aws

用户指南

AWS 登录

AWS 登录: 用户指南

Table of Contents

什么是 AWS 登录？

本指南可帮助您了解不同类型的用户登录 Amazon Web Services (AWS) 的不同方式。有关如何根据您的用户类型和要访问的 AWS 资源进行登录的更多信息，请参阅以下教程之一。

- 登录 AWS Management Console
- 登录 AWS 访问门户
- 以联合身份登录
- 通过登录 AWS Command Line Interface
- 使用登录 AWS 构建者 ID

如果您在登录时遇到问题 AWS 账户，请参阅AWS 账户 登录问题疑难解答。如需帮助， AWS 构建者 ID 请参阅对 AWS 生成器 ID 问题进行故障排除。想要创建一个 AWS 账户？ 报名参加 AWS. 有关注册对 AWS 您或您的组织有何帮助的更多信息，请参阅联系我们。

主题

术语

Amazon Web Services (AWS) 使用常用术语来描述登录流程。我们建议您阅读并理解这些术语。

管理员

也称为 AWS 账户 管理员或 IAM 管理员。管理员通常是信息技术（IT）人员，负责监管 AWS 账户。管理员比组织中的其他成员具有更高级别的 AWS 账户 权限。管理员为建立和实施设置 AWS 账户。他

们还会创建 IAM 用户或 IAM Identity Center 用户。管理员向这些用户提供用于登录 AWS的访问凭证和登录 URL。

Account

标准既 AWS 账户 包含您的 AWS 资源，也包含可以访问这些资源的身份。账户与账户所有者的电子邮件地址和密码关联。

凭证

也称作访问凭证或安全凭证。在身份验证和授权中，系统使用凭证来识别谁在执行调用并决定是否允许请求的访问。凭证是用户为 AWS 登录和获取 AWS 资源访问权限而提供的信息。人类用户的凭证包括电子邮件地址、用户名、用户定义的密码、账户 ID 或别名、验证码和一次性多重身份验证 (MFA) 代码。对于编程访问，您还可以使用访问密钥。我们建议尽可能使用短期访问密钥。

有关凭证的更多信息，请参阅AWS 安全凭证。

> **Note**
>
> 用户必须提交的凭证类型取决于其用户类型。

公司凭证

用户在访问公司网络和资源时提供的凭证。您的公司管理员可以将您设置 AWS 账户 为使用与您访问公司网络和资源相同的凭据。这些凭证由管理员或帮助中心员工提供给您。

配置文件

当您注册 AWS 建筑商 ID 时，您就创建了个人资料。您的配置文件包含您提供的联系信息，并让您能够管理多重身份验证 (MFA) 设备和活动会话。您还可以在配置文件中详细了解隐私条款以及我们如何处理您的数据。如需详细了解配置文件及其与 AWS 账户的关系，请参阅 AWS 构建者 ID 和其他 AWS 证书。

根用户凭证

根用户凭据是用于创建 AWS 账户的电子邮件地址和密码。为了提高安全性，我们强烈建议将 MFA 添加到根用户凭证。根用户凭证提供对账户中所有 AWS 服务和资源的完全访问权限。有关根用户的更多信息，请参阅 根用户。

User

用户是指有权对 AWS 产品进行 API 调用或访问 AWS 资源的个人或应用程序。每个用户均有一组唯一的无法与其他用户共享的安全凭证。这些凭证独立于 AWS 账户的安全凭证。有关更多信息，请参阅确定您的用户类型。

验证代码

在登录过程中，验证码使用多重身份验证 (MFA) 来验证您的身份。验证码的送达方式有多种类型。可以通过短信或电子邮件发送验证码。有关更多信息，请咨询您的管理员：

可供 AWS 登录的区域

AWS 登录有几种常用 AWS 区域版本。这种可用性使您可以更轻松地访问 AWS 服务和业务应用程序。有关登录支持的区域的完整列表，请参阅 AWS 登录端点和限额。

登录事件记录

CloudTrail 会在您的系统上自动启用 AWS 账户 ，并在活动发生时记录事件。以下资源可帮助您进一步了解登录事件的记录和监控。

- CloudTrail 记录登录的尝试 AWS Management Console。所有 IAM 用户、根用户和联合用户登录事件都会在 CloudTrail 日志文件中生成记录。有关更多信息，请参阅 AWS CloudTrail 用户指南中的 AWS Management Console 登录事件。
- 如果您使用区域终端节点登录 AWS Management Console，则会在终端节点的相应区域中 CloudTrail 记录`ConsoleLogin`事件。有关 AWS 登录端点的更多信息，请参阅《AWS 通用参考指南》中的AWS 登录端点和配额。
- 要详细了解如何 CloudTrail 记录 IAM Identity Center 的登录事件，请参阅 IAM 身份中心用户指南中的了解 IAM 身份中心登录事件。
- 要详细了解如何在 IAM 中 CloudTrail 记录不同的用户身份信息，请参阅AWS Identity and Access Management 用户指南 AWS CloudTrail中的使用记录 IAM 和 AWS STS API 调用。

确定您的用户类型

您的登录方式取决于您的 AWS 用户类型。您可以作为根用户、IAM 用户、IAM Identity Center 用户或联合身份管理 AWS 账户 。您可以使用 AWS Builder ID 配置文件来访问某些 AWS 服务和工具。下面列出了各种用户类型。

主题

根用户

也称为账户所有者或账户根用户。作为 root 用户，您可以完全访问您的中的所有 AWS 服务和资源 AWS 账户。首次创建时 AWS 账户，您首先需要一个单一登录身份，该身份可以完全访问账户中的所有 AWS 服务和资源。此身份是 AWS 账户 root 用户。您可以使用在创建账户所用的电子邮件地址和密码以根用户身份登录。根用户使用 AWS Management Console 登录：有关如何登录的分步说明，请参阅 以 root 用户身份登录 AWS Management Console。

> **Important**
>
> 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。

有关 IAM 身份（包括根用户）的更多信息，请参阅 IAM 身份（用户、用户组和角色）。

IAM 用户

IAM 用户是您在 AWS中创建的实体。此用户是 AWS 账户 中具有特定自定义权限的身份。IAM 用户凭证由用于登录 AWS Management Console 的用户名和密码组成。有关如何登录的分步说明，请参阅 以 IAM 用户 AWS Management Console 身份登录。

有关 IAM 身份（包括 IAM 用户）的更多信息，请参阅 IAM 身份（用户、用户组和角色）。

IAM Identity Center 用户

IAM Identity Center 用户是其成员，可以通过访问门户 AWS 获得对多个 AWS 账户 应用程序的访问权限。 AWS Organizations 如果公司已将 Active Directory 或其他身份提供者与 IAM Identity Center 集

成，则 IAM Identity Center 用户可以使用公司凭证登录。IAM Identity Center 也可以是身份提供者，管理员可以在其中创建用户。无论身份提供商是谁，IAM Identity Center 中的用户都使用 AWS 访问门户登录，访问门户是其组织的特定登录 URL。IAM Identity Center 用户不能通过 AWS Management Console URL 登录。

IAM Identity Center 中的人类用户可以通过以下任一方式获取 AWS 访问门户 URL：

- 来自管理员或帮助中心员工的消息
- 一封来自 AWS 的电子邮件，其中包含加入 IAM 身份中心的邀请

> **Tip**
>
> IAM Identity Center 服务从 no-reply@signin.aws 或 no-reply@login.awsapps.com 发出的所有电子邮件。我们建议您配置自己的电子邮件系统，以便接受来自这些发件人电子邮件地址的电子邮件，而不将其视为垃圾邮件。

有关如何登录的分步说明，请参阅 登录 AWS 访问门户。

> **Note**
>
> 我们建议您为组织 AWS 访问门户的特定登录 URL 添加书签，以便日后访问。

有关 IAM Identity Center 的更多信息，请参阅什么是 IAM Identity Center？

联合身份

联合身份是指可以使用知名的外部身份提供者 (IdP) 登录的用户，例如 Login with Amazon、Facebook、Google 或任何其他与 OpenID Connect (OIDC) 兼容的身份提供者。借助 Web 联合身份验证，您可以接收身份验证令牌，然后将该令牌交换为 AWS 该映射中的临时安全证书，转到有权使用您的资源的 IAM 角色 AWS 账户。 您不使用门户登录 AWS Management Console 或 AWS 访问门户。相反，使用的外部身份决定了您的登录方式。

有关更多信息，请参阅 以联合身份登录。

AWS 生成器 ID 用户

作为 AWS Builder ID 用户，您专门登录要访问的 AWS 服务或工具。 AWS Builder ID 用户可以补充 AWS 账户 您已经拥有或想要创建的任何内容。 AWS Builder ID 代表您的个人身份，您可以使用它来访问 AWS 服务和工具，而无需使用 AWS 账户。您还有配置文件，您可以在其中查看和更新自己的个人信息。有关更多信息，请参阅 使用登录 AWS 构建者 ID。

AWS Builder ID 与你的 S AWS kill Builder 订阅是分开的，后者是一个在线学习中心，你可以向 AWS 专家学习并在线培养云技能。有关 AWS 技能生成器的更多信息，请参阅AWS 技能生成器。

确定您的登录 URL

AWS 根据您的 AWS 用户类型 URLs ，使用以下任一方式进行访问。有关更多信息，请参阅 确定您的用户类型。

主题

- AWS 账户 root 用户登录网址
- AWS 访问门户
- IAM 用户登录 URL
- 联合身份 URL
- AWS 生成器 ID 网址

AWS 账户 root 用户登录网址

root 用户 AWS Management Console 从 AWS 登录页面访问:. https://console.aws.amazon.com/

此登录页面还提供以 IAM 用户身份登录的选项。

AWS 访问门户

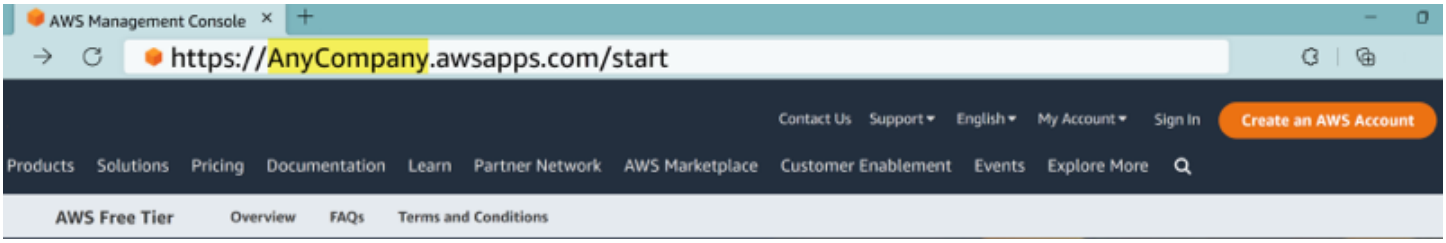
AWS 访问门户是 IAM Identity Center 中的用户登录和访问您的账户的特定登录网址。当管理员在 IAM Identity Center 中创建用户时，管理员可以选择该用户是收到加入 IAM Identity Center 的电子邮件邀请，还是收到来自管理员或帮助台员工的包含一次性密码和 AWS 访问门户 URL 的消息。特定登录 URL 的格式类似于以下示例：

```
https://d-xxxxxxxxxx.awsapps.com/start
```

或

```
https://your_subdomain.awsapps.com/start
```

特定登录 URL 不尽相同，因为管理员可以对其进行自定义。特定登录 URL 可能以字母 D 开头，后跟 10 个随机数字和字母。子域也可能用于登录 URL 中，并且可能包含公司名称，如以下示例所示：



> **Note**
>
> 我们建议您将 AWS 访问门户的特定登录 URL 添加为书签，以便日后可以访问。

有关 AWS 访问门户的更多信息，请参阅使用 AWS 访问门户。

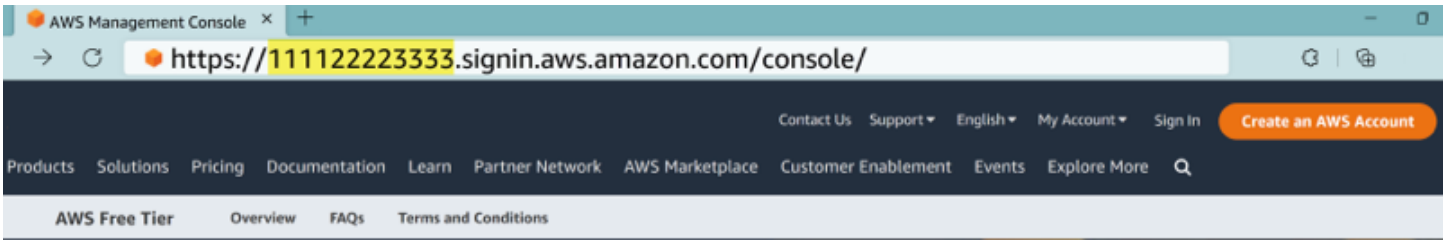
IAM 用户登录 URL

IAM 用户可以使用特定的 AWS Management Console IAM 用户登录 URL 访问。IAM 用户登录 URL 结合了您的 AWS 账户 ID 或别名和 `signin.aws.amazon.com/console`

以下示例说明 IAM 用户登录 URL 的格式：

```
https://account_alias_or_id.signin.aws.amazon.com/console/
```

如果您的账户 ID 是 111122223333，则您的登录 URL 将是：



如果您在 AWS 账户 使用 IAM 用户登录 URL 访问您的时遇到问题，请参阅中的弹性了解 AWS Identity and Access Management更多信息。

联合身份 URL

联合身份的登录 URL 不尽相同。外部身份或外部身份提供者 (IdP) 决定着联合身份的登录 URL。外部身份可能是 Windows Active Directory、Login with Amazon、Facebook 或 Google。有关如何以联合身份登录的更多详细信息，请联系您的管理员。

有关联合身份的更多信息，请参阅关于网络身份联合验证。

AWS 生成器 ID 网址

您的 AWS Builder ID 个人资料的网址是https://profile.aws.amazon.com/。使用您的 AWS 生成器 ID 时，登录 URL 取决于您要访问的服务。例如，要登录亚马逊 CodeCatalyst，请前往https://codecatalyst.aws/login。

要添加到允许列表的域

如果您使用网络内容过滤解决方案（例如下一代防火墙 (NGFW) 或安全 Web 网关 (SWG)）来过滤对特定 AWS 域或 URL 端点的访问，则必须将以下域或 URL 端点添加到您的网络内容过滤解决方案许可名单中。

AWS 将域名登录到许可名单

如果您或您的组织实施 IP 或域名过滤，则可能需要将域列入许可名单才能使用。 AWS Management Console在您尝试访问的网络上必须可以访问以下域 AWS Management Console。

- *[Region]*.signin.aws
- *[Region]*.signin.aws.amazon.com
- signin.aws.amazon.com
- *.cloudfront.net
- opfcaptcha-prod.s3.amazonaws.com

AWS 访问门户 要列入许可名单的域名

如果您使用网络内容过滤解决方案（例如下一代防火墙 (NGFW) 或安全 Web 网关 (SWG)）来过滤对特定 AWS 域或 URL 端点的访问，则必须将以下域或 URL 端点添加到您的网络内容过滤解决方案许可名单中。这样做可以使您访问自己的 AWS 访问门户.

- *[Directory ID or alias]*.awsapps.com

- *.aws.dev
- *.awsstatic.com
- *.console.aws.a2z.com
- oidc.*[Region]*.amazonaws.com
- *.sso.amazonaws.com
- *.sso.*[Region]*.amazonaws.com
- *.sso-portal.*[Region]*.amazonaws.com

AWS 构建者 ID 要列入许可名单的域名

如果您或您的组织实施 IP 或域名筛选，则您可能需要将域加入允许列表才能创建和使用 AWS 构建者 ID。在您尝试访问 AWS 构建者 ID的网络中必须可以访问以下域。

- view.awsapps.com/start
- *.aws.dev
- *.uis.awsstatic.com
- *.console.aws.a2z.com
- oidc.*.amazonaws.com
- *.sso.amazonaws.com
- *.sso.*.amazonaws.com
- *.sso-portal.*.amazonaws.com
- *.signin.aws
- *.cloudfront.net
- opfcaptcha-prod.s3.amazonaws.com
- profile.aws.amazon.com

AWS 账户 管理员的安全最佳实践

如果您是账户管理员并创建了新的账户 AWS 账户，我们建议您采取以下步骤来帮助您的用户在登录时遵循 AWS 安全最佳实践。

1. 以根用户身份登录以启用多重身份验证 (MFA)，并在 IAM Identity Center 中创建 AWS 管理用户（如果您尚未这样做）。然后，保护您的根用户凭证 ，请勿将其用于日常任务。

2. 以 AWS 账户 管理员身份登录并设置以下身份：

   - 为其他人员创建最低权限用户。
   - 为工作负载设置临时凭证。
   - 仅为需要长期凭证的使用案例创建访问密钥。

3. 添加权限以向这些身份授予访问权限。您可以开始使用 AWS 托管策略，然后转向最低权限权限。

   - 向 AWS IAM Identity Center（ AWS 单点登录的继任者）用户添加权限集。
   - 向用于工作负载的 IAM 角色添加基于身份的策略。
   - 对于需要长期凭证的使用案例，向 IAM 用户添加基于身份的策略。
   - 有关 IAM 用户的更多信息，请参阅 IAM 安全最佳实践。

4. 保存和共享有关 登录 AWS Management Console 的信息。这些信息不尽相同，具体取决于您创建的身份类型。

5. 请及时更新根用户电子邮件地址和主要账户联系人电话号码，以确保您可以收到与账户和安全相关的重要通知。

   - 修改 AWS 账户根用户的账户名称、电子邮件地址或密码。
   - 访问或更新主要账户联系人。

6. 回顾 IAM 安全最佳实践，了解其他身份和访问管理最佳实践。

登录 AWS Management Console

当您 AWS Management Console 从主登录 URL (https://console.aws.amazon.com/) AWS 登录时，必须选择您的用户类型，即根用户或 IAM 用户。如果您不确定自己是哪种类型的用户，请参阅 确定您的用户类型。

根用户具有不受限的账户访问权限，而且与创建 AWS 账户的人员关联。然后，根用户创建其他类型的用户，例如 IAM 用户和 AWS IAM Identity Center 中的用户，并为他们分配访问凭证。

I AM 用户是您内部 AWS 账户 具有特定自定义权限的身份。当 IAM 用户登录时，他们可以使用包含其 AWS 账户 或别名的登录 URL，例如 `https://account_alias_or_id.signin.aws.amazon.com/console/`而不是主 AWS 登录网址`https://console.aws.amazon.com/` 。

您可以在中的单个浏览器中同时登录最多 5 个不同的身份 AWS Management Console。这些角色可以是不同账户或同一个账户中的根用户、IAM 用户或联合角色的组合。有关详细信息，请参阅《AWS Management Console 入门指南》中的登录多个账户。

教程

- 以 root 用户身份登录 AWS Management Console
- 以 IAM 用户 AWS Management Console 身份登录

如果您不确定自己是哪种类型的用户，请参阅 确定您的用户类型。

教程

- 以 root 用户身份登录 AWS Management Console
- 以 IAM 用户 AWS Management Console 身份登录

以 root 用户身份登录 AWS Management Console

首次创建时 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。

> **Important**
>
> 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。

以根用户身份登录

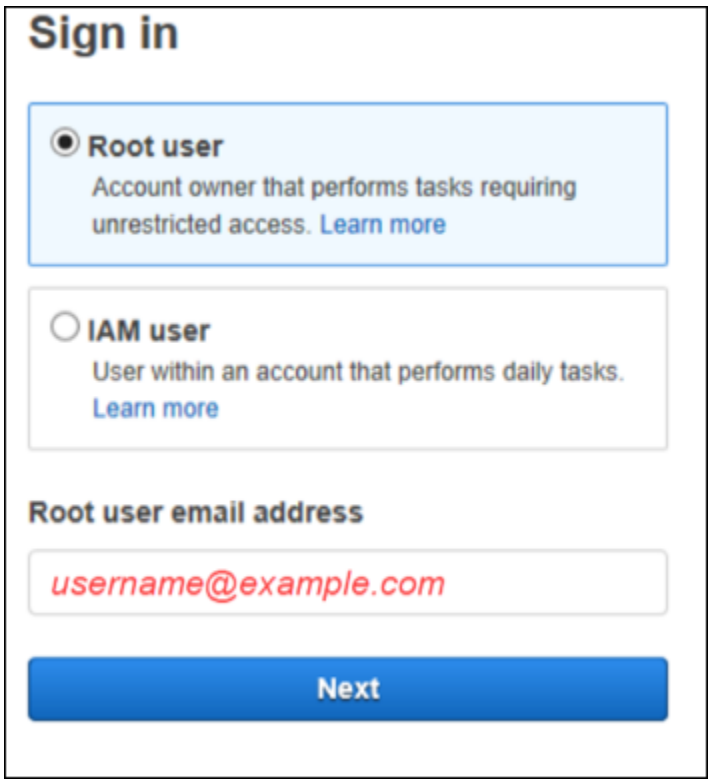
当你已经登录到另一个身份时，你可以以 root 用户身份登录 AWS Management Console。有关详细信息，请参阅《AWS Management Console 入门指南》中的登录多个账户。

AWS 账户 托管使用 AWS Organizations 可能没有 root 用户证书，您必须联系管理员才能在您的成员账户中执行 root 用户操作。如果您无法以 root 用户身份登录，请参阅AWS 账户 登录问题疑难解答。

1. 打开 a AWS Management Console t https://console.aws.amazon.com/。

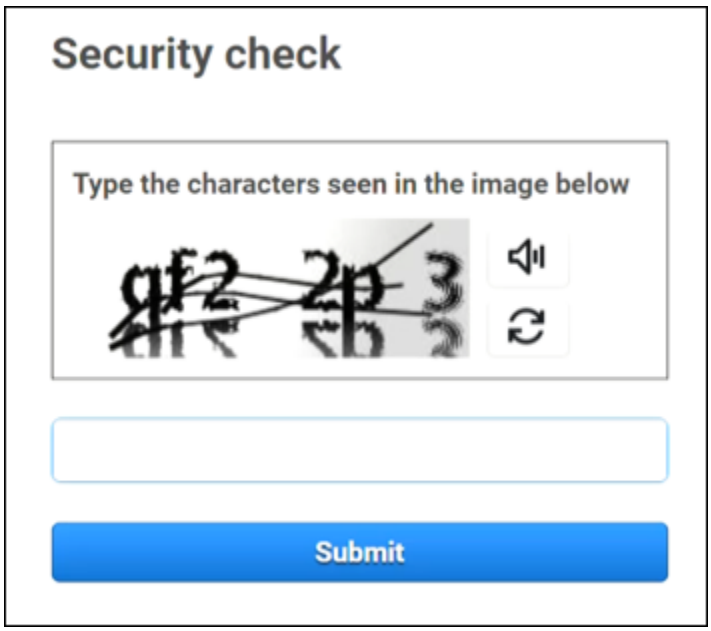
   > **Note**
   >
   > 如果您之前使用此浏览器以 IAM 用户身份登录过，则浏览器可能会显示 IAM 用户登录页面。选择使用根用户电子邮件登录。

2. 选择根用户。



3. 在根用户电子邮件地址下，输入与您的根用户关联的电子邮件地址。然后选择下一步。
4. 如果系统提示您需要完成安全检查，请输入您看到的字符以继续。如果您无法完成安全检查，请尝试收听音频或刷新安全检查页面，以获得一组新字符。

> **Tip**
>
> 按顺序输入您看到（或听到）的字母数字字符，不能包含空格。



5. 输入您的密码。

6. 使用 MFA 进行身份验证。默认情况下，对根用户强制执行 MFA。对于独立账户和成员账户的根用户，您必须手动启用 MFA，强烈建议这样做。有关更多信息，请参阅《用户指南》中的 AWS 账户 root 用户多重身份验证。AWS Identity and Access Management

> **Tip**
>
> 作为安全最佳实践，我们建议从 AWS 组织中的成员账户中移除所有 root 用户证书，以帮助防止未经授权的使用。如果您选择此选项，则成员账户无法以 root 用户身份登录、执行密码恢复或设置 MFA。在这种情况下，只有管理账户管理员才能执行需要成员账户中有 root 用户凭证的任务。有关详细信息，请参阅《AWS Identity and Access Management 用户指南》中的集中管理成员账户的根访问权限。

7. 选择登录。 AWS Management Console 出现了。

身份验证后，将 AWS Management Console 打开控制台主页。

其他信息

如果您想了解有关 AWS 账户 root 用户的更多信息，请参阅以下资源。

- 有关根用户的概述，请参阅 AWS 账户 根用户。
- 有关使用 root 用户的详细信息，请参阅使用 AWS 账户 root 用户。
- 有关如何重置 root 用户密码的 step-by-step说明，请参阅我忘记了 AWS 账户根用户密码。

以 IAM 用户 AWS Management Console 身份登录

I AM 用户是在中创建 AWS 账户 的、有权与 AWS 资源交互的身份。IAM 用户使用账户 ID 或别名、用户名和密码进行登录。IAM 用户名由您的管理员配置。IAM 用户名可以是友好名称（例如）*Zhang*，也可以是电子邮件地址（如）*zhang@example.com*。IAM 用户名不能包含空格，但可以包含大小写字母、数字和符号 + = , . @ _ -。

> **Tip**
>
> 如果 IAM 用户启用了多重身份验证 (MFA)，则您必须有权访问身份验证装置。有关更多信息，请参阅使用 MFA 设备访问 IAM 登录页面。

以 IAM 用户身份登录

在中已使用其他身份登录时，您可以以 IAM 用户身份登录 AWS Management Console。有关详细信息，请参阅《AWS Management Console 入门指南》中的登录多个账户。

1. 打开 a AWS Management Console t https://console.aws.amazon.com/。
2. 将显示主登录页面。输入账户 ID（12 位数字）或别名、您的 IAM 用户名和密码。

> **Note**
>
> 如果您之前已使用当前浏览器以 IAM 用户身份登录，或者使用账户登录 URL，则可能无需输入账户 ID 或别名。

3. 选择登录。
4. 如果您的 IAM 用户启用了 MFA，则 AWS 需要您使用身份验证器确认您的身份。有关更多信息，请参阅在 AWS中使用多重身份验证（MFA）。

身份验证后，将 AWS Management Console 打开控制台主页。

其他信息

如需了解有关 IAM 用户的更多信息，请参阅以下资源。

- 有关 IAM 的概述，请参阅什么是 Identity and Access Management？
- 有关 AWS 账户的详细信息 IDs，请参阅您的 AWS 账户 ID 及其别名。
- 有关如何重置您的 IAM 用户密码的 step-by-step说明，请参阅我忘记了 AWS 账户的 IAM 用户密码。

登录 AWS 访问门户

IAM 身份中心中的用户是的成员 AWS Organizations。IAM Identity Center 中的用户可以使用特定的登录 URL 登录 AWS 访问门户，从而访问多个 AWS 账户 业务应用程序。有关特定登录 URL 的更多信息，请参阅 AWS 访问门户。

在 IAM Ident AWS 账户 ity Center 中以用户身份登录之前，请收集以下必需信息。

- 企业用户名
- 企业密码
- 特定登录 URL

> **Note**
>
> 登录后，您的 AWS 访问门户会话有效期为 8 小时。您需要在 8 小时后重新登录。

登录到 AWS 访问门户

1. 在浏览器窗口中，粘贴通过电子邮件提供的登录 URL，例如 `https://your_subdomain.awsapps.com/start`。然后按 Enter。
2. 使用企业凭证（例如用户名和密码）登录。

   > **Note**
   >
   > 如果管理员向您发送了包含一次性密码 (OTP) 的电子邮件，而且这是您首次登录，请输入该密码。登录后，您必须创建新密码以备用于后续登录。

3. 如果系统要求您提供验证码，请在电子邮件中查看。然后将验证码复制并粘贴到登录页面中。

   > **Note**
   >
   > 验证码通常通过电子邮件发送，但送达方式可能有所不同。如果位收到含验证码的电子邮件，请向管理员咨询有关验证码的详细信息。

4. 如果对 IAM Identity Center 用户启用了 MFA，您可以使用其进行身份验证。

5. 身份验证后，您可以访问门户中显示的任何 AWS 账户 和应用程序。

   a. 要登录， AWS Management Console 请选择 “账户” 选项卡，然后选择要管理的个人账户。

      将显示用户的角色。选择账户的角色名称，以打开 AWS Management Console。选择 Access keys（访问密钥），以获取命令行或编程访问的凭证。

   b. 选择 Applications（应用程序）选项卡，以显示可用应用程序，然后您要访问的应用程序的图标。

以 IAM Identity Center 用户身份登录将会让您获得凭证，可在设定的时间段（称为“会话”）内访问资源。默认情况下，用户可以登录 AWS 账户 8 小时。IAM Identity Center 管理员可以指定不同的持续时间，从最少 15 分钟到最长 90 天不等。会话结束后，您可以重新登录。

其他信息

如需了解有关 IAM Identity Center 用户的更多信息，请参阅以下资源。

- 有关 IAM Identity Center 的概述，请参阅什么是 IAM Identity Center？
- 有关 AWS 访问门户的详细信息，请参阅使用 AWS 访问门户。
- 有关 IAM Identity Center 会话的详细信息，请参阅用户身份验证。
- 有关如何重置您的 IAM Identity Center 用户密码的 step-by-step说明，请参阅我忘记了我的 IAM 身份中心密码 AWS 账户。
- 如果您或您的组织实施 IP 或域名过滤，则可能需要将域名列入许可名单才能创建和使用您的 AWS 访问门户。有关将域名列入许可名单的详细信息，请参阅要添加到允许列表的域。

通过登录 AWS Command Line Interface

如果您计划使用 AWS Command Line Interface，我们建议您配置 IAM Identity Center 用户。 AWS 访问门户用户界面使 IAM Identity Center 用户可以轻松选择 AWS 账户 并使用 AWS CLI 来获取临时安全证书。有关如何获取这些凭证的更多信息，请参阅 的地区可用性 AWS 构建者 ID。您也可以 AWS CLI 直接配置为通过 IAM 身份中心对用户进行身份验证。

AWS CLI 使用 IAM 身份中心证书通过登录

- 检查您是否已满足先决条件。
- 如果您是首次登录，请使用 `aws configure sso` 向导配置您的配置文件。
- 配置配置文件后，运行以下命令，然后按照终端中的提示进行操作。

```
$ aws sso login --profile my-profile
```

其他信息

如需了解有关使用命令行登录的更多信息，请参阅以下资源。

- 有关使用 IAM 身份中心证书的详细信息，请参阅获取 AWS CLI 或的 IAM Identity Center 用户证书 AWS SDKs。
- 有关配置的详细信息，请参阅配置 AWS CLI 为使用 IAM 身份中心。
- 有关 AWS CLI 登录过程的更多详细信息，请参阅登录和获取凭证。

以联合身份登录

联合身份是指能够使用外部身份访问安全 AWS 账户 资源的用户。外部身份可能来自公司身份存储（如 LDAP 或 Windows Active Directory）或第三方（如 Login with Amazon、Facebook 或 Google）。联合身份无法使用门户登录 AWS Management Console 或 AWS 访问门户。使用的外部身份类型决定了联合身份的登录方式。

管理员必须创建包含 `https://signin.aws.amazon.com/federation` 的自定义 URL。有关更多信息，请参阅授权自定义身份凭证代理程序对 AWS Management Console的访问权限。

> **Note**
>
> 您的管理员创建联合身份。有关如何以联合身份登录的更多详细信息，请联系您的管理员。

有关联合身份的更多信息，请参阅关于网络身份联合验证。

使用登录 AWS 构建者 ID

AWS 构建者 ID 是一种个人档案，允许访问精选工具和服务，包括亚马逊 CodeCatalyst、A mazon Q 开发人员AWS 培训和认证。 AWS 构建者 ID 代表您的个人身份，独立于您在现有 AWS 账户中可能拥有的任何凭据和数据。与其他个人资料一样，在你实现个人、教育和职业目标的过程中，它会 AWS 构建者 ID 一直伴随着你。

任何 AWS 账户 你可能已经拥有或想要创作的 AWS 构建者 ID 补充。虽然 AWS 账户 充当你创建的 AWS 资源的容器并为这些资源提供安全边界，但你的 AWS 构建者 ID 代表你是一个个体。有关更多信息，请参阅 AWS 构建者 ID 和其他 AWS 证书。

AWS 构建者 ID 是免费的。您只需为自己消耗的 AWS 资源付费 AWS 账户。有关定价的更多信息，请参阅 AWS 定价。

如果您或您的组织实施 IP 或域名筛选，则您可能需要将域加入允许列表才能创建和使用 AWS 构建者 ID。有关将域名列入许可名单的详细信息，请参阅要添加到允许列表的域。

> **Note**
>
> AWS Builder ID 与您 AWS 的 Skill Builder 订阅是分开的，后者是一个在线学习中心，您可以在其中向 AWS 专家学习并在线培养云技能。有关 AWS 技能生成器的更多信息，请参阅AWS 技能生成器。

要使用登录 AWS 构建者 ID

1. 导航到您要访问的 AWS 工具或服务的AWS 构建者 ID 个人资料或登录页面。例如，要访问亚马逊 CodeCatalyst，请前往https://codecatalyst.aws并选择登录。
2. 在电子邮件地址中输入用于创建 AWS 构建者 ID的电子邮件地址，然后选择下一步。
3. （可选）如果您希望日后从此装置登录时不会被要求进行额外验证，请勾选这是受信任装置旁边的复选框。

> **Note**
>
> 出于安全考虑，我们会分析您的登录浏览器、位置和装置。如果您已告知我们信任此装置，则无需在每次登录时提供多重身份验证（MFA）代码。有关更多信息，请参阅 受信任装置。

4. 在输入密码页面上，输入密码，然后选择登录。
5. 在所需额外验证页面上，如果出现要求提供代码或安全密钥的请求，请按照浏览器的说明进行操作。

主题

的地区可用性 AWS 构建者 ID

AWS 构建者 ID 可在以下版本中找到 AWS 区域。使用的应用程序 AWS 构建者 ID 可能在其他地区运行。

名称	代码
美国东部（弗吉尼亚州北部）	us-east-1

创建你的 AWS 构建者 ID

AWS 构建者 ID 当你注册使用它的 AWS 工具和服务时，你就可以创建你的。注册 AWS 工具或服务的过程中，需提供您的电子邮件地址、姓名和密码。

密码必须符合以下要求：

- 密码区分大小写。

- 密码长度必须在 8 到 64 个字符之间。
- 密码必须包含下列四种类别中每种类别的至少一个字符：
  - 小写字母 (a-z)
  - 大写字母 (A-Z)
  - 数字 (0-9)
  - 非字母数字字符 (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)
- 不能与最近使用的三个密码重复。
- 不能使用通过第三方泄露的数据集公开的密码。

> **Note**
>
> 使用的工具和服务可 AWS 构建者 ID 指导您在需要 AWS 构建者 ID 时创建和使用您的。

要创建你的 AWS 构建者 ID

1. 导航到您要访问的 AWS 工具或服务的AWS 构建者 ID 个人资料或注册页面。例如，要访问亚马逊 CodeCatalyst，请前往https://codecatalyst.aws。
2. 在创建 AWS 构建者 ID 页面上，输入您的电子邮件地址。建议使用个人电子邮件。
3. 选择下一步。
4. 输入您的姓名, 然后选择下一步。
5. 在验证电子邮件页面上，输入我们向您的电子邮件地址发送的验证码。选择验证。您可能需要几分钟才能收到电子邮件，具体取决于电子邮件提供商。检查验证码是否被标记为垃圾邮件或被移入垃圾邮件文件夹中。如果您在五分钟 AWS 后仍未看到电子邮件，请选择 “重新发送验证码”。
6. 验证您的电子邮件后，请在 Choose a password page（选择密码页面）上输入 Password（密码）并 Confirm password（确认密码）。
7. 如果显示了 Captcha 验证码作为额外的安全验证，请输入您看到的字符。
8. 选择创建 AWS 构建者 ID。

受信任装置

从登录页面中选择 This is a trusted device（这是受信任装置）选项后，我们将认为在该装置上，此 Web 浏览器的所有将来登录均已获得授权。这意味着您不必在该受信任装置上提供 MFA 代码。但是，如果您的浏览器、Cookie 或 IP 地址发生变化，则可能需要使用 MFA 代码进行额外验证。

AWS 使用的工具和服务 AWS 构建者 ID

您可以使用登录 AWS 构建者 ID 以访问以下 AWS 工具和服务。要获得收费提供的功能或权益，则需要 AWS 账户.

默认情况下，当您使用您的工具或服务登录 AWS 工具或服务时，会话持续时间为 30 天 AWS 构建者 ID，Amazon Q Developer 除外，其会话持续时间为 90 天。会话结束后，您需要重新登录。

AWS 云社区

Community.aw s 是一个由 AWS 构建者社区开发的平台，您可以通过自己的平台进行访问。 AWS 构建者 ID在这里，您可以探索教育内容，分享个人想法和项目，评论他人的帖子，并关注您最喜爱的构建者。

Amazon CodeCatalyst

您将在开始使用 Amazon AWS 构建者 ID 时创建， CodeCatalyst并选择与议题、代码提交和拉取请求等活动关联的别名。邀请其他人加入您的 Amazon CodeCatalyst 空间，这里有您的团队构建下一个成功项目所需的工具、基础设施和环境。你需要一个 AWS 账户 才能将新项目部署到云端。

AWS Migration Hub

通过您的 AWS 构建者 ID访问 AWS Migration Hub (Migration Hub)。Migration Hub 提供了一个统一的平台来了解您的现有服务器、计划迁移，并跟踪每个应用程序的迁移状态。

Amazon Q 开发者版

Amazon Q Developer 是一款基于人工智能的生成式对话助手，可以帮助您理解、构建、扩展和操作 AWS 应用程序。有关更多信息，请参阅《Amazon Q Developer User Guide》中的 What is Amazon Q Developer?。

AWS re:Post

AWS re:Post为您提供专家技术指导，使您可以使用 AWS 服务更快地进行创新并提高运营效率。您无需使用 AWS 账户 或信用卡即可在 re: Post 上登录 AWS 构建者 ID 并加入社区。

AWS 初创企业

使用你的 AWS 构建者 ID 加入AWS 初创公司，在那里你可以使用学习内容、工具、资源和支持来发展你的初创公司 AWS。

AWS 培训 和认证

您可以使用访问AWS 培训 和认证 AWS 构建者 ID，在那里您可以通过 Skill Builder AWS Cloud 培养自己的AWS 技能，向 AWS 专家学习，并使用行业认可的证书验证您的云专业知识。

网站注册门户 (WRP)

您可以使用自己 AWS 构建者 ID 作为AWS 营销网站的永久客户身份和注册资料。如需注册参加新的网络研讨会，或者查看您已注册或参加的所有网络研讨会，请参阅我的网络研讨会。

编辑您的 AWS 构建者 ID 个人资料

您可随时更改配置文件信息。您可以编辑用于创建的电子邮件地址和姓名 AWS 构建者 ID，以及您的昵称。

您的 Name（姓名）是指在工具和服务中与其他用户互动时，其他用户对您的称呼。您的 Nickname（昵称）表明您希望如何让 AWS、朋友和其他密切合作伙伴了解您。

> **Note**
>
> 使用的工具和服务可 AWS 构建者 ID 指导您在需要 AWS 构建者 ID 时创建和使用您的。

编辑配置文件信息

1. 登录您的 AWS 构建者 ID 个人资料，网址为https://profile.aws.amazon.com。
2. 选择 My details（我的详细信息）。
3. 在 My details（我的详细信息）页面上，选择 Profile（配置文件）旁边的 Edit（编辑）按钮。
4. 在 Edit profile（编辑配置文件）页面上，根据需要对您的 Name（姓名）和 Nickname（昵称）进行更改。
5. 选择保存更改。页面顶部会显示一条绿色的确认消息，提示您已更新了配置文件。

若要编辑您的联系信息

1. 登录您的 AWS 构建者 ID 个人资料，网址为https://profile.aws.amazon.com。
2. 选择 My details（我的详细信息）。
3. 在 My details（我的详细信息）页面上，选择 Contact information（联系信息）旁边的 Edit（编辑）按钮。
4. 在 Edit contact information（编辑联系信息）页面上，更改您的 Email address（电子邮件地址）。
5. 选择验证电子邮件。随即显示对话框。

6. 在验证电子邮件对话框中，收到验证码电子邮箱后，在验证码中输入验证码。选择验证。

更改您的 AWS 构建者 ID 密码

密码必须符合以下要求：

- 密码区分大小写。
- 密码长度必须在 8 到 64 个字符之间。
- 密码必须包含下列四种类别中每种类别的至少一个字符：
  - 小写字母 (a-z)
  - 大写字母 (A-Z)
  - 数字 (0-9)
  - 非字母数字字符 (~!@#$%^&*_-+=`|\(){}[]:;'"<>,.?/)
- 不能与最近使用的三个密码重复。

> **Note**
>
> 使用的工具和服务可 AWS 构建者 ID 指导您在需要 AWS 构建者 ID 时创建和使用您的。

要更改您的 AWS 构建者 ID 密码

1. 登录您的 AWS 构建者 ID 个人资料，网址为https://profile.aws.amazon.com。
2. 选择安全性。
3. 在 Security（安全性）页面上，选择 Change password（更改密码）。这会将您带到新页面。
4. 在重新输入密码页面的密码下，输入您的当前密码。然后选择登录。
5. 在更改密码页面的新密码下，输入要使用的新密码。然后在确认密码下，重新输入要使用的新密码。
6. 选择更改密码。您将重定向到您的 AWS 构建者 ID 配置文件。

删除 AWS 构建者 ID的所有活动会话

在已登录装置下，您可以查看您当前登录的所有装置。如果您无法识别装置，作为安全最佳实践，请先更改密码，然后在各处注销。在 AWS 构建者 ID的 安全性页面上，您可以通过删除所有活动会话注销所有装置。

> **Note**
>
> AWS 构建者 ID 支持在 IDE 中为 Amazon Q 开发者提供为期 90 天的延长会话。对于每个新的 IDE 登录，您可以看到两个会话条目。当您退出 IDE 时，您可能会继续看到 Signed in devices（已登录设备）下列出的 IDE 会话，即使它们已不再有效。90 天到期后，这些会话就会消失。

删除所有活动会话

1. 登录您的 AWS 构建者 ID 个人资料，网址为https://profile.aws.amazon.com。
2. 选择安全性。
3. 在 Security（安全性）页面上，选择 Delete all active sessions（删除所有活动会话）。
4. 在删除所有会话对话框中，输入全部删除。删除所有会话即表示您注销所有可能已使用您的设备登录的设备 AWS 构建者 ID，包括不同的浏览器。然后选择删除所有会话。

删除你的 AWS 构建者 ID

> **Warning**
>
> 删除后 AWS 构建者 ID，您将无法再访问以前访问过的任何 AWS 工具和服务 AWS 构建者 ID。您的与 AWS 账户 您可能拥有的任何内容 AWS 构建者 ID 是分开的，删除您的内容并 AWS 构建者 ID 不会关闭您的 AWS 账户。

要删除你的 AWS 构建者 ID

1. 登录您的 AWS 构建者 ID 个人资料，网址为https://profile.aws.amazon.com。
2. 选择我的 AWS 构建者 ID 数据。
3. 在 “我的 AWS 构建者 ID 数据” 页面的 “删除” 下 AWS 构建者 ID，选择 “删除” AWS 构建者 ID。

4. 选中每份免责声明旁边的复选框，以确认您已准备好继续。

> **Important**
>
> 删除您的内容后 AWS 构建者 ID，仅与您的内容关联的所有剩余内容都 AWS 构建者 ID 将被删除，并且您将无法再使用您的应用程序访问或恢复您的内容 AWS 构建者 ID。您提供的与创建和管理您的个人信息相关的任何个人信息也 AWS 构建者 ID 将被删除，但 AWS 可能根据法律要求或允许保留个人信息的除外，例如您的删除请求记录或以无法识别您身份的形式提供的数据。
>
> 您可以在AWS 隐私声明中详细了解我们如何处理您的信息。
>
> 请记住，您可以通过访问 AWS 通信偏好中心来更新您的AWS 通信偏好或取消订阅。

5. 选择删除 AWS 构建者 ID。

管理 AWS 构建者 ID 多因素身份验证 (MFA)

多重身份验证 (MFA) 是一种用于增强安全性的简单而有效的机制。第一个因素（密码）是您记住的秘密，也称为知识因素。其他因素可以是拥有因素（您拥有的东西，例如安全密钥）或固有因素（您与生俱来的东西，例如生物识别扫描）。我们强烈建议您配置 MFA，以便为 AWS 构建者 ID增加额外一层保护。

> **Important**
>
> 建议注册多个 MFA 设备。如果您失去了对所有已注册 MFA 设备的访问权限，您将无法恢复您的 AWS 构建者 ID。

您可以注册内置身份验证器，也可以注册保存在物理安全位置的安全密钥。如果您无法使用内置身份验证器，则可以使用已注册的安全密钥。对于身份验证器应用程序，您也在这些应用中启用云备份功能或同步功能。这可有助于避免在 MFA 设备丢失或损坏的情况下，失去对配置文件的访问权限。

> **Note**
>
> 我们建议您定期检查已注册的 MFA 设备，确保它们处于最新状态且能正常运行。此外，不使用时，应将这些装置存放在物理安全位置。

可用的 MFA 类型适用于 AWS 构建者 ID

AWS 构建者 ID 支持以下多因素身份验证 (MFA) 设备类型。

FIDO2 身份验证器

FIDO2是一个包括 CTAP2 WebAuthn和基于公钥加密的标准。FIDO 凭证具有防网络钓鱼功能，因为它们是创建凭证的网站所独有的，例如 AWS。

AWS 支持 FIDO 身份验证器的两种最常见外形规格：内置身份验证器和安全密钥。有关最常见的 FIDO 身份验证器类型的更多信息，请参阅下文。

主题

- 内置身份验证器
- 安全密钥
- 密码管理器、密钥提供程序和其他 FIDO 身份验证器

内置身份验证器

某些设备内置了身份验证器，例如开启的 TouchID MacBook 或兼容 Windows Hello 的摄像头。如果您的设备兼容 FIDO 协议（包括）WebAuthn，则可以使用指纹或面部作为第二要素。有关更多信息，请参见 FIDO 身份验证。

安全密钥

您可以购买 FIDO2兼容的外部 USB、BLE 或 NFC 连接的安全密钥。当系统提示你输入 MFA 设备时，点击按键的传感器。 YubiKey 或者飞天制造兼容的设备。有关所有兼容安全密钥的列表，请参阅 FIDO 认证产品。

密码管理器、密钥提供程序和其他 FIDO 身份验证器

多个第三方提供商支持移动应用程序中的 FIDO 身份验证，例如密码管理器中的功能、带有 FIDO 模式的智能卡以及其他外形规格。这些兼容 FIDO 的设备可以与 IAM Identity Center 配合使用，但我们建议您在为 MFA 启用此选项之前亲自测试 FIDO 身份验证器。

> **Note**
>
> 有些 FIDO 身份验证器可以创建可发现的 FIDO 凭证，称为密钥。密钥可以绑定到创建密钥的设备，也可以同步并备份到云端。例如，您可以在支持的 Macbook 上使用 Apple Touch

ID 注册密钥，然后按照登录时屏幕上的提示使用 Google Chrome，在 iCloud 中使用密钥从 Windows 笔记本电脑登录网站。有关哪些装置支持可同步密钥以及当前密钥在操作系统和浏览器之间的互操作性的更多信息，请参阅 passkeys.dev 上的装置支持（此资源由 FIDO 联盟和万维网联盟 (W3C) 维护）。

身份验证器应用程序

身份验证器应用程序是基于一次性密码（OTP）的第三方身份验证器。您可将安装在移动装置或平板电脑上的身份验证器应用程序用作授权的 MFA 设备。第三方身份验证器应用程序必须符合 RFC 6238，这是一种标准的基于时间的一次性密码（TOTP）算法，且能够生成六位数身份验证码。

提示进行多重身份验证时，务必在显示的输入框中输入来自身份验证器应用程序的有效代码。分配给用户的每台 MFA 设备必须是唯一的。可为任意给定用户注册两个身份验证器应用程序。

您可从以下常见的第三方身份验证器应用程序中进行选择。但是，任何符合 TOTP 的应用程序都可使用 MFA AWS 构建者 ID 。

操作系统	经过测试的身份验证器应用程序
Android	1Password、Authy、Duo Mobile、Microsoft 身份验证器、Google 身份验证器
iOS	1Password、Authy、Duo Mobile、Microsoft 身份验证器、Google 身份验证器

注册您的 AWS 构建者 ID MFA 设备

> **Note**
>
> 注册 MFA 后，退出登录，然后在同一装置上重新登录，系统可能不会提示您在受信任的装置上进行 MFA。

使用身份验证器应用程序注册 MFA 设备

1. 登录您的 AWS 构建者 ID 个人资料，网址为https://profile.aws.amazon.com。

2. 选择安全性。
3. 在 Security（安全性）页面上，选择 Register device（注册装置）。
4. 在 Register MFA device（注册 MFA 设备）页面上，选择 Authenticator app（身份验证器应用程序）。
5. AWS 构建者 ID 操作并显示配置信息，包括二维码图形。此图形是秘密配置密钥的表示形式，适用于不支持 QR 代码的身份验证器应用程序上的手动输入。
6. 打开身份验证器应用程序。如需了解应用程序列表，请参阅 身份验证器应用程序。

   如果身份验证器应用程序支持多个 MFA 设备或账户，请选择相应的选项以创建新的 MFA 设备或账户。
7. 确定 MFA 应用程序是否支持 QR 代码，然后在 Set up your authenticator app（设置身份验证器应用程序）页面上执行以下操作之一：

   1. 选择 Show QR code（显示 QR 代码），然后使用该应用程序扫描 QR 代码。例如，您可选择摄像头图标或选择类似于 Scan code（扫描代码）的选项，然后使用装置的摄像头扫描此代码。
   2. 选择 Show secret key（显示密钥），然后将该密钥输入到 MFA 应用程序中。

   完成输入后，您的身份验证器应用程序将生成并显示一次性密码。
8. 在 Authenticator code（身份验证器代码）框中，输入当前显示在身份验证器应用程序中的一次性密码。选择分配 MFA。

   > **Important**
   >
   > 生成代码之后立即提交您的请求。如果生成代码后等待很长时间才提交请求，MFA 设备会成功与 AWS 构建者 ID关联，但 MFA 设备无法同步。这是因为基于时间的一次性密码（TOTP）很快会过期。这种情况下，您可以重新同步装置。有关更多信息，请参阅 尝试使用身份验证器应用程序注册或登录时，收到“An unexpected error has occurred”（出现意外错误）消息。
9. 要在中为您的设备起一个友好的名称 AWS 构建者 ID，请选择 “重命名”。此名称可帮助您区分此装置和您注册的其他装置。

MFA 设备现已准备就绪，可以与一起使用。 AWS 构建者 ID

将安全密钥注册为 AWS 构建者 ID MFA 设备

使用安全密钥注册 MFA 设备

1. 登录您的 AWS 构建者 ID 个人资料，网址为https://profile.aws.amazon.com。
2. 选择安全性。
3. 在 Security（安全性）页面上，选择 Register device（注册装置）。
4. 在 Register MFA device（注册 MFA 设备）页面上，选择 Security key（安全密钥）。
5. 确保已启用安全密钥。如果您使用单独的物理安全密钥，请将其连接到您的计算机。
6. 按照屏幕上的说明进行操作。您的体验取决于您的操作系统和浏览器。
7. 要在中为您的设备起一个友好的名称 AWS 构建者 ID，请选择 “重命名”。此名称可帮助您区分此装置和您注册的其他装置。

MFA 设备现已准备就绪，可以与一起使用。 AWS 构建者 ID

重命名您的 AWS 构建者 ID MFA 设备

重命名 MFA 设备

1. 登录您的 AWS 构建者 ID 个人资料，网址为https://profile.aws.amazon.com。
2. 选择安全性。位于此页面后，可看到 Rename（重命名）显示为灰色。
3. 选择要更改的 MFA 设备。这将允许您选择 Rename（重命名）。随即显示对话框。
4. 在打开的提示中，在 MFA device name（MFA 设备名称）中输入新名称，然后选择 Rename（重命名）。重命名装置将显示在 Multi-factor authentication (MFA) devices（多重身份验证（MFA）设备）下。

删除 MFA 设备

建议保留两个或多个活动 MFA 设备。移除装置之前，请参阅 注册您的 AWS 构建者 ID MFA 设备 以注册替代 MFA 设备。要禁用您的多重身份验证 AWS 构建者 ID，请从您的个人资料中删除所有已注册的 MFA 设备。

删除 MFA 设备

1. 登录您的 AWS 构建者 ID 个人资料，网址为https://profile.aws.amazon.com。
2. 选择安全性。

3. 选择要更改的 MFA 设备，然后选择 Delete（删除）。
4. 在 Delete MFA device?（要删除 MFA 设备吗？）模式窗口中，按照说明删除装置。
5. 选择删除。

已删除装置将不再显示在 Multi-factor authentication (MFA) devices（多重身份验证（MFA）设备）下。

隐私和数据 AWS 构建者 ID

本AWS 隐私声明概述了我们将如何处理您的个人数据。有关如何删除个人 AWS 构建者 ID 资料的信息，请参阅删除你的 AWS 构建者 ID。

索取您的 AWS 构建者 ID 数据

您可以请求和查看与您的个人信息 AWS 构建者 ID 以及您访问的 AWS 应用程序和服务相关的个人信息 AWS 构建者 ID。有关行使您的数据主体权利的更多信息，包括提供的与其他 AWS 网站、应用程序、产品、服务、活动和体验相关的个人信息，请参阅https://aws.amazon.com/privacy。

请求您的数据

1. 登录您的 AWS 构建者 ID 个人资料，网址为https://profile.aws.amazon.com。
2. 选择 “我的 AWS 构建者 ID 数据”。
3. 在 “我的 AWS 构建者 ID 数据” 页面的 “删除” 下 AWS 构建者 ID，选择 “请求您的数据”。
4. 页面顶部会显示一条绿色的确认消息，表示我们已收到您的请求并将在 30 天内完成审核。
5. 当您收到我们发送的请求已处理的电子邮件时，请返回您的 AWS 构建者 ID 个人资料的 “隐私和数据” 页面。选择最新可用的按钮 Download ZIP archive with your data（下载包含您数据的 ZIP 存档）。

   当您的数据请求待处理时，您将无法删除您的 AWS 构建者 ID。

AWS 构建者 ID 和其他 AWS 证书

您的凭 AWS 构建者 ID 据与任何 AWS 账户 或登录凭据是分开的。您可以对自己的电子邮件 AWS 构建者 ID 和的根用户电子邮件使用相同的电子邮件 AWS 账户。

一个 AWS 构建者 ID：

- 允许您访问使用的工具和服务 AWS 构建者 ID。
- 不会影响现有的安全控制措施，例如您在 AWS 账户 或应用程序上指定的策略和配置。
- 不会替换任何现有的根目录、IAM Identity Center 或 IAM 用户、凭证或账户。
- 无法获取 AWS IAM 凭证来访问 AWS Management Console AWS CLI、 AWS SDKs、或 AWS 工具包。

AWS 账户 是包含联系人和付款信息的资源容器。它为运营计费和计量 AWS 服务（例如 S3 或 Lambda）建立了安全边界。 EC2账户所有者可以登录 AWS Management Console。 AWS 账户 如需了解更多信息，请参阅登录到 AWS Management Console。

AWS 构建者 ID 与您现有的 IAM 身份中心身份有何关系

您作为身份所有者，可管理 AWS 构建者 ID。它与您在其他组织（例如学校或工作）中拥有的任何其他身份无关。你可以在 IAM Identity Center 中使用员工身份来代表你的工作自我，用一个 AWS 构建者 ID 来代表你的私人自我。这些身份独立运作。

AWS IAM Identity Center（ AWS 单点登录的继任者）中的用户由企业 IT 或云管理员或组织身份提供商（例如 Okta、Ping 或 Azure）的管理员管理。IAM Identity Center 中的用户可在 AWS Organizations中访问跨多个账户的资源。

多个 AWS 构建者 ID 配置文件

AWS 构建者 ID 只要每个 ID 使用唯一的电子邮件地址，您就可以创建多个 ID。但是，使用多个 AWS 构建者 ID 会让人难以回忆起 AWS 构建者 ID 你使用了哪个用途。如果可能，我们建议您在 AWS 工具和服务中的所有活动中使用单个 AWS 构建者 ID 。

退出 AWS

您注销 AWS 账户 的方式取决于您的 AWS 用户类型。您可以是账户根用户、IAM 用户、IAM Identity Center 中的用户、联合身份或 AWS Builder ID 用户。如果您不确定自己是哪种类型的用户，请参阅确定您的用户类型。

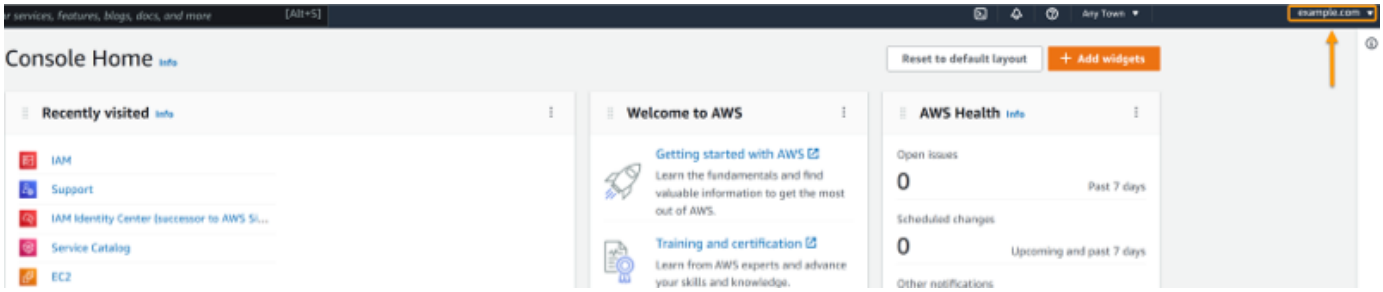
主题

- 退出 AWS Management Console
- 注销 AWS 访问门户
- 注销 AWS 生成器 ID

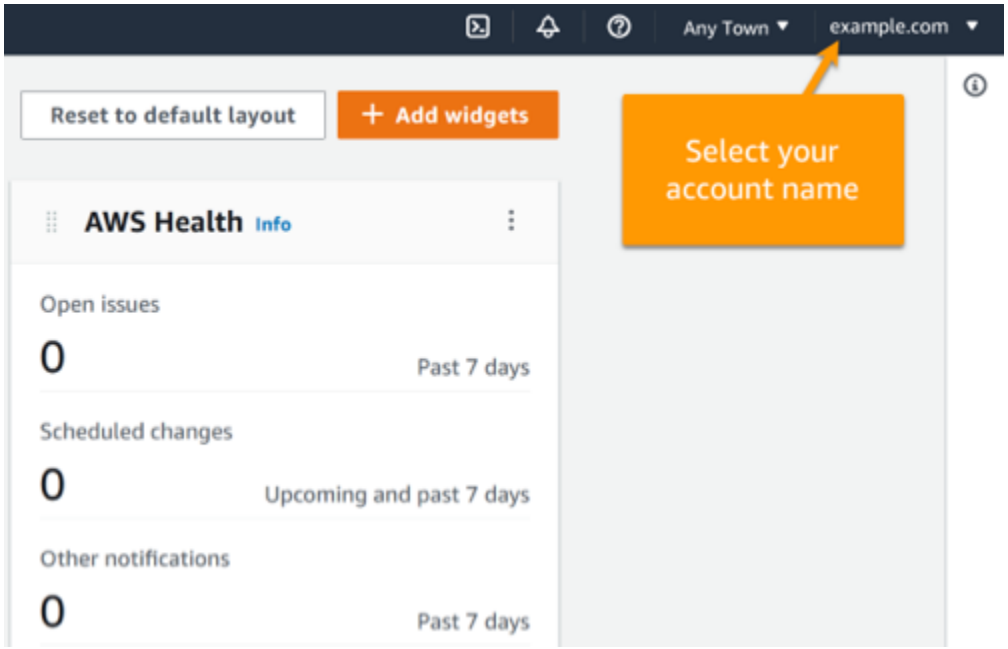
退出 AWS Management Console

要退出 AWS Management Console

1. 登录后 AWS Management Console，您会看到一个与下图所示页面相似的页面。您的账户名称或 IAM 用户名显示在右上角。



2. 在右上角的导航栏中，请选择您的用户名。



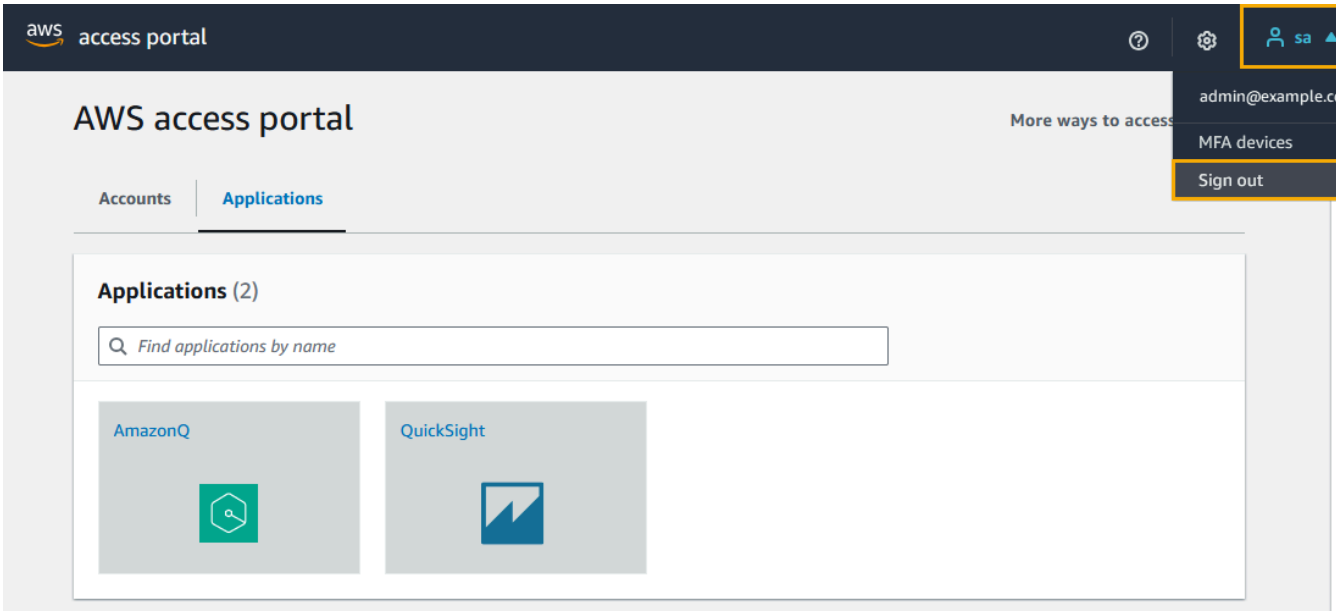
3. 选择 “注销” 选项。根据您登录的账户数量，按钮选项会有所不同。
   - 如果您只登录了一个帐户，请选择 “注销”。
   - 选择 “退出所有会话”，即可同时注销您的所有身份。
   - 选择 “退出当前会话”，注销您选择的身份。
4. 您将返回 AWS Management Console 网页。

有关登录多个账户的更多信息，请参阅《AWS Management Console 入门指南》中的登录多个账户。

注销 AWS 访问门户

要退出 AWS 访问门户

1. 在右上角的导航栏中，请选择您的用户名。
2. 选择注销，如下图所示。



3. 如果您成功注销，您现在会看到 AWS 访问门户登录页面。

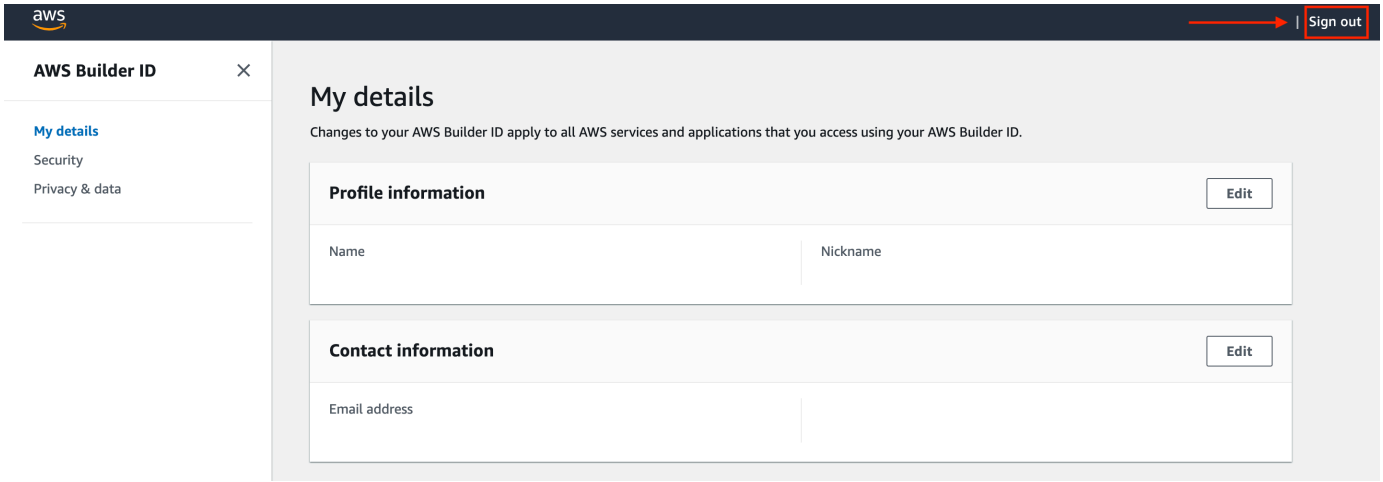
如果您使用外部身份提供商 (IdP) 作为身份源，则在您注销时，您的凭证的活动会话不会终止。如果您导航回 AWS 访问门户，则无需提供凭据即可自动登录。

注销 AWS 生成器 ID

要退出使用 AWS 构建器 ID 访问的 AWS 服务，必须注销该服务。如果您想退出 AWS 建筑商 ID 个人资料，请参阅以下步骤。

注销您的 AWS 建筑商 ID 个人资料

1. 登录 AWS Builder ID 个人资料后https://profile.aws.amazon.com/，您将进入 “我的详细信息”。
2. 在 AWS Builder ID 个人资料页面的右上角，选择注销。



3. 当你不再看到你的 AWS Builder ID 个人资料时，你就被注销了。

AWS 账户 登录问题疑难解答

使用此处的信息来帮助您解决登录 AWS 账户 问题和其他问题。有关登录的 step-by-step说明 AWS 账户，请参阅登录 AWS Management Console。

如果所有疑难解答主题都无法帮助您解决登录问题，则 支持 可以通过填写以下表格来创建案例：我是 AWS 客户，正在寻求账单或账户支持。作为安全最佳实践，除了您登录的账户之外， 支持 不能讨论任何 AWS 账户 其他账户的详细信息。AWS Support 也不能出于任何原因更改与账户关联的凭证。

> **Note**
>
> 支持 不公布用于联系支持代表的直接电话号码。

有关解决登录问题的更多帮助，请参阅如果我在登录或访问我的 AWS 账户登录时遇到问题该怎么办？如果您在登录 Amazon.com 时遇到问题，请参阅 Amazon 客户服务（而非本页）。

主题

- 我的 AWS Management Console 凭证不起作用
- 我的根用户需要重置密码
- 我无权访问我 AWS 账户的电子邮件
- 我的 MFA 设备遗失或停止工作
- 我无法访问 AWS Management Console 登录页面
- 如何查找我的 AWS 账户 ID 或别名
- 我需要账户验证码
- 我忘记了 AWS 账户根用户密码
- 我忘记了 AWS 账户的 IAM 用户密码
- 我忘记了我的联邦身份密码 AWS 账户
- 我无法登录现有的 AWS 账户 ，也无法 AWS 账户 使用相同的电子邮件地址创建新的
- 我需要重新激活已暂停的 AWS 账户
- 我需要联系 支持 以解决登录问题
- 我需要联系 AWS Billing 以解决账单问题

- 我对零售订单有疑问
- 我需要帮助来管理我的 AWS 账户
- 我的 AWS 访问门户凭证不起作用
- 我忘记了我的 IAM 身份中心密码 AWS 账户
- 当我尝试登录 IAM Identity Center 控制台时，我收到一条错误消息，上面写着“It’s not you, it’s us”（不是您，是我们）

我的 AWS Management Console 凭证不起作用

如果您记得用户名和密码，但凭证不起作用，则可能是您访问了错误的页面。尝试通过其他页面登录：

根用户登录页面

- 如果您创建或拥有 AWS 账户 并正在执行需要根用户凭证的任务，请在中输入您的账户电子邮件地址AWS Management Console。如需了解如何访问根用户，请参阅 以根用户身份登录。如果您忘记了根用户密码，则无法重置密码。请参阅我忘记了 AWS 账户根用户密码了解更多信息。如果您忘记了根用户的电子邮件地址，请检查电子邮件收件箱中是否有来自 AWS的电子邮件。
- 如果您尝试登录根用户帐户并收到错误消息：我的根用户帐户已禁用密码恢复，则您没有根用户凭据。您无法以 root 用户身份登录，也无法为账户的 root 用户执行密码恢复。 AWS 使用管理的成员账户 AWS Organizations 可能没有根用户密码、访问密钥、签名证书或有效的多因素身份验证 (MFA)。

  只有 IAM 的管理账户或委托管理员才能在您的成员账户中执行根用户操作。如果您需要执行需要根用户凭证的任务，则请联系您的管理员。有关更多信息，请参阅《AWS Identity and Access Management 用户指南》中的集中管理成员账户的根访问权限。

IAM 用户登录页面

- 如果您或其他人在中创建了 IAM 用户 AWS 账户，则必须知道该 AWS 账户 ID 或别名才能登录。在 AWS Management Console 中输入您的账户 ID 或别名、用户名和密码。如需了解如何访问 IAM 用户登录页面，请参阅 以 IAM 用户身份登录。如果您忘记了 IAM 用户密码，请参阅 我忘记了 AWS 账户的 IAM 用户密码，了解有关重置 IAM 用户密码的信息。如果您忘记了账户编号，请搜索您的电子邮件、浏览器收藏夹或浏览器历史记录，查找包含 `signin.aws.amazon.com/` 的 URL。您的账户 ID 或别名将位于 URL 中的 `"account="` 文本之后。如果您找不到您的账户 ID 或别名，请联系您的管理员。 支持 无法帮助您恢复这些信息。您只有在登录后才能看到您的账户 ID 或别名。

我的根用户需要重置密码

为保护您的账户安全，当您尝试登录 AWS Management Console时，可能会收到以下消息：

需要重置密码。出于安全考虑，您需要重置密码。为了保护您的账户安全，您必须选择下方的 Forgot password（忘记密码），然后重置您的密码。

除此消息外，当我们发现潜在问题时， AWS 还会通过与您的账户关联的电子邮件通知您。此电子邮件包含需要重置密码的原因。例如，当我们发现您的异常登录活动 AWS 账户 或与您 AWS 账户 相关的凭证会在网上公开时。

更新您的密码以确保您根用户凭证的安全。要了解如何重置您的根用户密码，请参阅我忘记了 AWS 账户的根用户密码。

我无权访问我 AWS 账户的电子邮件

创建时 AWS 账户，您需要提供电子邮件地址和密码。这些是 AWS 账户根用户的凭证。如果您不确定与您的电子邮件地址相关联的电子邮件地址 AWS 账户，请查找以 @signin .aws 或 @verify .signin.aws 结尾的已保存信件，发往贵组织中任何可能被用来打开. 的电子邮件地址。 AWS 账户询问团队、组织或家庭的其他成员。如果您认识的人创建了账户，他们可以帮助您获取访问权限。

如果您知道电子邮件地址，但无法再访问电子邮件，请首先尝试使用以下选项之一恢复对电子邮件的访问权限：

- 如果您拥有该电子邮件地址的域，则可以恢复已删除的电子邮件地址。或者，您可以为电子邮件账户设置“全部捕获”，该功能将捕获发送到邮件服务器中不再存在的电子邮件地址的所有邮件，并将其重定向到另一个电子邮件地址。
- 如果账户上的电子邮件地址属于您的公司电子邮件系统，我们建议您联系 IT 系统管理员。它们也许能够帮助您重新获得电子邮件的访问权限。

如果您仍然无法登录自己的 AWS 账户，则可以通过联系来查找其他支持选项支持。

我的 MFA 设备遗失或停止工作

如果您的 MFA 设备丢失、损坏或无法运行，则在发送 MFA 验证请求时，您不会收到一次性密码 (OTP)。

IAM 用户

您可以使用向同一 IAM 用户注册的另一台 MFA 设备登录。

IAM 用户必须联系管理员才能停用无法运行的 MFA 设备。如果没有管理员的帮助，这些用户将无法恢复 MFA 设备。您的管理员通常是信息技术 (IT) 人员，与组织中的其他成员 AWS 账户 相比，他们拥有更高的权限级别。此人创建了您的账户，并向用户提供了登录所需的访问凭证。

根用户

要恢复对根用户的访问权限，您必须使用向同一根用户注册的另一台 MFA 设备登录。然后，查看以下选项以恢复或更新您的 MFA 设备：

- 有关恢复 MFA 设备的 step-by-step说明，请参阅如果 MFA 设备丢失或停止工作怎么办？
- 有关如何更新 MFA 设备电话号码的 step-by-step说明，请参阅如何更新我的电话号码以重置丢失的 MFA 设备？
- 有关激活 MFA 设备的 step-by-step说明，请参阅中的为用户启用 MFA 设备。 AWS
- 如果您无法恢复 MFA 设备，请联系 支持。

> **Note**
>
> IAM 用户必须联系其管理员寻求有关 MFA 设备的帮助。 支持 无法帮助 IAM 用户解决 MFA 设备问题。

我无法访问 AWS Management Console 登录页面

如果登录页面未显示，则该域可能已被防火墙拦截。请联系网络管理员，根据用户类型和登录方式，将以下域或 URL 端点添加到网络内容过滤解决方案允许列表中。

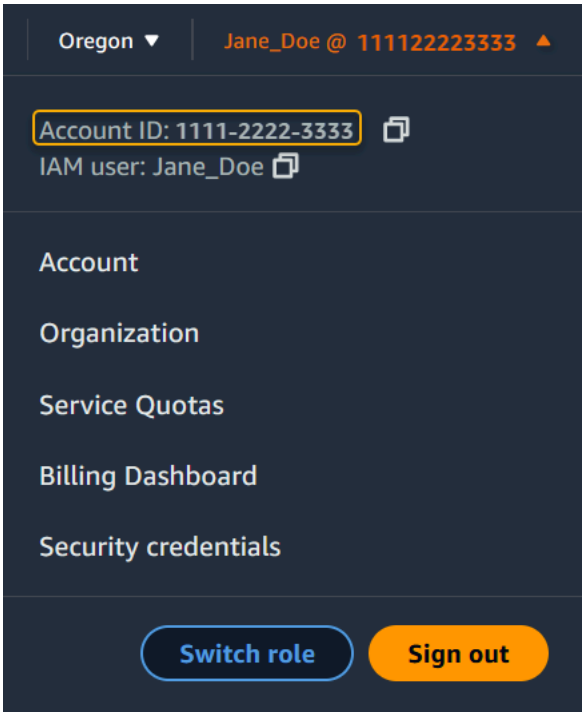
根用户和 IAM 用户	*.signin.aws.amazon.com
Amazon.com 账户登录	www.amazon.com
IAM Identity Center 用户和第一方应用程序登录	• *.awsapps.com (http://awsapps.com/) • *.signin.aws

如何查找我的 AWS 账户 ID 或别名

如果您是 IAM 用户并且尚未登录，则必须向管理员询问 AWS 账户 ID 或别名。您的管理员通常是信息技术 (IT) 人员，与组织中的其他成员 AWS 账户 相比，他们拥有更高的权限级别。此人创建了您的账户，并向用户提供了登录所需的访问凭证。

如果您是有权访问的 IAM 用户 AWS Management Console，则可以在您的登录 URL 中找到您的账户 ID。请查看管理员发来的电子邮件以获取登录 URL。账户 ID 是登录网址的前十二位数字。例如，在以下 URL 中`https://111122223333.signin.aws.amazon.com/console`，您的 AWS 账户 ID 是 111122223333。

登录后 AWS Management Console，您可以在您所在地区旁边的导航栏中找到您的账户信息。例如，在以下屏幕截图中，IAM 用户 Jane Doe 的得分为 1111-2222- AWS 账户 3333。



请参阅下表，详细了解如何根据用户类型查找您的 AWS 账户 。

用户类型和 AWS 账户 IDs

用户类型	过程		
根用户	在右上角的导航栏中，选择您的用户名，		

用户类型	过程		
	然后选择我的安全凭证。账号显示在账户标识符下面。		
IAM 用户	在右上角的导航栏中，选择您的用户名，然后选择我的安全凭证。账号显示在账户详情下面。		
担任的角色	在右上角的导航栏，选择 支持，然后选择支持中心。当前登录的 12 位账户号 (ID) 将显示在支持中心导航窗格中。		

有关您的 AWS 账户 ID 和别名以及如何找到它的更多信息，请参阅您的 AWS 账户 ID 及其别名。

我需要账户验证码

如果您提供了账户电子邮件地址和密码， AWS 有时会要求您提供一次性验证码。要检索验证码，请查看与您 AWS 账户 关联的电子邮件中是否有来自 Amazon Web Services 的消息。电子邮件地址以 @signin.aws 或 @verify.signin.aws 结尾。按照邮件中的说明操作。如果您在账户中未看到此类邮件，请检查垃圾邮件文件夹。如果您不再拥有该电子邮件的访问权限，请参阅 我无权访问我 AWS 账户的电子邮件。

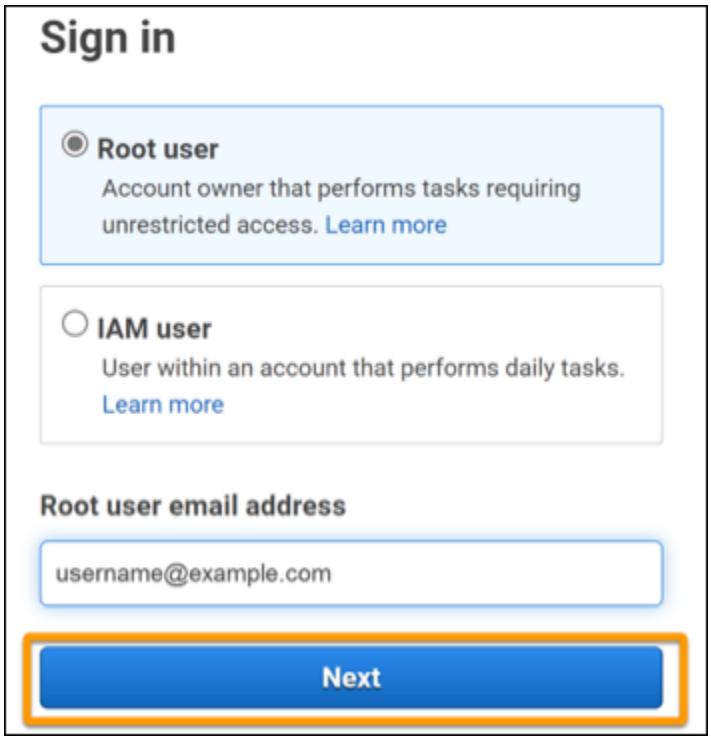
我忘记了 AWS 账户根用户密码

如果您是 root 用户，并且丢失或忘记了自己的密码 AWS 账户，则可以通过选择中的 “忘记密码” 链接来重置密码 AWS Management Console。您必须知道 AWS 账户的电子邮件地址，并且必须有权访问该电子邮件帐户。在密码恢复流程中，您可通过电子邮件收到密码重置链接。该链接将发送到您用来创建的电子邮件地址 AWS 账户。

要重置您使用 Organizations 创建的账户的密码，请参阅 AWS 以 root 用户身份访问成员账户。

重置根用户密码

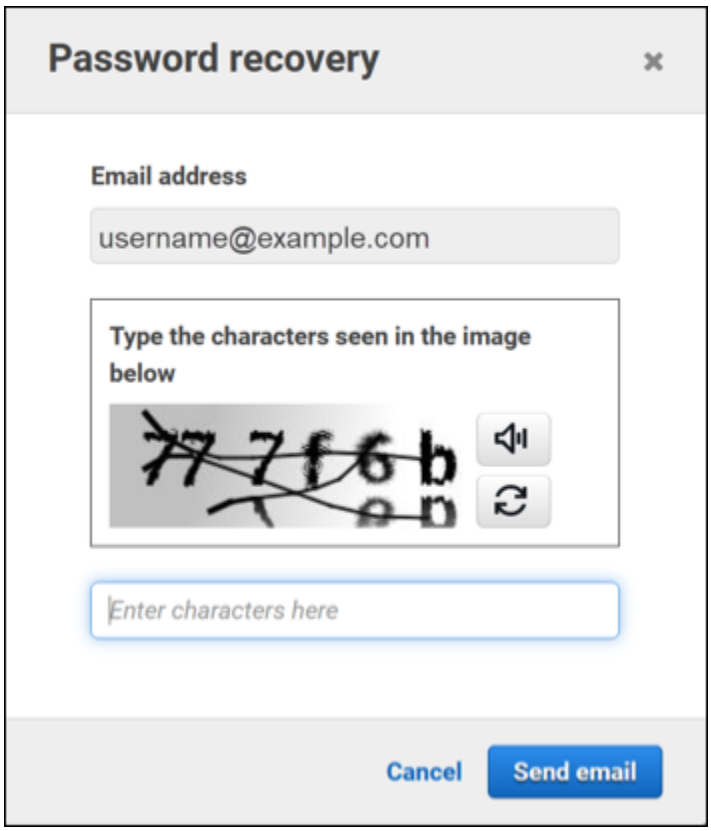
1. 使用您的 AWS 电子邮件地址开始以 root 用户身份登录AWS 管理控制台。然后选择下一步。



> **Note**
>
> 如果您已使用 IAM 用户凭证登录到 AWS Management Console，则必须注销，然后才能重置根用户密码。如果您看到特定于账户的 IAM 用户登录页面，请选择页面底部附近的使用根账户凭证登录。如有必要，请提供您的账户电子邮件地址并选择下一步来访问根用户登录页面。

2. 选择忘记密码？。

3. 完成密码恢复步骤。如果您无法完成安全检查，请尝试收听音频或刷新安全检查页面，以获得一组新字符。下图显示了密码恢复页面的示例。

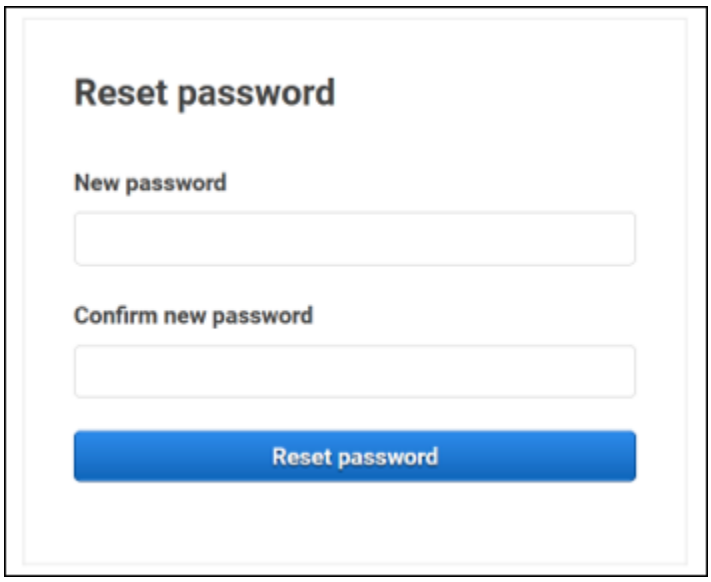


4. 完成密码恢复步骤后，您会收到一条消息，确认进一步的说明已发送到与 AWS 账户关联的电子邮件地址。

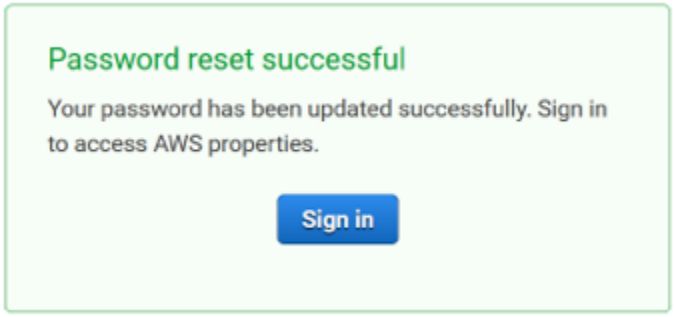
   包含密码重置链接的电子邮件会发送到用于创建 AWS 账户的电子邮件地址。

> **Note**
>
> 电子邮件来自以 @signin.aws 或 @verify.signin.aws 结尾的地址。

5. 选择 AWS 电子邮件中提供的链接以重置您的 AWS root 用户密码。
6. 该链接会将您定向到新网页以创建新的根用户密码。



您会收到密码重置成功的确认信息。下图显示了成功的密码重置操作。

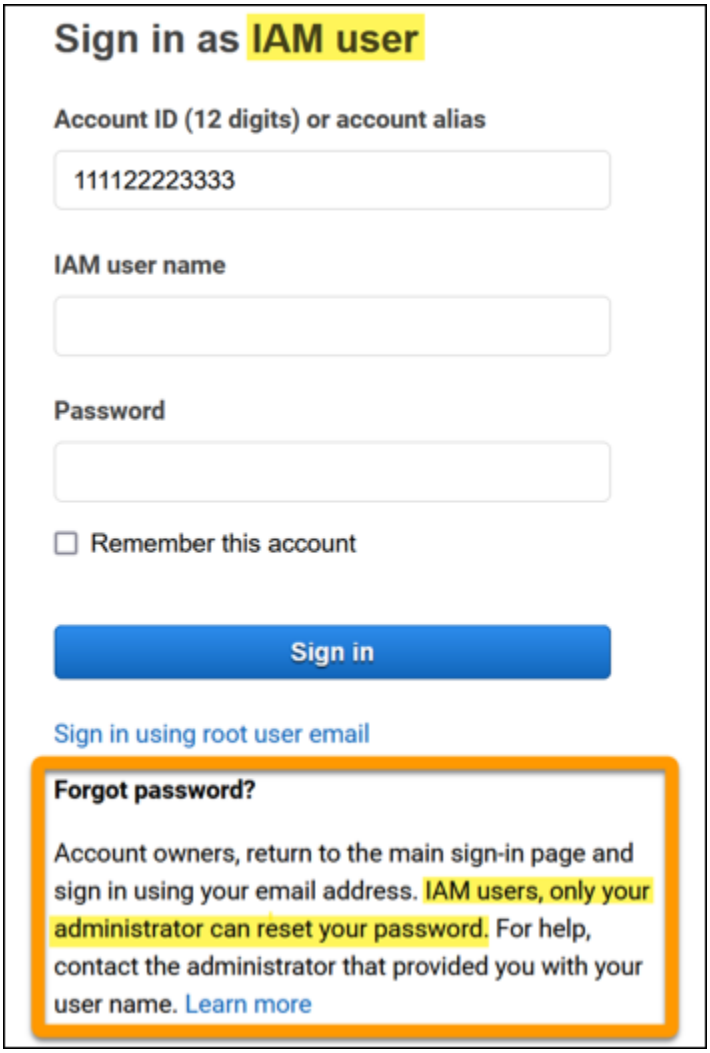


有关重置 root 用户密码的更多信息，请参阅如何恢复丢失或忘记的 AWS 密码？

我忘记了 AWS 账户的 IAM 用户密码

如需更改您的 IAM 用户密码，您必须拥有适当权限。有关重置 IAM 用户密码的更多信息，请参阅 IAM 用户如何更改自己的密码。

如果您无权重置密码，则只有 IAM 管理员才能重置 IAM 用户密码。IAM 用户应联系 IAM 管理员以重置密码。您的管理员通常是信息技术 (IT) 人员，与组织中的其他成员 AWS 账户 相比，他们拥有更高的权限级别。此人创建了您的账户，并向用户提供了登录所需的访问凭证。



出于安全考虑， 支持 无权查看、提供或更改您的证书。

有关重置 IAM 用户密码的更多信息，请参阅如何恢复丢失或忘记的 AWS 密码？

如需了解管理员如何管理您的密码，请参阅管理 IAM 用户密码。

我忘记了我的联邦身份密码 AWS 账户

联合身份登录后使用外部身份 AWS 账户 进行访问。使用的外部身份类型决定了联合身份的登录方式。您的管理员创建联合身份。有关如何重置密码的更多详细信息，请咨询您的管理员。您的管理员通常是信息技术 (IT) 人员，与组织中的其他成员 AWS 账户 相比，他们拥有更高的权限级别。此人创建了您的账户，并向用户提供了登录所需的访问凭证。

我无法登录现有的 AWS 账户 ，也无法 AWS 账户 使用相同的电子邮件地址创建新的

您只能将一个电子邮件地址与一个 AWS 账户根用户关联。如果您关闭了 root 用户账户，并且该账户的关闭时间超过 90 天，则无法 AWS 账户 使用与该账户关联的电子邮件地址重新打开账户或创建新账户。

如需解决这个问题，您可以使用子寻址，即在注册新账户时，在常规电子邮件地址后面添加一个加号 (+)。加号 (+) 后面可以是大写或小写字母、数字或其他支持 SMTP（简单邮件传输协议）的字符。例如，您可以使用 email+1@yourcompany.com 或 email+tag@yourcompany.com，其中，您的常规电子邮件地址是 email@yourcompany.com。尽管子寻址与常规电子邮件地址连接到同一个收件箱，但子寻址仍被视为新地址。我们建议您在注册新账户之前向附加的电子邮件地址发送一封测试电子邮件，以确认您的电子邮件提供商支持子寻址。

我需要重新激活已暂停的 AWS 账户

如果你的已暂停 AWS 账户 并且你想将其恢复，请参阅如何重新激活我的暂停状态？ AWS 账户

我需要联系 支持 以解决登录问题

如果您尝试了所有方法，则 支持 可以通过完成账单和账户支持请求来获得帮助。

我需要联系 AWS Billing 以解决账单问题

如果您无法登录 AWS 账户 并想联系 AWS Billing 以解决账单问题，则可以通过账单和账户支持请求进行联系。有关更多信息 AWS 账单与成本管理，包括您的费用和付款方式，请参阅获取帮助 AWS Billing。

我对零售订单有疑问

如果 www.amazon.com 账户有问题，或者您对零售订单有疑问，请参阅支持选项和联系我们。

我需要帮助来管理我的 AWS 账户

如果您在更改信用卡 AWS 账户、举报欺诈活动或关闭信用卡时需要帮助 AWS 账户，请参阅解决其他问题 AWS 账户。

我的 AWS 访问门户凭证不起作用

当您无法登录 AWS 访问门户时，请尝试记住您之前的访问方式 AWS。

如果您根本不记得使用过密码

您以前可能在没有使用 AWS 凭据 AWS 的情况下访问过。这对于通过 IAM Identity Center 进行企业单点登录很常见。通过 AWS 这种方式访问意味着您无需输入凭据即可使用公司凭证访问 AWS 账户或应用程序。

- AWS 访问门户-如果管理员允许您使用外部凭据 AWS 进行访问 AWS，则需要门户的 URL。检查您的电子邮件、浏览器收藏夹或浏览器历史记录，查找包含 `awsapps.com/start` 或 `signin.aws/platform/login` 的 URL。

  例如，您的自定义 URL 可能包含某个 ID 或域，例如 `https://d-1234567890.awsapps.com/start`。如果找不到您的门户链接，请联系您的管理员。 支持 无法帮助您恢复这些信息。

如果您记得用户名和密码，但凭证不起作用，则可能是您访问了错误的页面。在您的 Web 浏览器中查看网址，如果是 https://signin.aws.amazon.com/，则联合用户或 IAM Identity Center 用户无法使用其证书登录。

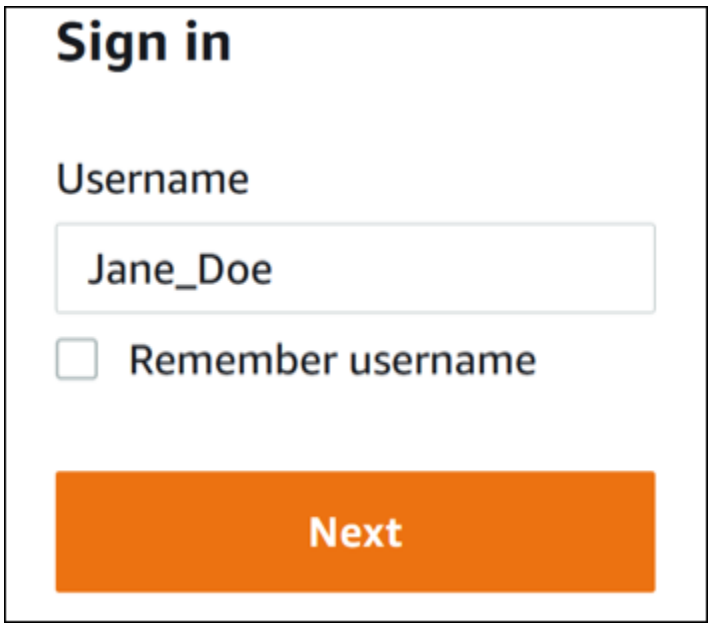
- AWS 访问门户 — 如果管理员为其设置了 AWS IAM Identity Center（ AWS 单点登录的继任者）身份源 AWS，则您必须在组织的 AWS 访问门户上使用您的用户名和密码登录。如需查找门户的 URL，请检查您的电子邮件、安全密码存储、浏览器收藏夹或浏览器历史记录中包含 `awsapps.com/start` 或 `signin.aws/platform/login` 的 URL。例如，您的自定义 URL 可能包含 ID 或域名，例如`https://d-1234567890.awsapps.com/start`.如果您找不到门户链接，请联系您的管理员。 支持 无法帮助您恢复这些信息。

我忘记了我的 IAM 身份中心密码 AWS 账户

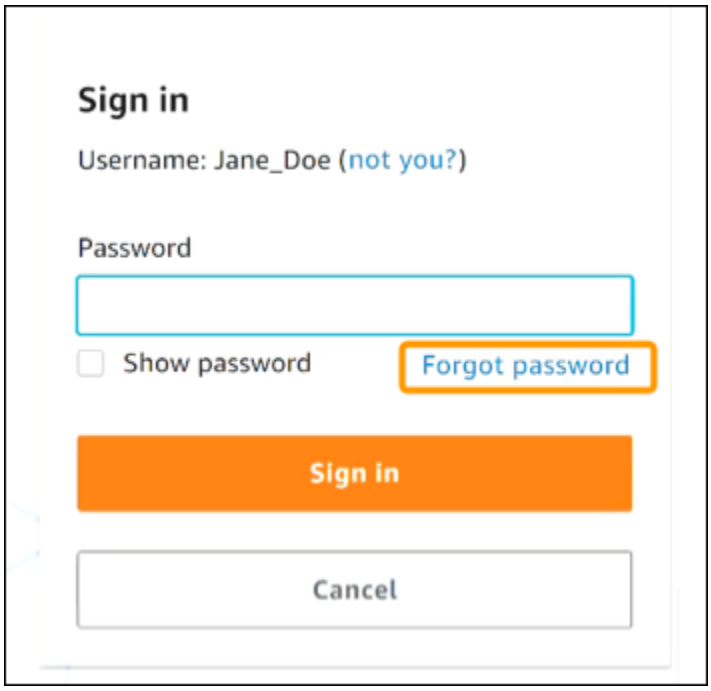
如果您是 IAM Identity Center 用户并且丢失或忘记 AWS 账户的密码，可以重置您的密码。您必须知道用于 IAM Identity Center 账户的电子邮件地址且有访问权限。密码重置链接会发送到您的 AWS 账户电子邮箱。

重置 IAM Identity Center 用户密码

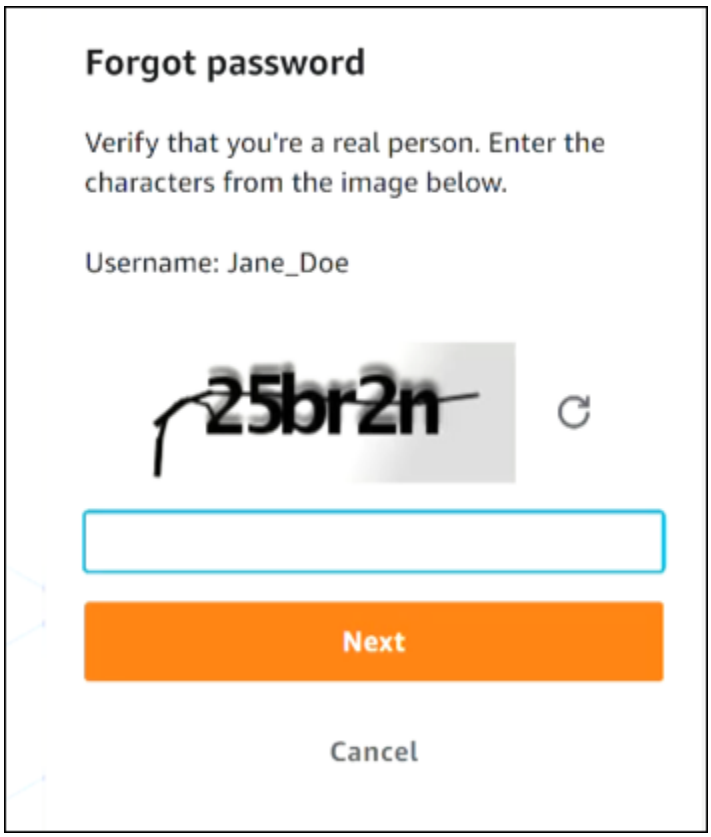
1. 使用您的 AWS 访问门户 URL 链接并输入您的用户名。然后选择下一步。



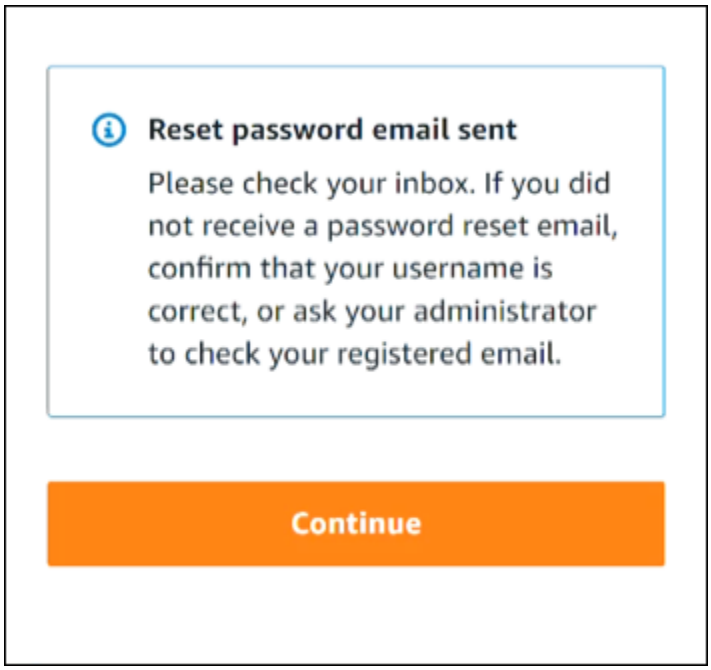
2. 选择忘记密码，如下图所示。



3. 完成密码恢复步骤。



4. 完成密码恢复步骤后，您会收到以下消息，确认已向您发送了可用于重置密码的电子邮件。



包含密码重置链接的电子邮件会发送到与 IAM Identity Center 用户账户关联的电子邮件地址。选择 AWS 电子邮件中提供的链接以重置您的密码。该链接会将您定向到新网页以创建新密码。创建新密码后，您会收到密码重置成功的确认信息。

如果您没有收到密码重置电子邮件，请向管理员确认您使用哪个电子邮件地址注册 IAM Identity Center 用户账户。

当我尝试登录 IAM Identity Center 控制台时，我收到一条错误消息，上面写着“It’s not you, it’s us”（不是您，是我们）

此错误表明您的 IAM Identity Center 实例或其用作身份源的外部身份提供者 (IdP) 存在设置问题。我们建议您执行以下操作：

- 验证您用于登录的设备上的日期和时间设置。我们建议您允许自动设置日期和时间。如果不可用，我们建议将您的日期和时间同步到已知的网络时间协议 (NTP) 服务器。
- 确认上传到 IAM Identity Center 的 IdP 证书与您的身份提供者提供的证书相同。您可以通过导航到 Settings（设置），从 IAM Identity Center console（IAM Identity Center 控制台）查看证书。在 Identity Source（身份源）选项卡的 Action”（操作）下，选择 Manage Authentication（管理身份验证）。您可能需要导入新的证书。
- 在您的 IdP 的 SAML 元数据文件中，确保 NameID 格式为 `urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress`。
- 如果您使用的是 AD Connector，请验证服务帐号的凭证是否正确且未过期。有关更多信息，请参阅中的更新您的 AD Connector 服务账号凭证 AWS Directory Service。

对 AWS 生成器 ID 问题进行故障排除

使用此处的信息可帮助您解决在使用 AWS 构建者 ID时可能遇到的问题。

主题

我的电子邮件地址已在使用中

如果您输入的电子邮件已在使用中，并且您将其识别为自己的电子邮件，那么您可能已经注册了 AWS Builder ID。尝试使用该电子邮件地址登录。如果忘记密码，请参阅 我忘记密码了。

我无法完成电子邮件验证

如果您注册了 AWS Builder ID 但尚未收到验证电子邮件，请完成以下疑难解答任务。

1. 检查您的垃圾邮件文件夹、广告邮件文件夹和已删除邮件文件夹。

> **Note**
>
> 此验证电子邮件的发件地址为 no-reply@signin.aws 或 no-reply@login.awsapps.com。我们建议您配置自己的电子邮件系统，以便接受来自这些发件人电子邮件地址的电子邮件，而不将其视为垃圾邮件或群发邮件。

2. 选择重新发送验证码，刷新收件箱，然后再次检查您的群发邮件文件夹、垃圾邮件文件夹和已删除邮件文件夹。
3. 如果您仍然看不到验证邮件，请仔细检查您的 AWS 建筑商 ID 电子邮件地址是否有错别字。如果您输入了错误的电子邮件地址，请使用自己的电子邮件地址重新注册。

当我尝试使用我的登录时，我收到一条错误消息，上面写着 “不是你，是我们” AWS 构建者 ID

如果您在尝试登录时收到此错误消息，则可能是您的本地设置或电子邮件地址有问题。

- 验证您用于登录的设备上的日期和时间设置。我们建议您允许自动设置日期和时间。如果不可用，我们建议将您的日期和时间同步到已知的网络时间协议 (NTP) 服务器。
- 检查您的电子邮件地址是否存在格式错误。尝试使用您的登录时，以下问题将返回错误 AWS 构建者 ID。
  - 电子邮件地址中的空格
  - 电子邮件地址中的正斜杠 (/)
  - 电子邮件地址中有两个句点 (.)
  - 电子邮件地址中有两个 & 符号 (@)
  - 电子邮件地址末尾的逗号 (,)
  - 电子邮件地址末尾的方括号 (])

我忘记密码了

重置忘记的密码

1. 在 “使用 AWS 建筑商 ID 登录” 页面上，在 “电子邮件地址” 中输入您用于创建 AWS 生成器 ID 的电子邮件。选择下一步。

2. 选择忘记密码？。我们会向您的 AWS Builder ID 关联的电子邮件地址发送一个链接，您可以在其中重置密码。
3. 按照电子邮件中的说明操作。

我无法设置新密码

出于安全考虑，无论何时设置或更改密码，都必须遵循以下要求：

- 密码区分大小写。
- 密码长度必须在 8 到 64 个字符之间。
- 密码必须包含下列四种类别中每种类别的至少一个字符：
  - 小写字母 (a-z)
  - 大写字母 (A-Z)
  - 数字 (0-9)
  - 非字母数字字符（ ~!@#$%^management portal*_-+=`|\(){}[]:;"'<>,.?/ ）
- 不能与最近使用的三个密码重复。
- 不能使用通过第三方泄露的数据集公开的密码。

我的密码不起作用

如果您记得自己的密码，但使用 AWS 生成器 ID 登录时密码不起作用，请确保：

- Caps Lock 已关闭。
- 您没有使用旧密码。
- 您使用的是 AWS 建筑商ID密码，而不是用于 AWS 账户.

如果您确认密码输入正确，但仍然不起作用，请按照中的说明我忘记密码了重置密码。 up-to-date

我的密码不起作用，我无法再访问发送到我的 AWS Builder ID 电子邮件地址的电子邮件

如果您仍然可以登录您的 AWS 建筑商 ID，请使用个人资料页面将您的 AWS 建筑商 ID 电子邮件更新为新的电子邮件地址。完成电子邮件验证后，您可以通过新的电子邮件地址登录 AWS 并接收通信。

如果您使用的是工作或大学的电子邮件地址，此后离开了公司或学校，从而无法接收发送到该地址的任何电子邮件，请联系该电子邮件系统的管理员。他们可能会将您的电子邮件转发到新地址、授予临时访问权限或共享邮箱中的内容。

我无法启用 MFA

要启用 MFA，请按照 管理 AWS 构建者 ID 多因素身份验证 (MFA) 中的步骤将一个或多个 MFA 设备添加到您的配置文件中。

我无法将身份验证器应用程序添加为 MFA 设备

若发现无法添加其他 MFA 设备，则可能已达到可在该应用程序中注册的 MFA 设备的限制。尝试移除未使用的 MFA 设备或使用其他身份验证器应用程序。

我无法删除 MFA 设备

若打算禁用 MFA，请按照 删除 MFA 设备 中的步骤移除您的 MFA 设备。但是，若想保持 MFA 的已启用状态，则应在尝试删除现有 MFA 设备之前添加其他 MFA 设备。更多有关添加其他 MFA 设备的信息，请参阅 管理 AWS 构建者 ID 多因素身份验证 (MFA)。

尝试使用身份验证器应用程序注册或登录时，收到“An unexpected error has occurred”（出现意外错误）消息

基于时间的一次性密码 (TOTP) 系统（例如 AWS Builder ID 与基于代码的身份验证器应用程序结合使用的系统）依赖于客户端和服务器之间的时间同步。确保安装身份验证器应用程序的设备已正确同步到可靠的时间源，或手动设置设备上的时间以匹配可靠来源，例如 NIST 或其他本地/区域等效时间。

尝试登录 Bu AWS ilder ID 时我收到 “不是你，是我们” 的消息

验证用于登录的设备上的日期和时间设置。建议允许自动设置日期和时间。如果不可用，我们建议将您的日期和时间同步到已知的网络时间协议 (NTP) 服务器。

注销未能将我立即完全注销

系统设计的初衷是立即注销，但完全注销可能需要最多一个小时。

我有问题需要解决

您可填写支持反馈表。在 “请求信息” 部分的 “我们如何为您提供帮助” 下，说明您正在使用 AWS 建筑商 ID。请尽量提供详细信息，以便我们能最有效地解决您的问题。

文档历史记录

下表描述了 AWS 登录文档的重要补充。我们还经常更新文档来处理发送给我们的反馈意见。

- 主要文档最新更新时间：2024 年 2 月 27 日

变更	说明	日期
更新了故障排除主题	添加了有关登录 AWS 构建者 ID 和的新疑难解答主题 AWS Management Console。	2024 年 2 月 27 日
更新了几个适用于组织的主题	更新了用户类型，删除了确定用户类型并将其内容合并到用户类型中，如何登录 AWS	2023 年 5 月 15 日
更新了几个主题和顶部横幅	更新了用户类型、确定用户类型、如何登录 AWS、什么是 AWS 登录？ 。还更新了根用户和 IAM 用户登录程序。	2023 年 3 月 3 日
更新了 AWS Management Console 登录的介绍段落	将确定用户类型移至页面顶部，并移除了账户根用户中存在的备注。	2023 年 2 月 27 日
已添加 AWS 构建者 ID	在《 AWS 登录用户指南》中添加了 AWS 构建者 ID 主题，并将内容集成到现有主题中。	2023 年 1 月 31 日
组织相关更新	基于客户反馈更新了目录，使其更清楚地显示登录方法。更新了登录教程。更新了术语和确定用户类型。改进了交叉链接，以定义 IAM 用户和根用户等术语。	2022 年 12 月 22 日

新指南	这是《 AWS 登录用户指南》的第一版。	2022 年 8 月 31 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。