aws

用户指南

Amazon One Enterprise

Amazon One Enterprise: 用户指南

Table of Contents

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 设备专为 Amazon One Enterprise 而设计，这是一种基于手掌的安全身份服务，用于企业访问控制。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 5GHz）、以太网、2 个 USB A 型、1 个 B 型 USB
- 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 Wiegand
- 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 包括一个控制台，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 企业版的工作方式

Amazon One Enterprise 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，也可以使用注册亚马逊 One Enterprise 安全访问服务 AWS Management Console。

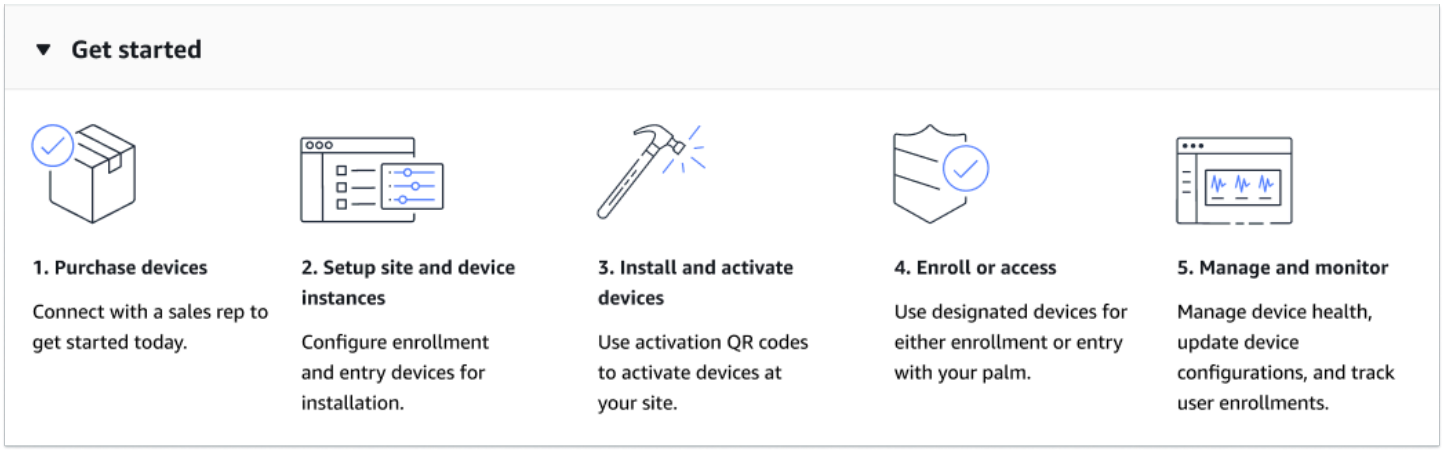
安装 Amazon One Enterprise 后，您可以激活设备并 AWS 账户 在 Amazon One Enterprise 控制台上使用您的设备进行注册，还可以使用身份验证应用程序。您还可以查看已注册员工的生物识别资料，也可以取消员工的注册。当员工离开公司或丢失徽章时，您可以轻松删除他们的生物识别数据。Amazon One 企业控制台还充当管理运营活动的集中位置，例如跟踪已安装的设备和查看月度账单。

员工可以在现场有人监督的招生站扫描徽章和手掌进行注册。员工注册后，只需将手掌悬停在 Amazon One 设备上即可进入或离开安全地点。

主题

Amazon One 企业版工作流程

下图显示了 Amazon One Enterprise 的基本工作流程。



1. 联系我们购买一台 Amazon One 设备。
2. 创建站点和设备实例，配置用于安装的注册和输入设备。
3. 安装完成后，通过扫描设备实例特有的安全 QR 码来激活 Amazon One 设备。
4. 要求员工注册手掌，然后用手掌进行身份验证以获得访问权限。

5. 利用管理和监控功能：确保设备运行状况，使配置保持最新，并跟踪用户注册以进行全面监督。

Amazon One 企业版关键术语

以下是 Amazon One Enterprise 的关键术语：

- 场地 — 客户管理客户在其中安装 Amazon One Enterprise 设备的物理建筑。场地必须满足您的 Amazon One Enterprise 设备的设施、网络和电源要求。
- 设备 — 用于身份验证的 Amazon One Enterprise 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
  - 处于活动状态
- 配置模板-应用于设备实例的一组包罗万象的配置。

开始使用

本章介绍开始使用 Amazon One Enterprise 的基本步骤：

1. 设置站点、设备实例和配置模板-按照以下步骤创建框架，用于添加存放您的 Amazon One 设备的物理位置，然后对其进行配置和管理。这些步骤使用 Amazon One Enterprise 控制台。您只能偶尔使用此流程，甚至只使用一次，具体取决于您选择拥有的站点、设备实例和配置模板的数量。
2. 安装和激活设备-在设置开始时按照以下步骤操作。设备激活要求安装人员通过手机访问 Amazon One Enterprise 控制台以获取激活二维码。
3. 设备和用户管理-请按照以下步骤操作 Amazon One Enterprise 控制台的日常使用。您可以使用这些步骤来监控设备运行状况、了解用户参与度指标和配置设备。

要了解有关亚马逊 One Enterprise 的更多信息，您可以访问亚马逊 One Enterprise 产品详情页面。

主题

设置亚马逊 One Enterprise

使用 Amazon One Enterprise 的第一步是使用 Amazon One Enterprise 控制台设置您的站点、设备实例和配置模板。

主题

步骤 1：创建账户和管理员用户

注册获取 AWS 账户

如果你没有 AWS 账户，请完成以下步骤来创建一个。

要注册 AWS 账户

1. 打开https://portal.aws.amazon.com/billing/注册。
2. 按照屏幕上的说明进行操作。

   在注册时，将接到一通电话，要求使用电话键盘输入一个验证码。

   当你报名参加 AWS 账户，一个 AWS 账户根用户已创建。root 用户可以访问所有内容 AWS 服务以及账户中的资源。作为安全最佳实践，请为用户分配管理访问权限，并且只使用根用户来执行需要根用户访问权限的任务。

AWS 注册过程完成后会向您发送一封确认电子邮件。您可以随时前往 https://aws.amazon.com/并选择“我的账户”，查看您当前的账户活动并管理您的账户。

创建具有管理访问权限的用户

在你注册之后 AWS 账户，保护你的 AWS 账户根用户，启用 AWS IAM Identity Center，然后创建一个管理用户，这样你就不会使用 root 用户来执行日常任务。

保护你的 AWS 账户根用户

1. 登录 。AWS Management Console以账户所有者的身份选择 Root 用户并输入你的 AWS 账户 电子邮件地址。在下一页上，输入您的密码。

   有关使用 root 用户登录的帮助，请参阅中以 root 用户身份登录 AWS 登录 用户指南。
2. 为您的 root 用户开启多重身份验证 (MFA)。

   有关说明，请参阅为您的MFA设备启用虚拟设备 AWS 账户 用户指南中的 root IAM 用户（控制台）。

创建具有管理访问权限的用户

1. 启用IAM身份中心。

有关说明，请参阅启用 AWS IAM Identity Center中的 AWS IAM Identity Center 用户指南。

2. 在 IAM Identity Center 中，向用户授予管理访问权限。

   有关使用教程 IAM Identity Center 目录 作为您的身份来源，请参阅使用默认设置配置用户访问权限 IAM Identity Center 目录中的 AWS IAM Identity Center 用户指南。

以具有管理访问权限的用户身份登录

- 要使用您的 Ident IAM ity Center 用户登录URL，请使用您在创建 Ident IAM ity Center 用户时发送到您的电子邮件地址的登录信息。

  有关使用 Ident IAM ity Center 用户登录的帮助，请参阅登录 AWS 访问中的门户 AWS 登录 用户指南。

将访问权限分配给其他用户

1. 在 IAM Identity Center 中，创建一个遵循应用最低权限权限的最佳实践的权限集。

   有关说明，请参阅中的创建权限集 AWS IAM Identity Center 用户指南。

2. 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，请参阅中的添加群组 AWS IAM Identity Center 用户指南。

第 2 步：添加 Amazon One 企业版用户

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 Enterprise 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 Enterprise 用户

1. 按照如何登录中所述的与您的用户类型相适应的登录过程进行操作 AWS 在 AWS 登录 用户指南。
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。这是他们的登录名 AWS.

> **Note**
>
> 中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AWSSTS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，您不能创建两个名为TESTUSER和 testuser 的用户。当用户名在策略中使用或作为策略的一部分使用时ARN，该名称区分大小写。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 “我要创建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，它会自动附加 AWS 为新用户命名的IAMUserChangePassword托管策略。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。有关在中使用标签的更多信息IAM，请参阅为IAM资源添加标签。
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
    - URL进入账户登录页面。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。

第 3 步：创建网站

现在你已经登录了 AWS Management Console，您可以使用 Amazon One Enterprise 控制台来创建您的网站。

> **Important**
>
> Amazon One Enterprise 仅在美国东部（弗吉尼亚北部）地区推出。

创建站点

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

步骤 4：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 企业控制台。
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。

步骤 5：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 企业控制台。
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 Enterprise 的全部功能以实现安全访问。

步骤 6：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（请参阅步骤 5：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 企业控制台。
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，请参阅步骤 5：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  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 Enterprise 的全部功能以实现安全访问。

安装和激活 Amazon One

设置 Amazon One Enterprise 控制台后，接下来的步骤是在您的网站上安装 Amazon One Enterprise 设备，然后将其激活。

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

主题

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。

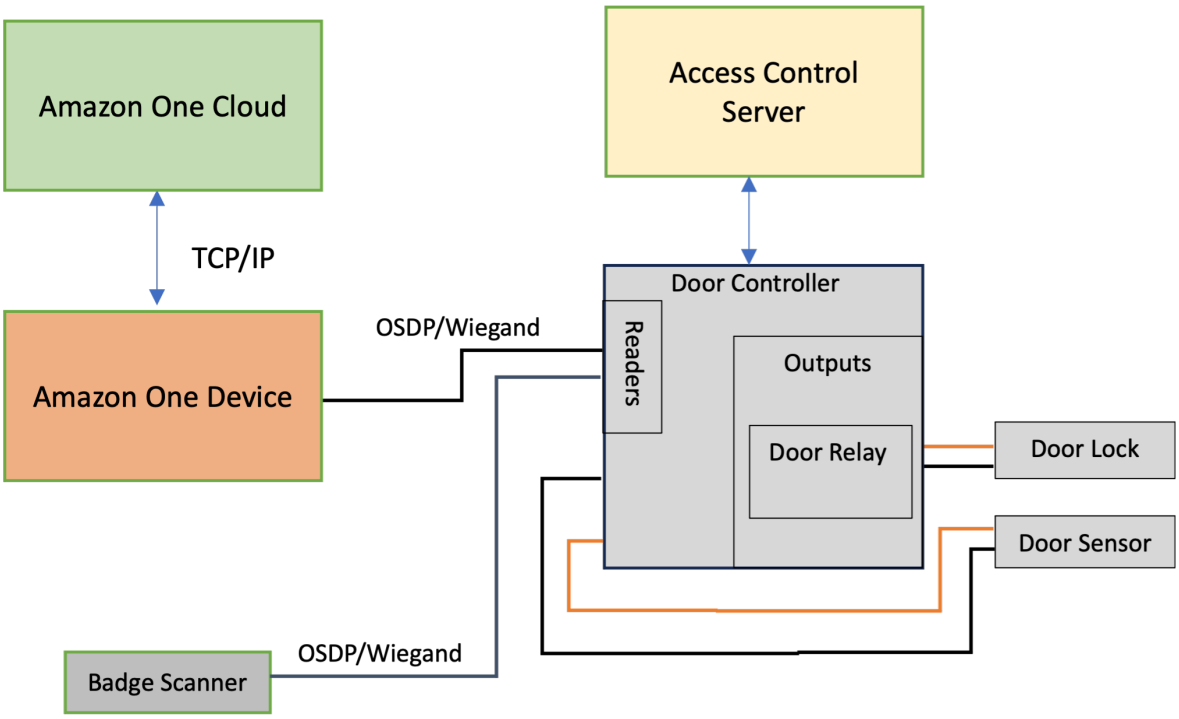
功率要求

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 Enterprise 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的个人的徽章通常存储在此服务器上。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接口连接到门控制器服务器。
  - 如果需要韦根接口，则可以使用COTSOSDP转韦根转换器。
  - 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。
  - Door Controller 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访问控制服务器。在 Amazon One Enterprise 中，可以将徽章扫描器连接到 Amazon One 注册设备，从而可以扫描员工的徽章并将其与他们的手掌个人资料相关联。

安装 Amazon One Enterprise 底座

本节概述了安装Amazon One Enterprise底座所需的位置要求和步骤。

在开始安装之前，请确保满足以下先决条件：

- 如果使用 POE + 为设备供电，请确保布置 Cat6 电缆，并且POE有 + 注入器或开关可供使用。
- 如果使用交流电源 (120V) 电源，则交流电源插座应在距离底座 20 英尺以AOE内可用。
- 地板必须平整干净。
- 基座不得阻挡门或车道。
- 所有多余的电缆都应存放在底座内并固定。

要安装 Amazon One 设备底座

1. 从包装中取出 Amazon One Enterprise 底座。

2. 拧下两个 M4 防篡改螺丝，拆下门。
3. 插上电源线。将电缆穿过底座底板上的孔。
4. 将多余的电源线卷在底座内。
5. 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。
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. 将门重新安装到底座上，然后重新拧上两个 M4 防篡改螺丝以固定。

安装壁挂式 Amazon One 设备

本节详细介绍了安装壁挂式 Amazon One 设备所需的位置要求和步骤。

在开始安装之前，请确保满足以下条件：

- 壁挂式 Amazon One 设备仅供室内使用。
- 墙是水平的。
- 安装后，壁挂支架的顶部距离地面不应超过 44-46 英寸。
- 所有多余的电缆都放在壁挂支架后面并固定。
- 对于以太网供电 (PoE++)：

  确保 IEEE 802.3bt（类型 3）6 POE ++ 类交换机（末端跨度）或喷油器（中跨度）可供使用，这些交换机已列入上市或认证并符合 62368-1 标准。IEC

  只能AOE与经批准的 PoE++ 来源一起使用。

  PoE++ 源必须位于同一建筑物内。

- 对于 15V 直流电源输入，您只能使用 Amazon One 设备以及已列出或认证的 2 NEC 类电源或经认可的功率受限的电源。

必需的工具：

- 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

壁挂式 Amazon One 设备随附：

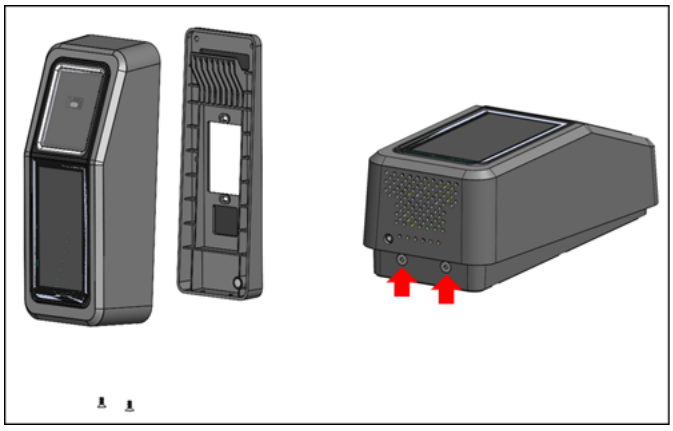
- 6x #8 石膏板锚
- 6x #8 -32 1 英寸长的螺丝
- 2x #6 -32 1 英寸机用螺丝
- 2x 6 位接线端子台连接器
- 2 个 Torx Security m4x10 平头螺丝

为您的 Amazon One 设备安装壁挂式安装板

<result>

</result>

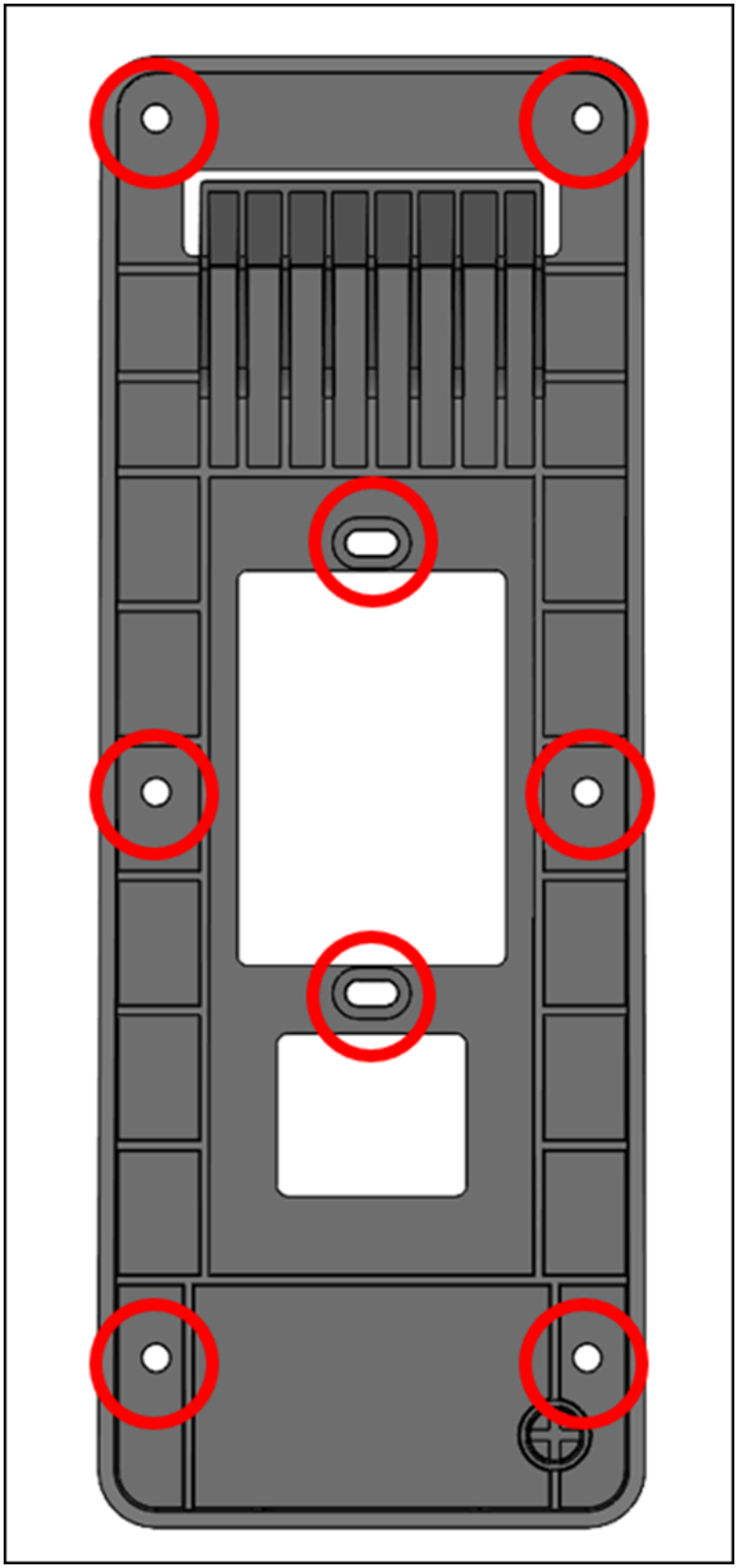
1. 从包装中取出您的 Amazon One 设备。
2. 拆下底部的两颗 Torx 安全螺丝，将安装板与 Amazon One 设备分开。



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。

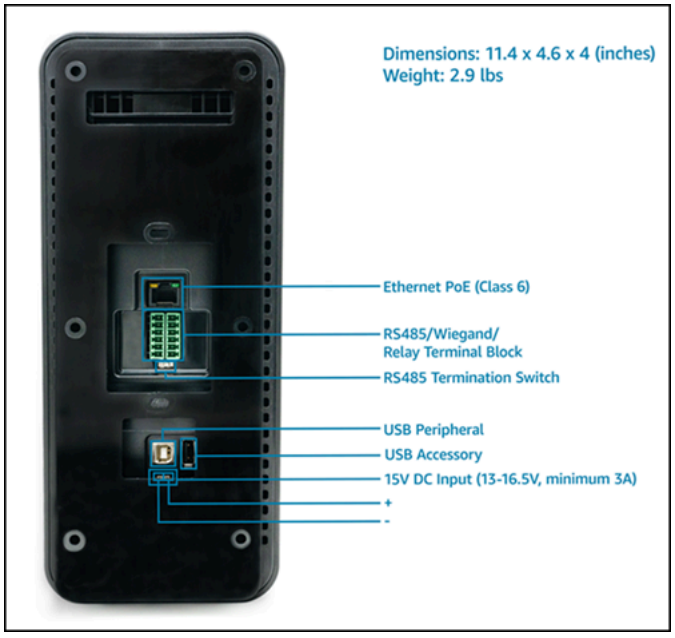
5. 在锚点位置使用 #8 木螺丝将墙板松散地固定在墙上。
6. 所有紧固件安装到位后，确保安装板处于水平状态。
7. 拧紧螺丝，将安装板固定在墙上。

连接您的壁挂式 Amazon One 设备

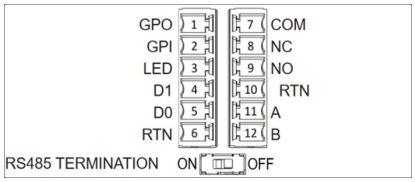
您可以使用 Weigand 访问控制协议配置 Amazon One 设备。OSDP为了简化安装，Amazon One 设备使用了接线端子连接器（Mfg P/N：Phoenix Contact 1767694）。您还可以选择将 Amazon One 设备配置为使用内部继电器或通用输入和输出连接直接控制外部设备。

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	LED	韦根 LED	韦根 — 可选 LED	
4	D1	Wiegand D1	韦根数据 1 — 白线	
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返回 — 黑线	
11	A	RS485_A/D1/ Clock	OSDPD1 — 白线	
12	B	RS485_b/D0/ Data	OSDPD0 — 绿色电线	

2. 安装电线时，从电线末端剥掉 3mm-5mm。

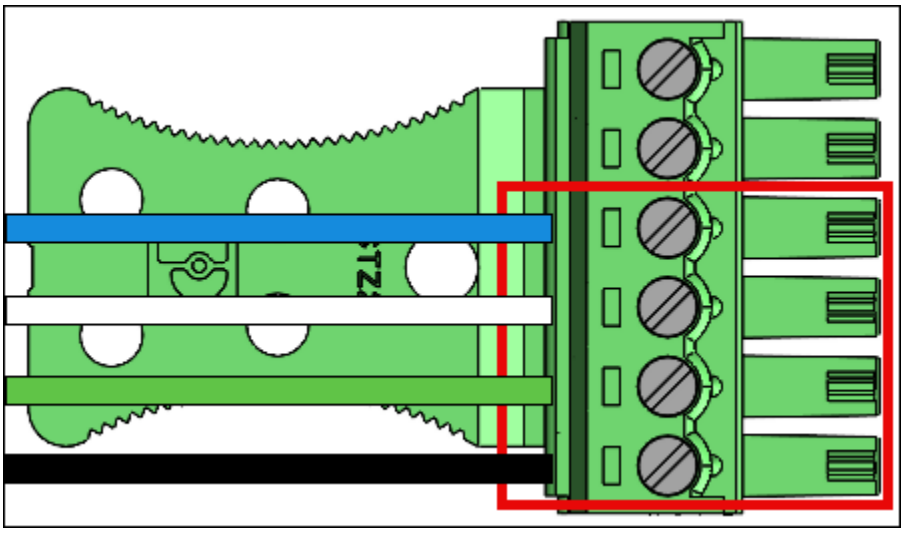
3. 将电线剥掉的一端插入所需的端子位置。
4. 使用一字螺丝刀，顺时针转动端子固定螺丝，将电线夹紧直至其紧固。不要过度拧紧。
5. 紧固后，轻轻地拉动电线以确保其固定到位。
6. 完成必要的连接后，将插头插入 Amazon One 设备接线板的相应插座中。
7. 将 Cat6 以太网电缆插入RJ45插孔。
8. 放置 Amazon One 设备，使墙板上的挂钩滑入设备背面的开口中。
9. 确保电缆没有卡在设备和安装板之间，然后让设备旋转并固定到位。
10. 用两颗 Torx Security m4x10 平头螺丝将你的 Amazon One 设备固定在安装板上。
11. 用手拧紧螺丝。不要过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

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)。



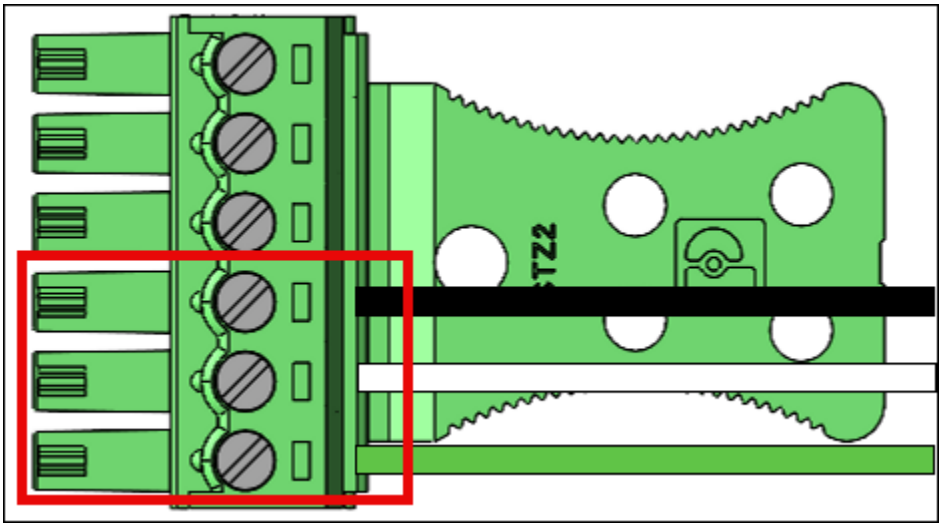
韦根输出接线

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

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)。

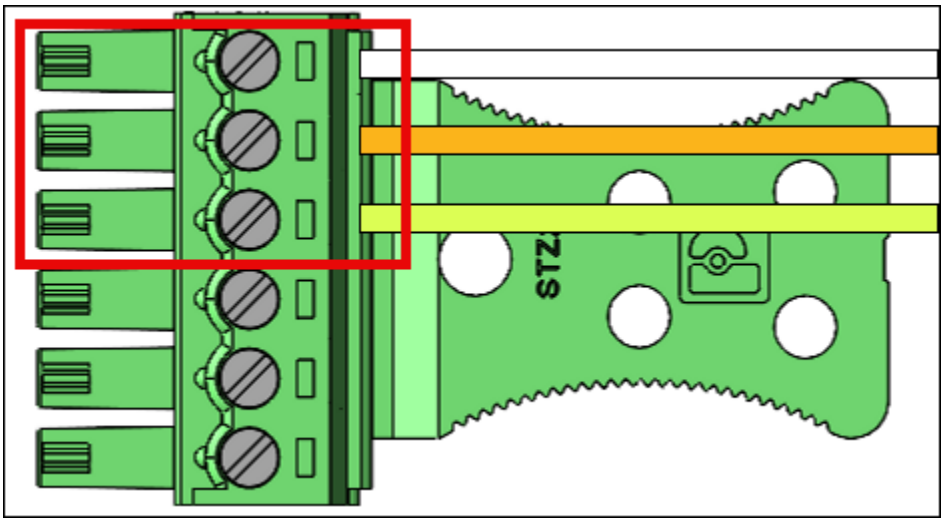


RS485接线

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

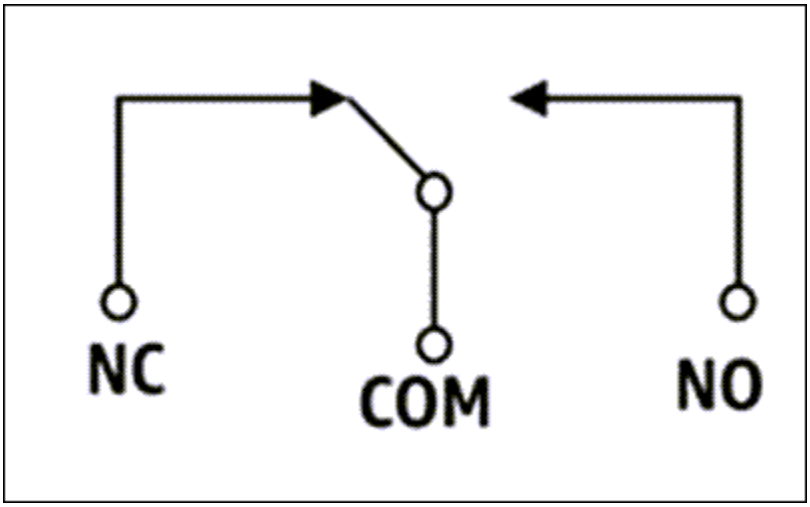
- 将白线插入引脚 7 (COM)。
- 将橙色电线插入引脚 8 (NC)。
- 将黄线插入引脚 9（否）。



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	

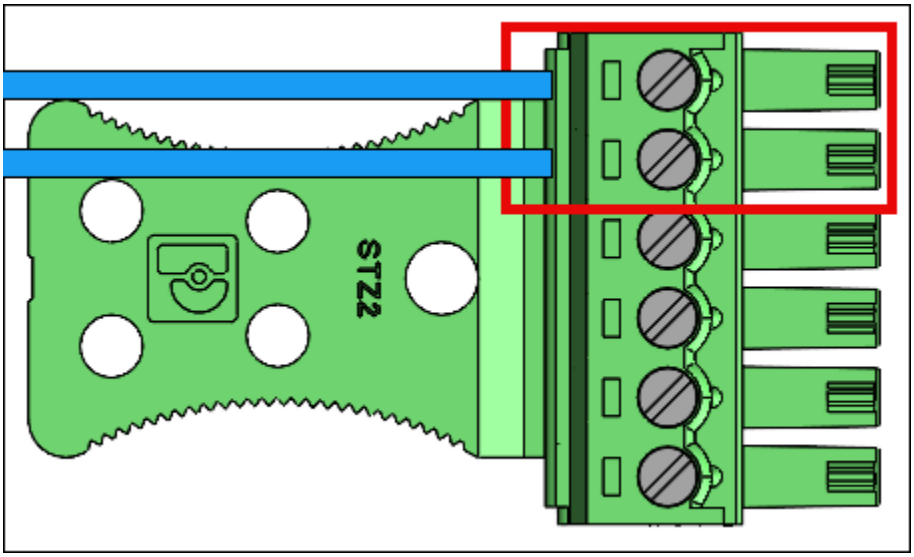
Pin	Connection	描述	使用	
8	NC	继电器常闭	触点继电器常闭 — 橙线	
9	NO	继电器常开	触点继电器常开 — 黄线	



继电器应按照规定的安全额定值运行 30 VAC /60VDC，最大值为 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)。



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

激活 Amazon One 设备要激活您的 Amazon One 设备，请参阅。

安装 Amazon One 设备 I/O 集线器以实现安全访问

本节详细介绍了安装带有 I/O Hub 的 Amazon One Enterprise (AOE) 设备所需的位置要求和步骤。

在开始安装之前，请确保满足以下条件：

- 带有 I/O 集线器的 Amazon One 设备仅供室内使用。
- 对于以太网供电 (PoE++)：

  确保 IEEE 802.3bt（类型 3）6 POE ++ 类交换机（末端跨度）或喷油器（中跨度）可供使用，这些交换机已列入上市或认证并符合 62368-1 标准。IEC

  只能使用具有经批准的 PoE++ 来源的 Amazon One 设备。

PoE++ 源必须位于同一建筑物内。

- 对于 15V 直流电源输入，您只能使用已列出或认证的 2 NEC 类电源或功率受限、经批准的电源的 Amazon One 设备。请参阅下面的 “可选 DC” 部分。

必需的工具：

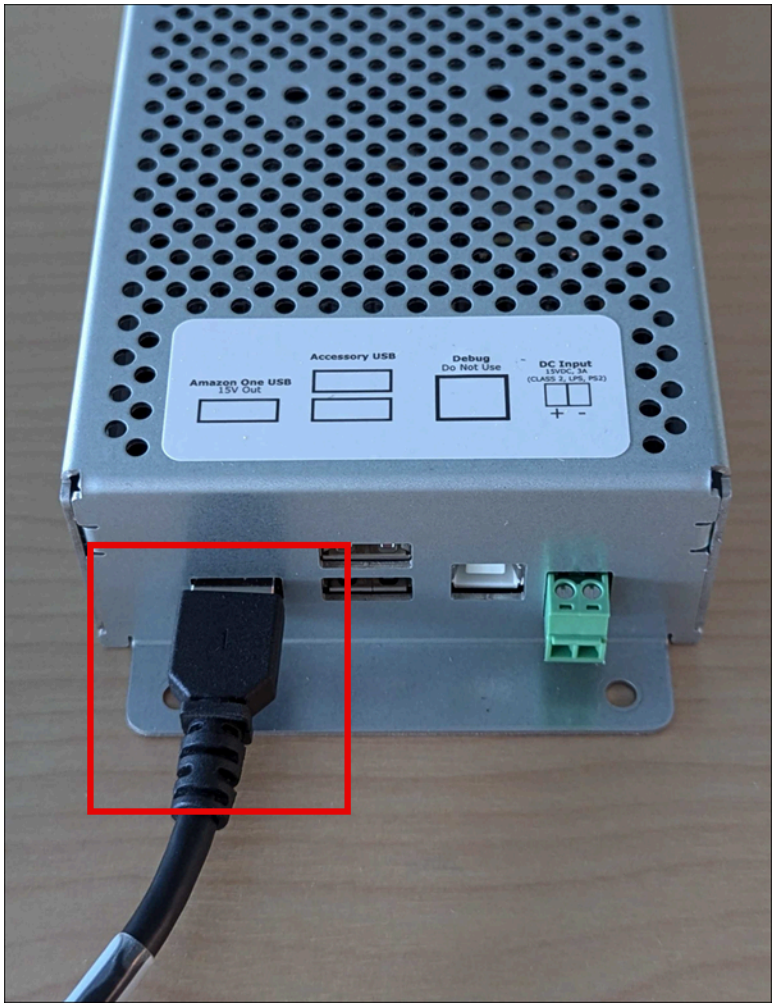
- 剥线钳
- #2 十字螺丝刀
- 0.5 毫米 x 2 毫米平头螺丝刀

带有 I/O 集线器的 Amazon One 设备随附：

- 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

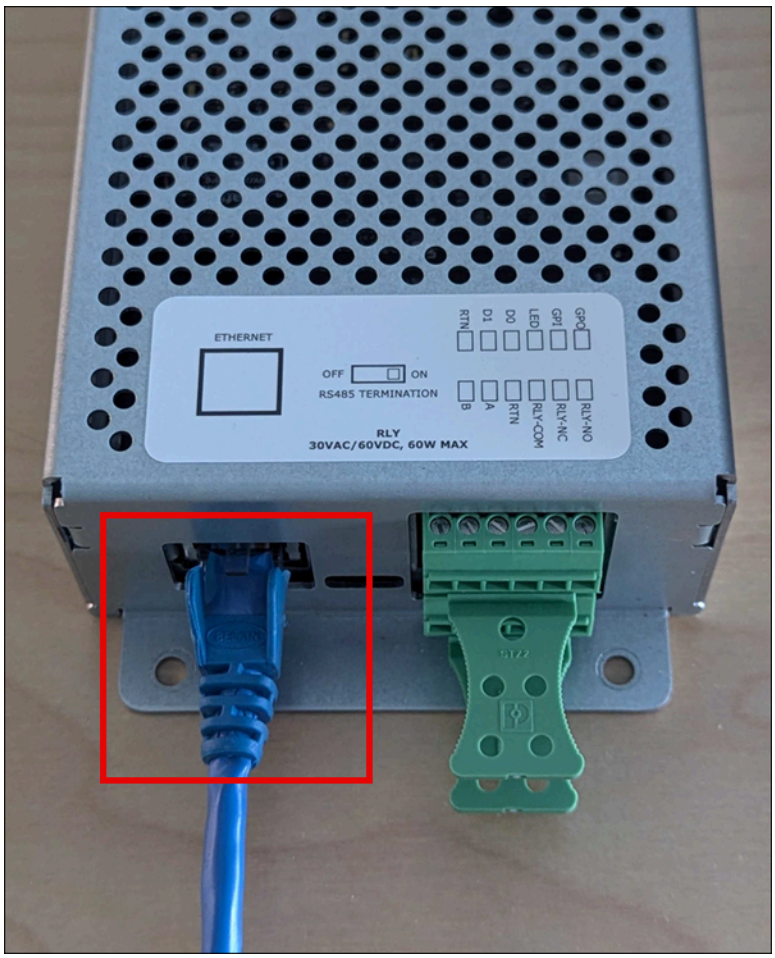
为您的 Amazon One 设备安装 I/O 集线器

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。



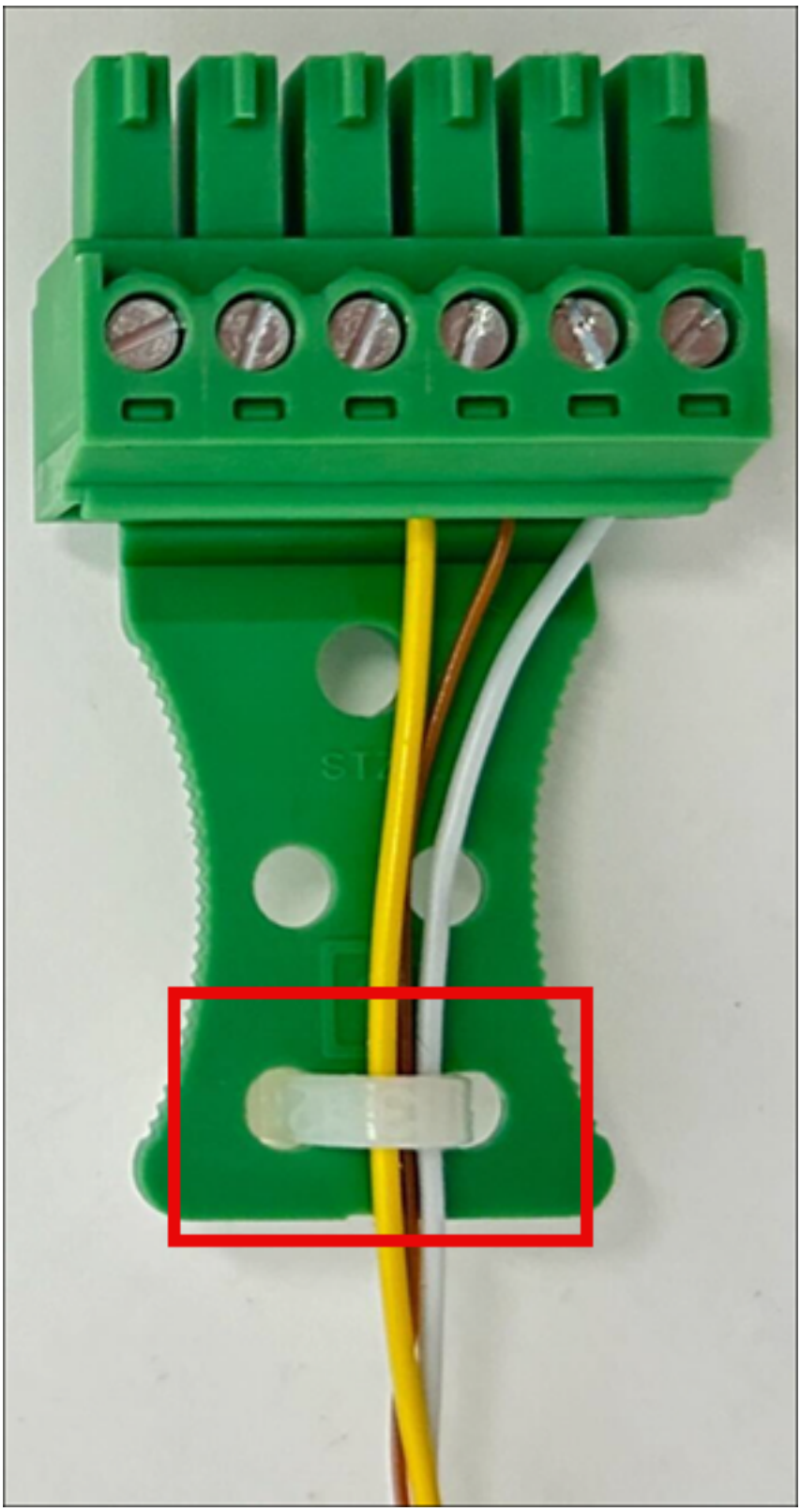
4. 要获POE得 ++ 电源，请将 POE ++ 电源的以太网电缆插入 I/O 集线器端口。

   可选：有关直流电源，请参阅下面的安装直流接线部分。

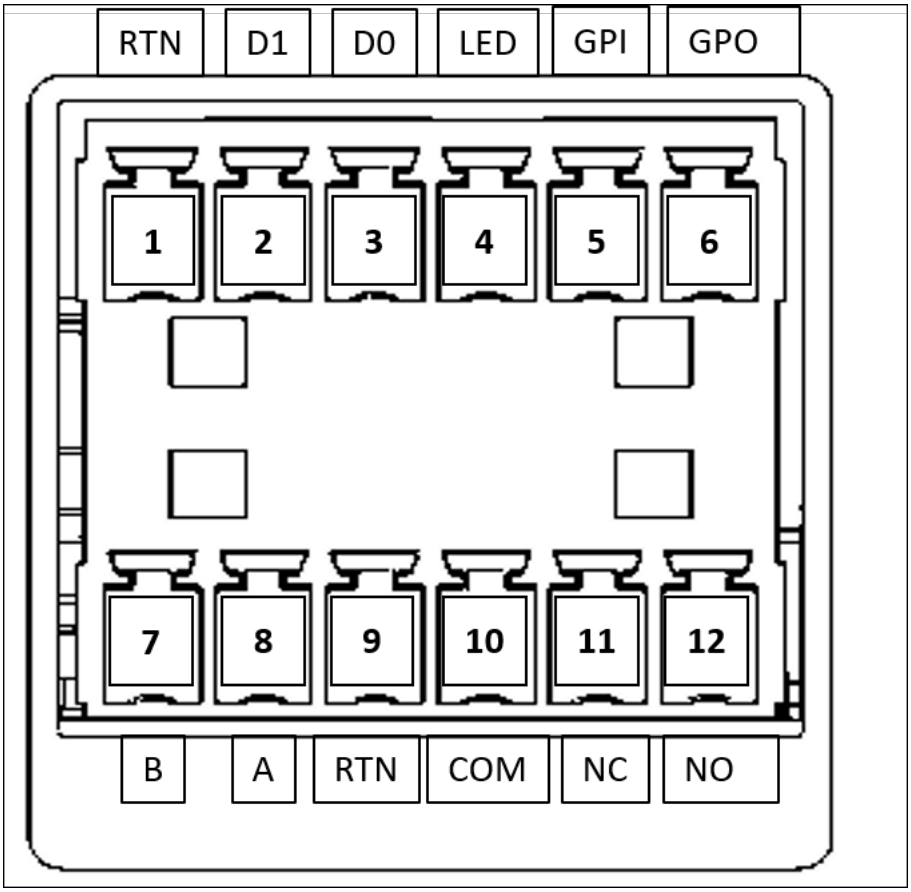


连接您的 Amazon One 设备的 I/O 集线器

- 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. 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。
2. 将接线板插头插入 I/O 集线器。

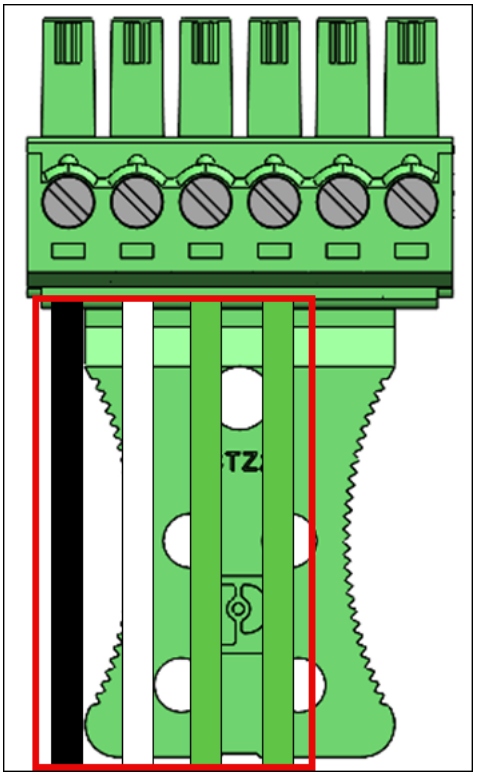


Pin	Connection	描述	使用	
1	RTN	信号返回	韦根接地 — 黑线	
2	D1	Wiegand D1	韦根数据 1 — 白线	
3	D0	Wiegand D0	韦根数据 0 — 绿线	
4	LED	韦根 LED	韦根 — 可选 LED	
5	GPI	通用输入	数字输入信号-可选	
6	GPO	通用输出	数字输出信号-可选	

Pin	Connection	描述	使用	
7	B	RS485_b/D0/ Data	OSDPD0 — 绿色电线	
8	A	RS485_A/D1/ Clock	OSDPD1 — 白线	
9	RTN	信号返回	OSDP返回 — 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	

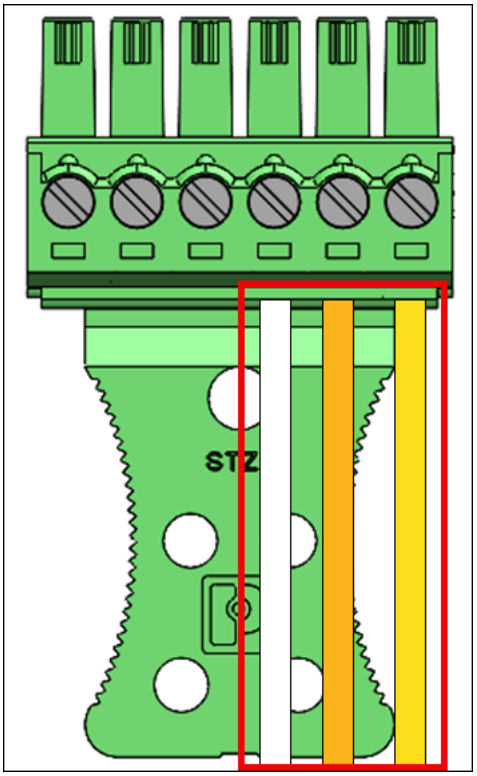
韦根连接

- 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)。

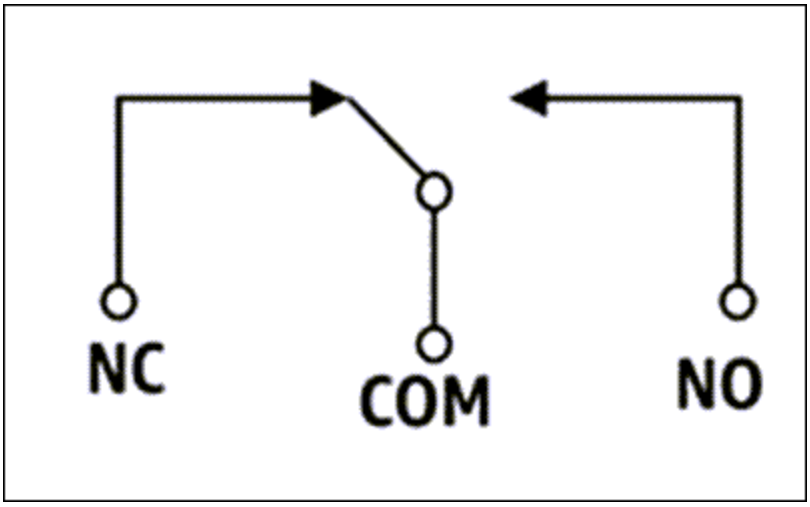


中继连接

- 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）。



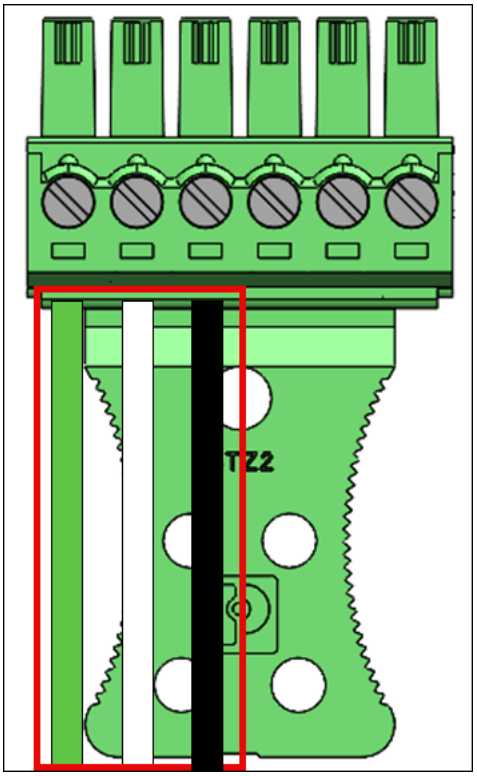
继电器图



继电器应按照规定的安全额定值运行 30 VAC /60VDC，最大值为 60W。

RS485连接

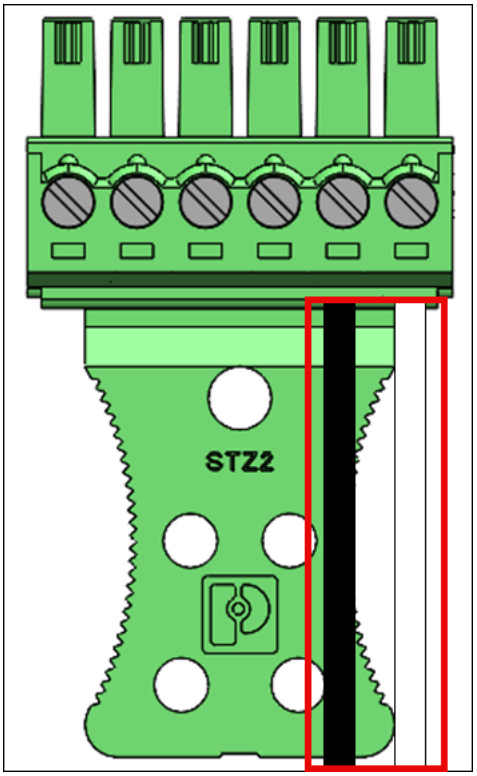
- 将绿色电线插入引脚 7 (B)。
- 将白线插入引脚 8 (A)。
- 将黑线插入引脚 9 (RTN)。



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

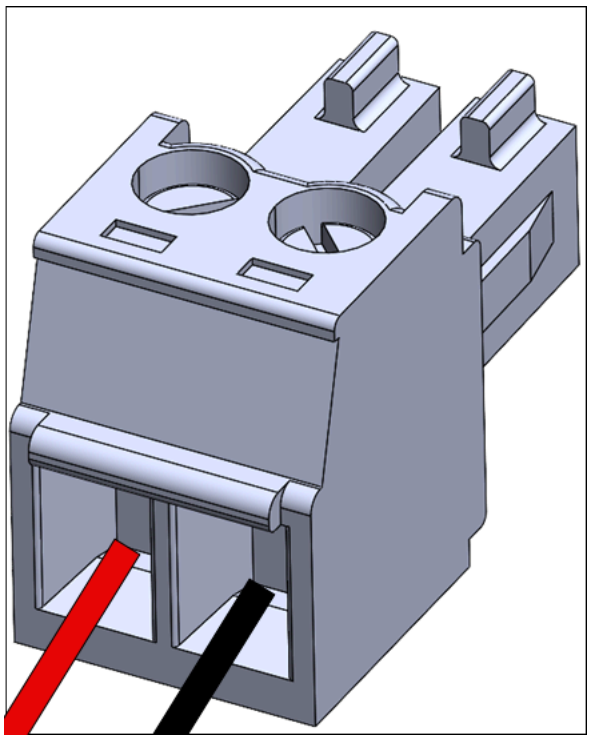
- 将黑线插入引脚 5 (GPI)。
- 将白线插入引脚 6 (GPO)。



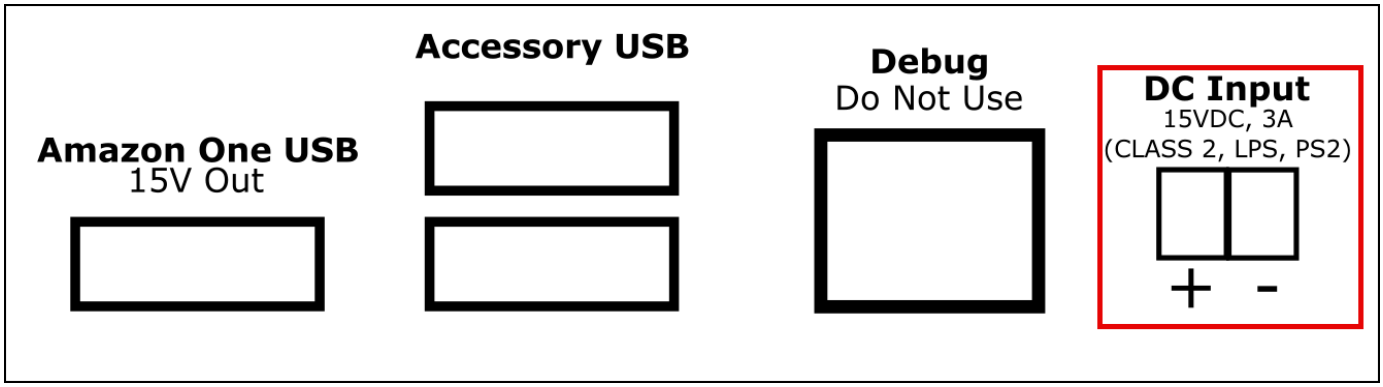
- 数字输入/输出连接应按所列方式运行。

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。



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，它就会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 第 2 步：添加 Amazon One 企业版用户。
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。
11. 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。

注册和入学

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

- 用户注册
- 通过身份验证进入

用户注册

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。

通过身份验证进入

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。

注册用户管理

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。

查看已注册的用户

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 — 徽章阅读器在注册时捕获的RFID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

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。

设备管理

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

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。

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

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 停用设备实例
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。

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

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

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（参见步骤 6：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。

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

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”。

Amazon One 企业版中的安全

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 Cloud。 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 企业版的合规性验证

亚马逊 One Enterprise 中的数据保护

这些区域有： AWS 分担责任模型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设施 AWS Cloud。 您有责任保持对托管在此基础架构上的内容的控制。您还负责以下各项的安全配置和管理任务 AWS 服务 你用的。有关数据隐私的更多信息，请参阅数据隐私FAQ。 有关欧洲数据保护的信息，请参阅 AWS 责任共担模型和GDPR博客文章 AWS 安全博客。

出于数据保护的目的，我们建议您进行保护 AWS 账户 凭据并使用设置个人用户 AWS IAM Identity Center 或者 AWS Identity and Access Management (IAM)。这样，每个用户只获得履行其工作职责所需的权限。我们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与之通信 AWS 资源的费用。我们需要 TLS 1.2，建议使用 TLS 1.3。
- 使用API进行设置和用户活动记录 AWS CloudTrail。 有关使用 CloudTrail 轨迹捕获的信息 AWS 活动，请参阅使用中的 CloudTrail 轨迹 AWS CloudTrail 用户指南。
- 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。
- 如果您在访问时需要 FIPS 140-3 经过验证的加密模块 AWS 通过命令行界面或API，使用FIPS端点。有关可用FIPS端点的更多信息，请参阅联邦信息处理标准 (FIPS) 140-3。

我们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）。这包括当你与 Amazon One Enterprise 或其他公司合作时 AWS 服务 使用控制台，API， AWS CLI，或 AWS SDKs。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URL向外部服务器提供，我们强烈建议您不要在中包含凭据信息，URL以验证您对该服务器的请求。

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自有密钥 — 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自有密钥，也无法审核其使用情况。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《密AWS钥管理服务开发者指南》中的AWS自有密钥。

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 来验证向AWS服务发送的所有入站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) 是一个 AWS 服务 可帮助管理员安全地控制对以下内容的访问权限 AWS 资源的费用。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。IAM是一个 AWS 服务 无需支付额外费用即可使用。

主题

受众

你怎么用 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 企业版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管理员提交更改服务用户权限的请求。查看此页面上的信息以了解的基本概念IAM。要详细了解贵公司如何IAM与 Amazon One Enterprise 配合使用，请参阅Amazon One Enterprise 如何 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。要查看可在中使用的 Amazon One Enterprise 基于身份的策略示例IAM，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

身份验证是您登录的方式 AWS 使用您的身份凭证。您必须经过身份验证（登录到 AWS) 作为 AWS 账户根用户、以IAM用户身份或通过担任IAM角色来完成。

你可以登录 AWS 使用通过身份源提供的凭证作为联合身份。 AWS IAM Identity Center （IAM身份中心）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，您的管理员之前使用IAM角色设置了联合身份。当你访问时 AWS 通过使用联合，您就是在间接担任角色。

根据您的用户类型，您可以登录 AWS Management Console 或者 AWS 访问门户。有关登录的更多信息 AWS，请参阅如何登录您的 AWS 账户中的 AWS 登录 用户指南。

如果你访问 AWS 以编程方式， AWS 提供了一个软件开发套件 (SDK) 和一个命令行界面 (CLI)，用于使用您的凭证对您的请求进行加密签名。如果你不使用 AWS 工具，你必须自己签署请求。有关使用推荐的方法自行签署请求的更多信息，请参阅签名 AWS APIIAM用户指南中的请求。

无论使用何种身份验证方法，您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) 来提高帐户的安全性。要了解更多信息，请参阅中的多重身份验证 AWS IAM Identity Center《用户指南》和《使用多因素身份验证》(MFA) AWS（在 IAM 用户指南中）。

AWS 账户 根用户

当你创建 AWS 账户，您从一个登录身份开始，该身份可以完全访问所有人 AWS 服务 以及账户中的资源。这个身份叫做 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。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。有关需要您以 root 用户身份登录的任务的完整列表，请参阅用户指南中的需要根用户凭证的IAM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进行访问 AWS 服务 通过使用临时证书。

联合身份是企业用户目录中的用户、Web 身份提供商、 AWS Directory Service、身份中心目录或任何访问的用户 AWS 服务 通过使用通过身份源提供的凭证。当联合身份访问时 AWS 账户，他们扮演角色，角色提供临时证书。

对于集中访问管理，我们建议您使用 AWS IAM Identity Center。 您可以在 Ident IAM ity 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，以便在您的所有用户和群组中使用 AWS 账户 和应用程序。有关IAM身份中心的信息，请参阅什么是IAM身份中心？ 在 AWS IAM Identity Center 用户指南。

IAM 用户和组

IAM用户是你内部的身份 AWS 账户 对个人或应用程序具有特定权限。在可能的情况下，我们建议使用临时证书，而不是创建拥有密码和访问密钥等长期凭证的IAM用户。但是，如果您有需要IAM用户长期

凭证的特定用例，我们建议您轮换访问密钥。有关更多信息，请参阅《IAM用户指南》中的定期轮换需要长期凭证的用例的访问密钥。

IAM群组是指定IAM用户集合的身份。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并授予该群组管理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》中的何时创建IAM用户（而不是角色）。

IAM角色

IAM角色是你内在的身份 AWS 账户 具有特定权限的。它与IAM用户类似，但与特定人员无关。你可以暂时扮IAM演一个角色 AWS Management Console 通过切换角色。你可以通过调用来扮演角色 AWS CLI 或者 AWS API操作或使用自定义URL。有关使用角色的方法的更多信息，请参阅IAM用户指南中的使用IAM角色。

IAM具有临时证书的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》中的为第三方身份提供商创建角色。如果您使用 IAM Identity Center，则需要配置权限集。为了控制您的身份在进行身份验证后可以访问的内容，Ident IAM ity Center 会将权限集关联到中的IAM角色。有关权限集的信息，请参阅中的权限集 AWS IAM Identity Center 用户指南。
- 临时IAM用户权限-IAM 用户或角色可以代入一个IAM角色，为特定任务临时获得不同的权限。
- 跨账户访问-您可以使用IAM角色允许其他账户中的某人（受信任的委托人）访问您账户中的资源。角色是授予跨账户访问权限的主要方式。但是，有些 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）。要了解角色和基于资源的跨账户访问策略之间的区别，请参阅IAM用户指南IAM中的跨账户资源访问权限。
- 跨服务访问 — 一些 AWS 服务 使用其他功能 AWS 服务。 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，你被视为校长。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使用委托人的权限调用 AWS 服务，再加上请求的 AWS 服务 向下游服务发出请求。FAS只有当服务收到需要与其他

服务进行交互的请求时，才会发出请求 AWS 服务 或需要完成的资源。在这种情况下，您必须具有执行这两个操作的权限。有关提出FAS请求时的政策详情，请参阅转发访问会话。

- 服务角色-服务IAM角色是服务代替您执行操作的角色。IAM管理员可以在内部创建、修改和删除服务角色IAM。有关更多信息，请参阅创建角色以向某人委派权限 AWS 服务（在 IAM 用户指南中）。
- 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。 该服务可以代替您执行操作。服务相关角色显示在您的 AWS 账户 并归该服务所有。IAM管理员可以查看但不能编辑服务相关角色的权限。

- 在 Amazon 上运行的应用程序 EC2 — 您可以使用IAM角色管理在EC2实例上运行的应用程序的临时证书 AWS CLI 或者 AWS API请求。这比在EC2实例中存储访问密钥更可取。要分配 AWS 在EC2实例中扮演角色并使其可供其所有应用程序使用，则可以创建附加到该实例的实例配置文件。实例配置文件包含角色并允许在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 Amazon EC2 实例上运行的应用程序授予权限。

要了解是使用IAM角色还是使用IAM用户，请参阅《用户指南》中的何时创建IAM角色（而不是IAM用户）。

使用策略管理访问

您可以控制访问权限 AWS 通过创建策略并将其附加到 AWS 身份或资源。策略是中的一个对象 AWS 当与身份或资源关联时，它定义了他们的权限。 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。大多数策略都存储在 AWS 作为JSON文件。有关JSON策略文档结构和内容的更多信息，请参阅《IAM用户指南》中的JSON策略概述。

管理员可以使用 AWS JSON用于指定谁有权访问什么的策略。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。要授予用户对其所需资源执行操作的权限，IAM管理员可以创建IAM策略。然后，管理员可以将IAM策略添加到角色中，用户可以代入这些角色。

IAM无论您使用何种方法执行操作，策略都会定义该操作的权限。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中获取角色信息 AWS Management Console，AWS CLI，或者 AWS API.

基于身份的策略

基于身份的策略是可以附加到身份（例如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用户指南中的创建IAM策略。

基于身份的策略可以进一步归类为内联策略或托管策略。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，您可以将其附加到您的多个用户、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或内联策略之间进行选择，请参阅《IAM用户指南》中的在托管策略和内联策略之间进行选择。

基于资源的策略

基于资源的JSON策略是您附加到资源的策略文档。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。你不能用 AWS 基于资源的策略IAM中的托管策略。

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。

亚马逊 S3， AWS WAF，Amazon VPC 就是支持的服务示例ACLs。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-权限边界是一项高级功能，您可以在其中设置基于身份的策略可以向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 是一项用于对多个进行分组和集中管理的服务 AWS 账户 你的企

业拥有的。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限制了成员账户中实体的权限，包括每个 AWS 账户根用户。 有关 Organizations 和的更多信息SCPs，请参阅《》中的服务控制策略 AWS Organizations 用户指南。

- 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。要了解如何做 AWS 决定在涉及多种策略类型时是否允许请求，请参阅IAM用户指南中的策略评估逻辑。

Amazon One Enterprise 如何 IAM

在使用IAM管理对 Amazon One Enterprise 的访问权限之前，请先了解 Amazon One Enterprise 有哪些IAM功能可供使用。

IAM您可以在 Amazon One Enterprise 上使用的功能

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	不支持
ABAC（策略中的标签）	是
临时凭证	是
主体权限	是

IAM特征	亚马逊 One 企业版支持
服务角色	否
服务相关角色	否

深入了解 Amazon One Enterprise 和其他公司的情况 AWS 服务适用于大多数IAM功能，请参阅 AWS《IAM用户指南》IAM中与之配合使用的服务。

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以附加到身份（例如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用户指南中的创建IAM策略。

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。要了解可以在JSON策略中使用的所有元素，请参阅IAM用户指南中的IAMJSON策略元素参考。

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JSON策略是您附加到资源的策略文档。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另一个账户中的IAM实体指定为基于资源的策略中的委托人。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状态时 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》IAM中的跨账户资源访问权限。

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用于指定谁有权访问什么的策略。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`Action`元素描述了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同名 AWS API操作。也有一些例外，例如没有匹配API操作的仅限权限的操作。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用于指定谁有权访问什么的策略。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。

ResourceJSON策略元素指定要应用操作的一个或多个对象。语句必须包含 Resource 或 NotResource 元素。最佳做法是，使用资源的 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ARN种资源的类型，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用于指定谁有权访问什么的策略。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。

如果您在一条语句中指定多个Condition元素，或者在单个Condition元素中指定多个键， AWS 使用逻辑AND运算对其进行评估。如果您为单个条件键指定多个值， AWS 使用逻辑OR运算评估条件。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，只有在资源上标有IAM用户的用户名时，您才能向IAM用户授予访问该资源的权限。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。要查看全部 AWS 全局条件键，请参见 AWS 《IAM 用户指南》中的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使用 Amazon One Enter

支持ABAC（策略中的标签）：是

基于属性的访问控制 (ABAC) 是一种基于属性定义权限的授权策略。In AWS，这些属性称为标签。您可以将标签附加到IAM实体（用户或角色）和许多实体 AWS 资源的费用。为实体和资源添加标签是的第一步。ABAC然后，您可以设计ABAC策略，允许在委托人的标签与他们尝试访问的资源上的标签匹配时进行操作。

ABAC在快速增长的环境中很有用，也有助于解决策略管理变得繁琐的情况。

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。

有关的更多信息ABAC，请参阅什么是ABAC？ 在《IAM用户指南》中。要查看包含设置步骤的教程ABAC，请参阅IAM用户指南中的使用基于属性的访问控制 (ABAC)。

在亚马逊 One Enterprise 上使用临时证书

支持临时凭证：是

一段时间 AWS 服务 使用临时证书登录时不起作用。欲了解更多信息，包括哪个 AWS 服务 使用临时证书，请参阅 AWS 服务 可以IAM在《IAM用户指南》中使用。

如果您登录，则使用的是临时证书 AWS Management Console 使用除用户名和密码之外的任何方法。例如，当你访问时 AWS 使用贵公司的单点登录 (SSO) 链接，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》中的切换到角色（控制台）。

您可以使用手动创建临时证书 AWS CLI 或者 AWS API。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，请参阅中的临时安全证书IAM。

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，你被视为校长。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使用委托人的权限调用 AWS 服务，再加上请求的 AWS 服务 向下游服务发出请求。FAS只有当服务收到需要与其他服务进行交互的请求时，才会发出请求 AWS 服务 或需要完成的资源。在这种情况下，您必须具有执行这两个操作的权限。有关提出FAS请求时的政策详情，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IAM角色是服务代替您执行操作的角色。IAM管理员可以在内部创建、修改和删除服务角色IAM。有关更多信息，请参阅创建角色以向某人委派权限 AWS 服务（在 IAM 用户指南中）。

> **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 Enterprise 服务相关角色

支持服务相关角色：否

服务相关角色是一种与服务相关联的服务角色 AWS 服务。 该服务可以代替您执行操作。服务相关角色显示在您的 AWS 账户 并归该服务所有。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 AWS 与之配合使用的服务IAM。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。他们也无法通过使用来执行任务 AWS Management Console, AWS Command Line Interface (AWS CLI)，或 AWS API。要授予用户对其所需资源执行操作的权限，IAM管理员可以创建IAM策略。然后，管理员可以将IAM策略添加到角色中，用户可以代入这些角色。

要了解如何使用这些示例策略文档创建IAM基于身份的JSON策略，请参阅IAM用户指南中的创建IAM策略。

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

基于身份的策略决定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。这些操作可能会使您付出代价 AWS 账户。 创建或编辑基于身份的策略时，请遵循以下准则和建议：

- 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 AWS 为许多常见用例授予权限的托管策略。它们在你的 AWS 账户。 我们建议您通过定义来进一步减少权限 AWS 特定于您的用例的客户托管政策。有关更多信息，请参阅 AWS 托管策略或 AWS 《IAM 用户指南》 中工作职能的托管策略。
- 应用最低权限权限-使用IAM策略设置权限时，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。有关使用应用权限IAM的更多信息，请参阅IAM用户指南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-您可以在策略中添加条件以限制对操作和资源的访问权限。例如，您可以编写一个策略条件来指定所有请求都必须使用发送SSL。如果通过特定条件使用

服务操作，则也可以使用条件来授予对服务操作的访问权限 AWS 服务之外的压缩算法（例如 AWS CloudFormation。 有关更多信息，请参阅《IAM用户指南》中的IAMJSON策略元素：条件。

- 使用 A IAM ccess Analyzer 验证您的IAM策略以确保权限的安全性和功能性 — A IAM ccess Analyzer 会验证新的和现有的策略，以便策略符合IAM策略语言 (JSON) 和IAM最佳实践。IAMAccess Analyzer 提供了 100 多项策略检查和可行的建议，可帮助您制定安全和实用的策略。有关更多信息，请参阅《IAM用户指南》中的 IAMAccess Analyzer 策略验证。
- 需要多因素身份验证 (MFA)-如果您的场景需要IAM用户或 root 用户 AWS 账户，请打开MFA以提高安全性。要要求MFA何时调用API操作，请在策略中添加MFA条件。有关更多信息，请参阅《IAM用户指南》中的配置MFA受保护的API访问权限。

有关中最佳做法的更多信息IAM，请参阅《IAM用户指南》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您的 Amazon One Enterprise 资源的详细信息 AWS 账户。 如果您创建的基于身份的策略比所需的最低权限更严格，则控制台将无法按预期运行，适用于使用该策略的实体（用户或角色）。

您无需为仅拨打控制台的用户设置最低控制台权限 AWS CLI 或者 AWS API。相反，只允许访问与他们尝试执行的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，还需要附上 Amazon One Enterprise *ConsoleAccess* 或 *ReadOnly* AWS 针对实体的托管策略。有关更多信息，请参阅《用户指南》中的向IAM用户添加权限。

允许用户查看他们自己的权限

此示例说明如何创建允许IAM用户查看附加到其用户身份的内联和托管策略的策略。此策略包括通过控制台或以编程方式使用控制台完成此操作的权限 AWS CLI 或者 AWS API.

```
{
    "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 AWS 托管策略`AmazonOneEnterpriseReadOnlyAccess`，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。该Resource元素列出了 AWS 允许用户对其执行这些操作的资源。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:*"]

  这允许执行所有 Amazon One Enterprise 操作，但不允许其他操作 AWS 服务的支持。
- "Action": ["*"]

  这允许所有 AWS 行动。此权限适用于充当 AWS 您账户的管理员。

只读策略不向用户授予执行诸如CreateDeviceInstanceUpdateDeviceInstance、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 企业规则操作支持的资源级权限 API

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。指定时ARN，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IDs时。

> **Important**
>
> 如果此表中未列出 Amazon One Enterprise 规则API操作，则它不支持资源级权限。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行动	资源
CreateDeviceInstance	设备实例 arn: aws: one:*region:accountID* :device-instance/*deviceInstanceId*
GetDeviceInstance	设备实例 arn: aws: one:*region:accountID* :device-instance/*deviceInstanceId*
UpdateDeviceInstance	设备实例

API行动	资源
	arn: aws: one:*region:accountID* :device-instance/*deviceInstanceId*
DeleteDeviceInstance	设备实例 arn: aws: one:*region:accountID* :device-instance/*deviceInstanceId*
CreateDeviceActivationQrCode	设备实例 arn: aws: one:*region:accountID* :device-instance/*deviceInstanceId*
DeleteAssociatedDevice	设备实例 arn: aws: one:*region:accountID* :device-instance/*deviceInstanceId*
RebootDevice	设备实例 arn: aws: one:*region:accountID* :device-instance/*deviceInstanceId*
CreateDeviceInstanceConfiguration	设备实例配置 arn: aws: one:*region:accountID* :device-instance/*deviceInstanceId* /配置/*version*
GetDeviceInstanceConfiguration	设备实例配置 arn: aws: one:*region:accountID* :device-instance/*deviceInstanceId* /配置/*version*
CreateSite	Site arn: aws: one:*region:accountID* :site/*siteId*

API行动	资源
DeleteSite	Site arn: aws: one:*region:accountID* :site/*siteId*
GetSiteAddress	Site arn: aws: one:*region:accountID* :site/*siteId*
UpdateSite	Site arn: aws: one:*region:accountID* :site/*siteId*
UpdateSiteAddress	Site arn: aws: one:*region:accountID* :site/*siteId*
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，您允许 AWS Config 规则读取操作，例如`GetSite`对指定规则的操作。

```
{
        "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"
           }
      ]
   }
```

使用资源级权限，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、群组、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用户和管理员群组以及访问管理。IAM

AWS 亚马逊 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托管式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 当新服务启动或现有服务 AWS 服务 有新API操作可用时，最有可能更新 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 Enterprise 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取和写入权限，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 Enterprise 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 Enterprise 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 Feed。

更改	描述	日期
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

对 Amazon One 企业版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 时可能遇到的常见问题，以及IAM。

主题

- 我无权在 Amazon One Enterprise 中执行任何操作
- 我想允许我以外的人进入 AWS 账户 访问我的 Amazon One 企业版资源

我无权在 Amazon One Enterprise 中执行任何操作

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

当mateojacksonIAM用户尝试使用控制台查看虚构*my-example-widget*资源的详细信息但没有虚构权限时，就会出现以下示例错误。one:*GetWidget*

```
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进入 AWS 账户 访问我的 Amazon One 企业版资源

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，可以担任角色。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Amazon One Enterprise 如何 IAM。
- 了解如何提供对您的资源的访问权限 AWS 账户 您拥有的，请参阅向其他IAM用户提供访问权限 AWS 账户 您在《IAM用户指南》中拥有的。
- 了解如何向第三方提供对您的资源的访问权限 AWS 账户，请参阅提供访问权限 AWS 账户IAM用户指南中归第三方所有。
- 要了解如何通过联合身份验证提供访问权限，请参阅《用户指南》中的向经过外部身份验证的用户提供访问权限（联合身份验证）。IAM
- 要了解使用角色和基于资源的策略进行跨账户访问的区别，请参阅IAM用户指南IAM中的跨账户资源访问权限。

Amazon One Enterprise 的操作、资源和条件键

Amazon One Enterprise（服务前缀:one）提供以下特定于服务的资源、操作和条件上下文密钥，供在IAM权限策略中使用。

主题

- Amazon One Enprise 定义的操作
- Amazon One Enterprise 定义的资源类型

- Amazon One Enterprise 的条件键

Amazon One Enprise 定义的操作

您可以在IAM策略声明的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。当您在策略中使用操作时，通常会允许或拒绝访问具有相同名称的API操作或CLI命令。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（“*”）。如果该列包含资源类型，则可以在带有该操作ARN的语句中指定该类型的资源类型。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。如果您使用IAM策略中的Resource元素限制资源访问权限，则必须为每种必需的资源类型包含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	

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
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*		
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*		

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

操作	描述	访问级别	资源类型（* 为必需）	条件键	相关操作
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*		
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

以下资源类型由此服务定义，可以在IAM权限策略语句的Resource元素中使用。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/${TagKey}
Device Instance Configuration	arn:aws:one: *region:accountID* :device-instance/ *deviceInstanceId* /configuration/ *version*	
Site	arn:aws:one: *region:accountID* :site/*siteId*	aws:ResourceTag/${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 定义了以下可在IAM策略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/${TagKey}	按请求中的标签筛选访问权限	String
aws:ResourceTag/${TagKey}	按与资源关联的标签筛选访问权限	String

条件键	描述	类型
aws:TagKeys	按请求中的标签键筛选访问权限	ArrayOfString

亚马逊 One 企业版的合规性验证

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：

- 安全与合规性快速入门指南 — 这些部署指南讨论了架构注意事项，并提供了在这些基础上 AWS 部署以安全性和合规性为重点的基准环境的步骤。
- 在 Amazon Web Services 上进行HIPAA安全与合规架构 — 本白皮书描述了各公司如何使用 AWS 来创建HIPAA符合条件的应用程序。

> **Note**
>
> 并非所有 AWS 服务 人都有HIPAA资格。有关更多信息，请参阅《HIPAA符合条件的服务参考》。

- AWS 合规资源AWS — 此工作簿和指南集可能适用于您所在的行业和所在地区。
- 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 提供了您内部安全状态的全面视图 AWS。Security Hub 通过安全控件评估您的 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件的列表，请参阅 Security Hub 控件参考。

- 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 可以帮助您满足各种合规性要求 PCIDSS，例如满足某些合规性框架规定的入侵检测要求。
- 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。

记录和监控亚马逊 One Enterprise

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 账户发出的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 《AWS CloudTrail 用户指南》。

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. 打开 EventBridge 控制台，网址为https://console.aws.amazon.com/events/。
2. 在导航窗格的 “总线” 下，选择 “规则”。
3. 选择创建规则。
4. 在默认规则详细信息页面上，为规则指定名称，选择带有事件模式的规则，然后选择下一步。
5. 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。
6. 在 “示例事件类型” 下，选择 “输入我自己的类型”。

7. 从其中一个中复制并粘贴示例事件。
8. 在 “创建方法” 中，选择 “自定义图案”。在事件模式部分，添加事件源为**aws:one**和所需的详细信息类型，然后选择下一步。JSON
9. 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。
10. 或者，您可以配置标签。
11. 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

设备状态更改事件是在中生成的JSON。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。

资源

包含发布设备状态更改事件的 deviceInstance arn 列表。

metadata

siteName

- 存在的站点 deviceInstance 的名称。

siteArn

- Arn 表示 deviceInstance 存在的站点。

数据

currentConnectivity

- 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：CONNECTED，DISCONNECTED

previousConnectivity

- 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：CONNECTED，DISCONNECTED

currentHealthStatus

- 表示是否 deviceInstance 已通过所有运行状况检查。
- 可能的值：HEALTHY，CRITICAL

previousHealthStatus

- 表示上次检查时是否 deviceInstance 通过了所有运行状况检查。
- 可能的值：HEALTHY，CRITICAL

assetTagId

- 与关联 assetTagId 的设备的deviceInstance。

deviceInstanceName

- 发布设备状态事件的名称。 deviceInstance

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。

资源

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。

requestSource

- 这是发起请求 deviceInstanceId 的设备。

createdTimestamp

- 事件的创建时间。

userStatus

- 用户的当前状态。
- 可能的值：ACTIVE，DELETED

associatedId

- 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

设备通过了所有运行状况，设备实例的运行状况更改为HEALTHY从CRITICAL健康状态。

```
{
    "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更改为CRITICAL从HEALTHY。

```
{
  "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更改为CONNECTED从DISCONNECTED。

```
{
  "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已更改为DISCONNECTED从CONNECTED。

```
{
  "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"
    }
  }
}
```

新成功注册

用户成功注册时发生的事件。

```
{
    "version": "0",
    "id": "aebc9c86-f20e-75db-caaa-63bf14926f59",
```

```
    "detail-type": "New Successful Enrollment",
    "source": "aws.one",
    "account": "679792848029",
    "time": "2023-11-22T02:55:17Z",
    "region": "us-east-1",
    "resources": [
        "arn:aws:one:us-east-1:679792848029:user"
    ],
    "detail": {
        "version": "1.0.0",
        "data": {
            "accountId": "679792848029",
            "enrollmentSource": "QfUuUnFqs5accJ",
            "createdTimestamp": "2023-11-22T02:55:17Z",
            "userStatus": "ACTIVE",
            "associatedIds": "[{\"associatedIdType\":\"badge\",\"associatedIdValue\":
\"1111358294500\"}]",
        }
    }
}
```


使用记录 Amazon One 企业API通话 AWS CloudTrail

Amazon One Enterprise 与 AWS CloudTrail一项服务集成，可记录用户、角色或 AWS 服务在 Amazon One Enterprise 中采取的操作。 CloudTrail 将 Amazon One Enterprise 的所有API呼叫记录为事件。捕获的呼叫包括来自 Amazon One Enterprise 控制台的调用和对 Amazon One Enterprise API 操作的代码调 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
- 为以下各项配置亚马逊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`

每个事件或日记账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 root 还是 AWS Identity and Access Management (IAM) 用户凭据发出。
- 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"
}
```

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	新增主题：安装 Amazon One 设备 I/O 集线器以实现安全访问 Amazon One Enterprise 用户指南	2024年8月14日
更新	新增主题：安装壁挂式 Amazon One 设备 Amazon One Enterprise 用户指南	2024 年 6 月 5 日
初始版本	Amazon One 企业用户指南的初始版本	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。