□□□□

- □□□□
- □□□□
- SIM □□□
- □□

设备概览
从仪表板 → 设备 中点击设备行即可打开设备。页面标题会显示设备 型号 （在可用时）和内部 ID。

历史数据与当前注册
当设备有多个注册时， Cerberus Enterprise 可以显示只读的历史记录。在这种情况下，页面会显示 历史数据
横幅以及一个返回当前注册数据的按钮。

顶部字段
顶部区域汇总设备身份、分配和管理状态。某些字段特定于平台，仅对 Android 或 Apple 设备显示。

ID和型号 ：只读标识符。
用户 ：显示当前分配的用户（如果有）。从用户菜单中，您可以 打开用户 或更改用户
，或在未设置用户时分配用户。
管理模式 和所有权 ：在界面中通过工具提示显示。
状态 ：当前设备状态（包含图标和工具提示详细信息）。处于丢失模式的设备在 Android 和 Apple
上都会显示 丢失 ，页面顶部的横幅会说明下一步该怎么做。
ADE 配置描述文件 （仅限 Apple
）：显示已分配的自动设备注册配置描述文件（如果有），并允许您打开或更改它。
政策 ：显示已分配的政策，并允许您打开或更改它，或在未设置时分配一个政策。
政策合规性状态 （已分配政策时）：指示设备是否合规。
政策版本 （已分配政策时）：指示设备是否已应用最新的政策版本。
Cerberus Enterprise 应用 （仅限 iPhone 和 iPad）： Cerberus 在设备上安装的 Cerberus Enterprise 应用的状态。 不可用 （iOS 或 iPadOS 低于 18.4
、公司设备没有序列号，或个人设备没有 Managed Apple Account）； 个人设备上尚不可用 ；
正在等待设备信息 ；正在等待 Managed Apple Account 的用户许可证 （个人设备， Apple
正在确认许可证）； 未安装 （应用不在您的 Apple Business 资料库中，或未设置 Apps and Books
，并提供指向 账户设置 的链接）； 已安装 · Apps and Books 需要注意
（令牌已过期或应用已离开您的资料库：应用会保持安装状态）； 配置不可用 ；正在安装 …
（如果设备在 30
分钟内未发送状态报告，工具提示会建议检查设备是否在线并重新启动它，这通常会重新开始安装）
；正在等待用户批准 ；用户已拒绝 和 安装失败 （两者都会显示 重试 ，它会再次询问设备）；
已安装 · 正在等待应用启动 （应用尚未打开）； 已安装 · 配置未被接受
；并且，在应用注册后，还会显示其版本、最后联系时间以及通知是否已开启。
注册时间 和上次状态报告 ：注册和上次报告状态的时间戳。
已取消注册 ：当设备已取消注册时显示。

某些数据和面板仅在设备政策中启用了相应类别时才可用。有关更多信息，请阅读 状态报告 和

位置和地理围栏 页面。

面板
设备页面由可展开的部分组成。根据平台和状态，您可能会看到以下一个或多个面板：

位置地图 ：一个带有选项卡的面板，包含当前设备的 位置 历史记录，在 Android 设备、 iPhone 和
iPad 上还包含用于地理围栏转换的 地理围栏 选项卡。
SIM 卡管理 ：设备 EID 以及已安装的 SIM 卡和 eSIM。在 Android 上还包括 eSIM
命令及其历史记录；在公司所有的 iPhone 和蜂窝网络 iPad 上还包括数据漫游、个人热点和
刷新蜂窝套餐 。请参阅专门的 SIM 卡管理 页面。
命令 ：向设备发送命令并查看命令历史记录（特定于平台）。
安全态势 ：设备的安全状态及其风险。在 Android 上还包括 Play Integrity
判定结果。在设备报告之前，会显示 未指定 ，或在尚未发送任何安全数据的 Android 设备上显示
尚未报告 。
设备不合规的原因 ：仅在设备不合规时显示，并带有红色警告图标；打开后可查看原因。在
Android 上，它会列出不符合要求的政策设置；在 Apple
上，它还会说明是否有合规性规则阻止了设备。
设备状态 （仅限 Apple）：设备报告的 OS 版本、软件更新进度、密码、 FileVault
、电池和账户，以及可用于该设备的 OS 更新。请参阅 命令 页面。
应用 （Android）：已安装的应用及其反馈和错误报告。
应用 （仅限 Apple
）：由政策安装的应用、通过命令安装的应用以及用户安装的应用，包括其安装状态、错误和操作（
重试、移除）。在 Mac 上，它还会列出由政策安装的软件包，包括其状态和 重新安装
；作为受管应用安装的软件包带有 受管
标签，备注会说明软件包何时以非受管方式安装及其原因，或何时在下载后一小时仍未找到其应用。
在 iPhone 和 iPad 上， Cerberus Enterprise 应用带有 由 Cerberus 安装 标签；它不会列在 政策
筛选条件下。设备未接受其受管配置的应用带有 配置未被接受 标签。在个人 iPhone 和 iPad
（用户注册）上，有一行显示其用户许可证供 App Store 应用使用的 Managed Apple Account ，等待许可证的应用会显示 正在等待用户许可证 或用户许可证失败
，用户取消了安装提示的应用会显示 正在等待用户批准安装 ，而 再次请求 会再次向 Apple
请求许可证或再次显示提示。请参阅 命令 页面。
描述文件、证书和安全 （仅限 Apple）：设备报告的配置描述文件、证书和安全状态。
清单变更 （仅限 Apple
）：设备上安装、移除或更新的应用、描述文件和证书的时间线，可搜索并按类型和变更进行筛选。
请参阅 命令 页面。

共享 iPad 用户 和 Mac 用户 （仅限 Apple）：共享 iPad 的用户和 Mac 的用户。请参阅 命令
页面。
状态报告 ：设备报告的额外数据，以类别和值的树状结构显示。

- [redacted]

[redacted]

[redacted]

- [redacted]
- [redacted] Android iPhone iPad [redacted] iPhone iPad [redacted]

[redacted] [redacted]

[redacted]

[redacted]

- [redacted]
- [redacted] / [redacted] Android[redacted]
- [redacted] Android [redacted]
- [redacted]

位置地图

本页面介绍 设备概览 中可用的特定设备位置工具。该面板包含用于查看位置历史的 位置 标签页，以及在 Android 设备、 iPhone 和 iPad 上用于查看地理围栏转换的 地理围栏 标签页。

先决条件
在 Android
上，仅当设备政策中启用了位置报告时，才会显示设备位置数据。要启用该功能，请打开政策并开启

位置和地理围栏 → 报告位置 。有关更多详细信息，请参阅 位置和地理围栏 。

在 iPhone 和 iPad 上，位置来自 Cerberus Enterprise
应用（在用户允许后），或来自设备处于丢失模式时的 定位设备 命令。 Mac 和其他 Apple
设备不会报告其位置。

在未完全受管理的设备上，位置数据可能仍取决于 Cerberus Enterprise
应用是否拥有所需的位置权限，以及设备是否启用了位置服务。

在个人设备（用户注册）上，仅当 Apple 政策开启了 个人设备上的位置和地理围栏 ，并且用户允许 Cerberus Enterprise
应用使用位置时，位置和地理围栏才可用。否则，其设备页面不会显示位置操作或实时跟踪。丢失模式
在个人设备上始终不可用。

有关可从仪表板使用的全局多设备地图，请参阅 仪表板位置地图 。

加载和无数据状态
位置数据加载时，面板会在地图上显示加载覆盖层。
如果设备没有可用的位置数据，面板会显示一条消息，内容为 无可用位置数据 。在 Android
上，如果位置报告已关闭，它还会提醒您在分配的政策中启用位置报告。在 Apple
上，它会说明位置来自何处，或此类型的设备不会报告位置。
如果日期筛选条件处于活动状态且没有匹配的样本，面板会显示 所选日期范围内无可用数据 。

位置标签页
打开 位置
标签页，查看单台设备的历史记录。可用的筛选条件包括最后已知位置、最近历史范围、自定义日期范围和实时跟踪。

最后 ：显示最后已知位置。
今天 、最近 7 天 和最近 30 天 ：显示所选时间段内记录的位置。
搜索 ：让您选择自定义日期范围。
实时 ：启动或停止当前设备的实时跟踪。

位置保留 90 天
：更早的位置每晚自动删除。每台已注册设备的最新位置始终保留，因此即使设备长时间未报告，它也
会保留在地图上。对于已移除的设备和过去的注册，超过 90 天的位置会全部删除。因此， 搜索
日期范围的开始时间不能早于 90 天前。

标记详情
点击位置标记时，会打开一个信息窗口，其中包含：

位置记录的时间戳。
报告的 准确度 （以米为单位）。
报告的 速度 ，前提是设备提供该信息。
报告的 航向 或方位，前提是设备提供该信息。

准确度圆圈
打开信息窗口后，标记周围会显示一个准确度圆圈。圆圈半径与报告的准确度（以米为单位）相对应。关闭信
息窗口后，圆圈会隐藏。

实时跟踪
在设备历史记录视图中，选择 实时 筛选条件会针对该特定设备启动实时跟踪请求。 Cerberus Enterprise 会在启动请求前请求确认。

实时跟踪的最长持续时间为 15 分钟 。

- Android iPhone iPad
- **iPhone iPad** Cerberus Enterprise iOS
  2

Android iPhone iPad

- **7** **30**
- **90**
  90

iPhone iPad
Cerberus Enterprise
App

Cerberus Enterprise

SIM 卡管理
设备页面提供了一个 SIM 卡管理 面板。在 Android 设备上，它管理设备上安装的 SIM 卡和 eSIM
配置文件，添加或移除 eSIM 配置文件，并显示发送到设备的 eSIM 命令历史记录。在公司所有的 iPhone
和蜂窝版 iPad 上，它会显示设备报告的 SIM 卡和 eSIM 套餐，并让设备下载运营商准备好的 eSIM
套餐：请参阅下方的 iPhone 和 iPad。

当设备政策中启用了 网络信息 报告时，完全托管设备会报告 SIM 信息（此选项由 Cerberus

Enterprise 始终启用）。请参阅 状态报告 页面。

设备 EID
EID（eUICC 标识符）用于标识设备的 eSIM 硬件。运营商使用它将 eSIM 配置文件绑定到设备，因此获取 EID 通常是 eSIM 配置工作流的第一步。

公司所有设备 （Android 13 及更高版本）： EID 会随设备状态自动报告，无需用户交互。
个人所有设备 （Android 13 及更高版本）：使用 请求 EID
按钮。用户会在设备上看到一条通知，请求共享 EID
，并可批准或拒绝该请求。仅在用户批准后才会显示 EID
。请求处于待处理状态时，该按钮保持禁用。

发送 EID 请求前会先显示确认对话框，因为用户会在设备上看到通知。

已安装的 SIM 卡
已安装的 SIM 卡 表格列出当前已知的设备 SIM 卡，包括实体 SIM 卡和 eSIM
配置文件。在个人所有设备上，即使设备未报告 SIM 信息，通过 添加 eSIM命令安装的 eSIM
配置文件也会显示。

运营商 ：与 SIM 卡关联的运营商名称（当报告时）。
电话号码 ：与 SIM 卡关联的电话号码（当报告时）。
ICCID：SIM 卡的集成电路卡标识符。
激活状态 ：eSIM 是否已激活。仅在 Android 15 及更高版本的 eSIM 上报告。
配置模式 ：eSIM 是由管理员配置还是由用户配置。仅在 Android 15 及更高版本的 eSIM 上报告。 SIM 卡类型 ：显示设备是否将该条目报告为 eSIM。

存在进行中或已执行（未失败）的移除命令的 eSIM 会显示临时的 正在移除
激活状态。当设备报告更新后的 SIM
卡列表时，该条目会从列表中消失。移除正在进行期间，移除按钮不可用，以避免重复发送同一命令。

移除 eSIM
使用已安装 eSIM 旁边的移除按钮，从设备中移除其配置文件。发送命令前，确认对话框会要求您确认要移除的
eSIM 的 ICCID。移除 eSIM 在 Android 15 及更高版本上受支持。

添加 eSIM
添加 eSIM部分会在设备上安装新的 eSIM 配置文件（在 Android 15 及更高版本上受支持）。它需要：

有效期 ：如果命令无法立即执行，其有效期有多长。
激活码 ： eSIM 配置文件的激活码，由运营商提供。您可以输入完整激活码，或仅输入 SM-DP+
地址，让设备发现运营商已链接到其 EID 的配置文件。
激活状态 ：eSIM 配置文件应在下载后自动激活，还是保持未激活状态以便用户手动激活。

命令历史记录
在添加 eSIM 部分下方，面板显示发送到设备的 eSIM 命令历史记录： 添加 eSIM、移除 eSIM和请求 EID
。该表格可排序并支持分页。某些行可以展开，以查看命令参数（例如激活码或 ICCID
）和执行状态，包括操作在设备上失败时的 eSIM 错误详情。

创建日期
命令
有效期
状态
错误 ：当命令执行报告 eSIM 错误状态时，显示该状态（例如 用户拒绝 、激活码无效 或找不到 ICCID
）。
执行日期

抹掉和取消注册时抹掉 eSIM
当您从命令面板抹掉设备时， 抹掉 eSIM标志控制是否在抹掉时移除 eSIM
配置文件。在具有工作资料的个人所有设备上，此标志默认启用（受管 eSIM 会被移除，个人所有的 eSIM
不受影响）。 取消注册设备 确认对话框中提供相同的标志。

iPhone 和 iPad

该面板仅在公司所有且不是用户注册的设备上，为 iPhone 和报告了蜂窝数据的 iPad（仅 Wi-Fi 的 iPad 没有）显示。设备信息会请求设备的蜂窝信息：注册时、每天、使用 刷新设备信息 时、其所有权变为公司所有时，以及 刷新蜂窝套餐 后几分钟。

- 设备 **EID**：随 SIM 卡报告的 EID，并有一个按钮可将其复制给运营商。如果设备未报告 EID，用户可在设置 > 通用 > 关于本机中找到它。
- 已报告 、数据漫游 、个人热点 和 调制解调器固件：设备是否已响应及其报告的状态。数据漫游和个人热点可通过命令面板中的 设备设置 进行更改，该面板也会显示当前状态。
- **SIM** 卡：每个 SIM 卡或 eSIM 套餐一行（双 SIM 设备有两行），包含设备报告的卡槽、其标签和类型（当设备随带 EID 报告时为 **eSIM**，否则为 **SIM** 卡）、运营商（设备漫游到其他网络时，工具提示中显示归属运营商）、电话号码、ICCID、EID、IMEI、用于数据和通话的 SIM 卡以及漫游状态。没有套餐的 eSIM 卡槽会以灰显方式显示为 无套餐。
- 此设备未报告 **SIM** 卡表示设备已响应但没有任何 SIM 卡；尚无蜂窝信息表示设备尚未响应：请使用 刷新设备信息 。

> 电话号码、 ICCID、IMEI 和 EID 可识别个人和线路：绝不会向个人所有设备或用户注册请求这些信息。当设备变为个人所有时，这些信息会立即移除，并在命令历史记录中旧设备信息命令的结果中隐藏。它不会被导出，也不会写入系统日志。

刷新蜂窝套餐

iPhone 和 iPad 无法通过激活码安装 eSIM。运营商会在其 eSIM 服务器（ SM-DP+）上将 eSIM 套餐绑定（预留）到设备的 EID，并向您提供该服务器的地址；随后 刷新蜂窝套餐 会要求设备下载等待它的套餐。面板中的 刷新蜂窝套餐 按钮会在命令面板中选择该命令，您可以在其中输入运营商 **eSIM** 服务器 **URL**：

- 一个 **https://** 地址，按原样发送。包含 http://、用户名或密码或 # 部分的地址不被接受。
- 一个主机名 ，例如 *smdp.carrier.example*，按 https://smdp.carrier.example 发送。
- 一个 **LPA** 激活码 （ LPA:1$server$code，即 eSIM 二维码的文本）：仅使用服务器部分，因为该命令无法携带激活码。运营商必须将该套餐绑定到设备 EID，否则设备找不到可下载的内容。

设备会在不询问用户的情况下安装并激活套餐，即使设备未受监督也是如此。命令历史记录中的成功仅表示设备接受了请求，并不表示已安装套餐：安装最多可能需要三分钟，Cerberus Enterprise 会在约三分钟后再次向设备请求其 SIM 卡，因此新套餐会出现在面板中。错误 36001（设备无法连接到其蜂窝系统）、 36002（不支持 eSIM）和 36003（蜂窝系统繁忙，请稍后重试）会在系统日志中说明。已下载过一次的套餐无法再次下载：如果安装失败，请

联系运营商。该命令也可在设备页面的 Apple 设备操作 菜单中同时对多台设备使用。

Apple 不允许的操作
通过激活码添加 eSIM：不可行，请使用 刷新蜂窝套餐 并配合已绑定到 EID 的套餐。
移除 eSIM：无法远程逐个移除 eSIM。抹掉设备且关闭 保留 eSIM 数据套餐 会移除所有 eSIM
。要停用单个套餐，请让运营商将其停用：套餐会保留在设备上，但无法连接。
请求 EID：无需此操作，公司所有设备的 EID 会随 SIM 卡一起提供。
Mac没有蜂窝或 eSIM 管理功能。

命令
设备页面提供了一个 命令 面板，用于向受管设备发送远程命令。可用命令取决于平台（ Android 或 Apple ）和设备状态。

只能向当前已注册的设备发送命令。对于已取消注册的设备、尚未注册的 ADE
设备以及过去注册的历史记录，面板仅显示命令历史记录。

如果设备当前不在线，命令将在设备连接到互联网后立即送达并执行。对于 Android 命令，您可以设置
有效期 参数，以确定未送达命令的有效时长。

Android (AMAPI) 命令
对于 Android 设备，命令面板包含 有效期 字段（数值 + 单位）和 命令
选择器。某些命令需要额外参数，这些参数会在您选择命令时动态显示。

常用参数

有效期 ：如果命令无法立即执行，其有效时长。
命令 ：选择要发送到设备的操作。

无额外字段的命令

锁定设备 ：锁定设备。
重新启动设备 ：重新启动设备。需要 Android 7.0 或更高版本。
关闭丢失模式 ：使设备退出丢失模式。
放弃所有权 ：从运行 Android 8.0
或更高版本的公司所有设备上移除工作配置文件及所有政策，并将其留作个人使用。个人配置文件的
应用和数据会保留。设备确认该命令后，将从服务器中删除。此操作无法撤销。

带有额外字段的命令

重置密码 ：需要 新密码 和确认新密码 。可选开关包括 立即锁定 、要求输入 和启动时不要求凭据 。
清除应用数据 ：需要目标 包名 。

- [illegible]
- [illegible] **eSIM**[illegible]

> eSIM [illegible] **eSIM**[illegible] **eSIM**[illegible] **EID**[illegible] **SIM** [illegible]

[illegible]

[illegible]

Android [illegible]

- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]
- [illegible]

Apple (MDM) [illegible]

[illegible] Apple [illegible] [illegible] Android [illegible]

[illegible]

- [illegible] **Bundle ID**[illegible]
- [illegible] 200 [illegible]

[illegible] iPhone [illegible] iPad [illegible] **Cerberus Enterprise** [illegible] **Cerberus Enterprise** [illegible] “[illegible]” [illegible] iOS [illegible] 2 [illegible]

设备操作

仅列出设备支持的命令：有些需要受监督的 iPhone 或 iPad，另一些在 Mac
上不可用。破坏性操作会要求确认。

锁定设备 ：锁定屏幕，可附带可选的消息和电话号码。 Mac 会重新启动并使用六位 PIN 锁定，该
PIN 会在发送命令后显示一次，并显示在命令详情中。 iPhone 会在您的消息上方显示 “丢失的
iPhone”标题，即使此命令不会启用丢失模式。
启用丢失模式 （受监督的 iPhone 和 iPad
）：锁定设备，并在锁定屏幕上显示您的消息、电话号码和脚注。丢失模式启用期间，页面会显示横
幅以及 定位设备 （位置会显示在位置地图上）、 播放声音 和禁用丢失模式 命令。
设备会告知持有者其位置已被定位：执行 定位设备 后，锁定屏幕会显示 iPhone 已定位
，以及时间和接收位置的服务器名称，并显示 继续 按钮。 iOS 会显示此通知，且无法关闭。
清除密码 ：移除 iPhone 或 iPad
的密码，例如当用户忘记密码时。如果政策要求密码，系统会要求用户设置新密码。
刷新设备信息 ：向设备请求其信息（监督状态、操作系统版本、安全状态、 MDM 证书）及其清单。
设备设置 ：打开一个窗口，用于更改设备名称、 Mac
的主机名、蓝牙、数据漫游、个人热点、时区、墙纸、是否允许激活锁，以及在共享 iPad
上更改其设置（见下文）。仅会发送您更改的设置；设备不支持的设置会被禁用并显示原因。设备可
以确认数据漫游或个人热点但并未实际应用（例如 SIM 套餐不包含个人热点），因此 Cerberus
Enterprise 会在约 30 秒后重新读取这些设置，如果未更改，则会在系统日志中写入警告。
重新启动设备 和 关闭设备 ：在确认后立即重新启动或关闭设备。
擦除设备 ：擦除所有内容和设置，并将设备从管理中移除。在 iPhone 和 iPad 上，您可以保留
eSIM 数据计划并跳过近距离设置； Mac 会获得六位 PIN。
恢复服务 （擦除设备 的选项，适用于 iOS 17 或更高版本的 iPhone 和 iPad
）：擦除后，设备会在无人操作的情况下自行重新设置，并使用其当前政策、用户和所有权重新注册
。请为设置选择设备政策中的 Wi-Fi
网络，除非设备有以太网或蜂窝数据：只能使用个人网络（带密码、不带证书），因为设备尚无用户
或证书。激活锁必须关闭。
刷新蜂窝数据计划 （ iPhone 和蜂窝版 iPad，iOS 13
或更高版本，不适用于用户注册）：输入运营商提供的 运营商 eSIM 服务器 URL（ https://
地址、主机名或 LPA 激活码，其中仅使用服务器部分），设备将下载运营商绑定到其 EID 的 eSIM

计划。设备 EID 显示在字段下方，以便发送给运营商。请参阅 SIM 管理 页面。
关闭 保留 eSIM 数据计划 会在擦除时移除所有 eSIM。政策限制 设备擦除时保留 eSIM
（受监督设备， iOS 17.2
或更高版本）适用于在设备上发起的擦除（密码尝试失败次数过多、抹掉所有内容和设置）： Apple
未记录其对此命令的影响。
注销用户 （共享 iPad）：注销当前用户并返回登录屏幕。尚未同步到 iCloud 的数据仍保留在 iPad
上。

共享 iPad

共享 iPad 可由多人使用，每人拥有自己的 Managed Apple Account

，或由访客使用临时会话。它通过启用共享 iPad 的 ADE 配置文件进行设置（请参阅 Apple Automated

Device Enrollment页面），其 注册类型 字段显示 共享 iPad。

共享 iPad 用户 ： iPad
的用户，包括已登录的用户、他们使用的存储空间，以及是否有某些数据尚未同步到 iCloud。使用
刷新 再次向 iPad
请求列表。用户可以连同其数据一起删除，但已登录的用户除外（请先将其注销）； 删除所有用户
需要 iPadOS 14 或更高版本。数据尚未同步时，确认对话框会警告数据将丢失。
设备设置
：每个用户的存储空间、预期用户数、用户和访客会话被注销前的闲置时间、仅限访客会话、登录屏
幕上建议的 Managed Apple Account
域、用户无需在线检查密码即可登录的天数，以及为新用户跳过语言和地区设置。空字段会保留其当
前值；需要较新 iPadOS 的设置会被禁用。

Mac 用户

在 Mac 上， Mac 用户 面板列出已注册到管理中的用户，通常是注册该 Mac
的用户。政策的账户会在其会话中安装。对于每个用户，它会显示其注册时间、其会话的最后一次报告以及账
户状态： 已是最新 、等待用户 （用户登录后 Mac 会安装它们）、 未应用 （附 Mac
报告的原因），或政策没有账户时的 无账户 。使用 重新加载 再次读取列表。

激活锁

激活锁 字段显示激活锁是否开启。开启后，已擦除的设备只能使用用户的 Apple
账户或设备的绕过代码重新设置。受监督设备仅在 设备设置 中允许时才会开启激活锁。 Cerberus Enterprise
会向受监督设备请求其绕过代码并存储：使用字段菜单中的 显示绕过代码
查看（仅管理员可查看，且每次查看都会记录到系统日志中），然后在设备的激活锁屏幕上将其作为密码输入
，并将 Apple 账户留空。

恢复锁和固件密码 (Mac)
搭载 Apple 芯片的 Mac 会显示 恢复锁 字段，基于 Intel 的 Mac 则显示 固件密码 字段。两者都会在启动时保护
Mac：使用恢复锁时， recoveryOS 会要求输入密码；使用固件密码时， Mac
在从其他磁盘或恢复模式启动时会要求输入密码。该字段显示 Mac 是否报告了密码，并在工具提示中显示
Cerberus Enterprise 存储该密码的时间以及上次验证的时间。

设置或更改密码 ： Cerberus Enterprise 会生成一个由 20
个字母组成的密码，这些字母在任何键盘布局下都位于相同按键上；或者由管理员输入一个密码（ 8
到 64
个字符，不带重音符号；其他角色只能生成密码，因为他们无法查看已存储的密码）。密码在发送前
会加密存储，并且仅在 Mac 确认后才替换已存储的密码。如果 Mac 已在 Cerberus Enterprise

- Mac
- Mac
- Mac

Intel Mac “ ” Apple 30

Mac macOS Cerberus Enterprise Mac Mac Mac Mac Cerberus Enterprise Apple

FileVault (Mac)

FileVault Mac Cerberus Enterprise Mac FileVault FileVault Apple **macOS**

- Mac Mac
- Mac Mac 7

Bootstrap Token (Mac)

macOS 10.15 Mac **Bootstrap Token** Mac Mac Apple Mac **Bootstrap Token**

- Mac

较早托管 ：存储的令牌是在 Mac 最近一次注册或 MDM
证书续订之前发送的。续订后这是预期情况：令牌会被保留， Mac
不会再次发送它。重新注册后它可能不再有效：请在 Mac 的 “终端 ”中运行 sudo profiles install
- type bootstraptoken。
未托管 ： Mac 尚未发送令牌。要立即发送， Mac 的管理员可在终端中运行 sudo profiles install
- type bootstraptoken（ sudo profiles status -type bootstraptoken会显示其是否已托管）。

工具提示还会说明 Mac 是否允许将该令牌用于身份验证。通过 Automated Device Enrollment 设置的 Mac 会自动允许；在其他搭载 Apple 芯片的 Mac 上，用户可以在 recoveryOS 的启动安全性实用工具中允许。
Intel Mac 无法将令牌用于身份验证（ 不支持 ），但已托管的令牌仍可为新用户提供安全令牌。每次 Mac
发送、移除或请求其令牌时，都会记录到系统日志中。

设备状态和操作系统更新

设备状态
面板显示设备报告的自身信息：操作系统版本和构建号、软件更新进度（待安装版本、截止时间、启动更新的
原因、失败情况）、是否设置了密码以及是否符合政策、 Mac 上的 FileVault
、电池健康状况以及在设备上配置的账户。

可用更新 列表显示设备可安装的操作系统更新，这些信息在注册时和每周收集。使用 检查更新
立即请求，使用 安装
立即安装更新（设备将在确认后重新启动），或仅下载并让用户安装。此功能适用于受监督的 iPhone 和 iPad 以及 Mac，最高支持 iOS、 iPadOS 和 macOS 26

：在更高版本上，以及要更新多台设备时，请使用政策的必需更新（请参阅 Apple 政策的 软件更新 页面）。

搭载 Apple 芯片的 Mac 只有在允许其 Bootstrap Token
用于身份验证且该令牌已托管时，才会在安装更新时不要求管理员密码（请参阅上文 Bootstrap Token
）。否则，确认对话框会说明用户可能需要在更新安装前输入管理员密码。

应用和清单

应用
面板在一个表格中列出设备的所有应用。由政策或命令安装的应用的安装状态由设备实时报告；版本、大小和
用户安装的应用来自最后一次应用列表，该列表在注册时和每周收集。使用 询问设备 立即请求。

管理 ：政策 用于由设备政策安装的应用， 受管理 用于通过 安装应用 等命令安装的应用， 不受管理
用于用户安装的应用。 Cerberus Enterprise 应用带有 由 Cerberus 安装 标签。
需要注意
：安装失败、被用户拒绝或移除，或正在等待用户操作的应用。打开某一行可查看错误；失败的政策
应用可以通过重试按钮重新安装。设备报告为未验证的内置应用和 App Store 应用不计入其中。
移除应用
：可以移除受管理的应用及其数据。要移除由政策安装的应用，请将其从政策中移除。当作为受管理
应用安装的 Mac 软件包从政策中移除时，政策也会自行发送此命令。

配置文件、证书和安全 面板显示设备报告的配置描述文件、证书和安全状态（密码、加密、 Mac 上的 FileVault 和防火墙）。

在个人所有的设备上，不会收集用户安装的应用，仅列出由 Cerberus Enterprise
管理的配置描述文件和证书。

清单变更
面板显示设备发送的两个列表之间发生的变化：安装、移除或更新的应用（包含旧版本和新版本）、安装、移
除或更新的配置文件，以及添加或移除的证书。当设备发送新列表时会检测到变更：应用和配置文件每周一次
，证书每天一次，或者当您使用 询问设备
时：显示的日期是检测到变更的日期，变更发生在上一列表和该列表之间。设备的第一个列表，以及新注册或
所有权变更后的第一个列表，仅作为起点记录。可按名称或标识符搜索，并按类型和变更进行筛选。变更会保
留 365 天。

当操作系统更新一次性替换许多 Apple 应用时，它们会显示为一行（例如 “23 Apple apps updated”
），您可以展开该行。 MDM 证书续期会显示为 MDM 证书已续期 。在个人所有的设备上，仅显示由
Cerberus Enterprise 管理的项目的变更。

Apple 历史记录列

创建日期
命令
状态 ：已发送 （等待设备，设备一连接就会送达）， 成功 ，已回答 （打开该行查看结果），
正在等待设备 （设备当前无法运行此命令）， 失败 （打开该行查看原因）或 已取消
（设备的命令队列已清空，例如设备重新注册时）。
执行日期

刷新
使用命令面板中的刷新操作重新加载命令历史记录。