2	MSCHAPV2 协议
		通用技术委员会	全球技术合作协议
	CA 证书	CA 证书	
	身份	身份	
	匿名身份	匿名身份	
	密码	密码	

TTLS	第 2 阶段身份验证协议	无	无附加协议
		PAP	PAP 协议
		MSCHAP	MSCHAP 协议
		MSCHAPV2	MSCHAPV2 协议
		通用技术委员会	全球技术合作协议
	CA 证书	CA 证书	
	身份	身份	
	匿名身份	匿名身份	
	密码	密码	

TLS	CA 证书	CA 证书
	身份	身份
	密码	密码

虚拟专用网

连接名称	VPN 连接名称

VPN 类型

虚拟专用网

VPN 客户端

AppTec360 VPN 客户端	
网关配置	选择网关 VPN 配置（请参阅**常规设置 > 通用网关 > VPN 设置**）。
始终在线的 VPN	启用本地锁定
启用 AppTec360 锁定	启用 AppTec360 锁定

内置（仅适用于三星设备）			
连接类型	PPTP	服务器	服务器
		启用 PPTP 加密	启用 PPTP 加密
	L2TP / IPSec PSK	服务器	服务器
		IPSec 预共享密钥	IPSec 预共享密钥
		启用 L2TP 秘密	启用 L2TP 秘密
		L2TP 秘密	L2TP 秘密
	IPSec XAuth PSK	服务器	服务器
		IPSec 识别码	IPSec 识别码
		IPSec 预共享密钥	IPSec 预共享密钥
DNS 搜索域	DNS 搜索域		
专家设置	DNS 服务器	DNS 服务器	
	转发路由	转发路由	

开放 VPN		
服务器	服务器	
OpenVPN 简介	OpenVPN 简介	
OpenVPN 应用程序	Android 版 OpenVPN（推荐）	
	连接 OpenVPN	
专家设置	DNS 服务器	DNS 服务器
	转发路由	转发路由

三星 / 强天鹅			
连接类型	PPTP	服务器	服务器
		用户名	用户名
		密码	密码
		启用 PPTP 加密	启用 PPTP 加密
	L2TP / IPSec PSK	服务器	服务器
		IPSec 预共享密钥	IPSec 预共享密钥
		用户名	用户名
		密码	密码
		启用 L2TP 秘密	L2TP 秘密
	IPSec XAuth PSK	服务器	服务器
		IPSec 识别码	IPSec 识别码
		IPSec 预共享密钥	IPSec 预共享密钥
		用户名	用户名
		密码	密码
专家设置	DNS 服务器	DNS 服务器	
	转发路由	转发路由	

思科任意连接		
服务器	服务器	
证书模式	残疾	残疾
	自动	自动
专家设置	DNS 服务器	DNS 服务器
	转发路由	转发路由

每个应用程序的 VPN

VPN 客户端

AppTec360 VPN 客户端		
网关配置	选择网关 VPN 配置（请参阅**常规设置 > 通用网关 > VPN 设置**）。	
VPN 应用程序	VPN 应用程序	
始终在线的 VPN	启用本地锁定	始终在线的 VPN
启用 AppTec360 锁定	启用 AppTec360 锁定	

三星 / 强天鹅			
连接类型	PPTP	服务器	服务器
		VPN 应用程序	VPN 应用程序
		用户名	用户名
		密码	密码
		启用 PPTP 加密	启用 PPTP 加密
	L2TP / IPSec PSK	服务器	服务器
		VPN 应用程序	VPN 应用程序
		IPSec 预共享密钥	IPSec 预共享密钥
		用户名	用户名
		密码	密码
		启用 L2TP 秘密	L2TP 秘密
	IPSec XAuth PSK	服务器	服务器
		VPN 应用程序	VPN 应用程序
		IPSec 识别码	IPSec 识别码
		IPSec 预共享密钥	IPSec 预共享密钥
		用户名	用户名
		密码	密码
专家设置	DNS 服务器	DNS 服务器	
	转发路由	转发路由	

限制条件

您可以在此设置与连接管理相关的限制。

允许数据漫游	允许漫游时使用移动数据
强制数据漫游	如果激活，移动数据漫游将永久激活（不建议使用！）。 该设置会覆盖 "允许数据漫游 "设置！
以下设置仅适用于 SAFE 2.x 或更高版本	
只允许拨打紧急电话	只允许拨打紧急电话
允许 WiFi	允许 WiFi
WiFi 网络最低安全级别	WiFi 网络最低安全级别 开放 = 允许使用所有类型的 WiFi
禁止用户添加 WiFi 网络	用户不能自己添加 WiFi 网络 只有在 "连接管理 "中定义了 WiFi 配置文件，才能进行此设置
允许短信和彩信	全部 = 允许所有短信和彩信流量 仅接收短信 = 仅允许接收短信 仅发出短信息 = 只允许发出短信息 无 = 不允许短信/彩信流量
允许漫游期间同步	允许漫游期间同步 开启 = 激活 关闭 = 禁用 用户选择 = 用户的选择
允许语音漫游	允许语音漫游 开启 = 激活 关闭 = 禁用 用户选择 = 用户的选择
使用系统 http 代理服务器	HTTP 代理服务器的使用由系统设置提供，取决于所连接的网络（WiFi 或 APN）。

PIM 管理

Gmail Exchange

信息：此配置将应用于 Gmail 应用程序。因此，您必须批准并安装 Gmail。

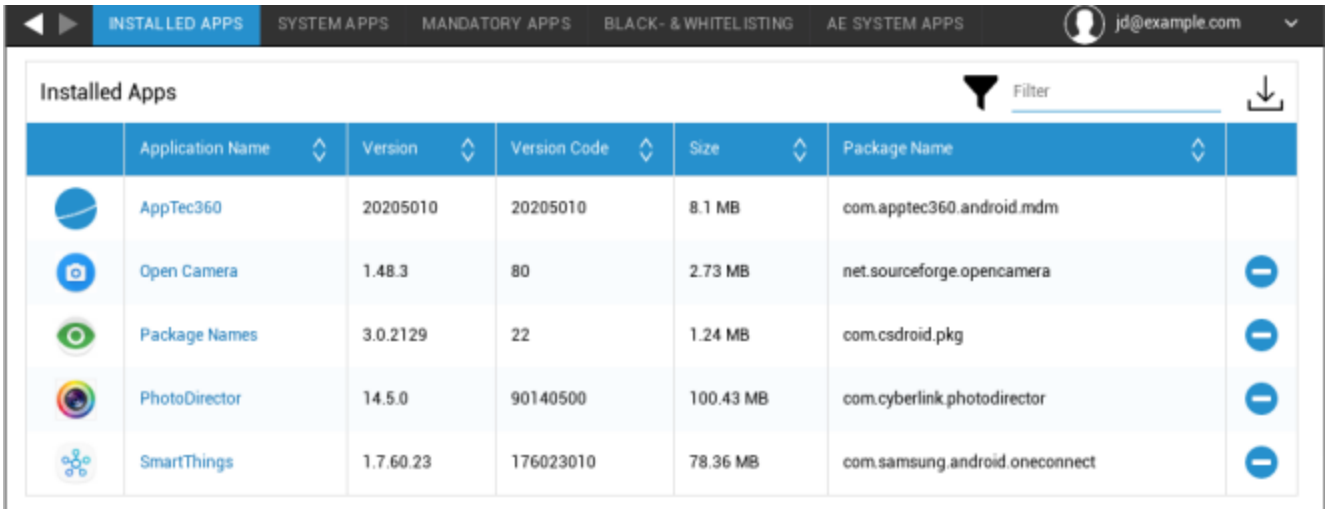
电子邮件地址	提供的用户电子邮件地址 请注意 "占位符"，您可以使用这些占位符来处理凭据，而无需在每台设备上手动执行更改。 只需点击一下，您就可以将它们展示在自己面前
服务器主机名	Exchange 服务器的服务器地址
登录名	终端用户设备的登录名，请注意 "此处的占位符
签名	可附加签名（提示：某些设备要求签名使用 HTML 格式）
同步的天数	天数，决定电子邮件何时同步返回
设备标识符	包含 EAS DeviceID 的字符串。该字符串是 EAS Protokols 的一部分，在某些地区可以使用
使用安全套接字层（SSL）	使用 SSL 连接
接受所有证书	接受所有证书。如果您的 Exchange 服务器使用自签名证书，请选择此选项

应用程序管理

企业应用管理器

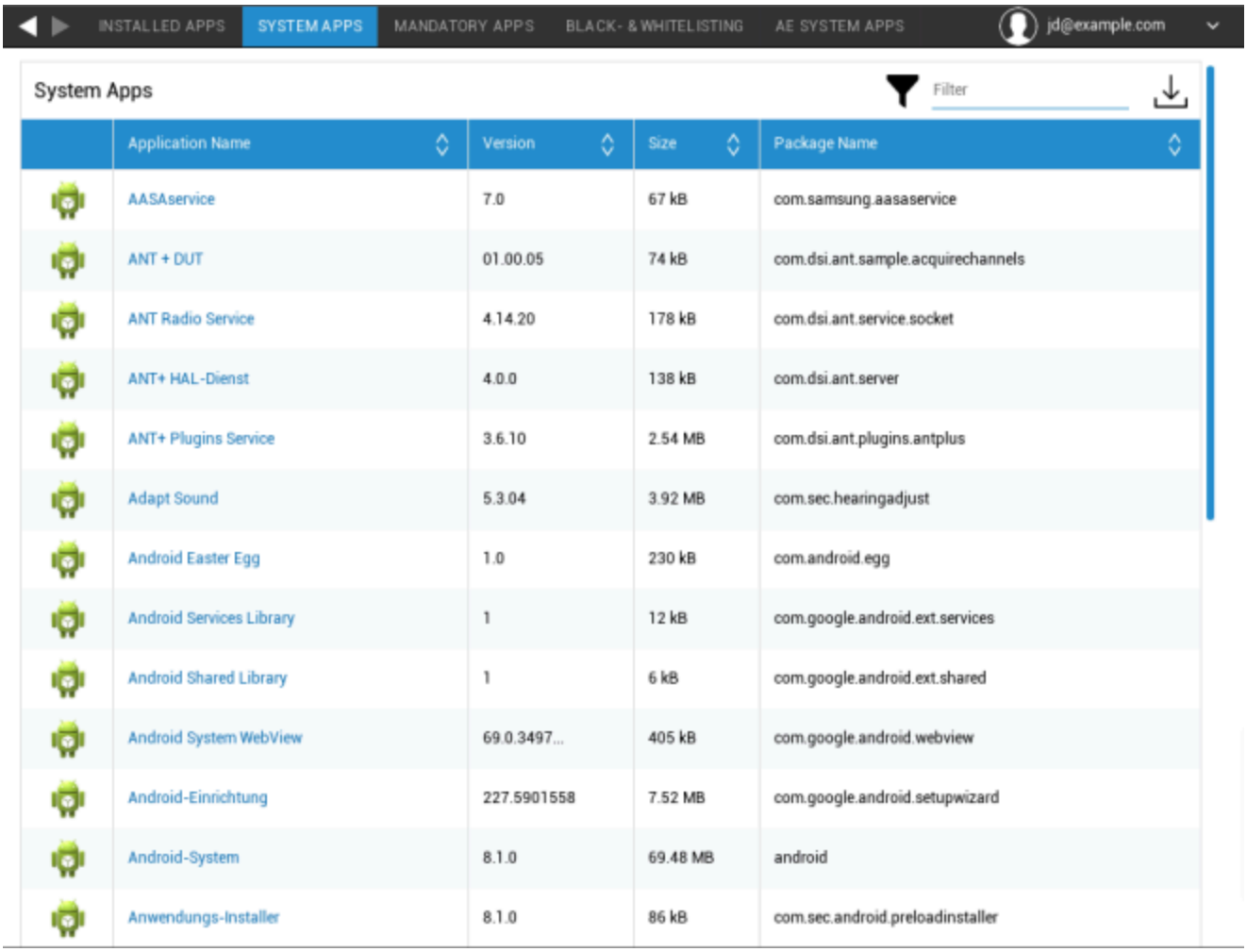
已安装的应用程序（仅限设备级别）

这里将显示终端用户设备上当前安装的所有应用程序。



系统应用程序（仅限设备级）

在 "系统应用程序 "下，将为您列出设备制造商已经安装在最终用户设备上的所有应用程序和服务。



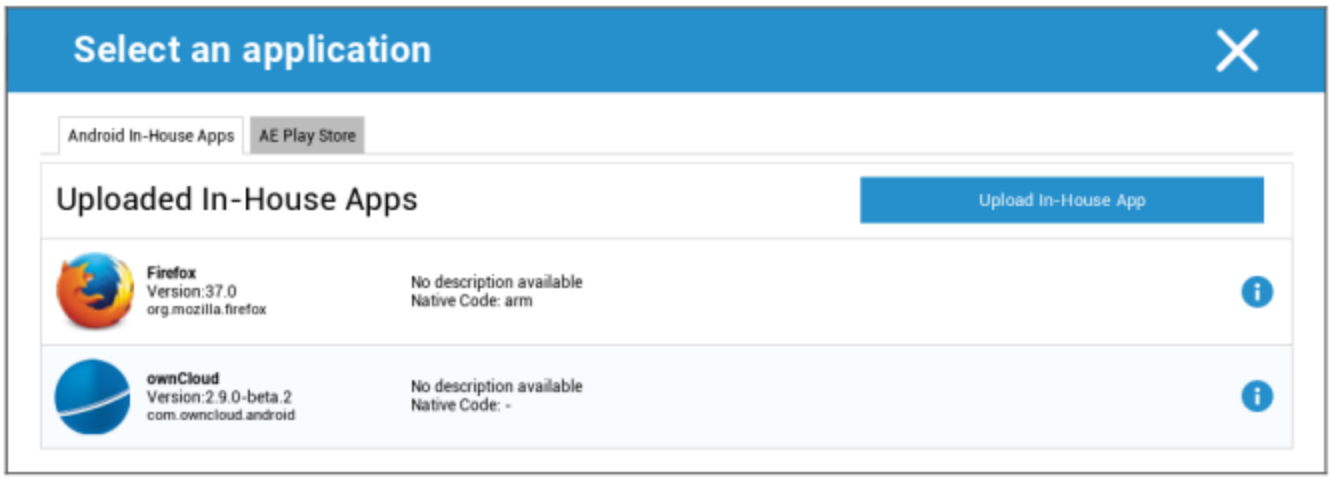
Application Name	Version	Size	Package Name
AASAservice	7.0	67 kB	com.samsung.aasaservice
ANT + DUT	01.00.05	74 kB	com.dsi.ant.sample.acquirechannels
ANT Radio Service	4.14.20	178 kB	com.dsi.ant.service.socket
ANT+ HAL-Dienst	4.0.0	138 kB	com.dsi.ant.server
ANT+ Plugins Service	3.6.10	2.54 MB	com.dsi.ant.plugins.antplus
Adapt Sound	5.3.04	3.92 MB	com.sec.hearingadjust
Android Easter Egg	1.0	230 kB	com.android.egg
Android Services Library	1	12 kB	com.google.android.ext.services
Android Shared Library	1	6 kB	com.google.android.ext.shared
Android System WebView	69.0.3497...	405 kB	com.google.android.webview
Android-Einrichtung	227.5901558	7.52 MB	com.google.android.setupwizard
Android-System	8.1.0	69.48 MB	android
Anwendungs-Installer	8.1.0	86 kB	com.sec.android.preloadinstaller

必须使用的应用程序

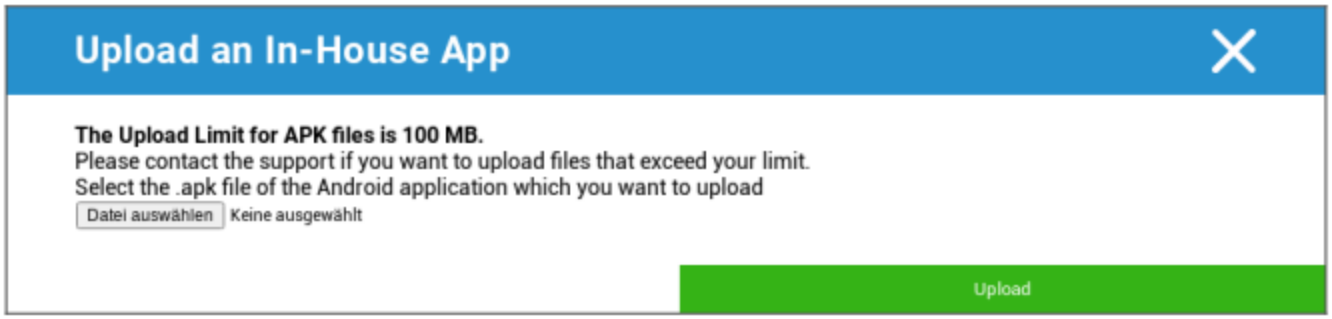
在 "强制应用程序 "下，您可以建立强制要求的应用程序。用户将不断被提示安装该指定应用程序。

通过 ，可以定义强制要求的应用程序。

这可以是您在常规设置中上传的 "Android 内部应用程序 "中的内部应用程序。

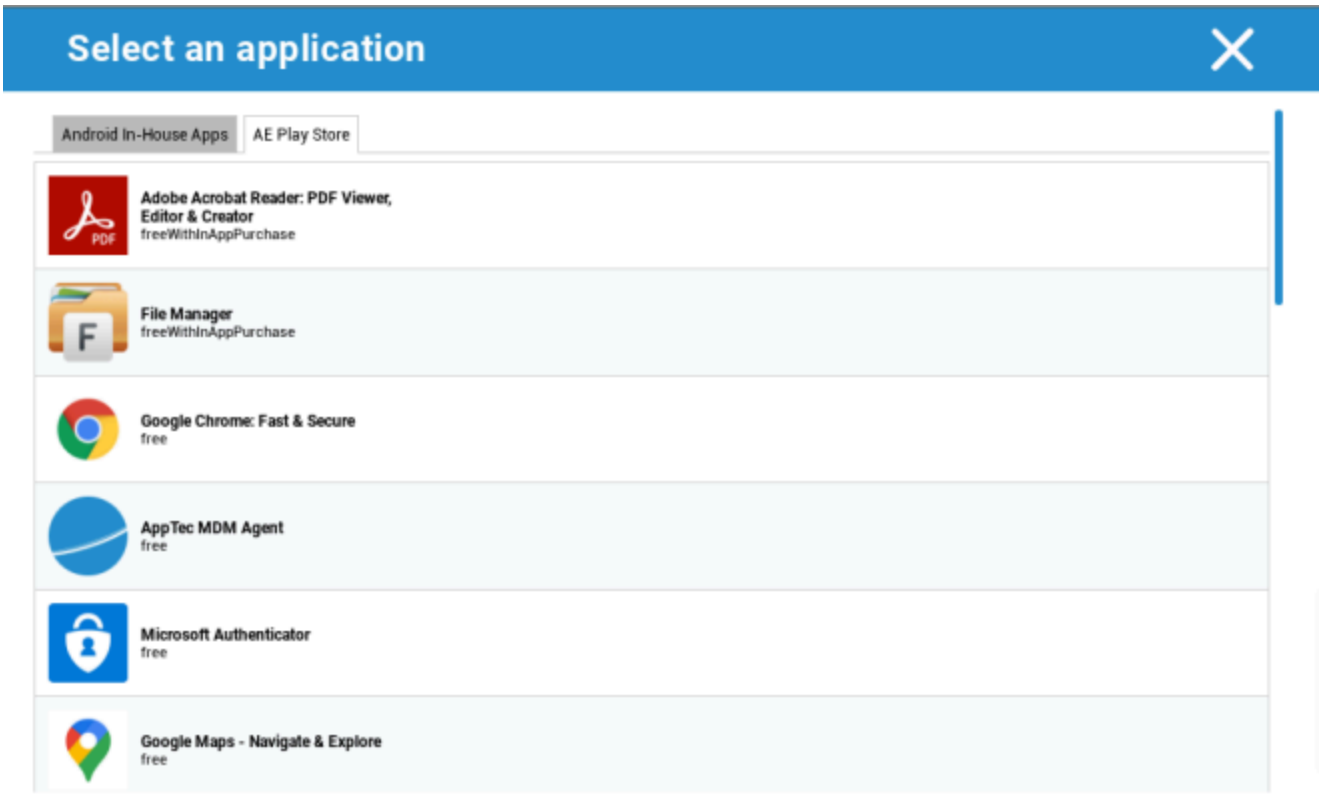


您也可以使用 "上传内部应用程序 "直接选择并上传 apk 文件。



如果安装的是内部应用程序，则可以激活 "保持更新"。如果激活了这一功能，并且在内部应用程序数据库中定义了更新的版本，则会在设备上更新应用程序。

也可以是 Google Work Play Store 中的 "AE Play Store "应用程序。



只有经过批准的 "AE Play Store 应用程序 "才会显示在此选项卡中。

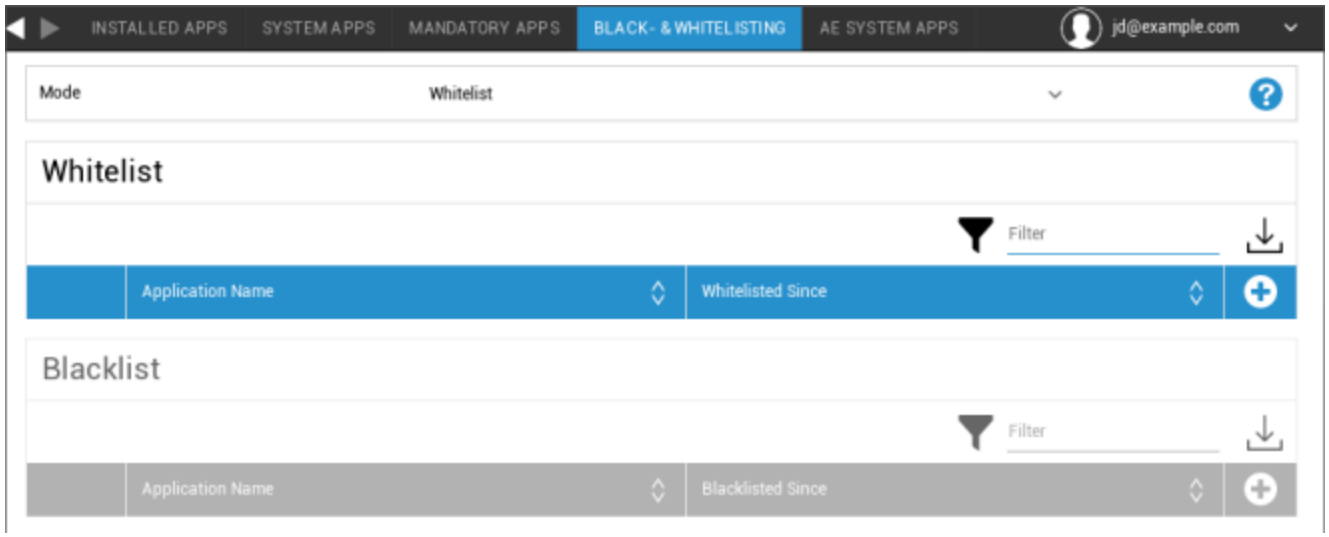
要批准 "AE Play Store 应用程序"，请进入 "常规设置">"应用程序管理">"AE Play"。

商店"，然后通过按钮添加应用程序，该按钮会将你重定向到 "Play Store 应用程序 "选项卡（或者你也可以
直接进入 "Play Store 应用程序 "选项卡）。

在 "Play Store 应用程序 "选项卡中，您可以搜索应用程序。点击应用程序后，应用程序页面将打开，在此您可以点击 "批准 "来批准应用程序。

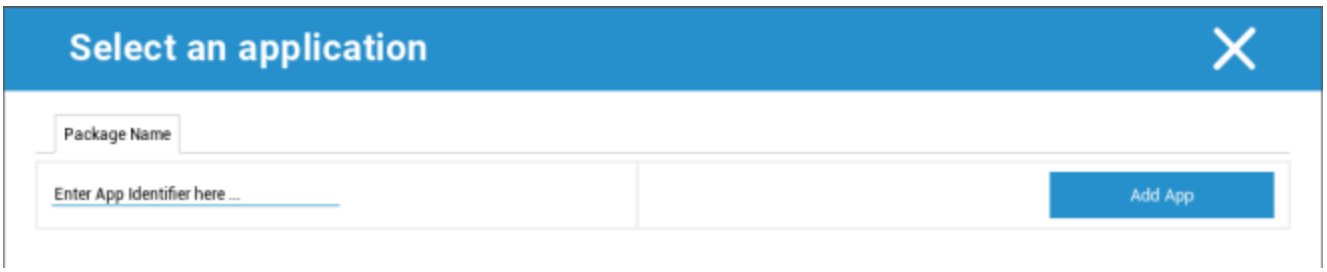
黑名单和白名单

在 "黑名单和白名单 "下，您可以选择 "白名单 "模式或 "黑名单 "模式。



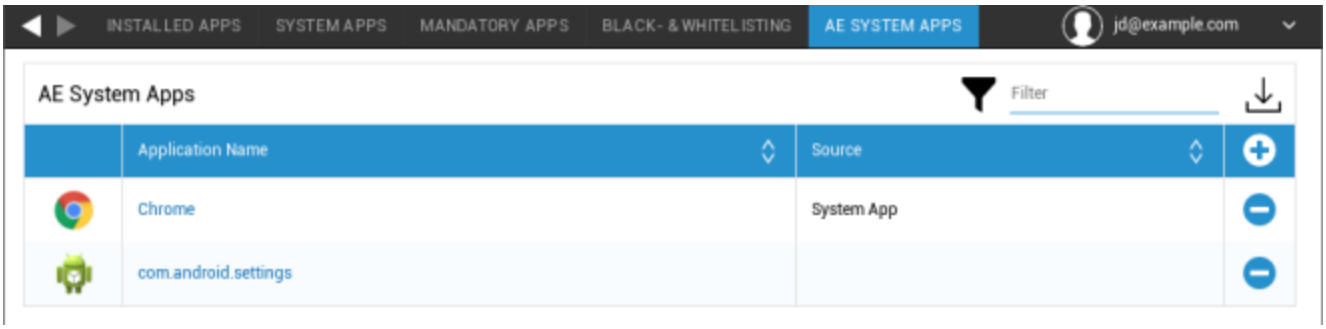
白名单	只有添加到列表中的应用程序和服务才能安装到最终用户设备上。如果这些应用程序和服务已经预装在最终用户设备上，它们将被激活和设置，以便用户运行。
	所有未添加到列表中的其他应用程序都不能安装到最终用户设备上。如果这些应用程序已经预装在最终用户设备上，它们将被停用和设置，这样用户就无法运行它们。
黑名单	添加到列表中的应用程序和服务不能安装到最终用户设备上。如果这些应用程序和服务已经预装在最终用户设备上，它们将被停用并设置为用户无法运行。
	所有未添加到列表中的其他应用程序都可以安装到最终用户设备上。如果这些应用程序已经预装在最终用户设备上，它们将被激活和设置，以便用户运行。

通过 ，您可以将其他应用程序或服务添加到当前使用的列表中。
您可以定义一个 "Packagename"（包名称）：

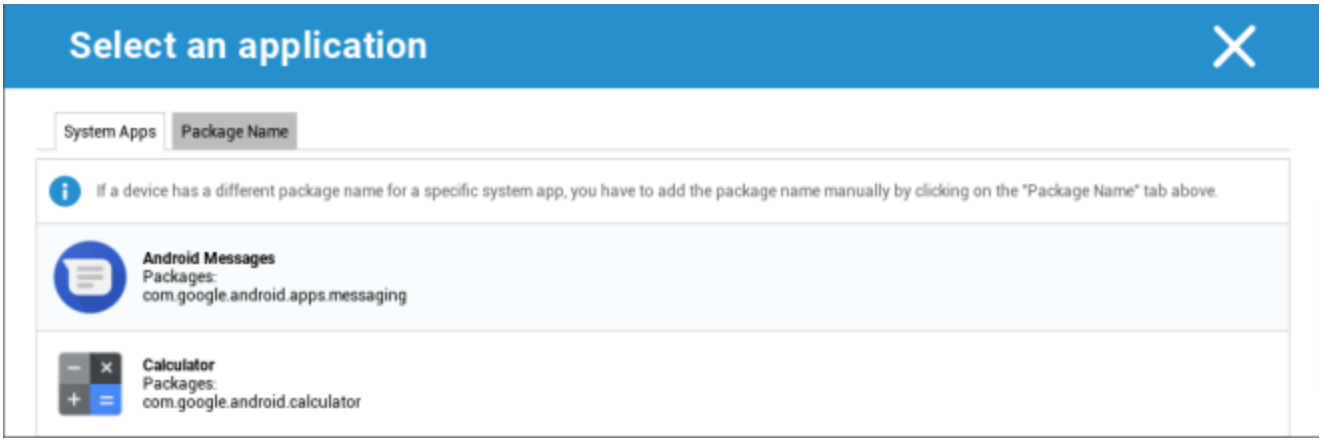


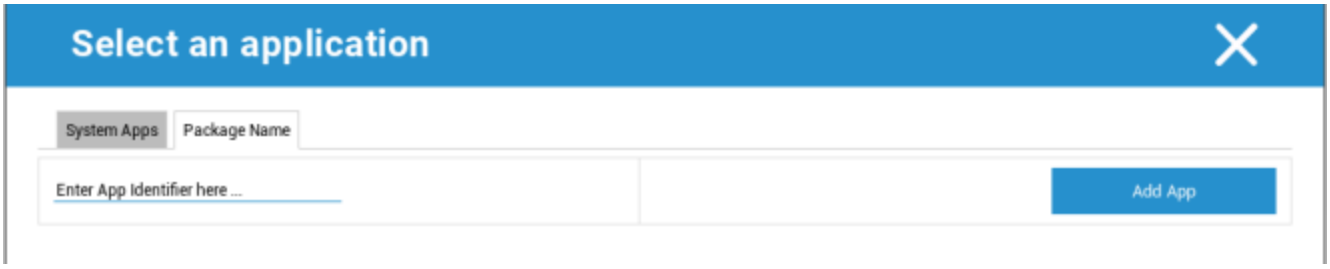
AE 系统应用程序

您可以在此定义一个列表，其中包含应在设备上激活的特定系统应用程序。



点击该按钮后，您可以从 Google 提供的可能的系统应用程序列表中进行选择，也可以直接输入应激活的系统应用程序的软件包名称。





请记住，Google 提供的列表中的系统应用程序只是可以成为系统应用程序的应用程序，并不一定是您设备上的系统应用程序。

不过，该列表只影响已预装的应用程序。

添加未预装在设备上的应用程序不会影响设备，无论该应用程序是来自 Google 提供的列表，还是直接输入应用程序的软件包名称。

限制和设置

应用程序管理设置

您可以在此配置设备有关应用程序更新的行为。

更新检查频率	指定 AppTec360 客户端搜索应用程序更新的时间间隔。默认值为 24 小时。
Wi-Fi 门限	大于指定大小的应用程序将通过 Wi-Fi 下载。如果选择 "仅限 WLAN"，则所有应用程序都将通过 WLAN 下载。

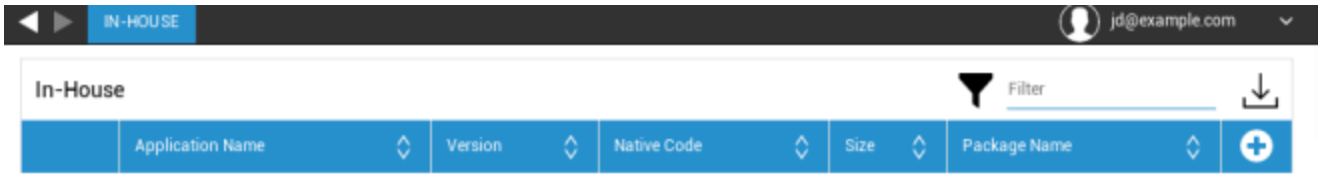
企业应用商店

内部

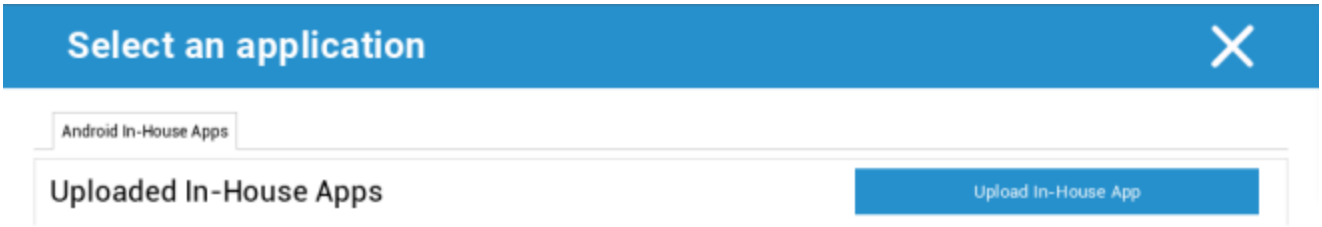
在 "内部 "点下，您可以上传和分发内部开发的应用程序。

有了这个符号，您就可以分发更多的内部应用程序。

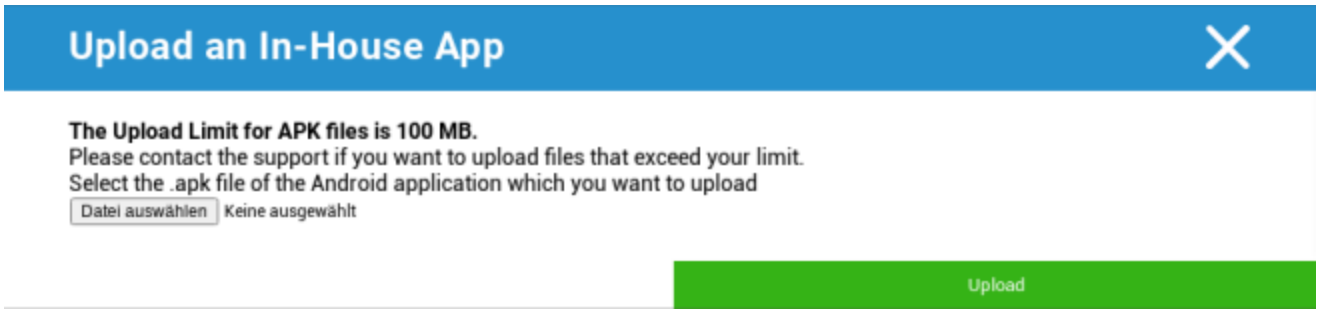
如果您安装的是内部应用程序，您可以激活 "保持更新"。如果
激活了这一功能，并且您在内部应用程序数据库中定义了更新的版本，则该应用程序将在设备上更新。



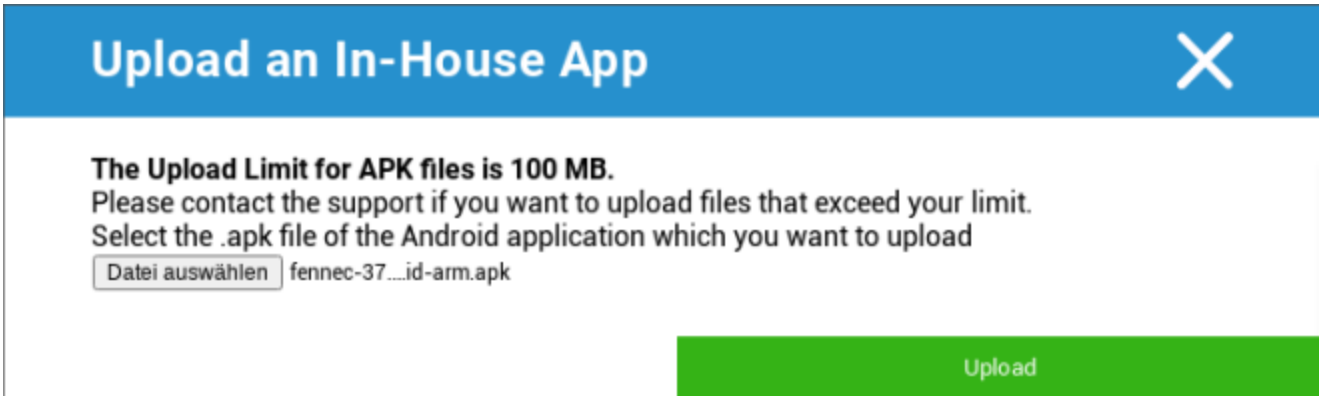
如果您没有分发内部应用程序，您将收到以下概述：



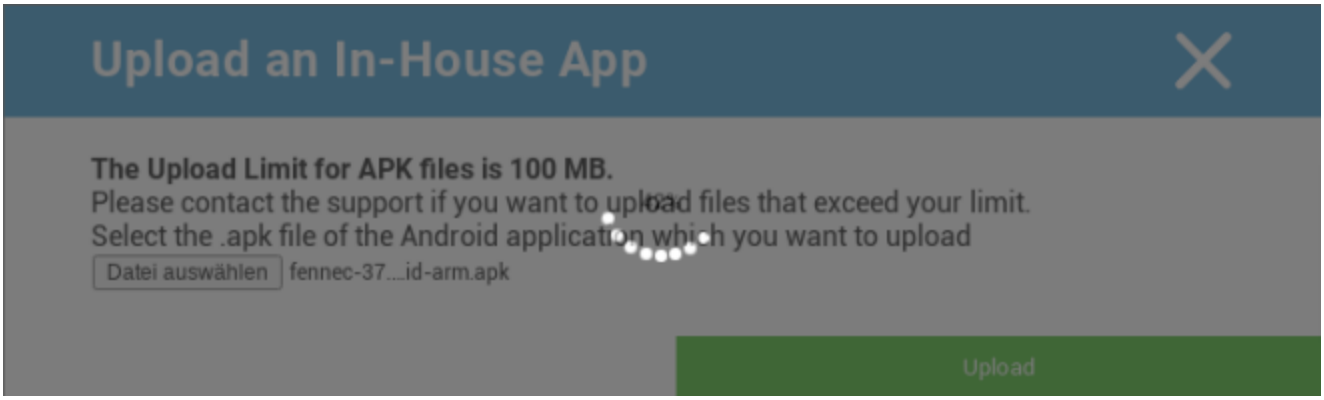
为此，请单击 "上传内部应用程序"，然后您将收到以下概览：



现在，用 "搜索... "选择一个 .apk 文件，然后点击 "上传"。



现在，您的应用程序将被上传，在圆圈中间，您将看到一个百分比指示器，
，显示您的应用程序已经上传了多少内容。



如果您的内部应用程序上传成功，您就可以在应用程序目录中找到上传的应用程序
。

现在，用户可以选择在最终用户
设备上的 AppTec360 商店 "内部 "类别下查看和安装该应用程序。

由于不涉及 Google PlayStore 应用程序，用户无需在各自的终端设备上存储 Google
ID。

企业 Play 商店

AE Play 商店

您可以在此向 Android 企业 Playstore 添加应用程序。请注意，您必须先用 AE 管理员账户批准 Apps，然后才能添加它们。

如需批准应用程序，请参阅 "强制性应用程序 "中的说明。

信息亭模式和启动器

信息亭模式

Kiosk 模式允许您预先定义一个应用程序或一个 URL。然后，
运行/访问该应用程序或 URL。

同样，各种硬件按钮也可以在信息亭模式中停用。

自动启动	一旦配置文件到达终端用户设备，就自动启动 Kiosk 模式
预定的信息亭模式?	您可以为信息亭模式规划一个时间，它将在您设定的时间自动开始和结束
开始时间	开始时间
时间（分钟	信息亭模式再次结束的时间（以分钟为单位

应用类型

单一应用程序	如果想以 Kiosk 模式启动应用程序，请在 "应用程序类型 "下选择 "软件包"。
信息亭应用	单击此处，选择应在 Kiosk 模式下启动的应用程序 您将看到常用的应用程序管理概览 您可以在 "Google Play 商店"、"Android 内部应用程序 "和 "软件包名称 "之间进行选择

应用类型

网址	如果要在 Kiosk 模式下启动 URL，请在 "应用程序类型 "下选择 "URL"。 然后定义所需的 URL 地址
闲置后清除浏览器	您可以在这里定义一个时间间隔（以分钟为单位），在该时间间隔之后重新启动信息亭模式。
清除网页缓存和 Cookie	如果激活此功能，则在重新启动 Kiosk 模式后，网络缓存（cookie 和缓存图片）将被清除
同源政策	如果激活该功能，则用户只能浏览指定 URL 的子页面 例如，您定义了以下 URL:www.mypage.com然后，用户可以在以下网址上网： www.mypage.com/subpage
白名单 URL	在这里您可以维护一个白名单，所有这些 URL 都是允许的 每行最多 1 个 URL URL 必须以 http:/ 或 https:// 开头
黑名单 URL	在这里您可以维护一个黑名单，所有这些 URL 都是不允许的 每行最多 1 个 URL URL 必须以 http:/ 或 https:// 开头
屏幕方向	该设置与屏幕调整有关 自动 = 自动 纵向 = 垂直格式 横向 = 横向模式

多功能应用程序	如果选择 "多应用 "信息亭模式，则将强制使用 AppTec360 启动器。
应用程序	应用程序：选择 Playstore 或内部应用程序作为 Kiosk 应用程序。也可以输入软件包名称。所选的 Kiosk 应用程序必须安装在设备上。请记住将 Kiosk 应用程序设置为必选。 主屏幕上的快捷方式：如果设置为 "开"，将在主屏幕上创建快捷方式。如果设置为 "关闭"，应用程序仍将显示在应用程序列表中。

启用退出密码	如果激活了该功能，用户就可以使用预先设置的密码结束信息亭模式。
退出密码	这是您预先设定的密码
自动折叠状态栏	如果启用该选项，状态栏将自动按字母顺序排列。使用该选项，用户可以看到状态栏的信息，但无法访问其功能
禁用状态栏	状态栏包含通知、快捷方式和信息。仅适用于配备 SAFE 4.0 或更高版本的三星设备。
禁用音量键	禁用音量键（仅适用于配备 SAFE 3.0 或更高版本的三星设备）
禁用开/关开关	禁用开/关开关（仅适用于配备 SAFE 3.0 或更高版本的三星设备）
禁用主页按钮	禁用主页按钮。如果激活了该功能，则只能在 AppTec360 控制台中终止 Kiosk 模式。 (仅适用于配备 SAFE 3.0 或更高版本的三星设备）
禁用导航栏	使用此功能可以禁用导航栏（返回/菜单） 如果激活了该功能，则只能在 AppTec360 控制台中终止 Kiosk 模式 (仅适用于配备 SAFE 3.0 或更高版本的三星设备）

AppTec360 启动器

启用 AppTec360 启动器	开启：启用 AppTec360 启动器。用户必须将其设置为默认启动器一次。 注：如果启用了 Kiosk 模式，且 Kiosk 模式设置为 "多应用程序"，则将强制使用 AppTec360 启动器。
大图标	打开：在启动器中显示更大版本的应用程序图标
隐藏 AppTec360 应用程序图标	开启：完全隐藏 AppTec360 应用程序
隐藏 AppTec360 商店图标	开启：完全隐藏 AppTec360 企业应用商店

AppTec360 设置

启用 AppTec360 设置应用程序	AppTec360 设置应用程序可控制 WiFi 和蓝牙连接
在多应用程序中启用设置信息亭模式	如果启用，用户可在多应用信息亭模式激活时访问 AppTec360 设置应用

遥控器

泼水节

要启动设备的远程控制会话，需要在设备上安装应用程序 "Splashtop Streamer"，方法是将该应用程序添加到**应用程序管理 → 企业应用程序管理器 → 必选应用程序**。

然后，为 Splashtop 配置以下设置：

启用 Splashtop	如果启用，AppTec360 将配置 Splashtop 应用程序以允许远程控制
部署代码	访问https://my.splashtop.com并登录您的 Splashtop 账户。单击 "添加计算机 "并从生成的页面中复制 12 位部署代码。
设置自定义部署网关?	部署网关
部署网关域/主机	部署网关
证书验证	证书验证

然后，您可以使用上下文菜单中的 Splashtop Remote Control（搜索栏旁边的齿轮，当设备被选中时或右键单击树中的设备）选项来启动远程控制会话。

TeamViewer

要启动设备的远程控制会话，需要在设备上安装应用程序 "TeamViewer QuickSupport"，方法是将该应用程序添加到**应用程序管理→企业应用程序管理器→必选应用程序**。

然后，您可以使用上下文菜单中的**TeamViewer Remote Control**选项（当设备被选中时，搜索栏旁边的齿轮或右键单击树中的设备）启动远程控制会话。

内容管理

内容框

在这里您可以激活内容框。

只要将 "启用 ContentBox "切换为 "开"，就会在终端用户设备上自动安装一个独立的 ContentBox 应用程序

。

安全浏览器

您可以在此配置 AppTec360 安全浏览器的设置。

只要将 "安全浏览器 "部分切换为 "打开"，就会在最终用户设备上自动安装一个单独的浏览器应用程序。

要求密码	要求用户设置并使用密码访问浏览器。
最低要求密码长度	设置密码所需的字符数
密码质量要求	设置所需的密码质量
限制下载/打开	
限制上传	
上传白名单	始终允许上传的 URL 列表。
允许复制	允许复制、剪切或共享网页内的文本。
允许屏幕捕捉	允许截图
数据清理频率	选择自动删除所有用户数据（历史记录、缓存等）的频率。
公司书签	书签将显示在浏览器书签中的 "公司书签 "文件夹中。 用户无法对其进行编辑。
隐藏地址栏	
浏览器内白名单（无通用网关）	启用客户端 URL 白名单。 • 公司书签始终列入白名单 • 仅支持 100 个 URL • 请使用通用网关进行无限制的黑名单和白名单设置
白名单 URL	允许使用的 URL 列表。
基于网关的黑白名单设置	黑名单有以下要求 • 正常运行的 AppTec360 通用网关（"常规设置"→"通用网关） • 带有指定 DNS 服务器的有效 VPN 配置（"常规设置"→"通用网关"→"VPN 设置） • 黑名单配置（"常规设置"→"通用网关"→"网域黑名单） • 配置文件中的有效 VPN 连接（"连接管理"→"VPN）

附加应用程序接口

三星 KNOX

限制条件

允许使用 SD 卡	
允许写入 SD 卡	
允许屏幕捕捉	
允许使用剪贴板	
在 Google 云中备份设置和应用程序数据	
重新安装应用程序时从 Google 云恢复设置	
允许 USB 调试	
允许谷歌崩溃报告	
允许出厂重置	
允许 OTA 升级	
允许 USB 主机存储	如果启用，用户可以连接任何笔式驱动器（便携式 USB 存储器）、外置硬盘或安全数字（SD）读卡器，并将其作为存储驱动器安装到设备上。
允许 USB 媒体播放器（MTP、PTP）	
允许麦克风	禁用第三方应用程序的麦克风
允许 NFC（近距离无线通信）	
允许未知来源（APK Sideloading）	如果启用，则允许侧载应用程序（APK 文件）。 一旦禁用此设置，用户就必须在重新允许安装未知来源的 APK 时手动启用它。
允许创建用户	如果启用，则允许用户在设备上创建多个账户，例如访客账户

电子邮件

电子邮件地址	
传入服务器协议	
传入服务器地址	
传入服务器端口	
传入服务器登录名/用户名	
传入服务器密码	
传入服务器使用 SSL	
传入服务器使用 TLS	
传入服务器接受所有证书	
发送服务器协议	
发件服务器地址	
外发服务器端口	
发件服务器使用额外的证书	如果禁用，系统也会将传入凭据用于传出服务器。
发件服务器登录名/用户名	
发件服务器密码	
传出服务器使用 SSL	
发件服务器使用 TLS	
发件服务器接受所有证书	
设置签名	
签名	注意：对于某些设备，必须以 HTML 格式指定签名。
收到新电子邮件时通知用户	

交流

电子邮件地址	
服务器主机名	Exchange 服务器的主机名
登录名	用于登录 Exchange 服务器的用户名
域名	如果启用了 ACL 网关配置，并且域字段不是空的，AppTec360 通用网关将使用以下名称 "Domain\Login Name "对设备进行验证
密码	
同步的天数	
同步电子邮件的频率	
漫游时同步	
设置签名	
签名	注意：对于某些设备，必须以 HTML 格式指定签名。
默认账户	
使用安全套接字层（SSL）	
使用传输层安全（TLS）	
接受所有证书	

APN

APN 显示名称	
接入点名称	APN 名称
发送服务器协议	
MCC - 移动电话国家代码	留空以使用已安装 SIM 卡的 mmc
MNC - 移动网络代码	留空以使用已安装 SIM 卡的 mnc
服务器地址	
服务器端口号	
服务器代理地址	
彩信服务器地址	默认留空
彩信端口号	默认留空
彩信代理地址	默认留空
用户名	
密码	
接入点类型	可接受的类型有 "default"、"mms "和 "supl"。
	如果传递的信息为空，则默认使用 "default,supl,mms"。
	默认留空。
首选 APN	

蓝牙

允许通过蓝牙发现设备	
允许蓝牙配对	
允许蓝牙耳机设备	
允许蓝牙免提设备	
允许蓝牙 A2DP 设备	A2DP（高级音频分配规范）允许在设备之间进行音频流传输
允许拨出电话	
允许通过蓝牙传输数据	
允许蓝牙连接	
允许通过蓝牙连接电脑	

连接

仅允许紧急呼叫允许无线网络连接	
Wi-Fi 网络最低安全级别	
禁止用户添加 Wi-Fi 网络	只有在 "连接管理 "中定义了至少一个活动的 Wi-Fi 配置文件，才能激活该限制。
允许短信和彩信	
允许漫游期间同步	
允许语音漫游	

安卓企业 – 带工作配置文件的完全托管设备 (COPE)

COPE 的一般解释

COPE 是**Corporate Owned Personally Enabled 的**缩写。

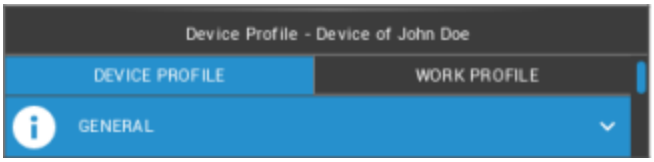
COPE 模式允许将安卓设备注册为集成了**安卓企业- 容器**配置文件的**安卓 企业- 完全管理设备** 。

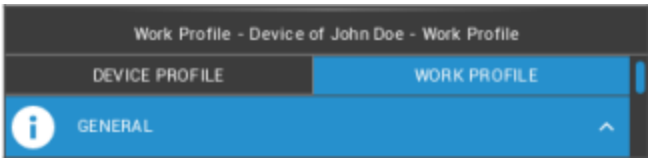
这既可以是已经注册为 "**安卓企业-完全托管设备 "**的安卓设备，并在其上额外设置了 "安卓**企业-容器"**；也可以是新注册的安卓设备，直接注册为 "安卓**企业-完全托管设备**"，并在其上设置了 "安卓**企业-容器"**。

COPE 模式仅适用于安卓 8、9 和 10 系统的设备

配置 COPE 设备的预案

由于 COPE 模式本身没有配置文件，因此在 COPE 配置文件中，**Android 企业 - 完全管理设备**和 **Android 企业 - 容器**的配置被分为两个配置文件。通过点击控制台左侧的相应按钮，可以在两个配置文件之间切换每个配置文件的配置：





这两个预案都可以按照每个预案的说明进行配置：

安卓企业 - 全面管理设备

安卓企业 - 容器

恢复到 AE 完全托管设备

可按照 "**移动管理**"中的说明删除 **Android 企业 - 容器**配置文件。

删除容器配置文件后，COPE 配置文件将转变为 "**Android 企业 - 完全管理设备**"配置文件。

安卓企业 – 容器配置

根据您当前选择的是组配置文件还是设备，概览及其子点有所不同，请仔细考虑！

一般情况

配置文件概览（仅限配置文件级别）

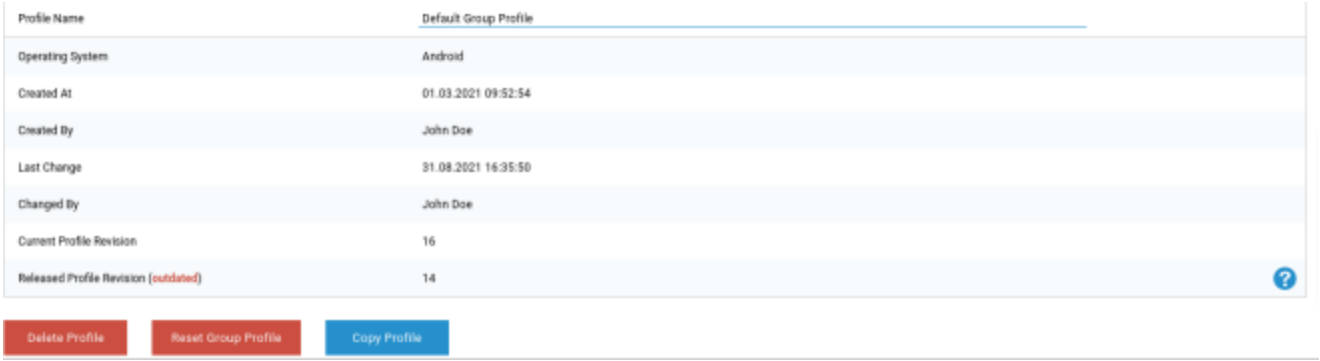
如果您在某个个人资料中，您将收到该个人资料的简要概述，包括名称、操作系统、创建日期、作者等。

简介名称	简介名称 - 可在此处直接重命名
操作系统	配置文件的有效操作系统
创建于	创建日期
创建者	创建者
最后的变化	最后更改日期
已更改	对该配置文件进行最后更改的用户
当前的简介修订	个人资料已更新的次数
已发布的简介修订版	配置文件已更新和已分配设备的次数

删除简介	删除简介
重置组配置文件	重置组配置文件
复制简介	复制简介

组概况概览（仅适用于组级）

打开群组资料时，您将快速浏览该资料。



简介名称	个人资料名称（可在此处更改）
操作系统	配置文件适用的操作系统
创建于	创建时间
创建者	个人资料创建者
最后的变化	最后一次更改配置文件的时间
已更改	最后更改的账户
当前的简介修订	修订已保存的配置文件状态
已发布的简介修订版	已分配的配置文件修订版（"立即分配"）。如果标签文字后面显示"（已过期）"，则表示您已经保存了配置文件，但尚未分配，因此设备仍将获得旧版本。

设备概述（仅限设备级别）

如果您正在使用一个设备，您将收到所选设备的概述，其中包含以下内容：

设备名称	设备名称
地点	位置坐标
电话号码	电话号码
指定的强制性应用程序	分配的强制性应用程序数量
操作系统版本	设备的操作系统版本
操作系统	操作系统（安卓企业版）
序列号	设备序列号
设备所有权	公司或私人设备
设备类型	AE 工作管理设备
扎根	状态，显示设备是否已被 root
符合要求	符合准则要求
IP 地址	设备的 IP 地址
最后查看	设备最后一次连接 AppTec 的时间点
最后一搏	最后一次向设备发送推送的时间点
用户分配	分配给该设备的用户或组

配置修订

在这里，您可以看到为设备分配的组配置文件的概览。

如果点击组配置文件，就可以直接进入该配置文件并进行设置。

使用此符号，可以将已分发的应用程序还原为群组配置文件的设置。

使用此符号，可以将所有使用过的应用程序还原为群组配置文件的设置。

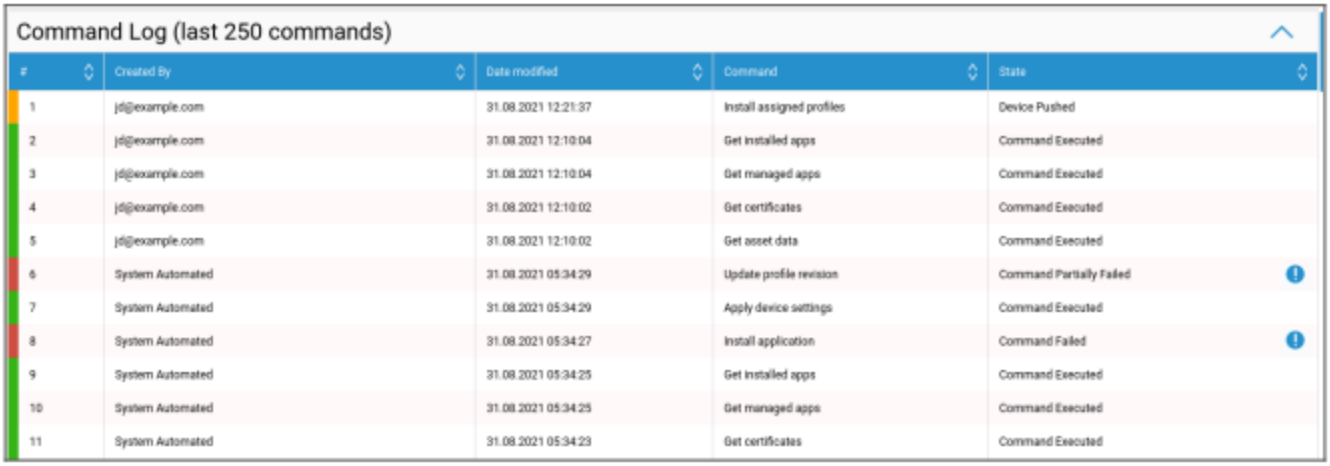
"最新版本可用 "表示组配置文件已更改并保存，但尚未分配。必须在组级别上使用 "立即分配 "来分配组配置文件，才能将更改应用到设备上。

设备日志（仅限设备级）

在这里，您将收到各种设备日志。如有需要，您可以直接在此查找错误原因。

命令日志

在这里，您可以查看为设备发出的命令及其状态。



可能的命令状态

设备已推送	推送请求已发送至推送服务（如 APNS），以通知设备连接回 EMM 服务器。
创建命令	该命令已在系统中创建。
发送命令	设备与服务器连接后，命令被发送到设备。
命令已执行	命令已成功执行。
命令失败	命令失败。*
命令部分失败	根据设备操作系统的不同，有些命令可能会被组合在一起。 其中，该命令组的某些部分出现故障。*
命令已执行，但最终失败	命令已执行，但也可能没有执行。
命令重发	命令被用户重新推送。
弃用	命令被丢弃。例如，该命令被其他命令取代，或设备重新注册，旧命令被删除。

*如果信息后面有感叹号，您可以用光标悬停在图标上，获取更多信息。

设备设置

客户端配置

在这里，您可以对安卓设备进行以下配置：

违规时间	用户响应超时限制，超时后将执行强制措施。
合规超时后的执法行动	当用户不执行导致设备状态合规的操作时采取强制措施
数据收集频率	收集设备/GPS 信息的频率
设备心跳频率	设备联系 AppTec 服务器的时间间隔 分钟1 分钟 最长24 小时
启用位置更新	如果激活，设备会向 AppTec 服务器发送位置更新
地点更新时间	确定设备向 AppTec 发送位置更新的时间间隔
使用 Google 定位精度进行位置更新	如果激活，位置更新将使用网络位置（如果在 "限制 "下停用，则此设置不会产生任何影响）。
使用 GPS 定位进行位置更新	如果激活，将使用 GPS 进行位置更新
允许模拟（伪造）位置	允许通过第三方应用程序伪造位置信息
失去连接行动	如果启用，则可以为设备在心跳时间间隔内未与 MDM 服务器建立连接的情况指定操作。例如，如果设备的心跳时间为 5 分钟，它就会在上午 10:35 连接到服务器。之后，设备离开 Wi-Fi 范围。上午 10:40 时的下一次心跳将失败，指定的操作将被执行。
行动	一旦设备不符合要求，应立即采取的行动。 • Lock Device = 锁定设备 • 擦除设备 = 设备将恢复出厂设置 • 擦除设备和 SD 卡 = 设备将恢复出厂设置，SD 卡存储将被删除
阈值	您可以指定触发指定操作所需的失败心跳阈值。

政策执行模式	默认值：	将定期提示用户执行未执行的操作
	懒惰的政策执行	永远不会提示用户执行未执行的操作。所有未执行的操作都将显示在 AppTec 客户端中
	积极执行政策：	会不停地提示用户执行未完成的操作

AppTec 版本锁	如果启用，可以指定 AppTec 应用程序的版本代码。AppTec 客户端只会更新到指定的版本。较新版本将被忽略。不可能降级。
版本代码	要锁定的 AppTec 应用程序的版本代码。
禁用 AppTec 通知	如果禁用，AppTec 客户端将不会在通知栏中显示通知。因此，用户可以通过任务管理器关闭 AppTec 客户端。如果关闭 AppTec 客户端，包括 Kiosk 模式和应用程序黑名单/白名单在内的多项功能将无法正常工作。 三星设备为 AppTec 客户端提供保护机制。支持 KNOX API 的三星设备默认禁用通知功能。 使用 Android 8.0 或更高版本的设备不应禁用该通知。

壁纸

设置自定义壁纸	启用/禁用自定义壁纸
壁纸	将壁纸模式设置为使用颜色代码或图像
指定颜色	以十六进制值指定背景颜色，如 #000000 表示黑色或 #ffffff 表示白色
将图像设为壁纸	上传要用作壁纸的图像文件

资产管理（仅限设备级）

设备信息

模型	设备型号
操作系统	操作系统
操作系统版本	操作系统版本
序列号	序列号
设备名称	设备名称
电池状态	电池状态
可用/总内存	可用/总内存
三星保险箱	三星 SAFE 界面，各种设置选项所需的界面
可用 SD 卡	可使用 SD 卡
模拟 SD 卡	模拟 SD 卡
可移动 SD 卡	可移动 SD 卡
SD 可用/总内存	SD 可用/SD 卡总内存

无线网络

IP 地址	设备 IP 地址
WiFi MAC	WiFi MAC 地址

细胞

现状	状态（已安装 SIM 卡）
电话号码	电话号码
漫游（语音/数据）	语音/数据漫游
漫游状态	当前漫游状态
IP 地址	IP 地址
运营商/承运商	运营商/承运商
蜂窝技术	蜂窝技术
IMEI	IMEI 号码
ICCID	这是 SIM 卡的 ID，通常也是智能卡或集成电路卡 (ICC)
IMSI	在 GSM 和 UMTS 移动网络中，国际移动用户标识（IMSI）提供了网络用户的明确标识 IMSI 最多由 15 位数字组成，配置方式如下： • 移动国家代码(MCC)，3 位数 • 移动网络代码(MNC)，2 或 3 位数 • 移动用户识别码 (MSIN)，1-10 位数
目前的 MCC/MNC	参见 "SIM MCC/MNC
SIM MCC/MNC	移动国家代码是国际电联根据 E.212 标准制定的国家标识符。它与移动网络代码（MNC）一起用于识别移动网络。 指 SIM 卡的国家/移动网络代码。 如果您漫游到另一个移动网络，那么从逻辑上讲，"当前 MCC/MNC "和 "SIM MCC/MNC "将是不同的。

蓝牙

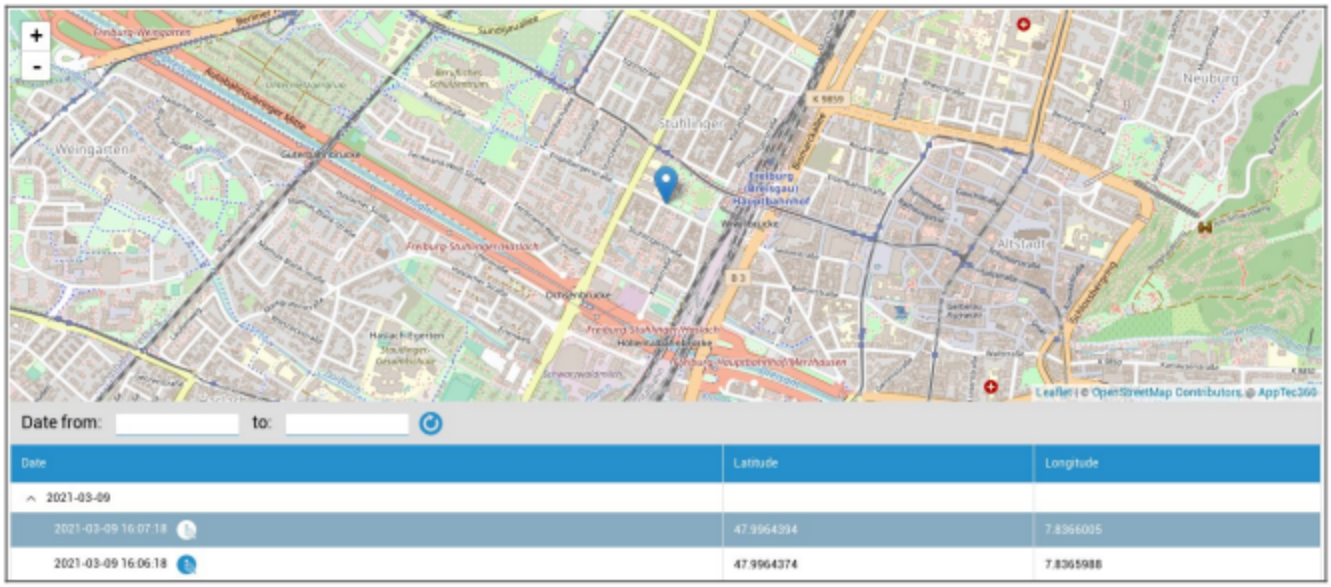
蓝牙 MAC	蓝牙 MAC 地址

安全管理

防盗（仅限设备级）

GPS 信息（仅限设备级别）

您可以在此确定当前/最后的设备位置。可以使用一个甚至两个密码来保护定位功能 - 请参阅 "常规设置"-"隐私"-"GPS 访问"：常规设置 - 隐私 - GPS 访问



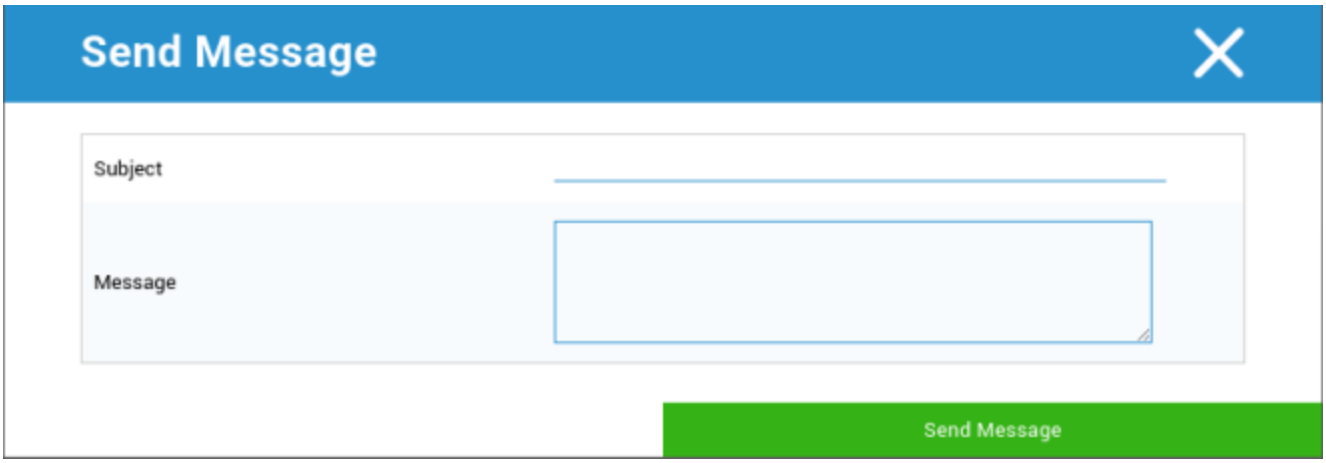
擦除和锁定（仅限设备级别）

在 "擦除和锁定 "下，您可以执行以下三项操作：

全面擦拭	设备将恢复出厂设置（公司和个人数据将被删除）。仅适用于 "增强的工作配置文件
企业擦拭	只从最终用户设备中删除企业数据（由 AppTec 提供的所有应用程序、数据等）
锁定屏幕	屏幕锁已激活，只需使用设备密码/PIN 解锁设备即可

信息（仅限设备级别）

您可以在这里填写主题和信息，然后将其发送到最终用户设备上。



安全配置

设备密码

在 "密码 "下，您可以设置设备密码，有以下设置选项供您选择

最小密码长度	规定密码必须包含的最少符号数	
密码质量	未说明	该政策对密码没有要求。
	生物特征弱	这项政策允许使用低安全性的生物识别技术。这意味着可以识别个人身份的技术，其识别率约为 3 位数的 PIN 码（错误检测率低于千分之一）。
	一些东西	该策略要求设置某种密码或模式，但不执行任何具体规则。
	字母	用户输入的密码必须至少包含字母（或其他符号）字符。
	字母数字	用户输入的密码必须至少包含数字和字母（或其他符号）字符。
	复杂	默认情况下，用户输入的密码必须至少包含一个字母、一个数字和一个特殊符号。利用这种密码质量，可以限制密码包含各种字符集，如至少包含一个大写字母等。
最小密码长度	设置密码所需的字符数。例如，可以要求 PIN 或密码至少有六个字符。	
密码所需的最小数字位数	密码所需的最小数字位数	
密码中至少需要小写字母	密码中至少需要小写字母	
密码中至少需要大写字母	密码中至少需要大写字母	
密码中需要的最少非字母字符	密码中需要的最少非字母字符	
密码所需的最少符号	密码所需的最少符号	

最长闲置时间锁定	时间锁定前用户最长不活动时间
密码过期超时	建立，在此时间间隔后密码失效，必须发布新密码

密码历史限制	不允许使用的密码数量
密码尝试失败次数上限	规定在执行完全设备擦除之前，错误输入密码的频率
允许生物识别身份验证	可通过指纹或虹膜扫描进行身份验证。仅适用于三星 KNOX 2.1 及更高版本

集装箱密码

在 "密码 "下，您可以指定一个容器密码，以下是
可用的设置选项

最小密码长度	规定密码必须包含的最少符号数	
密码质量	未说明	该政策对密码没有要求。
	生物特征弱	这项政策允许使用低安全性的生物识别技术。这意味着可以识别个人身份的技术，其识别率约为 3 位数的 PIN 码（错误检测率低于千分之一）。
	一些东西	该策略要求设置某种密码或模式，但不执行任何具体规则。
	字母	用户输入的密码必须至少包含字母（或其他符号）字符。
	字母数字	用户输入的密码必须至少包含数字和字母（或其他符号）字符。
	复杂	默认情况下，用户输入的密码必须至少包含一个字母、一个数字和一个特殊符号。利用这种密码质量，可以限制密码包含各种字符集，如至少包含一个大写字母等。
最小密码长度	设置密码所需的字符数。例如，可以要求 PIN 或密码至少有六个字符。	
密码所需的最小数字位数	密码所需的最小数字位数	
密码中至少需要小写字母	密码中至少需要小写字母	
密码中至少需要大写字母	密码中至少需要大写字母	
密码中需要的最少非字母字符	密码中需要的最少非字母字符	
密码所需的最少符号	密码所需的最少符号	

最长闲置时间锁定	时间锁定前用户最长不活动时间
密码过期超时	建立，在此时间间隔后密码失效，必须发布新密码
密码历史限制	不允许使用的密码数量

密码尝试失败次数上限	规定在执行完全设备擦除之前，错误输入密码的频率

防病毒

自动扫描	启用定期自动扫描
扫描时间间隔	检查间隔（快速/全面）
全自动扫描	启用全自动扫描
自动更新	启用自动更新
更新检查间隔	多久更新一次应用程序及其数据库（病毒/损坏的代码）
应用程序保护	启用应用程序自动扫描
SD 卡保护	启用自动 SD 卡扫描
仅 Wi-Fi 更新	启用后，只有当设备成功连接到 Wi-Fi 网络时才会应用更新

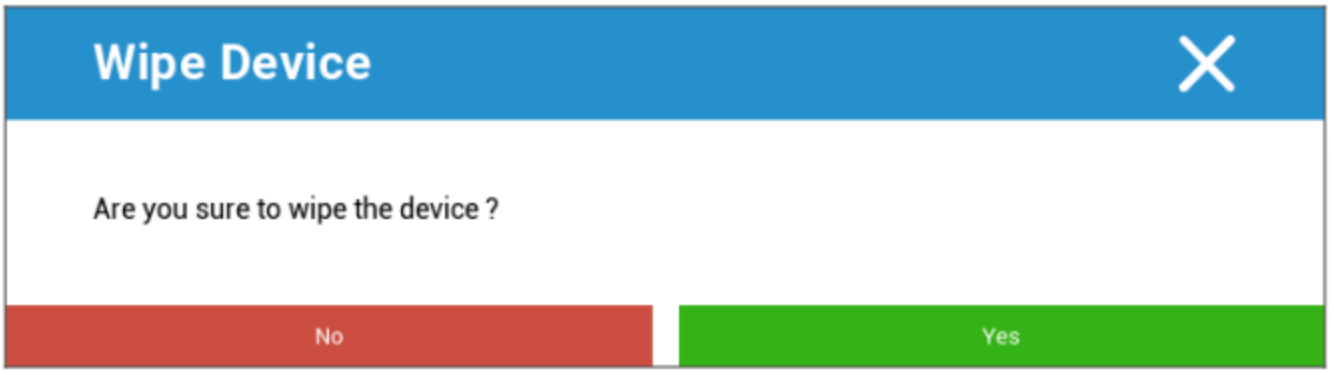
报废（仅限设备级）

擦除（仅限设备级）

在 "擦除 "下，您可以将设备恢复到出厂设置（仅适用于 "增强的工作配置文件"）。

在这里，企业数据和私人数据都将在最终用户设备上删除。

点击 "减号 "后，您将收到以下信息：



如果选择 "是"，则可以执行擦除操作。

在 "擦除报告 "下可显示以下项目

擦拭	进行擦拭的历史
日期	日期
现状	状态（例如擦除是否成功执行）

限制设置

限制条件

在这里，可以限制和阻止各种事物。

合规执行	提示用户模式 - 提示用户执行必要的操作。 模式锁定容器 - 隐藏所有应用程序，直至满足所有要求
运行时权限政策	提示用户新的权限请求 始终批准新的权限请求 始终拒绝新的权限请求 警告：如果权限是自动设置的，有些应用程序在识别权限时会出现问题。如果您总是授予权限，但遇到应用程序提示权限缺失的问题，请将其设置为 "提示用户 "并重新安装应用程序
允许外发剪贴板	允许从容器内部复制和粘贴到外部
允许来电显示解析	根据容器中的联系人显示来电名称
允许联系人搜索解析	拨打电话时，允许在容器联系人中搜索姓名
允许蓝牙联系人共享	允许在车内接触容器
禁止发出 NFC 光束	禁用容器的 NFC
允许未知来源	如果启用，用户可以通过安装 .apk 文件来侧载应用程序。
允许 USB 调试	如果启用，用户可以启用 USB 调试。
禁止修改账户	禁止创建、删除和修改容器中的账户 请注意，某些应用程序需要创建或修改账户才能正常运行

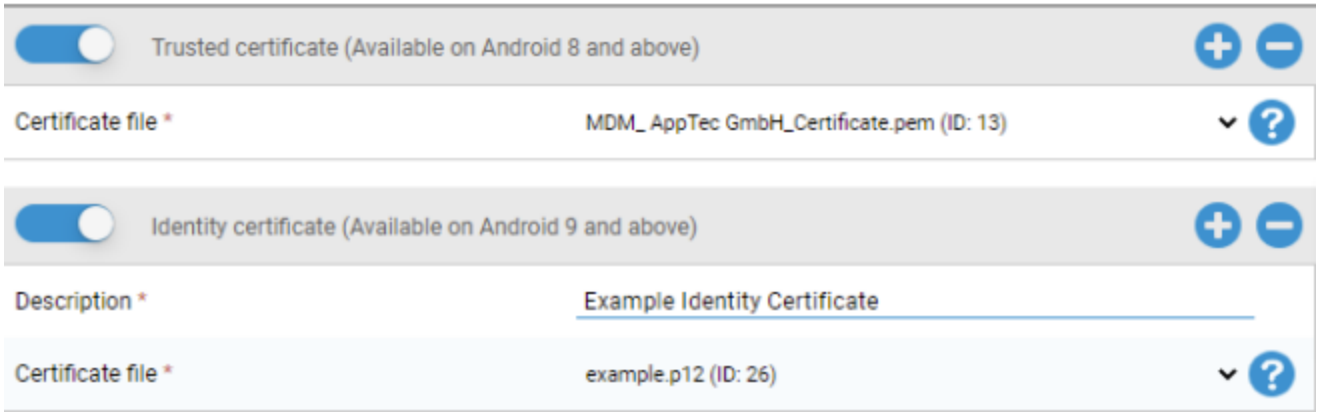
工作配置文件限制。仅适用于 Android 11 及更高版本的设备，带有增强型工作配置文件	
禁止照相机	指定工作配置文件中是否不允许使用摄像机。
禁止蓝牙	指定工作配置文件中是否禁止使用蓝牙。

启用出厂重置保护	激活此选项可将 Android 的 "出厂重置保护 "覆盖至您在 "常规设置"→"Android 配置"→"Android 企业"→"出厂重置保护 "中定义的 Google 帐户。如果启用此选项并重置设备，则必须提供已配置的 Google 帐户才能再次设置设备。
控制操作系统更新	启用此项可将更新行为设置为自动、窗口或延迟。
更新政策	自动：一有更新就自动安装。窗口安装：在每日维护窗口内自动安装。这也会将 Play 应用程序配置为在窗口内更新。强烈建议 kiosk 设备使用此方法，因为这是 Play 更新持续固定在前台的应用程序的唯一方法。推迟：推迟自动安装，最多 30 天。

个人档案限制。仅适用于 Android 11 及更高版本的设备，配备增强型工作配置文件	
禁止照相机	指定个人配置文件中是否禁止使用摄像机。
禁止蓝牙	指定个人配置文件中是否禁止使用蓝牙。
允许未知来源	如果启用，工作配置文件用户可以通过安装 .apk 文件来侧载应用程序。

证书管理

您可以在此向您的设备分发可信证书和身份证书。分发信任证书需要安卓 8 或更高版本，分发身份证书需要安卓 9 或更高版本。



使用 "+"可以添加多个证书。

受信任证书必须是 PEM 格式。

身份证书需要采用 PKCS12 格式。

连接管理

无线网络

为此，请对终端用户设备进行预配置，以便访问内部访问点

服务集标识符（SSID）	要连接的网络的 SSID
隐藏的网络	激活，以防接入点不广播 SSID

安全类型

建立 AP 的安全类型

WEP

密码	AP 密码

WPA/WPA2

密码	AP 密码

802.1x EAP

EAP 方法

工务司	身份	身份
	密码	密码

PEAP	第 2 阶段身份验证协议	无	无附加协议
		MSCHAPV2	MSCHAPV2 协议
		通用技术委员会	全球技术合作协议
	CA 证书	CA 证书	
	身份	身份	
	匿名身份	匿名身份	
	密码	密码	

TTLS	第 2 阶段身份验证协议	无	无附加协议
		PAP	PAP 协议
		MSCHAP	MSCHAP 协议
		MSCHAPV2	MSCHAPV2 协议
		通用技术委员会	全球技术合作协议
	CA 证书	CA 证书	
	身份	身份	
	匿名身份	匿名身份	
	密码	密码	

TLS	CA 证书	CA 证书
	身份	身份
	密码	密码

虚拟专用网

连接名称	VPN 连接名称

VPN 类型

虚拟专用网

VPN 客户端

AppTec VPN 客户端	
网关配置	选择网关 VPN 配置（请参阅**常规设置 > 通用网关 > VPN 设置**）。
始终在线的 VPN	启用本地锁定
启用 AppTec Lockdown	启用 AppTec Lockdown

内置（仅适用于三星设备）			
连接类型	PPTP	服务器	服务器
		启用 PPTP 加密	启用 PPTP 加密
	L2TP / IPSec PSK	服务器	服务器
		IPSec 预共享密钥	IPSec 预共享密钥
		启用 L2TP 秘密	启用 L2TP 秘密
		L2TP 秘密	L2TP 秘密
	IPSec XAuth PSK	服务器	服务器
		IPSec 识别码	IPSec 识别码
		IPSec 预共享密钥	IPSec 预共享密钥
DNS 搜索域	DNS 搜索域		
专家设置	DNS 服务器	DNS 服务器	
	转发路由	转发路由	

开放 VPN		
服务器	服务器	
OpenVPN 简介	OpenVPN 简介	
OpenVPN 应用程序	Android 版 OpenVPN（推荐）	
	连接 OpenVPN	
专家设置	DNS 服务器	DNS 服务器
	转发路由	转发路由

三星 / 强天鹅			
连接类型	PPTP	服务器	服务器
		用户名	用户名
		密码	密码
		启用 PPTP 加密	启用 PPTP 加密
	L2TP / IPSec PSK	服务器	服务器
		IPSec 预共享密钥	IPSec 预共享密钥
		用户名	用户名
		密码	密码
		启用 L2TP 秘密	L2TP 秘密
	IPSec XAuth PSK	服务器	服务器
		IPSec 识别码	IPSec 识别码
		IPSec 预共享密钥	IPSec 预共享密钥
		用户名	用户名
		密码	密码
专家设置	DNS 服务器	DNS 服务器	
	转发路由	转发路由	

思科任意连接		
服务器	服务器	
证书模式	残疾	残疾
	自动	自动
专家设置	DNS 服务器	DNS 服务器
	转发路由	转发路由

每个应用程序的 VPN

VPN 客户端

AppTec VPN 客户端		
网关配置	选择网关 VPN 配置（请参阅**常规设置 > 通用网关 > VPN 设置**）。	
VPN 应用程序	VPN 应用程序	
始终在线的 VPN	启用本地锁定	始终在线的 VPN
启用 AppTec Lockdown	启用 AppTec Lockdown	

三星 / 强天鹅			
连接类型	PPTP	服务器	服务器
		VPN 应用程序	VPN 应用程序
		用户名	用户名
		密码	密码
		启用 PPTP 加密	启用 PPTP 加密
	L2TP / IPSec PSK	服务器	服务器
		VPN 应用程序	VPN 应用程序
		IPSec 预共享密钥	IPSec 预共享密钥
		用户名	用户名
		密码	密码
		启用 L2TP 秘密	L2TP 秘密
	IPSec XAuth PSK	服务器	服务器
		VPN 应用程序	VPN 应用程序
		IPSec 识别码	IPSec 识别码
		IPSec 预共享密钥	IPSec 预共享密钥
		用户名	用户名
		密码	密码
专家设置	DNS 服务器	DNS 服务器	
	转发路由	转发路由	

限制条件

您可以在此设置与连接管理相关的限制条件

允许数据漫游	允许漫游时使用移动数据
强制数据漫游	如果激活，移动数据漫游将永久激活（不建议使用！）。 该设置会覆盖 "允许数据漫游 "设置！
使用系统 http 代理服务器	HTTP 代理服务器的使用由系统设置提供，取决于所连接的网络（WiFi 或 APN）。

PIM 管理

Gmail Exchange

信息：此配置将应用于 Gmail 应用程序。因此，您必须批准并安装 Gmail。

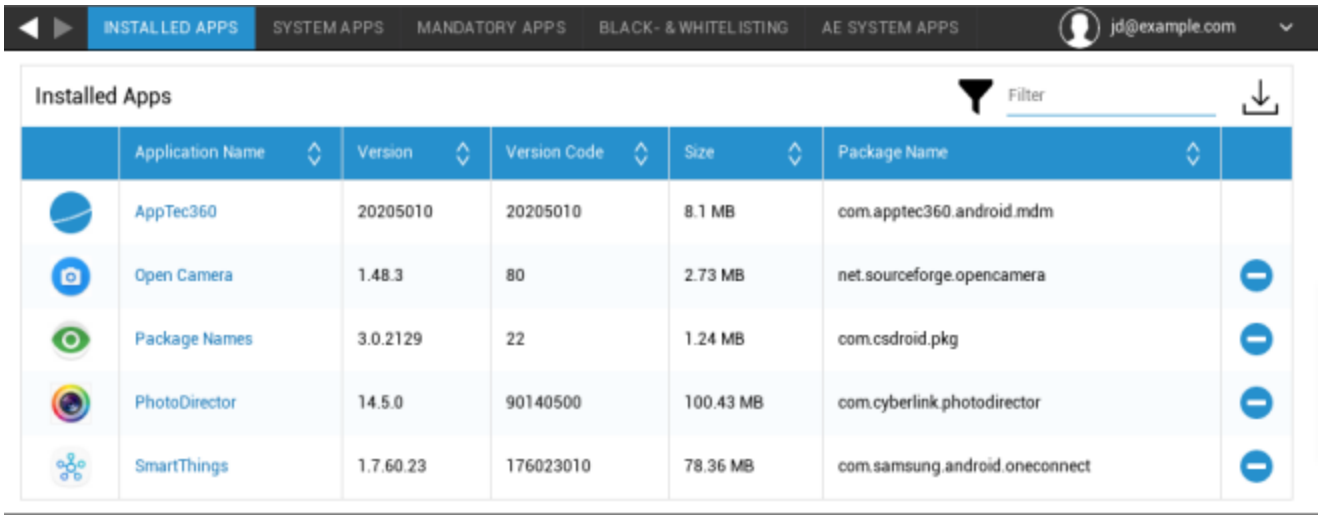
电子邮件地址	提供的用户电子邮件地址 请注意 "占位符"，您可以使用这些占位符来处理凭据，而无需在每台设备上手动执行更改。 只需点击一下，您就可以将它们展示在自己面前
服务器主机名	Exchange 服务器的服务器地址
登录名	终端用户设备的登录名，请注意 "此处的占位符
签名	可附加签名（提示：某些设备要求签名使用 HTML 格式）
同步的天数	天数，决定电子邮件何时同步返回
设备标识符	包含 EAS DeviceID 的字符串。该字符串是 EAS Protokols 的一部分，在某些地区可以使用
使用安全套接字层（SSL）	使用 SSL 连接
接受所有证书	接受所有证书。如果您的 Exchange 服务器使用自签名证书，请选择此选项
允许非托管账户	允许用户添加或删除除本管理配置中指定的帐户以外的任何 Exchange 帐户。如果启用此设置，则无法阻止用户向 Gmail 添加其他 Exchange 帐户。你也无法控制其他应用与用户添加的 Exchange 账户之间的数据共享。只有当用户需要在 Gmail 中维护多个 Exchange 工作账户时，才应启用此设置。
客户证书	客户端证书。仅当您的邮件服务器需要此证书时才需要。

应用程序管理

企业应用管理器

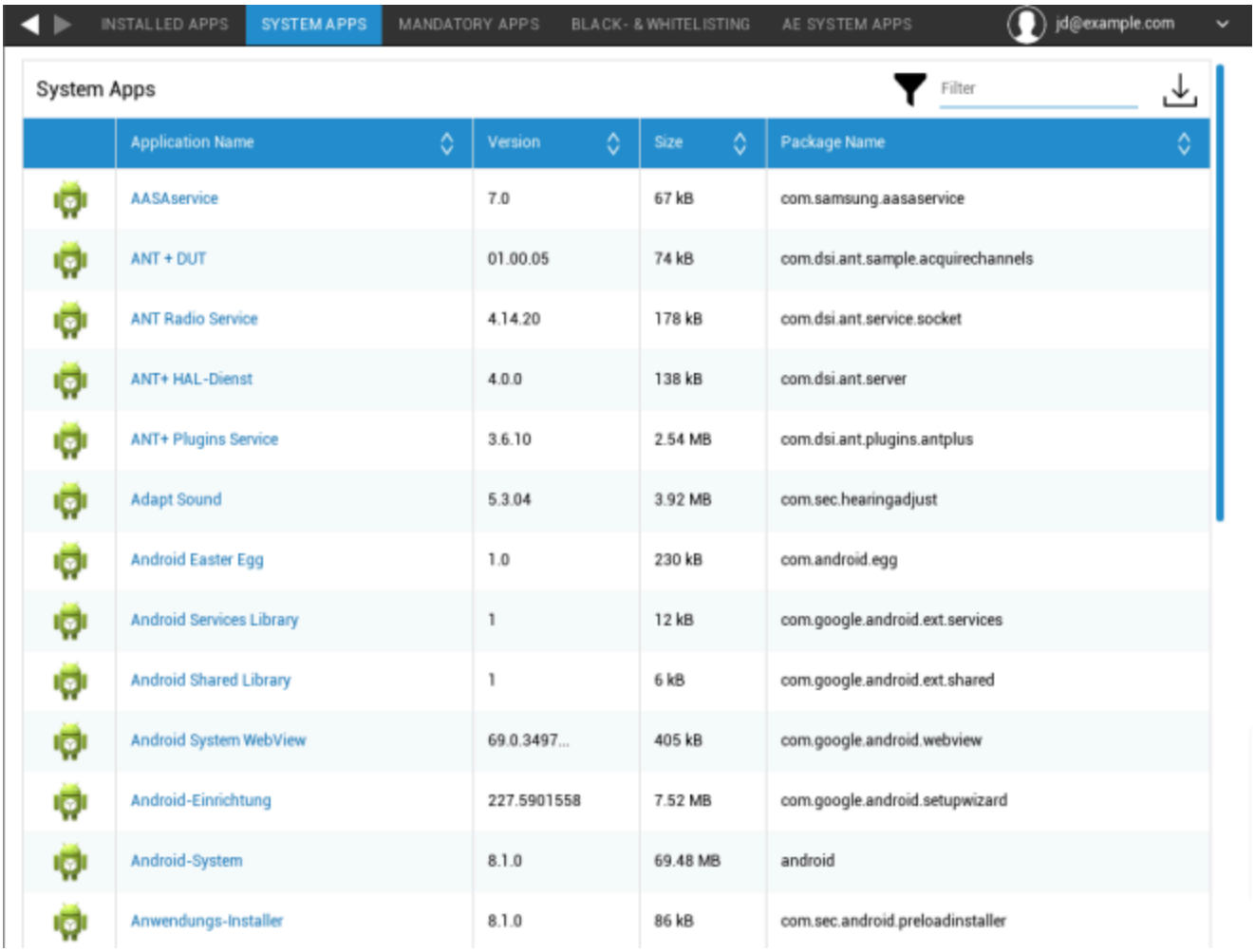
已安装的应用程序（仅限设备级别）

这里将显示当前安装在容器中的所有应用程序。


INSTALLED APPS
SYSTEM APPS
MANDATORY APPS
BLACK- & WHITELISTING
AE SYSTEM APPS
jd@example.com
Installed Apps
Filter
Application Name
Version
Version Code
Size
Package Name
AppTec360 20205010 20205010 8.1 MB com.apptec360.android.mdm
Open Camera 1.48.3 80 2.73 MB net.sourceforge.opencamera
Package Names 3.0.2129 22 1.24 MB com.csdroid.pkg
PhotoDirector 14.5.0 90140500 100.43 MB com.cyberlink.photodirector
SmartThings 1.7.60.23 176023010 78.36 MB com.samsung.android.oneconnect

系统应用程序（仅限设备级）

在 "系统应用程序 "下，将为您列出设备制造商已经安装在最终用户设备上的所有应用程序和服务。



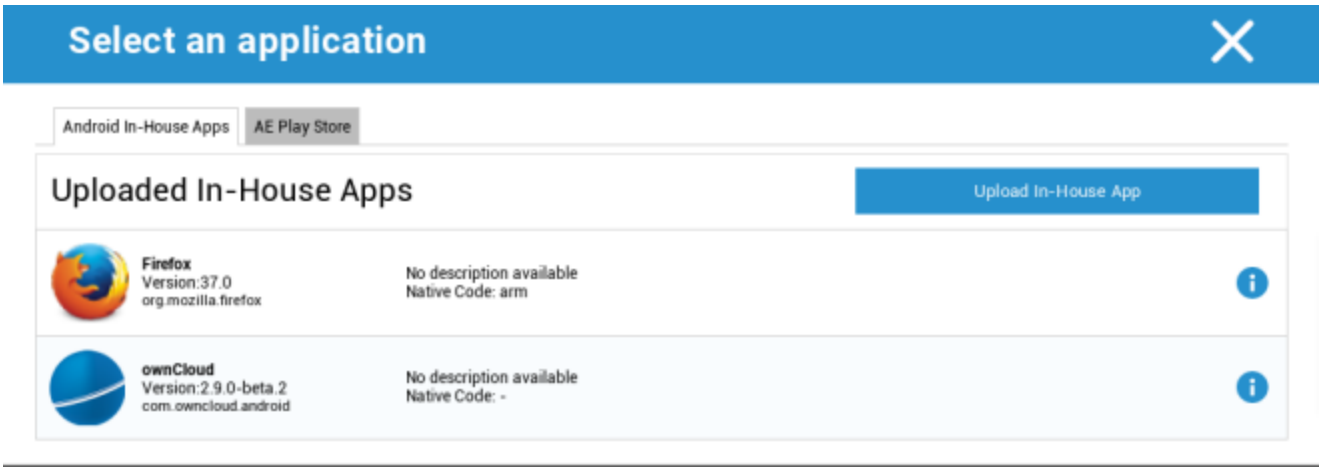
Application Name	Version	Size	Package Name
AASAservice	7.0	67 kB	com.samsung.aasaservice
ANT + DUT	01.00.05	74 kB	com.dsi.ant.sample.acquirechannels
ANT Radio Service	4.14.20	178 kB	com.dsi.ant.service.socket
ANT+ HAL-Dienst	4.0.0	138 kB	com.dsi.ant.server
ANT+ Plugins Service	3.6.10	2.54 MB	com.dsi.ant.plugins.antplus
Adapt Sound	5.3.04	3.92 MB	com.sec.hearingadjust
Android Easter Egg	1.0	230 kB	com.android.egg
Android Services Library	1	12 kB	com.google.android.ext.services
Android Shared Library	1	6 kB	com.google.android.ext.shared
Android System WebView	69.0.3497...	405 kB	com.google.android.webview
Android-Einrichtung	227.5901558	7.52 MB	com.google.android.setupwizard
Android-System	8.1.0	69.48 MB	android
Anwendungs-Installer	8.1.0	86 kB	com.sec.android.preloadinstaller

必须使用的应用程序

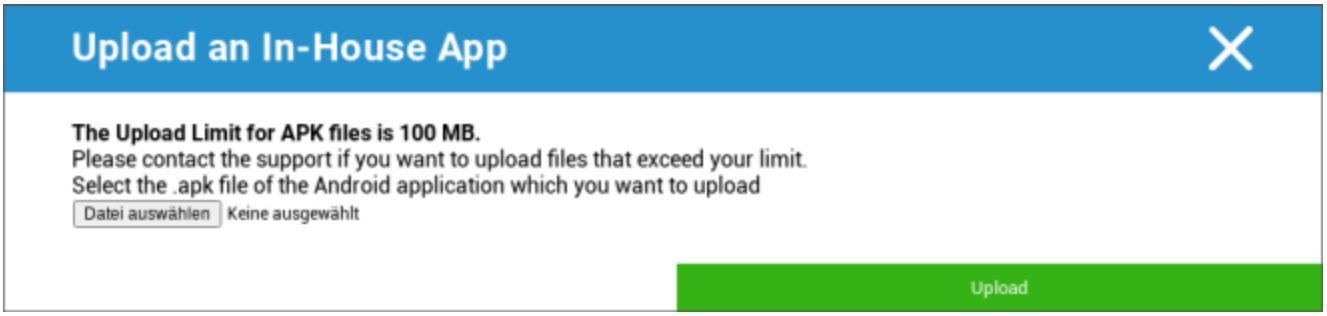
在 "强制应用程序 "下，您可以建立强制要求的应用程序。如果是 InHouse 应用程序，会不断提示用户安装指定的应用程序。Play Store 应用程序将自动安装。

通过 ，可以定义强制要求的应用程序。

这可以是您在常规设置中上传的 "Android 内部应用程序 "中的内部应用程序。

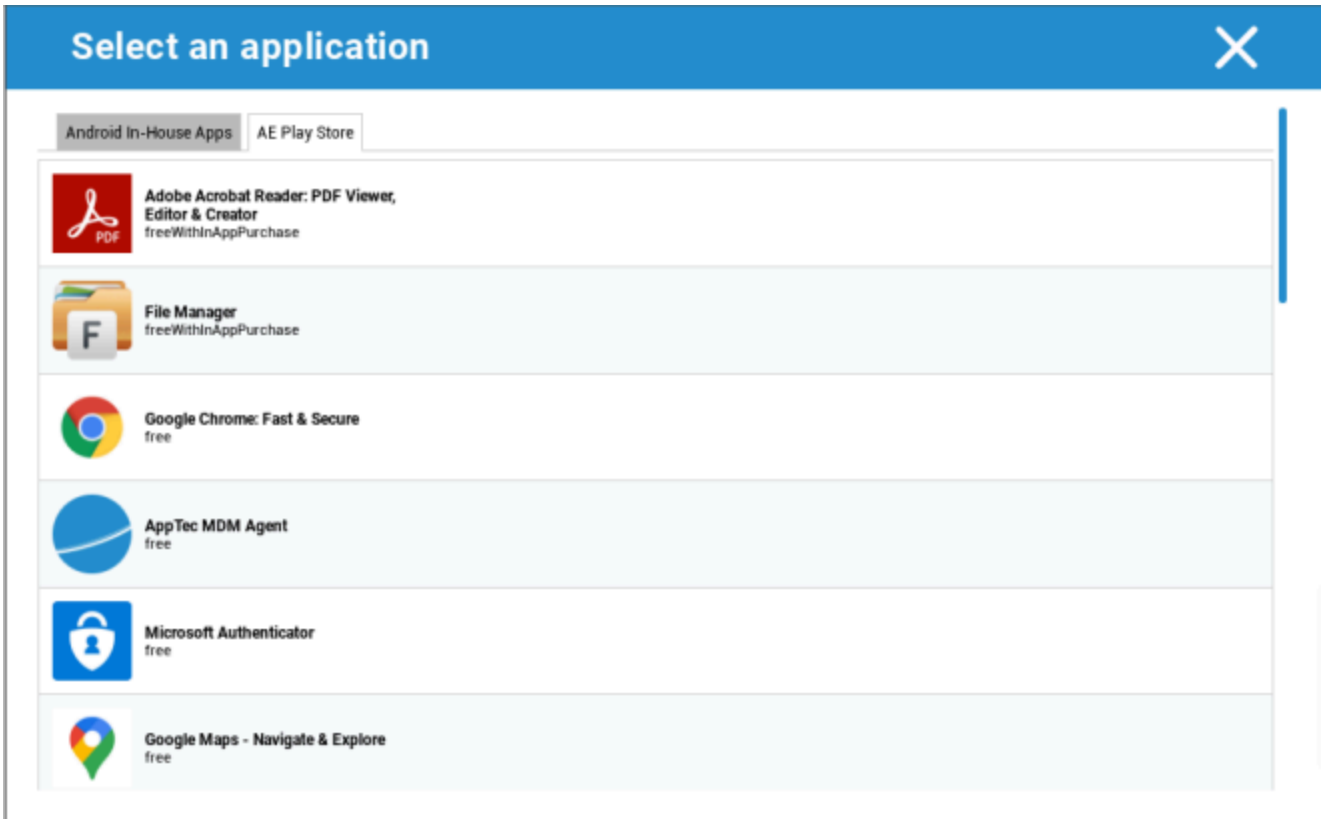


您也可以使用 "上传内部应用程序 "直接选择并上传 apk 文件。



如果安装的是内部应用程序，则可以激活 "保持更新"。如果激活了这一功能，并且在内部应用程序数据库中定义了更新的版本，则会在设备上更新应用程序。

也可以是 Google Work Play Store 中的 "AE Play Store "应用程序。



只有经过批准的 "AE Play Store 应用程序 "才会显示在此选项卡中。

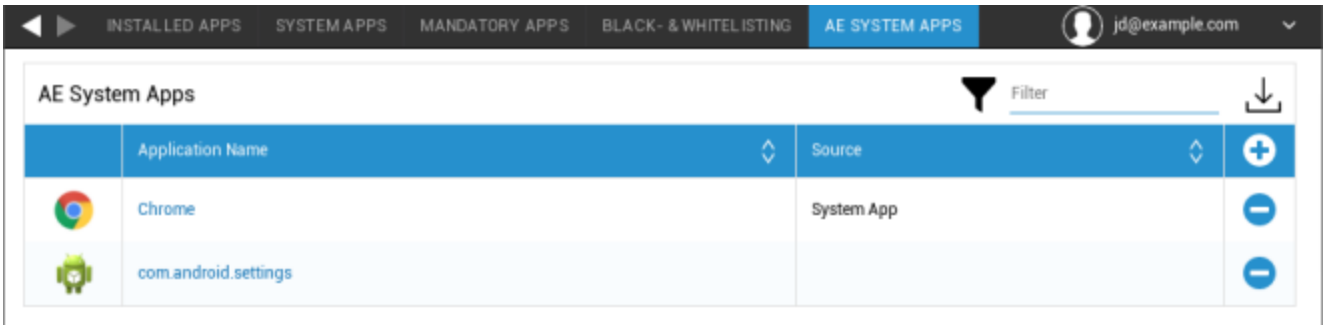
要批准 "AE Play Store 应用程序"，请进入 "常规设置">"应用程序管理">"AE Play"。

商店"，然后通过按钮添加应用程序，该按钮会将你重定向到 "Play Store 应用程序 "选项卡（也可以直接进入 "Play Store 应用程序 "选项卡）。

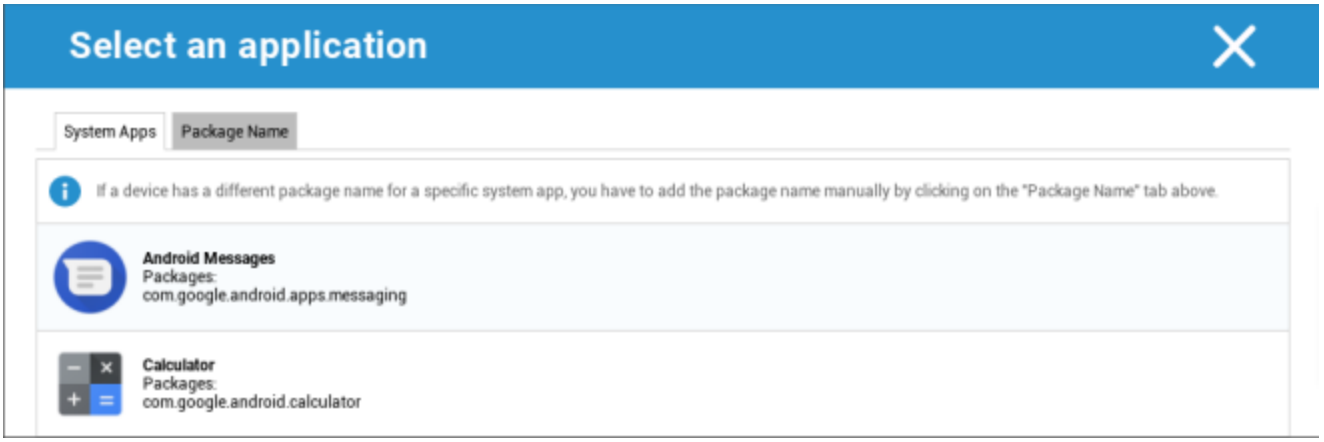
在 "Play Store 应用程序 "选项卡中，您可以搜索应用程序。点击一个应用程序后，应用程序页面就会打开，在此您可以点击 "批准 "来批准该应用程序。

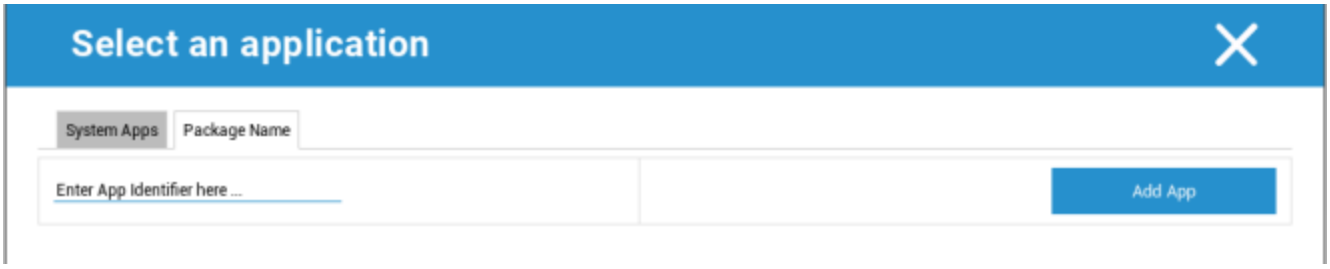
AE 系统应用程序

您可以在此定义一个列表，其中包含应在设备上激活的特定系统应用程序。



点击该按钮后，您可以从 Google 提供的可能的系统应用程序列表中进行选择，也可以直接输入应激活的系统应用程序的软件包名称。





请记住，Google 提供的列表中的系统应用程序只是可以成为系统应用程序的应用程序，并不一定是您设备上的系统应用程序。

不过，该列表只影响已预装的应用程序。

添加未预装在设备上的应用程序不会影响设备，无论该应用程序是来自 Google 提供的列表，还是直接输入应用程序的软件包名称。

限制和设置

应用程序管理设置

您可以在此配置设备有关应用程序更新的行为。

更新检查频率	指定 AppTec 客户端搜索应用程序更新的时间间隔。默认值为 24 小时。
Wi-Fi 门限	大于指定大小的应用程序将通过 Wi-Fi 下载。如果选择 "仅限 WLAN"，则所有应用程序都将通过 WLAN 下载。

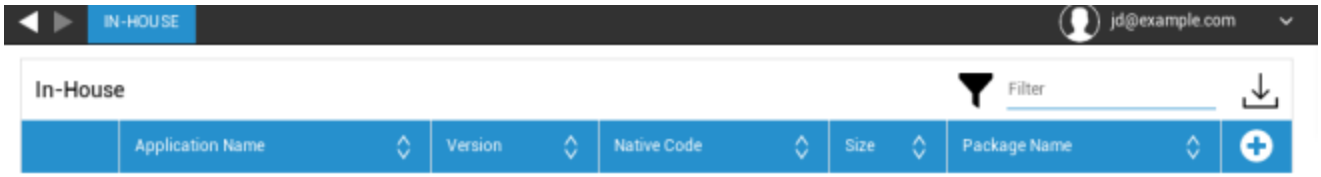
企业应用商店

内部

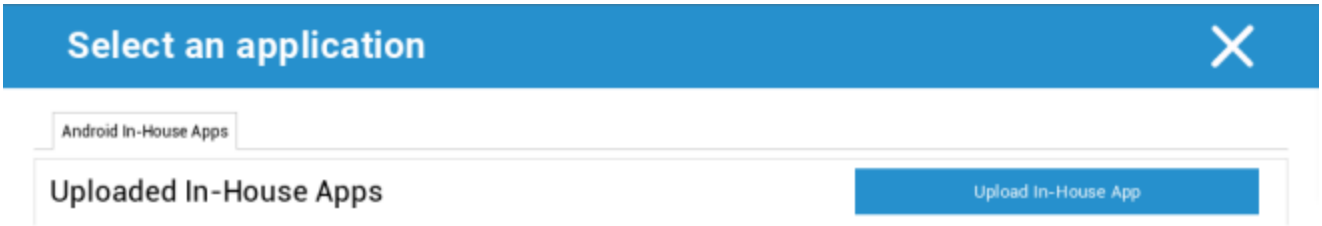
在 "内部 "点下，您可以上传和分发内部开发的应用程序。

有了这个符号，您就可以分发更多的内部应用程序。

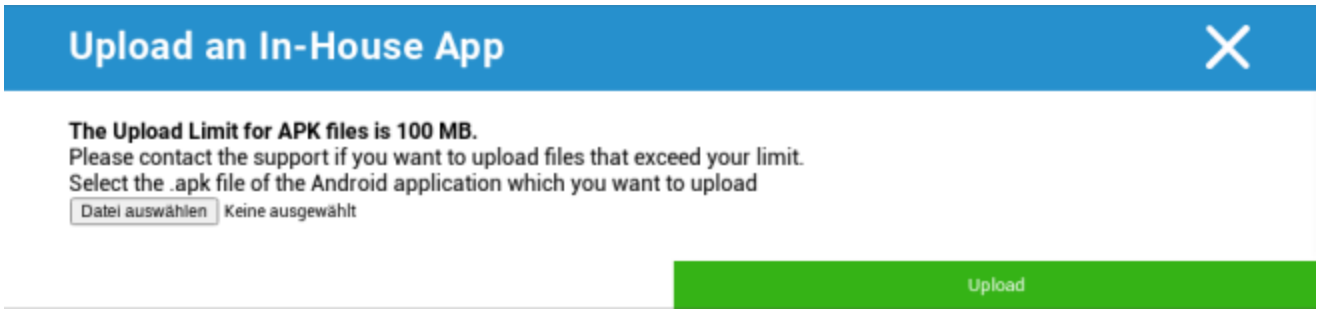
如果安装的是内部应用程序，则可以激活 "保持更新"。如果激活了这一功能，并且在内部应用程序数据库中定义了更新的版本，则会在设备上更新应用程序。



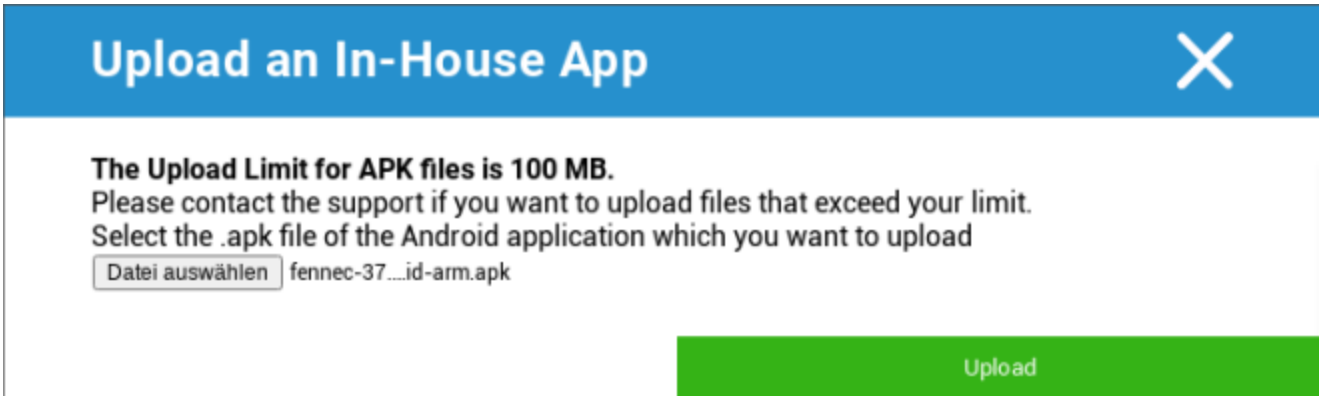
如果您没有分发内部应用程序，您将收到以下概述：



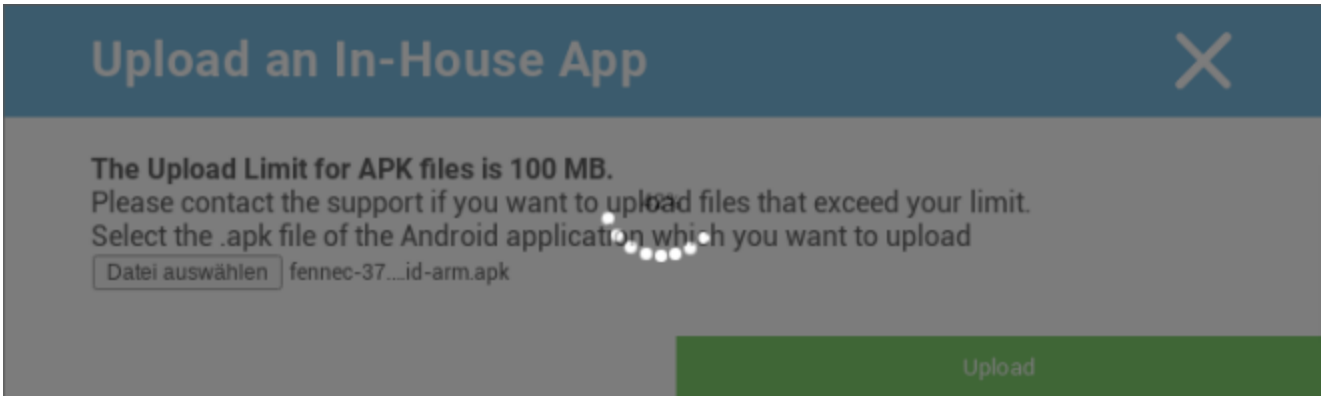
为此，请单击 "上传内部应用程序"，然后您将收到以下概览：



现在，用 "搜索... "选择一个 .apk 文件，然后点击 "上传"。



现在，您的应用程序将被上传，在圆圈中间，您将看到一个百分比指示器，显示您的应用程序已经上传了多少内容。



如果您的内部应用程序上传成功，您就可以在应用程序目录中找到上传的应用程序。

现在，用户可以选择在最终用户设备上的 AppTec 商店 "内部 "类别下查看并安装该应用程序。

由于不涉及 Google PlayStore 应用程序，用户无需在各自的终端设备上存储 Google ID。

企业 Play 商店

AE Play 商店

您可以在此向 Android 企业 Playstore 添加应用程序。请注意，在添加应用程序之前，您必须使用 AE 管理员账户批准应用程序。

如需批准应用程序，请参阅 "强制性应用程序 "中的说明。

内容管理

内容框

在这里您可以激活内容框。

只要将 "启用 ContentBox "切换为 "开"，就会在终端用户设备上自动安装一个单独的 ContentBox 应用程序。

安全浏览器

您可以在此配置 AppTec 安全浏览器的设置。

只要将 "安全浏览器 "部分切换为 "打开"，就会在最终用户设备上自动安装一个单独的浏览器应用程序。

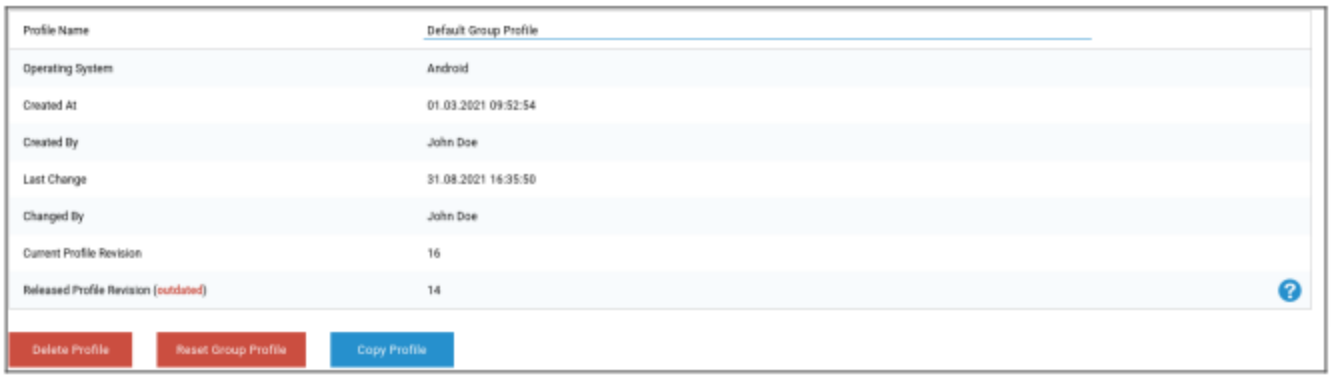
要求密码	要求用户设置并使用密码访问浏览器。
最低要求密码长度	设置密码所需的字符数
密码质量要求	设置所需的密码质量
限制下载/打开	
限制上传	
上传白名单	始终允许上传的 URL 列表。
允许复制	允许复制、剪切或共享网页内的文本。
允许屏幕捕捉	允许截图
数据清理频率	选择自动删除所有用户数据（历史记录、缓存等）的频率。
公司书签	书签将显示在浏览器书签中的 "公司书签 "文件夹中。 用户无法对其进行编辑。
隐藏地址栏	
浏览器内白名单（无通用网关）	启用客户端 URL 白名单。 • 公司书签始终列入白名单 • 仅支持 100 个 URL • 请使用通用网关进行无限制的黑名单和白名单设置
白名单 URL	允许使用的 URL 列表。
基于网关的黑白名单设置	黑名单有以下要求 • 一个正常工作的 AppTec 通用网关（"常规设置"→"通用网关） • 带有指定 DNS 服务器的有效 VPN 配置（"常规设置"→"通用网关"→"VPN 设置） • 黑名单配置（"常规设置"→"通用网关"→"网域黑名单） • 配置文件中的有效 VPN 连接（"连接管理"→"VPN）

安卓配置

一般情况

组概况概览（仅适用于组级）

打开群组资料时，您将快速浏览该资料。



简介名称	个人资料名称（可在此处更改）
操作系统	配置文件适用的操作系统
创建于	创建时间
创建者	个人资料创建者
最后的变化	最后一次更改配置文件的时间
已更改	最后更改的账户
当前的简介修订	修订已保存的配置文件状态
已发布的简介修订版	已分配的配置文件修订版（"立即分配"）。如果标签文字后面显示"（已过期）"，则表示您已经保存了配置文件，但尚未分配，因此设备仍将获得旧版本。

设备概述（仅限设备级别）

如果您正在使用一个设备，您将收到所选设备的概述，其中包含以下内容：

设备名称	设备名称
最后知道的地点	最后已知的 GPS 坐标
电话号码	电话号码
指定的强制性应用程序	分配的强制性应用程序数量
操作系统版本	设备的操作系统版本
操作系统	操作系统（安卓/iOS/Windows Phone）
序列号	设备序列号
设备所有权	公司或私人设备
设备类型	电话或平板电脑
扎根	状态，显示设备是否已被 root
符合要求	符合准则要求
IP 地址	IP 地址
最后查看	设备最后一次连接 AppTec 的时间点
最后一搏	服务器向设备发送推送的时间点
用户分配	将设备分配给其他用户的下拉菜单

配置修订（仅限设备级）

在这里，您将看到为设备分配的组配置文件的概览。

如果点击群组配置文件，就可以直接进入配置文件并进行设置。

使用该符号，可以将已分配的应用程序还原为群组配置文件的设置。

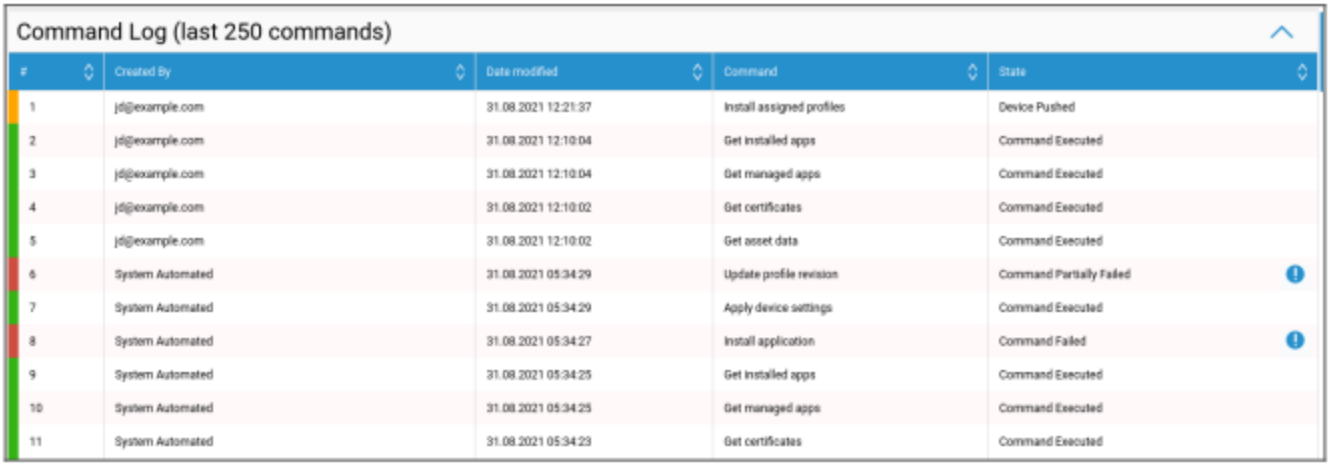
通过该符号，您可以重置设备配置文件，使其没有任何设置。

"最新版本可用 "表示组配置文件已更改并保存，但尚未分配。必须在组级别上使用 "立即分配 "来分配组配置文件，才能将更改应用到设备上。

设备日志（仅限设备级）

命令日志

在这里，您可以查看为设备发出的命令及其状态。



系统自动 "创建的命令由系统自动创建。

可能的命令状态

设备已推送	推送请求已发送至推送服务（如 APNS），以通知设备连接回 EMM 服务器。
创建命令	该命令已在系统中创建。
发送命令	设备与服务器连接后，命令被发送到设备。
命令已执行	命令已成功执行。
命令失败	命令失败。*
命令部分失败	根据设备操作系统的不同，有些命令可能会被组合在一起。 其中，该命令组的某些部分出现故障。*
命令已执行，但最终失败	命令已执行，但也可能没有执行。
命令重发	命令被用户重新推送。
弃用	命令被丢弃。例如，该命令被其他命令取代，或设备重新注册，旧命令被删除。

*如果信息后面有感叹号，您可以用光标悬停在图标上，获取更多信息。

设备设置

客户端配置

在这里，您可以对安卓设备进行以下配置：

禁用设备管理后的警告信息	禁用 "设备管理 "后的既定警告信息
违规时间	如果设备不符合要求，将执行 "符合要求后的执行行动 "的时限。 分钟1 分钟 最长24 小时
合规超时后的执法行动	一旦设备不符合要求，应立即采取的行动。 • 无所作为 = 不采取行动 • 锁定设备 = 锁定设备 • 擦除设备 = 设备将恢复出厂设置
数据收集频率	收集设备/GPS 信息的频率
设备心跳频率	设备联系 AppTec360 服务器的时间间隔 分钟1 分钟 最长24 小时
启用位置更新	如果激活，设备会向 AppTec360 服务器发送位置更新
地点更新时间	确定设备向 AppTec 发送位置更新的时间间隔
使用 Google 定位精度进行位置更新	如果激活，Google 定位精度（以前称为网络定位）将用于位置更新（如果在 "限制 "下停用，则此设置不会有任何影响）
使用 GPS 定位进行位置更新	如果激活，将使用 GPS 进行位置更新
允许模拟（伪造）位置	允许通过第三方应用程序伪造位置信息
失去连接行动	您可以设置在一定量的心跳失败后执行的特定操作
政策执行模式	定义 AppTec360 客户端要求用户执行某些需要用户输入的操作的积极程度。 间隔（默认）= 以间隔方式询问，这样用户就可以将其放在后台一段时间。 无警报 = 无弹出要求交互的窗口。您必须手动打开 AppTec360 客户端，检查是否有必要的操作 恒定警报 = 用户只能执行所需的操作。如果用户试图回避，AppTec360 客户端会强制将自己置于前台

AppTec360 版本锁定	让您定义 AppTec360 客户端的版本，这是客户端自我更新的最大版本。

壁纸

您可以在此定义自定义壁纸。

"指定颜色 "可让您定义十六进制格式的颜色（如 #000000）。只允许使用十六进制值。

"将图片设为壁纸 "可让您上传图片。请注意，不同的设备使用不同的启动器和操作系统版本，工作方式也不尽相同。由于尺寸和比例取决于设备，因此没有通用的指导线。

文件格式使用 JPG（或 JPEG）或 PNG。

资产管理（仅限设备级）

资产管理

设备信息

模型	**设备型号**
操作系统	操作系统
操作系统版本	操作系统版本
AE 支持	支持安卓企业（容器和完全托管）
序列号	序列号
设备名称	设备名称
电池状态	电池状态
可用/总内存	可用/总内存
三星 KNOX	三星 KNOX 应用程序接口级别
可用 SD 卡	可使用 SD 卡
模拟 SD 卡	模拟 SD 卡
可移动 SD 卡	可移动 SD 卡
SD 可用/总内存	SD 可用/SD 卡总内存

无线网络

IP 地址	设备 IP 地址
WiFi MAC	WiFi MAC 地址

细胞

现状	状态（已安装 SIM 卡）
电话号码	电话号码
漫游（语音/数据）	语音/数据漫游
漫游状态	当前漫游状态
IP 地址	IP 地址
运营商/承运商	运营商/承运商
蜂窝技术	蜂窝技术
IMEI	IMEI 号码
ICCID	这是 SIM 卡的 ID，通常也是智能卡或集成电路卡 (ICC)
IMSI	在 GSM 和 UMTS 移动网络中，国际移动用户标识（IMSI）提供了网络用户的明确标识 IMSI 最多由 15 位数字组成，配置方式如下： • 移动国家代码(MCC)，3 位数 • 移动网络代码(MNC)，2 或 3 位数 • 移动用户识别码 (MSIN)，1-10 位数
目前的 MCC/MNC	参见 "SIM MCC/MNC
SIM MCC/MNC	移动国家代码是国际电联根据 E.212 标准制定的国家标识符。它与移动网络代码（MNC）一起用于识别移动网络。 指 SIM 卡的国家/移动网络代码。 如果您漫游到另一个移动网络，那么从逻辑上讲，"当前 MCC/MNC "和 "SIM MCC/MNC "将是不同的。

蓝牙

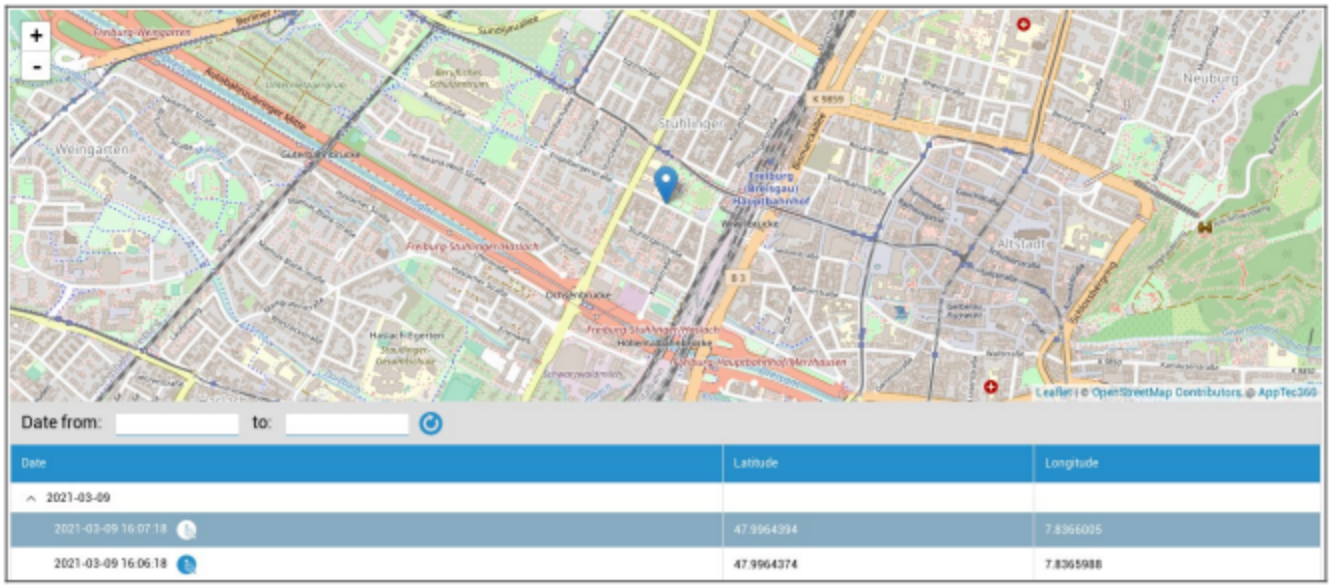
蓝牙 MAC	蓝牙 MAC 地址

安全管理

防盗（仅限设备级）

GPS 信息（仅限设备级别）

您可以在此确定当前/最后的设备位置。可以使用一个甚至两个密码来保护定位功能 - 请参阅 "常规设置"-"隐私"-"GPS 访问"：常规设置 - 隐私 - GPS 访问



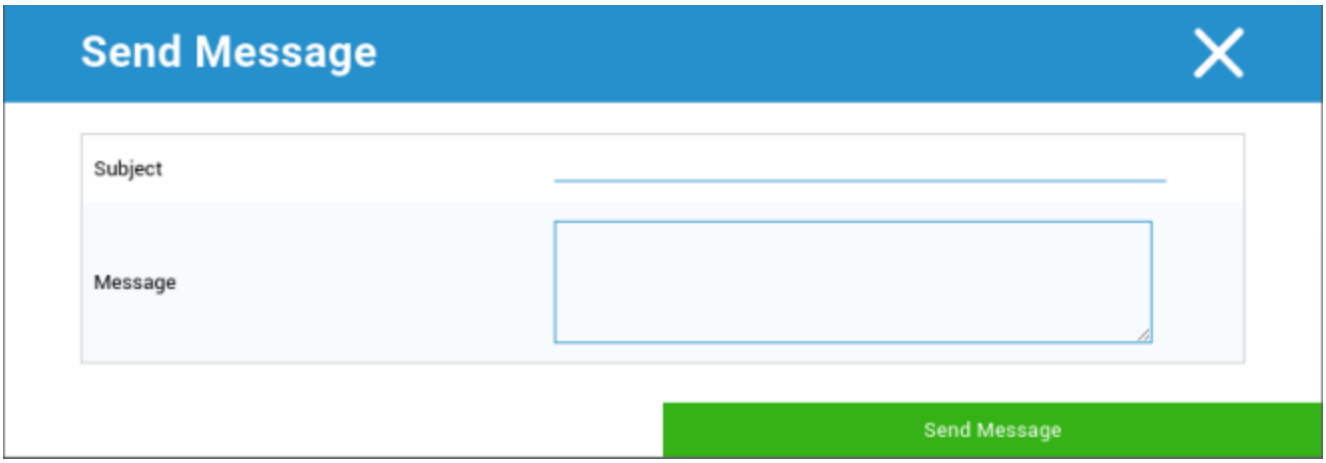
擦除和锁定（仅限设备级别）

在 "擦除和锁定 "下，您可以执行以下三项操作：

全面擦拭	设备恢复出厂设置（删除公司和个人数据）
企业擦拭	只从最终用户设备中删除企业数据（由 AppTec360 提供的所有应用程序、数据等）
锁定屏幕	屏幕锁已激活，只需使用设备密码/PIN 解锁设备即可

信息（仅限设备级别）

您可以填写主题和信息，然后将其发送到最终用户设备。该信息将显示在 AppTec360 客户端中。



安全配置

密码

在 "密码 "下，您可以设置设备密码，有以下设置选项供您选择

最小密码长度	规定密码必须包含的最少符号数
密码质量	密码强度 未指定 = 未指定 每个密码都可以 = 每个密码都可以接受 至少包含数字字符 = 必须至少包含数字字符 至少包含复杂字符 = 必须至少包含特殊字符 至少包含字母数字字符 = 必须至少包含字母数字字符 至少包含字母字符 = 必须至少包含字母字符
最长闲置时间锁定	最大屏幕超时。这只能配置用户可选择的最大值
密码中至少需要小写字母	密码中至少需要小写字母
密码中至少需要大写字母	密码中至少需要大写字母
密码中需要的最少非字母字符	密码中需要的最少非字母字符
密码所需的最小数字位数	密码所需的最小数字位数
密码所需的最少符号	密码所需的最少符号
密码过期超时	建立，在此时间间隔后密码失效，必须发布新密码
密码历史限制	不允许使用的密码数量
密码尝试失败次数上限	规定在执行完全设备擦除之前，错误输入密码的频率

加密

在这一点上，您可以加密内部设备内存和 SD 卡内存。

要求存储加密	如果激活此设置，只要设备支持此功能，就会对设备内存进行加密。 设备内存首次加密后，就无法再解除加密。 同样，密码策略也会自动切换为 6 个字母数字符号
要求 SD 卡加密	此设置仅适用于三星设备！ 如果激活此设置，外置 SD 卡将被加密，并且只能在最终用户设备上手动解除加密。 同样，密码策略也会自动切换为 6 个字母数字符号

防病毒

启用防病毒功能将在设备上安装 Ikarus。请注意，这需要单独的许可证，许可证可在常规设置 → 应用程序管理 → 第三方应用程序中输入。

自动扫描	定义 Ikarus 是否自动扫描以及执行扫描的频率 启用 "全自动扫描 "将执行全面扫描。否则将执行快速扫描
自动更新	启用病毒库自动更新并设置更新频率
应用程序保护	除了只扫描文件的常规扫描外，还可扫描应用程序
SD 卡保护	启用 SD 卡保护。否则，扫描仅限于本地存储空间
仅 Wi-Fi 更新	限制更新至 Wi-Fi

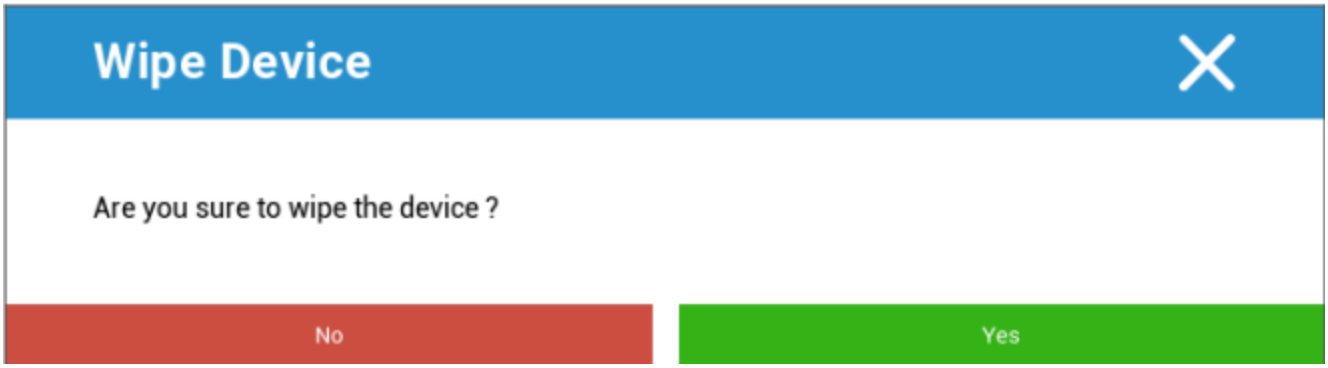
报废（仅限设备级）

擦除（仅限设备级）

在 "擦除 "下，可以将设备恢复出厂设置。在这里，最终用户设备上的公司和私人数据都将被删除。

点击 "减号 "后，您将收到以下信息

也要擦除 SD 卡吗?	SD 卡内存也将被清除



如果选择 "是"，则可以执行擦除操作。

在 "擦除报告 "下可显示以下项目

擦拭	进行擦拭的历史
日期	日期
现状	状态（例如擦除是否成功执行）

限制设置

限制条件

在这里，可以限制和阻止各种事物。

启用摄像头	允许使用照相机
强制自动同步	与 "同步 "界面有关 开 = 永久激活同步 关 = 同步永久停用 用户选择 = 由用户选择
强制蓝牙	开 = 蓝牙永久激活 关 = 蓝牙永久停用 用户选择 = 由用户选择
Force GPS	开 = GPS 永久激活 关闭 = GPS 永久停用 用户选择 = 由用户选择
强制提高谷歌定位精度	开启 = 永久互联网定位 关闭 = 永久停用互联网定位功能 用户选择 = 由用户选择

对于带有 KNOX 1.0 或更高版本界面的三星设备，可使用以下设置选项。

允许使用 SD 卡	允许使用 SD 卡
允许写入 SD 卡	允许 "写入 "SD 卡
允许屏幕捕捉	允许屏幕截图
允许使用剪贴板	允许使用剪贴板
在 Google 云中备份设置和应用程序数据	关闭 = 禁用 Google 备份 打开 = 激活 Google 备份 用户选择 = 由用户选择
允许 USB 调试	允许 USB 调试（例如用于创建设备日志 (ADB)
允许谷歌崩溃报告	允许从应用程序发送 Google 崩溃报告
允许出厂重置	允许用户将设备恢复出厂设置
允许 OTA 升级	允许 "空中 "更新
允许 USB 主机存储	如果激活，可连接 HD 或 SD 读卡器形式的 USB 存储器
允许 USB 媒体播放器（MTP、PTP）	允许 USB 媒体播放器（MTP、PTP）
允许麦克风	打开 = 允许第三方应用程序使用麦克风 关闭 = 禁用第三方应用程序的麦克风 用户选择 = 如果第三方应用程序可以访问麦克风，用户可以选择
允许 NFC（近距离无线通信）	允许 NFC
允许未知来源（APK Sideloading）	如果启用，则允许侧载应用程序（APK 文件）。 一旦禁用此设置，用户就必须在重新允许安装未知来源的 APK 时手动启用它。
允许创建用户	允许创建多个用户

AE 设备所有者

(设备必须处于 "安卓企业设备所有者模式"）建议将设备创建为 "安卓企业 "设备，而不是 "安卓 "设备。

安全	
禁止共享位置	指定是否禁止用户开启位置共享。
禁止安全启动	指定是否不允许用户将设备重新启动到安全启动模式。
禁止网络重置	指定是否禁止用户从 "设置 "中重置网络设置。
禁止出厂重置	指定是否禁止用户重置设备。

启用 ADB	允许通过 ADB 与电脑连接
禁用键盘防护	禁用键盘防护
设备所有者锁屏信息	设置要在锁屏上显示的设备所有者信息。
合规执行	提示用户模式 - 提示用户执行必要的操作。 模式锁定容器 - 隐藏所有应用程序，直至满足所有要求

应用程序管理	
允许跨配置文件应用程序链接	允许父配置文件中的应用程序处理来自受管配置文件的网络链接。
禁止应用程序控制	指定是否禁止用户修改设置或启动器中的应用程序。
禁止安装应用程序	指定是否禁止用户安装应用程序。
禁止卸载应用程序	指定是否禁止用户卸载应用程序。
运行时权限政策	指定如何处理来自应用程序的新权限请求。
允许未知来源	如果启用，用户可以通过安装 .apk 文件来侧载应用程序。

连接性	
禁止移动网络配置	指定是否禁止用户配置移动网络。
禁止 Tethering 配置	指定是否禁止用户配置 Tethering 和便携式热点。
禁止 VPN 配置	指定是否禁止用户配置 VPN。
禁止 Wifi 配置	指定是否禁止用户更改 WiFi 接入点。
禁止发出 NFC 光束	指定是否不允许用户使用 NFC 从应用程序传送数据。
锁定 WiFi 配置	此设置可控制由设备所有者应用程序创建的 WiFi 配置是否应被锁定（即只能由设备所有者应用程序编辑或删除，甚至不能由设置应用程序编辑或删除）。
启用数据漫游	激活数据漫游

蓝牙	
禁止蓝牙	指定设备是否禁止蓝牙。要求安卓 8.0
禁止蓝牙共享	指定设备是否禁止外发蓝牙共享。需要安卓 8.0
禁止蓝牙配置	指定是否禁止用户配置蓝牙。

账户管理	
禁止添加受管配置文件	指定是否禁止用户添加受管配置文件。需要安卓 8.0
禁止添加用户	指定是否禁止用户添加新用户。
禁止移除受管配置文件	指定除用户配置文件所有者外，是否可以删除该用户的受管配置文件。需要安卓 8.0
禁止修改账户	指定是否禁止用户添加和删除账户，除非 Authenticator 以编程方式添加了账户。

电话	
禁止拨出电话	指定不允许用户拨打外线电话。
禁止短信	指定不允许用户收发短信。

系统	
禁止创建窗口	指定不创建应用程序窗口以外的窗口。
禁止设置用户图标	指定是否不允许用户更改自己的图标。
禁止设置壁纸	禁止设置壁纸的用户限制。
禁用状态栏	禁用状态栏会阻止通知、快速设置和其他屏幕叠加功能，使用户无法从单一使用设备中逃脱。
启用自动计时	自动设置时间。
启用自动时区	自动设置时区。
插电时保持开机状态	当连接到电源时，设备将保持激活状态。

存储	
禁止禁用应用程序验证	指定是否禁止用户禁用应用程序验证。
禁止安装物理介质	指定是否禁止用户挂载物理外部介质。
启用备份服务	备份服务管理设备上的所有备份和还原机制。将此设置为假将阻止数据备份或还原。备份服务默认为关闭。需要安卓 8.0
启用 USB 大容量存储器	启用 USB 大容量存储器。

键盘	
禁止自动填写	指定是否不允许用户使用自动填充服务。要求安卓 8.0
禁止在预案之间复制和粘贴	指定复制到该预案剪贴板中的内容是否可以粘贴到相关预案中。

声音	
不允许音量调整	指定是否禁止用户调整主音量。
禁止麦克风静音	指定是否禁止用户调节麦克风音量。
静音装置	静音装置。

系统更新政策	
控制操作系统更新	启用此项可将更新行为设置为自动、窗口或延迟。

BYOD 容器

安卓企业

安卓企业

启用安卓企业版	启用 Android Enterprise (AE)。安卓 5.1 及以上版本支持 AE。
合规执行	提示用户模式 - 提示用户执行必要的操作。 模式锁定容器 - 隐藏所有应用程序，直至满足所有要求
运行时权限政策	提示用户新的权限请求 始终批准新的权限请求 始终拒绝新的权限请求 警告：如果权限是自动设置的，有些应用程序在识别权限时会出现问题。如果您总是授予权限，但遇到应用程序提示权限缺失的问题，请将其设置为 "提示用户 "并重新安装应用程序
允许外发剪贴板	允许从容器内部复制和粘贴到外部
允许来电显示解析	根据容器中的联系人显示来电名称
允许联系人搜索解析	拨打电话时，允许在容器联系人中搜索姓名
允许蓝牙联系人共享	允许在车内接触容器
禁止发出 NFC 光束	禁用容器的 NFC
允许未知来源	如果启用，用户可以通过安装 .apk 文件来侧载应用程序。
允许 USB 调试	如果启用，用户可以启用 USB 调试。
禁止修改账户	禁止创建、删除和修改容器中的账户 请注意，某些应用程序需要创建或修改账户才能正常运行

Gmail Exchange

允许您在容器中配置 Gmail。请注意，启用此配置并不会自动安装应用程序。您仍需将此应用程序添加为必选应用程序。

电子邮件地址	电子邮件地址
服务器主机名	服务器主机名
登录名	登录名
签名	签名
同步的天数	要同步的天数。
设备标识符	EAS 标识符。如果您的环境不需要此项，请将其留空。
使用安全套接字层（SSL）	启用 SSL 的使用。禁用此功能可能会降低安全性
接受所有证书	接受所有证书。启用此功能可能会降低安全性
允许非托管账户	允许用户添加其他账户
客户证书	如果 Exchange 服务器要求上传客户端证书，请上传客户端证书

AE 系统应用程序

在这里，你可以为安卓企业容器启用系统应用程序。请注意，指定的应用程序必须在系统存储中，否则不会发生任何情况。

集装箱密码

仅适用于 Android 7.0 或更高版本

允许您为容器设置特定的密码要求。

最小密码长度	规定密码必须包含的最少符号数
密码质量	密码强度 未指定 = 未指定 每个密码都可以 = 每个密码都可以接受 至少包含数字字符 = 必须至少包含数字字符 至少包含复杂字符 = 必须至少包含特殊字符 至少包含字母数字字符 = 必须至少包含字母数字字符 至少包含字母字符 = 必须至少包含字母字符
最长闲置时间锁定	容器锁定前的最长时间。这只能配置用户可以选择的最大值
密码中至少需要小写字母	密码中至少需要小写字母
密码中至少需要大写字母	密码中至少需要大写字母
密码中需要的最少非字母字符	密码中需要的最少非字母字符
密码所需的最小数字位数	密码所需的最小数字位数
密码所需的最少符号	密码所需的最少符号
密码过期超时	建立，在此时间间隔后密码失效，必须发布新密码
密码历史限制	不允许使用的密码数量
密码尝试失败次数上限	规定在删除容器之前，密码输入错误的频率

三星 KNOX

激活

在此，您可以启用三星 KNOX 容器。请注意，在 Android 10 或更高版本中，三星不再支持此功能。在安卓 10 或更高版本上使用安卓企业容器

诺克斯密码

制定与设备密码设置相关的准则

最小密码长度	规定密码必须包含多少个符号
密码质量	密码强度 每个密码都可以 = 每个密码都可以 至少有数字字符 = 必须至少有数字字符 至少包含复杂字符 = 至少包含特殊字符 至少包含字母数字字符 = 至少包含字母数字字符 至少包含字母字符 = 必须至少包含字母字符

所需的最小复杂字符数	必须有最少的复杂字符
最长闲置超时	键盘锁定前用户不活动的最长超时时间
允许指纹验证	允许指纹验证
允许虹膜身份验证	允许虹膜识别身份验证
最大密码年龄	规定密码过期后必须重新设置密码的时间
存储密码历史	不允许使用的前密码数量
密码尝试失败次数上限	规定在完全擦除设备之前，密码提交错误的频率

诺克斯安全系统

限制特定设备功能

启用摄像头	允许使用摄像机
允许三星 KNOX 应用程序商店	允许使用三星 KNOX 应用程序商店
允许 Google Play 服务	允许 Google Play 服务
允许浏览器	允许使用本地浏览器
允许截图	允许创建屏幕截图
允许导入联系人	如果激活，则允许从 KNOX 容器访问设备触点
允许导出联系人	如果激活，则允许从设备访问 KNOX 联系人
允许日历导入	如果激活，则允许从 KNOX 容器访问设备日历
允许导出日历	如果激活，则允许从设备访问 KNOX 日历
允许非安全键盘	允许使用非安全键盘
启用文件导入	将文件导入 KNOX 容器
启用文件导出	启用 KNOX 容器的文件导出功能

诺克斯交流中心

您可以在此配置 KNOX 容器的 Exchange 配置文件

电子邮件地址	提供的用户电子邮件地址 请注意 "占位符"，您可以使用这些占位符来处理凭据，而无需在每台设备上手动执行更改。 点击 "**显示占位符**"，您就可以自己显示它们了
服务器主机名	Exchange 服务器的服务器地址
登录名	终端用户设备的登录名，请注意此处的 "占位符"。
域名	域名地址
密码（仅限设备级）	可选择为单个设备提供密码，如果密码为空，系统将提示用户输入 Exchange 密码
同步的天数	天数，决定电子邮件何时同步返回
签名	可附上签名
默认账户	确定该电子邮件账户是标准账户
使用安全套接字层（SSL）	使用 SSL 连接
使用传输层安全（TLS）	使用 TLS 连接
接受所有证书	接受所有证书。如果您的 Exchange 服务器使用自签名证书，请选择此选项

诺克斯电子邮件

电子邮件地址	提供的用户电子邮件地址 请注意 "占位符"，您可以使用这些占位符来处理凭据，而无需在每台设备上手动执行更改。 点击 "**显示占位符**"，您就可以自己显示它们了
传入服务器协议	传入服务器协议 IMAP 或 POP
传入服务器地址	传入服务器地址
传入服务器端口	传入服务器端口
传入服务器登录名/用户名	传入服务器登录名/用户名
传入服务器密码	传入服务器密码
传入服务器使用 SSL	传入服务器使用 SSL
传入服务器使用 TLS	传入服务器使用 TLS
传入服务器接受所有证书	接收服务器接受所有类型的证书
发送服务器协议	发送服务器协议 SMTP
外发服务器端口	外发服务器端口
发件服务器使用额外的证书	传出服务器的附加凭证。如果设置为 "关闭"，则将使用传入服务器设置
发件服务器登录名/用户名	发件服务器登录名/用户名
发件服务器密码	发件服务器密码
传出服务器使用 SSL	传出服务器使用 SSL
发件服务器使用 TLS	发件服务器使用 TLS
发件服务器接受所有证书	传出服务器接受所有类型的证书
签名	此处可附上签名
收到新电子邮件时通知用户	收到新电子邮件时通知用户

诺克斯应用程序

在此建立您想要分发到终端用户设备的应用程序。这些应用程序将在 KNOX 容器中可用。要添加应用程序，请按照菜单 "必选应用程序 "中的步骤操作

应用名称	应用名称
强制执行	添加应用程序的时间点
资料来源	应用程序的来源（Play Store | 公司内部）

点击该符号，可再次删除相应的应用程序

连接管理

无线网络

为此，请对终端用户设备进行预配置，以便访问内部接入点

服务集标识符（SSID）	要连接的网络的 SSID
隐藏的网络	激活，以防接入点不广播 SSID
安全类型	建立 AP 的安全类型

安全类型

WEP

密码	AP 密码

WPA/WPA2

密码	AP 密码

802.1x EAP

EAP 方法	

工务司	身份	身份
	密码	密码

PEAP	第 2 阶段身份验证协议	无	无附加协议
		MSCHAPV2	MSCHAPV2 协议

		通用技术委员会	全球技术合作协议
	CA 证书	CA 证书	
	身份	身份	
	匿名身份	匿名身份	
	密码	密码	

EAP 方法	

TTLS	第 2 阶段身份验证协议	无	无附加协议
		PAP	PAP 协议
		MSCHAP	MSCHAP 协议
		MSCHAPV2	MSCHAPV2 协议
		通用技术委员会	全球技术合作协议
	CA 证书	CA 证书	
	身份	身份	
	匿名身份	匿名身份	
	密码	密码	

TLS	CA 证书	CA 证书
	身份	身份
	密码	密码

虚拟专用网

连接类型	**建立 VPN 连接类型**

如果选择 "Per-App VPN "作为 VPN 类型，可用的 VPN 客户端将发生变化。Per-App VPN 将 VPN 限制在某些应用程序中，并在启动特定应用程序时自动启动 VPN 连接。

AppTec360 VPN 客户端	将 AppTec360 VPN 客户端与通用网关结合使用
连接名称	VPN 连接名称
网关配置	选择通用网关的 VPN 配置

始终连接 VPN	强制 VPN 始终处于活动状态，因此所有流量都通过 VPN 传输。
启用本地锁定	当设备未连接到 VPN 时，阻止所有联网。请谨慎使用，因为如果配置不当，可能会导致完全失去连接。仅适用于安卓 7 或更高版本的安卓企业
启用 AppTec360 锁定	在 VPN 连接启动之前，禁止使用所有应用程序

思科 AnyConnect	
连接名称	VPN 连接名称
服务器	服务器地址
证书模式	禁用 = 已停用 自动 = 自动

L2TP（仅限 KNOX）	仅适用于三星设备
连接名称	连接名称
服务器	服务器地址
启用 L2TP 秘密	
DNS 搜索域	DNS 搜索域

连接类型	**建立 VPN 连接类型**

PPTP （仅限 KNOX）	仅适用于三星设备
连接名称	VPN 连接名称
服务器	服务器地址
启用加密	启用加密
DNS 搜索域	DNS 搜索域

L2TP / IPSec PSK（仅限 KNOX）	仅适用于三星设备
连接名称	VPN 连接名称
服务器	服务器地址
IPSec 预共享密钥	用于验证的预共享密钥
启用 L2TP 秘密	
L2TP 秘密	
DNS 搜索域	DNS 搜索域

IPSec XAuth PSK（仅限 KNOX）	仅适用于三星设备
连接名称	VPN 连接名称
服务器	服务器地址
IPSec 识别码	连接的用户名
IPSec 预共享密钥	连接密码
DNS 搜索域	DNS 搜索域

OpenVPN	
连接名称	连接名称

OpenVPN 简介	.ovpn 文件的内容将被复制到此处
OpenVPN 应用程序	使用 OpenVPN 有两种不同的应用程序 我们推荐使用 "OpenVPN for Android "应用程序。但也可以使用 "OpenVPN Connect "应用程序

限制条件

您可以在此设置与连接管理相关的限制。

允许数据漫游	允许漫游时使用移动数据
强制数据漫游	如果激活，移动数据漫游将永久激活（不建议使用！）。 该设置会覆盖 "允许数据漫游 "设置！
以下设置仅适用于三星 KNOX 2.0 或更高版本	
只允许拨打紧急电话	只允许拨打紧急电话
允许 WiFi	允许 WiFi
WiFi 网络最低安全级别	WiFi 网络最低安全级别 开放 = 允许使用所有类型的 WiFi
禁止用户添加 WiFi 网络	用户不能自己添加 WiFi 网络 只有在 "连接管理 "中定义了 WiFi 配置文件，才能进行此设置
允许短信和彩信	全部 = 允许所有短信和彩信流量 仅接收短信 = 仅允许接收短信 仅发出短信息 = 只允许发出短信息 无 = 不允许短信/彩信流量
允许漫游期间同步	允许漫游期间同步 开启 = 激活 关闭 = 禁用 用户选择 = 用户的选择
允许语音漫游	允许语音漫游 开启 = 激活 关闭 = 禁用 用户选择 = 用户的选择
使用系统 http 代理服务器	HTTP 代理服务器的使用由系统设置提供，取决于所连接的网络（WiFi 或 APN）。

APN

以下设置仅适用于 Samsung SAFE 2.0 或更高版本!

APN 显示名称	APN 显示名称	
接入点名称	APN 姓名	
发送服务器协议	未设置	
	无	
	PAP	PAP 协议
	查验	CHAP 协议
	PAP 或 CHAP	PAP 或 CHAP 协议
MCC - 移动电话国家代码	在此输入 MCC，如果使用插入的 SIM 卡的 MCC，则留空该字段	
MNC - 移动网络代码	在此输入 MNC，如果使用插入的 SIM 卡的 MCC，则留空该字段	
服务器地址	服务器地址	
服务器端口号	服务器端口号	
服务器代理地址	服务器代理地址	
彩信服务器地址	彩信服务器地址，如为标准地址，请留空	
彩信端口号	彩信端口号	
彩信代理地址	彩信代理地址	
用户名	用户名	
密码	密码	
接入点类型	允许的类型有"默认"、"毫米"、"超级"如果此字段留空，则将使用"default,supl,mms	
首选 APN	优先考虑注册护士	

蓝牙

在这里可以进行各种蓝牙设置。

以下设置仅适用于 Samsung KNOX 1.0 或更高版本!

允许通过蓝牙发现设备	允许通过蓝牙发现设备
允许蓝牙配对	允许蓝牙配对
允许蓝牙耳机设备	允许蓝牙耳机设备
允许蓝牙免提设备	允许蓝牙免提设备
允许蓝牙 A2DP 设备	允许设备之间进行蓝牙 A2DP 音频串流
允许拨出电话	允许通过 BT 拨出电话
允许通过蓝牙传输数据	允许通过蓝牙传输数据
允许蓝牙连接	允许将设备用作调制解调器（蓝牙互联网连接）
允许通过蓝牙连接电脑	允许通过蓝牙连接电脑

PIM 管理

交流

仅适用于 Samsung KNOX 1.0 或更高版本!

电子邮件地址	提供的用户电子邮件地址 请注意 "占位符"，您可以使用这些占位符来处理凭据，而无需在每台设备上手动执行更改。 点击 "**显示占位符**"，您就可以自己显示它们了
服务器主机名	Exchange 服务器的服务器地址
登录名	终端用户设备的登录名，请注意 "此处的占位符
域名	域名地址
密码（仅限设备级）	如果密码为空，系统将提示用户输入 Exchange 密码。
同步的天数	天数，决定电子邮件何时同步返回
签名	可附加签名（提示：某些设备要求签名使用 HTML 格式）
默认账户	确定该邮件账户是标准账户
使用安全套接字层（SSL）	使用 SSL 连接
使用传输层安全（TLS）	使用 TLS 连接
接受所有证书	接受所有证书。如果您的 Exchange 服务器使用自签名证书，请选择此选项

电子邮件

在这里，您可以将 IMAP 和 POP 账户分发到相应的最终用户设备。

以下设置仅适用于 Samsung KNOX 1.0 或更高版本！		
电子邮件地址	提供的用户电子邮件地址 请注意 "占位符"，您可以使用这些占位符来处理凭据，而无需在每台设备上手动执行更改。 点击 "**显示占位符**"，您就可以自己显示它们了	
传入服务器协议	传入服务器协议	IMAP 或 POP
传入服务器地址	传入服务器地址	
传入服务器端口	传入服务器端口	
传入服务器登录名/用户名	传入服务器登录名/用户名	
传入服务器密码（仅限设备级别）	传入服务器密码（仅限设备级别）	
传入服务器使用 SSL	传入服务器使用 SSL	
传入服务器使用 TLS	传入服务器使用 TLS	
传入服务器接受所有证书	接收服务器接受所有类型的证书	
发送服务器协议	发送服务器协议	SMTP
外发服务器端口	外发服务器端口	
发件服务器使用额外的证书	发出服务器的附加凭证。如果设置为 "关闭"，则将使用传入服务器设置	
发件服务器登录名/用户名	发件服务器登录名/用户名	
发送服务器密码（仅限设备级）	发件服务器密码	
传出服务器使用 SSL	传出服务器使用 SSL	
发件服务器使用 TLS	发件服务器使用 TLS	
发件服务器接受所有证书	发件服务器接受所有类型的证书	
签名	可在此处附上签名（提示：某些设备要求签名使用 HTML 格式）	
收到新电子邮件时通知用户	收到新电子邮件时通知用户	

AE Gmail Exchange

信息：此配置将应用于 Gmail 应用程序。因此，您必须批准并安装 Gmail。

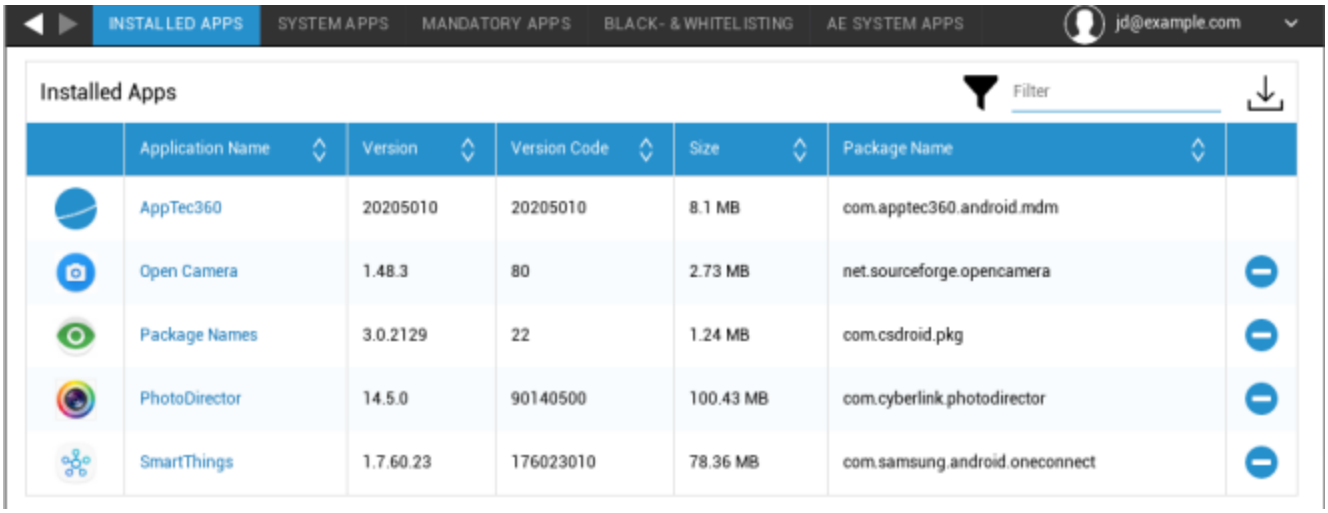
电子邮件地址	提供的用户电子邮件地址 请注意 "占位符"，您可以使用这些占位符来处理凭据，而无需在每台设备上手动执行更改。 点击 "显示占位符"，您就可以自己显示它们了
服务器主机名	Exchange 服务器的服务器地址
登录名	终端用户设备的登录名，请注意 "此处的占位符
签名	可附加签名（提示：某些设备要求签名使用 HTML 格式）
同步的天数	天数，决定电子邮件何时同步返回
设备标识符	EAS 标识符。如果您的环境不需要此项，请将其留空。
使用安全套接字层（SSL）	使用 SSL 连接
接受所有证书	接受所有证书。如果您的 Exchange 服务器使用自签名证书，请选择此选项
允许非托管账户	允许用户添加其他账户
客户证书	如果 Exchange 服务器要求上传客户端证书，请上传客户端证书

应用程序管理

企业应用管理器

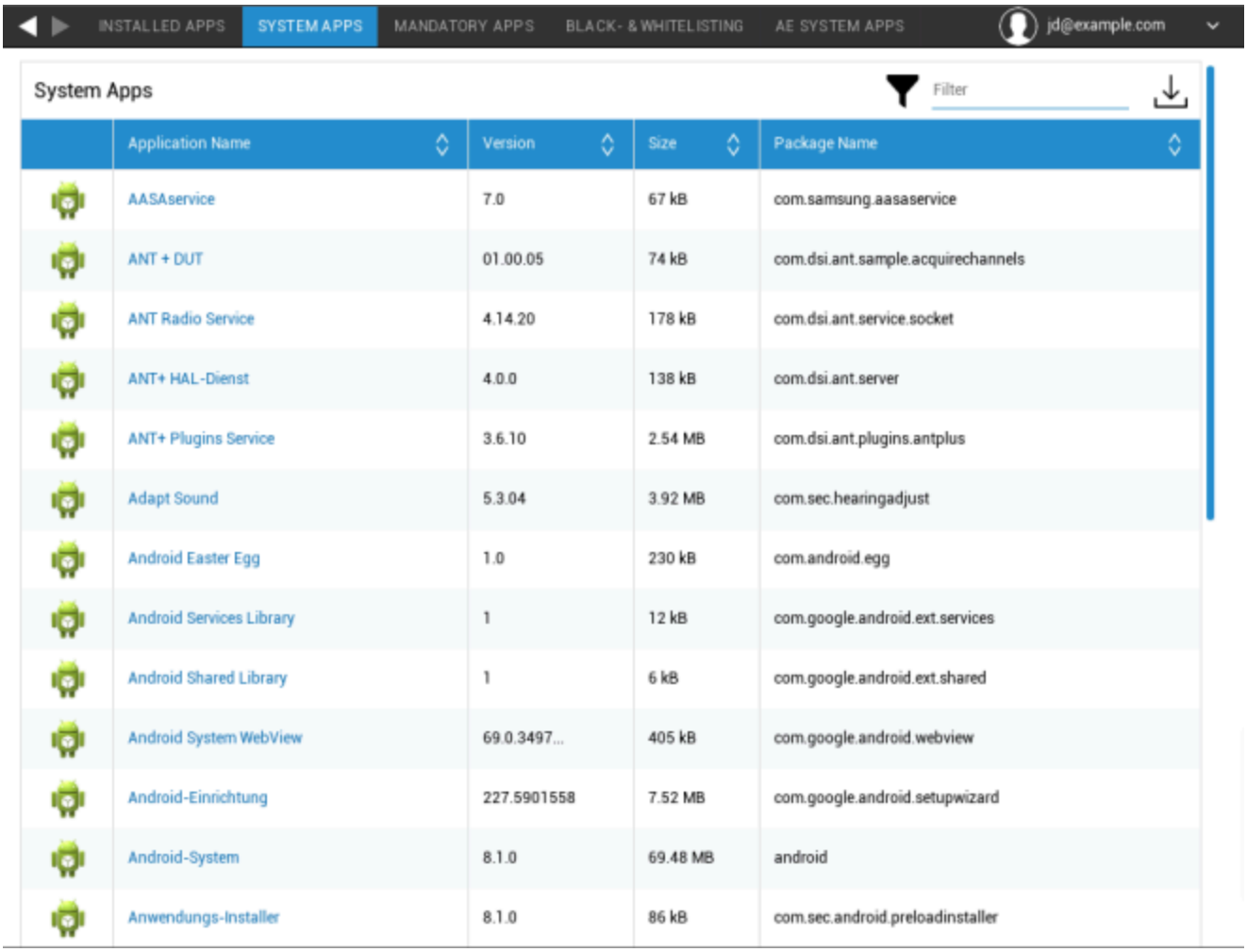
已安装的应用程序（仅限设备级别）

这里将显示当前安装在终端用户设备上的所有应用程序。


INSTALLED APPS
SYSTEM APPS
MANDATORY APPS
BLACK- & WHITELISTING
AE SYSTEM APPS
jd@example.com
Installed Apps
Filter
Application Name
Version
Version Code
Size
Package Name
AppTec360
20205010
20205010
8.1 MB
com.apptec360.android.mdm
Open Camera
1.48.3
80
2.73 MB
net.sourceforge.opencamera
Package Names
3.0.2129
22
1.24 MB
com.csdroid.pkg
PhotoDirector
14.5.0
90140500
100.43 MB
com.cyberlink.photodirector
SmartThings
1.7.60.23
176023010
78.36 MB
com.samsung.android.oneconnect

系统应用程序（仅限设备级）

在 "系统应用程序 "下，将列出所有预装系统的软件包名称和版本。



Application Name	Version	Size	Package Name
AASAservice	7.0	67 kB	com.samsung.aasaservice
ANT + DUT	01.00.05	74 kB	com.dsi.ant.sample.acquirechannels
ANT Radio Service	4.14.20	178 kB	com.dsi.ant.service.socket
ANT+ HAL-Dienst	4.0.0	138 kB	com.dsi.ant.server
ANT+ Plugins Service	3.6.10	2.54 MB	com.dsi.ant.plugins.antplus
Adapt Sound	5.3.04	3.92 MB	com.sec.hearingadjust
Android Easter Egg	1.0	230 kB	com.android.egg
Android Services Library	1	12 kB	com.google.android.ext.services
Android Shared Library	1	6 kB	com.google.android.ext.shared
Android System WebView	69.0.3497...	405 kB	com.google.android.webview
Android-Einrichtung	227.5901558	7.52 MB	com.google.android.setupwizard
Android-System	8.1.0	69.48 MB	android
Anwendungs-Installer	8.1.0	86 kB	com.sec.android.preloadinstaller

必须使用的应用程序

在 "必须安装的应用程序 "中，您可以定义哪些应用程序必须安装在设备上。根据配置和设备的不同，应用程序将自动安装或提示用户安装。

请注意，建议使用 Android Enterprise，以便于管理应用程序。

方案如下：

普通 Play 商店应用程序

Playstore 应用程序的安装始终需要用户交互。此外，还必须在设备上配置 Google 账户。

内部应用程序安装

在三星设备上，这些应用程序将静默安装。唯一例外的是容器，用户必须确认安装。

在其他任何情况下，用户都必须确认应用程序的安装。

安卓企业 Play 商店应用程序

这些应用程序将始终静默安装，无需用户交互。

要添加必选应用程序，请单击 "+"，然后从列表中选择所需的应用程序。请注意，如果设备配置为 Android Enterprise 完全管理或容器，则无法从 "Google Play Store "标签页安装应用程序。

如果使用 Android 企业版，请从 "AE Play Store "部分选择应用程序。要在此提供应用程序，请进入 "常规设置"→"AE Play 商店"→"Play 商店应用程序"，在 Google Enterprise Play 商店中确认这些应用程序。

删除强制应用程序时，该应用程序也将从设备上卸载。

您可以点击必选应用程序列表中的应用程序名称，进入 "配置 "选项卡配置应用程序。这需要使用 Android Enterprise，而且应用程序必须支持该功能。因此，可用选项取决于所选应用程序。

AE 系统应用程序

您可以在此启用安卓企业设备的系统应用程序。请注意，指定的应用程序必须在系统存储中，否则不会发生任何操作。296

限制和设置

黑名单和白名单

您可以在此定义黑名单或白名单。黑名单中的所有应用程序都将被阻止。不在白名单中的所有应用程序都将被阻止。如果黑名单为空，则不会阻止任何程序；如果白名单为空，则会阻止所有程序*。

**所有强制性应用程序和来自企业应用商店的应用程序都将自动列入白名单。无需手动添加*

点击 "+"时，你可以搜索要添加到黑名单或白名单的应用程序，也可以手动输入软件包名称。

系统应用程序限制

在 "系统应用程序限制 "下，你可以阻止预装的应用程序和服务。

禁用浏览器	禁用标准浏览器
禁用日历	禁用本地日历
禁用计算器	禁用计算器
禁用 Chrome 浏览器	禁用 Chrome 浏览器
禁用时钟	禁用时钟
禁用联系人	禁用联系人
禁用拨号器	禁用本地拨号器
禁用电子邮件	禁用电子邮件
禁用 Exchange	禁用 Exchange 账户
禁用 Facebook	禁用 Facebook 应用程序
禁用图库	禁用原生图库应用程序
禁用 Gmail	禁用 Gmail
禁用谷歌图书	禁用谷歌图书
禁用 Google Play Kiosk	禁用 Google Play Kiosk
禁用谷歌地图	禁用谷歌地图
禁用谷歌音乐	禁用谷歌音乐
禁用谷歌电影	禁用谷歌电影
禁用 Google Play 商店	禁用 Google Play 应用商店（公共应用商店）
禁用 Google Plus	禁用 Google Plus
禁用谷歌搜索	禁用谷歌搜索
禁用 Google Talk / Google Hangouts	禁用 Google Talk / Google Hangouts
禁用音乐播放器	禁用本机音乐播放器应用程序
禁用设置	禁用设备设置
禁用模拟工具包	禁用模拟工具包服务
禁用短信/彩信	禁用短信/彩信
禁用街景	禁用街景服务
禁用 Youtube	禁用 Youtube

三星应用程序

在 "Samsung Apps "下，您可以为三星设备定义其他设置和/或限制。

禁用 AllShare Play / Samsung Link	禁用 AllShare Play / Samsung Link
禁用 ChatON	禁用 ChatON
禁用游戏中心	禁用游戏中心
禁用群组游戏	禁用群组游戏
禁用帮助	禁用三星帮助
禁用 KNOX	禁用三星 KNOX 容器
禁用备忘录	禁用语音备忘录
禁用我的文件	禁用我的文件
禁用光学读卡器	禁用光学读卡器
禁用北极星办公室	禁用北极星办公室
禁用阅读器集线器/三星图书	禁用阅读器集线器/三星图书
禁用 S 备忘录	禁用三星备忘录应用程序
禁用 S 翻译器	禁用三星翻译应用程序
禁用 S Voice	禁用 S 语音助手
禁用三星应用程序	禁用三星应用程序商店
禁用 Samsung Hub	禁用三星娱乐商店
禁用视频播放器	禁用视频播放器
禁用录音机	禁用录音机
禁用 WatchON	禁用 WatchON（模拟遥控器）

华为应用程序

在 "华为应用程序 "下，您可以定义华为设备的其他设置和/或限制。

禁用 DLNA	禁用 DLNA
禁用应用程序安装程序	禁用应用程序安装程序
禁用文件管理器	禁用文件管理器
禁用备份管理器	禁用备份管理器
禁用系统更新程序	禁用系统更新程序
禁用工具箱	禁用工具箱
禁用天气	禁用天气
禁用调频收音机	禁用调频收音机

应用程序管理设置

在这里，您可以定义 InHouse 应用程序的更新行为。

更新检查频率定义了 AppTec360 应用程序查找 InHouse 应用程序更新的频率。一旦检测到新版本，就会下载并安装。

Wi-Fi 阈值定义了如果应用程序大于您配置的阈值，下载是否应仅限于 Wi-Fi 连接。如果阈值较小或您未定义阈值，应用程序将在 WLAN 和蜂窝网络中下载。

企业应用商店

请注意，在这里（企业应用程序商店）添加的应用程序不会自动安装到设备上。用户必须在设备上打开企业应用商店并手动安装应用程序。

如果要在设备上自动安装应用程序，请转到 "应用程序管理"→"企业应用程序管理器"→"强制应用程序"，然后在其中添加所需的应用程序。

在这一点上，您可以向用户分发可选应用程序。

Playstore

点击 "+"，在商店中添加 Play Store 应用程序。如果使用安卓企业版，请转到 "应用程序管理企业版播放商店"。另外请注意，必须在设备上配置一个谷歌账户，才能安装此处定义的应用程序。

内部

在 "内部 "点下，您可以上传和分发内部开发的应用程序。

点击 "+"，将 InHouse 应用程序添加到企业应用程序商店，然后用户就可以安装了。在此对话框中还可以上传新的 InHouse 应用程序。

企业 Play 商店

请注意，在此添加应用程序（企业版 Play Store）不会使其自动安装到设备上。用户必须在设备上打开 Play Store 并手动安装应用程序。

如果要在设备上自动安装应用程序，请转到 "应用程序管理"→"企业应用程序管理器"→"强制应用程序"，然后在其中添加所需的应用程序。

在这一点上，您可以向用户分发可选应用程序。

您可以在此向 Android 企业 Playstore 添加应用程序。请注意，您必须在 "常规设置"→"AE Play Store"→"Play Store 应用程序 "中批准应用程序。这些应用程序将被添加到正常的 Google Play 商店。

此外，请注意首先要在常规设置 → 应用程序管理 → AE Play 商店 → 商店布局中定义应用程序的布局。

应用程序必须在布局中，然后才能成功添加到商店中。

信息亭模式和启动器

信息亭模式

Kiosk 模式允许您预先定义一个应用程序或一个 URL。然后就可以专门运行/访问该应用程序或 URL。

同样，各种硬件按钮也可以在信息亭模式中停用。

自动启动	一旦配置文件到达终端用户设备，就自动启动 Kiosk 模式
预定的信息亭模式?	您可以为信息亭模式规划一个时间，它将在您设定的时间自动开始和结束
开始时间	开始时间
时间（分钟	信息亭模式再次结束的时间（以分钟为单位

应用类型

单一应用程序	如果想以 Kiosk 模式启动应用程序，请在 "应用程序类型 "下选择 "软件包"。
信息亭应用	单击此处，选择应在 Kiosk 模式下启动的应用程序 您将看到常用的应用程序管理概览 您可以在 "Google Play 商店"、"Android 内部应用程序 "和 "软件包名称 "之间进行选择

应用类型

网址	如果要在 Kiosk 模式下启动 URL，请在 "应用程序类型 "下选择 "URL"。 然后定义所需的 URL 地址
闲置后清除浏览器	您可以在这里定义一个时间间隔（以分钟为单位），在该时间间隔之后重新启动信息亭模式。
清除网页缓存和 Cookie	如果激活此功能，则在重新启动 Kiosk 模式后，网络缓存（cookie 和缓存图片）将被清除
同源政策	如果激活该功能，则用户只能浏览指定 URL 的子页面 例如，您定义了以下 URL:www.mypage.com然后，用户可以在以下网址上网： www.mypage.com/subpage
白名单 URL	在这里您可以维护一个白名单，所有这些 URL 都是允许的 每行最多 1 个 URL URL 必须以 http:/ 或 https:// 开头
黑名单 URL	在这里您可以维护一个黑名单，所有这些 URL 都是不允许的 每行最多 1 个 URL URL 必须以 http:/ 或 https:// 开头
屏幕方向	该设置与屏幕调整有关 自动 = 自动 纵向 = 垂直格式 横向 = 横向模式

多功能应用程序	如果选择 "多应用 "信息亭模式，则将强制使用 AppTec360 启动器。
应用程序	应用程序：选择 Playstore 或内部应用程序作为 Kiosk 应用程序。也可以输入软件包名称。所选的 Kiosk 应用程序必须安装在设备上。请记住将 Kiosk 应用程序设置为必选。 主屏幕上的快捷方式：如果设置为 "开"，将在主屏幕上创建快捷方式。如果设置为 "关闭"，应用程序仍将显示在应用程序列表中。

启用退出密码	如果激活了该功能，用户就可以使用预先设置的密码结束信息亭模式。
退出密码	这是您预先设定的密码
自动折叠状态栏	如果启用该选项，状态栏将自动按字母顺序排列。使用该选项，用户可以看到状态栏的信息，但无法访问其功能
禁用状态栏	状态栏包含通知、快捷方式和信息。仅适用于 KNOX 1.0 或更高版本的三星设备。
禁用音量键	禁用音量键（仅适用于配备 KNOX 1.0 或更高版本的三星设备）
禁用开/关开关	禁用开/关开关（仅适用于配备 KNOX 1.0 或更高版本的三星设备）
禁用主页按钮	禁用主页按钮。如果激活了该功能，则只能在 AppTec360 控制台中终止 Kiosk 模式。 (仅适用于配备 KNOX 1.0 或更高版本的三星设备）
禁用导航栏	使用此功能可以禁用导航栏（返回/菜单） 如果激活了该功能，则只能在 AppTec360 控制台中终止 Kiosk 模式 (仅适用于配备 KNOX 1.0 或更高版本的三星设备）

应用程序更新设置	
允许应用程序更新	即使 Kiosk 模式处于激活状态，也会提示用户执行应用程序更新。在装有 Samsung KNOX 的设备上，应用程序将静默更新。
更新窗口	设置提示用户安装应用程序更新的时间间隔。

TeamViewer	
启用无人值守访问	如果启用，管理员就可以远程控制设备，而无需用户交互。设备上需要安装应用程序 TeamViewer Host。

AppTec360 启动器

启用 AppTec360 启动器	开启：启用 AppTec360 启动器。用户必须将其设置为默认启动器一次。 注：如果启用了 Kiosk 模式，且 Kiosk 模式设置为 "多应用程序"，则将强制使用 AppTec360 启动器。
大图标	打开：在启动器中显示更大版本的应用程序图标
隐藏 AppTec360 应用程序图标	开启：完全隐藏 AppTec360 应用程序
隐藏 AppTec360 商店图标	开启：完全隐藏 AppTec360 企业应用商店

AppTec360 设置

启用 AppTec360 设置应用程序	AppTec360 设置应用程序可控制 WiFi 和蓝牙连接
在多应用程序中启用设置信息亭模式	如果启用，用户可在多应用信息亭模式激活时访问 AppTec360 设置应用

遥控器

泼水节

显示 Splashtop 设置的当前状态。在这里，您将看到通过 Splashtop 远程访问设备所需的步骤。您还需要在此输入部署代码，该代码可从 Splashtop 网站获取。连接设备需要部署代码。

Teamviewer

显示 Teamviewer 设置的当前状态。您将在此看到通过 Teamviewer 远程访问设备所需的步骤。

内容管理

内容框

在此您可以为该设备启用内容盒。激活后，Contentbox 应用程序将安装在设备上。

安全浏览器

在此，您可以为该设备启用安全浏览器。激活后，设备上将安装安全浏览器应用程序。该浏览器可以配置为在设备上提供仅限于您需要的 Web 浏览器。

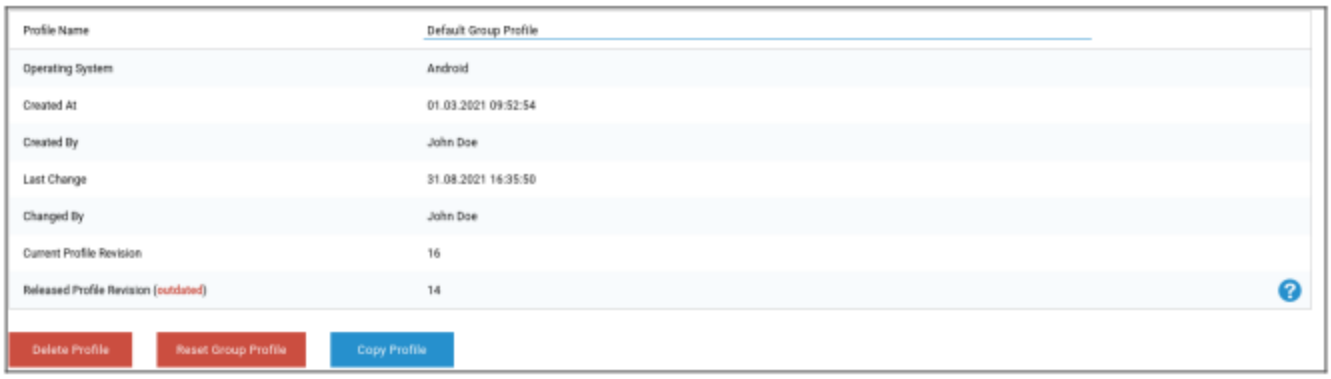
要求密码	要求用户设置并使用密码访问浏览器。
限制下载/打开	阻止从网站下载
限制上传	限制上传至某些 URL。不提供 URL 可完全阻止上传
允许复制	允许复制、剪切或共享网页内的文本。
允许屏幕捕捉	允许截图
数据清理频率	选择自动删除所有用户数据（历史记录、缓存等）的频率。
公司书签	书签将显示在浏览器书签中的 "公司书签 "文件夹中。用户无法对其进行编辑。
隐藏地址栏	隐藏地址栏，使用户看不到正在访问的 URL
浏览器内白名单（无通用网关）	启用客户端 URL 白名单。- 公司书签始终在白名单中 - 仅支持 100 个 URL - 请使用通用网关进行无限制的黑名单和白名单设置
基于网关的黑白名单设置	黑名单有以下要求：- 正常运行的 AppTec360 通用网关（"常规设置"→"通用网关"） - 具有指定 DNS 服务器的正常 VPN 配置（"常规设置"→"通用网关"→"VPN 设置"） - 黑名单配置（"常规设置"→"通用网关"→"网域黑名单"） - 配置文件中有效的 VPN 连接（"连接管理"→"VPN"）。

配置 Windows 10 电脑

一般情况

组概况概览（仅适用于组级）

打开群组资料时，您将快速浏览该资料。



简介名称	个人资料名称（可在此处更改）
操作系统	配置文件适用的操作系统
创建于	创建时间
创建者	个人资料创建者
最后的变化	最后一次更改配置文件的时间
已更改	最后更改的账户
当前的简介修订	修订已保存的配置文件状态
已发布的简介修订版	已分配的配置文件修订版（"立即分配"）。如果标签文字后面显示"（已过期）"，则表示您已经保存了配置文件，但尚未分配，因此设备仍将获得旧版本。

设备概述（仅限设备级别）

设备概述，包括以下内容：

个人计算机名称	个人计算机名称
客户	设备的 Windows 类型
最后知道的地点	设备最后已知位置的经纬度
指定的强制性应用程序	分配给设备的强制应用程序数量
PC UID	PC 的 UID
操作系统版本	显示您的 Windows 版本
操作系统版本	当前安装的 Windows 版本
操作系统构建	当前的 Windows 版本
操作系统	当前安装的操作系统
序列号	设备序列号
设备所有权	配置的所有权类型
设备类型	设备类型
扎根	显示设备是否已 root
符合要求	显示设备是否符合标准
最后查看	更改个人资料的日期和时间
用户分配	显示此设备当前分配给的用户或组。 您可以从下拉列表中选择不同的用户或组移动设备。

设置

允许自动更新	允许或禁止 os 自动更新。

配置修订（仅限设备级）

在这里，您将看到为设备分配的组配置文件的概览。

如果点击群组配置文件，就可以直接进入配置文件并进行设置。

使用该符号，可以将已分配的应用程序还原为群组配置文件的设置。

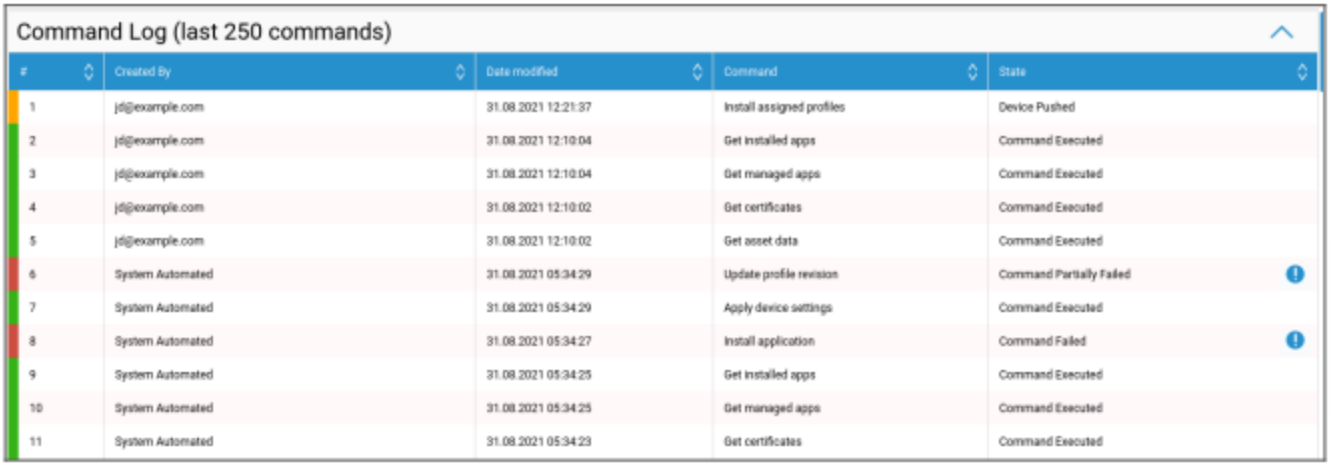
通过该符号，您可以重置设备配置文件，使其没有任何设置。

"最新版本可用 "表示组配置文件已更改并保存，但尚未分配。必须在组级别上使用 "立即分配 "来分配组配置文件，才能将更改应用到设备上。

设备日志（仅限设备级）

命令日志

在这里，您可以查看为设备发出的命令及其状态。



系统自动 "创建的命令由系统自动创建。

可能的命令状态

设备已推送	推送请求已发送至推送服务（如 APNS），以通知设备连接回 EMM 服务器。
创建命令	该命令已在系统中创建。
发送命令	设备与服务器连接后，命令被发送到设备。
命令已执行	命令已成功执行。
命令失败	命令失败。*
命令部分失败	根据设备操作系统的不同，有些命令可能会被组合在一起。 其中，该命令组的某些部分出现故障。*
命令已执行，但最终失败	命令已执行，但也可能没有执行。
命令重发	命令被用户重新推送。
弃用	命令被丢弃。例如，该命令被其他命令取代，或设备重新注册，旧命令被删除。

*如果信息后面有感叹号，您可以用光标悬停在图标上，获取更多信息。

资产管理（仅限设备级）

设备信息

制造商	设备制造商
模型	设备型号
型号	型号
操作系统	操作系统
操作系统版本	操作系统版本
序列号	序列号
ExchangeID	ExchangeID
总内存	总内存
显示分辨率	显示分辨率
电话语言	设备语言
固件版本	固件版本
DM 客户端版本	设备管理客户端版本
硬件版本	设备硬件版本
CPU 架构	CPU 架构（处理器类型）

细胞

SIM 卡运营商网络	运营商网络
电话号码	电话号码
漫游状态	漫游状态
IMEI	IMEI
IMSI	IMSI
调制解调器固件	调制解调器固件

同步信息

即时 DM 连接	设备应立即与 AppTec 建立连接
初始重试时间	首次连接的初始重试时间
连接重试	从连接管理器断开连接或出现 WinInet 级错误后，重试新连接的次数
最长睡眠时间	软件包发送错误后的最长休眠时间
首次同步重试	入学后第一阶段的时间
首次重试间隔	入学后第一阶段的时间
第二次同步重试	入学后第二阶段的时间
第二次重试间隔	入学后第二阶段的时间
常规同步重试	入学后其他阶段的时间
常规重试间隔	入学后其他阶段的时间

安全管理

防盗（仅限设备级）

GPS 信息（仅限设备级别）

在这里可以确定当前/最后的设备位置。可以使用一个甚至两个密码保护定位功能 - 请参阅："常规设置">"隐私">"GPS 访问"："常规设置">"隐私">"GPS 访问

GPS 设置

启用 GPS 跟踪	启用定期同步 GPS 信息功能。
跟踪间隔	设置 GPS 信息同步间隔。

安全配置

密码

最小密码长度	最小密码长度	
密码组成	指定密码必须包含的特定字符数 其中包括大写字母、小写字母、数字和特殊符号	
密码质量	您可以在此设置密码质量	
	字母数字	只有数字和字母
	数字	只有数字
	数字或字母数字	数字或数字和字母
最长闲置时间锁定	用户在设备上不活动的分钟数，之后设备将被锁定。用户必须在此时间后通过输入设备密码来解锁设备。	
密码过期	设置必须设置新密码之前的时间	
密码历史限制	不允许使用的以前使用过的密码数量	
密码尝试失败次数上限	在对设备进行完全擦除之前，错误输入密码的次数	

杀毒软件

防病毒设置 - 设置扫描配置	
扫描类型	选择执行快速扫描还是全面扫描
设置扫描开始	选择 Windows Defender 开始扫描的时间
扫描频率	选择 Windows Defender 扫描应运行的日期
签名更新频率	指定用于检查签名的时间间隔（小时

配置扫描的文件类型	
允许扫描档案文件	允许或禁止扫描正在访问的压缩文件（如 .zip）。
允许扫描脚本	允许或禁止 Windows Defender 脚本扫描功能。
允许扫描电子邮件	允许或禁止扫描电子邮件。
允许扫描网络文件	允许或禁止扫描网络文件。
允许全面扫描映射的网络驱动器	允许或禁止扫描映射的网络驱动器（仅在启用全面扫描时启用）。
控制双向扫描	控制应监控哪些文件集。
允许全面扫描移动硬盘	允许或不允许全面扫描移动硬盘。仅在启动全面扫描时。

扫描排除的文件类型	
忽略扫描的文件类型	定义一组文件扩展名类型。每个文件扩展名对应每个字段。
忽略目录路径	定义一组目录路径，以便不对其进行扫描。每个字段一个路径。例如"C:\Example"、"C:\Windows "或 "C:\Users"。
从扫描中排除进程	从 Microsoft Defender Antivirus 扫描中排除特定进程已打开的文件。.每个字段一个路径。例如"C:\myFile.exe"、"C:\Windows\myProcess.exe"、"C:\myScript.bat

额外设置	
允许实时监控	允许或禁止 Windows Defender 实时监控功能
允许行为监控	允许或禁止 Windows 行为监控功能
允许云保护	允许或不允许 Windows Defender 向微软发送有关其发现的任何问题的信息。微软将分析这些信息，进一步了解影响设备的问题，并提供改进的解决方案。
	发送样本的行为
允许 Windows Defender IOAV 保护	允许或禁止 Windows Defender IOAV 保护
允许访问 Defenders "开启访问保护 "用户界面	
平均 CPU 负载系数	表示 Windows Defender 扫描的平均 CPU 负载系数（单位：%）。

恶意软件处理	
严重程度低	您可以为每个严重性级别定义设备处理恶意软件的方式。 可用的选项有 • 清洁 • 隔离 • 移除 • 允许 • 用户定义 • 街区
中等严重程度	
高度严重性	
严重程度	
保留已清理恶意软件的天数	隔离文件/项目在系统中的存储天数。默认值为 0，它将项目保留在隔离区中，不会自动删除。最大值为 90。

安全中心

Windows 安全中心 - Windows 安全设置	
禁用病毒和威胁防护用户界面	
隐藏勒索软件数据恢复用户界面	
禁用账户保护用户界面	
禁用防火墙和网络保护用户界面	
禁用应用程序和浏览器控制用户界面	
禁止更改漏洞保护	禁止用户更改漏洞利用保护设置
禁用设备安全用户界面	
隐藏 TPM 故障排除	隐藏 TPM 故障排除设置
禁用清除 TPM 按钮	
禁用设备性能和健康 UI	
禁用家庭选项用户界面	

定制祝酒词	
启用自定义支持信息	启用后，可在安全中心应用程序的右下角显示贵公司的自定义支持联系信息。
电子邮件地址	设置公司电子邮件地址
公司名称	设置公司名称
公司电话	设置公司电话
帮助 URL	设置公司的帮助 URL

额外设置	
禁用通知	禁用 Windows Defender 安全中心通知的显示。
隐藏 TPM 固件更新建议	在检测到有漏洞的固件时，隐藏更新 TPM 固件的建议。
显示公司名称和联系人选项	在 Windows Defender 安全中心飞出的联系卡中显示您的公司名称和联系选项。
隐藏安全启动	隐藏安全启动区。
隐藏安全通知区域控件	隐藏 Windows 安全通知区域控件

防火墙配置

防火墙配置 - 全局设置	
忽略验证设置	如果不支持验证组中指定的所有验证套件，则忽略整个验证组
数据包队列类型	为 IPsec 隧道网关方案的加密接收和清除转发路径指定如何启用接收端软件的扩展。
禁用执行状态 FTP 过滤	如果禁用，则不会执行有状态文件传输协议 (FTP) 过滤以允许二级连接
安全关联空闲时间	此字段配置安全关联空闲时间（秒）。在此指定时间内未看到网络流量后，安全关联将被删除。
预共享密钥编码	设置预共享密钥编码
IPSec 例外	配置互联网协议例外
证书吊销列表检查	

防火墙配置文件（域配置文件/私人配置文件/公共配置文件）	
为该配置文件启用防火墙	
禁用通知	当应用程序被阻止监听某个端口时，禁用向用户显示通知。
阻止对组播广播的单播响应	
执行授权应用程序防火墙规则	如果不执行，本地存储中的授权应用程序防火墙规则将被忽略，也不执行
执行全局端口防火墙规则	如果不执行，本地存储中的全局端口防火墙规则将被忽略，也不执行。只有在组策略存储中设置或枚举该设置，或从 GroupPolicyRSoPStore 枚举该设置时，该设置才有意义。
执行防火墙规则	如果不执行，本地存储的防火墙规则将被忽略，也不执行
执行连接安全规则	如果不执行，本地存储的连接安全规则将被忽略或不执行
默认出站操作	防火墙默认情况下对出站连接执行的操作
默认入站操作	防火墙默认对入站连接执行的操作
禁用隐身模式	隐身模式是 Windows 防火墙中的一种机制，有助于防止恶意用户发现有关网络计算机及其运行服务的信息。
禁止对未经请求的流量做出响应	如果禁用，防火墙的隐身模式规则不得阻止主机响应未经请求的网络流量（如果该流量由 IPsec 保护）。

防火墙规则

防火墙规则	
名称	规则名称
说明	规则说明
行动	指定此规则是阻止流量还是允许流量。请注意，"阻止 "选项也可能阻止 MDM 服务器和设备之间的流量（取决于其他配置）。
方向	
启用边缘遍历（仅在**方向**设置**为入站流量**时可用）	表示允许特定的入站流量使用 Teredo 隧道技术在 NAT 和其他边缘设备之间进行隧道传输。

计划与服务	
定义应用程序，所有其他	如果未启用，则会考虑所有申请
软件包系列名称	规则适用的软件包系列名称。
应用程序的文件路径	规则将适用的完整应用程序，如 C:\Windows\System\Notepad.exe
完全合格的二进制名称	规则适用的完全限定二进制名称。FQBN 是以下形式的字符串：{发布者/产品/文件名,版本}。
服务名称	输入服务名称（如 "EventLog"）。您可以通过运行 "Get-Service "命令在 Powershell 中获取服务名称列表。

协议和端口				
规程	规则使用的协议。			
	可用值： - 任何 - 定制 - 霍波特 - ICMPv4 - IGMP - TCP - UDP - IPv6 - IPv6 路由 - IPv6-碎片 - GRE - ICMPv6 - IPv6-NoNxt - IPv6 选项 - VRRP - PGM - L2TP	设置为自定义时	插入介于 0 和 255 之间的协议编号	协议编号
		当设置为 TCP 或 UDP 时	指定本地端口，否则将使用所有端口	规则将使用的本地端口，也允许使用范围端口
			当地港口	单个端口或一系列端口。例如 100-120、200、300-320。
			指定远程端口，否则将使用所有端口	规则将使用的远程端口，也允许使用范围端口
			远程端口	单个端口或一系列端口。例如 100-120、200、300-320。

范围		
指定本地 IP，否则任意 IP		本地 IP 的集合，也可以是以 - 分隔的 IP 范围。
	本地 IP 地址	一组单个 IP 或以 - 分隔的 IP 范围
指定远程 IP，否则任意远程 IP		指定一组远程 IP，也可以是用"-"分隔的 IP 范围。
	远程 IP 地址	指定单个 IP 或 IP 范围
	代币	可与远程地址一起设置的令牌。Windows 10 1809 及更高版本支持 Intranet、RmtIntranet 和 Ply2Renders 标记。

高级设置	
指定配置文件，否则将使用所有配置文件	如果禁用，将使用所有配置文件
域名	域名简介

私人	私人简介
公众	公众简介
指定接口，否则将使用所有接口	如果禁用，将使用所有接口
局域网	局域网接口
远程访问	远程访问界面
无线	无线接口

当地校长	
添加授权本地用户	允许添加将使用此规则的本地用户列表
授权用户	此规则的授权本地用户列表。用户必须采用安全描述定义语言 (SDDL) 格式，如 PC_NAME/USERNAME。如果服务名称被设置为使用此规则，则不得填写此字段

限制设置

设备功能

允许使用 SD 卡	允许使用 SD 卡
允许相机	允许使用摄像机
允许定位服务	允许设备定位服务
允许应用程序侧载	允许安装未知来源的应用程序
允许开发者模式	允许开发人员模式
允许蜂窝数据漫游	允许蜂窝数据漫游
允许 Cortana	允许语音助手 Cortana
允许搜索使用位置	允许搜索使用位置
允许添加非微软电子邮件帐户	指定是否允许用户添加非 MSA 电子邮件帐户。
允许微软账户连接	指定是否允许使用 MSA 帐户进行与电子邮件无关的连接验证和服务。
允许同步我的设置	允许在整个设备上同步设置
企业保护域名	指定以"; "分隔的企业域名。
允许用户禁用系统还原	允许用户禁用系统还原。 **警告!** 此功能只能在企业公司或组织拥有或提供的设备上使用，或者在用户拥有的设备上使用，如果用户允许由企业公司完全管理该设备。如果禁用此策略设置，系统还原将被关闭，并且无法访问系统还原向导。配置系统还原或通过系统保护创建还原点的选项也会被禁用。
允许用户取消注册	允许用户从设备上删除企业部分，从而断开与 AppTec360 服务器的连接。如果发生这种情况，将无法再管理设备 **警告!** 此功能只能在企业公司或组织拥有或提供的设备上使用，或者在用户拥有的设备上使用，前提是用户允许设备由企业公司完全管理。如果禁用此策略设置，用户将无法删

	除 MDM 注册。 指定是否允许用户通过工作场所控制面板删除工作场所账户。MDM 服务器始终可以远程删除账户。

比特锁

BitLocker 配置

常规设置	
要求设备加密	提示用户启用设备加密。根据 Windows 版本和系统配置，可能会询问用户： - 确认未启用其他提供商的加密。 - 要关闭 BitLocker 驱动器加密，然后再打开 BitLocker。
加密方法	
操作系统驱动器的加密方法	
固定数据驱动器的加密方法	
移动数据驱动器的加密方法	
禁用第三方磁盘加密警告	禁用关于设备正在使用第三方磁盘加密服务的警告提示。 从 Windows 10（1803 版）开始，此设置仅支持 Azure Active Directory 加入的设备。
允许在非管理员用户登录时运行加密功能	仅支持已加入 Azure Active Directory 的设备

AppTec360 扩展	
静音加密	如果选择 "要求设备加密"，AppTec360 管理服务将自动对设备驱动器进行静默加密。
自动生成用户证书	加密后的操作系统硬盘将受到自动生成的用户凭据的保护。 如果有 TPM，可以使用 TPM PIN 或 6 位数文本密码。 生成的证书会发送到指定设备注册的电子邮件地址。 如果关闭该选项，则只能使用 TPM 进行静默加密保护。 在这种情况下，对于没有 TPM 的设备，静默加密将失败。
加密固定硬盘	任何可用的固定数据驱动器也将加密，并使用存储在操作系统驱动器上的密钥进行 "自动解锁 "保护。

操作系统驱动器设置	

启动时要求额外的身份验证	此设置允许您配置 BitLocker 是否在每次启动计算机时都要求进行身份验证。 此设置在设置 BitLocker 时应用。 如果启用此设置，用户可以在 BitLocker 设置向导中配置高级启动选项。
阻止没有兼容 TPM 的 BitLocker	
仅 TPM	
TPM 和 PIN	
TPM 和密钥	
TPM、密钥和 PIN 码	如果需要使用 PIN 和 USB 闪存驱动器（密钥），用户必须使用命令行工具 "manage-bde "而不是 BitLocker 驱动器加密设置向导来设置 BitLocker。

要求最小 PIN 码长度	
	最少字符数

配置预启动恢复信息和 URL	配置整个恢复信息，或替换操作系统驱动器锁定时预启动密钥恢复屏幕上显示的现有 URL。 注意：并非所有字符和语言都支持预启动。强烈建议您测试使用的字符是否能正确显示在预启动恢复屏幕上。
	启动前恢复信息选项
	自定义恢复信息
	自定义恢复 URL

操作系统硬盘恢复选项		此设置可让您控制在没有所需凭证的情况下如何恢复受 BitLocker 保护的操作系统驱动器。 此设置在设置 BitLocker 时应用。 默认情况下，允许使用基于证书的数据恢复代理，恢复选项可由用户指定，包括恢复密码和恢复密钥，恢复信息不会备份到 AD DS。
	基于块证书的数据恢复代理	指定数据恢复代理是否可用于受 BitLocker 保护的操作系统硬盘。 在使用数据恢复代理之前，必须在组策略管理控制台或本地组策略编辑器的公钥策略项目中添加该代理。 有关添加数据恢复代理的详细信息，请参阅 Microsoft TechNet 上的《BitLocker 驱动器加密部署指南》。
	BitLocker 恢复密码设置	
	BitLocker 恢复密钥设置	
	将 BitLocker 恢复信息保存到 Active Directory 域服务中	
	AD DS BitLocker 恢复存储配置	存储密钥包有助于从物理损坏的硬盘中恢复数据。
	要求将恢复数据存储到 AD DS	防止用户启用 BitLocker，除非计算机已连接到域，并且

固定驱动器设置	
固定硬盘恢复选项	此设置可让您控制在没有所需凭证的情况下如何恢复受 BitLocker 保护的固定硬盘。 此设置在设置 BitLocker 时应用。 默认情况下，允许使用基于证书的数据恢复代理，恢复选项可由用户指定，包括恢复密码和恢复密钥，恢复信息不会备份到 AD DS。
基于块证书的数据恢复代理	
BitLocker 恢复密码设置	
BitLocker 恢复密钥设置	
将 BitLocker 恢复信息保存到 Active Directory 域服务中	
AD DS BitLocker 恢复存储配置	存储密钥包有助于从物理损坏的硬盘中恢复数据。
要求将恢复数据存储到 AD DS	防止用户启用 BitLocker，除非计算机已连接到域，且 BitLocker 恢复信息已成功备份到 AD DS。 注意：恢复密码会自动生成。
拒绝写入未受保护的固定硬盘	

可移动驱动器设置	
拒绝写入未受保护的移动硬盘	拒绝写入不受 Bitlocker 保护的可移动数据驱动器。注意：如果组策略中已启用 "可移动磁盘：拒绝写入访问"，则此策略设置将被忽略。
拒绝对其他组织配置的设备进行写入访问	只有识别字段与计算机识别字段相匹配的硬盘才能获得写入权限。这些字段由 "为贵组织提供唯一标识符 "组策略设置定义。

BitLocker 状态

在此，您可以看到 BitLocker 加密硬盘的当前状态

C [OS Drive]
加密状态
加密 (%)
保护状态
加密方法
钥匙保护器
恢复密码

点击 "旋转恢复密码 "按钮，即可旋转 BitLocker 恢复密码。

证书管理

证书列表

下面是显示的设备上安装的证书列表。

证书配置

您可以在此配置证书及其在设备上的安装方式。

可信证书	
说明	证书说明
范围	证书部署范围：当前用户与设备
证书存储	"不受信任的证书 "仅在 Windows 10（1803 版）中可用
证书文件	上传 PKCS#1 文件

身份证明			
说明	证书说明		
范围	证书部署范围：当前用户与设备		
关键位置	要安装私钥的密钥存储提供程序。		
		TPM。如果没有 TPM，则失败	
	TPM。如果没有 TPM，则退回到软件 KSP		
	软件密钥存储提供商	将私人密钥标记为可导出	
	Windows Hello for Business	容器名称	指定 Windows Hello for Business（以前称为 Microsoft Passport for Work）容器名称。
		密码提示文本	指定证书注册过程中 Windows Hello for Business PIN 提示符上显示的自定义文本。
证书	上传 PKCS#12 文件		

SCEP

说明	SCEP 服务器说明		
部署范围	证书部署范围：当前设备与用户		
SCEP 服务器 URL	一台或多台通过 SCEP 签发证书的服务器		
主题	X.500 名称的表示。例如："C=US，O=微软公司，CN=foo，1.2.5.3=bar"。		
主题替代名称	类型	电子邮件地址	
		DNS	
		通用资源识别号	
		用户主要名称（UPN）	
CA 指纹	证书颁发机构证书的 SHA1 指纹。E.g. 31:8F:1E:78:5C:D5:12:9F:7E:3B:AD:F3:1C:C0:19:03:96:43:A9:E5		
有效期单位	天、月或年		
有效期			
挑战	用作自动注册的预共享密文		
重试	如果服务器发送 PENDING（等待）响应，设备应重试的次数。默认值为 5，最大值为 30。		
重试延迟	重试前等待的分钟数。默认值为 5，最小值为 1。		
关键尺寸	密钥大小（比特		
哈希算法	哈希算法系列		
主要用途	密钥用途扩展项定义了证书所含密钥的用途（如加密、签名）。至少需要选择 "数字签名 "或 "密钥加密 "中的一项。		
扩展密钥用途	指定扩展密钥的使用。指定相应的 OID 列表，如 1.3.6.1.5.5.7.3.2（客户端身份验证）		
关键位置	要安装私钥的密钥存储提供程序。		
		TPM。如果没有 TPM，则失败	
	TPM。如果没有 TPM，则退回到软件 KSP		
	软件密钥存储提供商		
	Windows Hello for Business	容器名称	指定 Windows Hello for Business（以前称为 Microsoft Passport for Work）容器名称。

		密码提示文本	指定证书注册过程中 Windows Hello for Business PIN 提示符上显示的自定义文本。	

连接管理

无线网络

在此设置下，执行终端用户设备访问内部接入点的预配置

服务集标识符（SSID）	将建立连接的网络的 SSID
自动加入	激活自动加入网络
隐藏的网络	激活，以防接入点不广播 SSID

安全类型

建立 AP 安全类型

WEP 开放系统	
密码	AP 密码

WPA PSK	
密码	AP 密码

WPA EAP	
认证类型	身份验证类型，仅适用于 "PEAP-MSCAHPv2"。
快速重新连接	设备可在接入点之间切换，无需再次进行身份验证
访客访问	该用户没有账户，因此应注册为访客
检疫检查	客户端必须执行 NAP（网络访问保护）检查，并与系统共享结果，然后由系统决定客户端是否可以连接
要求密码绑定	只能通过密码绑定进行身份验证
服务器验证	客户端会检查服务器证书是否有效。如果有效，将建立连接
提示获取证书	允许用户接受不受信任的证书
服务器名称	提供显示提供网络身份验证和授权的 RADIUS 服务器名称的选项

WPA2-PSK	
密码	AP 密码

WPA2 EAP	
认证类型	身份验证类型，仅适用于 "PEAP-MSCAHPv2"。
快速重新连接	
访客访问	
检疫检查	激活网络访问保护 NAP
要求密码绑定	只能通过密码绑定进行身份验证
服务器验证	
提示获取证书	提示输入已验证的服务器证书、名称或根证书验证 (CA)
服务器名称	设备应信任的服务器列表
无	未建立安全保障
使用代理服务器	使用代理服务器
服务器地址	代理服务器地址
服务器端口	代理服务器的服务器端口

使用代理服务器

启用代理服务器。

服务器地址	该网络使用的代理服务器地址。
服务器端口	该网络使用的代理服务器端口。

无线网络限制

您可以在此定义各种 Wifi 限制。

允许 WiFi	允许/拒绝 WiFi
允许互联网共享	允许使用热点
允许自动连接到 WiFi 感知热点	允许自动连接到 WiFi 感知热点
允许手动 WiFi 配置	允许用户连接 AppTec 未定义的 WiFi 网络
无线局域网扫描频率	确定 WLAN 扫描时间间隔。数值越大，识别 WIFI 网络的能力越强。

虚拟专用网

在此进行适当设置，以配置 VPN 连接

连接名称	指示的连接名称		
VPN 类型	每个应用程序 VPN 连接用于保护某些应用程序的流量安全。		
	虚拟专用网	始终开启	这将在登录时自动连接 VPN，并保持连接，直到用户手动断开连接。
	每个应用程序的 VPN	VPN 应用程序	定义使用此 VPN 连接的应用程序
		每个应用程序锁定	每应用程序锁定功能使选定的应用程序只能通过此 VPN 连接进行连接。 此功能取决于 Windows Defender 防火墙。
	WIP 简介	此连接的 WIP 域名	企业 ID，将此 VPN 配置文件与 Windows 信息保护 (WIP) 策略连接时需要使用该 ID

连接类型

AppTec360 VPN	
对于 "AppTec360 VPN"，需要允许应用程序侧载。请在 "安全管理"→"限制设置"→"设备功能 "中启用 "允许应用程序侧载"。	
网关配置	要配置带有黑名单的 VPN 连接，请选择带有指定 DNS 服务器的 VPN 配置。您可以在 "常规设置"→"通用网关"→"VPN 设置 "中设置 VPN 配置。

IKEv2		
服务器	VPN 服务器列表	
设备隧道	在用户登录前启用连接。	
验证方法	EAP	EAP XML
	机器证书	
加密算法		
完整性检查算法		
Diffie-Hellman 组		
密码转换算法		
认证转换算法		
完美前向保密（PFS）组		

PPTP		
服务器	VPN 服务器列表	
验证方法	EAP	EAP XML

L2TP		
服务器	VPN 服务器列表	
验证方法	EAP	EAP XML
加密算法		
完整性检查算法		
Diffie-Hellman 组		
密码转换算法		
认证转换算法		
完美前向保密（PFS）组		

自动		
服务器	VPN 服务器列表	
验证方法	EAP	EAP XML

通用 VPN 配置

每次登录时记住凭据	
使用内部 DNS 注册 IP 地址	
网络流量过滤规则	将 VPN 连接限制为已定义的规则集。
DNS 后缀搜索列表	添加到 DNS 搜索列表的 DNS 后缀，用于路由短名称。
名称解析策略表 (NRPT) 规则	名称解析策略表 (NRPT) 规则定义连接到 VPN 时 DNS 如何解析名称。
可信网络检测	用于识别受信任网络的 DNS 后缀列表。
分离式隧道	分离式隧道技术意味着流量可以通过网络堆栈决定的任何接口传输。
分割隧道路由	要添加到 VPN 接口路由表的路由列表。
代理设置	配置该网络使用的代理
代理地址	代理服务器地址为完全限定的主机名或 IP 地址。
港口	代理服务器端口。
代理自动配置 URL	URL 以自动检索代理设置。

VPN 限制

在这里，您可以定义各种 VPN 限制。

允许 VPN 设置	本指南允许/禁止用户停用和更改 VPN 设置
允许通过蜂窝网络使用 VPN	如果设备正在使用移动数据，则允许/禁止设备建立 VPN 连接
允许 VPN 通过蜂窝漫游	如果设备正在漫游，允许/禁止设备建立 VPN 连接

蓝牙

您可以在此确定是否允许/禁止使用蓝牙。

允许蓝牙	激活/禁用蓝牙

PIM 管理

Exchange Active Sync

在终端用户设备上设置 ActiveSync 账户

账户名称	电子邮件帐户名
服务器主机名	服务器地址/FQDN
域名	服务器域
电子邮件地址	电子邮件地址
用户名	用户名
用户密码	您还可以选择在此处为用户附加密码
使用 SSL	使用 SSL 连接
同步间隔	这里可以确定同步间隔 手动同步 = 用户必须下载其电子邮件并执行手动同步
邮件年龄过滤器	邮件同步前的时间量 无过滤器 = 无限制
日志级别	建立 ActiveSync 流量的日志级别
同步电子邮件	激活 = 同步电子邮件
同步联系人	激活 = 联系人已同步
同步日历	激活 = 日历已同步
同步任务	激活 = 任务同步

电子邮件

在终端用户设备上建立 POP3/IMAP4 账户。

账户说明	电子邮件帐户名
发件人姓名	显示的发件人姓名
域名	电子邮件帐户的域名
电子邮件地址	用户电子邮件地址
用户名	用户名
用户密码	您还可以选择在此处为用户附加密码
替代发件服务器证书	如果外发服务器需要其他证书，可在此处定义
传出域名	外发域名
发件服务器用户名	发件服务器用户名
发件服务器密码	发件服务器密码
电子邮件协议	POP3 或 IMAP4，可用作协议
内收邮件服务器主机名	接收邮件服务器主机名
使用 SSL 接收邮件	对接收的电子邮件使用 SSL
外发邮件服务器主机名	外发邮件服务器主机名
使用 SSL 发送邮件	使用 SSL 发送电子邮件
传出服务器验证	需要进行传出服务器验证
同步间隔	这里可以确定同步间隔 手动同步 = 用户必须下载其电子邮件并执行手动同步
邮件年龄过滤器	邮件同步前的时间量 无过滤器 = 无限制

应用程序管理

企业应用管理器

已安装的应用程序

以下是当前安装在显示设备上的应用程序列表。

必须使用的应用程序

您可以在此配置设备上必须安装的应用程序列表。

每次设备连接到 MDM 时，都会检查该列表，并安装该列表中恰好未安装在设备上的所有应用程序，无论该应用程序是否已卸载或以前从未安装过。

您可以上传 Windows 10 内部应用程序，然后将其添加到此列表中，也可以添加 Microsoft Office 配置，但需要事先在 "常规设置">"应用程序管理">"Microsoft Office "中进行配置。

系统应用程序限制

收件箱应用程序
允许警报和时钟
允许计算器
允许相机
允许联系支持
允许 Cortana
允许文件资源管理器
允许开始
Allow Groove Music
允许使用地图
允许发送信息
允许 Microsoft Edge
允许电影和电视
允许资金
允许新闻
允许使用 OneDrive
允许 OneNote
允许使用 Outlook 日历和邮件
允许人们
允许电话
允许拍照
允许使用 Powerpoint
允许设置
允许 Skype
允许运动
允许存储
允许使用录音机
允许钱包
允许天气

允许使用 Windows 反馈中心
允许 Word
允许 Xbox

设置页面
允许账户工作场所
允许高级信息
允许应用程序角
允许阻止和过滤
允许颜色配置文件
允许驾驶模式
允许电子邮件和账户
允许均衡器
允许键盘
允许导航栏
允许网络飞行模式
允许网络互联网共享
允许网络服务
允许网络 Wi-Fi
允许电脑系统蓝牙
允许为您的设备评分
允许恢复更新
允许共享
允许启动
允许时间 语言
允许时间 地区
允许 Windows 默认锁定屏幕
允许工作或学校账户

黑名单和白名单

在 "黑名单和白名单 "下，您可以选择 "白名单 "模式或 "黑名单 "模式。

白名单	只有添加到列表中的应用程序和服务才能安装到最终用户设备上。如果这些应用程序和服务已经预装在最终用户设备上，它们将被激活和设置，以便用户运行。
	所有未添加到列表中的其他应用程序都不能安装到最终用户设备上。如果这些应用程序已经预装在最终用户设备上，它们将被停用和设置，这样用户就无法运行它们。
黑名单	添加到列表中的应用程序和服务不能安装到最终用户设备上。如果这些应用程序和服务已经预装在最终用户设备上，它们将被停用并设置为用户无法运行。
	所有未添加到列表中的其他应用程序都可以安装到最终用户设备上。如果这些应用程序已经预装在最终用户设备上，它们将被激活和设置，以便用户运行。

通过 ，您可以将其他应用程序或服务添加到当前使用的列表中。

通过 ，您可以在当前非活动列表中添加其他应用程序或服务。

您可以从 "Windows 应用程序商店 "中添加应用程序，也可以直接输入 "应用程序标识符 "添加到黑名单或白名单中。

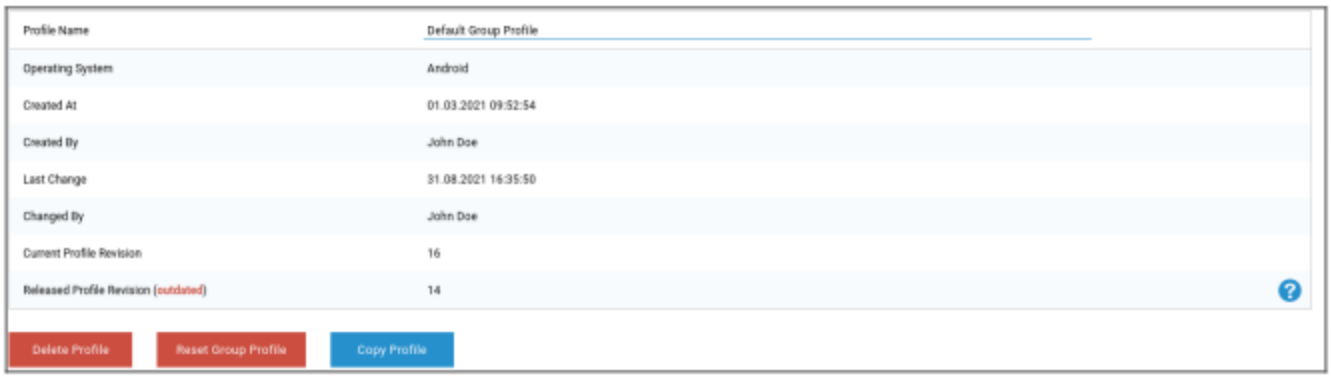
MacOS 配置

根据您选择的是配置文件还是设备，显示屏及其子点会有所不同，请仔细留意！

一般情况

组概况概览（仅适用于组级）

打开群组资料时，您将快速浏览该资料。



简介名称	个人资料名称（可在此处更改）
操作系统	配置文件适用的操作系统
创建于	创建时间
创建者	个人资料创建者
最后的变化	最后一次更改配置文件的时间
已更改	最后更改的账户
当前的简介修订	修订已保存的配置文件状态
已发布的简介修订版	已分配的配置文件修订版（"立即分配"）。如果标签文字后面显示"（已过期）"，则表示您已经保存了配置文件，但尚未分配，因此设备仍将获得旧版本。

设备概述（仅限设备级别）

设备概述

设备名称	设备名称
模型	模型
操作系统	操作系统
序列号	设备序列号
设备所有权	配置的所有权类型
设备类型	设备类型
符合要求	显示设备是否符合标准
IP 地址	设备连接服务器的 IP 地址
最后查看	设备最后一次连接的时间
最后一搏	最后一次向设备推送的时间
任务	在这里，您可以将设备移动到其他用户或组

配置修订（仅限设备级）

在这里，您将看到为设备分配的组配置文件的概览。

如果点击群组配置文件，就可以直接进入配置文件并进行设置。

使用该符号，可以将已分配的应用程序还原为群组配置文件的设置。

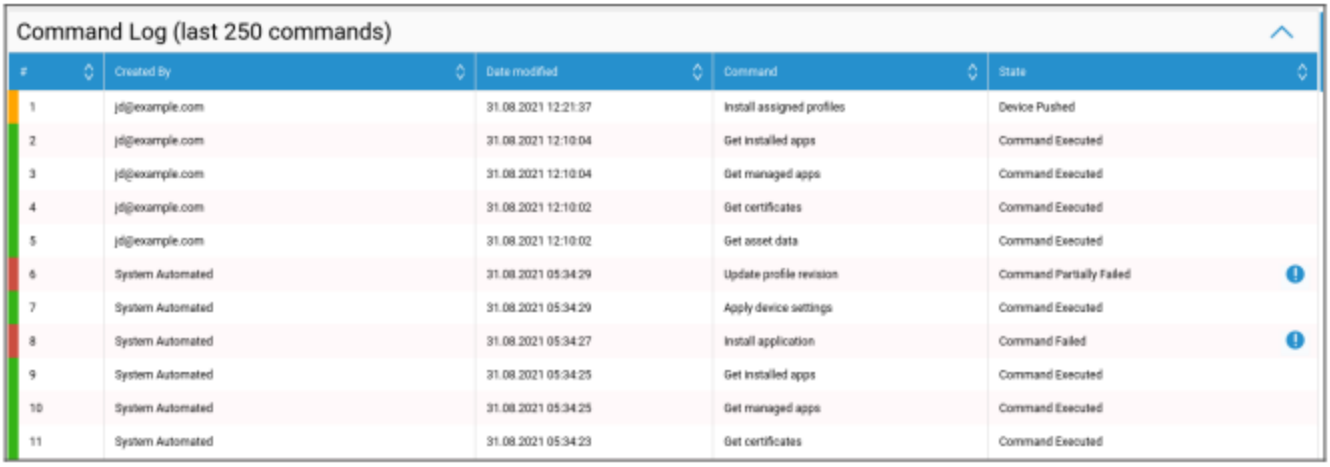
通过该符号，您可以重置设备配置文件，使其没有任何设置。

"最新版本可用 "表示组配置文件已更改并保存，但尚未分配。必须在组级别上使用 "立即分配 "来分配组配置文件，才能将更改应用到设备上。

设备日志（仅限设备级）

命令日志

在这里，您可以查看为设备发出的命令及其状态。



系统自动 "创建的命令由系统自动创建。

可能的命令状态

设备已推送	推送请求已发送至推送服务（如 APNS），以通知设备连接回 EMM 服务器。
创建命令	该命令已在系统中创建。
发送命令	设备与服务器连接后，命令被发送到设备。
命令已执行	命令已成功执行。
命令失败	命令失败。*
命令部分失败	根据设备操作系统的不同，有些命令可能会被组合在一起。 其中，该命令组的某些部分出现故障。*
命令已执行，但最终失败	命令已执行，但也可能没有执行。
命令重发	命令被用户重新推送。
弃用	命令被丢弃。例如，该命令被其他命令取代，或设备重新注册，旧命令被删除。

*如果信息后面有感叹号，您可以用光标悬停在图标上，获取更多信息。

资产管理（仅限设备级）

设备信息

型号	型号
主机名	主机名
本地主机名	本地主机名
操作系统	操作系统
操作系统版本	操作系统版本
UDID	UDID
可用/总内存	可用/总内存

无线网络

IP 地址	IP 地址
WiFi MAC	WiFi MAC

细胞

电话号码	电话号码
漫游状态	漫游状态
漫游（语音/数据）	漫游（语音/数据）
IP 地址	IP 地址
运营商/承运商	运营商/承运商
SIM 卡运营商网络	运营商网络
载体版本	载体版本
ICCID	ICCID
目前的 MCC/MNC	目前的 MCC/MNC
SIM MCC/MNC	SIM MCC/MNC

蓝牙

蓝牙 MAC	蓝牙 MAC

更新管理（仅限设备级）

更新信息

此选项卡显示有关设备上系统更新设置的信息。

已启用自动检查功能	如果系统自动检查更新。
已启用应用程序自动更新	如果系统会自动安装应用程序更新。
启用自动操作系统更新	如果系统将自动安装操作系统更新。
已启用自动安全更新	如果系统将自动安装安全更新。
启用应用程序更新后台下载	如果系统会在后台下载应用更新。
目录 URL	客户端正在使用的软件更新目录的 URL。
是默认目录	如果 "是"，则目录为默认目录。
进行定期检查	如果 "是"，则开始新的扫描。
上次扫描日期	上次软件更新扫描的日期。
上次扫描结果	上次软件更新扫描的结果代码。

安全管理

防盗

擦拭和锁定

全面擦拭	发送命令重置设备
企业擦拭	从设备上删除 MDM 并删除所有 MDM 数据（如账户、应用程序）
锁定屏幕	让设备返回锁定屏幕

安全配置

密码

允许停用代码	决定是否强制用户设置 PIN 码。只需设置此值（而不设置其他值），用户就会被强制输入密码，但不会要求输入密码的长度或质量。
允许简单值	允许用户使用相同、递增和递减的数字字符串（如 1234、1111）
要求字母数字值	密码必须至少包含一个字母
最小密码长度	最小密码长度
最少复合字符数	密码中字母数字符号的最少数量
密码最长有效期	必须更改密码的天数
最大自动锁定	锁定设备的最长时间
设备锁定的最长宽限期	设备在解锁时不提示输入密码的锁定时间
最大密码有效期（1-730 天，或无）	必须更改密码的天数
密码历史记录（1-50 个密码或无密码）	重复使用前的唯一密码数

证书

PKCS#1	
说明	输入证书描述
证书	上传 pkcs1 文件

PKCS#12	
说明	输入证书描述
证书	上传 pkcs12 文件

限制设置

设备功能

允许相机	允许使用摄像机
允许游戏中心	如果为假，Game Center 将被禁用，其图标也会从主屏幕上移除。
允许多人游戏	为假时，禁止多人游戏。
允许添加游戏中心好友	为假时，禁止添加好友到 Game Center。
允许使用 iCloud 照片库	如果设置为 false，则禁用 iCloud 照片库。任何未从 iCloud 照片库完全下载到设备的照片都将从本地存储中删除。
允许触摸 ID	如果为假，则会阻止 Touch ID 解锁设备。

iCloud

在配对 iCloud 时阻止某些功能

允许文件同步	允许文件同步
允许 iCloud 钥匙串同步	允许 iCloud 钥匙串同步
允许 iCloud 笔记	为假时，禁止 MacOS iCloud Notes 服务
允许 iCloud BTMM	为假时，禁止 MacOS Back to My Mac iCloud 服务。
允许 iCloud FMM	为假时，禁止 MacOS 查找我的 Mac iCloud 服务。
允许使用 iCloud 书签	为假时，禁止 MacOS iCloud 书签同步。
允许使用 iCloud 邮件	为假时，禁止 MacOS Mail iCloud 服务。
允许使用 iCloud 日历	为假时，禁止 MacOS 云 iCloud 服务。
允许 iCloud 提醒	为假时，禁止使用 iCloud 提醒服务。
允许使用 iCloud 地址簿	为假时，禁止 MacOS iCloud 地址簿服务。

媒体管理

注销时弹出	注销时弹出所有可移动媒体
允许网络	允许网络媒体访问
允许内部磁盘	允许访问内部磁盘。
要求验证	使用该媒体时需要进行身份验证
只读	用户只能从介质中读取数据
允许外置硬盘	允许访问外部磁盘。
要求验证	使用该媒体时需要进行身份验证
只读	用户只能从介质中读取数据
允许使用磁盘镜像	允许访问图像。
要求验证	使用该媒体时需要进行身份验证
只读	用户只能从介质中读取数据
允许使用 DVD-RAM	允许访问 DVD-RAM 磁盘。
要求验证	使用该媒体时需要进行身份验证
只读	用户只能从介质中读取数据
允许使用 DVD	允许访问 DVD 磁盘。
要求验证	使用该媒体时需要进行身份验证
允许使用光盘	允许访问 CD 磁盘。
要求验证	使用该媒体时需要进行身份验证

连接管理

无线网络

您可以在此添加和配置 Wi-Fi 连接

服务集标识符（SSID）	将建立连接的网络的 SSID
自动加入	启用网络自动连接
隐藏的网络	启用，以防无线接入点不广播 SSID
代理设置	为每个接入点配置代理
无	不要使用代理服务器
手册	建立手动代理
代理服务器 URL	访问代理设置的地址
港口	为代理建立端口
认证	代理验证的用户名
密码	代理验证密码
自动	自动建立代理
代理服务器 URL	代理设置文件的 URL
安全类型	为 AP 建立安全类型
WEP	
密码	AP 密码
WPA/WPA2	
密码	AP 密码
WEP 企业 - WPA / WPA2 Enterprise / 任何企业	见表 错误：下面未找到参考源
无	不建立安全保障
禁用 MAC 地址随机化	在与该 Wi-Fi 网络关联时，禁用该网络的 MAC 地址随机化。这也会在 "设置 "中显示隐私警告，表明该网络的隐私保护功能已降低。

企业 Wi-Fi 配置

注意：只有当 "安全类型 "设置为企业类型时才可用。

协议	目标网络支持的身份验证协议
TLS	启用/禁用
TTLS	启用/禁用
内部认证	应使用的身份验证协议：PAP、CHAP、MSCHAP、MSCHAPv2
LEAP	启用/禁用
PEAP	启用/禁用
EAP-FAST	启用/禁用
EAP-SIM	启用/禁用
使用 PAC	使用 PAC（受保护的访问控制）
PAC	配置供应 PAC
匿名提供 PAC	匿名提供 PAC
认证	
用户名	认证用户名
不要使用 每连接 密码	不要使用每次连接密码
密码	使用的密码
身份证明	上传/选择验证证书
外部特征	可以从外部看到的身份
信任	
可信证书 1	上传第一个可信证书
可信证书 2	上传第二个可信证书
可信证书 3	上传第三个可信证书
可信服务器 证书名称	预期服务器证书的名称 (以逗号分隔的列表)

虚拟专用网

根据所选连接类型的不同，可能会显示不同的字段。

连接名称	VPN 配置文件名称
VPN 类型	
虚拟专用网	所有设备网络流量都将通过 VPN 连接传输。
连接类型	建立 VPN 连接类型
IPsec（思科）	思科的 IPsec 协议
L2TP	L2TP 协议
自定义 SSL	通过自定义 SSL 连接
IKEv2	IKEv2 协议
代理设置	为 VPN 连接配置代理服务器
无	不设立代理
手册	手动建立代理
代理服务器 URL	访问代理设置的地址
港口	为代理建立端口
认证	用于在代理处进行身份验证的用户名
密码	代理认证密码
自动	自动建立代理
代理服务器 URL	访问代理设置的 URL

HTTP 代理服务器

代理类型	
手册	手动建立代理
代理服务器 URL	访问代理设置的地址
港口	建立代理端口
认证	用于在代理处进行身份验证的用户名
密码	代理认证密码
自动	自动建立代理
代理 PAC URL	代理 PAC URL
如果 PAC 无法连接，允许直接连接	如果 PAC 无法访问，允许直接连接（不使用 VPN
允许绕过代理访问专用网络	允许绕过代理访问专用内部网络

AirPrint

IP 地址	打印机 IP 地址
资源路径	通往 AirPrint 设备的明确路径

AirPlay

设备名称	设备名称
密码	配对密码
白名单	定义设备列表，设备可专门与之配对

PIM 管理

Exchange Active Sync

账户名称	账户名称。
电子邮件地址	账户地址（如 max@company.com）
服务器主机名	内部主机名
登录名	域 "和 "登录名 "必须为空，设备才会提示用户。
域名	域 "和 "登录名 "必须为空，设备才会提示用户。 如果启用了 ACL 网关配置，且域字段不是空的，AppTec360 通用网关将使用以下名称 "Domain\Login Name "验证设备
密码	账户密码（例如 secretUserPassword）
邮件同步的过去	要同步的过去邮件天数
使用 SSL	为内部 Exchange 主机使用 SSL
高级选项	显示高级选项
服务器端口	内部端口
服务器路径	内部路径
外部主机名	外部主机
外部端口	外部端口
外部路径	外部路径
对外使用 SSL 交换主机	为外部 Exchange 主机使用 SSL

电子邮件

在终端用户设备上设置 POP3 / IMAP 账户

账户说明	姓名 电子邮件账户
账户类型	
IMAP	
路径前缀	特殊文件夹的路径前缀
持久性有机污染物	
用户显示名称	用户显示名称
电子邮件地址	用户电子邮件地址

来信	传入服务器设置
邮件服务器地址	邮件服务器地址
邮件服务器端口	邮件服务器端口
用户名	各自的用户名
认证类型	认证类型
无	无验证类型
密码（仅限设备级）	密码提示
MDM 挑战-回应	
NTLM	NTLM 身份验证
HTTP MD5 摘要	
使用 SSL	必要时使用 SSL

外寄邮件	外发服务器设置
邮件服务器地址	邮件服务器地址
邮件服务器端口	邮件服务器端口
用户名	用户名
认证类型	
无	无验证方法
密码（仅限设备级）	密码提示
MDM 挑战-回应	
NTLM	NTLM 身份验证
HTTP MD5 摘要	
使用 SSL	必要时使用 SSL
传出密码与传入密码相同	传出密码与传入密码相同
仅用于邮件	如果所有外发邮件都通过邮件应用程序发送，则激活

CalDav

配置 CalDav 帐户的设置和分配

账户说明	账户显示名称
主机名	主机名和/或 IP 地址
港口	CalDav 账户的端口
主要网址	账户的主要 URL
用户名	各自的 CalDav 用户名
密码（仅限设备级）	各自的 CalDav 密码
使用 SSL	必要时使用 SSL

卡达维

配置 CardDav 账户的设置和分配

账户说明	账户显示名称
主机名	主机名和/或 IP 地址
港口	CardDav 账户的端口
主要网址	账户的主要 URL
用户名	相应的 CardDav 用户名
密码（仅限设备级）	各自的 CardDav 密码
使用 SSL	必要时使用 SSL

LDAP

在此区域，设置 LDAP 连接，以便在最终用户设备和 Active Directory 之间进行动态证书交换。

请注意，所选用户需要相应的读取权限。

账户说明	账户说明
账户用户名	访问 LDAP 的用户
账户密码	LDAP 访问密码
账户主机名	LDAP 服务器主机名/IP 地址
使用 SSL	必要时使用 SSL

在第二部分，您可以定义用于在 LDAP 注册表中搜索的单个筛选器。

说明	范围	搜索基地
过滤器说明	LDAP 注册表中的搜索级别	定义单个过滤器

仪表板和报告

仪表板设置

在这里，您可以查看现有的仪表盘、编辑仪表盘或创建新仪表盘。每个仪表盘都有自己的数据集显示和图表配置。

仪表板设置控制

公众	将仪表板设置为公开，这样其他用户就可以看到仪表板。当然，用户必须能够登录并查看仪表板。如果未激活 "公开"，则只有创建者可以查看。
默认值	将仪表板设置为默认设置，以便下次访问仪表板视图时自动打开。
	显示仪表盘及其图表
	删除仪表板
	编辑仪表板名称和设置
	复制仪表板
	添加全新的仪表板

仪表板视图

这将显示所选仪表板的数据和图表，还可以更改这些数据和图表。

仪表板控制

	您可以定义在仪表板中显示哪些数据、要显示的数据量以及显示这些数据的大小
	返回控制面板概览
	将当前打开的仪表板重置为默认设置
	保存您对当前打开的仪表板所做的所有更改（例如显示哪些数据）。
	将图表类型更改为柱状图
	将图表类型更改为饼图
	将图表类型更改为圆环图
	将图表类型更改为极区图
	更改排序顺序

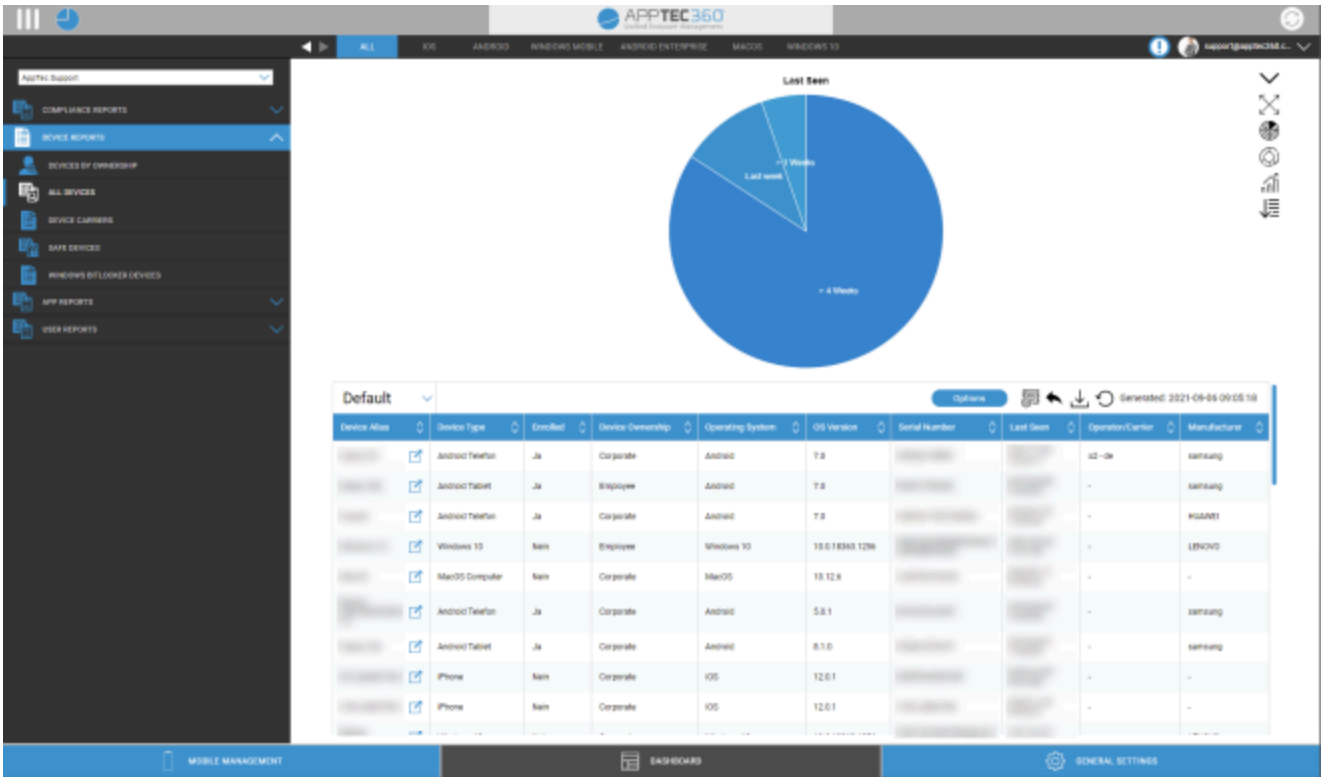
扩展报告

扩展报告 "提供有关设备和用户信息的详细概览和图表。

有一些默认报告，但所有报告都可以手动更改，添加或删除要显示的数据。

请注意，您只能手动更改显示的数据。所选报告类别定义了所依据的数据。例如，在 "设备报告 "的 "所有设备 iOS "中，您永远无法在 iOS 报告中看到 Android 设备。

在左上角，您可以将报告数据限制为某个组（及其所有子组）。默认情况下，该组设置为根节点，因此会将所有设备和用户都考虑在内。



扩展报告控制

在每个概览中，您可以使用以下功能以任何方式更改报告：

	隐藏图表（如果已显示图表）
	显示图表（如果图表隐藏）
	展开图表（如果图表已折叠）
	折叠图表（如果图表已展开）
	将图表类型更改为柱状图
	将图表类型更改为饼图
	将图表类型更改为圆环图
	将图表类型更改为极区图
	更改排序顺序
	修改显示概览的以下部分： • 添加/删除栏 • 指定列的显示顺序 • 显示/隐藏表格上方的图表 • 选择用于图表的列 • 过滤表格数据
	打开设置管理器，保存和加载不同的报告
	将当前打开的报告重置为默认值
	将当前报告导出为 .csv 文件
	重新生成数据并重新加载当前报告

下几页将列出所有默认报告。

合规报告

扎根设备

已root/越狱的设备概览。

本报告的默认栏：

设备别名
设备所有者
电子邮件
操作系统
电话号码
最后查看
制造商

漫游设备

所有正在漫游的设备概览

本报告的默认栏：

设备别名
设备所有者
电子邮件
设备类型
操作系统
电话号码
最后查看

支持漫游的设备

已激活漫游但不一定正在漫游的所有设备概览。

本报告的默认栏：

设备别名
设备所有者
电子邮件
设备类型
操作系统
电话号码
最后查看

受监控设备

在受监控模式下受监控的所有设备概览（仅限 iOS）

本报告的默认栏：

设备别名
设备所有者
电子邮件
设备类型
最后查看

非活动设备

过去 7 天内未连接服务器的所有设备概览

本报告的默认栏：

设备别名
设备所有者
电子邮件
设备类型
操作系统
最后查看

设备报告

按所有权划分的设备

在这里，你可以看到目前有多少设备被部署为企业（公司设备）和员工（私人设备）设备。

本报告的默认栏：

设备别名
设备所有者
设备类型
设备所有权
操作系统

所有设备

在这里，您可以看到所有设备的概览和最重要的信息。

本报告的默认栏：

设备别名
设备类型
已注册
设备所有权
操作系统
操作系统版本
序列号
最后查看
运营商/承运商
制造商

设备载体

在这里，您可以看到有关运营商（手机提供商）的概述。

本报告的默认栏：

设备别名
设备所有者
电子邮件
操作系统
操作系统版本
运营商/承运商

安全设备

在这里，您可以看到哪些设备使用了 SAFE 版本。

由于概述和/或 SAFE 仅适用于三星设备，因此在这一点下不会看到常用的选项卡。

本报告的默认栏：

设备别名
设备所有者
电子邮件
设备类型
最后查看
安全版本

Windows BitLocker 设备

在此，您可以看到使用 BitLocker 的 Windows 设备概览。

本报告的默认栏：

设备别名
设备所有者
电子邮件
BitLocker 状态

应用程序报告

在这里，你可以获得有关应用程序的各种概述。在所有这些报告中，您都可以点击某个条目，进一步查看设备上安装的版本和安装频率。在此视图中，您可以再次点击特定版本，查看哪些设备安装了该特定版本。

注意：系统从设备获取最新信息可能需要一些时间。此外，报告也不是每分钟都更新。如果您刚分配了一个新的应用程序或版本，可能需要耐心等待才能看到当前状态。手动重新加载报告将强制报告显示最新数据。

已安装的应用程序

在这里，您可以概览所有已安装的应用程序。

本报告的默认栏：

名称	相关应用程序和/或服务的名称
标识符	明确的应用程序/服务 ID
总计数	该应用程序/服务在最终用户设备上的安装频率

安装最多的应用程序

在这里，您可以概览安装次数最多的应用程序。

本报告的默认栏：

名称	相关应用程序和/或服务的名称
标识符	明确的应用程序/服务 ID
总计数	该应用程序/服务在最终用户设备上的安装频率

必须使用的应用程序

在这里，您可以了解强制性（强制要求）应用程序的概况。

本报告的默认栏：

名称	相关应用程序和/或服务的名称
标识符	明确的应用程序/服务 ID
应用程序源	涉及哪个 AppStore： • Google PlayStore（安卓） • iTunes AppStore（iOS）
操作系统	操作系统

黑名单应用程序

在此，您可以概览所有已定义的黑名单应用程序。

本报告的默认栏：

名称	相关应用程序和/或服务的名称
标识符	明确的应用程序/服务 ID
应用程序源	涉及哪个 AppStore： • Google PlayStore（安卓） • iTunes AppStore（iOS）
操作系统	操作系统

用户报告

关税

在这里，您可以概览用户的电话资费和 SIM 卡。

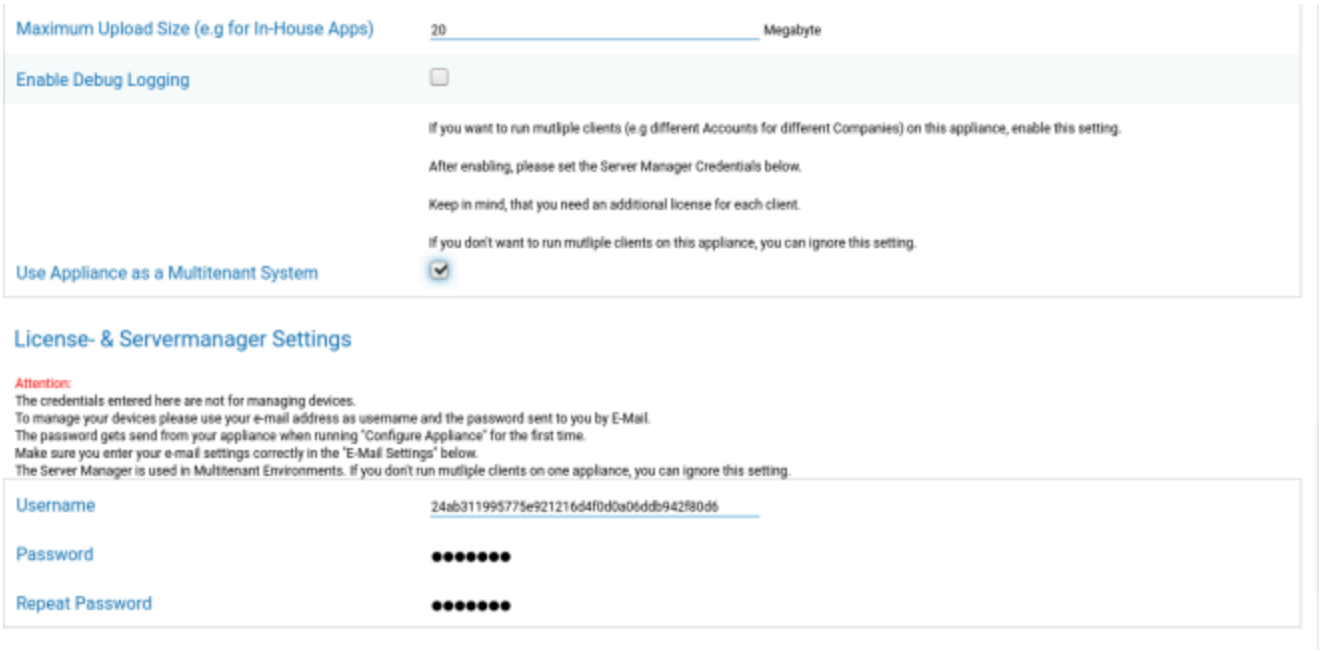
本报告的默认栏：

电子邮件
名称
电话号码
载体
电费
选择权
价格
合同取消
合同开始
时间
移动数据
数据卷
multiSIM
类型
simCardSerial1
simCardSerial2
simCardSerial3
引脚1
引脚2
puk1
puk2
备注

多租户管理

AppTec360 EMM 能够托管多个独立租户，每个租户都有自己的用户和群组、权限和全局设置。

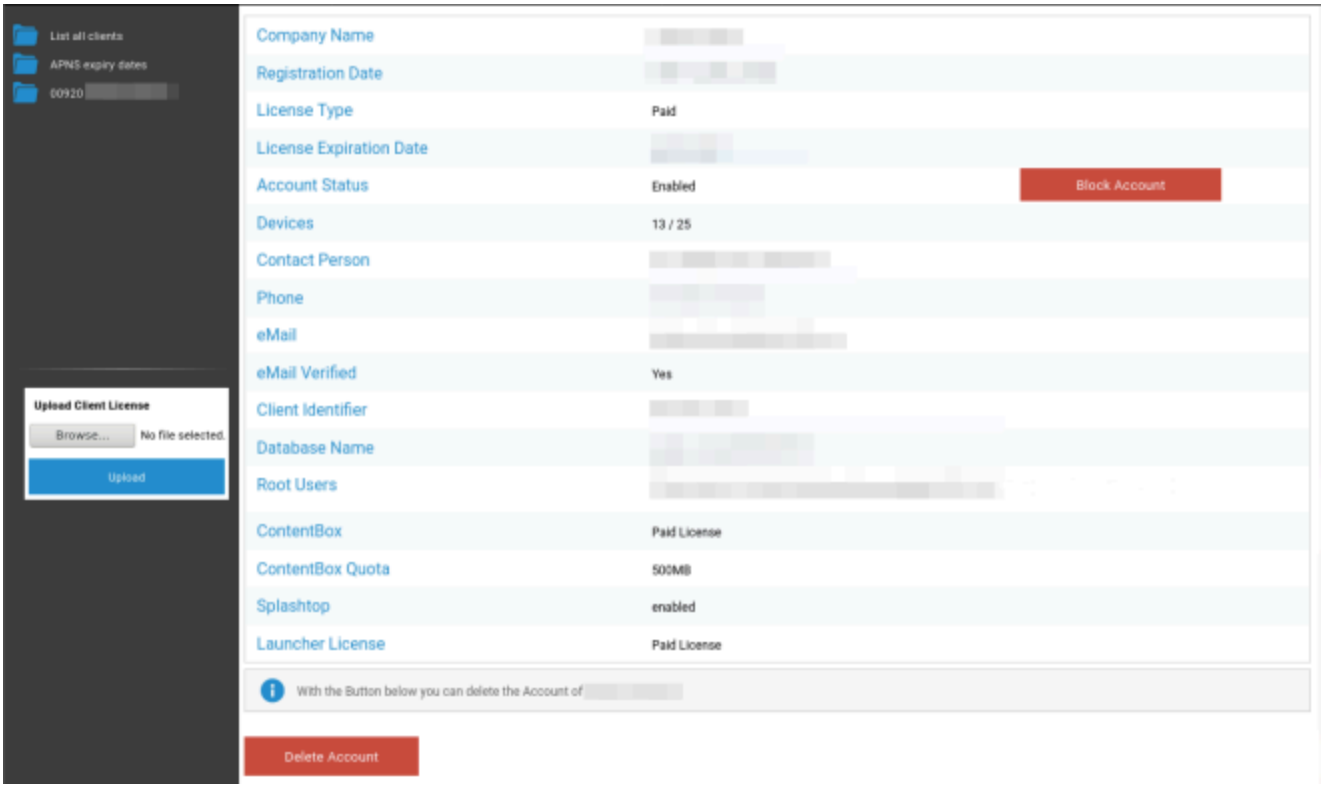
要启用多租户功能，必须在设备配置界面的 "第三步 - 服务器设置 "中启用。



在新菜单中为服务器管理器设置用户名和密码。保存设置并运行 "第五步 - 许可协议 "中的 "配置设备 "以应用设置。

配置完成后，您就可以通过正常的移动管理界面使用设置的凭据登录了。

登录后，您可以看到以下视图。



左侧是所有租户（本例中只有一个租户的 ID 是 920），右侧是该客户的相关信息。您还可以选择阻止访问该账户以及删除该客户（注意：这将删除与该客户有关的所有数据）。

您可以在左侧上传新的客户许可证，既可以是现有客户的许可证更新，也可以是自动创建新客户的新许可证。创建新客户后，包含登录密码的电子邮件将自动发送到许可证的电子邮件地址。

如需获取新的或更新的客户端许可证（如需要更多设备许可证），请联系您的销售代表。

其他意见

列出所有客户

显示系统中所有客户的概况。

客户 ID	客户 ID
标识符	客户标识符
数据库	数据库
公司名称	公司名称
电子邮件	联系人 电子邮件
已验证	联系人的电子邮件是否经过验证
国家	国家
设备	注册设备数量
注册日期	许可证转让的时间点
最后登录	最后一次登录管理员账户
许可证	许可证类型显示（免费|付费）
CB 许可	ContentBox 许可证类型（免费/付费）
现状	当前 AppTec-Client 状态
已过期	如果许可证已过期，则显示
iOS	iOS 设备数量
安卓	安卓设备数量
Windows 移动	Windows 移动设备数量
MacOS	MacOS 设备数量
Windows 10	Windows 10 设备数量
安卓企业	安卓企业设备数量
IOS BYOD（用户注册）	IOS BYOD（用户注册）设备数量
物联网	物联网设备数量

APNS 有效期

显示所有客户端的所有 APNS 证书过期日期概览。

客户 ID	客户 ID
公司名称	公司名称
过期日期	Apple APNS 证书的到期日期
信息	过期信息

联系方式

其他问题？请联系我们：

一般技术问题

support@apptec360.com

+41 61 511 3210

有关安装虚拟设备的问题

consulting@apptec360.com

+41 61 511 3214

免责声明