用户指南

Amazon One

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon One: 用户指南

Copyright © 2025 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

Amazon 的商标和商业外观不得用于任何非 Amazon 的商品或服务，也不得以任何可能引起客户混淆、贬低或诋毁 Amazon 的方式使用。所有非 Amazon 拥有的其他商标均为各自所有者的财产，这些所有者可能附属于 Amazon、与 Amazon 有关联或由 Amazon 赞助，也可能不是如此。

Table of Contents

什么是亚马逊 One Enterprise？ 1
Amazon One 设备 1
Amazon One 企业版控制台 2
购买 Amazon One 设备 3
Amazon One 企业版定价 3
Amazon One 的工作原理 4
Amazon One 工作流程 4
Amazon One 关键术语 4
设置 Amazon One 主机 6
注册一个 AWS 账户 6
创建具有管理访问权限的用户 7
保护您的 AWS 账户 7
创建具有管理权限的用户 7
以管理员身份登录 8
为其他用户分配访问权限 8
添加 Amazon One 用户 8
创建站点 10
创建设备实例 11
创建配置模板 12
配置设备实例以进行激活 13
安装和激活 Amazon One 15
了解需求 15
支持的标准 15
网络要求 16
功率要求 16
了解安装概念 16
安装 Amazon One Pedestal 17
安装可壁挂的 Amazon One 设备 19
安装 Amazon One 设备 I/O 集线器以实现安全访问 29
激活 Amazon One 设备 40
注册和输入用户 42
创建端点策略 42
正在进行入境身份验证 42
管理用户 43

查看已注册用户 ... 43
删除已注册用户及其生物识别信息 ... 43
管理 Amazon One 设备 ... 45
维护和清洁 Amazon One 设备 ... 45
清洁 Amazon One 设备 ... 45
现场管理 ... 46
更改网站名称 ... 46
更新网站地址 ... 46
设备实例管理 ... 47
查看设备实例状态 ... 47
重启 Amazon One 设备 ... 48
更新 Amazon One 设备配置 ... 48
更新 Wi-Fi 凭证 ... 48
停用设备实例 ... 49
安全性 ... 50
数据保护 ... 50
使用默认的静态数据加密 ... 51
传输中数据加密 ... 51
身份和访问管理 ... 51
受众 ... 52
使用身份进行身份验证 ... 52
使用策略管理访问 ... 55
亚马逊 One Enterprise 如何使用 IAM ... 57
基于身份的策略示例 ... 62
AWS 托管策略 ... 70
操作、资源和条件键 ... 73
操作 ... 73
资源类型 ... 77
条件键 ... 78
合规性验证 ... 78
监控 ... 80
监控事件 ... 80
订阅 Amazon One 企业版活动 ... 80
设备状态更改事件类型 ... 81
用户个人资料事件类型 ... 83
示例事件 ... 84

设备运行状况已更改为正常 84
设备运行状况更改为 “严重” 85
设备连接已更改为在线 86
设备连接已更改为离线 86
CloudTrail 日志 87
Amazon One 企业版信息位于 CloudTrail 87
了解 Amazon One 企业版日志文件条目 88
故障排除 91
排查 身份和访问问题 91
我无权在 Amazon One 中执行任何操作 91
我想允许我以外的人访问我 AWS 账户 的 Amazon One 资源 92
对 Amazon One 主机进行故障排除 92
我无法创建网站 92
我无法创建设备实例 93
我无法创建配置模板 93
我无法创建激活二维码 93
对 Amazon One 设备进行故障排除 93
空白屏幕 94
我无法连接到 Wi-Fi 或网络 94
重启带有活动警报的设备 95
系统错误 95
无法识别二维码 95
无法读取二维码 95
检测到多个 QR 码 96
设备实例不存在 96
未找到网站 96
邮政编码不匹配 96
网关超时 97
我无法配置设备 97
设备已重新启动，但出现错误消息和错误代码 97
设备屏幕上有亚马逊徽标，没有其他活动 97
暂时不可用 98
我们这边出了点问题 98
暂时停止服务 98
Amazon One 设备出现物理损坏 98
无法读取 palm 99

手掌无法识别 99
由于长时间处于非活动状态，设备已锁定 99
设备因篡改事件而被锁定 100
文档历史记录 101
..... cii

什么是亚马逊 One Enterprise？

Amazon One Enterprise 是一项新的基于手掌的身份验证服务，让员工无需使用徽章或密码即可安全访问建筑物和企业资产。 PINs

主题

- Amazon One 设备
- Amazon One 企业版控制台
- 购买 Amazon One 设备
- Amazon One 企业版定价

Amazon One 设备

Amazon One 设备专为 Amazon One Enterprise 而设计，Amazon One Enterprise 是一种安全、基于手掌的身份服务，用于企业 请注意以下设备规格：

- 用户输入 — Palm 生物识别、二维码匹配
- 主机接口 — Wi-Fi（2.4 GHz 和 5 GHz）、以太网、2 个 USB A 型、1 个 USB B Type-B
- 用户反馈 — 5.5 英寸触摸屏、Lightring、扬声器、耳机
- 物理访问控制协议 — OSDP 和韦根
- 电源 — POE，提供 110/220 VAC 输入交流转直流适配器，30W @ 15V
- 安全-防篡改开关
- 尺寸 (HxWx深 mm) — 86 x 85 x 256

Amazon One 企业版控制台

Amazon One Enterprise 包含一个控制台，可以通过以下方式使用该控制台：

- IT 或设施经理使用 Amazon One Enterprise 来创建和管理站点。该网站类似于团队在监控和管理 Amazon One Enterprise 设备和用户资料时执行任务的实际地点。IT 或设施经理的任务包括：
  - 创建一个将所有 Amazon One 设备实例包含在物理位置的站点
  - 添加管理员用户来管理站点，添加安装程序用户来访问激活 QR 码
- 管理员使用 Amazon One Enterprise 创建设备实例和管理亚马逊 One 设备。管理员任务包括：
  - 在站点下创建设备实例
  - 创建要应用于设备实例的配置模板
  - 监控设备运行状况并更新设备配置
  - 取消用户注册

- 安装程序使用 Amazon One Enterprise 访问激活二维码来激活设备。安装程序任务包括：
  - 在主机上访问激活二维码
  - 选择与要激活的设备实例相对应的二维码
  - 在安装了 Amazon One 设备的情况下扫描选定的二维码

购买 Amazon One 设备

联系我们，了解有关 Amazon One Enterprise 的更多信息，业务发展团队成员将与您联系，分享有关我们产品的更多详细信息，包括定价，并回答您可能遇到的任何问题。

Amazon One 企业版定价

联系我们，了解有关 Amazon One Enterprise 定价的更多信息。

Amazon One 的工作原理

Amazon One 是一项基于云的生物识别服务，它使用 Amazon One 设备使用手掌生物识别技术对用户进行身份验证。您可以联系我们订购 Amazon One 设备。

安装 Amazon One 设备后，您可以在 Amazon One 控制台和身份验证应用程序上使用您的 AWS 账户激活和注册您的设备。您可以查看已注册用户的生物识别个人资料。如果需要，您可以取消他们的注册并删除他们的生物识别数据。

Amazon One 控制台是管理运营活动的集中中心，例如跟踪设备和查看月度账单。用户可以在现场的受监管注册站扫描手掌进行注册。注册后，用户只需将手掌悬停在支持 Amazon One 的设备上，即可无缝进入或退出安全地点。

主题

- Amazon One 工作流程
- Amazon One 关键术语

Amazon One 工作流程

以下详细介绍了 Amazon One 的基本工作流程：

1. 请联系我们，购买并安装 Amazon One 设备。
2. 安装设备后，激活 Amazon One。
3. 登录您的 Amazon One 账户。
4. 配置用户注册和输入设备。
5. 注册员工手掌。
6. 使用管理和监控功能来确保设备运行状况，使配置保持最新状态，并跟踪用户注册以进行全面监督。

Amazon One 关键术语

以下是 Amazon One 的关键术语：

- 地点 — 客户管理客户在其中安装 Amazon One 设备的物理建筑。站点必须满足您的 Amazon One 设备的设施、网络和电源要求。

- 设备 — 用于身份验证的 Amazon One 手掌扫描生物识别设备。
- 设备实例-具有配置的设备的逻辑表示形式。使用设备实例允许交换 Amazon One 设备，同时自动继承先前设置的配置和名称。设备实例具有用户定义的名称（与您的访问控制软件共享命名约定）和一组通信配置。设备实例有三种主要状态：
  - 需要配置
  - 已准备好激活
  - 活动
- 配置模板-应用于设备实例的一组包罗万象的配置。

设置 Amazon One 主机

本章介绍开始使用 Amazon One 主机的基本步骤。

设置站点、设备实例和配置模板-按照以下步骤创建一个框架，用于添加存放您的 Amazon One 设备的物理位置，然后使用 Amazon One Enterprise 控制台对其进行配置和管理。您只能偶尔使用此流程，甚至只使用一次，具体取决于站点的数量、设备实例和您的配置模板。

主题

- 注册一个 AWS 账户
- 创建具有管理访问权限的用户
- 添加 Amazon One 用户
- 创建站点
- 创建设备实例
- 创建配置模板
- 配置设备实例以进行激活

注册一个 AWS 账户

如果您没有 AWS 账户，请完成以下步骤创建一个。

如需注册 AWS 账户

1. 打开 https://portal.aws.amazon.com/billing/signup
2. 按照屏幕上的说明操作。

   在注册时，将接到电话，要求使用电话键盘输入一个验证码。

   当您注册亚马逊云科技账户时，系统会创建一个亚马逊云科技账户根用户。根用户有权访问该账户中的所有亚马逊云科技服务和资源。作为安全最佳实践，为用户分配管理访问权限，并且仅使用 root 用户来执行需要 root 用户访问权限的任务

注册过程完成后，AWS 会向您发送一封确认电子邮件。您可以随时前往我的账户并选择 “我的账户”，查看当前账户活动https://aws.amazon.com/并管理账户

创建具有管理访问权限的用户

注册 AWS 账户后，请保护您的 AWS 账户根用户，启用 AWS IAM IAM Identity Center，并创建一个管理用户，这样您就不会使用根用户执行日常任务。

主题

- 保护您的 AWS 账户
- 创建具有管理权限的用户
- 以管理员身份登录
- 为其他用户分配访问权限

保护您的 AWS 账户

现在，您已经登录了自己的 Amazon One 账户，请保护您的账户。

为了保护您的 AWS 账户根用户

1. 选择根用户并输入您的 AWS 账户电子邮件地址，以账户所有者的身份登录 AWS 管理控制台。
2. 在下一页上，输入您的密码。

   有关使用根用户登录的帮助，请参阅 AWS 登录用户指南中的以根用户身份登录。
3. 为您的根用户启用多重身份验证（MFA）。

   有关说明，请参阅《IAM 用户指南》中的为您的亚马逊云科技账户根用户启用虚拟 MFA 设备（控制台）。

创建具有管理权限的用户

既然您已经保护了自己的 Amazon One 账户，请创建一个具有管理权限的用户。

创建具有管理访问权限的用户

1. 启用 IAM Identity Center。

   有关说明，请参阅 AWS IAM 身份中心用户指南中的启用 AWS IAM 身份中心。
2. 在 IAM Identity Center 中，为用户授予管理访问权限。

有关使用 IAM 身份中心目录作为身份源的教程，请参阅 AWS IAM 身份中心用户指南中的使用默认 IAM 身份中心目录配置用户访问权限。

以管理员身份登录

现在，您已经创建了一个具有管理权限的用户，请以管理员身份登录。

以具有管理权限的用户身份登录

- 使用您在创建 IAM 身份中心用户时发送到您的电子邮件地址的登录 URL，使用您的 IAM 身份中心用户登录。

  要获取使用 IAM Identity Center 用户登录方面的帮助，请参阅《Amazon 登录用户指南》中的登录 Amazon 访问门户。

为其他用户分配访问权限

现在，您已经以管理员身份登录，可以向其他用户分配访问权限。

为其他用户分配访问权限

- 将用户分配到一个组，然后为该组分配单点登录访问权限。

  有关说明，请参阅 AWS IAM 身份中心用户指南中的添加群组。

添加 Amazon One 用户

除了管理员用户之外，您还可以添加没有管理员权限的用户。例如，这些用户可能是安装人员，他们访问 Amazon One 控制台只是为了检索设备激活二维码来激活 Amazon One 设备。

添加 Amazon One 用户

1. 按照用户指南中的如何登录中所述的与您的用户类型相适应 AWS 的登录过程进行AWS 登录 操作。
2. 在导航窗格中，选择 “用户”，然后选择 “添加用户”。
3. 在指定用户详细信息页面中的用户详细信息下的用户名中，输入新用户的名称。这是 AWS的登录名。

> **Note**
>
> 中的 IAM 资源的数量和大小 AWS 账户 是有限的。有关更多信息，请参阅 IAM 和 AWS STS 配额。用户名可以是最多 64 个字母、数字和以下字符的组合：加号 (+)、等号 (=)、逗号 (,)、句点 (.)、at 符号 (@)、下划线 (_) 和连字符 (-)。账户中的名称必须唯一。名称不区分大小写。例如，您不能创建名为 TESTUSER 和 testuser 的两个用户。在策略中使用用户名或将其作为 ARN 的一部分时，用户名区分大小写。在控制台中向客户显示用户名时（例如在登录过程中），用户名不区分大小写。

4. 系统会询问您是否正在向某人提供控制台访问权限。选择 “向用户提供访问权限 — AWS Management Console 可选”。
5. 选择 “我想创建 IAM 用户”。
6. 对于控制台密码，请选择下列选项之一：
   - 自动生成的密码-为用户提供一个符合账户密码策略的随机生成的密码。在转到找回密码页面后，您可以查看或下载密码。
   - 自定义密码-为用户分配您在字段中输入的密码。
7. （可选）默认情况下，“用户必须在下次登录时创建新密码（推荐）” 处于选中状态，以确保用户在首次登录时需要更改密码。

> **Note**
>
> 如果管理员启用了允许用户更改其密码账户密码策略设置，则此复选框不执行任何操作。否则，它会自动将名为 `IAMUserChangePassword` 的 AWS 托管策略附加到新用户。该策略授予他们更改其密码的权限。

8. 选择下一步。
9. 在 设置权限 页面上，选择 直接附加策略。
10. 选择要附加到用户的策略。
    - AmazonOneEnterpriseReadOnlyAccess
    - AmazonOneEnterpriseInstallerAccess

> **Note**
>
> AmazonOneEnterpriseInstallerAccess 托管策略仅允许用户在 Amazon One Enterprise 控制台中访问激活二维码。此政策非常适合雇用第三方来安装 Amazon One 设备的企业。

11. 选择下一步。
12. （可选）在查看和创建页面上的标签下，选择添加新标签，通过以键值对的形式附加标签来向用户添加元数据。有关将在 IAM 中使用标签的更多信息，请参阅 Tagging IAM resources（标记 IAM 资源）。
13. 查看您到目前为止所做的所有选择。如果您已准备好继续，请选择创建用户。
14. 在找回密码页面上，获取分配给用户的密码：
    - 选择密码旁边的显示以查看用户密码，以便手动记录此密码。
    - 选择 “下载.csv”，将用户的登录凭据下载为.csv 文件，您可以将其保存到安全位置。
15. 选择电子邮件登录说明。您的本地邮件客户端将打开并显示一份草稿，您可以对草稿进行自定义并发送给用户。电子邮件模板包括每个用户的以下详细信息：
    - 用户名称
    - 账户登录页面的 URL。使用以下示例，换入正确的账户 ID 号或账户别名：

```
https://AWS-account-ID or alias.signin.aws.amazon.com/console
```

> **Important**
>
> 用户的密码未 包括在生成的电子邮件中。在向用户提供密码时，必须符合您所在组织的安全准则。

创建站点

既然您已经登录了 AWS Management Console，就可以使用 Amazon One 控制台来创建您的网站了。

> **Important**
>
> Amazon One 仅在美国东部（弗吉尼亚北部）地区上市。

创建站点

1. 在 https://console.aws.amazon.com/on e-enterprise 上打开 Amazon One 控制台。
2. 选择 “转至概览”。
3. 在导航窗格中，选择 Sites (站点)。
4. 选择 “创建站点”。
5. 在 “站点信息” 下的 “站点名称” 中，输入该站点的名称。
6. 在 “物理地址” 下，输入要安装您的 Amazon One 设备的站点的地址。
7. （可选）要向网站添加标签，请在标签下输入键值对，然后选择添加新标签。要在创建网站之前删除此标签，请选择 “移除”。
8. 选择 “创建站点” 来创建站点。

创建设备实例

现在，您已经在 AWS 管理控制台中创建了一个站点，可以使用 Amazon One 控制台创建设备实例。

创建设备实例

1. 在 https://console.aws.amazon.com/on e-enterprise 上打开 Amazon One 控制台。
2. 在导航窗格中，选择设备实例。确保您位于 “未激活的实例” 选项卡上。
3. 在 “实例详细信息” 下，从 “站点” 下拉列表中选择一个站点，或者选择 “创建站点” 按钮创建一个新站点。
4. 手动输入每个单独的设备实例名称。
5. （可选）要向设备实例添加标签，请在标签下输入键值对，然后选择添加新标签。要在创建设备实例之前删除此标签，请选择移除。
6. 选择创建实例以创建设备实例。

> **Note**
>
> 注意：需要先配置设备实例，然后才能进行安装。

创建配置模板

现在，您已经创建了设备实例，可以使用 Amazon One 控制台来创建配置模板。

创建配置模板

1. 在 https://console.aws.amazon.com/on e-enterprise 上打开 Amazon One 控制台。
2. 在导航窗格中，选择配置模板。
3. 选择创建模板。
4. 在模板信息下，在模板名称中，输入配置模板的名称。
5. 在 “设备配置” 下，选择一种操作模式。

   To configure Enrollment operating mode

   1. （可选）在 Wifi 配置下，提供您的 Wifi 凭证。
   2. （可选）要向网站添加标签，请在标签下输入键值对，然后选择添加新标签。要在创建网站之前删除此标签，请选择 “移除”。
   3. 选择 配置。

   To configure Entry operating mode

   1. 在 “控制面板设置” 下，提供 Amazon One 设备与您的控制面板通信的通信设置。
   2. 在 “徽章格式设置” 下，提供用于指定公司徽章格式布局的配置设置。
   3. （可选）在 Wifi 配置下，提供您的 Wifi 凭证。
   4. （可选）要向网站添加标签，请在标签下输入键值对，然后选择添加新标签。要在创建网站之前删除此标签，请选择 “移除”。
   5. 选择 配置。

> **Important**
>
> 您必须配置至少一台注册设备和一台入口设备，才能启用 Amazon One 的全部功能以实现安全访问。

配置设备实例以进行激活

创建设备实例后，您可以使用先前创建的配置模板配置设备实例（参见创建配置模板），也可以手动添加配置。

配置设备实例以进行激活

1. 在 https://console.aws.amazon.com/on e-enterprise 上打开 Amazon One 控制台。
2. 在导航窗格中，选择设备实例。确保您位于 “未激活的实例” 选项卡上。
3. 选择一个或多个要配置的实例。
4. 选择 配置。
5. 在 “设备配置” 下，选择两种输入法之一：
   a. 对于 “使用模板” 选项，从下拉列表中选择一个模板。查看或更改此导入的配置信息。

      有关 “创建模板” 选项，请参阅创建配置模板。
   b. 在 “手动输入” 选项中，选择一种操作模式。

      To configure Enrollment operating mode

      a. （可选）在 Wifi 配置下，提供 Wifi 凭证。
      b. （可选）要向网站添加标签，请在标签下输入键值对，然后选择添加新标签。要在创建网站之前删除此标签，请选择 “移除”。
      c. 选择 配置。

      To configure Entry operating mode

      a. 在 “控制面板设置” 下，提供 Amazon One 设备与您的控制面板通信的通信设置。
      b. 在 “徽章格式设置” 下，提供用于指定公司徽章格式布局的配置设置。
      c. （可选）在 Wifi 配置下，提供 Wifi 凭证。

d. （可选）要向网站添加标签，请在标签下输入键值对，然后选择添加新标签。要在创建网站之前删除此标签，请选择 “移除”。

e. 选择 配置。

6. 在 “未激活的实例” 表下，应显示 Ready for activation 实例状态。
7. 验证激活 QR 码是否可用于激活。在导航窗格中，选择激活二维码。
8. 从 “选择站点” 下拉列表中，选择一个站点。
9. 在 “站点信息” 下，验证网站地址。
10. 在激活二维码下，每个设备实例都有对应的二维码。选择获取二维码以显示激活二维码。

> **Important**
>
> 您必须配置至少一台注册设备和一台入口设备，才能启用 Amazon One 的全部功能以实现安全访问。

安装和激活 Amazon One

成功设置您的 Amazon One 主机后，接下来的步骤包括在您的站点上安装 Amazon One 设备并确保这些设备已正确激活。此过程包括将设备物理放置在指定区域，将它们连接到您的网络，以及完成激活过程以实现无缝的用户识别和交易功能。激活后，您的 Amazon One 设备即可为您的客户或员工提供安全的非接触式体验。

> **Note**
>
> 本节重点介绍安装，并使用移动浏览器访问 AWS Management Console 以获取设备激活二维码。

主题

- 了解需求
- 了解安装概念
- 安装 Amazon One Pedestal
- 安装可壁挂的 Amazon One 设备
- 安装 Amazon One 设备 I/O 集线器以实现安全访问
- 激活 Amazon One 设备

了解需求

Amazon One 设备可以安装在任何有电气控制门的公司或营业场所。

控制面板要求

Amazon One 设备可以作为读卡器连接到大多数标准门禁控制面板。Amazon One 设备支持以下协议：

- OSDP (v1 和 v2)
- 韦根

网络要求

Amazon One 设备必须始终连接到互联网才能正常运行。互联网连接可通过有线以太网或 Wi-Fi 提供。所需的最低带宽为 10 Mbps。

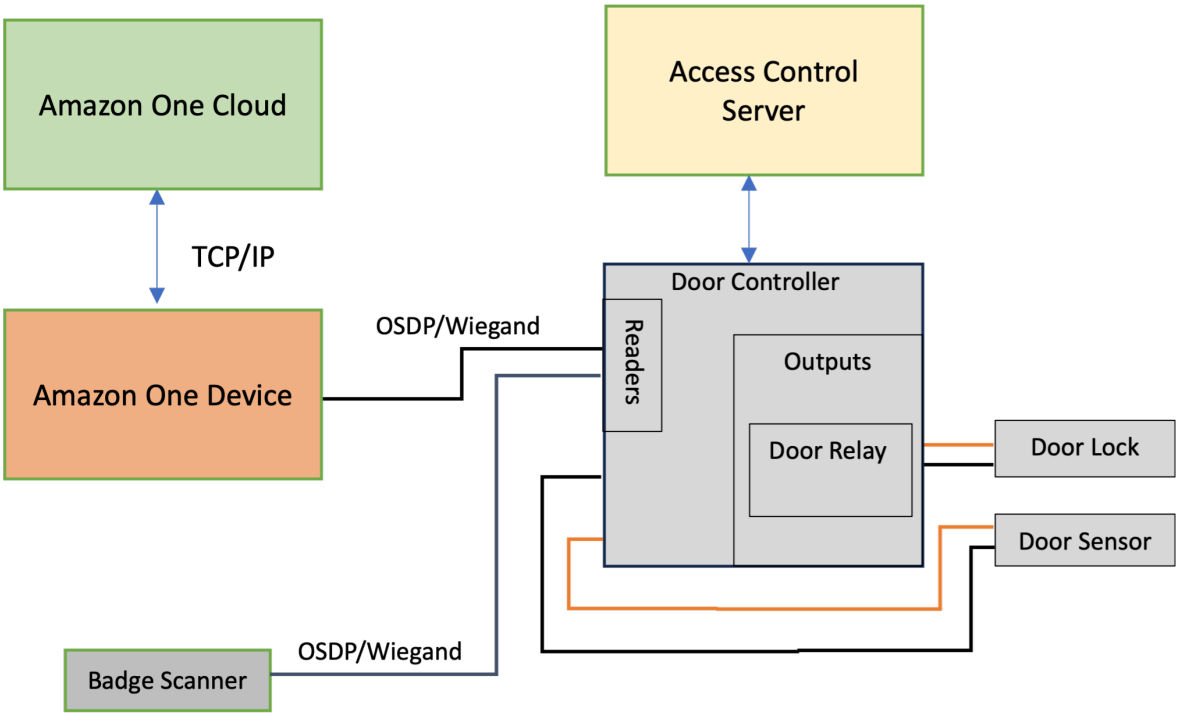
功率要求

可以通过以下两种方式之一为 Amazon One 设备供电：

- 使用包装盒中提供的 120V 电源适配器。
- 使用支持 PoE+ 的设备。

了解安装概念

为了正确保护建筑物访问权限，Amazon One 建议您将设备作为典型访问控制环境的一部分进行安装，如以下方框图所示。



访问控制环境通常由以下组件组成：

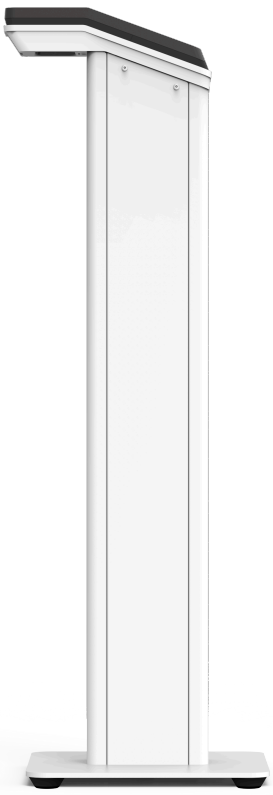
- Amazon One 设备：这是一种手掌识别设备，它将执行生物识别身份验证，以识别试图进入建筑物安全区域的个人。

- 访问控制服务器：此组件通常控制用户对安全区域的访问权限。有权进入该区域 IDs 的个人的徽章存储在此服务器上。该服务器缓存与相应门控制器 IDs 相关的内容。
- 门控制器：
  - Amazon One 设备通过 OSDP 接口连接到门控服务器。
  - 如果需要韦根接口，则可以使用 COTS OSDP-to-Wiegand 转换器。
  - 成功进行身份验证后，Amazon One 设备会将用户的徽章 ID 发送到门禁控制器。
  - 门控器会做出决定，然后允许 Amazon One 设备显示 “已授予访问权限” 或 “拒绝访问” 消息。
- 徽章扫描器：徽章扫描仪通常用于扫描 RFID 徽章并将徽章编号发送到门禁服务器。在 Amazon One 中，徽章扫描器可以连接到 Amazon One 设备，允许用户扫描他们的徽章，从而将徽章与他们的手掌个人资料相关联。

安装 Amazon One Pedestal

Amazon One Pedestal 是 Amazon One 识别和交易系统的关键组件，旨在为用户提供无缝的非接触式体验。该设备具有安全的生物识别身份验证功能。您可以将其集成到各个位置，以提供顺畅的访问或支付解决方案。

本节提供安装 Amazon One Pedestal 的位置要求和 step-by-step说明。适当的准备和安装是确保系统安全高效运行的关键，为用户提供流畅、可靠的体验。



安装 Amazon One Pedestal 的先决条件和准备工作

在开始安装之前，请确保满足以下条件以实现安全、可靠和有效的设置：

- 电源要求：如果您使用 POE+（以太网供电）为设备供电，请验证是否已安装 Cat6 电缆，并且有 POE+ 馈电器或交换机可供使用。或者，如果使用的是交流电源 (120V)，请确保在距离底座 20 英尺以内有可触及的交流电源插座。
- 物理设置：地板必须平坦、干净且没有任何碎屑，以确保底座安装的稳定和安全。
- 基座位置：将基座安装在不会阻挡门、车道或出入点的位置，便于在该区域周围移动。
- 电缆管理：将所有多余的电缆布线并固定在底座内，以避免混乱并防止在正常使用过程中造成任何潜在的损坏。

确认这些先决条件后，您就可以继续安装过程了。

安装 Amazon One Pedestal

1. 从包装中取出 Amazon One Pedestal。
2. 拧下两个 M4 防篡改螺丝，拆下门。
3. 插上电源线。
4. 将电缆穿过底座底板上的孔。
5. 将多余的电源线卷在底座内。
6. 将以太网电缆（Cat5E 或更高）穿过底座的底板，然后插入以太网端口。
7. 在基座底座上方 2 英寸处的以太网电缆上安装铁氧体回路。
8. 将 RS485 串行电缆从门禁控制面板（或徽章读取器）连接到底座，长度超过 1 英尺。
9. 在基座底座上方 2 英寸处的 RS485 电缆上安装铁氧体回路。
10. 接通电源插座并确认 Amazon One 设备已开机。
11. 将门重新安装到基座上，然后重新拧紧两个 M4 防篡改螺丝以固定。

安装您的 Amazon One 设备后，就可以激活设备了。

安装可壁挂的 Amazon One 设备

壁挂式 Amazon One 设备是一款多功能、紧凑的生物识别系统，旨在为各种环境中的用户提供无缝的非接触式体验。它使用先进的手掌识别技术进行安全访问或支付，非常适合零售空间、办公室入口等人流量大的场所。

本节概述了安装壁挂式 Amazon One 设备的必要位置要求和详细步骤，以确保最佳性能和安全性。

安装壁挂式 Amazon One 设备的先决条件和准备工作

在开始安装之前，请确保满足以下条件，以保证设备有效运行并在您的空间内正确设置：

- 仅限室内使用：壁挂式 Amazon One 设备仅供室内使用，因此请确保将其安装在适当的环境中。
- 墙壁要求：墙壁必须处于水平状态，以确保设备的正确对齐和功能。
- 安装高度：安装后，壁挂支架的顶部应与地面不超过 44-46 英寸，以确保用户易于使用。
- 电缆管理：确保所有多余的电缆都布线在壁挂支架后面并牢固固定，以防止损坏或混乱。

- 以太网供电 (PoE++)：如果使用以太网供电 (PoE++)，请验证是否有 IEEE 802.3bt（类型 3）6 类 PoE++ 交换机（末端）或注入器（中跨度）可用。PoE++ 来源必须经过上市或认证，并且符合 IEC 62368-1 标准。重要的是，PoE++ 源必须与设备位于同一建筑物内。仅在 AOE 设备上使用经批准的 PoE++ 来源。
- 15V 直流电源输入：如果使用 15V 直流电源输入，请确保仅使用 NEC 2 级或经功率限制批准的电源。电源必须列出或通过认证，以确保安全性和兼容性。

必要工具

- 如果需要墙锚，则使用 1/4 英寸的干墙钻头或砖石钻头
- 剥线钳
- 7/64” 钻头用于钻导向孔
- #2 十字螺丝刀
- 0.5 毫米 x 2 毫米平头螺丝刀
- T12 安全 Torx 驱动程序
- 铅笔
- 级别

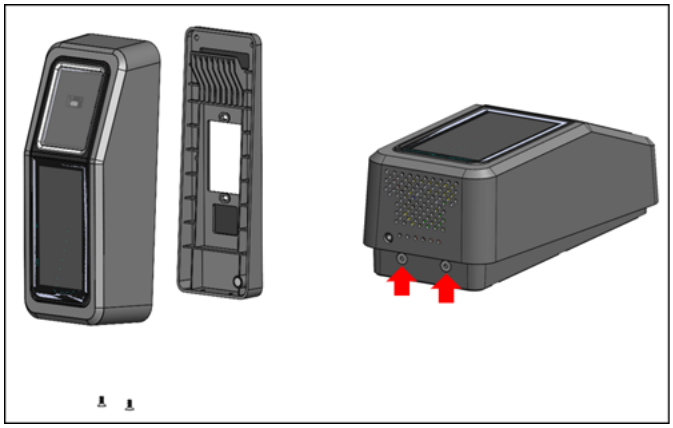
包含在壁挂式的 Amazon One 设备中

- 6x #8 石膏板锚
- 6x #8 -32 1 英寸长的螺丝
- 2x #6 -32 1 英寸机用螺丝
- 2x 6 位接线端子台连接器
- 2 个 Torx Security m4x10 平头螺丝

确认这些先决条件后，您可以继续执行安装步骤，以安全地安装和配置壁挂式 Amazon One 设备。

为您的 Amazon One 设备安装壁挂式安装板

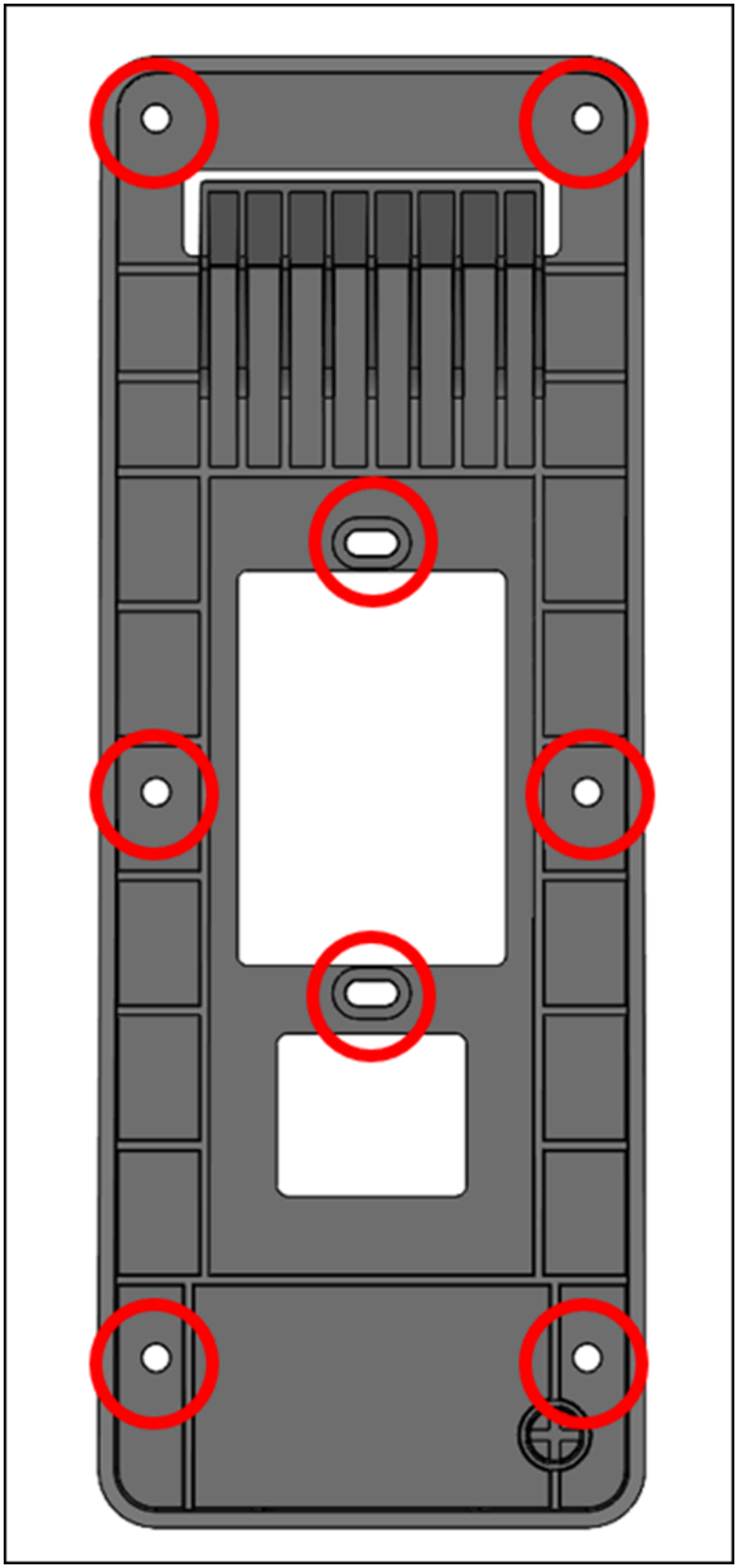
1. 从包装中取出您的 Amazon One 设备。
2. 拆下底部的两颗 Torx 安全螺丝，将安装板与 Amazon One 设备分开。



3. 将安装板放在墙上的所需位置。使用支架作为模板来标记外面的六个螺丝孔，如下图所示。

   （可选）如果安装位置有单个排气箱可用，请执行以下操作：

   - 将随附的 #6 -32 机器螺丝穿过长方形孔，将板块松散地安装到帮派箱上。
   - 确保安装板处于水平状态。
   - 使用安装板作为模板，用铅笔标记六个螺钉位置。你可以使用长方形孔和 #6 -32 螺钉作为安装板的额外支撑。请勿使用 #6 -32 螺钉位置作为安装墙板的主要方式。



4. 如果安装在灰泥、石膏板、砖块或混凝土表面上，请在每个标记的位置钻1/4英寸的孔，然后通过将墙锚压入孔中直到锚与墙壁齐平来安装墙锚。

   如果安装在木质表面上，则不需要锚固件，在标记的位置只需要7/64英寸的导向孔。

5. 在锚点位置使用 #8 木螺丝将墙板松散地固定在墙上。
6. 所有紧固件安装到位后，确保安装板处于水平状态。
7. 拧紧螺丝，将安装板固定在墙上。

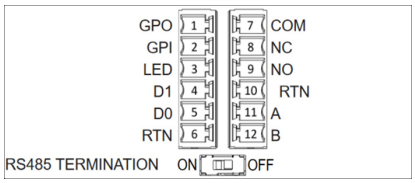
连接您的壁挂式 Amazon One 设备

您可以使用 OSDP 和 Weigand 访问控制协议配置 Amazon One 设备。为了简化安装，Amazon One 设备使用了接线端子连接器（Mfg P/N：Phoenix Contact 1767694）。您还可以选择将 Amazon One 设备配置为使用内部继电器或通用输入和输出连接直接控制外部设备。

1. 要为您的应用确定合适的接线配置，请参阅下图和连接表。

   有关信号的详细电气特性，请参阅接线说明。

   连接



Pin	Connection	描述	使用
1	GPO	通用输出	数字输出信号-可选
2	GPI	通用输入	数字输入信号-可选
3	导致了	Wiegand LED	韦根 LED — 可选
4	D1	Wiegand D1	韦根数据 1 — 白线

Pin	Connection	描述	使用
5	D0	Wiegand D0	韦根数据 0 — 绿线
6	RTN	信号返回	Wiegand Ground — 黑线
7	Com	继电器共用	触点继电器常用 — 白线
8	NC	继电器常闭	触点继电器常闭 — 橙线
9	NO	继电器常开	触点继电器常开 — 黄线
10	RTN	信号返回	OSDP 回归 — 黑线
11	A	RS485_A/D1/Clock	OSDP D1 — 白线
12	B	RS485_b/D0/Data	OSDP D0 — Green wire

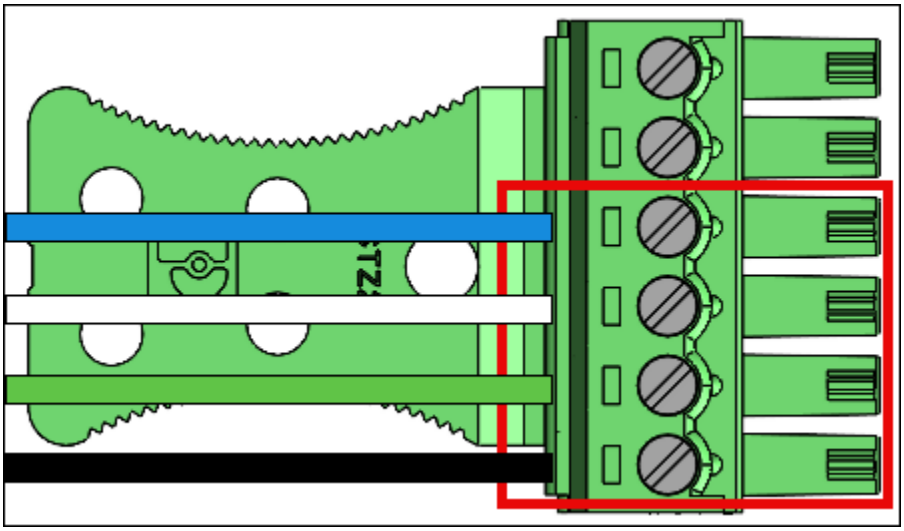
2. 安装电线时，从电线末端剥掉 3mm-5mm。
3. 将电线剥掉的一端插入所需的端子位置。
4. 使用一字螺丝刀，顺时针转动端子固定螺丝，将电线夹紧直至其紧固。不要过度拧紧。
5. 紧固后，轻轻地拉动电线以确保其固定到位。
6. 完成必要的连接后，将插头插入 Amazon One 设备接线板的相应插座中。
7. 将 Cat6 以太网电缆插入 RJ45 插孔。
8. 放置 Amazon One 设备，使墙板上的挂钩滑入设备背面的开口中。
9. 确保电缆没有卡在设备和安装板之间，然后让设备旋转并固定到位。
10. 用两颗 Torx Security m4x10 平头螺丝将你的 Amazon One 设备固定在安装板上。
11. 用手拧紧螺丝。不要过度收紧。

连接壁挂式 Amazon One 设备

仅为您的应用安装所需的电线。

韦根连接

- 将蓝线插入引脚 3 (LED)。
- 将白线插入引脚 4 (D1)。
- 将绿色电线插入引脚 5 (D0)。
- 将黑线插入引脚 6 (RTN)。



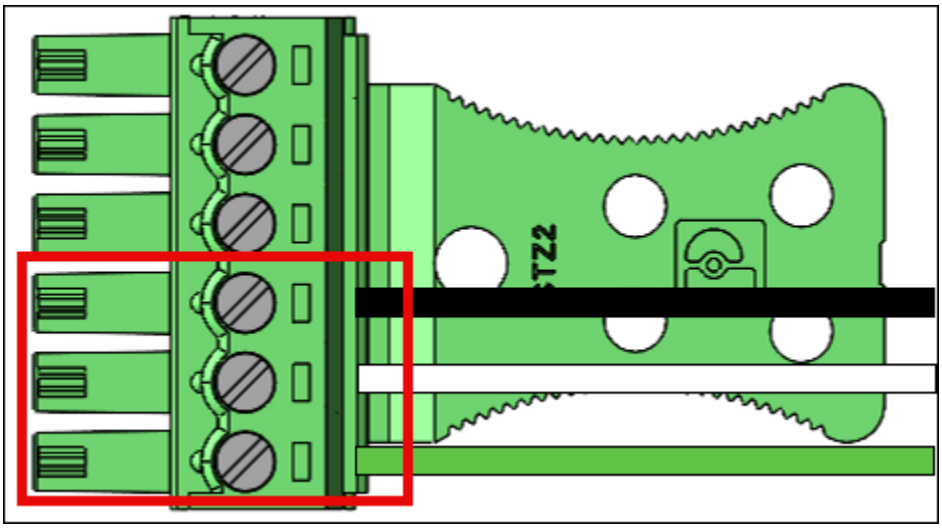
韦根输出接线

Pin	Connection	描述	使用
3	导致了	Wiegand LED	韦根 LED 输入 — 可选 (5V TTL)
4	D1	Wiegand D1	Wiegand D1 输出 (5V TTL)
5	D0	Wiegand D0	Wiegand D0 输出 (5V TTL)
6	RTN	信号返回	韦根 GND 参考文献

如果设备是线路上的最后一台设备，请将 RS485 终端开关 “打开”。该开关激活线路上的 120 欧姆电阻器端接。

RS485 连接

- 将黑线插入引脚 10 (RTN)。
- 将白线插入引脚 11 (A)。
- 将绿色电线插入引脚 12 (B)。



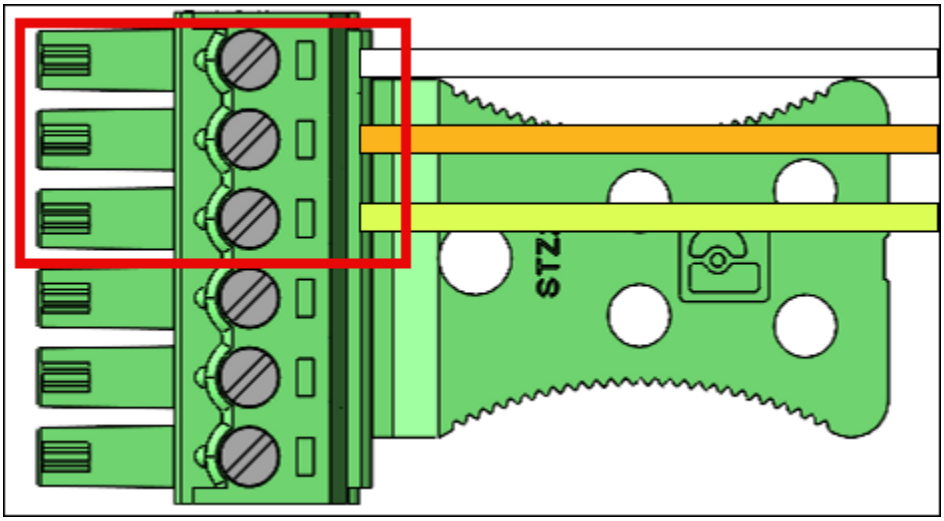
RS485 接线

Pin	Connection	描述	使用
10	RTN	信号返回	地面
11	A	RS485_A/D1/Clock	RS485 同相信号
12	B	RS485_b/D0/Data	RS485 反转信号

中继连接

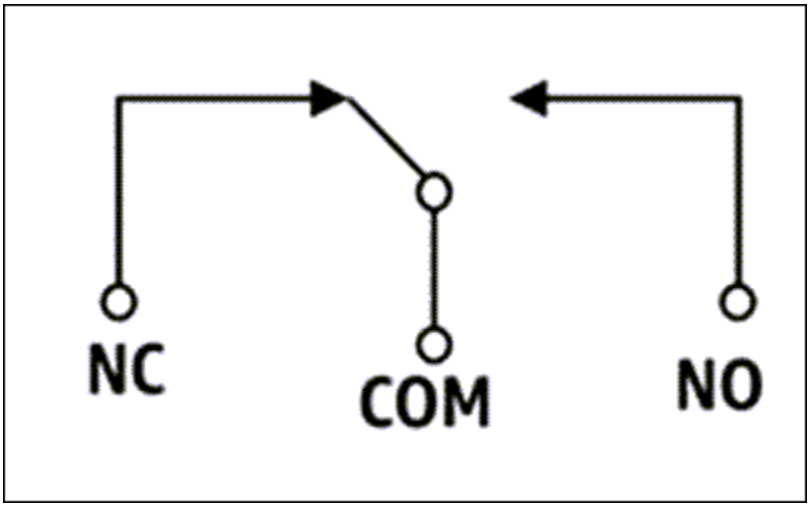
- 将白线插入引脚 7 (COM)。
- 将橙色电线插入引脚 8 (NC)。

- 将黄线插入引脚 9（否）。



继电器接线

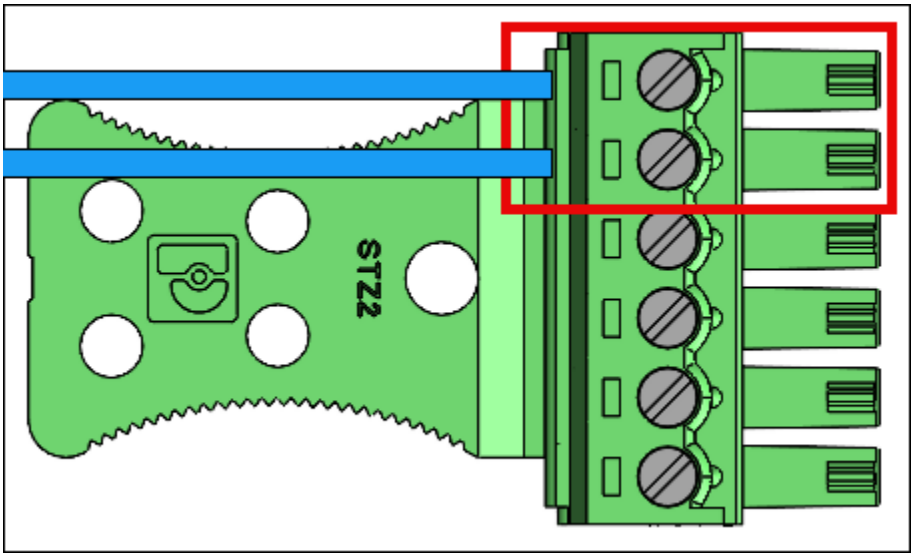
Pin	Connection	描述	使用
7	COM	继电器共用	触点继电器常用 — 白线
8	NC	继电器常闭	触点继电器常闭 — 橙线
9	NO	继电器常开	触点继电器常开 — 黄线



继电器应按照规定的安全额定值运行 30VAC/60VDC，最大 60W。

数字输入/输出连接

- 将蓝线插入引脚 1 (GPO)。
- 将蓝线插入引脚 2 (GPI)。



数字输入/输出接线

Pin	Connection	描述	使用	
1	GPO	通用输出	数字输出信号 (5V)	

Pin	Connection	描述	使用	
2	GPI	通用输入	数字输入信号 (3.6V — 5V)	

- 数字输入/输出连接应按所列方式运行。

安装您的 Amazon One 设备后，就可以激活设备了。

安装 Amazon One 设备 I/O 集线器以实现安全访问

带有 I/O 集线器的 Amazon One 设备是 Amazon One Enterprise 系统不可或缺的一部分，旨在增强各种环境的安全性并简化访问控制。该设备利用生物识别手掌识别为用户提供安全的非接触式身份验证，非常适合在办公楼、受限入口或需要无缝访问管理的设施等高度安全的区域中使用。I/O 集线器充当设备和现有安全基础设施之间的桥梁，可实现与门锁、警报器和其他门禁系统的通信。

本节提供安装带有 I/O Hub 的 Amazon One 设备的位置要求和 step-by-step说明。适当的准备和安装是确保系统安全高效运行的关键，为用户提供流畅、可靠的体验。

安装带有 I/O Hub 的 Amazon One 设备的先决条件和准备工作

在开始安装之前，请确保满足以下条件，以确保安全、可靠和有效的设置：

- 仅限室内使用：带有 I/O 集线器的 Amazon One 设备专为室内使用而设计。确保将其安装在适当的环境中。
- 以太网供电 (PoE++)：如果使用以太网供电 (PoE++)，请验证是否有 IEEE 802.3bt（类型 3）6 类 PoE++ 交换机（末端）或注入器（中跨度）可用。PoE++ 来源必须经过上市或认证，并且符合 IEC 62368-1 标准。重要的是，PoE++ 源必须与设备位于同一建筑物内。仅在 AOE 设备上使用经批准的 PoE++ 来源。

- 15V 直流电源输入：如果您使用的是 15V 直流电源输入，请确保仅使用 NEC 2 级或功率受限、经批准的电源。电源必须列出或通过安全认证。有关更多详细信息，请参阅下面的 “可选 DC” 部分。

必要工具

- 剥线钳

- #2 十字螺丝刀
- 0.5 毫米 x 2 毫米平头螺丝刀

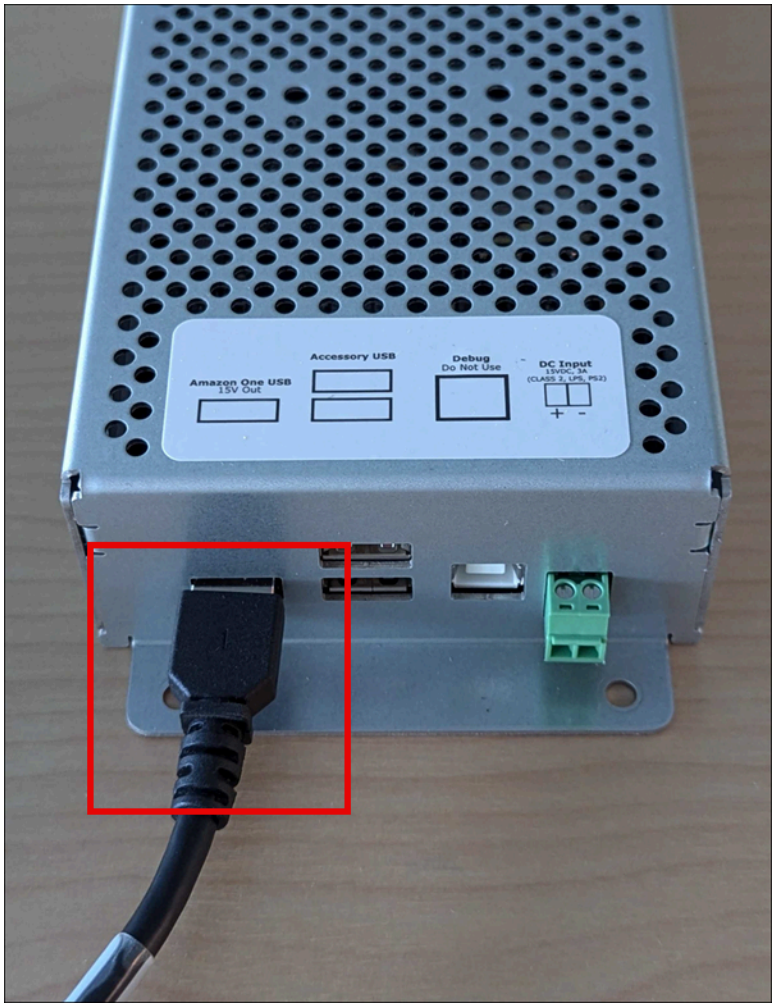
包含在带有 I/O 集线器的 Amazon One 设备中

- 2x 6 位接线端子台连接器
- 直流插头连接器
- 72 英寸电源/数据线

确认这些先决条件后，您就可以继续安装过程，确保使用 I/O Hub 安全高效地设置您的 Amazon One 设备。适当的准备工作将有助于确保设备按预期运行，并顺利集成到您的安全访问系统中。

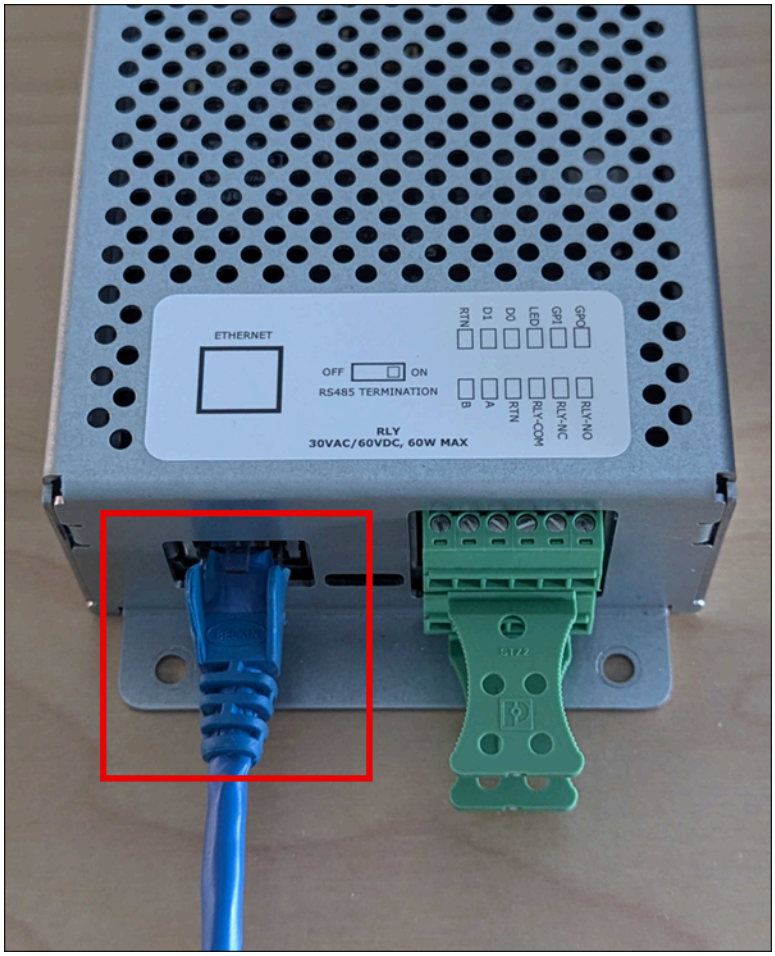
为您的 Amazon One 设备安装 I/O 集线器

1. 从包装中取出带有 I/O Hub 的 Amazon One 设备。
2. 将 I/O 集线器固定在所需位置。
3. 将 Amazon One USB 电缆插入 I/O 集线器端口。



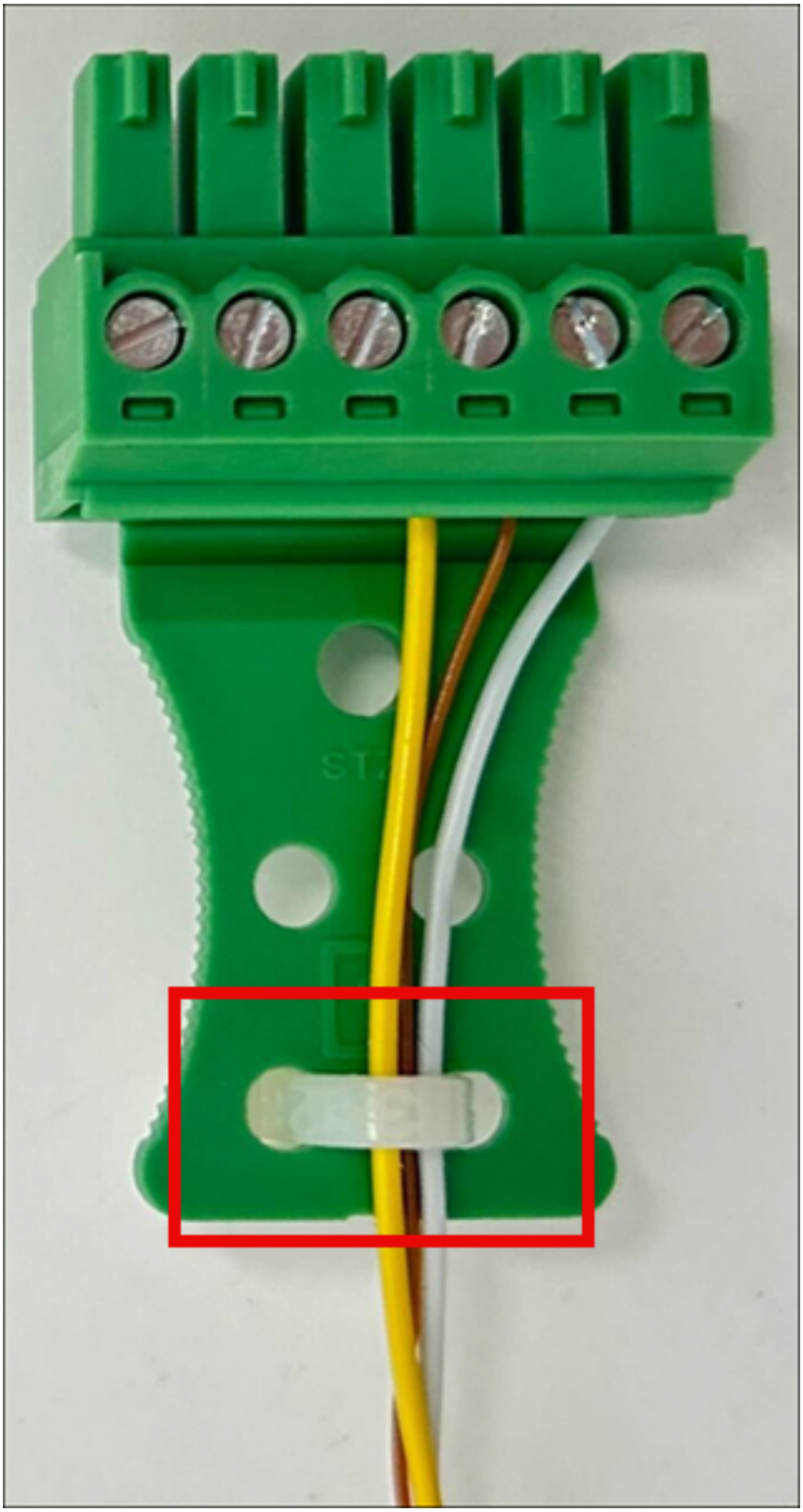
4. 要获得 POE++ 电源，请将 POE++ 电源上的以太网电缆插入 I/O 集线器端口。

   可选：有关直流电源，请参阅下面的 “安装直流接线” 部分。



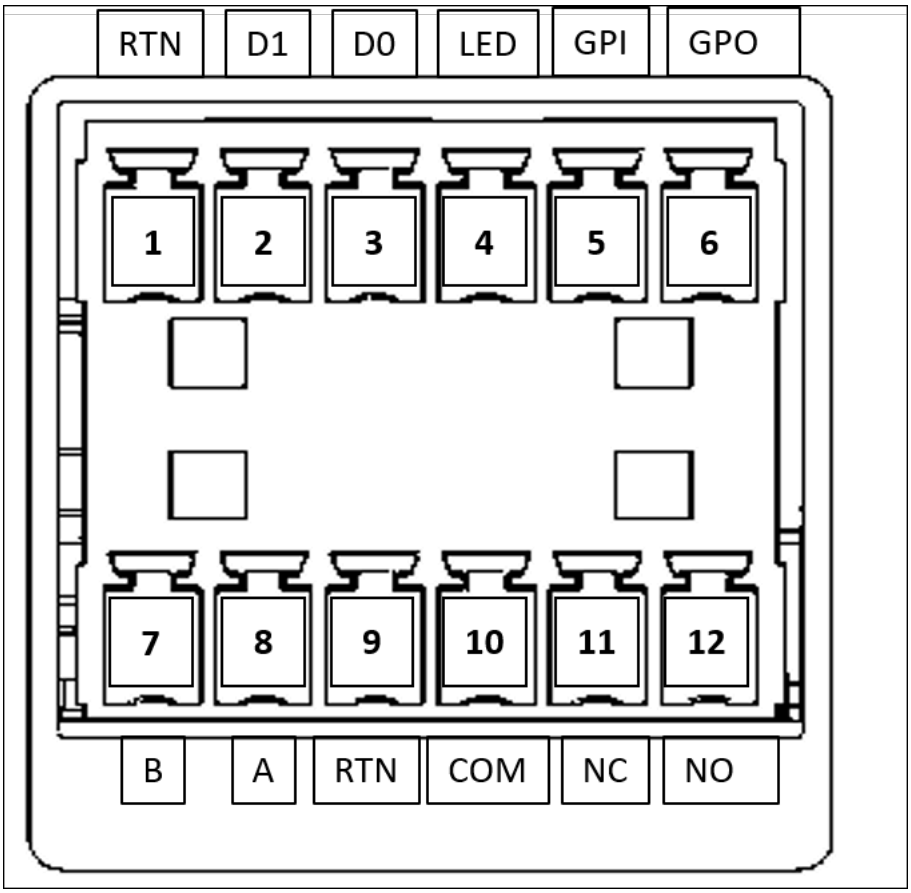
连接您的 Amazon One 设备的 I/O 集线器

- 安装滴水环，以避免液体意外顺着电源线流入 I/O 集线器。
- 安装应力消除夹以保护电线免受损坏或应力，如下图所示。



1. 将接线板插头插入 I/O 集线器。
2. 通过接线端子插头仅插入应用所需的电线。请参阅以下接线表和示意图。

连接

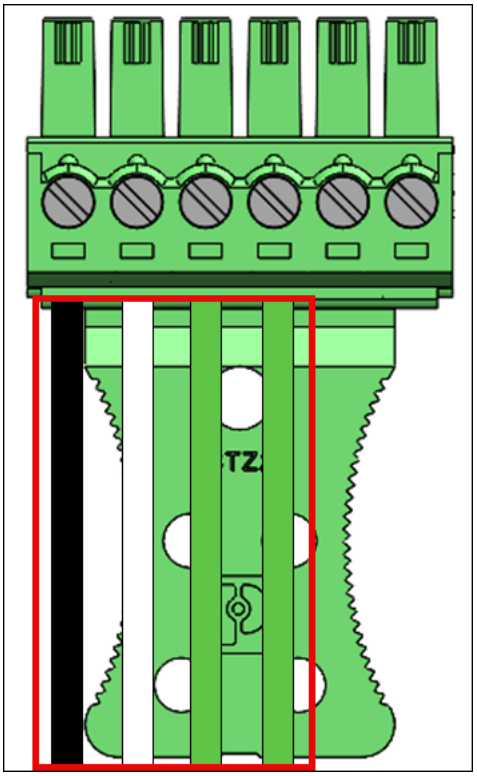


Pin	Connection	描述	使用
1	RTN	信号返回	韦根接地 — 黑线
2	D1	Wiegand D1	韦根数据 1 — 白线
3	D0	Wiegand D0	韦根数据 0 — 绿线
4	导致了	Wiegand LED	韦根 LED — 可选
5	GPI	通用输入	数字输入信号-可选

Pin	Connection	描述	使用
6	GPO	通用输出	数字输出信号-可选
7	B	RS485_b/D0/Data	OSDP D0 — Green wire
8	A	RS485_A/D1/Clock	OSDP D1 — 白线
9	RTN	信号返回	OSDP 回归 — 黑线
10	COM	继电器共用	触点继电器常用 — 白线
11	NC	继电器常闭	触点继电器常闭 — 橙线
12	NO	继电器常开	触点继电器常开 — 黄线

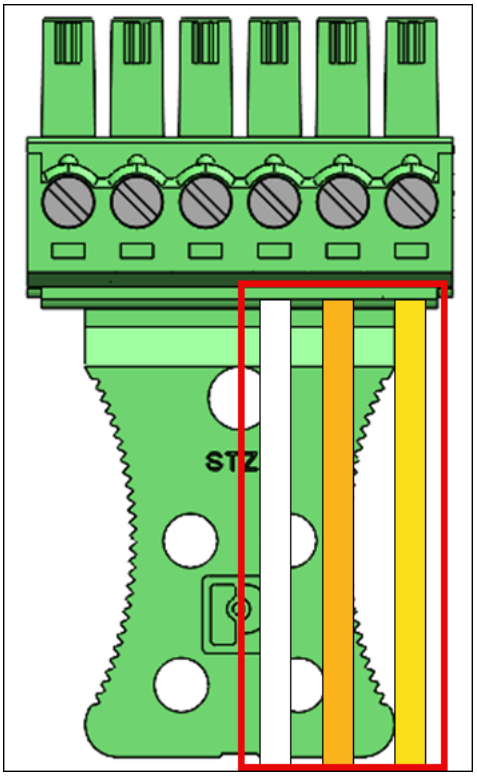
韦根连接

- 将黑线插入引脚 1 (RTN)。
- 将白线插入引脚 2 (D1)。
- 将绿色电线插入引脚 3 (D0)。
- 可选：将绿色电线插入引脚 4（LED）。

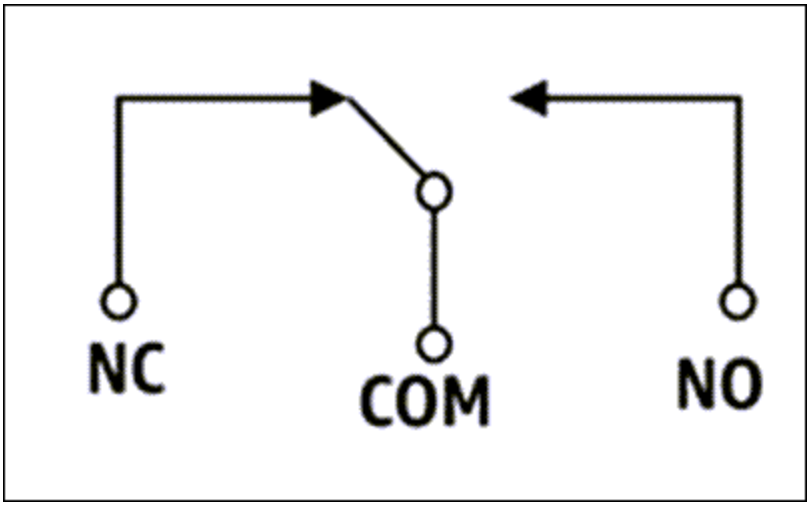


中继连接

- 将白线插入引脚 10 (COM)。
- 将橙色电线插入引脚 11 (NC)。
- 将黄线插入引脚 12（否）。



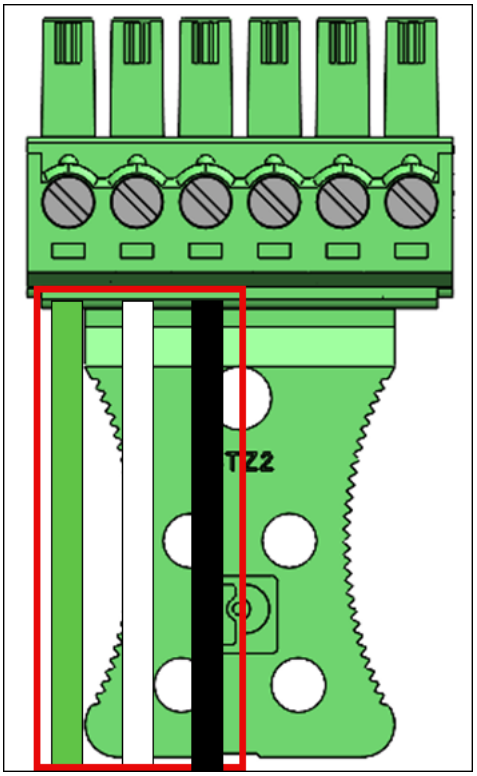
继电器图



继电器应按照规定的安全额定值运行 30VAC/60VDC，最大 60W。

RS485 连接

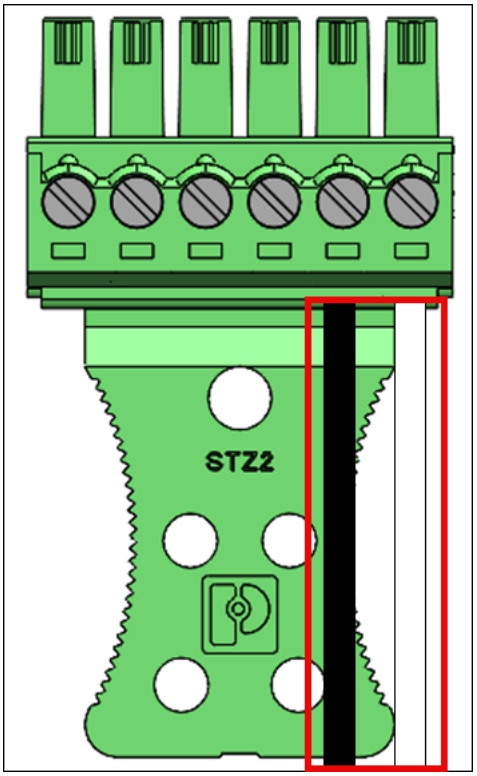
- 将绿色电线插入引脚 7 (B)。
- 将白线插入引脚 8 (A)。
- 将黑线插入引脚 9 (RTN)。



如果设备是线路上的最后一台设备，请将 RS485 终端开关 “打开”。该开关激活线路上的 120 欧姆电阻器端接。

数字输入/输出连接

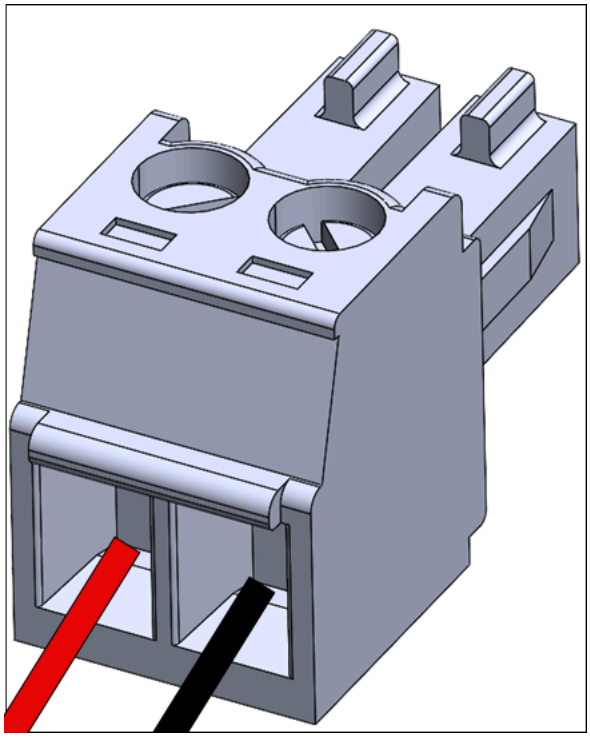
- 将黑线插入引脚 5 (GPI)。
- 将白线插入引脚 6 (GPO)。



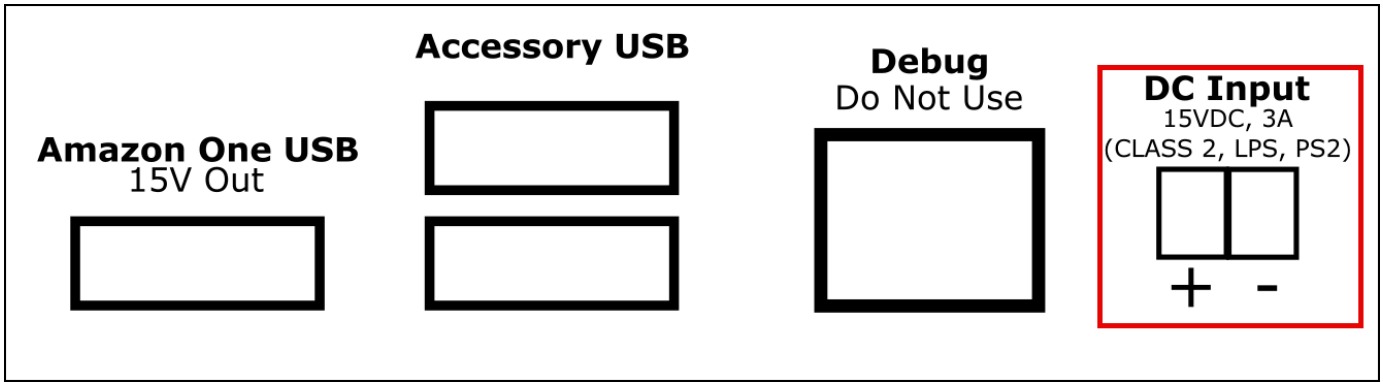
- 数字输入/输出连接应按所列方式运行。

可选：安装直流电线

1. 从红线末端剥掉 3mm-5mm 表示正极 (+)，从黑色电线末端剥掉 3mm-5mm 表示负极 (-)。
2. 将直流电线剥掉的一端插入直流插头。



3. 将电线拧到位。
4. 将有线直流插头插入直流输入端口。



安装您的 Amazon One 设备后，就可以激活设备了。

激活 Amazon One 设备

当您的 Amazon One 设备安装并开机后，就可以将其激活了。

激活您的 Amazon One 设备

1. 在 Amazon One 设备上，点击屏幕开始操作。

2. 选择 “以太网” 或 “Wifi” 连接到互联网。

   一旦设备连接到互联网，它将开始下载最新的软件包。
3. 当屏幕显示软件下载完成时！ ，选择 “确定”。
4. 选择二维码。

   Amazon One 设备屏幕将显示扫描二维码。
5. 要检索激活二维码，请在 https://console.aws.amazon.com/on e-enterprise 上打开 Amazon One 企业控制台。

   > **Note**
   >
   > 我们强烈建议您向安装人员授予有限的权限，以便他们只能访问您的 Amazon One Enterprise 控制台中的激活二维码。请参阅 添加 Amazon One 用户。
6. 在导航窗格中，选择激活二维码。
7. 从 “选择站点” 下拉列表中，选择安装 Amazon One 设备的站点。
8. 在 “站点信息” 下，确认网站地址。
9. 在激活二维码下，查找您正在激活的设备实例名称，然后选择相应的获取二维码以检索二维码。
10. 使用 Amazon One 设备扫描二维码。请注意，为了安全起见，二维码会定期刷新，您只能使用一次二维码。
11. 输入网站邮政编码，确认显示的站点是否正确，然后选择 “确认设置”。
12. 当 Amazon One 设备屏幕显示激活完成时！ ，设备已准备就绪，可以使用。

注册和输入用户

现在，您的Amazon One设备已激活，您的员工可以开始注册手掌并对手掌进行身份验证以获得访问权限。

主题

- 创建端点策略
- 正在进行入境身份验证

创建端点策略

用户必须先完成注册流程，然后才能对其手掌进行身份验证才能进入。在允许用户注册之前，安全人员应始终检查用户的身份。

在 Amazon One 设备上注册您的手掌

1. 在 Amazon One Enterprise 注册设备上，按开始。
2. 使用连接到 Amazon One Enterprise 注册设备的徽章扫描器扫描员工徽章。

   成功扫描徽章后，Amazon One 设备屏幕上会显示徽章已扫描。
3. 通读使用条款，然后按确定。
4. 通读同意——你的 Palm 生物识别信息，如果你同意，请按 “我同意”。
5. 按照屏幕上的说明完成注册过程。

正在进行入境身份验证

成功注册手掌后，您就可以在 Amazon One Enterprise 入口设备上用手掌进行身份验证了。

对您的手掌进行身份验证以便在 Amazon One 设备上进入

- 将手掌悬停在设备顶部，然后按照屏幕上的说明扫描手掌。

管理用户

您可以使用已注册用户管理页面来跟踪已注册用户并删除用户生物识别信息。关联的生物识别信息被删除的用户将无法再访问 Amazon One 设备进行身份验证。

主题

- 查看已注册用户
- 删除已注册用户及其生物识别信息

查看已注册用户

以下步骤详细说明了如何注册用户。

查看已注册用户

1. 在 https://console.aws.amazon.com/on e-enterprise 上打开 Amazon One 企业控制台。
2. 在导航窗格中，选择已注册用户管理。
3. 在 “已注册用户” 下，您可以找到所有已注册用户和以下详细信息：
   - 徽章 ID — 注册时由 RFID 徽章阅读器捕获的徽章标识符信息。
   - 注册来源-用于注册的 Amazon One 设备的详细信息。
   - 注册日期-注册日期和时间。

删除已注册用户及其生物识别信息

以下步骤详细说明了如何删除已注册用户及其生物识别信息。

删除已注册用户及其生物识别信息

1. 在 https://console.aws.amazon.com/on e-enterprise 上打开 Amazon One 企业控制台。
2. 在导航窗格中，选择已注册用户管理。
3. 在 “已注册用户” 下，选择要删除其手掌生物识别数据的用户的徽章 ID。
4. 选择 “删除生物识别信息”。
5. 选择 “删除” 以确认删除用户的生物识别数据。

> **Important**
>
> 此操作会导致从 Amazon One Enterprise 中永久删除用户的手掌生物识别信息。用户需要使用亚马逊 One Enterprise 注册设备重新注册，才能使用 Amazon One Enterprise 进行身份验证。删除用户的生物识别信息还会永久删除 Amazon One Enterprise 中的其他个人资料属性，例如徽章 ID。

管理 Amazon One 设备

安装并激活 Amazon One 设备后，它将开始在 Amazon One Enterprise 控制台上报告设备运行状况。您可以使用 Amazon One Enterprise 控制台执行设备管理任务，例如重启设备或更新配置。

主题

- 维护和清洁 Amazon One 设备
- 现场管理
- 设备实例管理

维护和清洁 Amazon One 设备

维护您的 Amazon One 设备可提供最佳的设备操作环境和设备体验。

在清洁 Amazon One 设备之前，请确保满足以下条件：

- 虽然您不必启用或禁用 Amazon One，但请确保设备已接通电源、网络连接以及所有外围设备和配套设备（如果适用）已连接。
- 如果网络连接不可用（如果出现这种情况，Amazon One 设备上将显示错误屏幕）、Amazon One 设备上会显示错误屏幕或控制台上出现设备连接问题，请将问题上报给您的管理员。
- 对设备进行物理保护，使未经授权的人员无法对其进行篡改。
- 每天目视检查 Amazon One 设备，检查是否存在与 Amazon One 设备的任何未经授权的连接。
- 检查设备的各个侧面是否有被篡改的迹象，包括设备和外壳的可见螺丝，确保没有缝隙/开口暴露任何一台 Amazon One 设备的内部组件/电路。
- 如果出现任何错误或故障，请按照 Amazon One 设备屏幕上的说明进行操作，或者参阅故障排除指南来修复问题。

清洁 Amazon One 设备

定期清洁 Amazon One 设备会清除任何污迹或痕迹，例如指纹和手印。

> **Note**
>
> 请勿使用本指南中列出的清洁产品以外的任何其他清洁产品。建议的清洁时间表是每周一次或两次，或者每当设备上有污垢、灰尘或污迹时，但每天不要超过一次。

1. 用异丙醇 (IPA) 湿巾擦拭亚马逊 One 设备。仅清洁设备的触摸表面。除非 Amazon One 的指示，否则请勿触摸光学窗或使用任何其他清洁产品。
2. 用干燥的超细纤维布擦去所有条纹。
3. 轻轻除尘（不要擦拭）光学窗口上任何可见的污垢或碎屑。将光学窗口的清洁限制为每天不超过一次and/or when the window is visually dirty (e.g., finger/hand prints/smudges）。本来不打算触摸设备的这一部分，但新客户可能会无意中触摸。
4. 如果适用，请使用 KIC 智能卡清洁器清洁读卡器的内部。
5. 每周清洁设备一到两次，或者每当设备上有污垢、灰尘或污迹时。

现场管理

站点代表安装和运行设备实例集合的物理位置。您可以使用网站来整理共享相同物理地址的 Amazon One 设备。

主题

- 更改网站名称
- 更新网站地址

更改网站名称

以下步骤详细说明了如何更改设备的站点名称。

更改网站名称

1. 在 https://console.aws.amazon.com/on e-enterprise 上打开 Amazon One 企业控制台。
2. 在导航窗格中，选择 “站点”。
3. 在 “站点” 下，选择要为其编辑名称的站点。
4. 选择编辑。
5. 在 “站点信息” 下，输入所需的站点名称和站点描述（可选）。
6. 选择 “保存更改” 进行更新。

更新网站地址

以下步骤详细说明了如何更新设备的网站地址。

更新网站地址

1. 在 https://console.aws.amazon.com/on e-enterprise 上打开 Amazon One 企业控制台。
2. 在导航窗格中，选择 “站点”。
3. 在 “站点” 下，选择您要更新其地址的站点。
4. 在 “设备实例” 下，确保激活的实例数为 0。
5. （可选）如果激活的实例数不为 0，请参阅
6. 选择编辑。
7. 在 “物理地址” 下输入正确的实际地址。
8. 选择 “保存更改” 进行更新。

设备实例管理

设备实例是具有配置的设备的逻辑表示形式。使用设备实例允许交换 Amazon One 设备，同时自动继承先前设置的配置和名称。设备实例具有用户定义的名称（与您的访问控制软件共享命名约定）和一组通信配置。

主题

- 查看设备实例状态
- 重启 Amazon One 设备
- 更新 Amazon One 设备配置
- 更新 Wi-Fi 凭证
- 停用设备实例

查看设备实例状态

以下步骤详细说明了如何查看设备实例的状态。

查看设备实例状态

1. 在 https://console.aws.amazon.com/on e-enterprise 上打开 Amazon One 企业控制台。
2. 在导航窗格中，选择设备实例。
3. 在 “已激活的实例” 下，您将看到已激活的 Amazon One 设备列表。
4. 选择设备实例名称以查看设备实例的详细信息。

重启 Amazon One 设备

以下步骤详细介绍了如何重启您的 Amazon One 设备。

重启 Amazon One 设备

1. 在 https://console.aws.amazon.com/on e-enterprise 上打开 Amazon One 企业控制台。
2. 在导航窗格中，选择设备实例。
3. 在 “已激活的实例” 下，选择要重启的设备的实例名称。
4. 选择 “重启” 以重启 Amazon One 设备。

更新 Amazon One 设备配置

以下步骤详细介绍了如何更新 Amazon One 设备配置。

更新 Amazon One 设备配置

1. 在 https://console.aws.amazon.com/on e-enterprise 上打开 Amazon One 企业控制台。
2. 在导航窗格中，选择设备实例。
3. 在 “已激活的实例” 下，选择要更新的设备的实例名称。
4. 在 “设备配置” 下，选择 “编辑”。

> **Note**
>
> 要更改 Amazon One 设备模式，必须先停用设备实例，然后将其配置为所需的设备模式（参见配置设备实例以进行激活）。然后，您可以完成设备激活过程（请参阅激活 Amazon One 设备）。

5. 进行所需更改后，选择更新设备配置以确认更新。

更新 Wi-Fi 凭证

以下步骤详细说明了如何更新 Wi-Fi 凭证。

要更新 Wifi 凭证

1. 在 https://console.aws.amazon.com/on e-enterprise 上打开 Amazon One 企业控制台。

2. 在导航窗格中，选择设备实例。
3. 在 “已激活的实例” 下，选择要更新的设备的实例名称。
4. 在 “网络” 下，选择 “编辑”。
5. 在 Wi-Fi 配置下，进行所需的更改。
6. 选择更新网络以确认更新。

停用设备实例

以下步骤详细说明了如何停用设备实例。

停用设备实例

1. 在 https://console.aws.amazon.com/on e-enterprise 上打开 Amazon One 企业控制台。
2. 在导航窗格中，选择设备实例。
3. 在 “已激活的实例” 下，选择要停用的设备实例的名称。
4. 选择停用设备。
5. 要确认停用，请在消息框中键入 “停用”，然后选择 “停用设备”。

安全性

云安全 AWS 是重中之重。作为 AWS 客户，您可以受益于专为满足大多数安全敏感型组织的要求而构建的数据中心和网络架构。

安全是双方共同承担 AWS 的责任。责任共担模式将其描述为云的安全性和云中的安全性：

- 云安全 — AWS 负责保护在云中运行 AWS 服务的基础架构 AWS 云。 AWS 还为您提供可以安全使用的服务。作为AWS 合规计划合规计划合规计划合的一部分，第三方审计师定期测试和验证我们安全的有效性。要了解适用于 Amazon One Enterprise 的合规计划，请参阅按合规计划AWS 提供的范围内的AWS 服务划分的范围内服务。
- 云端安全-您的责任由您使用的 AWS 服务决定。您还需要对其他因素负责，包括您的数据的敏感性、您公司的要求以及适用的法律法规。

本文档可帮助您了解在使用 Amazon One Enterprise 时如何应用分担责任模型。以下主题向您展示如何配置 Amazon One Enterprise 以满足您的安全与合规目标。您还将学习如何使用其他 AWS 服务来帮助您监控和保护您的 Amazon One Enterprise 资源。

主题

- 亚马逊 One Enterprise 中的数据保护
- Amazon One Enterprise 的身份和访问管理
- Amazon One Enterprise 的操作、资源和条件键
- 亚马逊 One 企业版合规性验证

亚马逊 One Enterprise 中的数据保护

分担责任模型 AWS 分担责任模型适用于 Amazon One Enterprise 中的数据保护。如本模型所述 AWS ，负责保护运行所有内容的全球基础架构 AWS 云。您负责维护对托管在此基础结构上的内容的控制。您还负责您所使用的 AWS 服务 的安全配置和管理任务。有关数据隐私的更多信息，请参阅数据隐私常见问题。有关欧洲数据保护的信息，请参阅 AWS Security Blog 上的 AWS Shared Responsibility Model and GDPR 博客文章。

出于数据保护目的，我们建议您保护 AWS 账户 凭证并使用 AWS IAM Identity Center 或 AWS Identity and Access Management (IAM) 设置个人用户。这样，每个用户只获得履行其工作职责所需的权限。还建议您通过以下方式保护数据：

- 对每个账户使用多重身份验证（MFA）。
- 使用 SSL/TLS 与资源通信。 AWS 我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 使用设置 API 和用户活动日志 AWS CloudTrail。有关使用 CloudTrail 跟踪捕获 AWS 活动的信息，请参阅《AWS CloudTrail 用户指南》中的使用跟 CloudTrail 踪。
- 使用 AWS 加密解决方案以及其中的所有默认安全控件 AWS 服务。
- 使用高级托管安全服务（例如 Amazon Macie），它有助于发现和保护存储在 Amazon S3 中的敏感数据。
- 如果您在 AWS 通过命令行界面或 API 进行访问时需要经过 FIPS 140-3 验证的加密模块，请使用 FIPS 端点。有关可用的 FIPS 端点的更多信息，请参阅《美国联邦信息处理标准（FIPS）第 140-3 版》。

强烈建议您切勿将机密信息或敏感信息（如您客户的电子邮件地址）放入标签或自由格式文本字段（如名称字段）。这包括您 AWS 服务 使用控制台、API 或与 Amazon One Enterprise 或其他公司合作时 AWS SDKs。 AWS CLI在用于名称的标签或自由格式文本字段中输入的任何数据都可能会用于计费或诊断日志。如果您向外部服务器提供网址，强烈建议您不要在网址中包含凭证信息来验证对该服务器的请求。

使用默认的静态数据加密

Amazon One Enterprise 默认提供加密，以使用 AWS 加密密钥保护静态敏感数据。

AWS 拥有的密钥 — Amazon One Enterprise 默认使用这些密钥来自动加密敏感的最终用户数据。您无法查看、管理或使用 AWS 拥有的密钥，也无法审计其使用情况。但是，无需采取任何措施或更改任何计划即可保护用于加密数据的密钥。有关更多信息，请参阅 AWS Key Management Service 开发人员指南中的 AWS 拥有的密钥。

传输中数据加密

Amazon One Enterprise 使用传输层安全 (TLS) 来保护数据，使用签名版本 4 来验证所有向 AWS 服务发出的入站 API 请求。默认情况下，此加密处于启用状态。

Amazon One Enterprise 的身份和访问管理

AWS Identity and Access Management (IAM) AWS 服务 可帮助管理员安全地控制对 AWS 资源的访问权限。IAM 管理员控制谁可以通过身份验证（登录）和授权（拥有权限）使用 Amazon One Enterprise 资源。您可以使用 IAM AWS 服务 ，无需支付额外费用。

主题

- 受众
- 使用身份进行身份验证
- 使用策略管理访问
- 亚马逊 One Enterprise 如何使用 IAM
- Amazon One Enterprise 的基于身份的策略示例
- AWS Amazon One 企业版的托管策略

受众

您的使用方式 AWS Identity and Access Management (IAM) 会有所不同，具体取决于您在 Amazon One Enterprise 中所做的工作。

服务用户 — 如果您使用 Amazon One Enterprise 服务完成工作，则您的管理员会为您提供所需的凭证和权限。当您使用更多 Amazon One Enterprise 功能来完成工作时，您可能需要额外的权限。了解如何管理访问权限有助于您向管理员请求适合的权限。如果您无法访问 Amazon One Enterprise 中的某项功能，请参阅对 Amazon One 身份和访问进行故障排除。

服务管理员 — 如果您负责公司的 Amazon One Enterprise 资源，则可能拥有对 Amazon One Enterprise 的完全访问权限。您的工作是确定您的服务用户应访问哪些 Amazon One Enterprise 功能和资源。然后，您必须向 IAM 管理员提交请求以更改服务用户的权限。请查看该页面上的信息以了解 IAM 的基本概念。要详细了解贵公司如何在 Amazon One Enterprise 中使用 IAM，请参阅亚马逊 One Enterprise 如何使用 IAM。

IAM 管理员 — 如果您是 IAM 管理员，则可能需要详细了解如何编写策略来管理 Amazon One Enterprise 的访问权限。要查看您可以在 IAM 中使用的基于身份的 Amazon One Enterprise 策略示例，请参阅。Amazon One Enterprise 的基于身份的策略示例

使用身份进行身份验证

身份验证是您 AWS 使用身份凭证登录的方式。您必须以 IAM 用户身份或通过担 AWS 账户根用户任 IAM 角色进行身份验证（登录 AWS）。

您可以使用通过身份源提供的凭据以 AWS 联合身份登录。 AWS IAM Identity Center （IAM Identity Center）用户、贵公司的单点登录身份验证以及您的 Google 或 Facebook 凭据就是联合身份的示例。当您以联合身份登录时，您的管理员以前使用 IAM 角色设置了身份联合验证。当你使用联合访问 AWS 时，你就是在间接扮演一个角色。

根据您的用户类型，您可以登录 AWS Management Console 或 AWS 访问门户。有关登录的更多信息 AWS，请参阅《AWS 登录 用户指南》中的如何登录到您 AWS 账户的。

如果您 AWS 以编程方式访问，则会 AWS 提供软件开发套件 (SDK) 和命令行接口 (CLI)，以便使用您的凭据对请求进行加密签名。如果您不使用 AWS 工具，则必须自己签署请求。有关使用推荐的方法自行签署请求的更多信息，请参阅《IAM 用户指南》中的用于签署 API 请求的AWS 签名版本 4。

无论使用何种身份验证方法，您都可能需要提供其他安全信息。例如， AWS 建议您使用多重身份验证 (MFA) 来提高账户的安全性。要了解更多信息，请参阅《AWS IAM Identity Center 用户指南》中的多重身份验证和《IAM 用户指南》中的 IAM 中的AWS 多重身份验证。

AWS 账户 root 用户

创建时 AWS 账户，首先要有一个登录身份，该身份可以完全访问账户中的所有资源 AWS 服务 和资源。此身份被称为 AWS 账户 root 用户，使用您创建账户时使用的电子邮件地址和密码登录即可访问该身份。强烈建议您不要使用根用户执行日常任务。保护好根用户凭证，并使用这些凭证来执行仅根用户可以执行的任务。有关要求您以根用户身份登录的任务的完整列表，请参阅 IAM 用户指南中的需要根用户凭证的任务。

联合身份

作为最佳实践，要求人类用户（包括需要管理员访问权限的用户）使用与身份提供商的联合身份验证 AWS 服务 通过临时证书进行访问。

联合身份是指您的企业用户目录、Web 身份提供商、Identity C enter 目录中的用户，或者任何使用 AWS 服务 通过身份源提供的凭据进行访问的用户。 AWS Directory Service当联合身份访问时 AWS 账户，他们将扮演角色，角色提供临时证书。

要集中管理访问权限，建议您使用 AWS IAM Identity Center。您可以在 IAM Identity Center 中创建用户和群组，也可以连接并同步到您自己的身份源中的一组用户和群组，以便在您的所有 AWS 账户 和应用程序中使用。有关 IAM Identity Center 的信息，请参阅 AWS IAM Identity Center 用户指南中的什么是 IAM Identity Center？。

IAM 用户和群组

I AM 用户是您 AWS 账户 内部对个人或应用程序具有特定权限的身份。在可能的情况下，我们建议使用临时凭证，而不是创建具有长期凭证（如密码和访问密钥）的 IAM 用户。但是，如果您有一些特定的使用场景需要长期凭证以及 IAM 用户，建议您轮换访问密钥。有关更多信息，请参阅《IAM 用户指南》中的对于需要长期凭证的用例，应在需要时更新访问密钥。

IAM 组是一个指定一组 IAM 用户的身份。您不能使用组的身份登录。您可以使用组来一次性为多个用户指定权限。如果有大量用户，使用组可以更轻松地管理用户权限。例如，您可以拥有一个名为的群组，IAMAdmins并向该群组授予管理 IAM 资源的权限。

用户与角色不同。用户唯一地与某个人员或应用程序关联，而角色旨在让需要它的任何人代入。用户具有永久的长期凭证，而角色提供临时凭证。要了解更多信息，请参阅《IAM 用户指南》中的 IAM 用户的使用案例。

IAM 角色

I AM 角色是您内部具有特定权限 AWS 账户 的身份。它类似于 IAM 用户，但与特定人员不关联。要在中临时担任 IAM 角色 AWS Management Console，您可以从用户切换到 IAM 角色（控制台）。您可以通过调用 AWS CLI 或 AWS API 操作或使用自定义 URL 来代入角色。有关使用角色的方法的更多信息，请参阅《IAM 用户指南》中的代入角色的方法。

具有临时凭证的 IAM 角色在以下情况下很有用：

- 联合用户访问：要向联合身份分配权限，请创建角色并为角色定义权限。当联合身份进行身份验证时，该身份将与角色相关联并被授予由此角色定义的权限。有关用于联合身份验证的角色的信息，请参阅《IAM 用户指南》中的针对第三方身份提供商创建角色（联合身份验证）。如果您使用 IAM Identity Center，则需要配置权限集。为控制您的身份在进行身份验证后可以访问的内容，IAM Identity Center 将权限集与 IAM 中的角色相关联。有关权限集的信息，请参阅《AWS IAM Identity Center 用户指南》中的权限集。
- 临时 IAM 用户权限：IAM 用户可代入 IAM 用户或角色，以暂时获得针对特定任务的不同权限。
- 跨账户存取：您可以使用 IAM 角色以允许不同账户中的某个人（可信主体）访问您的账户中的资源。角色是授予跨账户访问权限的主要方式。但是，对于某些资源 AWS 服务，您可以将策略直接附加到资源（而不是使用角色作为代理）。要了解用于跨账户访问的角色和基于资源的策略之间的差别，请参阅 IAM 用户指南中的 IAM 中的跨账户资源访问。
- 跨服务访问 — 有些 AWS 服务 使用其他 AWS 服务服务中的功能。例如，当您在服务中拨打电话时，该服务通常会在 Amazon 中运行应用程序 EC2 或在 Amazon S3 中存储对象。服务可能会使用发出调用的主体的权限、使用服务角色或使用服务相关角色来执行此操作。
  - 转发访问会话 (FAS) — 当您使用 IAM 用户或角色在中执行操作时 AWS，您被视为委托人。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS 使用调用委托人的权限以及 AWS 服务 向下游服务发出请求的请求。 AWS 服务只有当服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两项操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。

- 服务角色 - 服务角色是服务代表您在您的账户中执行操作而分派的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的创建向 AWS 服务委派权限的角色。
- 服务相关角色-服务相关角色是一种与服务相关联的服务角色。 AWS 服务服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。

- 在 A@@ mazon 上运行的应用程序 EC2 — 您可以使用 IAM 角色管理在 EC2 实例上运行并发出 AWS CLI 或 AWS API 请求的应用程序的临时证书。这比在 EC2 实例中存储访问密钥更可取。要为 EC2 实例分配 AWS 角色并使其可供其所有应用程序使用，您需要创建一个附加到该实例的实例配置文件。实例配置文件包含该角色，并允许在 EC2 实例上运行的程序获得临时证书。有关更多信息，请参阅 IAM 用户指南中的使用 IAM 角色向在 A mazon EC2 实例上运行的应用程序授予权限。

使用策略管理访问

您可以 AWS 通过创建策略并将其附加到 AWS 身份或资源来控制中的访问权限。策略是其中的一个对象 AWS ，当与身份或资源关联时，它会定义其权限。 AWS 在委托人（用户、root 用户或角色会话）发出请求时评估这些策略。策略中的权限确定是允许还是拒绝请求。大多数策略都以 JSON 文档的 AWS 形式存储在中。有关 JSON 策略文档的结构和内容的更多信息，请参阅 IAM 用户指南中的 JSON 策略概览。

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

默认情况下，用户和角色没有权限。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。管理员随后可以向角色添加 IAM 策略，用户可以代入角色。

IAM 策略定义操作的权限，无关乎您使用哪种方法执行操作。例如，假设您有一个允许 `iam:GetRole` 操作的策略。拥有该策略的用户可以从 AWS Management Console AWS CLI、或 AWS API 获取角色信息。

基于身份的策略

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的使用客户托管策略定义自定义 IAM 权限。

基于身份的策略可以进一步归类为内联策略或托管式策略。内联策略直接嵌入单个用户、组或角色中。托管策略是独立的策略，您可以将其附加到中的多个用户、群组和角色 AWS 账户。托管策略包括

AWS 托管策略和客户托管策略。要了解如何在托管策略和内联策略之间进行选择，请参阅《IAM 用户指南》中的在托管策略与内联策略之间进行选择。

基于资源的策略

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。委托人可以包括账户、用户、角色、联合用户或 AWS 服务。

基于资源的策略是位于该服务中的内联策略。您不能在基于资源的策略中使用 IAM 中的 AWS 托管策略。

访问控制列表 (ACLs)

访问控制列表 (ACLs) 控制哪些委托人（账户成员、用户或角色）有权访问资源。 ACLs 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

Amazon S3 和 Amazon VPC 就是支持的服务示例 ACLs。 AWS WAF要了解更多信息 ACLs，请参阅《亚马逊简单存储服务开发者指南》中的访问控制列表 (ACL) 概述。

其他策略类型

AWS 支持其他不太常见的策略类型。这些策略类型可以设置更常用的策略类型向您授予的最大权限。

- 权限边界：权限边界是一个高级特征，用于设置基于身份的策略可以为 IAM 实体（IAM 用户或角色）授予的最大权限。您可为实体设置权限边界。这些结果权限是实体基于身份的策略及其权限边界的交集。在 `Principal` 中指定用户或角色的基于资源的策略不受权限边界限制。任一项策略中的显式拒绝将覆盖允许。有关权限边界的更多信息，请参阅IAM 用户指南中的 IAM 实体的权限边界。
- 服务控制策略 (SCPs)- SCPs 是指定组织或组织单位 (OU) 的最大权限的 JSON 策略 AWS Organizations。 AWS Organizations 是一项用于对您的企业拥有的多 AWS 账户 项进行分组和集中管理的服务。如果您启用组织中的所有功能，则可以将服务控制策略 (SCPs) 应用于您的任何或所有帐户。SCP 限制成员账户中的实体（包括每个 AWS 账户根用户实体）的权限。有关 Organization SCPs s 和的更多信息，请参阅《AWS Organizations 用户指南》中的服务控制策略。
- 资源控制策略 (RCPs) — RCPs 是 JSON 策略，您可以使用它来设置账户中资源的最大可用权限，而无需更新附加到您拥有的每个资源的 IAM 策略。RCP 限制成员账户中资源的权限，并可能影响身份（包括身份）的有效权限 AWS 账户根用户，无论这些身份是否属于您的组织。有关 Organizations 的更多信息 RCPs，包括 AWS 服务 该支持的列表 RCPs，请参阅《AWS Organizations 用户指南》中的资源控制策略 (RCPs)。

- 会话策略：会话策略是当您以编程方式为角色或联合用户创建临时会话时作为参数传递的高级策略。结果会话的权限是用户或角色的基于身份的策略和会话策略的交集。权限也可以来自基于资源的策略。任一项策略中的显式拒绝将覆盖允许。有关更多信息，请参阅 IAM 用户指南中的会话策略。

多个策略类型

当多个类型的策略应用于一个请求时，生成的权限更加复杂和难以理解。要了解在涉及多种策略类型时如何 AWS 确定是否允许请求，请参阅 IAM 用户指南中的策略评估逻辑。

亚马逊 One Enterprise 如何使用 IAM

在使用 IAM 管理对亚马逊 One Enterprise 的访问权限之前，请先了解有哪些 IAM 功能可用于亚马逊 One Enterprise。

您可以在 Amazon One Enterprise 上使用的 IA

IAM 特征	亚马逊 One 企业版支持
基于身份的策略	是
基于资源的策略	否
策略操作	是
策略资源	是
策略条件键	是
ACLs	否
ABAC（策略中的标签）	是
临时凭证	是
主体权限	是
服务角色	否
服务相关角色	否

要全面了解 Amazon One Enterprise 和其他 AWS 服务如何与大多数 IAM 功能配合使用，请参阅 IAM 用户指南中与 IAM 配合使用的AWS 服务。

Amazon One Enterprise 基于身份的政策

支持基于身份的策略：是

基于身份的策略是可附加到身份（如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的使用客户管理型策略定义自定义 IAM 权限。

通过使用 IAM 基于身份的策略，您可以指定允许或拒绝的操作和资源以及允许或拒绝操作的条件。您无法在基于身份的策略中指定主体，因为它适用于其附加的用户或角色。要了解可在 JSON 策略中使用的所有元素，请参阅《IAM 用户指南》中的 IAM JSON 策略元素引用。

Amazon One Enterprise 的基于身份的策略示例

要查看 Amazon One Enterprise 基于身份的策略示例，请参阅。Amazon One Enterprise 的基于身份的策略示例

Amazon One 企业版中基于资源的政策

支持基于资源的策略：否

基于资源的策略是附加到资源的 JSON 策略文档。基于资源的策略的示例包括 IAM 角色信任策略和 Amazon S3 存储桶策略。在支持基于资源的策略的服务中，服务管理员可以使用它们来控制对特定资源的访问。对于在其中附加策略的资源，策略定义指定主体可以对该资源执行哪些操作以及在什么条件下执行。您必须在基于资源的策略中指定主体。委托人可以包括账户、用户、角色、联合用户或 AWS 服务。

要启用跨账户访问，您可以将整个账户或其他账户中的 IAM 实体指定为基于资源的策略中的主体。将跨账户主体添加到基于资源的策略只是建立信任关系工作的一半而已。当委托人和资源处于不同位置时 AWS 账户，可信账户中的 IAM 管理员还必须向委托人实体（用户或角色）授予访问资源的权限。他们通过将基于身份的策略附加到实体以授予权限。但是，如果基于资源的策略向同一个账户中的主体授予访问权限，则不需要额外的基于身份的策略。有关更多信息，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。

亚马逊 One Enterprise 的政策行动

支持策略操作：是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

JSON 策略的 `Action` 元素描述可用于在策略中允许或拒绝访问的操作。策略操作通常与关联的 AWS API 操作同名。有一些例外情况，例如没有匹配 API 操作的仅限权限 操作。还有一些操作需要在策略中执行多个操作。这些附加操作称为相关操作。

在策略中包含操作以授予执行关联操作的权限。

要查看 Amazon One 企业版操作列表，请参阅Amazon One Enterprise 的操作、资源和条件键。

Amazon One Enterprise 中的策略操作在操作前使用以下前缀：

```
one
```

要在单个语句中指定多项操作，请使用逗号将它们隔开。

```
"Action": [
      "one:action1",
      "one:action2"
         ]
```

您也可以使用通配符（*）指定多个操作。例如，要指定以单词 `Describe` 开头的所有操作，包括以下操作：

```
"Action": "one:Describe*"
```

要查看 Amazon One Enterprise 基于身份的策略示例，请参阅。Amazon One Enterprise 的基于身份的策略示例

亚马逊 One Enterprise 的政策资源

支持策略资源：是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

`Resource` JSON 策略元素指定要向其应用操作的一个或多个对象。语句必须包含 `Resource` 或 `NotResource` 元素。作为最佳实践，请使用其 Amazon 资源名称（ARN）指定资源。对于支持特定资源类型（称为资源级权限）的操作，您可以执行此操作。

对于不支持资源级权限的操作（如列出操作），请使用通配符（*）指示语句应用于所有资源。

```
"Resource": "*"
```

要查看 Amazon One Enterprise 资源类型及其列表 ARNs，以及要了解您可以使用哪些操作来指定每种资源的 ARN，请参阅。Amazon One Enterprise 的操作、资源和条件键

要查看 Amazon One Enterprise 基于身份的策略示例，请参阅。Amazon One Enterprise 的基于身份的策略示例

亚马逊 One Enterprise 的政策条件密钥

支持特定于服务的策略条件键：是

管理员可以使用 AWS JSON 策略来指定谁有权访问什么。也就是说，哪个主体可以对什么资源执行操作，以及在什么条件下执行。

在 `Condition` 元素（或 `Condition` 块）中，可以指定语句生效的条件。`Condition` 元素是可选的。您可以创建使用条件运算符（例如，等于或小于）的条件表达式，以使策略中的条件与请求中的值相匹配。

如果您在一个语句中指定多个 `Condition` 元素，或在单个 `Condition` 元素中指定多个键，则 AWS 使用逻辑 AND 运算评估它们。如果您为单个条件键指定多个值，则使用逻辑OR运算来 AWS 评估条件。在授予语句的权限之前必须满足所有的条件。

在指定条件时，您也可以使用占位符变量。例如，只有在使用 IAM 用户名标记 IAM 用户时，您才能为其授予访问资源的权限。有关更多信息，请参阅《IAM 用户指南》中的 IAM 策略元素：变量和标签。

AWS 支持全局条件密钥和特定于服务的条件密钥。要查看所有 AWS 全局条件键，请参阅 IAM 用户指南中的AWS 全局条件上下文密钥。

要查看 Amazon One Enterprise 条件密钥列表以及可以将条件键与哪些操作和资源一起使用，请参阅Amazon One Enterprise 的操作、资源和条件键。

要查看 Amazon One Enterprise 基于身份的策略示例，请参阅。Amazon One Enterprise 的基于身份的策略示例

ACLs 在 Amazon One 企业版中

支持 ACLs：否

访问控制列表 (ACLs) 控制哪些委托人（账户成员、用户或角色）有权访问资源。 ACLs 与基于资源的策略类似，尽管它们不使用 JSON 策略文档格式。

ABAC 与 Amazon One Enterp

支持 ABAC（策略中的标签）：是

基于属性的访问控制（ABAC）是一种授权策略，该策略基于属性来定义权限。在中 AWS，这些属性称为标签。您可以向 IAM 实体（用户或角色）和许多 AWS 资源附加标签。标记实体和资源是 ABAC 的第一步。然后设计 ABAC 策略，以在主体的标签与他们尝试访问的资源标签匹配时允许操作。

ABAC 在快速增长的环境中非常有用，并在策略管理变得繁琐的情况下可以提供帮助。

要基于标签控制访问，您需要使用 `aws:ResourceTag/key-name`、`aws:RequestTag/key-name` 或 `aws:TagKeys` 条件键在策略的条件元素中提供标签信息。

如果某个服务对于每种资源类型都支持所有这三个条件键，则对于该服务，该值为是。如果某个服务仅对于部分资源类型支持所有这三个条件键，则该值为部分。

有关 ABAC 的更多信息，请参阅《IAM 用户指南》中的使用 ABAC 授权定义权限。要查看设置 ABAC 步骤的教程，请参阅《IAM 用户指南》中的使用基于属性的访问权限控制（ABAC）。

在亚马逊 One Enterprise 上使用临时证书

支持临时凭证：是

当你使用临时证书登录时，有些 AWS 服务 不起作用。有关更多信息，包括哪些 AWS 服务 适用于临时证书，请参阅 IAM 用户指南中的AWS 服务 与 IA M 配合使用的信息。

如果您使用除用户名和密码之外的任何方法登录，则 AWS Management Console 使用的是临时证书。例如，当您 AWS 使用公司的单点登录 (SSO) 链接进行访问时，该过程会自动创建临时证书。当您以用户身份登录控制台，然后切换角色时，您还会自动创建临时凭证。有关切换角色的更多信息，请参阅《IAM 用户指南》中的从用户切换到 IAM 角色（控制台）。

您可以使用 AWS CLI 或 AWS API 手动创建临时证书。然后，您可以使用这些临时证书进行访问 AWS。 AWS 建议您动态生成临时证书，而不是使用长期访问密钥。有关更多信息，请参阅 IAM 中的临时安全凭证。

Amazon One 企业版的跨服务主体权限

支持转发访问会话（FAS）：是

当您使用 IAM 用户或角色在中执行操作时 AWS，您被视为委托人。使用某些服务时，您可能会执行一个操作，然后此操作在其他服务中启动另一个操作。FAS 使用调用委托人的权限以及 AWS 服务 向下游服务发出请求的请求。 AWS 服务只有当服务收到需要与其他 AWS 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两项操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。

亚马逊 One Enterprise 的服务角色

支持服务角色：否

服务角色是由一项服务担任、代表您执行操作的 IAM 角色。IAM 管理员可以在 IAM 中创建、修改和删除服务角色。有关更多信息，请参阅《IAM 用户指南》中的创建向 AWS 服务委派权限的角色。

> **Warning**
> 更改服务角色的权限可能会中断 Amazon One Enterprise 的功能。只有在 Amazon One Enterprise 提供相关指导时才编辑服务角色。

Amazon One 企业版的服务相关角色

支持服务相关角色：否

服务相关角色是一种链接到的服务角色。 AWS 服务服务可以代入代表您执行操作的角色。服务相关角色出现在您的中 AWS 账户 ，并且归服务所有。IAM 管理员可以查看但不能编辑服务相关角色的权限。

有关创建或管理服务相关角色的详细信息，请参阅能够与 IAM 搭配使用的AWS 服务。在表中查找服务相关角色列中包含 Yes 的表。选择是链接以查看该服务的服务相关角色文档。

Amazon One Enterprise 的基于身份的策略示例

默认情况下，用户和角色无权创建或修改 Amazon One Enterprise 资源。他们也无法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或 AWS API 执行任务。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。管理员随后可以向角色添加 IAM 策略，用户可以代入角色。

要了解如何使用这些示例 JSON 策略文档创建基于 IAM 身份的策略，请参阅《IAM 用户指南》中的创建 IAM 策略（控制台）。

有关 Amazon One Enterprise 定义的操作和资源类型（包括每种资源类型的格式）的详细信息，请参阅服务授权参考Amazon One Enterprise 的操作、资源和条件键中的。 ARNs

主题

- 策略最佳实践
- 使用 Amazon One 企业版控制台
- 允许用户查看他们自己的权限
- 对 Amazon One 企业版的只读访问权限
- 完全访问亚马逊 One Enterprise
- Amazon One 企业规则 API 操作支持的资源级权限
- 附加信息

策略最佳实践

基于身份的策略决定了是否有人可以在您的账户中创建、访问或删除亚马逊One Enterprise资源。这些操作可能会使 AWS 账户产生成本。创建或编辑基于身份的策略时，请遵循以下指南和建议：

- 开始使用 AWS 托管策略并转向最低权限权限 — 要开始向用户和工作负载授予权限，请使用为许多常见用例授予权限的AWS 托管策略。它们在你的版本中可用 AWS 账户。我们建议您通过定义针对您的用例的 AWS 客户托管策略来进一步减少权限。有关更多信息，请参阅《IAM 用户指南》中的AWS 托管式策略或工作职能的AWS 托管式策略。
- 应用最低权限：在使用 IAM 策略设置权限时，请仅授予执行任务所需的权限。为此，您可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用 IAM 应用权限的更多信息，请参阅《IAM 用户指南》中的 IAM 中的策略和权限。
- 使用 IAM 策略中的条件进一步限制访问权限：您可以向策略添加条件来限制对操作和资源的访问。例如，您可以编写策略条件来指定必须使用 SSL 发送所有请求。如果服务操作是通过特定的方式使用的，则也可以使用条件来授予对服务操作的访问权限 AWS 服务，例如 AWS CloudFormation。有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：条件。
- 使用 IAM Access Analyzer 验证您的 IAM 策略，以确保权限的安全性和功能性 – IAM Access Analyzer 会验证新策略和现有策略，以确保策略符合 IAM 策略语言（JSON）和 IAM 最佳实践。IAM Access Analyzer 提供 100 多项策略检查和可操作的建议，以帮助您制定安全且功能性强的策略。有关更多信息，请参阅《IAM 用户指南》中的使用 IAM Access Analyzer 验证策略。
- 需要多重身份验证 (MFA)-如果 AWS 账户您的场景需要 IAM 用户或根用户，请启用 MFA 以提高安全性。若要在调用 API 操作时需要 MFA，请将 MFA 条件添加到您的策略中。有关更多信息，请参阅《IAM 用户指南》中的使用 MFA 保护 API 访问。

有关 IAM 中的最佳实操的更多信息，请参阅《IAM 用户指南》中的 IAM 中的安全最佳实践。

使用 Amazon One 企业版控制台

要访问 Amazon One Enterprise 控制台，您必须拥有一组最低权限。这些权限必须允许您列出和查看有关您的 Amazon One Enterprise 资源的详细信息 AWS 账户。如果创建比必需的最低权限更为严格的基于身份的策略，对于附加了该策略的实体（用户或角色），控制台将无法按预期正常运行。

对于仅调用 AWS CLI 或 AWS API 的用户，您无需为其设置最低控制台权限。相反，只允许访问与其尝试执行的 API 操作相匹配的操作。

为确保用户和角色仍然可以使用 Amazon One Enterprise 控制台，还要为实体附加 Amazon One Enterprise *ConsoleAccess* 或*ReadOnly* AWS 托管策略。有关更多信息，请参阅《IAM 用户指南》中的为用户添加权限。

允许用户查看他们自己的权限

该示例说明了您如何创建策略，以允许 IAM 用户查看附加到其用户身份的内联和托管式策略。此策略包括在控制台上或使用 AWS CLI 或 AWS API 以编程方式完成此操作的权限。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "ViewOwnUserInfo",
            "Effect": "Allow",
            "Action": [
                "iam:GetUserPolicy",
                "iam:ListGroupsForUser",
                "iam:ListAttachedUserPolicies",
                "iam:ListUserPolicies",
                "iam:GetUser"
            ],
            "Resource": ["arn:aws:iam::*:user/${aws:username}"]
        },
        {
            "Sid": "NavigateInConsole",
            "Effect": "Allow",
            "Action": [
                "iam:GetGroupPolicy",
                "iam:GetPolicyVersion",
                "iam:GetPolicy",
```

```
                "iam:ListAttachedGroupPolicies",
                "iam:ListGroupPolicies",
                "iam:ListPolicyVersions",
                "iam:ListPolicies",
                "iam:ListUsers"
            ],
            "Resource": "*"
        }
    ]
}
```

对 Amazon One 企业版的只读访问权限

以下示例显示了一个 AWS 托管策略，`AmazonOneEnterpriseReadOnlyAccess`该策略授予对 Amazon One Enterprise 的只读访问权限。

```
{
  "Version": "2012-10-17",
  "Statement": [
    {
      "Effect": "Allow",
      "Action": [
        "one:Get*",
        "one:List*"
      ],
      "Resource": "*"
    }
  ]
}
```

在这些策略语句中，`Effect` 元素指定是允许还是拒绝操作。`Action` 元素列出了允许用户执行的特定操作。`Resource` 元素列出允许用户对其执行这些操作的 AWS 资源。对于控制对 Amazon One Enterprise 操作的访问权限的策略`*`，`Resource`元素始终设置为，通配符表示 “所有资源”。

`Action`元素中的值对应 APIs 于服务支持的值。这些操作前面加上，表示它们`config:`指的是 Amazon One Enterprise 操作。您可以在 `*` 元素中使用 `Action` 通配符，如以下示例所示：

- `"Action": ["one:*DeviceInstanceConfiguration"]`

  这允许所有以 “DeviceInstance” (`GetDeviceInstanceConfiguration`，`CreateDeviceInstanceConfiguration` 结尾的 Amazon One Enterprise 操作。

- `"Action": ["one:*"]`

  这允许所有 Amazon One Enterprise 操作，但不允许对其他 AWS 服务执行操作。
- `"Action": ["*"]`

  这允许所有 AWS 操作。此权限适用于担任您账户 AWS 管理员的用户。

只读策略不向用户授予执行诸如`CreateDeviceInstance``UpdateDeviceInstance`、和之类的操作的权限`DeleteDeviceInstance`。使用此政策的用户不得创建设备实例、更新设备实例或删除设备实例。有关 Amazon One 企业版操作的列表，请参阅Amazon One Enterprise 的操作、资源和条件键。

完全访问亚马逊 One Enterprise

以下示例显示了一项授予对 Amazon One Enterprise 完全访问权限的策略。它授予用户执行所有 Amazon One Enterprise 操作的权限。

> **Important**
>
> 此策略授予广泛的权限。在授予完全访问权限之前，请考虑从最低权限集开始，并根据需要授予其他权限。这样做比起一开始就授予过于宽松的权限而后再尝试收紧权限来说是更好的做法。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "one:*"
            ],
            "Resource": "*"
        },
    ]
}
```

Amazon One 企业规则 API 操作支持的资源级权限

资源级权限指的是能够指定允许用户对哪些资源执行操作的能力。Amazon One Enterprise 支持某些亚马逊 One Enterprise 规则 API 操作的资源级权限。这意味着，对于某些 Amazon One Enterprise 规则

操作，您可以控制何时允许用户使用这些操作的条件。这些条件可以是必须满足的操作，也可以是允许用户使用的特定资源。

下表描述了目前支持资源级权限的 Amazon One Enterprise 规则 API 操作。它还描述了每个操作支持的资源及其 ARNs对应的资源。指定 ARN 时，可以在路径中使用* 通配符；例如，当您无法或不想指定确切的资源时。 IDs

> **Important**
>
> 如果此表中未列出 Amazon One Enterprise 规则 API 操作，则该操作不支持资源级权限。如果 Amazon One Enterprise 规则操作不支持资源级权限，则可以向用户授予使用该操作的权限，但必须为策略声明的资源元素指定*。

API 操作	资源
CreateDeviceInstance	设备实例 arn: aws: one:: device-instance/ *region:accountID deviceInstanceId*
GetDeviceInstance	设备实例 arn: aws: one:: device-instance/ *region:accountID deviceInstanceId*
UpdateDeviceInstance	设备实例 arn: aws: one:: device-instance/ *region:accountID deviceInstanceId*
DeleteDeviceInstance	设备实例 arn: aws: one:: device-instance/ *region:accountID deviceInstanceId*
CreateDeviceActivationQrCode	设备实例 arn: aws: one:: device-instance/ *region:accountID deviceInstanceId*

API 操作	资源
DeleteAssociatedDevice	设备实例 arn: aws: one:: device-instance/ *region:accountID deviceInstanceId*
RebootDevice	设备实例 arn: aws: one:: device-instance/ *region:accountID deviceInstanceId*
CreateDeviceInstanceConfiguration	设备实例配置 arn: aws: one:: device-instance/ /configuration/ *region:accountID deviceInstanceId version*
GetDeviceInstanceConfiguration	设备实例配置 arn: aws: one:: device-instance/ /configuration/ *region:accountID deviceInstanceId version*
CreateSite	Site arn: aws: one:: site/ *region:accountID siteId*
DeleteSite	Site arn: aws: one:: site/ *region:accountID siteId*
GetSiteAddress	Site arn: aws: one:: site/ *region:accountID siteId*
UpdateSite	Site arn: aws: one:: site/ *region:accountID siteId*
UpdateSiteAddress	Site arn: aws: one:: site/ *region:accountID siteId*

API 操作	资源
CreateDeviceConfigurationTemplate	设备配置模板 arn: aws: one::/*region:accountID* device-configuration-template*templateId*
DeleteDeviceConfigurationTemplate	设备配置模板 arn: aws: one::/*region:accountID* device-configuration-template*templateId*
GetDeviceConfigurationTemplate	设备配置模板 arn: aws: one::/*region:accountID* device-configuration-template*templateId*
UpdateDeviceConfigurationTemplate	设备配置模板 arn: aws: one::/*region:accountID* device-configuration-template*templateId*

例如，您希望允许特定用户对特定规则进行的读访问，但拒绝特定用户对特定规则进行的写访问。

在第一个策略中，您可以允许 AWS Config 规则读取操作，例如`GetSite`对指定规则的读取操作。

```
{
        "Version": "2012-10-17",
        "Statement": [
            {
                "Sid": "VisualEditor0",
                "Effect": "Allow",
                "Action": [
                    "one:GetSite",
                    "one:GetSiteAddress"
                ],
                "Resource": [
                    "arn:aws:one:region:accountID:site/siteId"
                ]
            }
        ]
```

```
    }
```

在第二项策略中，您拒绝对特定规则执行 Amazon One Enterprise 规则的写入操作。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Deny",
            "Action": [
                "one:DeleteSite",
                "one:UpdateSiteAddress"
               ],
            "Resource": "arn:aws:one:region:accountID:site/siteId"
           }
      ]
   }
```

借助资源级权限，您可以允许读取权限和拒绝写入权限，以便对 Amazon One Enterprise 规则 API 操作执行特定操作。

附加信息

要了解有关创建 IAM 用户、组、策略和权限的更多信息，请参阅 IAM 用户指南中的创建您的第一个 IAM 用户和管理员组和访问控制。

AWS Amazon One 企业版的托管策略

AWS 托管策略是由创建和管理的独立策略 AWS。 AWS 托管策略旨在为许多常见用例提供权限，以便您可以开始为用户、组和角色分配权限。

请记住， AWS 托管策略可能不会为您的特定用例授予最低权限权限，因为它们可供所有 AWS 客户使用。我们建议通过定义特定于您的使用场景的客户管理型策略来进一步减少权限。

您无法更改 AWS 托管策略中定义的权限。如果 AWS 更新 AWS 托管策略中定义的权限，则更新会影响该策略所关联的所有委托人身份（用户、组和角色）。 AWS 最有可能在启动新的 API 或现有服务可以使用新 AWS 服务 的 API 操作时更新 AWS 托管策略。

有关更多信息，请参阅《IAM 用户指南》中的 AWS 托管策略。

AmazonOneEnterpriseFullAccess

该策略授予管理权限，允许访问所有 Amazon One Enterprise 资源和操作。

`one:*`允许您执行所有 Amazon One 企业版操作。

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "FullAccessStatementID",
   "Effect": "Allow",
   "Action": [
    "one:*"
   ],
   "Resource": "*"
  }
 ]
}
```

AmazonOneEnterpriseReadOnlyAccess

该政策授予对所有 Amazon One Enterprise 资源和操作的只读权限。

`one:Get*`获取 Amazon One 企业版资源。

`one:List*`列出 Amazon One 企业版资源。

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "ReadOnlyAccessStatementID",
   "Effect": "Allow",
   "Action": [
    "one:Get*",
    "one:List*"
```

```
    ],
    "Resource": "*"
   }
  ]
}
```

AmazonOneEnterpriseInstallerAccess

此政策授予有限的读写权限，允许您为任何已配置的设备实例创建激活二维码，以便在任何站点激活设备。

`one:CreateDeviceActivationQrCode`允许您创建二维码来激活设备。

`one:GetDeviceInstance`让您获取有关 Amazon One 设备实例的信息。

`one:GetSite`让您获取有关 Amazon One 企业网站的信息。

`one:GetSiteAddress`让您获取 Amazon One 企业网站的实际地址。

`one:ListDeviceInstances`让您列出 Amazon One 设备实例。

`one:ListSites`让您列出 Amazon One 企业版网站。

```
{
 "Version": "2012-10-17",
 "Statement": [
  {
   "Sid": "InstallerAccessStatementID",
   "Effect": "Allow",
   "Action": [
    "one:CreateDeviceActivationQrCode",
    "one:GetDeviceInstance",
    "one:GetSite",
    "one:GetSiteAddress",
    "one:ListDeviceInstances",
    "one:ListSites"
   ],
   "Resource": "*"
  }
 ]
}
```

亚马逊 One Enterprise 更新 AWS 了托管政策

查看自该服务开始跟踪这些更改以来对 Amazon One Enterprise AWS 托管政策所做的更新的详细信息。要获取有关此页面变更的自动提醒，请在 Amazon One 企业文档历史记录页面上订阅 RSS 提要。

更改	描述	日期
已添加 Amazon One E AmazonOneMetricPub lishAccess	名为的角色权限策略 AmazonOneMetricPub lishAccess 允许 Amazon One Enterprise PutMetric Data 在 CloudWatch 命名空间 AWS/ AmazonOne 上执行 CloudWatch：。	2025 年 2 月 6 日
亚马逊 One Enterprise 开始跟踪更改	Amazon One Enterprise 开始跟踪其 AWS 托管策略的变更。	2023 年 12 月 1 日

Amazon One Enterprise 的操作、资源和条件键

Amazon One Enterprise（服务前缀：one）提供了以下可在 IAM 权限策略中使用的服务特定资源、操作和条件上下文键。

主题

- Amazon One Enterprise 定义的操作
- Amazon One Enterprise 定义的资源类型
- Amazon One Enterprise 的条件键

Amazon One Enterprise 定义的操作

您可以在 IAM 策略语句的 `Action` 元素中指定以下操作。可以使用策略授予在 AWS中执行操作的权限。您在策略中使用一项操作时，通常使用相同的名称允许或拒绝对 API 操作或 CLI 命令的访问。但在某些情况下，单一动作可控制对多项操作的访问。还有某些操作需要多种不同的动作。

操作表的资源类型列指示每项操作是否支持资源级权限。如果该列没有任何值，您必须在策略语句的 `Resource` 元素中指定策略应用的所有资源（“*”）。通过在 IAM policy 中使用条件来筛选访问权限，以控制是否可以在资源或请求中使用特定标签键。如果操作具有一个或多个必需资源，则调用方必须

具有使用这些资源来使用该操作的权限。必需资源在表中以星号 (*) 表示。如果您在 IAM policy 中使用 `Resource` 元素限制资源访问权限，则必须为每种必需的资源类型添加 ARN 或模式。某些操作支持多种资源类型。如果资源类型是可选的（未指示为必需），则可以选择使用一种可选资源类型。

操作表的条件键列包括可以在策略语句的 `Condition` 元素中指定的键。有关与服务资源关联的条件键的更多信息，请参阅资源类型表的条件键列。

> **Note**
>
> 资源条件键在资源类型表中列出。您可以在操作表的资源类型（* 为必需）列中找到应用于某项操作的资源类型的链接。资源类型表中的资源类型包括条件密钥列，这是应用于操作表中操作的资源条件键。

有关下表中各列的详细信息，请参阅操作表。

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateDeviceInstance	授予创建设备实例的权限	写入		aws:RequestTag/${TagKey} aws:TagKeys	
GetDeviceInstance	授予获取有关设备实例信息的权限	读取	设备实例 *		
ListDeviceInstances	授予列出设备实例的权限	读取			
UpdateDeviceInstance	授予更新设备实例的权限	写入	设备实例 *		
DeleteDeviceInstance	授予删除设备实例的权限	写入	设备实例 *		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
CreateDeviceActivationQrCode	授予在设备实例上创建 QR 码以激活设备的权限	写入	设备实例*		
DeleteAssociatedDevice	授予删除设备与设备实例之间关联的权限	写入	设备实例*		
RebootDevice	授予重启设备的权限	写入	设备实例*		
CreateDeviceInstanceConfiguration	授予创建设备实例配置的权限	写入			
GetDeviceInstanceConfiguration	授予获取有关设备实例配置信息的权限	读取	配置*		
CreateSite	授予创建网站的权限	写入		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteSite	授予删除设备实例的权限	写入	网站*		
GetSite	授予获取有关网站信息的权限	读取	网站*		
ListSites	授予列出网站的权限	读取			
GetSiteAddress	授予获取有关网站地址信息的权限	读取	网站*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
UpdateSite	授予更新网站的权限	写入	网站*		
UpdateSiteAddress	授予更新网站地址的权限	写入	网站*		
CreateDeviceConfigurationTemplate	授予创建设备实例的权限	写入		aws:RequestTag/${TagKey} aws:TagKeys	
DeleteDeviceConfigurationTemplate	授予删除设备配置模板的权限	写入	device-configuration-template*		
GetDeviceConfigurationTemplate	授予获取有关设备配置模板信息的权限	读取	device-configuration-template*		
ListDeviceConfigurationTemplates	授予列出设备配置模板的权限	读取			
UpdateDeviceConfigurationTemplate	授予更新设备配置模板的权限	写入	device-configuration-template*		

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
TagResource	授予权限以标记资源	标记	设备实例、站点、device-configuration-template	aws:RequestTag/${TagKey} aws:TagKeys	
UntagResource	授予权限以取消标记资源	标记	设备实例、站点、device-configuration-template	aws:TagKeys	
ListTagForResources	授予权限以列出资源的标签	读取			

Amazon One Enterprise 定义的资源类型

以下资源类型是由该服务定义的，可以在 IAM 权限策略语句的 `Resource` 元素中使用这些资源类型。操作表中的每个操作指定了可以使用该操作指定的资源类型。您也可以在策略中包含条件键，从而定义资源类型。这些键显示在资源类型表的最后一列。有关下表中各列的详细信息，请参阅资源类型表。

资源类型	ARN	条件键
Device Instance	`arn:aws:one:` *`region:accountID`* `:device-instance/` *`deviceInstanceId`*	aws:ResourceTag/${TagKey}

资源类型	ARN	条件键
Device Instance Configuration	`arn:aws:one:` *`region:accountID`* `:device-instance/` *`deviceInstanceId`* `/configuration/` *`version`*	
Site	`arn:aws:one:` *`region:accountID`* `:site/`*`siteId`*	aws:ResourceTag/${TagKey}
Device Configuration Template	`arn:aws:one:` *`region:accountID`* `:device-configuration-template/` *`templateId`*	aws:ResourceTag/${TagKey}

Amazon One Enterprise 的条件键

Amazon One Enterprise 定义了以下可以在 IAM policy 的 `Condition` 元素中使用的条件键。您可以使用这些键进一步细化应用策略语句的条件。有关下表中各列的详细信息，请参阅条件键表。

要查看适用于所有服务的全局条件键，请参阅可用的全局条件键。

条件键	描述	类型
aws:RequestTag/${TagKey}	按请求中的标签筛选访问权限	字符串
aws:ResourceTag/${TagKey}	按与资源关联的标签筛选访问权限	字符串
aws:TagKeys	按请求中的标签键筛选访问权限	ArrayOfString

亚马逊 One 企业版合规性验证

要了解是否属于特定合规计划的范围，请参阅AWS 服务 “按合规计划划分的范围” ”，然后选择您感兴趣的合规计划。 AWS 服务 有关一般信息，请参阅AWS 合规计划AWS。

您可以使用下载第三方审计报告 AWS Artifact。有关更多信息，请参阅中的 “下载报告” 中的 “ AWS Artifact。

您在使用 AWS 服务 时的合规责任取决于您的数据的敏感性、贵公司的合规目标以及适用的法律和法规。 AWS 提供了以下资源来帮助实现合规性：

- Security Compliance & Governance：这些解决方案实施指南讨论了架构考虑因素，并提供了部署安全性和合规性功能的步骤。
- 符合 HIPAA 要求的服务参考：列出符合 HIPAA 要求的服务。并非所有 AWS 服务 人都符合 HIPAA 资格。
- AWS 合AWS 规资源 — 此工作簿和指南集可能适用于您的行业和所在地区。
- AWS 客户合规指南 — 从合规角度了解责任共担模式。这些指南总结了保护的最佳实践， AWS 服务 并将指南映射到跨多个框架（包括美国国家标准与技术研究院 (NIST)、支付卡行业安全标准委员会 (PCI) 和国际标准化组织 (ISO)）的安全控制。
- 使用AWS Config 开发人员指南中的规则评估资源 — 该 AWS Config 服务评估您的资源配置在多大程度上符合内部实践、行业准则和法规。
- AWS Security Hub— 这 AWS 服务 可以全面了解您的安全状态 AWS。Security Hub 通过安全控制措施评估您的 AWS 资源并检查其是否符合安全行业标准和最佳实践。有关受支持服务及控制措施的列表，请参阅 Security Hub 控制措施参考。
- Amazon GuardDuty — 它通过监控您的 AWS 账户环境中是否存在可疑和恶意活动，来 AWS 服务 检测您的工作负载、容器和数据面临的潜在威胁。 GuardDuty 通过满足某些合规性框架规定的入侵检测要求，可以帮助您满足各种合规性要求，例如 PCI DSS。
- AWS Audit Manager— 这 AWS 服务 可以帮助您持续审计 AWS 使用情况，从而简化风险管理以及对法规和行业标准的合规性。

监控 Amazon One 企业版

监控是维护 Amazon One Enterprise 和其他 AWS 解决方案的可靠性、可用性和性能的重要组成部分。 AWS 提供以下监控工具，用于监视 Amazon One Enterprise，在出现问题时进行报告，并在适当时自动采取措施：

- Amazon EventBridge 可用于实现 AWS 服务自动化，并自动响应系统事件，例如应用程序可用性问题或资源更改。来自 AWS 服务的事件几乎实时 EventBridge 地传送到。您可以编写简单的规则来指示您关注的事件，并指示要在事件匹配规则时执行的自动化操作。有关更多信息，请参阅 Amazon EventBridge 用户指南。
- AWS CloudTrail捕获由您的账户或代表您的 AWS 账户进行的 API 调用和相关事件，并将日志文件传输到您指定的 Amazon S3 存储桶。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。有关更多信息，请参阅 用户指南。AWS CloudTrail

监控亚马逊中的 Amazon One Enterprise 事件 EventBridge

您可以在中监控 Amazon One Enterprise 事件 EventBridge，它会提供来自您自己的应用程序、software-as-a-service (SaaS) 应用程序和 AWS 服务的实时数据流。 EventBridge将该数据路由到目标，例如 AWS Lambda 和 Amazon 简单通知服务。这些事件提供了近乎实时的系统事件流，这些事件描述了 AWS 资源的变化。

订阅 Amazon One 企业版活动

Amazon One 设备和用户个人资料状态更改事件使用发布 EventBridge，也可以通过创建新规则在 EventBridge 控制台中启用。尽管事件不是有序的，但它们有时间戳，允许您使用数据。尽最大努力发出事件。

订阅 Amazon One Enterprise 活动

1. 登录您的 AWS 控制台，网址为https://console.aws.amazon.com/events/。
2. 打开 EventBridge 控制台，网址为https://console.aws.amazon.com/events/。
3. 在导航窗格中的总线下，选择规则。
4. 选择创建规则。
5. 在默认规则详细信息页面上，为规则指定名称。
6. 选择 Rule with an event pattern（具有事件模式的规则），然后选择 Next（下一步）。

7. 在 “生成事件模式” 页面的 “事件源” 下，确认已选择AWS 事件或 EventBridge 合作伙伴事件。
8. 在示例事件类型下，选择 AWS 事件。
9. 在 “创建方法” 中，选择 “自定义图案”。
10. 在事件模式部分中，添加一个 JSON，事件源为`aws:one`和所需的详细信息类型：

```
"
source": ["aws.one"],
"detail-type": ["New Successful Enrollment",
"New Successful Un-enrollment",
"Unsuccessful Enrollment",
"Unsuccessful Un-enrollment",
"Successful Recognition",
"Unsuccessful Recognition"]
}
```

    您可以从上面的列表中选择所需的详细信息类型，然后删除不需要的内容。
11. 选择下一步。
12. 在选择目标页面上，选择您选择的目标，其中包括 Lambda 函数、SQS 队列或 SNS 主题。有关配置目标的信息，请参阅 Amazon EventBridge 目标。

    例如，要查看某人何时进入时钟，请选择 “成功识别”。然后查看活动详情（见附录），看看谁在计时。

    要完成工作流程，您可以执行外部 API 或其他目标。
13. 或者，您可以配置标签。
14. 请在审核和创建页面，选择创建。有关配置规则的更多信息，请参阅 EventBridge《 EventBridge 用户指南》中的规则。

设备状态更改事件类型

设备状态更改事件以 JSON 格式生成。对于每种事件类型，都会按照规则中的配置向您选择的目标发送一个 JSON blob。有以下详细信息类型可供选择：

设备健康状态更改为 “健康”

设备通过了所有运行状况检查。

设备 Health 状态更改为 “严重”

设备未通过一项或多项运行状况检查。

设备连接已更改为离线

设备未连接到互联网。

设备连接已更改为在线

设备已连接到互联网。

resources

包含已发布设备状态更改事件的 DeviceInstance arn 列表。

metadata

siteName

- 设备实例所在站点的名称。

SiteArn

- Arn 表示存在设备实例的站点。

数据

当前连接

- 表示 DeviceInstance 是已连接到互联网还是已断开与互联网的连接。
- 可能的值：已连接、已断开连接

上一页连接

- 表示事件发生前 DeviceInstance 是已连接到互联网还是已断开与互联网的连接。
- 可能的值：已连接、已断开连接

currentHealthStatus

- 表示设备实例是否已通过所有运行状况检查。
- 可能的值：“健康”、“严重”

previousHealthStatus

- 表示上次检查时 DeviceInstance 是否通过了所有运行状况检查。
- 可能的值：“健康”、“严重”

assetTagId

- 与设备实例关联的设备的。 assetTagId

deviceInstanceName

- 发布设备状态事件的设备实例的名称。

用户个人资料事件类型

与用户个人资料相关的事件详细信息类型有：

新成功注册

当用户成功注册时。

新成功取消注册

当用户成功取消注册时。

注册失败

当用户注册失败时。

取消注册失败

当用户取消注册失败时。

成功认可

当用户成功扫描 palm 进行身份验证时。

识别失败

当手掌扫描识别失败时。

resources

包含发布用户个人资料事件的用户个人资料 arn 列表。

数据

accountId

- 发起请求的设备的相关 AWS 账户。

请求来源

- 这是发起请求 deviceInstanceId 的设备。

已创建时间戳

- 事件的创建时间。

用户状态

- 用户的当前状态。
- 可能的值：“活动”、“已删除”

关联的 ID

- 用户的关联 ID，例如徽章 ID。

reason

- 对于不成功的事件，将显示此值。它包含事件失败的原因。

示例事件

以下示例显示了 Amazon One Enterprise 的事件。

主题

- 设备运行状况已更改为正常
- 设备运行状况更改为 “严重”
- 设备连接已更改为在线
- 设备连接已更改为离线

设备运行状况已更改为正常

设备通过了所有运行状况，设备实例的运行状况从 “危急” 状态更改为 “正常”。

```
{
    "version": "0",
    "id": "11232345564-96a4-ef3f-b739-b6aa5b193afb",
    "detail-type": "Device Health Status Changed To Healthy",
    "source": "aws.one",
    "account": "123456789012",
    "time": "2022-10-22T18:43:48Z",
    "region": "us-east-1",
```

```
    "resources": ["arn:aws:one:us-east-1:123456789012:device-instance/12345678901234"],
    "detail": {
    "version": "1.0.0",
    "metadata": {
      "siteName": "Site name",
      "siteArn": "arn:aws:one:us-east-1:123456789012:site/12345678901234"
    },
    "data": {
      "currentHealthStatus": "HEALTHY",
      "previousHealthStatus": "CRITICAL",
      "assetTagId": "0000195169",
      "deviceInstanceName": "Device name"
    }
  }
}
```

设备运行状况更改为 “严重”

设备未通过一项或多项运行状况检查，并且设备实例的运行状况从 “正常” 更改为 “严重”。

```
{
  "version": "0",
  "id": "11232345564-96a4-ef3f-b739-b6aa5b193afb",
  "detail-type": "Device Health Status Changed To Critical",
  "source": "aws.one",
  "account": "123456789012",
  "time": "2022-10-22T18:43:48Z",
  "region": "us-east-1",
  "resources": ["arn:aws:one:us-east-1:123456789012:device-instance/12345678901234"],
  "detail": {
    "version": "1.0.0",
    "metadata": {
      "siteName": "Site name",
      "siteArn": "arn:aws:one:us-east-1:123456789012:site/12345678901234"
    },
    "data": {
      "currentHealthStatus": "CRITICAL",
      "previousHealthStatus": "HEALTHY",
      "assetTagId": "0000195169",
      "deviceInstanceName": "Device name"
    }
  }
}
```

设备连接已更改为在线

设备已连接到互联网，并且设备实例的连接状态从 “已断开连接” 更改为 “已连接”。

```
{
  "version": "0",
  "id": "11232345564-96a4-ef3f-b739-b6aa5b193afb",
  "detail-type": "Device Connectivity Changed To Online",
  "source": "aws.one",
  "account": "123456789012",
  "time": "2022-10-22T18:43:48Z",
  "region": "us-east-1",
  "resources": ["arn:aws:one:us-east-1:123456789012:device-instance/12345678901234"],
  "detail": {
    "version": "1.0.0",
    "metadata": {
      "siteName": "Site name",
      "siteArn": "arn:aws:one:us-east-1:123456789012:site/12345678901234"
    },
    "data": {
      "currentConnectivity": "CONNECTED",
      "previousConnectivity": "DISCONNECTED",
      "assetTagId": "0000195169",
      "deviceInstanceName": "Device name"
    }
  }
}
```

设备连接已更改为离线

设备未连接到互联网，并且设备实例的连接状态从 “已连接” 更改为 “已断开连接”。

```
{
  "version": "0",
  "id": "11232345564-96a4-ef3f-b739-b6aa5b193afb",
  "detail-type": "Device Connectivity Changed To Offline",
  "source": "aws.one",
  "account": "123456789012",
  "time": "2022-10-22T18:43:48Z",
  "region": "us-east-1",
  "resources": ["arn:aws:one:us-east-1:123456789012:device-instance/12345678901234"],
  "detail": {
    "version": "1.0.0",
```

```
    "metadata": {
      "siteName": "Site name",
      "siteArn": "arn:aws:one:us-east-1:123456789012:site/12345678901234"
    },
    "data": {
      "currentConnectivity": "DISCONNECTED",
      "previousConnectivity": "CONNECTED",
      "assetTagId": "0000195169",
      "deviceInstanceName": "Device name"
    }
  }
}
```

使用记录 Amazon One 企业 API 调用 AWS CloudTrail

Amazon One Enterprise 与 AWS CloudTrail一项服务集成，该服务提供用户、角色或 AWS 服务在 Amazon One Enterprise 中采取的操作的记录。 CloudTrail 将 Amazon One Enterprise 的所有 API 调用记录为事件。捕获的调用包括来自亚马逊 One Enterprise 控制台的调用和对 Amazon One Enterprise API 操作的代码调用。如果您创建跟踪，则可以允许将 CloudTrail 事件持续传输到 Amazon S3 存储桶，包括针对 Amazon One Enterprise 的事件。如果您未配置跟踪，您仍然可以在 CloudTrail 控制台的 “事件历史记录” 中查看最新的事件。通过收集的信息 CloudTrail，您可以确定向 Amazon One Enterprise 发出的请求、发出请求的 IP 地址、谁提出了请求、何时提出请求以及其他详细信息。

要了解更多信息 CloudTrail，请参阅《AWS CloudTrail 用户指南》。

Amazon One 企业版信息位于 CloudTrail

CloudTrail 在您创建账户 AWS 账户 时已在您的账户上启用。当 Amazon One Enterprise 中发生活动时，该活动会与其他 AWS 服务 CloudTrail 事件一起记录在事件历史记录中。您可以在中查看、搜索和下载最近发生的事件 AWS 账户。有关更多信息，请参阅使用事件历史记录查看 CloudTrail 事件。

要持续记录您的事件 AWS 账户，包括 Amazon One Enterprise 的事件，请创建跟踪。跟踪允许 CloudTrail 将日志文件传输到 Amazon S3 存储桶。预设情况下，在控制台中创建跟踪记录时，此跟踪记录应用于所有 AWS 区域。跟踪记录 AWS 分区中所有区域的事件，并将日志文件传送到您指定的 Amazon S3 存储桶。此外，您可以配置其他 AWS 服务，以进一步分析和处理 CloudTrail 日志中收集的事件数据。有关更多信息，请参阅下列内容：

- 创建跟踪记录概述
- CloudTrail 支持的服务和集成
- 配置 Amazon SNS 通知 CloudTrail

- 接收来自多个地区的 CloudTrail 日志文件和接收来自多个账户的 CloudTrail 日志文件

所有 Amazon One Enterprise 操作均由记录 CloudTrail 并记录在Amazon One Enterprise 的操作、资源和条件键。例如，调用`RebootDevice`和`DeleteDeviceInstance`操作会在 CloudTrail 日志文件中生成条目。`ListSites`

每个事件或日志条目都包含有关生成请求的人员信息。身份信息有助于您确定以下内容：

- 请求是使用根证书还是 AWS Identity and Access Management (IAM) 用户凭证发出。
- 请求是使用角色还是联合用户的临时安全凭证发出的。
- 请求是否由其他 AWS 服务发出。

有关更多信息，请参阅 CloudTrail userIdentity 元素。

了解 Amazon One 企业版日志文件条目

跟踪是一种配置，允许将事件作为日志文件传输到您指定的 Amazon S3 存储桶。 CloudTrail 日志文件包含一个或多个日志条目。事件代表来自任何来源的单个请求，包括有关请求的操作、操作的日期和时间、请求参数等的信息。 CloudTrail 日志文件不是公共 API 调用的有序堆栈跟踪，因此它们不会按任何特定的顺序出现。

以下示例显示了演示该`CreateSite`操作的 CloudTrail 日志条目。

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "AIDAKDBGOAT6C2EXAMPLE:J_DOE",
        "arn": "arn:aws:sts::123456789012:assumed-role/Admin/J_DOE",
        "accountId": "123456789012",
        "accessKeyId": "AKIALAVPULGA71EXAMPLE",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "AIDAKDBGOAT6C2EXAMPLE",
                "arn": "arn:aws:iam::123456789012:role/Admin",
                "accountId": "123456789012",
                "userName": "Admin"
            },
            "webIdFederationData": {},
```

```
            "attributes": {
                "creationDate": "2023-10-11T06:28:04Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-10-11T07:19:09Z",
    "eventSource": "one.amazonaws.com",
    "eventName": "CreateSite",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "XXX.XXX.XXX.XXX",
    "userAgent": "userAgent",
    "requestParameters": {
        "name": "***",
        "description": "***",
        "address": {
            "addressLine1": "***",
            "addressLine2": "***",
            "addressLine3": "***",
            "city": "EXAMPLE_CITY",
            "postalCode": "12345",
            "countryCode": "EXAMPLE_COUNTRY",
            "stateOrRegion": "EXAMPLE_STATE"
        },
        "clientToken": "abc12d34-567e-8910-1112-12fghi0jk13l"
    },
    "responseElements": {
        "stateOrRegion": "EXAMPLE_STATE",
        "createdAtInMillis": 1697008749263,
        "city": "EXAMPLE_CITY",
        "countryCode": "EXAMPLE_COUNTRY",
        "deviceInstanceCount": 0,
        "postalCode": "12345",
        "name": "***",
        "description": "***",
        "siteId": " abCdefG12hijkL",
        "siteArn": "arn:aws:one:us-east-1:123456789012:site/abCdefG12hijkL",
        "tags": "***"
    },
    "requestID": "1abcd23e-f4gh-567j-klm8-9np01q234r56",
    "eventID": "1234a56b-c78d-9e0f-g1h2-34jk56m7n890",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
```

```
    "recipientAccountId": "123456789012",
    "eventCategory": "Management"
}
```

对亚马逊One进行故障排除

如果您在使用 Amazon One 应用程序或其中一台 Amazon One 设备时遇到问题，请使用这些建议来解决问题。然后，如果您仍然遇到问题，请联系 AWS Support。

主题

- 对 Amazon One 身份和访问进行故障排除
- 对 Amazon One 主机进行故障排除
- 对 Amazon One 设备进行故障排除

对 Amazon One 身份和访问进行故障排除

使用以下信息来帮助您诊断和修复在使用 Amazon One Enterprise 和 IAM 时可能遇到的常见问题。

主题

- 我无权在 Amazon One 中执行任何操作
- 我想允许我以外的人访问我 AWS 账户 的 Amazon One 资源

我无权在 Amazon One 中执行任何操作

如果您收到错误提示，指明您无权执行某个操作，则必须更新策略以允许执行该操作。

当 `mateojackson` IAM 用户尝试使用控制台查看有关虚构 *`my-example-widget`* 资源的详细信息，但不拥有虚构 `one:`*`GetWidget`* 权限时，会发生以下示例错误。

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 one:GetWidget on resource: my-example-widget
```

在此情况下，必须更新 `mateojackson` 用户的策略，以允许使用 `one:`*`GetWidget`* 操作访问 *`my-example-widget`* 资源。

如果您需要帮助，请联系您的 AWS 管理员。您的管理员是提供登录凭证的人。

我想允许我以外的人访问我 AWS 账户 的 Amazon One 资源

您可以创建一个角色，以便其他账户中的用户或您组织外的人员可以使用该角色来访问您的资源。您可以指定谁值得信赖，可以代入角色。对于支持基于资源的策略或访问控制列表 (ACLs) 的服务，您可以使用这些策略向人们授予访问您的资源的权限。

要了解更多信息，请参阅以下内容：

- 要了解 Amazon One Enterprise 是否支持这些功能，请参阅亚马逊 One Enterprise 如何使用 IAM。
- 要了解如何提供对您拥有的资源的访问权限 AWS 账户 ，请参阅 IAM 用户指南中的向您拥有 AWS 账户 的另一个 IAM 用户提供访问权限。
- 要了解如何向第三方提供对您的资源的访问权限 AWS 账户，请参阅 IAM 用户指南中的向第三方提供访问权限。 AWS 账户
- 要了解如何通过身份联合验证提供访问权限，请参阅《IAM 用户指南》中的为经过外部身份验证的用户（身份联合验证）提供访问权限。
- 要了解使用角色和基于资源的策略进行跨账户访问之间的差别，请参阅《IAM 用户指南》中的 IAM 中的跨账户资源访问。

对 Amazon One 主机进行故障排除

如果您在使用 Amazon One 应用程序或其中一台 Amazon One 设备时遇到问题，请使用这些建议来解决问题。然后，如果您仍然遇到问题，请联系 AWS Support。

主题

- 我无法创建网站
- 我无法创建设备实例
- 我无法创建配置模板
- 我无法创建激活二维码

我无法创建网站

- 请联系您的 Amazon One 控制台管理员为您提供访问权限。
- 如果问题仍然存在，请联系 AWS Support。

我无法创建设备实例

- 请联系您的 Amazon One 控制台管理员为您提供访问权限。
- 如果问题仍然存在，请联系 AWS Support。

我无法创建配置模板

- 请联系您的 Amazon One 控制台管理员为您提供访问权限。
- 如果问题仍然存在，请联系 AWS Support。

我无法创建激活二维码

- 请联系您的 Amazon One 控制台管理员为您提供访问权限。
- 如果问题仍然存在，请联系 AWS Support。

对 Amazon One 设备进行故障排除

如果您在使用 Amazon One 主机或其中一台 Amazon One 设备时遇到问题，请使用这些建议来解决问题。然后，如果您仍然遇到问题，请联系 AWS Support。

主题

- 空白屏幕
- 我无法连接到 Wi-Fi 或网络
- 重启带有活动警报的设备
- 系统错误
- 无法识别二维码
- 无法读取二维码
- 检测到多个 QR 码
- 设备实例不存在
- 未找到网站
- 邮政编码不匹配
- 网关超时
- 我无法配置设备

- 设备已重新启动，但出现错误消息和错误代码
- 设备屏幕上有亚马逊徽标，没有其他活动
- 暂时不可用
- 我们这边出了点问题
- 暂时停止服务
- Amazon One 设备出现物理损坏
- 无法读取 palm
- 手掌无法识别
- 由于长时间处于非活动状态，设备已锁定
- 设备因篡改事件而被锁定

空白屏幕

当设备断电或在重启期间卡住时，就会发生这种情况。

要解决此问题，请执行以下操作：

- 请稍等片刻（少于 30 秒），以防设备正在重启。
- 如果设备处于空白状态时灯环闪烁，请等待最多 30 秒。
- 检查电源线是否已插入电源插座以及是否牢固地插入 Amazon One 设备的背面。另外，请检查电源线是否损坏。
- 检查电源。
- 检查所有电缆是否已正确连接到 Amazon One 和 USB 集线器。
- 从控制台重启设备。
- 如果重启设备无法解决问题，请将 Amazon One USB 集线器从电源上拔下，然后重新插上。
- 如果问题仍然存在，请联系 AWS Support。

我无法连接到 Wi-Fi 或网络

当设备断开连接时，就会发生这种情况。

要解决此问题，请执行以下操作：

- 如果连接到 Wi-Fi，请使用另一台设备检查 Wi-Fi 是否出现在可用网络中。

- 检查 Wi-Fi 路由器是否已开启且在覆盖范围内。
- 网络恢复后，设备将重新连接。
- 如果问题仍然存在，请联系 AWS 支持。

重启带有活动警报的设备

当从控制台请求重启时，即使设备处于离线状态或面临网络问题，该操作也要等待 15 分钟，设备才会收到命令并尝试重启。

要解决此问题，请执行以下操作：

- 等待重启完成。
- 如果问题仍然存在，请联系 AWS 支持。

系统错误

出现这种情况是由于内部错误造成的。

要解决此问题，请执行以下操作：

- 在屏幕上选择 “重新启动” 以重新启动应用程序。
- 尝试两次后，如果问题仍未解决，请联系 AWS Support。

无法识别二维码

发生这种情况的原因是未经授权的二维码或二维码已过期。

要解决此问题，请执行以下操作：

- 选择 “重试” 返回二维码屏幕。
- 在 AWS 控制台上创建新的二维码，然后扫描有效的二维码。

无法读取二维码

当应用程序无法读取二维码时，就会发生这种情况。

要解决此问题，请执行以下操作：

- 选择 “重试” 返回二维码屏幕。
- 如果问题仍然存在，请取消激活工作流程并重新启动。

检测到多个 QR 码

当扫描多个二维码时，就会发生这种情况。

要解决此问题，请执行以下操作：

- 选择 “重试” 返回二维码屏幕。
- 一次只能扫描一个有效的二维码。

设备实例不存在

当设备实例被删除或在 AWS 控制台中不存在时，就会发生这种情况。

要解决此问题，请执行以下操作：

- 选择 “重试” 返回二维码屏幕。
- 检查 AWS 控制台以获取正确的设备实例。如果缺少设备实例，请联系您的管理员。
- 为该设备实例创建新的二维码，然后扫描新的二维码。

未找到网站

当网站被删除或在 AWS 控制台中不存在时，就会发生这种情况。

要解决此问题，请执行以下操作：

- 请查看 AWS 控制台以获取站点信息。如果该网站不存在，请联系您的管理员。

邮政编码不匹配

当输入的邮政编码与为设备配置的邮政编码不同的邮政编码时，就会发生这种情况。

要解决此问题，请执行以下操作：

- 选择 “重试”，返回到 “邮政编码” 屏幕。

- 检查您的网站邮政编码是否正确。
- 如果问题仍然存在，请联系您的管理员在 AWS 控制台上查看网站邮政编码。

网关超时

当网关在指定时间内没有响应时，就会发生这种情况。

要解决此问题，请执行以下操作：

- 选择 “重新启动” 以重新启动应用程序。
- 两次尝试后，如果问题仍未解决，请联系 AWS Support。

我无法配置设备

当操作未能将配置保存到设备磁盘上时，就会发生这种情况。

要解决此问题，请执行以下操作：

- 选择 “重新启动” 以重新启动应用程序。
- 两次尝试后，如果问题仍未解决，请联系 AWS Support。

设备已重新启动，但出现错误消息和错误代码

要解决此问题，请执行以下操作：

- 选择 “重新启动”，然后让设备恢复。
- 如果设备无法恢复，请从电源上拔下 USB 集线器并重新连接。
- 如果问题仍然存在，请联系 AWS Support。

设备屏幕上有亚马逊徽标，没有其他活动

要解决此问题，请执行以下操作：

- 请稍等片刻（少于 30 秒），以防设备正在重启。
- 从电源上拔下 USB 集线器并重新连接。
- 如果问题仍然存在，请联系 AWS Support。

暂时不可用

要解决此问题，请执行以下操作：

- 确保与主机设备/系统的 USB 连接是安全的。
- 断开并重新连接所有连接到 USB 集线器的电缆。
- 如果问题仍然存在，请联系 AWS Support。

我们这边出了点问题

当出现内部错误时，就会发生这种情况。

要解决此问题，请执行以下操作：

1. 关闭设备。
2. 断开其电源的连接。
3. 等待 30 秒钟。
4. 将设备重新插入其电源。
5. 打开设备电源。
6. 如果问题仍然存在，请联系 AWS Support。

暂时停止服务

当设备被 Amazon One 停止使用时，就会发生这种情况。

要解决此问题，请执行以下操作：

- 联系 AWS Support。

Amazon One 设备出现物理损坏

要解决此问题，请执行以下操作：

- 请联系 AWS Support 了解后续步骤，并提供尽可能多的细节，例如发生了什么、发生的时间以及发生的原因。

无法读取 palm

要解决此问题，请执行以下操作：

- 仔细检查 Amazon One 设备是否没有条纹和污迹。
- 确保客户的手掌没有绷带、袖子和明显的污垢/油脂等闭塞物。
- 如果问题仍然存在，并且设备无法读取任何手掌，请联系 AWS Support。

手掌无法识别

要解决此问题，请执行以下操作：

- 让客户尝试使用另一只手掌。
- 确保客户已经注册。如果没有，请让他们在线或在设备上注册。
- 如果问题仍然存在，并且设备无法读取任何手掌触点，请联系 AWS Support。

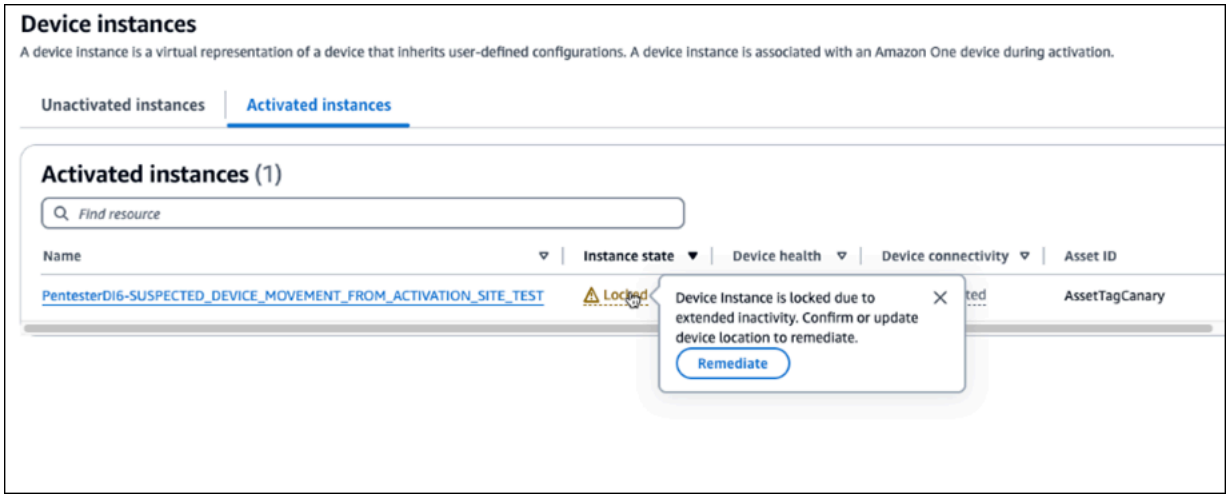
由于长时间处于非活动状态，设备已锁定

当设备怀疑自己已从激活站点移出时，它会将用户拒之门外。当设备超过最长 120 小时的离线时间时，就会发生这种情况。

执行以下操作来解锁设备：

1. 登录您的 AWS 控制台，然后选择设备实例。
2. 在页面顶部的错误横幅中，选择 “修复”。

   可选：在已激活的实例中，选择已锁定，然后选择修复。



3. 如果设备仍在原始激活站点，请选择 “是，设备位于此站点”。
4. 如果设备位于其他站点，请选择 “否，设备位于其他站点”。选择 “否” 将停用该设备。在新站点激活设备。

设备因篡改事件而被锁定

出于安全考虑，Amazon One 设备将被锁定，以防发生任何篡改事件。

要解决此问题，请执行以下操作：

- 联系 AWS Support。

Amazon One 企业版用户指南的文档历史记录

下表描述了 Amazon One Enterprise 的文档版本。

变更	说明	日期
更新	添加了服务相关角色部分	2025 年 2 月 4 日
更新	新增：场景驱动的内容	2024 年 10 月 10 日
更新	新增主题：对 Amazon One 企业版控制台进行故障排除	2024 年 10 月 10 日
更新	新增主题：对 Amazon One 企业版设备进行故障排除	2024 年 10 月 10 日
更新	增加了章节：设置 Amazon One Enterprise	2024 年 10 月 10 日
更新	新增主题：维护和清洁 Amazon One 企业版设备	2024 年 10 月 10 日
更新	重新整理的内容	2024 年 10 月 10 日
更新	新增主题：安装 Amazon One Enterprise 设备 I/O 中心以实现安全访问	2024 年 8 月 14 日
更新	新增主题：安装壁挂式 Amazon One Enterprise 设备	2024 年 6 月 5 日
初始版本	Amazon One 企业用户指南的首次发布	2023 年 11 月 27 日

本文属于机器翻译版本。若本译文内容与英语原文存在差异，则一律以英文原文为准。