



用户指南

AWS 登录



AWS 登录: 用户指南

Copyright © 2024 Amazon Web Services, Inc. and/or its affiliates. All rights reserved.

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

Table of Contents

什么是 AWS 登录？	1
术语	1
管理员	1
账户	2
凭证	2
企业凭证	2
配置文件	2
根用户凭证	2
用户	3
验证代码	3
用户类型	3
根用户	4
IAM 用户	4
IAM Identity Center 用户	5
联合身份	5
AWS Builder ID 用户	6
关于登录 URL	6
AWS 账户 根用户登录 URL	6
AWS 访问门户	6
IAM 用户登录 URL	7
联合身份 URL	8
AWS Builder ID URL	8
安全最佳实操	8
区域可用性	9
如何登录 AWS	10
登录 AWS Management Console	10
以根用户身份登录	11
以 IAM 用户身份登录	14
登录 AWS 访问门户	15
登录 AWS 访问门户	15
通过登录 AWS Command Line Interface	17
其他信息	17
以联合身份登录	17
使用登录 AWS 构建者 ID	18

要使用登录 AWS 构建者 ID	18
创建你的 AWS 构建者 ID	19
AWS 工具和服务	20
要列入许可名单的域名	21
用你的 AWS 构建者 ID	22
隐私与数据	29
AWS 构建者 ID 和其他 AWS 证书	30
区域可用性	31
如何注销 AWS	32
注销 AWS Management Console	32
注销 AWS 访问门户	34
注销 AWS Builder ID	34
AWS 账户 登录问题疑难解答	36
我的 AWS Management Console 凭证不起作用	37
我无权访问我 AWS 账户的电子邮件	37
我的 MFA 设备遗失或停止工作	38
我无法访问 AWS Management Console 登录页面	38
如何查找我的 AWS 账户 ID 或别名	39
我需要账户验证码	40
我忘记了 AWS 账户根用户密码	40
我忘记了 AWS 账户的 IAM 用户密码	43
我忘记了我的联邦身份密码 AWS 账户	44
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	45
我需要重新激活已暂停的 AWS 账户	45
我需要联系 AWS Support 以解决登录问题	45
我需要联系 AWS Billing 以解决账单问题	45
我对零售订单有疑问	45
我需要帮助来管理我的 AWS 账户	45
我的 AWS 访问门户凭证不起作用	46
我忘记了我的 IAM 身份中心密码 AWS 账户	46
当我尝试登录时，我收到一条错误消息，上面写着“不是你，是我们”	49
对 AWS 生成器 ID 问题进行故障排除	50
我的电子邮件地址已在使用中	50
我无法完成电子邮件验证	50
当我尝试登录时，我收到一条错误消息，上面写着“不是你，是我们”	51
我忘记密码了	51

我无法设置新密码	51
我的密码不起作用	52
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	52
我无法启用 MFA	52
我无法将身份验证器应用程序添加为 MFA 设备	53
我无法删除 MFA 设备	53
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	53
注销未能将我立即完全注销	53
我有问题需要解决	53
文档历史记录	54
.....	lvi

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 AWS 账户时遇到问题，请参阅 [AWS 账户 登录问题疑难解答](#)。如需有关 AWS 构建者 ID 的帮助，请参阅 [对 AWS 生成器 ID 问题进行故障排除](#)。想要创建 AWS 账户？[注册 AWS](#)。如需详细了解注册 AWS 对您或您的组织有何帮助，请参阅[联系我们](#)。

主题

- [术语](#)
- [用户类型](#)
- [关于登录 URL](#)
- [AWS 账户 管理员的安全最佳实践](#)
- [AWS 登录的区域可用性](#)

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。管理员比其组织中的其他成员拥有更高的 AWS 账户 权限级别。管理员为 AWS 账户 建立和实施设置。他们还创建 IAM 或 IAM Identity Center 用户。管理员向这些用户提供访问凭证和登录 URL 以供登录 AWS。

账户

标准 AWS 账户 包含您的 AWS 资源以及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相关联。

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。凭证是用户为了登录和获取 AWS 资源访问权限而提供给 AWS 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。

企业凭证

用户在访问公司网络和资源时提供的凭证。公司管理员可以将您的 AWS 账户 设置为使用您用于访问公司网络和资源的那些凭证。这些凭证由管理员或帮助中心员工提供给您。

配置文件

注册 AWS Builder ID 时，就会创建配置文件。配置文件包括您提供的联系信息以及管理多重身份验证 (MFA) 设备和活动会话的能力。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](#)。

用户

用户是有权对 AWS 产品进行 API 调用或访问 AWS 资源的人员或应用程序。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 [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：

用户类型

登录方式取决于您是哪种类型的 AWS 用户。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。

根用户

此账户所有者具有所有 AWS 服务和资源的完全访问权限。如果您创建 AWS 账户并使用根用户电子邮件和密码登录，则您就是根用户。有关更多信息，请参阅 [根用户](#)。

IAM 用户

AWS 账户中的一种身份，具有特定的自定义权限。如果您没有创建 AWS 账户，且管理员或帮助中心员工给您提供了包括 AWS 账户 ID 或账户别名、IAM 用户名和密码的登录凭证，则您就是 IAM 用户。有关更多信息，请参阅 [IAM 用户](#)。

IAM Identity Center 用户

其 AWS 账户是 AWS Organizations 一部分的用户，使用唯一的 URL 通过 AWS 访问门户登录。可以直接在 IAM Identity Center 也可以在 Active Directory 或其他外部身份提供者中创建这些用户。有关更多信息，请参阅 [IAM Identity Center 用户](#)。

如果以下任何一种情况属实，则您就是 IAM Identity Center 用户：

- 您收到来自管理员或 no-reply@login.awsapps.com 的电子邮件，其中包含 AWS 访问门户 URL。
- 您使用相同的凭证登录公司系统和 AWS 访问门户，且您的 AWS 账户是 AWS Organizations 的一部分。

联合身份

使用外部身份提供者 (IdP) 登录的用户。有关更多信息，请参阅 [联合身份](#)。

如果您符合以下任何一种情况，则您就是联合身份：

- 使用第三方凭证（例如 Login with Amazon、Facebook 或 Google）访问 AWS 账户 或资源。
- 使用相同的凭证登录公司系统和 AWS 服务，且使用自定义的公司门户登录 AWS。

AWS 构建者 ID

一种个人配置文件，让您可以登录要访问的 AWS 服务或工具。如果您登录的是 AWS 工具和服务，例如、和，则您就是 AWS 构建者 ID 用户 CodeWhisperer。AWS re:Post CodeCatalyst 有关更多信息，请参阅 [AWS Builder ID 用户](#)。

根用户

也称为账户所有者或账户根用户。作为根用户，您可以完全访问 AWS 账户 中的所有 AWS 服务和资源。当您首次创建 AWS 账户时，最初使用的是一个对账户中所有 AWS 服务和资源有完全访问权限的单个登录身份。此身份称作 AWS 账户根用户。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 AWS 账户 时，最初使用的是一个对账户中所有 AWS 服务和资源拥有完全访问权限的登录身份。此身份称为 AWS 账户根用户，使用您创建账户时所用的电子邮件地址和密码登录，即可获得该身份。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。有关需要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 AWS Organizations 的成员, 可以通过 AWS 访问门户获得对多个 AWS 账户和应用程序的访问权限。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。无论身份提供者如何, IAM Identity Center 用户都使用 AWS 访问门户登录 (此访问门户是用户所属组织的特定登录 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
- 来自 AWS 的电子邮件, 其中包含加入 IAM Identity Center 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。使用网络身份联合验证, 您可以接收身份验证令牌, 然后用该令牌交换 AWS 中的临时安全凭证, 这些凭证映射到

有权使用您 AWS 账户 中的资源的 IAM 角色。您未使用 AWS Management Console 或 AWS 访问门户登录。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 Builder 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 用户是对您已有或想要创建的 AWS 账户 的补充。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](#)。

关于登录 URL

根据您的 AWS 用户类型，使用以下 URL 之一访问 AWS。有关更多信息，请参阅 [用户类型](#)。

主题

- [AWS 账户 根用户登录 URL](#)
- [AWS 访问门户](#)
- [IAM 用户登录 URL](#)
- [联合身份 URL](#)
- [AWS Builder ID URL](#)

AWS 账户 根用户登录 URL

根用户从 AWS 登录页面 <https://console.aws.amazon.com/> 访问 AWS Management Console。

此登录页面还提供以 IAM 用户身份登录的选项。

AWS 访问门户

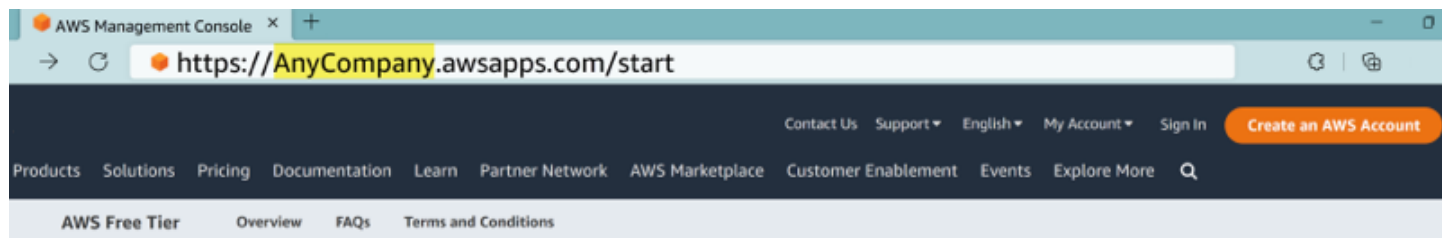
AWS 访问门户是 IAM Identity Center 用户用于登录和访问账户的特定登录 URL。当管理员在 IAM Identity Center 中创建用户时，管理员可以设置用户获取登录 URL 的方式：用户会收到邀请其加入 IAM Identity Center 的电子邮件；或者，用户会收到来自管理员或帮助中心员工的消息，其中包含一次性密码和 AWS 访问门户 URL。特定登录 URL 的格式类似于以下示例：

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

或者

```
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

我们建议您为 AWS 访问门户的特定登录 URL 添加书签，以便日后访问。

有关 AWS 访问门户的更多信息，请参阅[使用 AWS 访问门户](#)。

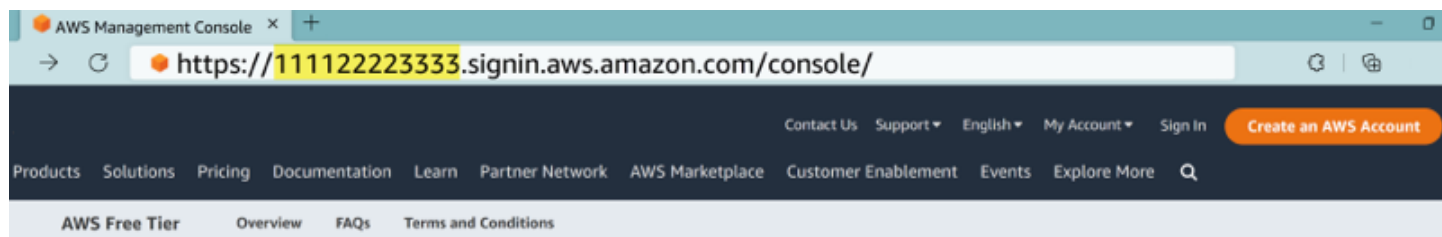
IAM 用户登录 URL

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

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：



如果您在使用 IAM 用户登录 URL 访问 AWS 账户时遇到问题，请参阅[AWS Identity and Access Management 中的弹性](#)了解更多信息。

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 Builder ID URL

AWS Builder ID 配置文件的 URL 是 <https://profile.aws.amazon.com/>。使用 AWS Builder 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>。

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 AWS 账户，我们建议您执行以下步骤，以帮助用户在登录时遵循 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](#)（如果尚未如此执行）。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](#)，并转向[最低权限](#)。
 - [向 AWS IAM Identity Center \(AWS 单点登录后继者 \) 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 [如何登录 AWS](#) 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。

AWS 登录的区域可用性

可在几个常用的 AWS 区域 进行 AWS 登录。这种可用性让您能更轻松地访问 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](#)。

如何登录 AWS

您的登录方式 AWS 取决于您的 AWS 用户类型。有不同类型的 AWS 用户。您可以是账户根用户、IAM 用户、IAM Identity Center 用户、联合身份，或使用 AWS 构建者 ID。有关更多信息，请参阅 [用户类型](#)。

您可以使用以下任一方法登录进行访问 AWS：

- [登录 AWS Management Console](#) 以根用户或 IAM 用户身份
- [登录 AWS 访问门户](#) 以 IAM Identity Center 用户身份
- [以联合身份登录](#)
- [通过登录 AWS Command Line Interface](#) 和其他编程方法，如 API 和 SDK (软件开发套件)
- [使用登录 AWS 构建者 ID](#)

如果要创建新的 AWS 账户，请参阅《AWS 安装指南》AWS 账户中的“[第 1 部分：设置新的](#)”。

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。

[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。

[IAM 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/>。

如果您不确定自己是哪种类型的用户，请参阅 [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](#)。

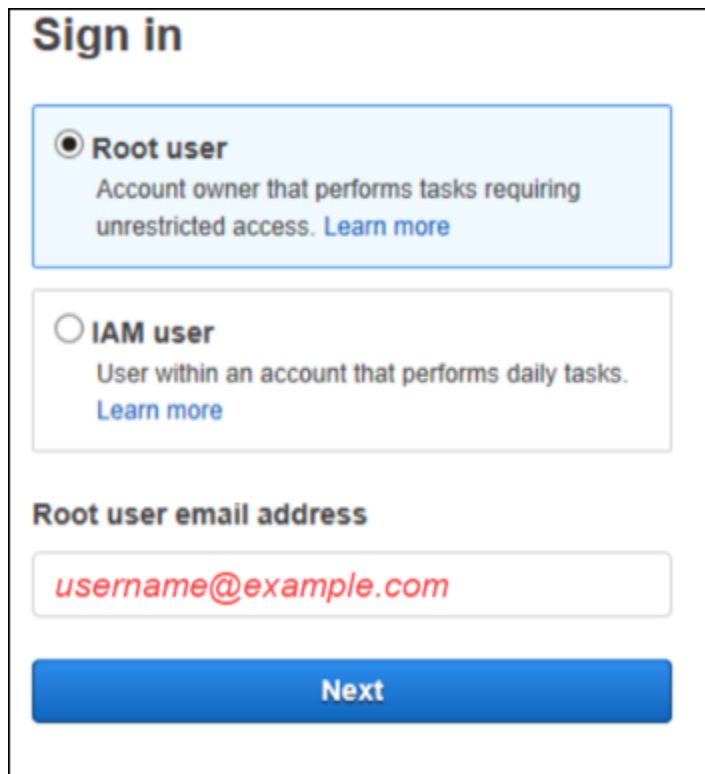
以根用户身份登录

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。如需返回主登录页面，请选择使用根用户电子邮件登录。

2. 选择根用户。

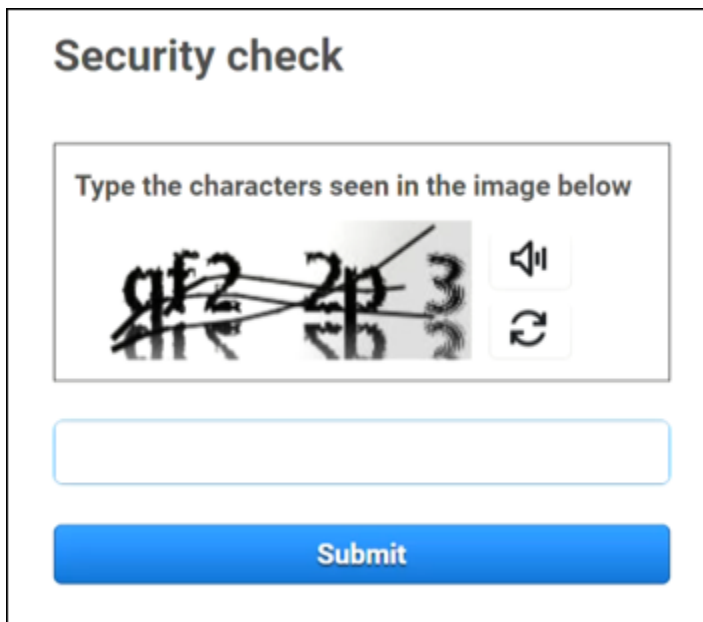


The screenshot shows the AWS 'Sign in' interface. At the top, the title 'Sign in' is displayed. Below it, there are two radio button options: 'Root user' (selected) and 'IAM user'. The 'Root user' option includes the text 'Account owner that performs tasks requiring unrestricted access. Learn more'. The 'IAM user' option includes the text 'User within an account that performs daily tasks. Learn more'. Below these options is a section titled 'Root user email address' with a text input field containing the placeholder text 'username@example.com'. At the bottom of the form is a blue button labeled 'Next'.

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。

i 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。



The image shows a 'Security check' screen. At the top, it says 'Security check'. Below that, there is a box with the text 'Type the characters seen in the image below'. Inside this box, there is a distorted image of the characters '2', '2', and '3'. To the right of the image are two icons: a speaker icon and a refresh icon. Below the box is an empty text input field. At the bottom of the screen is a blue button labeled 'Submit'.

5. 输入您的密码。



The image shows a 'Root user sign in' screen. At the top, it says 'Root user sign in' with an information icon. Below that, it says 'Email: *username@example.com*'. There are two fields: 'Password' and 'Forgot password?'. Below the 'Password' field is an empty text input field. At the bottom of the screen is a blue button labeled 'Sign in'. Below the button are two links: 'Sign in to a different account' and 'Create a new AWS account'.

6. 使用 MFA 进行身份验证。为了安全起见，我们强烈建议您[对根用户激活 MFA](#)。如果未对根用户启用 MFA，则您可能需要完成一次性密码 (OTP) 质询以验证您的登录尝试。
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

[IAM 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（例如 *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

1. 打开 a AWS Management Console t <https://console.aws.amazon.com/>。
2. 将显示主登录页面。选择 IAM 用户，输入账户 ID（12 位数字）或别名，然后选择下一步。

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. 输入您的 IAM 用户名和密码，然后选择登录。
4. 如果 IAM 用户启用了 MFA，您可以使用其进行身份验证。

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 ID 的详细信息，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 Identity 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 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。如果您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。

将显示您的用户的角色。为要开设的账户选择角色名 AWS Management Console。选择访问密钥以获取命令行或编程访问凭证。

- b. 选择应用程序选项卡以显示可用的应用程序，然后选择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，用户可以在 8 小时内登录。AWS 账户 IAM 身份中心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](#)。

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。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 AWS 软件开发工具包的 IAM 身份中心用户证书](#)。
- 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](#)、[Amazon 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。与其他个人配置文件一样，在您实现个人、教育和职业目标的过程中，AWS 构建者 ID 会一直跟随着您。

任何 AWS 账户 您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](#)。

主题

- [要使用登录 AWS 构建者 ID](#)
- [创建你的 AWS 构建者 ID](#)
- [AWS 使用的工具和服务 AWS 构建者 ID](#)
- [要列入许可名单的域名 AWS 构建者 ID](#)
- [用你的 AWS 构建者 ID](#)
- [隐私和数据 AWS 构建者 ID](#)
- [AWS 构建者 ID 和其他 AWS 证书](#)
- [区域可用性](#)

要使用登录 AWS 构建者 ID

1. 前往使用登录 AWS 构建者 ID 页面<https://profile.aws.amazon.com/> (或使用提供的 URL 访问您的服务)。
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。

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 工具或服务的注册页面或 [AWS 构建者 ID 个人资料](#)。

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。如果您在五分钟内仍未看到电子邮件，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。

AWS 云社区

[Community.aws](#) 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，您可以发现教育内容，分享您的个人想法和项目，评论他人的帖子，并关注您最喜欢的构建者。

亚马逊 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

使用您的访问权限 [AWS Migration Hub](#) (Migration Hub) AWS 构建者 ID。Migration Hub 提供了一个地方来发现您的现有服务器、规划迁移和跟踪每个应用程序迁移的状态。

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[什么是 Amazon Q 开发者？](#) 在 Amazon Q 开发者用户指南中。

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](#)。

要列入许可名单的域名 AWS 构建者 ID

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创建和使用。AWS 构建者 ID在您尝试访问的网络上必须可以访问以下域 AWS 构建者 ID。

- 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

用你的 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。创建后，您可以更新和管理您的安全设置，AWS 构建者 ID 例如多重身份验证 (MFA)、密码和会话。

要了解使用哪些 AWS 工具和服务 AWS 构建者 ID，请参阅[AWS 使用的工具和服务 AWS 构建者 ID](#)。

主题

- [编辑您的 AWS 构建者 ID 个人资料](#)
- [更改您的 AWS 构建者 ID 密码](#)
- [删除所有活动会话](#)
- [删除你的 AWS 构建者 ID](#)
- [管理 AWS 构建者 ID 多因素身份验证 \(MFA\)](#)

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。您的昵称表示您希望如何被 AWS 朋友和其他与您密切合作的人所认识。

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。

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。

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，您将无法再访问之前注册的任何 AWS 工具和服务。

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 Privacy & data (隐私与数据)。
3. 在隐私与数据页面中的删除 AWS 构建者 ID 下，选择删除 AWS 构建者 ID。

- 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


AWS 构建者 ID 永久删除您的数据会删除与您关联的所有数据，AWS 构建者 ID 并且您将无法再从应用程序访问或恢复数据。

- 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。

建议注册多个 MFA 设备。例如，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。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。

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](#) 是一个包含 CTAP2 的标准，[WebAuthn](#) 并且基于公钥加密。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个因素。有关更多信息，请参见 [FIDO 身份验证](#)。

安全密钥

您可购买与 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，例如密码管理器的功能、带有 FIDO 模式的智能卡以及其他形式。这些兼容 FIDO 的装置可以与 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一下 FIDO 身份验证器。

Note

某些 FIDO 身份验证器可以创建可发现的 FIDO 凭证，这些凭证称为密钥。密钥可以绑定到创建密钥的装置，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，然后从带有 Google Chrome 浏览器的 Windows 笔记本电脑按照登录时屏幕上的提示使用 iCloud 中的密钥登录网站。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 Assign MFA (分配 MFA) 。

Important

生成代码之后立即提交您的请求。如果您生成代码后等待时间过长才提交请求，则 MFA 设备已成功与您的关联 AWS 构建者 ID，但是 MFA 设备不同步。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

使用安全密钥注册 MFA

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 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。如需禁用 AWS 构建者 ID 的多重身份验证，请从配置文件中移除所有已注册的 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](#)。

请求您的数据

我们将对您的数据与隐私保持透明。您可请求和查看 AWS 构建者 ID 存储的与您有关的数据。

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 Privacy & data (隐私与数据) 。
3. 在隐私与数据页面您的 AWS 构建者 ID 数据下，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) 。

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 软件开发工具包或工具包。

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 and 计量 AWS 服务 (例如 S3、EC2 或 Lambda) 建立了安全边界。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。您可以在 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 身份中心 (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。

区域可用性

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

如何注销 AWS

注销 AWS 账户 的方式取决于您是哪种类型的 AWS 用户。您可以是账户根用户、IAM 用户、IAM Identity Center 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 [用户类型](#)。

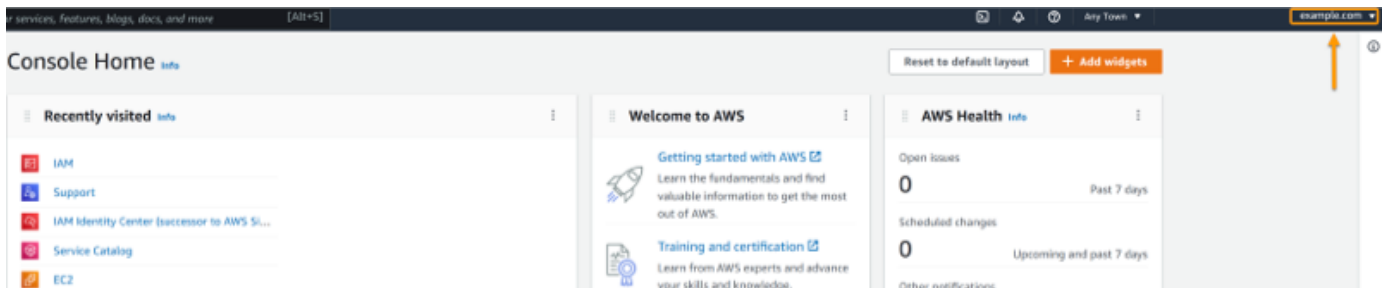
主题

- [注销 AWS Management Console](#)
- [注销 AWS 访问门户](#)
- [注销 AWS Builder ID](#)

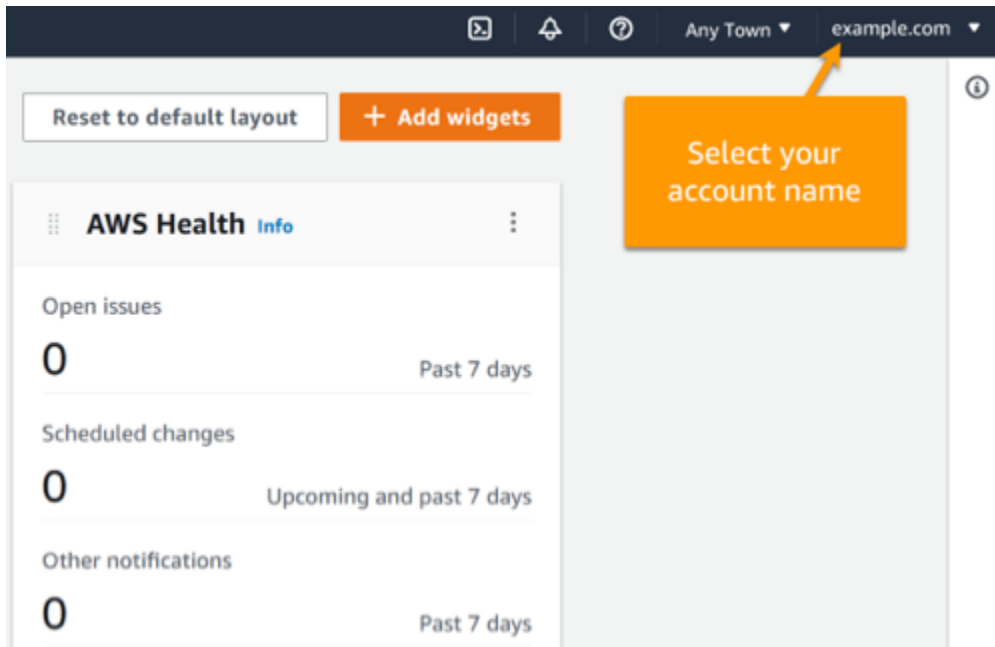
注销 AWS Management Console

如需注销 AWS Management Console。

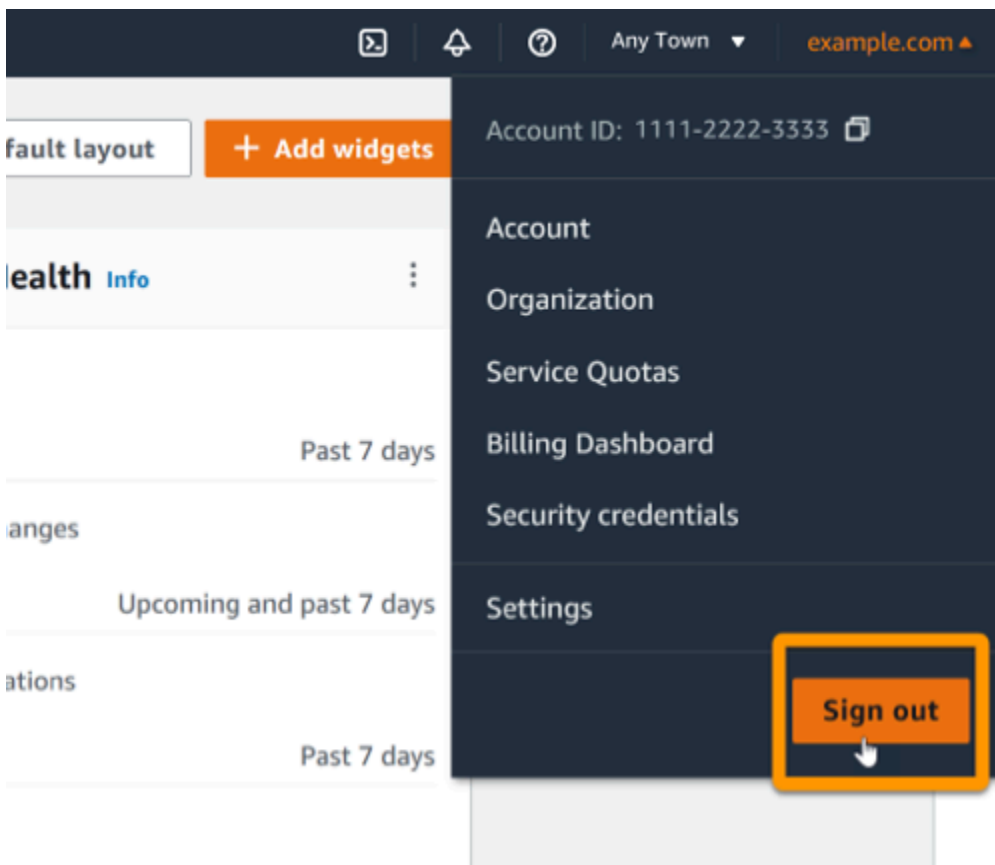
1. 登录 AWS Management Console 后，您将看到类似于下图所示的页面。您的账户名称或 IAM 用户名显示在右上角。



2. 在右上角的导航栏中，请选择您的用户名。



3. 选择注销，如下图所示。

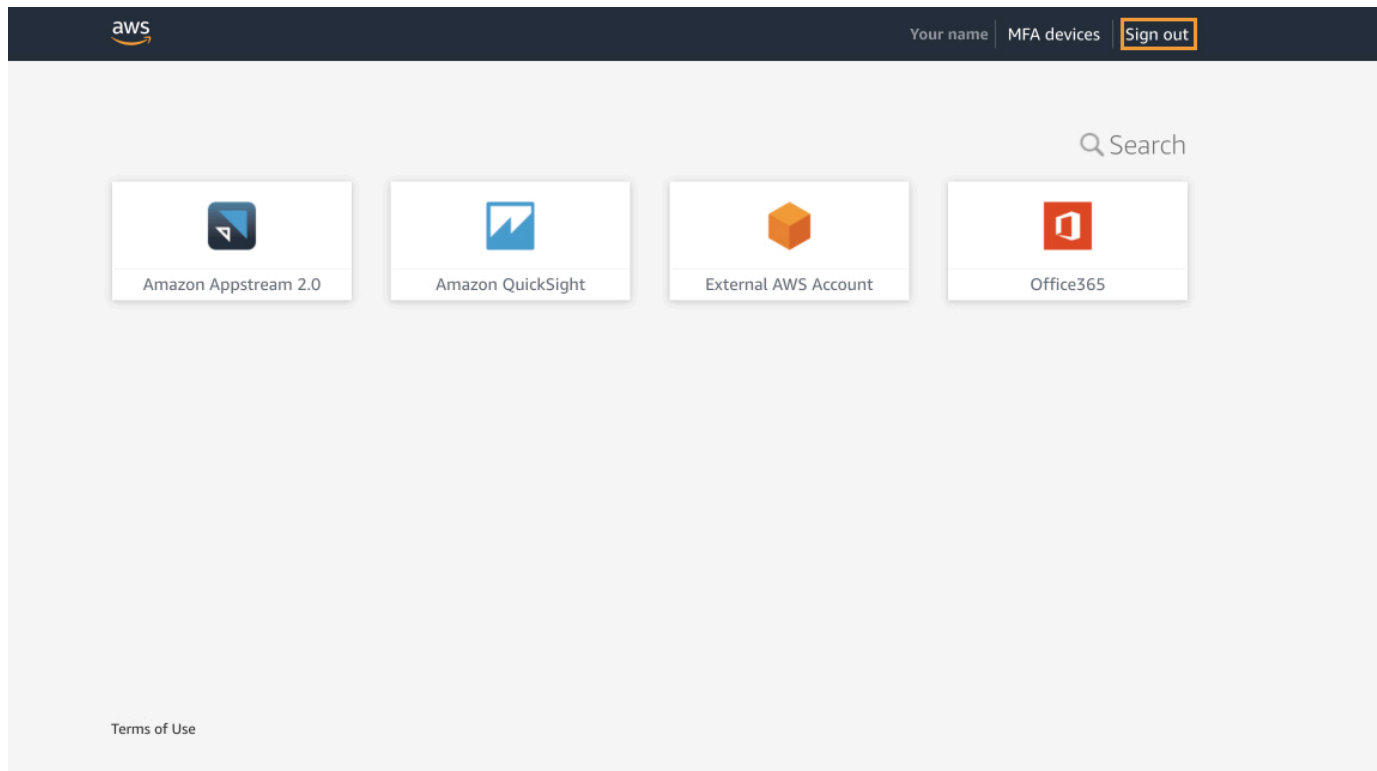


4. 您将返回到 AWS Management Console 网页。

注销 AWS 访问门户

如需注销 AWS 访问门户

1. 选择访问门户右上角的注销。



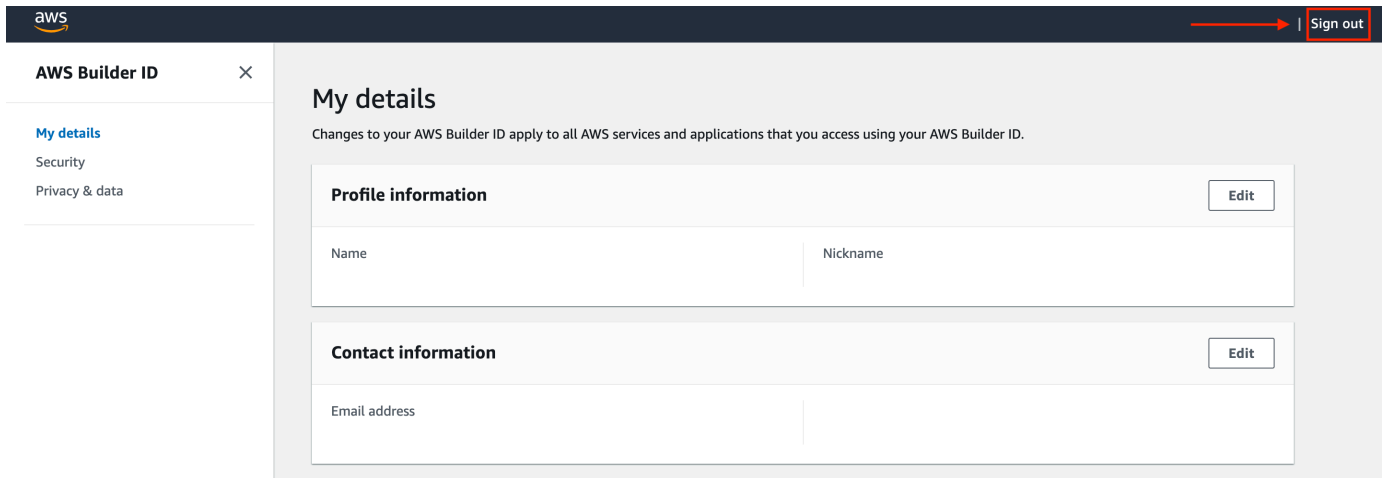
2. 如果注销成功，您现在会看到 AWS 访问门户登录页面。

注销 AWS Builder ID

如需注销使用 AWS Builder ID 访问的 AWS 服务，必须注销该服务。如需注销 AWS Builder ID 配置文件，请参阅以下程序。

如需注销 AWS Builder ID 配置文件

1. 访问 <https://profile.aws.amazon.com/> 并登录 AWS Builder ID 配置文件后，您将进入我的详细信息页面。
2. 在 AWS Builder ID 配置文件页面的右上角，选择注销。



3. 如果您不再能看到自己的 AWS Builder ID 配置文件，即表示您注销成功。

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[如何登录 AWS](#)。

如果所有疑难解答主题都无法帮助您解决登录问题，则 AWS Support 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，AWS Support 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

AWS Support 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 AWS Support 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“不是你，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据的任务，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。
- 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。AWS Support 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，该信件发送到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 [AWS Support](#)。

我的 MFA 设备遗失或停止工作

如果您的 AWS 账户 root 用户 MFA 设备丢失、损坏或无法运行，则可以恢复对账户的访问权限。IAM 用户必须与管理员联系，才能将装置停用。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。

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 [AWS Support](#)。

Note

IAM 用户必须联系管理员寻求有关 MFA 设备的帮助。AWS Support 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。

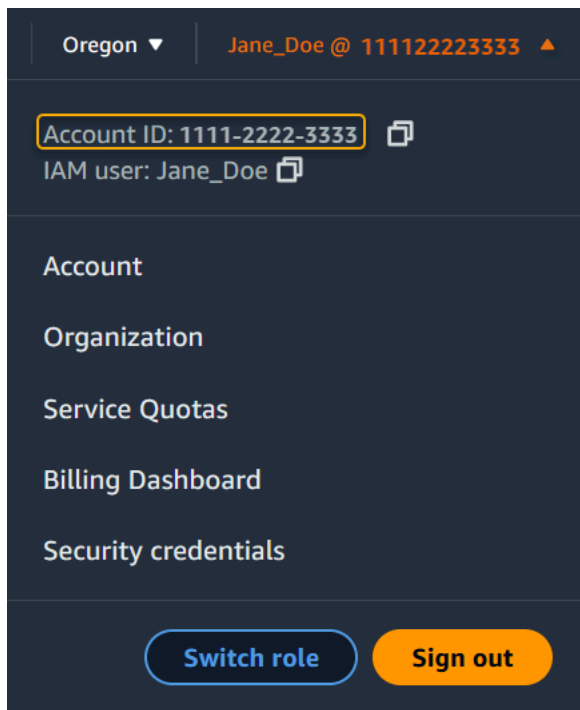
根用户和 IAM 用户	*.signin.aws.amazon.com
Amazon.com 账户登录	www.amazon.com
IAM Identity Center 用户和第一方应用程序登录	<ul style="list-style-type: none">• *.awsapps.com (http://awsapps.com/)• *.signin.aws

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。

如果您是拥有访问的 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。



有关如何 AWS 账户 根据您的用户类型找到您的用户的更多信息，请参阅下表。

用户类型和 AWS 账户 ID

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

如果您提供了账户的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](#)。

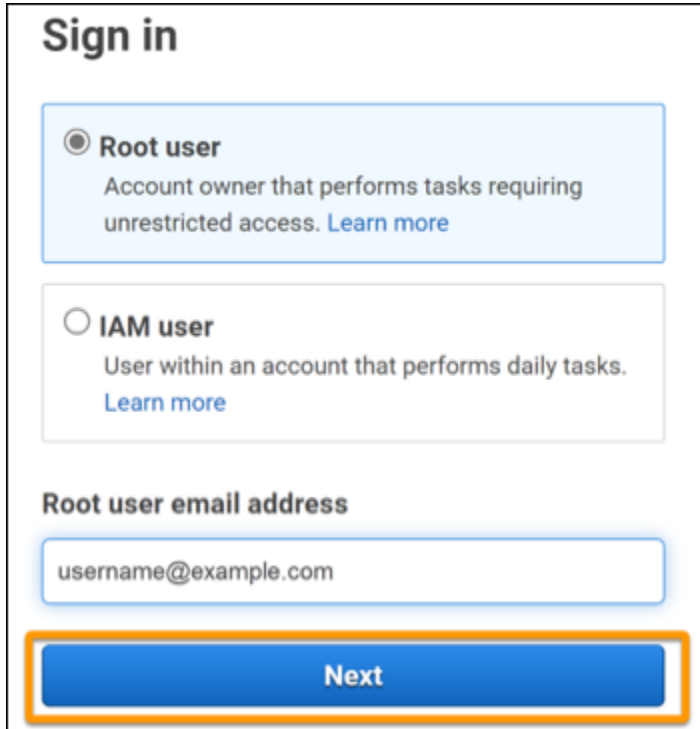
我忘记了 AWS 账户根用户密码

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。



The screenshot shows the AWS 'Sign in' page. At the top, the title 'Sign in' is displayed. Below it, there are two radio button options: 'Root user' (selected) and 'IAM user'. The 'Root user' option includes the text 'Account owner that performs tasks requiring unrestricted access. [Learn more](#)'. The 'IAM user' option includes the text 'User within an account that performs daily tasks. [Learn more](#)'. Below these options is a text input field labeled 'Root user email address' containing the placeholder text 'username@example.com'. At the bottom of the form, a blue 'Next' button is highlighted with a thick orange border.

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？。



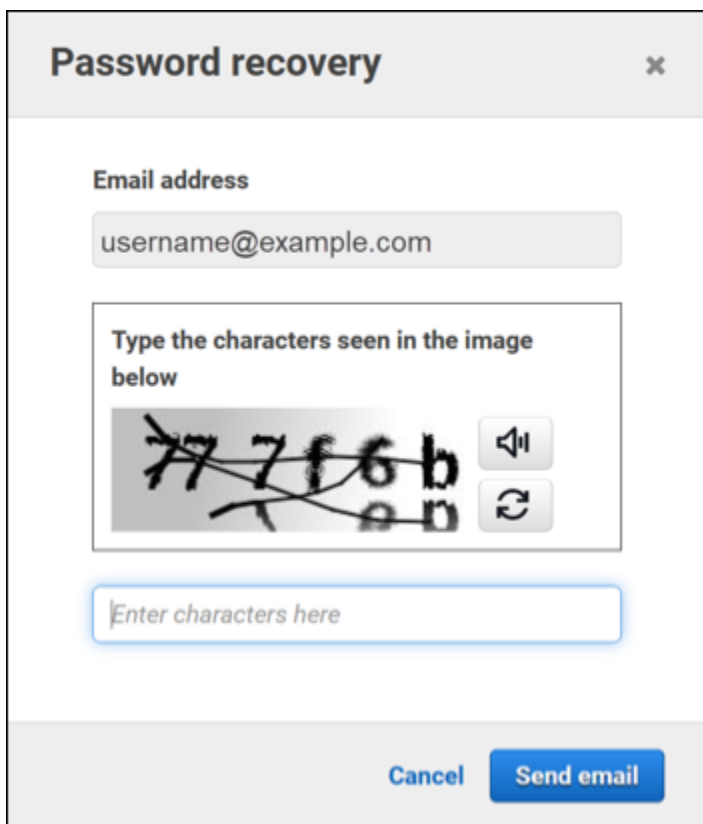
Root user sign in

Email: username@example.com

Password [Forgot password?](#)

Sign in

- 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。



Password recovery

Email address

username@example.com

Type the characters seen in the image below

777f6b

Enter characters here

Cancel Send email

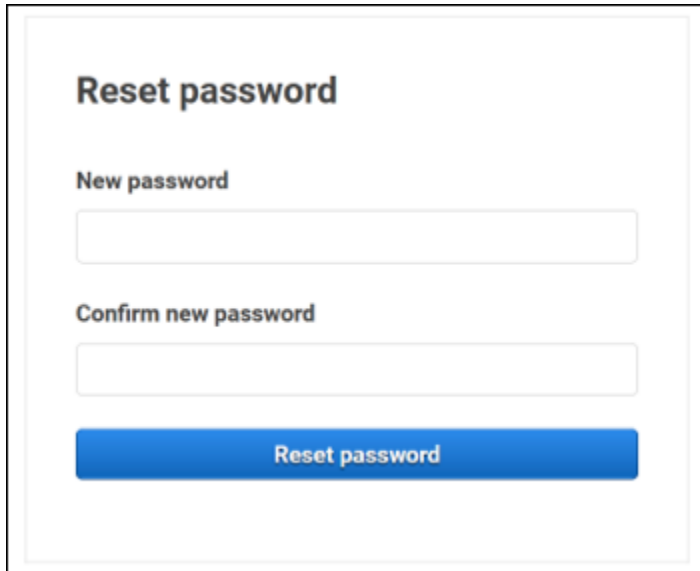
- 完成密码恢复步骤后，您会收到一条消息，确认进一步的说明已发送到与 AWS 账户关联的电子邮件地址。

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。



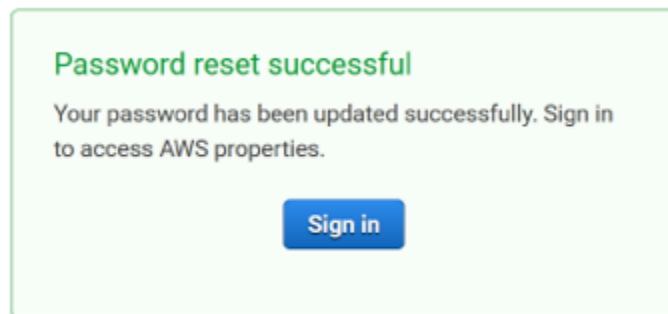
Reset password

New password

Confirm new password

Reset password

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。



Password reset successful

Your password has been updated successfully. Sign in to access AWS properties.

Sign in

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。

Sign in as IAM user

Account ID (12 digits) or account alias

111122223333

IAM user name

Password

Remember this account

Sign in

[Sign in using root user email](#)

Forgot password?

Account owners, return to the main sign-in page and sign in using your email address. IAM users, only your administrator can reset your password. For help, contact the administrator that provided you with your user name. [Learn more](#)

出于安全考虑，AWS Support 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 AWS Support 以解决登录问题

如果您尝试了所有方法，则 AWS Support 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 Billing and Cost Management，包括您的费用和付款方式，请参阅[获取相关帮助 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 AWS 未使用 AWS 凭据的情况下进行过访问。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。AWS Support 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。查看 Web 浏览器中的 URL，如果是 `https://signin.aws.amazon.com/`，则联合用户或 IAM Identity Center 用户无法使用其凭证登录。

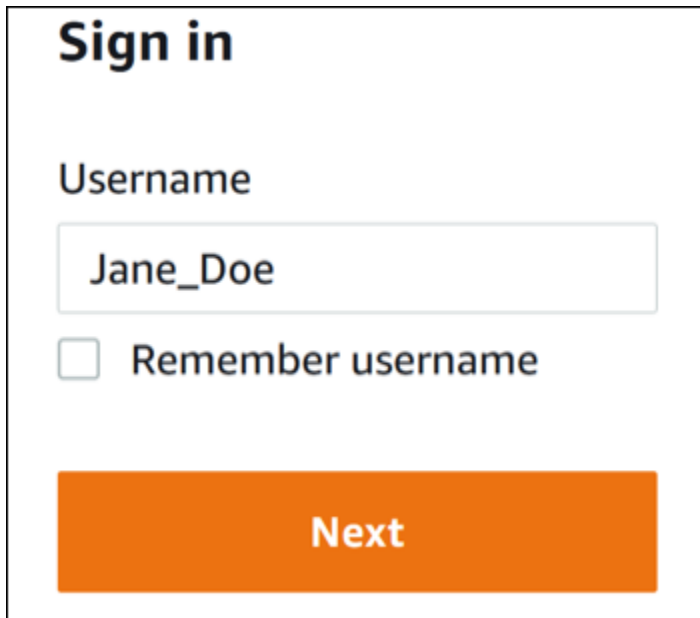
- AWS 访问门户 — 如果管理员为其设置了 AWS IAM Identity Center (AWS 单点登录的继任者) 身份源 AWS，则您必须在组织的 AWS 访问门户上使用您的用户名和密码登录。如需查找门户的 URL，请检查您的电子邮件、安全密码存储、浏览器收藏夹或浏览器历史记录中包含 `awsapps.com/start` 或 `signin.aws/platform/login` 的 URL。例如，您的自定义 URL 可能包含 ID 或域名，例如 `https://d-1234567890.awsapps.com/start`。如果您找不到门户链接，请联系您的管理员。AWS Support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



Sign in

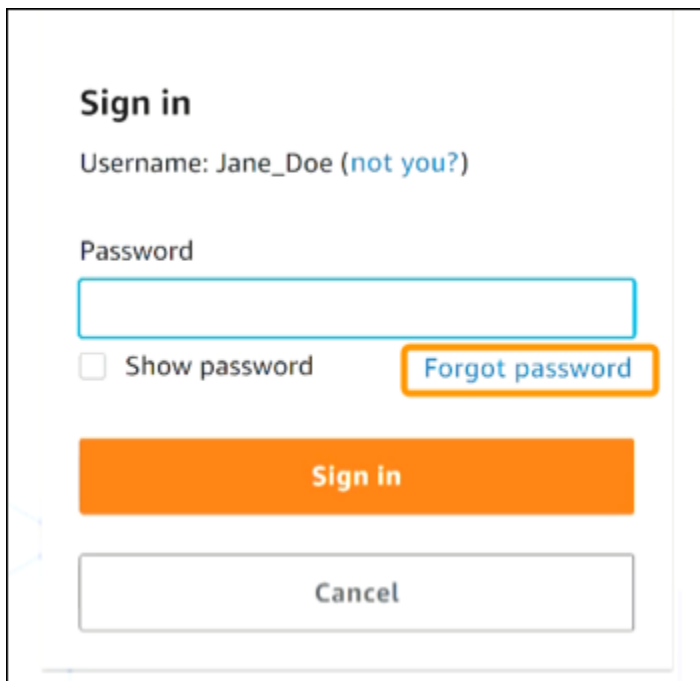
Username

Jane_Doe

Remember username

Next

2. 选择忘记密码，如下图所示。



Sign in

Username: Jane_Doe (not you?)

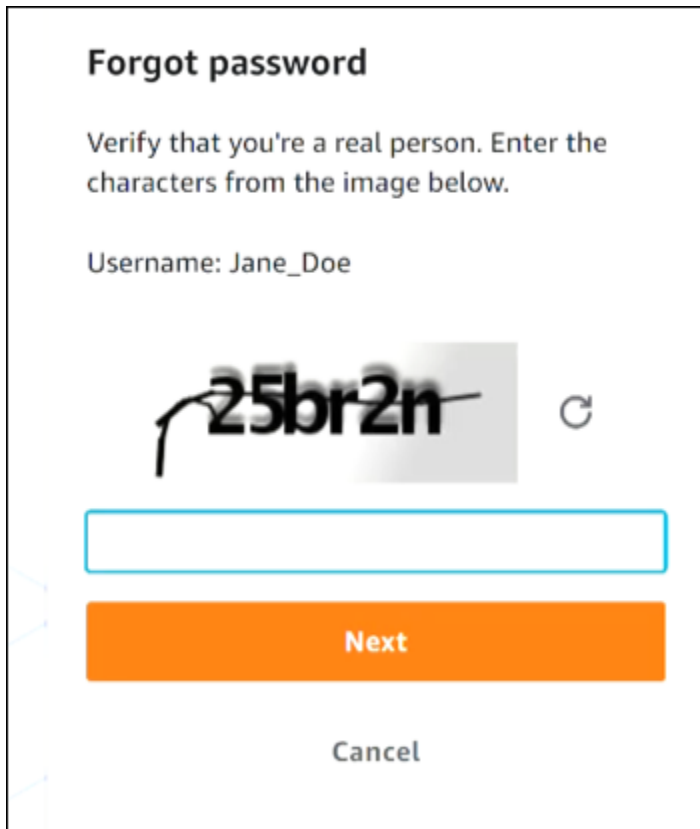
Password

Show password [Forgot password](#)

Sign in

Cancel

3. 完成密码恢复步骤。



Forgot password

Verify that you're a real person. Enter the characters from the image below.

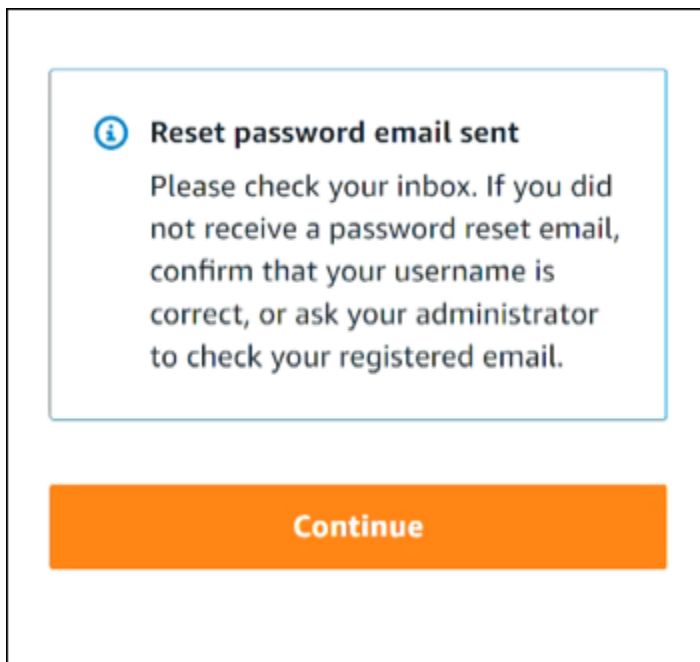
Username: Jane_Doe

25br2n

Next

Cancel

- 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。



Reset password email sent

Please check your inbox. If you did not receive a password reset email, confirm that your username is correct, or ask your administrator to check your registered email.

Continue

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“不是你，是我们”

此错误表示您的 IAM Identity Center 实例或其用作身份源的外部身份提供商 (IdP) 的实例存在设置问题。我们建议您验证以下内容：

- 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商提供的证书相同。您可以通过导航到“设置”，从[IAM 身份中心控制台](#)查看证书。在“身份源”选项卡的“操作”下，选择“管理身份验证”。您可能需要导入新证书。
- 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

使用此处的信息来帮助您解决可能遇到的问题 AWS 构建者 ID。

主题

- [我的电子邮件地址已在使用中](#)
- [我无法完成电子邮件验证](#)
- [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](#)
- [我忘记密码了](#)
- [我无法设置新密码](#)
- [我的密码不起作用](#)
- [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](#)
- [我无法启用 MFA](#)
- [我无法将身份验证器应用程序添加为 MFA 设备](#)
- [我无法删除 MFA 设备](#)
- [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](#)
- [注销未能将我立即完全注销](#)
- [我有问题需要解决](#)

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. 检查您的群发邮件文件夹、垃圾邮件文件夹和已删除电子邮件文件夹。

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

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](#)。

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，但在使用 AWS Builder ID 登录时密码不起作用，请确保要求：

- 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，但仍然无法使用，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端之间的时间同步。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。

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。

- 最新主要文档更新：2024 年 2 月 27 日

变更	说明	日期
更新的疑难解答主题	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。