管理指南

# Amazon WorkSpaces 安全浏览器

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

# Amazon WorkSpaces 安全浏览器: 管理指南

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

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

# Table of Contents


什么是 Amazon WorkSpaces 安全浏览器？ ..... 1
- 发行历史记录 ..... 1
- 需知信息 ..... 2
- 相关服务 ..... 3
- 架构 ..... 4
- 访问 ..... 4

设置 ..... 6
- 注册并创建用户 ..... 6
  - 注册获取 AWS 账户 ..... 6
  - 创建具有管理访问权限的用户 ..... 6
- 授权以编程方式访问 ..... 8
- 网络连接 ..... 9
  - VPC 设置 ..... 9
  - 用户连接 ..... 23

入门 ..... 26
- Web 门户创建 ..... 26
  - 网络设置 ..... 27
  - 门户设置 ..... 27
  - 用户设置 ..... 29
  - 身份提供者配置 ..... 30
  - 启动 ..... 39
- Web 门户测试 ..... 39
- Web 门户分发 ..... 40

管理您的 Web 门户 ..... 41
- 查看 Web 门户详细信息 ..... 41
- 编辑 Web 门户 ..... 42
- 删除 Web 门户 ..... 42
- 管理服务配额 ..... 42
  - 请求增加服务配额 ..... 43
  - 请求增加门户 ..... 44
  - 请求增加最大并发会话数 ..... 44
  - 限额示例 ..... 45
  - 其他服务配额 ..... 45
- 重新验证 SAML IdP 令牌 ..... 46

设置用户访问日志记录 ..... 46
日志示例 ..... 48
管理浏览器策略 ..... 49
教程：设置自定义浏览器策略 ..... 50
编辑基准浏览器策略 ..... 55
配置输入法编辑器 ..... 56
配置会话内本地化 ..... 58
支持的语言代码 ..... 58
用户浏览器设置 ..... 60
管理 IP 访问控制 ..... 61
创建 IP 访问控制组 ..... 61
关联 IP 访问设置 ..... 62
编辑 IP 访问控制组 ..... 62
删除 IP 访问控制组 ..... 63
管理单点登录扩展 ..... 63
确定单点登录扩展的域 ..... 64
将单点登录扩展添加到新的 Web 门户 ..... 64
将单点登录扩展添加到现有 Web 门户 ..... 65
编辑或删除单点登录扩展 ..... 65
设置 URL 筛选 ..... 65
使用控制台设置 URL 筛选 ..... 66
使用 JSON 编辑器或文件上传设置 URL 筛选 ..... 66
深层链接 ..... 67
设置深层链接 ..... 67
为深层链接使用 URL 筛选 ..... 68
会话管理控制面板 ..... 68
控制面板访问 ..... 68
控制面板筛选器 ..... 68
终止会话 ..... 69
会话历史记录 ..... 69
保护传输中数据 ..... 69
数据保护设置 ..... 70
内联数据修改 ..... 70
默认密文配置 ..... 72
基本行内修改 ..... 73
自定义内联密文 ..... 75

创建数据保护设置 ..... 75
关联数据保护设置 ..... 76
编辑数据保护设置 ..... 77
删除数据保护设置 ..... 77
工具栏控件 ..... 78
安全性 ..... 79
数据保护 ..... 79
数据加密 ..... 80
互联网络流量隐私 ..... 89
用户访问日志记录 ..... 89
身份和访问管理 ..... 89
受众 ..... 90
使用身份进行身份验证 ..... 90
使用策略管理访问 ..... 93
Amazon WorkSpaces 安全浏览器如何与 IAM 配合使用 ..... 95
基于身份的策略示例 ..... 101
AWS 托管策略 ..... 103
故障排除 ..... 112
使用服务相关角色 ..... 114
事件响应 ..... 117
合规性验证 ..... 117
恢复能力 ..... 118
基础结构安全性 ..... 119
配置和漏洞分析 ..... 119
接口 VPC 终端节点 (AWS PrivateLink) ..... 120
Amazon WorkSpaces 安全浏览器的注意事项 ..... 120
为 Amazon WorkSpaces 安全浏览器创建接口 VPC 终端节点 ..... 120
为您的接口 VPC 终端节点创建终端节点策略 ..... 121
故障排除 ..... 121
安全最佳实践 ..... 122
监控 ..... 123
使用监控 CloudWatch ..... 123
CloudTrail 日志 ..... 125
中的信息 CloudTrail ..... 125
日志文件条目 ..... 126
用户访问日志记录 ..... 128

用户指南 ..... 129
浏览器和设备兼容性 ..... 129
Web 门户访问 ..... 129
会话指南 ..... 130
启动会话 ..... 130
使用工具栏 ..... 131
使用浏览器 ..... 133
结束会话 ..... 133
排查用户问题 ..... 133
单点登录扩展 ..... 135
单点登录扩展兼容性 ..... 135
安装单点登录扩展 ..... 135
排查单点登录扩展问题 ..... 136
文档历史记录 ..... 137
..... cxli

# 什么是 Amazon WorkSpaces 安全浏览器？

> **Note**
>
> 亚马逊 WorkSpaces 安全浏览器以前被称为 Amazon WorkSpaces Web。

Amazon S WorkSpaces ecure Browser 是一项完全托管的云原生托管浏览器服务，用于安全访问私有网站和 software-as-a-service (SaaS) Web 应用程序、与在线资源交互以及使用一次性容器浏览互联网。 WorkSpaces Secure Browser 可与用户现有的 Web 浏览器配合使用，而不会给 IT 部门带来管理设备、基础架构、专用客户端软件或虚拟专用网络 (VPN) 连接的负担。Web 内容流式传输到用户的 Web 浏览器，而实际的浏览器和 Web 内容则相互隔离 AWS。通过使用与 Amazon WorkSpaces 和 Amazon AppStream 2.0 等 AWS 最终用户计算服务相同的底层技术， WorkSpaces 安全浏览器可以比传统虚拟桌面更具成本效益，并且与为公司自有设备提供管理软件相比，可以降低复杂性。 WorkSpaces 安全浏览器通过流式传输网络内容来降低数据泄露的风险。不会将 HTML、文档对象模型（DOM）或敏感的公司数据传输到本地计算机。通过将设备、企业网络和 Internet 相互隔离，几乎消除了浏览器受攻击面。

您可以对所有会话强制执行企业浏览器策略（包括 URL 允许/阻止），并对剪贴板、文件传输功能和打印机进行会话级控制。您还可以使用 IP 访问控制来限制对可信网络或设备的访问。 WorkSpaces 安全浏览器易于设置和操作。每次会话都会使用全新且经过全面修补的 Chrome 浏览器版本启动，并应用公司策略和设置。

## Amazon WorkSpaces 安全浏览器的发布历史记录

2024 年 5 月 20 日，亚马逊 WorkSpaces 网络更名为亚马逊 WorkSpaces 安全浏览器。对于现有客户，使用该服务管理用户或资源的方式没有发生变化。以下列表描述了因此次重命名而发生的适用更新。

为了向后兼容，workspaces-web API 命名空间保持不变。因此，以下资源仍然相同：

- CLI 命令。
- 亚马逊 CloudWatch 指标。有关更多信息，请参阅 the section called “使用监控 CloudWatch”。
- 服务端点。有关更多信息，请参阅 Amazon WorkSpaces 安全浏览器终端节点和配额。
- AWS CloudFormation 资源。有关更多信息，请参阅 Amazon WorkSpaces 安全浏览器资源类型参考。

- 包含 workspaces-web 的服务相关角色。有关更多信息，请参阅 the section called “使用服务相关角色”。
- URLs 包含工作区-Web 的控制台。
- URLs 包含工作区-Web 的文档。有关更多信息，请参阅 Amazon WorkSpaces 安全浏览器文档。
- 现有 ReadOnly 托管角色。有关更多信息，请参阅 the section called “AWS 托管策略”。
- KMS 授权名称。
- UAL（用户活动日志记录）Kinesis 流前缀。

此外，现有门户 URLs 保持不变。 URLs 对于在 2024 年 5 月 20 日之前创建的门户，使用 <UUID>.workspaces-web.com 的格式。 WorkSpaces 安全浏览器门户继续使用这种格式和 workspaces-web.com 域。

# 使用 Amazon WorkSpaces 安全浏览器时需要知道的条款

为了帮助您开始使用 WorkSpaces 安全浏览器，您应该熟悉以下概念。

身份提供者（IdP）

身份提供者会验证您的用户的凭证。然后，它发出身份验证断言以提供对服务提供商的访问权限。您可以将现有 IdP 配置为使用 WorkSpaces 安全浏览器。

配置身份提供者 (IdP) 的过程因 IdP 而异。

您必须将服务提供者元数据文件上传到您的 IdP。否则，用户将无法登录。您还必须向您的用户授予在您的 IdP 中使用 WorkSpaces 安全浏览器的访问权限。

身份提供者 (IdP) 元数据文档

WorkSpaces 安全浏览器需要您的身份提供商 (IdP) 提供的特定元数据才能建立信任。您可以上传从 IdP 下载的元数据交换文件，将此元数据添加到 WorkSpaces 安全浏览器。

服务提供者（SP）

服务提供者接受身份验证断言并向用户提供服务。 WorkSpaces 安全浏览器充当已通过 IdP 身份验证的用户的服务提供商。

服务提供者（SP）元数据文档

您将需要将服务提供者元数据详细信息添加到您身份提供者 (IdP) 的配置界面中。此配置过程的详细信息因提供者而异。

SAML 2.0

用于在 IdP 和服务提供者之间交换身份验证和授权数据的标准。

Virtual Private Cloud (VPC)

您可以使用现有或新的 VPC、相应的子网和安全组将您的内容与 WorkSpaces 安全浏览器链接。

子网必须具有稳定的 Internet 连接，并且 VPC 和子网还必须与任何内部网站和软件即服务（SaaS）网站保持稳定连接，以便用户能够访问这些资源。

列出的子网和安全组来自与您的 WorkSpaces 安全浏览器控制台相同的区域。 VPCs

Trust store (信任存储)

如果通过 WorkSpaces 安全浏览器访问网站的用户收到隐私错误，例如 NET::ERR_CERT_INVALID，则该网站可能正在使用由私有证书颁发机构 (PCA) 签名的证书。您可能需要在信任商店 PCAs 中添加或更改。此外，如果用户的设备要求您安装特定证书才能加载网站，则需要将该证书添加到您的信任存储中，以允许您的用户在 WorkSpaces 安全浏览器中访问该网站。

可公开访问的网站通常不需要对信任存储进行任何更改。

Web 门户

Web 门户为您的用户提供通过浏览器访问内部网站和 SaaS 网站的权限。您可以在任何支持的区域为每个账户创建一个 Web 门户。要请求提高多个门户的限额，请联系支持人员。

Web 门户端点

Web 门户端点是您的用户在使用为门户配置的身份提供者登录后启动您 Web 门户的接入点。

该端点在 Internet 上公开提供，可以嵌入到您的网络中。

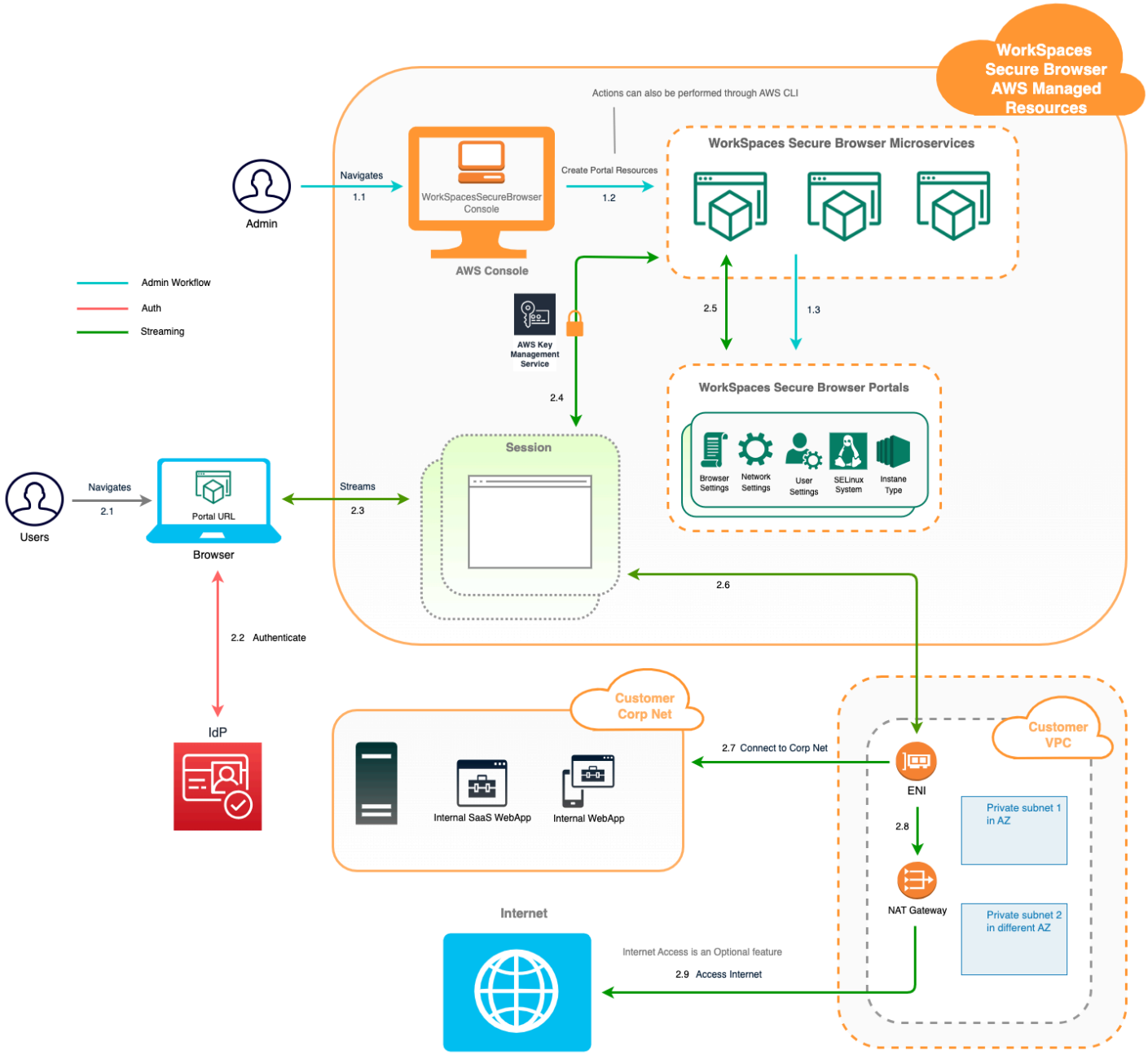
# AWS 与 Amazon WorkSpaces 安全浏览器相关的服务

有几项 AWS 服务与 WorkSpaces 安全浏览器有关。

WorkSpaces 安全浏览器是 Amazon WorkSpaces 在 AWS 最终用户计算产品组合中推出的一项功能。与 WorkSpaces 和 AppStream 2.0 相比， WorkSpaces 安全浏览器专为便于处理基于 Web 的安全工作负载而构建。 WorkSpaces Secure Browser 由自动管理，容量、扩展和图像均由 AWS 按需配置和更新。例如，您可以选择为需要访问桌面资源的软件开发人员提供永久性 Workspace Desktop，为只需要在台式计算机上访问少数内部网站和 SaaS 网站（包括托管在网络之外的网站）的联络中心用户提供 WorkSpaces 安全浏览器。

# Amazon WorkSpaces 安全浏览器的架构

下图显示了 WorkSpaces 安全浏览器的架构。




# 访问 Amazon WorkSpaces 安全浏览器

您可以通过多种方式访问 WorkSpaces 安全浏览器。

管理员通过 WorkSpaces WorkSpaces 安全浏览器控制台、SDK、CLI 或 API 访问安全浏览器。您的用户通过 WorkSpaces 安全浏览器端点访问它。

# 设置 Amazon WorkSpaces 安全浏览器

在配置 WorkSpaces 安全浏览器以访问内部网站和 SaaS 应用程序之前，必须满足以下先决条件。

主题


- 注册并创建用户
- 授权以编程方式访问
- 适用于 Amazon WorkSpaces 安全浏览器的联网


## 注册并创建用户

### 注册获取 AWS 账户

如果您没有 AWS 账户，请完成以下步骤来创建一个。

报名参加 AWS 账户

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

   注册过程的一部分涉及接听电话或短信，并在电话键盘上输入验证码。

   当您注册时 AWS 账户，就会创建AWS 账户根用户一个。根用户有权访问该账户中的所有 AWS 服务 和资源。作为最佳安全实践，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

注册后，请保护您的安全 AWS 账户 AWS 账户根用户 AWS IAM Identity Center，启用并创建管理用户，这样您就不会使用 root 用户执行日常任务。

保护你的 AWS 账户根用户

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

   要获取使用根用户登录方面的帮助，请参阅《AWS 登录 用户指南》中的 Signing in as the root user。

2. 为您的根用户启用多重身份验证（MFA）。

   有关说明，请参阅 I A M 用户指南中的为 AWS 账户 根用户启用虚拟 MFA 设备（控制台）。

创建具有管理访问权限的用户

1. 启用 IAM Identity Center。

   有关说明，请参阅《AWS IAM Identity Center 用户指南》中的 Enabling AWS IAM Identity Center。

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

   有关使用 IAM Identity Center 目录 作为身份源的教程，请参阅《用户指南》 IAM Identity Center 目录中的使用默认设置配置AWS IAM Identity Center 用户访问权限。

以具有管理访问权限的用户身份登录

- 要使用您的 IAM Identity Center 用户身份登录，请使用您在创建 IAM Identity Center 用户时发送到您的电子邮件地址的登录网址。

  有关使用 IAM Identity Center 用户登录的帮助，请参阅AWS 登录 用户指南中的登录 AWS 访问门户。

将访问权限分配给其他用户

1. 在 IAM Identity Center 中，创建一个权限集，该权限集遵循应用最低权限的最佳做法。

   有关说明，请参阅《AWS IAM Identity Center 用户指南》中的 Create a permission set。

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《AWS IAM Identity Center 用户指南》中的 Add groups。

# 授权以编程方式访问

如果用户想在 AWS 外部进行交互，则需要编程访问权限 AWS Management Console。授予编程访问权限的方式取决于正在访问的用户类型 AWS。

要向用户授予编程式访问权限，请选择以下选项之一。

| 哪个用户需要编程式访问权限？ | 目的 | 方式 |
| --- | --- | --- |
| 人力身份<br><br>（在 IAM Identity Center 中管理的用户） | 使用临时证书签署向 AWS CLI AWS SDKs、或发出的编程请求 AWS APIs。 | 按照您希望使用的界面的说明进行操作。<br><br>• 有关的 AWS CLI，请参阅《AWS Command Line Interface 用户指南》 AWS IAM Identity Center中的配置 AWS CLI 以使用。<br>• 有关工具和 AWS SDKs AWS APIs，请参阅《工具参考指南》中的 IAM 身份中心身份验证AWSSDKs 和工具参考指南。 |
| IAM | 使用临时证书签署向 AWS CLI AWS SDKs、或发出的编程请求 AWS APIs。 | 按照 IAM 用户指南中的将临时证书与 AWS 资源配合使用中的说明进行操作。 |
| IAM | （不推荐使用）<br>使用长期凭证签署向 AWS CLI AWS SDKs、或发出的编程请求 AWS APIs。 | 按照您希望使用的界面的说明进行操作。<br><br>• 有关信息 AWS CLI，请参阅用户指南中的使用 IAM 用户证书进行身份验证。AWS Command Line Interface<br>• 有关 AWS SDKs 和工具，请参阅《工具参考指南》AWS SDKs 和《工具参考指南》 |

| 哪个用户需要编程式访问权限？ | 目的 | 方式 |
| --- | --- | --- |
| | | 中的使用长期凭证进行身份验证。<br>• 有关信息 AWS APIs，请参阅 IAM 用户指南中的管理 IAM 用户的访问密钥。 |

# 适用于 Amazon WorkSpaces 安全浏览器的联网

以下主题说明了如何设置 WorkSpaces 安全浏览器流媒体实例，以便用户可以连接到这些实例。它还说明了如何使您的 WorkSpaces 安全浏览器流式传输实例能够访问 VPC 资源和互联网。

主题


- 为 Amazon WorkSpaces 安全浏览器设置 VPC
- 为 Amazon WorkSpaces 安全浏览器启用用户连接


## 为 Amazon WorkSpaces 安全浏览器设置 VPC

要为 WorkSpaces 安全浏览器设置和配置 VPC，请完成以下步骤。

主题


- Amazon WorkSpaces 安全浏览器的 VPC 要求
- 为 Amazon WorkSpaces 安全浏览器创建新 VPC
- 为 Amazon WorkSpaces 安全浏览器启用互联网浏览
- WorkSpaces 安全浏览器的 VPC 最佳实践
- Amazon WorkSpaces 安全浏览器支持的可用区域


### Amazon WorkSpaces 安全浏览器的 VPC 要求

在创建 WorkSpaces 安全浏览器门户期间，您将在账户中选择一个 VPC。至少选择两个位于两个不同可用区的子网。这些 VPCs 和子网必须满足以下要求：

- VPC 必须具有默认租约。 VPCs 不支持使用专用租赁。

- 出于可用性考虑，我们需要至少两个在两个不同可用区中创建的子网。您的子网必须有足够的 IP 地址才能支持预期 WorkSpaces 的安全浏览器流量。使用允许足够客户端 IP 地址数的子网掩码配置您的各个子网，以容纳预期的最大并发用户数。有关更多信息，请参阅 为 Amazon WorkSpaces 安全浏览器创建新 VPC。
- 所有子网都必须与用户使用 WorkSpaces 安全浏览器访问的任何内部内容（无论位于内部内容 AWS Cloud 还是内部内容）保持稳定的连接。

出于可用性和扩展方面的考虑，我们建议您选择位于不同可用区中的三个子网。有关更多信息，请参阅为 Amazon WorkSpaces 安全浏览器创建新 VPC。

WorkSpaces Secure Browser 不会为流媒体实例分配任何公有 IP 地址来实现互联网访问。这将使您的流实例可以通过 Internet 进行访问。因此，任何连接到您公有子网的流实例都无法访问 Internet。如果您想让您的 WorkSpaces 安全浏览器门户同时访问公共 Internet 内容和私有 VPC 内容，请完成中的步骤为 Amazon WorkSpaces 安全浏览器启用不受限制的互联网浏览（推荐）。

## 为 Amazon WorkSpaces 安全浏览器创建新 VPC

本节介绍如何使用 VPC 向导创建具有一个公有子网和一个私有子网的 VPC。作为此过程的一部分，向导将创建 Internet 网关和 NAT 网关。还会创建一个与公有子网关联的自定义路由表。然后，会更新与私有子网关联的主路由表。NAT 网关是在您 VPC 的公有子网中自动创建的。

使用向导创建 VPC 配置后，您将添加第二个私有子网。有关此配置的更多信息，请参阅带有公有子网和私有子网（NAT）的 VPC。

主题


- 分配弹性 IP 地址
- 创建新的 VPC
- 添加第二个私有子网
- 验证并命名子网路由表


### 分配弹性 IP 地址

在创建 VPC 之前，您必须在 WorkSpaces 安全浏览器区域中分配弹性 IP 地址。分配后，您就可以将该弹性 IP 地址与 NAT 网关进行关联。借助弹性 IP 地址，您可以迅速将地址重新映射到 VPC 中的另一个流实例，从而屏蔽流实例故障。有关更多信息，请参阅弹性 IP 地址。

> **Note**
>
> 使用弹性 IP 地址可能会产生费用。有关更多信息，请参阅弹性 IP 地址定价页面。

如果您还没有弹性 IP 地址，请完成以下步骤。如果需要使用现有的弹性 IP 地址，请首先确保它当前不与其他实例或网络接口关联。

分配弹性 IP 地址

1. 打开 Amazon EC2 控制台，网址为https://console.aws.amazon.com/ec2/。
2. 在导航窗格中的 “网络与安全” 下，选择 Elastic IPs。
3. 选择 Allocate New Address (分配新地址)，然后选择 Allocate (分配)。
4. 记下控制台上显示的弹性 IP 地址。
5. 在弹性 IPs窗格的右上角，单击 × 图标关闭窗格。

创建新的 VPC

完成以下步骤，创建具有一个公有子网和一个私有子网的新 VPC。

创建新的 VPC

1. 打开位于 https://console.aws.amazon.com/vpc/ 的 Amazon VPC 控制台。
2. 在导航窗格中，选择 VPC Dashboard (VPC 控制面板)。
3. 选择 Launch VPC Wizard (启动 VPC 向导)。
4. 在 Step 1: Select a VPC Configuration (步骤 1：选择 VPC 配置) 中，选择 VPC with Public and Private Subnets (带有公有子网和私有子网的 VPC)，然后选择 Select (选择)。
5. 在 Step 2: VPC with Public and Private Subnets (步骤 2：具有公有子网和私有子网的 VPC) 中，如下所示配置 VPC：
   - 对于 IPv4 CIDR 块，请为 VPC 指定一个 IPv4 CIDR 块。
   - 对于 IPv6 CIDR 块，请保留默认值 “无 IPv6 CIDR 块”。
   - 在 VPC 名称中，输入 VPC 的唯一名称。
   - 按照如下所示配置公有子网：
     - 对于公有子网的 IPv4 CIDR，请为该子网指定 CIDR 块。
     - 对于 Availability Zone (可用区)，保留默认值 No Preference (无首选项)。

  - 在公有子网名称中，输入子网的名称。例如 **`WorkSpaces Secure Browser Public Subnet`**。
- 按照如下所示配置第一个私有子网：
  - 对于私有子网的 IPv4 CIDR，请为该子网指定 CIDR 块。记下您指定的值。
  - 对于 Availability Zone (可用区)，选择特定区并记下您的选择。
  - 在私有子网名称中，输入子网的名称。例如 **`WorkSpaces Secure Browser Private Subnet1`**。
- 对于其余字段，在适用时保留默认值。
- 在弹性 IP 分配 ID 中，输入与您创建的弹性 IP 地址相对应的值。此地址之后会分配给 NAT 网关。如果您没有弹性 IP 地址，请使用位于的 Amazon VPC 控制台创建一个弹性 IP 地址https://console.aws.amazon.com/vpc/。
- 对于服务端点，如果您的环境需要 Amazon S3 端点，请指定一个。

  要指定 Amazon S3 端点，请执行以下操作：

  1. 选择 Add Endpoint (添加端点)。
  2. 对于服务，请选择 com.amazonaws。 ***`Region`***.s3 条目， AWS 区域 你在*`Region`*哪里创建 VPC。
  3. 对于 Subnet (子网)，选择 Private subnet (私有子网)。
  4. 对于 Policy (策略)，保留默认值 Full Access (完全访问)。
- 对于 Enable DNS hostnames (启用 DNS 主机名)，保留默认值 Yes (是)。
- 对于 Hardware tenancy (硬件租赁)，保留默认值 Default (默认值)。
- 选择创建 VPC。
- 设置您的 VPC 可能需要几分钟。创建了 VPC 后，选择 OK。

## 添加第二个私有子网

在上一步中，您创建了具有一个公有子网和一个私有子网的 VPC。完成以下步骤，以向您的 VPC 中添加第二个私有子网。我们建议您在与第一个私有子网不同的可用区中添加第二个私有子网。

### 添加第二个私有子网

1. 在导航窗格中，选择 Subnets(子网)。
2. 选择您在上一步骤中创建的第一个私有子网。在 Description (描述) 选项卡上的子网列表下方，记录此子网的可用区。

3. 在子网窗格的左上角，选择 Create Subnet (创建子网)。
4. 对于名称标签，输入私有子网的名称。例如 **`WorkSpaces Secure Browser Private Subnet2`**。
5. 对于 VPC，选择上一步骤中已创建的 VPC。
6. 对于可用区，请选择一个可用区，而不是您用于第一个私有子网的可用区。选择不同的可用区可提高容错能力，并有助于防止容量不足错误。
7. 对于 IPv4 CIDR 块，请为新子网指定唯一的 CIDR 块范围。例如，如果您的第一个私有子网的 IPv4 CIDR 块范围为**`10.0.1.0/24`**，则可以**`10.0.2.0/24`**为第二个私有子网指定 CIDR 块范围为。
8. 选择创建。
9. 创建子网后，选择 Close (关闭)。

验证并命名子网路由表

在您创建并配置 VPC 后，请完成以下步骤来为路由表指定名称。您需要验证您的路由表中的以下详细信息是否正确：

- 与 NAT 网关所在子网关联的路由表必须包含使 Internet 流量指向 Internet 网关的路由。这可确保您的 NAT 网关可以访问 Internet。
- 与私有子网关联的路由表必须配置为将 Internet 流量指向 NAT 网关。这使您的私有子网中的流实例可以与 Internet 通信。

验证并命名子网路由表

1. 在导航窗格中，选择子网，然后选择您创建的公有子网。例如，WorkSpaces 安全浏览器 2.0 公有子网。
2. 在路由表选项卡上，选择路由表的 ID。例如，rtb-12345678。
3. 选择 路由表。在名称下，选择编辑（铅笔）图标，然后输入表的名称。例如，输入名称 **`workspacesweb-public-routetable`**。然后选中复选标记以保存名称。
4. 选中公有路由表的同时，在路由选项卡上，确认有两个路由：一个用于发送本地流量，另一个路由用于向 VPC 的互联网网关发送所有其他流量。下表对这两种路由进行了说明：

| 目标位置 | 目标 | 描述 |
| --- | --- | --- |
| 公有子网 IPv4 CIDR 块（例如 10.0.0/20） | 本地 | 从资源发往公有子网 IPv4 CIDR 块内 IPv4 地址的所有流量。此流量在 VPC 内本地路由。 |
| 发往所有其他 IPv4 地址的流量（例如 0.0.0.0/0） | 出站（igw-ID） | 发往所有其他 IPv4 地址的流量将路由到 VPC 向导创建的互联网网关（由 IGW-ID 标识）。 |

5. 在导航窗格中，选择 Subnets(子网)。然后，选择您创建的第一个私有子网（例如 **WorkSpaces Secure Browser Private Subnet1**）。
6. 在路由表选项卡上，选择路由表的 ID。
7. 选择 路由表。在名称下，选择编辑（铅笔）图标，然后输入表的名称。例如，输入名称 **workspacesweb-private-routetable**。然后选中复选标记以保存名称。
8. 在 Routes (路由) 选项卡上，验证路由表包含以下路由：

| 目标位置 | 目标 | 描述 |
| --- | --- | --- |
| 公有子网 IPv4 CIDR 块（例如 10.0.0/20） | 本地 | 从资源发往公有子网 IPv4 CIDR 块内 IPv4 地址的所有流量都在 VPC 内本地路由。 |
| 发往所有其他 IPv4 地址的流量（例如 0.0.0.0/0） | 出站（nat-ID） | 发往所有其他 IPv4 地址的流量将路由到 NAT 网关（由 NAT-ID 标识）。 |
| 目标是 S3 存储桶的流量（在指定了 S3 端点时适用）[pl-ID (com.amazonaws.region.s3)] | 存储（vpce-ID） | 目标是 S3 存储桶的流量将路由到 S3 端点（由 vpce-ID 标识）。 |

9. 在导航窗格中，选择 Subnets(子网)。然后选择您创建的第二个私有子网（例如 **WorkSpaces Secure Browser Private Subnet2**）。

10. 在路由表选项卡上，验证所选路由表是否为私有路由表（例如，**workspacesweb-private-routetable**）。如果路由表不同，请选择编辑，然后选择私有路由表。

## 为 Amazon WorkSpaces 安全浏览器启用互联网浏览

您可以选择启用不受限制的 Internet 浏览（推荐选项）或受限的 Internet 浏览。

主题


- 为 Amazon WorkSpaces 安全浏览器启用不受限制的互联网浏览（推荐）
- 为 Amazon WorkSpaces 安全浏览器启用受限的互联网浏览
- Amazon WorkSpaces 安全浏览器的互联网连接端口


### 为 Amazon WorkSpaces 安全浏览器启用不受限制的互联网浏览（推荐）

按照以下步骤配置带有 NAT 网关的 VPC，以实现不受限制的 Internet 浏览。这允许 WorkSpaces 安全浏览器访问公共 Internet 上的站点，以及托管在您的 VPC 中或与您的 VPC 连接的私有站点。

#### 配置带有 NAT 网关的 VPC 以实现不受限制的 Internet 浏览

如果您希望您的 WorkSpaces 安全浏览器门户同时访问公共互联网内容和私有 VPC 内容，请按照以下步骤操作：

> **Note**
>
> 如果您已配置 VPC，请完成以下步骤，将 NAT 网关添加到 VPC。如果您需要创建新 VPC，请参阅为 Amazon WorkSpaces 安全浏览器创建新 VPC。

1. 要创建 NAT 网关，请完成创建 NAT 网关中的步骤。确保此 NAT 网关具有公有连接，并且位于您 VPC 的公有子网中。
2. 您必须至少指定两个位于不同可用区的子网。将子网分配给不同的可用区有助于确保实现更好的可用性和容错能力。有关如何创建第二个私有子网的信息，请参阅the section called “第二个私有子网”。

> **Note**
>
> 为确保每个流媒体实例都能访问互联网，请勿将公有子网连接到您的 WorkSpaces 安全浏览器门户。

3. 更新与您的私有子网关联的路由表，以将面向 Internet 的流量指向该 NAT 网关。这使您的私有子网中的流实例可以与 Internet 通信。有关如何将路由表与私有子网关联的信息，请完成配置路由表中的步骤。

为 Amazon WorkSpaces 安全浏览器启用受限的互联网浏览

WorkSpaces 安全浏览器门户的推荐网络设置是使用带有 NAT 网关的私有子网，这样门户就可以浏览公共 Internet 和私有内容。有关更多信息，请参阅 the section called “不受限制的 Internet 浏览”。但是，您可能需要使用 Web 代理来控制从 WorkSpaces 安全浏览器门户到互联网的出站通信。例如，如果您使用 Web 代理作为访问 Internet 的网关，则可以实施预防性安全控制措施，例如域允许列表和内容筛选。这还可以通过在本地缓存经常访问的资源（例如网页或软件更新），来减少带宽使用量并提高网络性能。对于某些使用案例，您可能拥有只能通过使用 Web 代理访问的私有内容。

您可能已经了解如何在托管设备上或虚拟环境的映像上配置代理设置。但是，如果您无法控制设备（例如，当用户使用的设备不是由企业拥有或管理时），或者如果您需要管理虚拟环境的映像，这就会带来挑战。借助 WorkSpaces 安全浏览器，您可以使用 Web 浏览器中内置的 Chrome 政策来设置代理设置。为此，您可以为 WorkSpaces 安全浏览器设置 HTTP 出站代理。

此解决方案基于推荐的出站 VPC 代理设置。代理解决方案基于开源 HTTP 代理 Squid。然后，它使用 WorkSpaces 安全浏览器设置将 WorkSpaces 安全浏览器门户配置为连接到代理端点。有关更多信息，请参阅如何设置具有域白名单和内容筛选功能的出站 VPC 代理。

此解决方案为您提供了以下优势：

- 一种出站代理，包括一组由网络负载均衡器托管的自动缩放 Amazon EC2 实例。代理实例位于公有子网中，每个实例都附有弹性 IP，因此它们可以访问 Internet。
- 部署到私有子网 WorkSpaces 的安全浏览器门户。您无需配置 NAT 网关即可启用 Internet 访问。相反，您需要配置浏览器策略，以便所有 Internet 流量都通过出站代理。如果您想使用自己的代理，则 WorkSpaces 安全浏览器门户设置将与之类似。

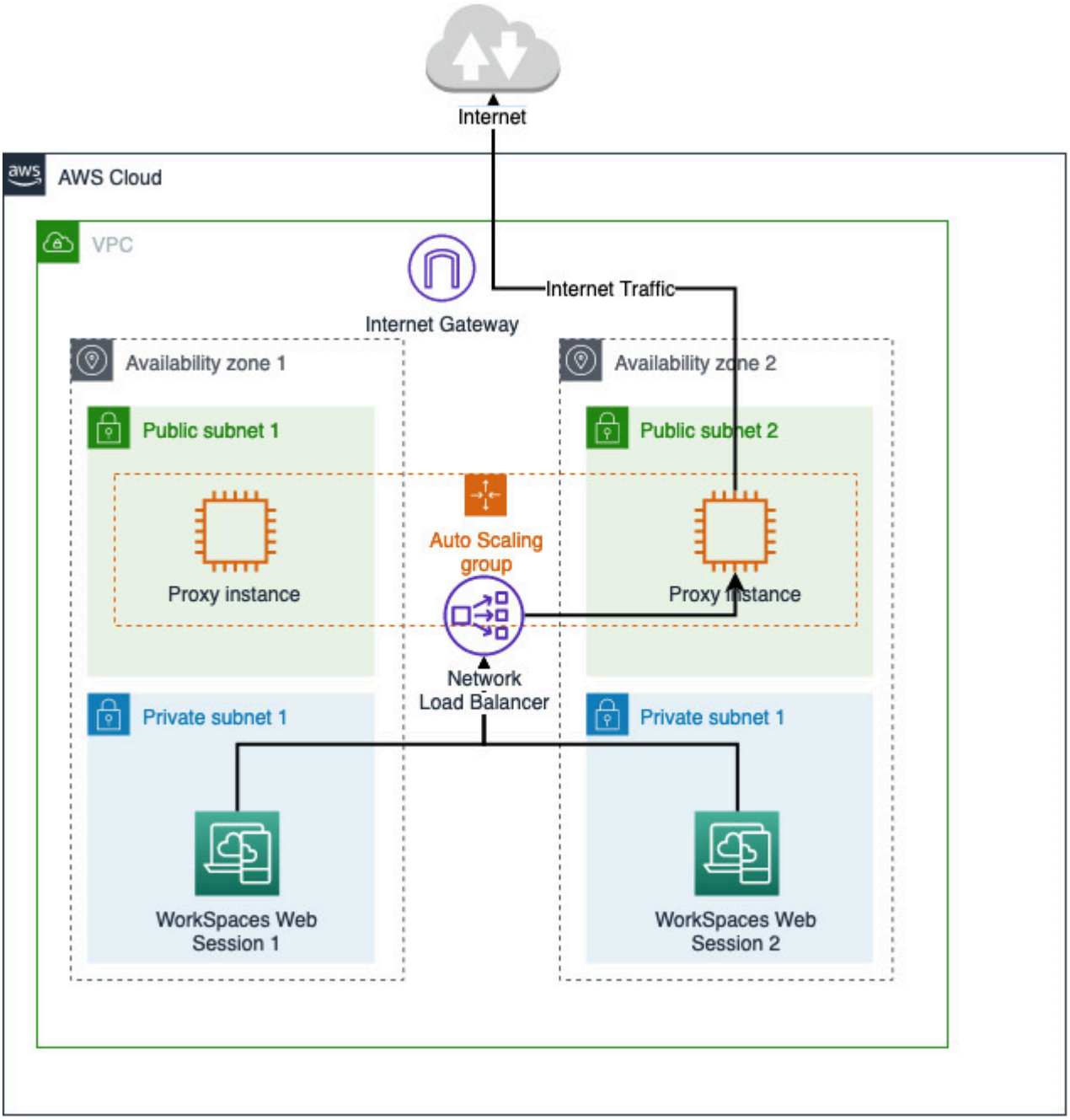
主题

- Amazon WorkSpaces 安全浏览器的互联网浏览架构受限

- Amazon WorkSpaces 安全浏览器的受限互联网浏览先决条件
- 亚马逊 WorkSpaces 安全浏览器的 HTTP 出站代理
- Amazon WorkSpaces 安全浏览器的互联网浏览受限疑难解答

## Amazon WorkSpaces 安全浏览器的互联网浏览架构受限

下面是 VPC 中的典型代理设置示例。Amazon 代理 EC2实例位于公有子网中，并与弹性 IP 关联，因此它们可以访问互联网。网络负载均衡器托管自动扩缩组的代理实例。这样可以确保代理实例可以自动扩展，并且网络负载均衡器是单个代理端点，可供 WorkSpaces 安全浏览器会话使用。




Amazon WorkSpaces 安全浏览器的受限互联网浏览先决条件

在开始之前，请确保您满足以下先决条件：

- 您需要一个已经部署的 VPC，其公有子网和私有子网分布在多个可用区（AZs）。有关如何设置 VPC 环境的更多信息，请参阅默认 VPCs。

- 您需要一个可以从 WorkSpaces 安全浏览器会话所在的私有子网访问的单个代理终端节点（例如，网络负载均衡器 DNS 名称）。如果您想使用现有代理，请确保它还有一个可以从您的私有子网访问的端点。

亚马逊 WorkSpaces 安全浏览器的 HTTP 出站代理

要为 WorkSpaces 安全浏览器设置 HTTP 出站代理，请按照以下步骤操作。

1. 要将出站代理示例部署到您的 VPC，请按照如何设置具有域白名单和内容筛选功能的出站 VPC 代理中的步骤操作。
   a. 按照 “安装（一次性设置）” 中的步骤将 CloudFormation模板部署到您的账户。确保选择正确的 VPC 和子网作为 CloudFormation 模板参数。
   b. 部署后，找到 CloudFormation 输出参数OutboundProxyDomain和OutboundProxyPort。这是您代理的 DNS 名称和端口。
   c. 如果您已经拥有自己的代理，请跳过此步骤，并使用您代理的 DNS 名称和端口。
2. 在 WorkSpaces 安全浏览器的控制台中，选择您的门户，然后选择编辑。
   a. 在网络连接详细信息中，选择有权访问代理的 VPC 和私有子网。
   b. 在策略设置中，使用 JSON 编辑器添加以下 ProxySettings策略。`ProxyServer` 字段应为您代理的 DNS 名称和端口。有关 ProxySettings 策略的更多详细信息，请参阅ProxySettings。

```
{
    "chromePolicies":
    {
        ...
        "ProxySettings": {
            "value": {
                "ProxyMode": "fixed_servers",
                "ProxyServer": "OutboundProxyLoadBalancer-0a01409a46943c47.elb.us-
west-2.amazonaws.com:3128",
                "ProxyBypassList": "https://www.example1.com,https://
www.example2.com,https://internalsite/"
            }
        },
    }
}
```

3. 在您的 WorkSpaces 安全浏览器会话中，您将看到代理已应用于 Chrome 设置 Chrome 使用管理员提供的代理设置。

4. 访问 chrome://policy 和 Chrome 策略选项卡，确认该策略已应用。
5. 验证您的 WorkSpaces 安全浏览器会话是否可以在没有 NAT 网关的情况下成功浏览互联网内容。在 CloudWatch 日志中，验证是否记录了 Squid 代理访问日志。

### Amazon WorkSpaces 安全浏览器的互联网浏览受限疑难解答

应用 Chrome 政策后，如果您的 WorkSpaces 安全浏览器会话仍然无法访问互联网，请按照以下步骤尝试解决您的问题：

- 验证是否可以从 WorkSpaces 安全浏览器门户所在的私有子网访问代理终端节点。为此，请在私有子网中创建一个 EC2 实例，然后测试私有 EC2 实例与代理终端节点的连接。
- 验证代理是否可以访问 Internet。
- 验证 Chrome 策略是否正确。
  - 确认策略 `ProxyServer` 字段的以下格式：`<Proxy DNS name>:<Proxy port>`。前缀中不应包含 `http://` 或 `https://`。
  - 在 WorkSpaces 安全浏览器会话中，使用 Chrome 导航至 chrome: //政策，并确保该 ProxySettings 政策已成功应用。

### Amazon WorkSpaces 安全浏览器的互联网连接端口

每个 WorkSpaces Secure Browser 流式传输实例都有一个客户网络接口，该接口可提供与您的 VPC 内资源的连接，如果设置了带有 NAT 网关的私有子网，则还可连接到 Internet。

要连接 Internet，以下端口必须针对所有目标打开。如果您在使用经过修改的安全组或自定义安全组，需要手动添加必需的规则。有关更多信息，请参阅安全组规则。

> **Note**
>
> 这适用于出口流量。

- TCP 80 (HTTP)
- TCP 443 (HTTPS)
- UDP 8433

## WorkSpaces 安全浏览器的 VPC 最佳实践

以下建议可帮助您更安全有效地配置 VPC。

### VPC 整体配置

- 确保您的 VPC 配置可以支持扩展需求。
- 确保您的 WorkSpaces 安全浏览器服务配额（也称为限制）足以满足您的预期需求。要申请增加配额，你可以使用 Service Quotas 控制台，网址为https://console.aws.amazon.com/servicequotas/。有关默认 WorkSpaces 安全浏览器配额的信息，请参阅the section called “管理服务配额”。
- 如果您计划为流会话提供 Internet 访问权限，建议您在公有子网中配置一个带有 NAT 网关的 VPC。

### 弹性网络接口

- 在直播期间，每个 WorkSpaces 安全浏览器会话都需要自己的 elastic network 接口。 WorkSpaces Secure Browser 创建的弹性网络接口 (ENIs) 与队列所需的最大容量一样多。默认情况下， ENIs 每个区域的限制为 5000。有关更多信息，请参阅网络接口。

  在为超大型部署（例如数千个并发流式传输会话）规划容量时，请考虑峰值使用量可能需要的容量数量。 ENIs 建议您将 ENI 限制保持在您为 Web 门户配置的最大并发使用限制或高于该限制。

### 子网

- 在制定扩大用户规模的计划时，请记住，每个 WorkSpaces 安全浏览器会话都需要来自已配置子网的唯一客户端 IP 地址。因此，子网上配置的客户端 IP 地址空间的大小决定了可以同时进行流会话的用户数量。
- 建议使用允许足够客户端 IP 地址数的子网掩码配置各个子网，以容纳预期的最大并发用户数。此外，考虑添加额外的 IP 地址来容纳预期的增长。有关更多信息，请参阅 VPC 和子网大小调整 IPv4。
- 出于可用性和扩展方面的考虑，我们建议您在所需区域中 WorkSpaces 安全浏览器支持的每个唯一可用区中配置一个子网。有关更多信息，请参阅 the section called “创建新的 VPC”。
- 请确保可通过您的子网访问 Web 应用程序所需的网络资源。

### 安全组

- 使用安全组向您的 VPC 提供额外的访问控制。

属于您的 VPC 的安全组允许您控制 WorkSpaces 安全浏览器流式传输实例与 Web 应用程序所需的网络资源之间的网络流量。确保安全组提供了对 Web 应用程序所需网络资源的访问权限。

## Amazon WorkSpaces 安全浏览器支持的可用区域

当您创建用于 WorkSpaces 安全浏览器的虚拟私有云 (VPC) 时，您的 VPC 的子网必须位于您启动 WorkSpaces 安全浏览器的区域中的不同可用区中。可用区是被设计为可以隔离其他可用区的故障的不同位置。通过启动独立可用区内的实例，您可以保护您的应用程序不受单一位置故障的影响。每个子网都必须完全位于一个可用区之内，不能跨越多个可用区。我们建议您为所需区域中每个受支持的可用区配置一个子网，以实现最大的弹性

可用区由区域代码后跟一个字母标识符表示；例如，`us-east-1a`。为确保资源分配到区域的各可用区，我们将可用区独立映射到每个 AWS 账户的名称。例如，您的 `us-east-1a` 账户的可用区 AWS 可能与另一 `us-east-1a` 账户的 AWS 不在同一位置。

要跨账户协调可用区，您必须使用 AZ ID（可用区的唯一、一致的标识符）。例如，`use1-az2`是该`us-east-1`区域的可用区 ID，它在每个 AWS 账户中的位置都相同。

IDs 通过查看可用区，您可以确定一个账户中的资源相对于另一个账户中的资源的位置。例如，如果您在 AZ ID 为 `use1-az2` 的可用区中与另一个账户共享一个子网，则在 AZ ID 也为 `use1-az2` 的可用区中该账户便可使用这一子网。每个 VPC 和子网的 AZ ID 均显示在 Amazon VPC 控制台中。

WorkSpaces 安全浏览器在每个受支持区域的可用区域的子集中可用。下表列 IDs 出了您可以用于每个区域的可用区。要查看您账户中可用区 IDs 与可用区的映射，请参阅AWS RAM 用户指南中的资源可用 IDs 区。

| 区域名称 | 区域代码 | 支持的可用区 IDs |
| --- | --- | --- |
| 美国东部（弗吉尼亚州北部） | `us-east-1` | `use1-az1`, `use1-az2`, `use1-az4`, `use1-az5`, `use1-az6` |
| 美国西部（俄勒冈州） | `us-west-2` | `usw2-az1`, `usw2-az2`, `usw2-az3` |
| 亚太地区（孟买） | `ap-south-1` | `aps1-az1`, `aps1-az3` |
| 亚太地区（新加坡） | `ap-southeast-1` | `apse1-az1` ，`apse1-az2` ，`apse1-az3` |

| 区域名称 | 区域代码 | 支持的可用区 IDs |
| --- | --- | --- |
| 亚太地区（悉尼） | ap-southeast-2 | apse2-az1 ，apse2-az2 ，apse2-az3 |
| 亚太地区（东京） | ap-northeast-1 | apne1-az1 ，apne1-az2 ，apne1-az4 |
| 加拿大（中部） | ca-central-1 | cac1-az1, cac1-az2, cac1-az4 |
| 欧洲地区（法兰克福） | eu-central-1 | euc1-az2, euc1-az2, euc1-az3 |
| 欧洲地区（爱尔兰） | eu-west-1 | euw1-az1, euw1-az2, euw1-az3 |
| 欧洲地区（伦敦） | eu-west-2 | euw2-az1, euw2-az2 |

有关可用区和可用区的更多信息 IDs，请参阅 A mazon EC2 用户指南中的区域、可用区和本地区域。

## 为 Amazon WorkSpaces 安全浏览器启用用户连接

WorkSpaces 安全浏览器配置为通过公共互联网路由流媒体连接。需要互联网连接才能对用户进行身份验证并交付 WorkSpaces 安全浏览器运行所需的网络资产。要允许此流量，您必须允许Amazon WorkSpaces 安全浏览器允许使用的域名中列出的域。

以下主题提供有关如何启用用户与 WorkSpaces 安全浏览器的连接的信息。

主题

- Amazon WorkSpaces 安全浏览器的 IP 地址和端口要求
- Amazon WorkSpaces 安全浏览器允许使用的域名

### Amazon WorkSpaces 安全浏览器的 IP 地址和端口要求

要访问 WorkSpaces 安全浏览器实例，用户设备需要通过以下端口进行出站访问：

- 端口 443 (TCP)

- 端口 443 用于当使用 Internet 端点时用户设备和流实例之间的 HTTPS 通信。通常情况下，如果最终用户在流式传输会话期间浏览 Web，则 Web 浏览器会在较高范围内随机选择一个源端口来用于流式传输流量。您必须确保允许流量返回到该端口。
- 此端口必须向Amazon WorkSpaces 安全浏览器允许使用的域名中列出的所需域开放。
- AWS 以 JSON 格式发布其当前 IP 地址范围，包括会话网关和 CloudFront 域可能解析到的范围。有关如何下载 .json 文件并查看当前范围的信息，请参阅 AWS IP 地址范围。或者，如果您正在使用 AWS Tools for Windows PowerShell，则可以使用Get-AWSPublicIpAddressRange PowerShell命令访问相同的信息。有关更多信息，请参阅查询 AWS的公有 IP 地址范围。

- （可选）端口 53（UDP）
  - 端口 53 用于用户设备和您 DNS 服务器之间的通信。
  - 如果您不使用 DNS 服务器进行域名解析，则此端口是可选的。
  - 此端口必须对您的 DNS 服务器的 IP 地址开放，以便解析公有域名。

## Amazon WorkSpaces 安全浏览器允许使用的域名

为了让用户能够从其本地浏览器访问 Web 门户，您必须将以下域添加到用户尝试从中访问服务的网络上的允许列表中。

在下表中，*{region}*替换为运营门户网站的区域代码。例如，s3。 *{region}*对于欧洲（爱尔兰）地区的门户网站，.amazonaws.com 应为 s3.eu-west-1.amazonaws.com。有关区域代码的列表，请参阅Amazon WorkSpaces 安全浏览器终端节点和配额。

| 类别 | 域或 IP 地址 |
| --- | --- |
| WorkSpaces 安全的浏览器流媒体资产 | s3。 *{region}*.amazonaws.co<br>s3.amazonaws.com<br>appstream2。 *{region}*.aws.amazon.com<br>*.amazonappstream.com<br>*.shortbread.aws.dev |
| WorkSpaces 安全浏览器静态资产 | *.workspaces-web.com<br>di5ry4hb4263e.cloudfront.net |

| 类别 | 域或 IP 地址 |
| --- | --- |
| WorkSpaces 安全浏览器身份验证 | *.auth。*{region}*.amazoncognito.co<br>认知身份。*{region}*.amazonaws.co<br>cognito-idp。*{region}*.amazonaws.co<br>*.cloudfront.net |
| WorkSpaces 安全浏览器指标和报告 | *.execute-api。*{region}*.amazonaws.co<br>unagi-na.amazon.com |

根据您配置的身份提供者，您可能还需要允许列出其他域。查看 IdP 的文档，确定需要允许列出哪些域名才能让 WorkSpaces 安全浏览器使用该提供商。如果您使用的是 IAM Identity Center，请参阅 IAM Identity Center 先决条件以了解更多信息。

# 开始使用 Amazon WorkSpaces 安全浏览器

按照以下步骤创建 WorkSpaces 安全浏览器门户，并允许用户通过现有浏览器访问内部网站和 SaaS 网站。您可以在任何支持的区域为每个账户创建一个 Web 门户。

> **Note**
>
> 要申请提高多个门户的限制，请联系支持人员，并提供您的 AWS 账户 身份证件、要申请的门户数量以及 AWS 区域。

使用 Web 门户创建向导时，此过程通常需要 5 分钟，而门户变为活动状态最多需要 15 分钟。

设置门户网站不收取任何费用。 WorkSpaces Secure Browser 为积极使用该服务的用户提供 pay-as-you-go定价，包括低廉的月度价格。无需预付费用、许可证或长期订阅。

> **Important**
>
> 在开始之前，您必须完成 Web 门户的必要先决条件。有关 Web 门户先决条件的更多信息，请参阅设置 Amazon WorkSpaces 安全浏览器。

主题


- 为 Amazon WorkSpaces 安全浏览器创建门户
- 在 Amazon WorkSpaces 安全浏览器中测试您的门户网站
- 在 Amazon WorkSpaces 安全浏览器中分发您的门户网站


## 为 Amazon WorkSpaces 安全浏览器创建门户

按照以下步骤创建 Web 门户。

主题


- 为 Amazon WorkSpaces 安全浏览器配置网络设置
- 为 Amazon WorkSpaces 安全浏览器配置门户设置
- 为 Amazon WorkSpaces 安全浏览器配置用户设置

- 为 Amazon WorkSpaces 安全浏览器配置您的身份提供商
- 使用 Amazon WorkSpaces 安全浏览器启动门户网站

## 为 Amazon WorkSpaces 安全浏览器配置网络设置

要为 WorkSpaces 安全浏览器配置网络设置，请按照以下步骤操作。

1. 在https://console.aws.amazon.com/workspaces-web/家中打开 WorkSpaces 安全浏览器控制台。
2. 依次选择WorkSpaces 安全浏览器、Web 门户，然后选择创建 Web 门户。
3. 在步骤 1：指定网络连接页面上，完成以下步骤，将您的 VPC 连接到您的 Web 门户并配置您的 VPC 和子网。

   1. 要了解网络详情，请选择与您希望用户通过 WorkSpaces 安全浏览器访问的内容相关的 VPC。
   2. 选择最多 3 个符合以下要求的私有子网。有关更多信息，请参阅 适用于 Amazon WorkSpaces 安全浏览器的联网。
      - 您必须选择最少两个私有子网才能创建门户。
      - 为确保 Web 门户的高可用性，建议您在 VPC 的唯一可用区内提供最大数量的私有子网。
   3. 选择安全组。

## 为 Amazon WorkSpaces 安全浏览器配置门户设置

在步骤 2：配置 Web 门户设置页面上，完成以下步骤，以自定义用户启动会话时的浏览体验。

1. 在 Web 门户详细信息下的显示名称中，输入 Web 门户的可识别名称。
2. 在实例类型下，从下拉菜单中选择 Web 门户的实例类型。然后，输入 Web 门户的最大并发用户限制。有关更多信息，请参阅 the section called “管理服务配额”。

   > **Note**
   >
   > 选择新的实例类型将更改每个月活跃用户的费用。有关更多信息，请参阅 Amazon WorkSpaces 安全浏览器定价。

3. 在用户访问日志记录下的 Kinesis 流 ID 中，选择您要将数据发送到的 Amazon Kinesis 数据流。有关更多信息，请参阅 the section called “设置用户访问日志记录”。
4. 在策略设置 下，完成以下操作：

- 对于策略选项，选择可视化编辑器或 JSON 文件上传。您可以使用任何一种方法来提供 Web 门户的策略配置详细信息。有关更多信息，请参阅 the section called “管理浏览器策略”。
  - WorkSpaces 安全浏览器包括对 Chrome 企业政策的支持。您可以使用可视化编辑器或手动上传策略文件来添加和管理策略。您可以随时在任一选项之间切换。
  - 上传策略文件时，可以在控制台中看到文件中的可用策略。但是，您无法在可视化编辑器中编辑所有策略。控制台在 JSON 文件中的其他 JSON 策略下列出了您无法使用可视化编辑器编辑的策略。要对这些策略进行更改，必须手动对其进行编辑。
- （可选）对于启动 URL - 可选，输入用作用户启动浏览器时显示的主页的域。您的 VPC 必须与此 URL 建立稳定的连接。
- 选择或清除私密浏览和历史记录删除，以便在用户会话期间开启或关闭这些功能

> **Note**
>
> URLs 在私密浏览时或用户删除浏览器历史记录之前访问过的内容无法记录在用户访问日志中。有关更多信息，请参阅 the section called “设置用户访问日志记录”。

- 在 URL 过滤下，您可以配置哪些 URLs 用户可以在会话期间访问。有关更多信息，请参阅 the section called “设置 URL 筛选”。
- （可选）对于浏览器书签 - 可选，为任何书签输入您希望用户在其浏览器中看到的显示名称、域和文件夹。然后，选择添加书签。

> **Note**
>
> 域是浏览器书签的必填字段。
> 在 Chrome 中，用户可以在书签工具栏的管理的书签文件夹中找到管理的书签。

- （可选）为门户添加标签。您可以使用标签来搜索或筛选您的 AWS 资源。标签由密钥和可选值组成，并与您的门户资源相关联。

5. 在 IP 访问控制(可选) 下，选择是否限制对可信网络的访问。有关更多信息，请参阅 the section called “管理 IP 访问控制”。
6. 选择下一步以继续。

# 为 Amazon WorkSpaces 安全浏览器配置用户设置

在步骤 3：选择用户设置页面上，完成以下步骤，以选择您的用户在会话期间可以从顶部导航栏访问哪些功能，然后选择下一步：

1. 在 “权限” 下，选择是否启用单点登录扩展程序。有关更多信息，请参阅 the section called “管理单点登录扩展”。
2. 对于允许用户从其 Web 门户打印到本地设备，选择允许或不允许。
3. 对于允许用户深度链接到其 Web 门户，选择允许或不允许。有关深层链接的更多信息，请参阅 the section called “深层链接”。
4. 在 “工具栏控件” 下，在 “功能” 下选择所需的设置。
5. 在 “设置” 下，管理会话开始时的工具栏演示视图，包括工具栏状态（停靠或分离）、主题（深色或浅色模式）、图标可见性以及会话的最大显示分辨率。将这些设置保持为未配置状态，以允许最终用户完全控制这些选项。有关更多信息，请参阅 the section called “工具栏控件”。
6. 对于会话超时，请指定以下内容：

   - 对于 Disconnect timeout in minutes (断开连接超时 (分钟))，请选择在用户断开连接后流式传输会话保持活动状态的时间。如果在此时间间隔内出现连接断开或网络中断的情况后，用户尝试重新连接到流式传输会话，他们将连接到其上一个会话。否则，他们会建立一个新会话，连接到新的流实例。

     如果用户结束会话，则断开连接超时不适用。系统而是会提示用户保存任何打开的文档，然后立即断开流实例的连接。用户正在使用的实例随即终止。

   - 对于 Idle disconnect timeout in minutes (空闲断开连接超时 (分钟))，请选择用户在与流式传输会话断开连接以及 Disconnect timeout in minutes (断开连接超时 (分钟)) 时间间隔开始之前可以处于空闲（非活动）状态的时间。在由于处于不活动状态而断开连接之前，用户将收到通知。在 Disconnect timeout in minutes (断开连接超时 (分钟)) 中指定的时间间隔过去之前，如果他们尝试重新连接到流式传输会话，则会将他们连接到以前的会话。否则，他们会建立一个新会话，连接到新的流实例。如果将该值设置为 0，则会禁用该值。如果禁用了该值，则不会由于处于不活动状态而断开连接用户。

     > **Note**
     >
     > 如果用户在流式传输会话期间停止提供键盘或鼠标输入，则将其视为处于空闲状态。文件上传和下载、音频输入、音频输出以及像素更改不符合用户活动条件。在 Idle

disconnect timeout in minutes (空闲断开连接超时 (分钟)) 中的时间间隔过去之后，如果用户继续处于空闲状态，则会将他们断开连接。

# 为 Amazon WorkSpaces 安全浏览器配置您的身份提供商

按照以下步骤配置身份提供者（IdP）。

主题

- 为 Amazon WorkSpaces 安全浏览器选择身份提供者类型
- 更改 Amazon WorkSpaces 安全浏览器的身份提供者类型

## 为 Amazon WorkSpaces 安全浏览器选择身份提供者类型

WorkSpaces 安全浏览器提供两种身份验证类型：标准身份验证和AWS IAM Identity Center。在配置身份提供者页面上，选择要对门户使用的身份验证类型。

- 对于标准（默认选项），将您的第三方 SAML 2.0 身份提供者（例如 Okta 或 Ping）直接与您的门户联合。有关更多信息，请参阅 the section called “标准身份验证类型”。标准类型支持 SP 发起的身份验证流和 IdP 发起的身份验证流。
- 对于 IAM Identity Center（高级选项），将 IAM Identity Center 与您的门户联合。要使用此身份验证类型，您的 IAM 身份中心和 WorkSpaces 安全浏览器门户必须位于同一类型 AWS 区域。有关更多信息，请参阅 the section called “IAM Identity Center 身份验证类型”。

主题

- 为 Amazon WorkSpaces 安全浏览器配置标准身份验证类型
- 为 Amazon WorkSpaces 安全浏览器配置 IAM 身份中心身份验证类型

### 为 Amazon WorkSpaces 安全浏览器配置标准身份验证类型

标准 身份验证类型是默认身份验证类型。它可以借助符合 SAML 2.0 标准的 IdP，支持服务提供者发起（SP 发起）的登录流和身份提供者发起（IdP 发起）的登录流。要配置标准身份验证类型，请按照以下步骤操作，将您的第三方 SAML 2.0 IdP（例如 Okta 或 Ping）直接与您的门户联合。

主题

- 在 Amazon WorkSpaces 安全浏览器上配置您的身份提供商

- 在您自己的 IdP 上配置 IdP
- 在亚马逊 WorkSpaces 安全浏览器上完成 IdP 配置
- 特定 IdPs 于 Amazon WorkSpaces 安全浏览器的使用指南

在 Amazon WorkSpaces 安全浏览器上配置您的身份提供商

按照以下步骤配置身份提供者：

1. 在创建向导的配置身份提供者页面上，选择标准。
2. 选择继续使用标准 IdP。
3. 下载 SP 元数据文件，并保持各个元数据值的选项卡处于打开状态。
   - 如果 SP 元数据文件可用，请选择下载元数据文件以下载服务提供者（SP）元数据文档，然后在下一步中将服务提供者元数据文件上传到您的 IdP。否则，用户将无法登录。
   - 如果您的提供者未上传 SP 元数据文件，请手动输入元数据值。
4. 在选择 SAML 登录类型下方，在 SP 发起和 IdP 发起的 SAML 断言之间进行选择，或选择仅限 SP 发起的 SAML 断言。
   - SP 发起和 IdP 发起的 SAML 断言允许您的门户支持这两种类型的登录流。通过支持 IdP 发起的登录流的门户，您可以向服务身份联合验证端点呈现 SAML 断言，而无需用户通过访问门户 URL 启动会话。
     - 选择此选项后，该门户可接受未经请求的 IdP 发起的 SAML 断言。
     - 此选项要求在 SAML 2.0 身份提供者中配置默认中继状态。您门户的中继状态参数位于控制台的 IdP 发起的 SAML 登录下，或者您可以从 `<md:IdPInitRelayState>` 下的 SP 元数据文件中进行复制。
     - 注意
       - 以下为中继状态的格式：`redirect_uri=https%3A%2F%2Fportal-id.workspaces-web.com %2Fsso&response_type=code&client_id=1example23456789&identity_provider=Ex Identity-Provider`。
       - 如果您从 SP 元数据文件中复制并粘贴该值，请确保将 `&` 更改为 `&`。`&` 是一个 XML 转义字符。
   - 选择仅限 SP 发起的 SAML 断言，使门户仅支持 SP 发起的登录流。此选项将拒绝 IdP 发起的登录流中未经请求的 SAML 断言。

> **Note**
>
> 某些第三方 IdPs 允许您创建自定义 SAML 应用程序，该应用程序可以利用 SP 启动的流程提供 IDP 启动的身份验证体验。例如，请参阅添加 Okta 书签应用程序。

5. 选择是否要启用签署向该提供商发出的 SAML 请求。通过 SP 发起的身份验证，您的 IdP 可以验证身份验证请求是否来自门户，从而阻止接受其他第三方请求。
   a. 下载签名证书并将其上传到您的 IdP。相同的签名证书可用于单次注销。
   b. 在您的 IdP 中启用签名请求。名称可能会有所不同，具体取决于 IdP。

   > **Note**
   >
   > RSA-SHA256 是唯一支持的请求和默认请求签名算法。

6. 选择是否要启用需要加密的 SAML 断言。这支持您对来自您的 IdP 的 SAML 断言进行加密。它可以防止数据在 IdP 和安全浏览器之间的 SAML 断言中被拦截。 WorkSpaces

   > **Note**
   >
   > 此步骤中没有加密证书。它将在您的门户启动后创建。启动门户后，下载加密证书并将其上传到您的 IdP。然后，在您的 IdP 中启用断言加密（名称可能有所不同，具体取决于 IdP）。

7. 选择是否要启用单点注销。单点注销允许您的最终用户通过一个操作退出其 IdP WorkSpaces 和安全浏览器会话。
   a. 从 WorkSpaces 安全浏览器下载签名证书并将其上传到您的 IdP。这与上一步中用于请求签名的签名证书相同。
   b. 使用单点注销需要您在 SAML 2.0 身份提供者中配置单点注销 URL。您可以在控制台的服务提供者（SP）详细信息 - 显示各个元数据值下找到门户的单点注销 URL，也可以从 `<md:SingleLogoutService>` 下方的 SP 元数据文件中找到。
   c. 在您的 IdP 中启用单点注销。名称可能会有所不同，具体取决于 IdP。

### 在您自己的 IdP 上配置 IdP

要在您自己的 IdP 上配置 IdP，请按照以下步骤操作。

1. 在浏览器中打开一个新标签页。
2. 将您的门户元数据添加到 SAML IdP。

   将您在上一步中下载的 SP 元数据文档上传到该 IdP，或者复制元数据值并将其粘贴到 IdP 中的正确字段中。某些提供者不允许上传文件。

   此过程的详细信息因提供者而异。有关如何将门户详细信息添加到 IdP 配置的帮助，请在the section called “具体指导方针 IdPs”中查看提供者文档。
3. 确认 SAML 断言的 NameID。

   确保 SAML IdP 使用用户电子邮件字段填充 SAML 断言的 NameID。NameID 和用户电子邮件用于在门户中唯一标识您的 SAML 联合用户。使用持久性 SAML 名称 ID 格式。
4. 可选：为 IdP 发起的身份验证配置中继状态。

   如果您在上一步中选择了接受 SP 发起和 IdP 发起的 SAML 断言，请按照the section called “在安全浏览器上 WorkSpaces 配置 IdP”中的步骤 2 操作，为您的 IdP 应用程序设置默认中继状态。
5. 可选：配置请求签名。如果您在上一步中选择了签署向该提供者发出的 SAML 请求，请按照the section called “在安全浏览器上 WorkSpaces 配置 IdP”中的步骤 3 操作，将签名证书上传到您的 IdP 并启用请求签名。有些人 IdPs（例如 Okta）可能需要您的 Name ID 属于 “永久” 类型才能使用请求签名。请务必按照上述步骤操作，确认您的 SAML 断言的 NameID。
6. 可选：配置断言加密。如果您选择了需要此提供者提供加密的 SAML 断言，请等到门户创建完成，然后按照下文“上传元数据”中的步骤 4 操作，将加密证书上传到您的 IdP 并启用断言加密。
7. 可选：配置单点注销。如果您选择了单点注销，请按照the section called “在安全浏览器上 WorkSpaces 配置 IdP”中的步骤 5 操作，将签名证书上传到您的 IdP，填写单点注销 URL，然后启用单点注销。
8. 向 IdP 中的用户授予使用 WorkSpaces 安全浏览器的访问权限。
9. 从 IdP 下载元数据交换文件。您将在下一步中将此元数据上传到 WorkSpaces 安全浏览器。

在亚马逊 WorkSpaces 安全浏览器上完成 IdP 配置

要在 WorkSpaces 安全浏览器上完成 IdP 配置，请按照以下步骤操作。

1. 返回到 WorkSpaces 安全浏览器控制台。在创建向导的配置身份提供者页面的 IdP 元数据下，上传元数据文件，或输入来自您的 IdP 的元数据 URL。该门户使用来自 IdP 的这些元数据来建立信任。
2. 要上传元数据文件，请在 IdP 元数据文档下，选择选择文件。上传您在上一步中下载的 XML 格式的 IdP 元数据文件。

3. 要使用元数据 URL，请前往您在上一步中设置的 IdP，并获取其元数据 URL。返回 WorkSpaces 安全浏览器控制台，在 IdP 元数据 URL 下，输入您从 IdP 获得的元数据 URL。
4. 完成后，选择下一步。
5. 对于启用了需要此提供者提供加密的 SAML 断言选项的门户，您需要从门户 IdP 详细信息部分下载加密证书，并将其上传到您的 IdP。然后，可以在那里启用该选项。

> **Note**
>
> WorkSpaces 安全浏览器要求在 IdP 设置的 SAML 断言中映射和设置主题或名称 ID。您的 IdP 可以自动创建这些映射。如果这些映射配置不正确，您的用户将无法登录 Web 门户并启动会话。
>
> WorkSpaces 安全浏览器要求在 SAML 响应中包含以下声明。您可以通过控制台或 CLI *<Your SP ACS URL>* 从门户的服务提供商详细信息或元数据文档中查找*<Your SP Entity ID>*和查找。
>
> - 一项 `AudienceRestriction` 声明，所具有的 `Audience` 值将您的 SP 实体 ID 设置为响应的目标。示例：
>
> ```
> <saml:AudienceRestriction>
> <saml:Audience><Your SP Entity ID></saml:Audience>
> </saml:AudienceRestriction>
> ```
>
> - 一项 `Response` 声明，具有原始 SAML 请求 ID 的 `InResponseTo` 值。示例：
>
> ```
> <samlp:Response ... InResponseTo="<originalSAMLrequestId>">
> ```
>
> - 一项 `SubjectConfirmationData` 声明，具有 SP ACS URL 的 `Recipient` 值，以及与原始 SAML 请求 ID 匹配的 `InResponseTo` 值。示例：
>
> ```
> <saml:SubjectConfirmation>
> <saml:SubjectConfirmationData ...
> Recipient="<Your SP ACS URL>"
> InResponseTo="<originalSAMLrequestId>"
> />
> </saml:SubjectConfirmation>
> ```
>
> WorkSpaces 安全浏览器会验证您的请求参数和 SAML 断言。对于 IdP 发起的 SAML 断言，必须将您的请求的详细信息的格式设置为 HTTP POST 请求正文中的 `RelayState` 参数。请求正文还必须包含您的 SAML 断言，作为 `SAMLResponse` 参数。如果您已经执行了上一步操作，则这两个参数都应该存在。

以下是 IdP 发起的 SAML 提供者的 POST 正文示例。

```
SAMLResponse=<Base64-encoded SAML assertion>&RelayState=<RelayState>
```

特定 IdPs 于 Amazon WorkSpaces 安全浏览器的使用指南

为确保正确配置门户的 SAML 联合，请参阅以下链接以获取常用 IdPs文档。

| IdP | SAML 应用程序设置 | 用户管理 | IdP 发起的身份验证 | 请求签名 | 断言加密 | 单点注销 |
|---|---|---|---|---|---|---|
| Okta | Create SAML app integrations | User management | Application Integration Wizard SAML field reference | Application Integration Wizard SAML field reference | Application Integration Wizard SAML field reference | Application Integration Wizard SAML field reference |
| Entra | Create your own application | Quickstart: Create and assign a user account | Enable single sign-on for an enterprise application | SAML Request Signature Verification | Configure Microsoft Entra SAML token encryption | Single Sign-Out SAML Protocol |
| Ping | Add a SAML application | Users | Enabling IdP-initiated SSO | 为企业配置身份验证 PingOne 请求登录 | 企业版是否 PingOne 支持加密？ | SAML 2.0 single logout |
| One Login | SAML Custom Connector (Advanced) (4266907) | 将用户添加到“OneLogin 手动” | SAML Custom Connector (Advanced) (4266907) | SAML Custom Connector (Advanced) (4266907) | SAML Custom Connector (Advanced) (4266907) | SAML Custom Connector (Advanced) (4266907) |

| IdP | SAML 应用程序设置 | 用户管理 | IdP 发起的身份验证 | 请求签名 | 断言加密 | 单点注销 |
|---|---|---|---|---|---|---|
| IAM Identity Center | 设置您自己的 SAML 2.0 应用程序 | 设置您自己的 SAML 2.0 应用程序 | 设置您自己的 SAML 2.0 应用程序 | 不适用 | 不适用 | 不适用 |

为 Amazon WorkSpaces 安全浏览器配置 IAM 身份中心身份验证类型

对于 IAM Identity Center 类型（高级选项），将 IAM Identity Center 与您的门户联合。只有在以下条件适用于您时，才选择此选项：

- 您的 IAM 身份中心的配置 AWS 账户 与 AWS 区域 您的 Web 门户网站相同。
- 如果您正在使用 AWS Organizations，则表示您使用的是管理账户。

在创建具有 IAM Identity Center 身份验证类型的 Web 门户之前，您必须将 IAM Identity Center 设置为独立提供者。有关更多信息，请参阅开始使用 IAM Identity Center 中的常见任务。或者，您可以将您的 SAML 2.0 IdP 连接到 IAM Identity Center。有关更多信息，请参阅连接到外部身份提供者。否则，将没有任何用户或组可以分配给您的 Web 门户。

如果您已经在使用 IAM Identity Center，则可以选择 IAM Identity Center 作为提供者类型，然后按照以下步骤在您的 Web 门户中添加、查看或删除用户或组。

> **Note**
>
> 要使用此身份验证类型，您的 IAM 身份中心必须与您的 WorkSpaces 安全浏览器门户处于 AWS 区域 相同 AWS 账户 和相同的位置。如果您的 IAM 身份中心位于单独的 AWS 账户 或 AWS 区域，请按照标准身份验证类型的说明进行操作。有关更多信息，请参阅 the section called “标准身份验证类型”。
> 如果您正在使用 AWS Organizations，则只能使用管理账户创建与 IAM Identity Center 集成的 WorkSpaces 安全浏览器门户。

主题

- 通过 IAM Identity Center 创建 Web 门户
- 通过 IAM Identity Center 管理您的 Web 门户

- 向 Web 门户中添加其他用户和组
- 查看或删除 Web 门户的用户和组

通过 IAM Identity Center 创建 Web 门户

要通过 IAM Identity Center 创建 Web 门户，请按照以下步骤操作。

通过 IAM Identity Center 创建 Web 门户

1. 在步骤 4：配置身份提供者的门户创建过程中，选择 AWS IAM Identity Center。
2. 选择继续使用 IAM Identity Center。
3. 在分配用户和组页面上，选择用户和/或组选项卡。
4. 选中要添加到门户中的用户或组旁边的复选框。
5. 创建门户后，您关联的用户可以使用其 IAM Identity Center 用户名和密码登录 WorkSpaces 安全浏览器。

通过 IAM Identity Center 管理您的 Web 门户

要通过 IAM Identity Center 管理您的 Web 门户，请按照以下步骤操作。

通过 IAM Identity Center 管理您的 Web 门户

1. 创建门户后，它将在 IAM Identity Center 控制台中作为已配置的应用程序列出。
2. 要访问此应用程序的配置，请在侧栏中选择应用程序，然后查找名称与您的 Web 门户显示名称匹配的已配置应用程序。

> **Note**
>
> 如果您尚未输入显示名称，则会改为显示门户的 GUID。GUID 是您的 Web 门户端点 URL 前缀的 ID。

向 Web 门户中添加其他用户和组

要向现有 Web 门户中添加其他用户和组，请按照以下步骤操作。

向现有 Web 门户中添加其他用户和组

1. 打开 WorkSpaces 安全浏览器控制台，网址为https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/。
2. 选择 “WorkSpaces 安全浏览器”、“门户网站”，选择您的 Web 门户，然后选择 “编辑”。
3. 选择身份提供者设置和分配其他用户和组。在此处，您可以将用户和组添加到您的 Web 门户。

> **Note**
>
> 您无法从 IAM Identity Center 控制台添加用户或组。您必须从 WorkSpaces 安全浏览器门户的编辑页面执行此操作。

查看或删除 Web 门户的用户和组

要查看或删除 Web 门户的用户和组，请执行分配的用户表中提供的操作。有关更多信息，请参阅管理对应用程序的访问

> **Note**
>
> 您无法在 S WorkSpaces ecure BrowserPortal 的编辑页面中查看或删除用户和群组。必须从 IAM Identity Center 控制台的编辑页面执行此操作。

## 更改 Amazon WorkSpaces 安全浏览器的身份提供者类型

您可以随时更改门户的身份验证类型。为此，请按照以下步骤操作。

- 要从 IAM Identity Center 更改为标准，请按the section called “标准身份验证类型”中的步骤操作。
- 要从标准更改为 IAM Identity Center，请按the section called “IAM Identity Center 身份验证类型”中的步骤操作。

对身份提供者类型的更改最多可能需要 15 分钟才能部署，并且不会自动终止正在进行的会话。

您可以通过 AWS CloudTrail 检查`UpdatePortal`事件来查看门户的身份提供商类型更改。该类型将在事件的请求和响应有效载荷中显示。

## 使用 Amazon WorkSpaces 安全浏览器启动门户网站

Web 门户配置完毕后，您可以按照以下步骤启动门户。

1. 在步骤 5：查看和启动页面上，查看您为 Web 门户选择的设置。您可以选择编辑 来更改给定部分中的设置。您也可以稍后通过控制台的 Web 门户选项卡更改这些设置。
2. 完成后，选择启动 Web 门户。
3. 要查看 Web 门户的状态，请选择 Web 门户，选择您的门户，然后选择查看详细信息。

   门户具有下列状态之一：

   - 不完整 - Web 门户的配置缺少所需的身份提供者设置。
   - 待定 - Web 门户正在对其设置应用更改。
   - 激活 - Web 门户已准备就绪，可供使用。
4. 最多等待 15 分钟，让您的门户变为活动状态。

## 在 Amazon WorkSpaces 安全浏览器中测试您的门户网站

创建门户网站后，您可以登录 WorkSpaces 安全浏览器端点，像最终用户一样浏览连接的网站。

如果已完成the section called “身份提供者配置”中的这些步骤，则可以跳过本节，进入在 Amazon WorkSpaces 安全浏览器中分发您的门户网站。

1. 在https://console.aws.amazon.com/workspaces-web/家打开 WorkSpaces 安全浏览器控制台？region=us-e ast-1#/。
2. 选择 “WorkSpaces 安全浏览器”、“门户网站”，选择您的 Web 门户，然后选择 “查看详细信息”
3. 在 Web 门户端点下，转到您门户的指定 URL。Web 门户端点是您的用户在使用为门户配置的身份提供者登录后启动您 Web 门户的接入点。其在 Internet 上公开提供，可以嵌入到您的网络中。
4. 在 WorkSpaces 安全浏览器登录页面上，选择登录、SAML，然后输入您的 SAML 凭据。
5. 当您看到 “您的会话正在准备中” 页面时，您的 WorkSpaces 安全浏览器会话即会启动。请勿关闭或退出此页面。
6. Web 浏览器启动，显示您的启动 URL 以及通过浏览器策略设置配置的任何其他行为。
7. 现在，您可以通过选择链接或 URLs 进入地址栏来浏览已连接的网站。

# 在 Amazon WorkSpaces 安全浏览器中分发您的门户网站

当您准备好让用户开始使用 WorkSpaces 安全浏览器时，您可以从以下选项中进行选择来分发门户：

- 将您的门户添加到 SAML 应用程序网关，以便用户直接从其 IdP 启动会话。您可以借助符合 SAML 2.0 标准的 IdP 通过 IdP 发起的登录流来完成此操作。有关更多信息，请参阅the section called “标准身份验证类型”中的 SP 发起和 IdP 发起的 SAML 断言。或者，您可以创建自定义 SAML 应用程序，该应用程序可以使用 SP 发起的流程提供 IdP 发起的身份验证体验。有关更多信息，请参阅创建书签应用程序集成。
- 将门户 URL 添加到您拥有的网站，然后使用浏览器重定向将用户引导到 Web 门户。
- 通过电子邮件将门户 URL 发送给您的用户，或者向下推送到您作为浏览器主页或书签管理的设备。

# 在 Amazon WorkSpaces 安全浏览器中管理您的门户网站

设置 Web 门户后，您可以执行以下操作来对其进行管理。

主题


- 在 Amazon WorkSpaces 安全浏览器中查看门户网站详情
- 在 Amazon WorkSpaces 安全浏览器中编辑门户
- 在 Amazon WorkSpaces 安全浏览器中删除门户网站
- 在 Amazon WorkSpaces 安全浏览器中管理门户网站的服务配额
- 控制在 Amazon 安全浏览器中重新验证 SAML IdP 令牌的时间间隔 WorkSpaces
- 在 Amazon WorkSpaces 安全浏览器中设置用户访问登录
- 在 Amazon WorkSpaces 安全浏览器中管理浏览器策略
- 为 Amazon WorkSpaces 安全浏览器配置输入法编辑器
- 为 Amazon WorkSpaces 安全浏览器配置会话内本地化
- 在 Amazon WorkSpaces 安全浏览器中管理 IP 访问控制
- 在 Amazon WorkSpaces 安全浏览器中管理单点登录扩展
- 在 Amazon WorkSpaces 安全浏览器中设置 URL 过滤
- Amazon WorkSpaces 安全浏览器中的深度链接
- 使用 Amazon WorkSpaces 安全浏览器中的会话管理控制面板
- 使用 FIPS 终端节点和 Amazon WorkSpaces 安全浏览器保护传输中的数据
- 在 Amazon WorkSpaces 安全浏览器中管理数据保护设置
- 在 Amazon WorkSpaces 安全浏览器中管理工具栏控件


## 在 Amazon WorkSpaces 安全浏览器中查看门户网站详情

要查看 Web 门户详细信息，请按照以下步骤操作。

1. 打开 WorkSpaces 安全浏览器控制台，网址为https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/。
2. 选择 “WorkSpaces 安全浏览器”、“门户网站”，选择您的 Web 门户，然后选择 “查看详细信息”。

# 在 Amazon WorkSpaces 安全浏览器中编辑门户

要编辑 Web 门户，请按照以下步骤操作。

1. 打开 WorkSpaces 安全浏览器控制台，网址为https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/。
2. 选择 “WorkSpaces 安全浏览器”、“门户网站”，选择您的 Web 门户，然后选择 “编辑”。

> **Note**
>
> 对网络设置或超时设置的更改会立即结束所有活动的门户会话。用户已断开连接，必须重新连接才能开始新会话。对剪贴板权限、文件传输权限或打印到本地设备的更改从第一个新会话开始生效。当前处于活动状态的会话不会断开连接。连接到活动会话的用户在断开连接并连接到新会话之前不会受到更改的影响。

# 在 Amazon WorkSpaces 安全浏览器中删除门户网站

要删除 Web 门户，请按照以下步骤操作。

1. 打开 WorkSpaces 安全浏览器控制台，网址为https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/。
2. 选择 “WorkSpaces 安全浏览器”、“门户网站”，选择您的 Web 门户，然后选择 “删除”。

# 在 Amazon WorkSpaces 安全浏览器中管理门户网站的服务配额

在您创建时 AWS 账户，我们会自动为资源使用设置默认服务配额（也称为限制）AWS 服务。管理员必须知道可能需要增加两个配额才能支持其使用案例。这两个配额是您可以在每个区域创建的 Web 门户数量，以及每个区域中每种可用实例类型可以支持的最大并发会话数。您可以从 AWS 控制台的 Service Quotas 页面申请增加这些配额。

下表列出了默认服务配额限制。

| AWS 区域 按账户内的默认配额 | 值 |
| --- | --- |
| Web 门户 | 3 |

| AWS 区域 按账户内的默认配额 | 值 |
| --- | --- |
| 最大并行会话数 - standard.regular | 25 |
| 最大并行会话数 - standard.large | 10 |
| 最大并行会话数 - standard.xlarge | 5 |

要随时查看每个区域分配给您的账户的服务配额，请参阅服务配额页面。

> **Important**
>
> 服务配额 AWS 区域 一次影响一个。在每个需要更多资源 AWS 区域 的地方，您都必须申请增加服务配额。有关更多信息，请参阅 Amazon WorkSpaces 安全浏览器终端节点和配额。

主题


- 在 Amazon WorkSpaces 安全浏览器中申请增加服务配额
- 请求在 Amazon WorkSpaces 安全浏览器中增加门户
- 在 Amazon WorkSpaces 安全浏览器中请求最大并发会话数增加
- Amazon WorkSpaces 安全浏览器的限制示例
- Amazon WorkSpaces 安全浏览器中的其他服务配额


## 在 Amazon WorkSpaces 安全浏览器中申请增加服务配额

要请求增加服务限额，请按照以下步骤操作。

1. 打开 AWS Support 控制面板。
2. 选择提高服务限制。

> **Important**
>
> WorkSpaces 安全浏览器服务配额一次影响一个区域。您必须在需要更多资源的每个 AWS 区域都请求增加服务配额。有关更多信息，请参阅 AWS 服务端点。

3. 在使用案例描述下，输入以下信息：

- 如果您请求增加 Web 门户的数量，请指定此资源类型，并包括您的 AWS 账户 ID、您想要增加 Web 门户的区域以及新的限额值。
- 如果您请求增加最大并发会话数，请指定此资源类型，并包括您的 AWS 账户 ID、您想要增加最大并发会话数的区域、Web 门户 ARN 和新的限额值。

4. （可选）要同时请求提升多个服务配额，请在请求部分完成一个提升配额的请求，然后选择添加另一个请求。

## 请求在 Amazon WorkSpaces 安全浏览器中增加门户

门户是该服务的基础资源。每个门户是 SAML 2.0 身份提供者与您的 Internet 网络连接和任何私有 Web 内容之间的关联。每个门户可以有单独的门户浏览器策略和用户设置，因此，管理员通常会在同一区域创建多个门户以应对不同的使用案例。例如，您可以为组 A 提供访问具有限制性策略（例如，禁用剪贴板和文件传输功能）的特定网站的权限，为组 B 提供在不进行 URL 筛选的情况下访问通用 Internet 的权限。您可以在任何受支持的 AWS 区域创建门户。要查看当前的服务可用性，请参阅按区域划分的 AWS 服务。

请求增加服务配额

1. 打开您所需区域对应的服务配额页面。
2. 选择 Web 门户数量。
3. 选择请求增加账户级别配额。
4. 在增加配额值下，输入您想要的配额总量。

## 在 Amazon WorkSpaces 安全浏览器中请求最大并发会话数增加

最大并发会话数配额是指同时连接到门户的最多用户数。如果未正确设置最大并发会话的服务配额限制，则用户在登录时可能会发现会话不可用。除了增加此服务配额外，客户还必须确保其 VPC 和子网有足够的 IP 空间来支持最大并发会话数。

请求增加最大并发会话数

1. 打开您所需区域对应的服务配额页面。
2. 针对要增加的实例类型，选择每个门户的最大并发会话数。
3. 选择请求增加账户级别配额。
4. 在增加配额值下，输入您想要的配额总量。

> **Note**
>
> 如需大幅增加或紧急增加，请转至服务配额历史记录页面，选择请求状态列中的链接，链接到您的支持案例，然后添加回复，其中包含有关您的使用案例和/或紧急程度的详细信息。这些信息可以帮助服务团队确定请求的优先顺序，并确保为您的账户分配足够的容量。

## Amazon WorkSpaces 安全浏览器的限制示例

例如，假设管理员正在美国东部（弗吉尼亚州北部）为总共 125 名用户配置两个 Web 门户。在创建 Web 门户之前，管理员确定第一个 Web 门户（门户 A）将支持 100 名用户。在为这些用户测试工作流时，管理员确定他们将需要 XL 实例类型来支持会话期间的音频和视频流传输。第二个 Web 门户（门户 B）需要可供最多 25 名用户使用，才能支持访问托管在客户 VPC 中的单个静态网页。在测试此使用案例时，管理员确定标准实例类型可以支持此使用案例。

对于门户 A，管理员必须提交服务配额增加请求，将 XL 实例的限制从默认区域（即 5）提高到 100。完成后，管理员可以通过编辑 Web 门户来分配容量。对于门户 B，管理员无需请求增加配额即可继续操作（也就是说，因为该区域的标准实例类型默认配额为 25）。

## Amazon WorkSpaces 安全浏览器中的其他服务配额

您可以查看服务配额页面上列出的其他配额并请求提高配额。实际上，大多数客户会发现没有必要请求提高这些限额。这些配额大致分为两种类型：数量和速率。

对于数量配额，当您提交服务配额增加请求以提高 Web 门户数量时，创建唯一门户所需的子资源数量将自动增加。这将反映在服务配额页面上。例如，如果您请求将门户数量从 3 增加到 5，则浏览器和用户设置的服务配额将自动从 3 增加到 5。您可以根据需要选择重复使用或创建新的子资源。

在极少数情况下，客户可能会发现增加其他资源配额的数量或速率的使用案例。例如，管理员可能希望增加浏览器设置的数量，以测试其他门户配置。将 case-by-case根据情况对这些服务配额申请进行审查和满足。

对于速率配额，无论账户门户限制如何，都无需调整“服务配额”中显示的速率限制。

# 控制在 Amazon 安全浏览器中重新验证 SAML IdP 令牌的时间间隔 WorkSpaces

当用户访问 WorkSpaces 安全浏览器门户时，他们可以登录以启动直播会话。除非他们在不到 5 分钟前登录，否则每个会话都从起始页开始。门户会检查身份提供者（IdP）令牌，以确定是否在启动会话时提示用户输入凭证。没有有效 IdP 令牌的用户必须输入用户名、密码，以及多因素身份验证（MFA，可选），才能启动流会话。如果用户已经通过登录自己的 IdP 或受同一 IdP 保护的应用程序生成 SAML IdP 令牌，则不会要求他们提供登录凭证。

如果用户拥有有效的 SAML IdP 令牌，则他们可以 WorkSpaces 访问安全浏览器。您可以控制重新验证 SAML IdP 令牌所需的时间间隔。

控制重新验证 SAML IdP 令牌的时间间隔

1. 与您的 SAML IdP 提供者一起设置 IdP 超时时间。建议将 IdP 超时时间配置为用户完成任务所需的最短时间。
   - 有关 Okta 的更多信息，请参阅为所有策略强制使用有限的会话生命周期。
   - 有关 Azure AD 的更多信息，请参阅配置身份验证会话控制。
   - 有关 Ping 的更多信息，请参阅会话。
   - 有关的更多信息 AWS IAM Identity Center，请参阅设置会话持续时间。
2. 设置 WorkSpaces 安全浏览器门户的非活动状态和空闲超时值。这些值控制从用户上次互动到 WorkSpaces 安全浏览器会话因不活动而结束的时间间隔。会话结束后，用户将失去其会话状态（包括打开的选项卡、未保存的 Web 内容和历史记录），并在下一个会话开始时恢复到全新状态。有关更多信息，请参阅the section called “Web 门户创建”中的步骤 5。

   > **Note**
   >
   > 如果用户的会话超时，但该用户仍有有效的 SAML IdP 令牌，则他们无需输入用户名和密码即可开始 WorkSpaces 新的安全浏览器会话。要控制如何重新验证令牌，请按照上一步中的指南进行操作。

# 在 Amazon WorkSpaces 安全浏览器中设置用户访问登录

您可以设置用户访问日志记录来记录以下用户事件：

- 会话开始-标志着 WorkSpaces 安全浏览器会话的开始。
- 会话结束-标志着 WorkSpaces 安全浏览器会话的结束。
- URL 导航 - 记录用户加载的 URL。

> **Note**
>
> URL 导航日志记录在浏览器历史记录中。 URLs 未记录在浏览器历史记录中（无论是在隐身模式下访问过，还是从浏览器历史记录中删除）都不会记录在日志中。客户可以根据自己的浏览器策略来决定是关闭无痕模式还是删除历史记录。

此外，还包括每个事件的以下信息：

- 事件时间
- 用户名
- Web 门户 ARN

客户有责任了解他们在使用 WorkSpaces 安全浏览器时可能出现的法律问题，并确保他们在使用 WorkSpaces 安全浏览器时遵守所有适用的法律和法规。其中包括规范雇主监控员工使用 WorkSpaces 安全浏览器的能力的法律，包括在应用程序中执行的活动。

在您的 WorkSpaces 安全浏览器门户上激活用户访问日志可能会导致亚马逊 Kinesis Data Streams 收取费用。有关定价详细信息，请参阅 Amazon Kinesis Data Streams 定价。

要在 WorkSpaces 安全浏览器控制台中激活用户访问日志记录，请在用户访问日志下，选择要用于接收数据的 Kinesis Stream ID。记录的数据将直接传送到该数据流。

有关如何使用 Amazon Kinesis Data Streams 的更多信息，请参阅什么是 Amazon Kinesis Data Streams？

> **Note**
>
> 要从 WorkSpaces 安全浏览器接收日志，您必须拥有以 “amazon-workspaces-web-*” 开头的 Amazon Kinesis 数据流。您的 Amazon Kinesis 数据流必须关闭服务器端加密，或者必须 AWS 托管式密钥 用于服务器端加密。
> 有关在 Amazon Kinesis 中设置服务器端加密的更多信息，请参阅如何开始使用服务器端加密？。

主题


- Amazon WorkSpaces 安全浏览器的用户访问日志示例


## Amazon WorkSpaces 安全浏览器的用户访问日志示例

以下是每个可用事件的示例，包括验证StartSession、VisitPage、和EndSession。

每个事件始终包含以下字段：

- timestamp，以毫秒为单位的纪元时间。
- eventType，字符串形式。
- details，另一个 json 对象。
- portalArn 和 userName，除 Validation 之外的每个事件都包含这两个字段。

```
{
  "timestamp": "1665430373875",
  "eventType": "Validation",
  "details": {
    "permission": "Kinesis:PutRecord",
    "userArn": "userArn",
    "operation": "AssociateUserAccessLoggingSettings",
    "userAccessLoggingSettingsArn": "userAccessLoggingSettingsArn"
  }
}

{
  "timestamp": "1665179071723",
  "eventType": "StartSession",
  "details": {},
  "portalArn": "portalArn",
  "userName": "userName"
}

{
  "timestamp": "1665179084578",
  "eventType": "VisitPage",
  "details": {
    "title": "Amazon",
    "url": "https://www.amazon.com/"
  },
```

```
  "portalArn": "portalArn",
  "userName": "userName"
}

{
  "timestamp": "1665179155953",
  "eventType": "EndSession",
  "details": {},
  "portalArn": "portalArn",
  "userName": "userName"
}
```

# 在 Amazon WorkSpaces 安全浏览器中管理浏览器策略

使用 WorkSpaces 安全浏览器，您可以使用适用于最新稳定版本的 Chrome 政策来设置自定义浏览器政策。您可以将 300 多种策略应用于 Web 门户。如需了解更多信息，请参阅the section called “教程：设置自定义浏览器策略”和 Chrome 企业版策略列表。

通过使用控制台视图创建 Web 门户，您可以应用以下策略：

- `StartURL`
- 书签和书签文件夹
- 打开和关闭私密浏览
- 历史记录删除
- 通过 `AllowURL` 和 `BlockURL` 进行 URL 筛选

有关使用控制台视图策略的更多信息，请参阅入门。

WorkSpaces Secure Browser 将基本浏览器策略配置以及您指定的任何策略应用于所有门户。您可以通过自定义 JSON 文件编辑其中一些策略。有关更多信息，请参阅 the section called “编辑基准浏览器策略”。

主题

- 教程：在 Amazon WorkSpaces 安全浏览器中设置自定义浏览器策略
- 在 Amazon WorkSpaces 安全浏览器中编辑基本浏览器策略

# 教程：在 Amazon WorkSpaces 安全浏览器中设置自定义浏览器策略

您可以通过上传 JSON 文件来为 Linux 设置任何支持的 Chrome 策略。要详细了解 Chrome 策略，请参阅 Chrome 企业版策略列表并选择 Linux 平台。然后，搜索并查看最新稳定版本的策略。

在以下教程中，您可以创建具有以下策略控制措施的 Web 门户：

- 设置书签
- 设置默认启动页面
- 阻止用户安装其他扩展
- 阻止用户删除历史记录
- 阻止用户使用无痕模式
- 为所有会话预安装 Okta 插件扩展。

主题


- 步骤 1：创建 Web 门户
- 步骤 2：收集策略
- 步骤 3：创建自定义 JSON 策略文件
- 步骤 4：向模板添加您的策略
- 第 5 步：将您的策略 JSON 文件上传到您的 Web 门户


## 步骤 1：创建 Web 门户

要上传您的 Chrome 政策 JSON 文件，您必须创建一个 WorkSpaces 安全浏览器门户。有关更多信息，请参阅 the section called “Web 门户创建”。

## 步骤 2：收集策略

从 Chrome 策略中搜索并找到您想要的策略。然后，在下一步中，您可以使用这些策略创建 JSON 文件。

1. 转到 Chrome 企业版策略列表。
2. 选择平台 Linux，然后选择最新的 Chrome 版本。
3. 搜索您要设置的策略。在此示例中，搜索扩展以查找用于管理扩展的策略。每项策略都包括描述、Linux 首选项名称和示例值。
4. 从搜索结果中可以看出，如果一起使用，有 3 个策略可以满足业务要求：

- ExtensionSettings –在浏览器启动时安装扩展。
- ExtensionInstallBlocklist –阻止安装特定扩展。
- ExtensionInstallAllowlist— 允许安装某些扩展。

5. 其他策略可满足其余要求；
   - ManagedBookmarks— 向网页添加书签。
   - RestoreOnStartupURLs— 配置每当启动新的浏览器窗口时打开哪些网页。
   - AllowDeletingBrowserHistory— 配置用户是否可以删除其浏览历史记录。
   - IncognitoModeAvailability— 配置用户是否可以访问隐身模式。

## 步骤 3：创建自定义 JSON 策略文件

使用在上一步中找到的文本编辑器、模板和策略创建 JSON 文件。

1. 打开文本编辑器。
2. 复制下面的模板并粘贴到文本编辑器中：

```
{
  "chromePolicies":
    {
        "ManagedBookmarks":
        {
            "value":
            [
                {
                    "name": "Bookmark 1",
                    "url": "bookmark-url-1"
                },
                {
                    "name": "Bookmark 2",
                    "url": "bookmark-url-2"
                },
            ]
        },
        "RestoreOnStartup":
        {
            "value": 4
        },
        "RestoreOnStartupURLs":
```

```
        {
            "value":
            [
                "startup-url"
            ]
        },
        "ExtensionInstallBlocklist": {
            "value": [
                "insert-extensions-value-to-block",
            ]
        },
        "ExtensionInstallAllowlist": {
            "value": [
                "insert-extensions-value-to-allow",
            ]
        },
        "ExtensionSettings":
        {
            "value":
            {
                "insert-extension-value-to-force-install":
                {
                    "installation_mode": "force_installed",
                    "update_url": "https://clients2.google.com/service/update2/crx",
                    "toolbar_pin": "force_pinned"
                },
            }
        },
        "AllowDeletingBrowserHistory":
        {
            "value": should-allow-history-deletion
        },
        "IncognitoModeAvailability":
        {
            "value": incognito-mode-availability
        }
    }
}
```

## 步骤 4：向模板添加您的策略

将您的自定义策略添加到模板中，以满足每项业务要求。

1. 设置书签 URLs。
   a. 在 `value` 键下方，为要添加的每个书签添加 `name` 和 `url` 键对。
   b. 将 `bookmark-url-1` 设置为 `https://www.amazon.com`。
   c. 将 `bookmark-url-2` 设置为 `https://docs.aws.amazon.com/workspaces-web/latest/adminguide/`。

```
    "ManagedBookmarks":
        {
            "value":
            [
                {
                    "name": "Amazon",
                    "url": "https//www.amazon.com"
                },
                {
                    "name": "Bookmark 2",
                    "url": "https://docs.aws.amazon.com/workspaces-web/latest/
adminguide/"
                },
            ]
        },
```

2. 设置启动程序 URLs。此策略允许管理员设置用户启动新浏览器窗口时显示的网页。
   a. 将 `RestoreOnStartup` 设置为 4。这将`RestoreOnStartup`操作设置为打开列表 URLs 。您还可以在启动时使用其他操作 URLs。有关更多信息，请参阅 Chrome 企业版策略列表。
   b. 设置为 https://www.aboutamazon.com/`RestoreOnStartupURLs`news。

```
     "RestoreOnStartup":
        {
            "value": 4
        },
    "RestoreOnStartupURLs":
        {
            "value":
```

```
            [
                "https://www.aboutamazon.com/news"
            ]
        },
```

3. 要防止用户删除其浏览器历史记录，请将 `AllowDeletingBrowserHistory` 设置为 `false`。

```
    "AllowDeletingBrowserHistory":
        {
            "value": false
        },
```

4. 要为用户关闭无痕模式访问权限，请将 `IncognitoModeAvailability` 设置为 `1`。

```
    "IncognitoModeAvailability":
        {
            "value": 1
        }
```

5. 使用以下策略设置和实施 Okta 插件：
   - `ExtensionSettings` –在浏览器启动时安装扩展。扩展值可从 Okta 插件帮助页面获得。
   - `ExtensionInstallBlocklist` –阻止安装特定扩展。默认情况下，使用一个 `*` 值来阻止所有扩展。管理员可以控制允许在 `ExtensionInstallAllowlist` 上添加哪些扩展。
   - `ExtensionInstallAllowlist` 允许您安装某些扩展。由于 `ExtensionInstallBlocklist` 设置为 `*`，因此在此处添加 Okta 插件值以允许安装它。

   下面显示了开启 Okta 插件的策略示例：

```
        "ExtensionInstallBlocklist": {
            "value": [
                "*",
                ]
        },
        "ExtensionInstallAllowlist": {
            "value": [
```

```
                "glnpjglilkicbckjpbgcfkogebgllemb",
                ]
        },
        "ExtensionSettings": {
            "value": {
                "glnpjglilkicbckjpbgcfkogebgllemb": {
                    "installation_mode": "force_installed",
                    "update_url": "https://clients2.google.com/service/update2/crx",
                    "toolbar_pin": "force_pinned"
            }
        }
```

### 第 5 步：将您的策略 JSON 文件上传到您的 Web 门户

1. 打开 WorkSpaces 安全浏览器控制台，网址为https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/。
2. 选择 “WorkSpaces 安全浏览器”，然后选择 Web 门户。
3. 选择您的 Web 门户，然后选择编辑。
4. 选择策略设置，然后选择 JSON 文件上传。
5. 选择选择文件。导航到、选择并上传您的 JSON 文件。
6. 选择保存。

## 在 Amazon WorkSpaces 安全浏览器中编辑基本浏览器策略

为了提供服务， WorkSpaces 安全浏览器将基本浏览器策略应用于所有门户。除了您在控制台视图或 JSON 上传中指定的策略外，还会应用此基准策略。以下是该服务以 JSON 格式应用的策略列表：

```
{
    "chromePolicies":
    {
        "DefaultDownloadDirectory": {
            "value": "/home/as2-streaming-user/MyFiles/TemporaryFiles"
        },
        "DownloadDirectory": {
            "value": "/home/as2-streaming-user/MyFiles/TemporaryFiles"
        },
        "DownloadRestrictions": {
```

```
            "value": 1
        },
        "URLBlocklist": {
            "value": [
                "file://",
                "http://169.254.169.254",
                "http://[fd00:ec2::254]",
            ]
        },
        "URLAllowlist": {
            "value": [
                "file:///home/as2-streaming-user/MyFiles/TemporaryFiles",
                "file:///opt/appstream/tmp/TemporaryFiles",
            ]
        }
    }
}
```

客户无法更改以下策略：

- `DefaultDownloadDirectory` – 无法编辑此策略。该服务会覆盖对此策略所做的任何更改。
- `DownloadDirectory` – 无法编辑此策略。该服务会覆盖对此策略所做的任何更改。

客户可以更新其 Web 门户的以下策略：

- `DownloadRestrictions` – 默认设置为 `1`，以防止被 Chrome Safe Browsing 识别为恶意的下载。有关更多信息，请参阅防止用户下载有害文件。您可以将该值从 `0` 设置为 `4`。
- 可以使用控制台视图 URL 筛选功能或 JSON 上传来扩展 `URLAllowlist` 和 `URLBlocklist` 策略。但是，基线 URLs 不能被覆盖。从您的 Web 门户下载的 JSON 文件中看不到这些策略。但是，如果您在会话期间访问“chrome://policy”，则远程浏览器会显示已应用的策略。

# 为 Amazon WorkSpaces 安全浏览器配置输入法编辑器

输入法编辑器 (IME) 是一种实用程序，它为最终用户提供了使用键盘布局而不是 QWERTY 键盘的语言输入文本的选项。 IMEs 帮助用户使用语言集更大、更复杂的语言（例如日语、中文和韩语）输入文本。 WorkSpaces 默认情况下，安全浏览器会话包括 IME 支持。用户可以在会话中从 IME 工具栏或使用键盘快捷键选择其他语言。

WorkSpaces 安全浏览器的 IME 目前支持以下语言：

- English
- 简体中文（拼音）
- 繁体中文（Bopomofo）
- 日语
- 韩语

要从 IME 工具栏中选择语言，请执行以下操作：

1. 选择位于黑色顶部面板栏右侧的语言选择器下拉列表。默认情况下，选择器将显示 en，表示英语。
2. 在下拉菜单中，选择所需的语言。
3. 在选择语言后显示的子菜单中，选择其他语言详细信息。

要使用键盘快捷键选择语言，请执行以下操作：

- 全部 IMEs
  - 要往后循环 IME（或移动至右侧键盘布局），请按 Shift+Control+Left Alt。
- 日语
  - 要选择平假名，请按 F6
  - 要选择片假名，请按 F7
  - 要选择拉丁语，请按 F10。
  - 要选择宽拉丁语，请按 F9。
  - 要选择直接输入，请按 ALT +、ALT+@、Zenkaku Hankaku。
- 韩语
  - 要选择朝鲜语，请按 Shift+Space
  - 要选择汉字，请按 F9。

要删除 IME 工具栏和菜单，或者要关闭 WorkSpaces 安全浏览器会话中的屏幕键盘，请联系 支持。

# 为 Amazon WorkSpaces 安全浏览器配置会话内本地化

当用户启动会话时， WorkSpaces 安全浏览器会检测用户的本地浏览器语言和时区设置，并将其应用于会话。这将会影响会话期间的显示语言，并有助于确保显示的时间与用户所在位置的当前时间相匹配。

会话语言按以下优先顺序确定：

1. 门户网站浏览器设置中的ForcedLanguages政策。有关更多信息，请参阅 ForcedLanguages。
2. 最终用户的本地浏览器语言设置。
3. 默认值为 英语(en-US)。

时区由最终用户浏览器中指定的本地时区设置决定。如果时区设置无效，则使用 UTC。

WorkSpaces 安全浏览器中的以下组件支持本地化：

- WorkSpaces 安全浏览器登录页面
- WorkSpaces 安全浏览器门户状态消息（包括加载消息和错误）
- Chrome 浏览器
- 系统上下文菜单和另存为窗口

主题


- Amazon WorkSpaces 安全浏览器支持的语言代码
- 在用户浏览器设置中选择语言


## Amazon WorkSpaces 安全浏览器支持的语言代码

以下列表显示了 WorkSpaces 安全浏览器当前支持的语言代码。如果用户的本地浏览器设置为使用不支持的语言代码，则会话默认为英语（en-US）。

- 德语
  - de – 德语
  - de-AT – 德语（奥地利）
  - de-DE – 德语（德国）
  - de-CH – 德语（瑞士）

  - de-LI – 德语（列支敦士登）
- English
  - en – 英语
  - en-AU – 英语（澳大利亚）
  - en-CA – 英语（加拿大）
  - en-IN – 英语（印度）
  - en-NZ –英语（新西兰）
  - en-ZA – 英语（南非）
  - en-GB – 英语（英国）
  - en-US – 英语（美国）
- 西班牙语
  - es – 西班牙语
  - es-AR – 西班牙语（阿根廷）
  - es-CL – 西班牙语（智利）
  - es-CO – 西班牙语（哥伦比亚）
  - es-CR – 西班牙语（哥斯达黎加）
  - es-HN – 西班牙语（洪都拉斯）
  - es-419 – 西班牙语（拉丁美洲）
  - es-MX – 西班牙语（墨西哥）
  - es-PE – 西班牙语（秘鲁）
  - es-ES – 西班牙语（西班牙）
  - es-US – 西班牙语（美国）
  - es-UY – 西班牙语（乌拉圭）
  - es-VE – 西班牙语（委内瑞拉）
- 法语
  - fr – 法语
  - fr-CA – 法语（加拿大）
  - fr-FR – 法语（法国）
  - fr-CH – 法语（瑞士）



- 印度尼西亚语

  - id – 印度尼西亚语
  - id-ID – 印度尼西亚语（印度尼西亚）
- 意大利语
  - it – 意大利语
  - it-IT – 意大利语（意大利）
  - it-CH – 意大利语（瑞士）
- 日语
  - ja – 日语
  - ja-JP – 日语（日本）
- 韩语
  - ko – 韩语
  - ko-KR – 韩语（韩国）
- 葡萄牙语
  - pt – 葡萄牙语
  - pt-BR – 葡萄牙语（巴西）
  - pt-PT – 葡萄牙语（葡萄牙）
- 中文
  - zh – 中文
  - zh-CN – 中文（中国）
  - zh-HK – 中文（香港）
  - zh-TW – 中文（台湾）

## 在用户浏览器设置中选择语言

要设置用户的本地浏览器设置，请按照相应的步骤操作。

- 在 Chrome 中，选择设置、语言，然后根据偏好对语言进行排序。
- 在 Firefox 中，选择设置、常规、语言，然后从下拉菜单中选择语言。
- 在 Edge 中，选择设置、语言，然后根据偏好对语言进行排序。

# 在 Amazon WorkSpaces 安全浏览器中管理 IP 访问控制

WorkSpaces 安全浏览器允许您控制可以从哪些 IP 地址访问您的门户网站。通过使用 IP 访问设置，您可以定义和管理可信 IP 地址组，并仅允许用户在连接到可信网络时访问其门户。

默认情况下， WorkSpaces 安全浏览器允许用户从任何地方访问其门户网站。IP 访问控制组充当虚拟防火墙，用于筛选用户可用来连接 Web 门户的 IP 地址。当与您的 Web 门户关联时，IP 访问设置将在身份验证之前检测用户 IP，以确定他们是否符合连接资格。连接后， WorkSpaces Secure Browser 会持续监控用户的 IP 地址，以确保他们通过可信网络保持连接。如果用户的 IP 发生变化， WorkSpaces 安全浏览器将检测并终止会话。

要指定 CIDR 地址范围，请向 IP 访问控制组添加规则，然后将该组与您的 Web 门户关联。您可以将每个 IP 访问设置与一个或多个 Web 门户相关联。要为您的受信任网络指定公有 IP 地址和 IP 地址范围，请向 IP 访问控制组添加规则。如果您的用户通过 NAT 网关或 VPN 访问其 Web 门户，您必须创建允许从 NAT 网关或 VPN 的公有 IP 地址发出的流量的规则。

> **Note**
>
> 客户有责任了解在使用 WorkSpaces 安全浏览器时可能出现的法律问题，并且必须确保他们在使用 WorkSpaces 安全浏览器时遵守所有适用的法律和法规。这包括规范雇主监控员工使用 WorkSpaces 安全浏览器的能力的法律，包括在应用程序中执行的活动。

主题


- 在 Amazon WorkSpaces 安全浏览器中创建 IP 访问控制组
- 将 IP 访问设置与 Amazon WorkSpaces 安全浏览器中的门户网站关联
- 在 Amazon WorkSpaces 安全浏览器中编辑 IP 访问控制组
- 在 Amazon WorkSpaces 安全浏览器中删除 IP 访问控制组


## 在 Amazon WorkSpaces 安全浏览器中创建 IP 访问控制组

要创建 IP 访问控制组，请按照以下步骤操作。

1. 打开 WorkSpaces 安全浏览器控制台，网址为https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/。
2. 在导航窗格中，选择 IP 访问控制。
3. 选择创建 IP 访问控制组。

4. 在创建 IP 访问控制组对话框中，输入该组的名称（必填项）和描述（可选项）。
5. 输入将与源关联的 IP 地址或 CIDR IP 范围，以及描述（可选）。
6. 在标签下，选择是否为每个 IP 访问控制组标记键值对。
7. 添加完规则和标签后，选择保存。

## 将 IP 访问设置与 Amazon WorkSpaces 安全浏览器中的门户网站关联

要将 IP 访问控制组与现有 Web 门户关联，请按照以下步骤操作。

1. 打开 WorkSpaces 安全浏览器控制台，网址为https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/。
2. 在导航窗格中，选择 Web 门户。
3. 选择 Web 门户，然后选择编辑。
4. 在 IP 访问控制组下，选择 Web 门户的 IP 访问控制组。
5. 选择保存。

要在创建新 Web 门户时关联 IP 访问控制组，请执行以下步骤。

1. 完成the section called “门户设置”中的步骤 1 到 4，以访问 IP 访问控制(可选)。
2. 选择创建 IP 访问控制。
3. 在创建 IP 组对话框中，输入组的名称（必填项）和描述（可选项）。
4. 输入将与源关联的 IP 地址或 CIDR IP 范围，以及描述（可选）。
5. 在标签下，选择是否为每个 IP 访问控制组标记键值对。
6. 添加完规则和标签后，选择创建 IP 访问控制。
7. 启动后，您的 IP 访问控制组将与此 Web 门户关联。

## 在 Amazon WorkSpaces 安全浏览器中编辑 IP 访问控制组

您可以随时从 IP 访问设置中删除规则。如果您删除了用于允许连接到 Web 门户的规则，则当前在进行会话的所有用户都将断开与 Web 门户的连接。

要编辑 IP 访问控制组，请按照以下步骤操作。

1. 打开 WorkSpaces 安全浏览器控制台，网址为https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/。

2. 在导航窗格中，选择 IP 访问控制。
3. 选择所需组，然后选择 Edit。
4. 编辑现有规则源和描述（可选），或添加其他规则。
5. 在标签下，选择是否为每个 IP 访问控制组标记键值对。
6. 添加完规则和标签后，选择保存。
7. 如果您更新了现有 IP 访问设置，请等待最多 15 分钟，以使新规则或编辑后的规则生效。

## 在 Amazon WorkSpaces 安全浏览器中删除 IP 访问控制组

您可以随时从 IP 访问控制组中删除规则。如果您删除了用于允许连接到 Web 门户的规则，则当前在进行会话的所有用户都将断开与 Web 门户的连接。

要删除 IP 访问控制组，请按照以下步骤操作。

1. 打开 WorkSpaces 安全浏览器控制台，网址为https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/。
2. 在导航窗格中，选择 IP 访问控制组。
3. 选择组，然后选择删除。

# 在 Amazon WorkSpaces 安全浏览器中管理单点登录扩展

您可以为最终用户启用扩展，以获得更好的门户登录体验。例如，如果您使用 Okta 作为门户的 SAML 2.0 身份提供者 (IdP)，并且还将其用作您希望用户在会话期间访问的网站的 IdP，则可以将 Okta 登录 Cookie 发送给使用扩展的会话。之后，当用户访问需要 Okta 域 Cookie 的网站时，他们无需在会话期间登录即可访问该网站。

Chrome 和 Firefox 浏览器均支持该扩展。该扩展支持登录会话的用户允许的域实现 Cookie 同步。该扩展无需用户登录，它可以在后台运行，无需用户在安装后采取任何操作即可实现 Cookie 同步。扩展不存储任何数据。

默认情况下，Chrome 的无痕窗口或 Firefox 私密浏览窗口未启用扩展。用户可以手动启用扩展。有关 Chrome 的更多信息，请参阅无痕模式下的扩展。有关 Firefox 的更多信息，请参阅私密浏览下的扩展。

当用户登录门户时，系统会提示他们安装扩展。有关该扩展的用户体验的详细信息，请参阅the section called “单点登录扩展”。

主题


- 在 Amazon WorkSpaces 安全浏览器中识别单点登录扩展程序的域名
- 在 Amazon WorkSpaces 安全浏览器中向新的门户网站添加单点登录扩展程序
- 在 Amazon WorkSpaces 安全浏览器中向现有门户网站添加单点登录扩展程序
- 在 Amazon WorkSpaces 安全浏览器中编辑或移除单点登录扩展程序


## 在 Amazon WorkSpaces 安全浏览器中识别单点登录扩展程序的域名

首先，确定您的 SAML IdP 和网站需要哪些域。您最多可添加 10 个域。

您有责任测试和确定要同步的 Cookie 的相应域。可能需要在 IdP 或网站身份验证级别进行更改，以确保单点登录按预期运行。

要了解最常见的 IdP 可使用哪些域，请参阅下表：

IdP 和域

| IdP | 域 |
| --- | --- |
| Okta | okta.com |
| Entra ID | microsoftonline.com |
| AWS Identity Center | awsapps.com |
| One Login | onelogin.com |
| Duo | duosecurity.com |

## 在 Amazon WorkSpaces 安全浏览器中向新的门户网站添加单点登录扩展程序

要在创建新的 Web 门户时支持使用扩展，请按照以下步骤操作。

1. 按照the section called “Web 门户创建”中的步骤进行操作，直到进入the section called “用户设置”。
2. 在the section called “用户设置”的第 1 步中的用户权限下，选择允许，为您的 Web 门户启用扩展。

3. 输入要进行 Cookie 同步的域，然后选择添加新域。
4. 完成the section called “用户设置”中的步骤和the section called “Web 门户创建”中的其余部分，创建您的 Web 门户。

## 在 Amazon WorkSpaces 安全浏览器中向现有门户网站添加单点登录扩展程序

要将扩展添加到现有 Web 门户，请按照以下步骤操作。

1. 在https://console.aws.amazon.com/workspaces-web/家中打开 WorkSpaces 安全浏览器控制台。
2. 选择要编辑的 Web 门户。
3. 选择用户设置、用户权限和允许，为您的 Web 门户启用扩展。
4. 输入要进行 Cookie 同步的域，然后选择添加新域。
5. 保存您的门户更改。门户将提示用户在 15 分钟内安装扩展。

## 在 Amazon WorkSpaces 安全浏览器中编辑或移除单点登录扩展程序

要编辑域或删除扩展，请按照以下步骤操作。

1. 在https://console.aws.amazon.com/workspaces-web/家中打开 WorkSpaces 安全浏览器控制台。
2. 选择要编辑的 Web 门户。
3. 选择用户设置、用户权限和不允许，为您的 Web 门户删除扩展。
4. 删除或编辑各个域。
5. 删除后，会话将不再同步 Cookie，即使用户的浏览器中安装了 WorkSpaces 安全浏览器扩展程序。

# 在 Amazon WorkSpaces 安全浏览器中设置 URL 过滤

您可以使用 Chrome 政策来筛选哪些 URLs 用户可以通过远程浏览器进行访问。Chrome 政策提供了两种过滤机制 URLs： URLAllowlist 和 URLBlocklist。您可以使用 WorkSpaces 安全浏览器控制台界面将 URL 过滤配置为门户设置，也可以将其添加为自定义 JSON 语句的一部分（在内联编辑器中或作为 JSON 文件上传）。

主题

- 在 Amazon WorkSpaces 安全浏览器中使用控制台设置 URL 过滤
- 使用 JSON 编辑器设置网址过滤，或者为 Amazon WorkSpaces 安全浏览器上传文件

## 在 Amazon WorkSpaces 安全浏览器中使用控制台设置 URL 过滤

要使用控制台设置 URL 筛选，请按照以下步骤操作。

1. 打开 WorkSpaces 安全浏览器控制台，网址为https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/。
2. 选择 “WorkSpaces 安全浏览器”、“门户网站”，选择您的 Web 门户，然后选择 “查看详细信息”。
3. 对于 URL 筛选，可以从以下选项中进行选择：
   - 允许所有人访问 URLs：默认情况下，门户网站允许所有人访问 URLs。可以将特定网站添加到 BlockURL 列表中，以防止用户在会话期间访问这些网站。例如，将 www.anycorp.com 添加到 BlockURL 列表将阻止用户在会话期间导航到 www.anycorp.com。
   - 禁止访问所有 URL URLs：默认情况下，门户网站会阻止对所有 URL 的访问。可以将特定网站添加到 URL 允许列表中，以整理用户可以访问的网站列表，并屏蔽任何其他网站的流量。考虑将每个 URL 添加为书签，以便用户在会话期间能够一键访问。
   - 高级配置：选择此选项可并行创建 allowURL 和 blockURL 列表。URL 允许名单的优先级高于 URL 禁止名单。选择此选项可按路径筛选 URL。例如，可以将 www.anycorp.com 添加到阻止列表，然后将 www.anycorp.com/hr 添加到允许列表。这允许用户访问 www.anycorp。 com/hr, but they won't be able to access other URL paths, such as www.anycorp.com/finance。

有关使用 “屏蔽” 和 “允许” 的更多指导 URLs，请参阅允许或阻止访问网站。按照 Chrome 的黑名单过滤器格式添加到 URLs 这些列表中，以获得最佳效果。有关更多信息，请参阅 URL 阻止列表筛选器格式。

## 使用 JSON 编辑器设置网址过滤，或者为 Amazon WorkSpaces 安全浏览器上传文件

要使用 JSON 编辑器或文件上传功能设置 URL 筛选，请按照以下步骤操作。

1. 在策略设置模块中，选择 JSON 编辑器，并绕过控制台 UI 模块以查看编辑器或文件上传视图。
   - 编辑器允许客户在控制台中内联创建自定义策略语句。在创建策略期间，编辑器会突出显示 JSON 语句中的错误。

- 借助文件上传功能，客户能够添加在控制台之外创建的 JSON 文件（例如从现有 Chrome 浏览器导出的 JSON 文件）。

2. 请参阅 Chrome 政策详情，了解 URLAllowlist URLBlocklist 并正确格式化您的门户网站的允许/拒绝网址列表。有关更多信息，请参阅URLAllowlist 和URLBlocklist。

# Amazon WorkSpaces 安全浏览器中的深度链接

当用户登录 WorkSpaces 安全浏览器时，他们将在管理员设置的主页上开始会话。您还可以允许门户在会话期间接收将用户连接到特定网站的深层链接。选择深层链接后，门户将显示深层链接中指定的 URL。该链接显示在为启动会话而配置的主页旁边，或者如果会话已在进行中，则该链接会单独显示。此功能允许管理员使用 WorkSpaces 安全浏览器创建更具动态性的用户体验。

深度链接在 WorkSpaces 安全浏览器会话中打开页面。如果会话已经在运行，它将在新选项卡中打开深层链接。如果会话尚未运行，它将在新选项卡中打开深层链接 URL，在单独的选项卡中打开门户默认主页。如果深层链接包含多个 URL，它将首先显示深层链接 URL，并在单独的选项卡中打开每个后续 URL（包括默认主页）。

主题


- 在 Amazon WorkSpaces 安全浏览器中设置深度链接
- 在 Amazon WorkSpaces 安全浏览器中对深度链接使用网址过滤


## 在 Amazon WorkSpaces 安全浏览器中设置深度链接

要允许访问深层链接，请在创建用户设置时选择允许。您想要深层链接的网站必须经过 URL 编码。例如，将用户链接到 “https://www.example.com/？ query=true”，更新指向 %2F%3Fquery%3DTrue 的链接。 https%3A%2F%2Fwww.example.com

一个深度链接最多可以包含 10 个 URLs，用逗号分隔。例如：

https://<uuid>.workspaces-web.com/？deepLinks= %2F%3fquery%3DTrue，%2F%3fquery %3DTrue2，%2F%3fquery%3DTrue3，%2F%3Fquery%3fquery%3DTr https%3A%2F %2Fwww.example.com ue4。https%3A%2F%2Fwww.example.com https%3A%2F %2Fwww.example.com https%3A%2F%2Fwww.example.com

有关允许深层链接的更多信息，请参阅the section called “用户设置”。

## 在 Amazon WorkSpaces 安全浏览器中对深度链接使用网址过滤

您与之共享此门户链接的任何用户都可以操纵深层链接值来访问网站，但前提是，该域可以从门户访问并且不在 URL 阻止列表中。要创建限制性允许列表或阻止列表以防止用户通过您的门户访问非预期的域，请使用 URL 筛选。

可以在门户的浏览器设置中使用 URL 筛选来编辑门户的允许列表和阻止列表。<uuid>为此，请按以下格式将网址附加到允许名单的门户网址，其中 UUID 是门户 ID：https: //.workspaces-web.com/？deepLinks= %2F%3Fquery%3DTrue https%3A%2F%2Fwww.example.com

有关更多信息，请参阅the section called “设置 URL 筛选”和允许或阻止访问网站。

# 使用 Amazon WorkSpaces 安全浏览器中的会话管理控制面板

使用 WorkSpaces 安全浏览器控制台上的会话管理仪表板来监控和管理活动和已完成的会话。

## 控制面板访问

要访问控制面板，请按照以下步骤操作。

要访问控制面板，请执行以下步骤：

1. 打开 WorkSpaces 安全浏览器控制台，网址为https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/。
2. 选择WorkSpaces 安全浏览器、Web 门户，然后选择您的 Web 门户。
3. 选择会话选项卡或选择查看会话，在下面的拆分面板中打开控制面板。

## 控制面板筛选器

在会话面板中，您可以按以下属性或值筛选会话：

- 状态
  - 活动 - 表示会话当前正在运行。要终止会话，请参阅下文。
  - 已终止 - 表示会话不再处于活动状态。
- 会话 ID
- 用户名
- 会话开始时间

## 终止会话

要终止会话，请按照以下步骤操作。

要终止会话，请执行以下步骤：

1. 在会话控制面板上，选择要停止的会话。
2. 选择终止。
3. 已断开连接的用户将失去会话的所有状态。所有打开的选项卡、浏览器历史记录和下载到安全浏览器的文件都将被回收。

## 会话历史记录

控制面板包含过去 35 天的会话。无论有没有筛选器，都可以使用 CLI 列出会话。会话历史记录以 JSON 格式提供，管理员可以对其进行处理、管理，并将其存储在单独的存储库中。

以下是在 US-West-2（俄勒冈州）区域管理会话的 CLI 命令示例。

要列出 Web 门户的所有会话，请运行以下命令：

```
aws workspaces-web list-sessions --portal-arn arn:aws:workspaces-web:us-west-2:<accountId>:portal/<portalId>
```

要列出 Web 门户特定用户的所有会话，请运行以下命令：

```
aws workspaces-web list-sessions --portal-arn arn:aws:workspaces-web:us-west-2:<accountId>:portal/<portalId> --username <username>
```

# 使用 FIPS 终端节点和 Amazon WorkSpaces 安全浏览器保护传输中的数据

默认情况下，当您以管理员身份使用控制台、 AWS 命令行界面 (AWS CLI) 或 AWS SDK 与 WorkSpaces 安全浏览器服务通信时，或者在用户会话期间，所有传输中的数据都使用 TLS 1.2 进行加密。

如果在通过命令行界面或 API 访问 AWS 时需要经过 FIPS 140-3 验证的加密模块，请使用 FIPS 端点。当您使用 FIPS 端点时，所有传输中数据都会使用符合联邦信息处理标准（FIPS）140-3 的加

密标准进行加密。有关 FIPS 端点的信息，包括 WorkSpaces 安全浏览器端点列表，请参阅https://aws.amazon.com/compliance/fips。

使用 FIPS 端点创建门户后，将使用 FIPS 140-3 端点自动进行所有用户会话和管理更改。您可以使用 `AWS_USE_FIPS_ENDPOINT=true` 环境变量来找到 FIPS 端点并通过 SDK 发送请求。示例如下：

```
$ export AWS_USE_FIPS_ENDPOINT=true
$ aws workspaces-web list-portal
```

您也可以使用 `–endpoint-url` 选项将请求直接发送到 FIPS 端点。以下是 US-West-2（俄勒冈州）区域的调用列表门户示例：

```
$ aws workspaces-web list-portal --endpoint-url https://workspaces-web-fips.us-
west-2.amazonaws.com
```

# 在 Amazon WorkSpaces 安全浏览器中管理数据保护设置

数据保护设置用于帮助防止数据在会话期间被共享。可以创建设置并将其应用于多个门户。

主题


- Amazon WorkSpaces 安全浏览器中的内联数据编辑
- Amazon WorkSpaces 安全浏览器中的默认编辑配置
- Amazon WorkSpaces 安全浏览器中的基本内联修改
- Amazon WorkSpaces 安全浏览器中的自定义内联修改
- 在 Amazon WorkSpaces 安全浏览器中创建数据保护设置
- 在 Amazon WorkSpaces 安全浏览器中关联数据保护设置
- 在 Amazon WorkSpaces 安全浏览器中编辑数据保护设置
- 删除 Amazon WorkSpaces 安全浏览器中的数据保护设置


## Amazon WorkSpaces 安全浏览器中的内联数据编辑

通过向门户网站添加内联数据密文，您可以自动预测和编辑网页中显示的一串文本中的某些数据。您可以通过从内置模式（例如社会保险号或信用卡号）中进行选择来创建密文政策，也可以使用正则表达式

和关键字创建自己的自定义数据类型。策略包括可配置的执行级别和对应在 URLs 何处实施编辑的控制措施。

以下组件决定何时对数据进行编辑：

- 数据保护设置-数据保护设置是包含您的数据类型和强制标准的资源的名称。要使用此资源，请先创建您的设置，然后将其与门户关联。当用户启动会话时，您的设置将在会话期间强制执行。
- 会话内浏览器扩展程序-当您将密文设置与门户关联时，会话浏览器将使用系统强制执行的浏览器扩展程序启动，该扩展程序会强制执行您的设置。数据保护设置根据您的置信度和 URL 强制配置通过模式匹配（正则表达式）和关键字搜索来强制执行密文。内容是根据文本字符串预测出来的，然后再显示在屏幕上。该扩展程序还设置了相关的浏览器政策，以控制用户绕过密文的能力（例如禁用隐私浏览、访问开发者工具和网络检查）。

以下 Chrome 浏览器政策变更由会话内浏览器扩展程序强制执行。有关更多信息，请参阅 Chrome 企业版策略列表。

- 强制执行浏览器政策，防止用户在不进行密文的情况下查看会话：
  - IncognitoModeAvailability = 1
  - DeveloperToolsAvailability = 2
  - BrowserAddPersonEnabled= false
  - BrowserGuestModeEnabled= false
- 该扩展程序还通过取消下载事件来防止用户从 URLs 强制执行数据保护设置的 HTML 文件中下载。

通常，您应该对私密的结构化网站（例如您的客户管理工具、票务系统或维基）使用修改，而不是用于非结构化的公共浏览（例如Facebook或Google）。您可以从内置数据类型中进行选择（完整列表见下文），也可以使用自己的正则表达式值和关键字定义自定义数据类型。管理员负责测试和验证每种数据类型、置信度和 URL 强制措施是否按预期运行。 AWS 无法保证与第三方提供的自定义网站或应用程序兼容。

WorkSpaces Secure Browser 目前不支持以非文本格式编辑支持或自定义的数据类型，包括以下格式的文本：

- 图片，例如 JPEG、PNG 或 GIF
- 允许用户使用动态文字处理或编辑功能的网页，例如 Google 文档或表格
- 在浏览器中访问的音频或视频流，例如 YouTube 视频
- PDFs 通过 Chrome 浏览器查看

请勿对不支持的格式的内容使用密文。管理员负责验证网站和内容的兼容性，然后才授予用户访问他们打算编辑的内容的权限。

## Amazon WorkSpaces 安全浏览器中的默认编辑配置

默认的密文配置将自动对数据保护设置中的所有内置数据类型应用置信度和 URL 强制执行。添加内置数据类型时，您可以选择覆盖默认配置。

置信级别允许您使用格式、关键字和未格式化文本的组合来微调内置数据类型的密文逻辑。选择应用密文的严格程度，包括 “高”、“中” 或 “低”。除非在数据类型级别应用替代，否则默认值将适用于所有数据类型。通常，从默认配置为 “中” 开始，然后通过验证您的网站是否按预期强制执行编辑来进行完善。

| 信心等级 | 描述 | 示例 |
| --- | --- | --- |
| 高 | 需要格式化的文本模式匹配才能对内容进行编辑。 | 123-45-6798 的 SSN 将被编辑，而 123456789 不会。 |
| 中 | Redaction 同时考虑格式化和未格式化的文本，并在逻辑中添加关联的关键字。 | 123-45-6798的SSN将被删除。如果在关键词（例如 “社会安全号码”）附近检测到123456789，则会被编辑。 |
| 低 | 对两种格式化模式和不带关键字的未格式化模式都强制执行密文。 | 无论哪种格式（123-45-6798 和 123456789）的 SSN 都是在不需要关键字的情况下进行编辑的。 |

您必须为所有数据类型设置默认的密文配置。可从以下选项中进行选择：

- 全部 URLs
- 具体 URLs
- 高级配置

除非在数据类型级别应用替代，否则默认值将适用于所有数据类型。网址强制使用与 Chrome 政策类似的逻辑来管理允许名单和屏蔽名单。有关使用阻止和允许的指导 URLs，请参阅允许或阻止访问网站。 URLs 要获得最佳效果，请按照 Chrome 的黑名单过滤器格式添加到这些列表中。有关更多信息，请参阅 URL 阻止列表筛选器格式。

# Amazon WorkSpaces 安全浏览器中的基本内联修改

内联数据编辑支持内置模式（例如社会保险号和信用卡号），您可以在基本内联密文下找到这些模式。从下拉菜单中选择数据类型，然后为每种数据类型指定替换值。所有数据类型都遵循上面的默认配置强制模式，但您可以选择覆盖置信度，并微调每种数据类型的域强制模式。

要输入默认配置中的替代值，请选择置信度覆盖。例如，将默认配置设置为 “中” 时，您可能会在测试期间注意到其中一种数据类型未经过可靠编辑。您可以将覆盖设置为 “低” 以增加密文的机会，而无需调整用于其他数据类型的逻辑。

要在 URLs 不更改默认配置的情况下微调密文的应用方式，请应用网址强制覆盖。例如，您可以设置使用网址覆盖来强制在客户关系管理系统中删除电子邮件地址，而不会中断用户对公司目录网站或基于 Web 的电子邮件中的电子邮件地址的访问权限。

以下是数据类型及其相应的内置模式的列表 IDs：

| builtInPattern我是 | 数据类型 |
| --- | --- |
| awsAccessKey: | AWS 访问密钥 |
| awsSecretKey: | AWS 密钥 |
| 卡号： | 信用卡号 |
| 加密： | 加密货币地址 |
| cusipNum： | CUSIP 号码 |
| 日期: | 日期 |
| Deanum： | 美国缉毒局的数字 |
| dob: | 出生日期 |
| 驾驶执照： | 美国驾照 |
| 电子邮件地址： | 电子邮件地址 |
| ein: | 美国雇主识别号 |
| 截止日期: | 信用卡到期日期 |

| builtInPattern我是 | 数据类型 |
| --- | --- |
| healthInsuranceNum: | Medicare Health 保险索赔编号 |
| HipaCode: | HIPAA ICD-10 代码 |
| indivTaxId: | 美国个人税号 |
| iPaddr： | IP 地址 |
| isin: | 国际证券识别码 |
| 智威汤逊: | JSON Web 令牌 |
| 位置坐标： | 位置坐标 |
| macAddr： | MAC 地址 |
| medicareBeneficiaryId: | 医疗保险受益人号码 |
| npi: | 国家提供者识别码 |
| ndc： | 国家药品法规 (NDC) |
| PassportNum: | 美国护照号码 |
| phoneNum: | 电话号码 |
| 路由号码： | ABA 路由号码 |
| ssn: | 美国社会安全号码 |
| SwiftCode： | 斯威夫特代码 |
| 时间: | Time |
| vin: | 美国车辆识别码 |

## Amazon WorkSpaces 安全浏览器中的自定义内联修改

客户可以使用正则表达式定义自己的模式，例如自定义内部应用程序 IDs。要创建您的自定义内联密文模式，请按照以下步骤操作：

1. 转到您的数据保护设置。
2. 选择 “自定义内嵌密文” 并添加。
3. 输入自定义数据类型的名称。
4. 输入您的正则表达式值。
   - 正则表达式的值必须与 JavaScript 正则表达式的字面语法相匹配。有关详细信息，请参阅正则表达式。正则表达式的示例是`/ex[am]+ple/i`。
   - 请务必在您计划支持的网站上测试您的自定义模式。如果编写的自定义模式存在错误，则可能会引入意想不到的性能问题。
5. 指定重置价值。
6. 选择 “更多选项” 可获得更多可选的自定义设置，包括以下内容：
   - 添加关键字以微调密文逻辑。关键字可以提高执法的准确性。在 Javascript 正则表达式文字语法中添加关键字。有关详细信息，请参阅正则表达式。

     例如，如果您要为内部系统中 IDs 使用的客户端创建自定义密文模式，则可以向关键字字段中添加`/client name/i`内容以通知扫描和检测逻辑。
   - 在不更改默认配置的情况下，应用网址强制覆盖来微调密文的应用方式。 URLs

     例如，您可以设置使用网址覆盖来强制客户关系管理系统中的电子邮件地址密文，而不会中断用户对公司目录网站或基于 Web 的电子邮件中的电子邮件地址的访问权限。
   - 输入数据类型的描述（可选）。

## 在 Amazon WorkSpaces 安全浏览器中创建数据保护设置

您可以在 WorkSpaces 安全浏览器中创建数据保护设置。

创建数据保护设置

1. 打开 WorkSpaces 安全浏览器控制台，网址为https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/。
2. 在左侧导航窗格中，选择数据保护设置。
3. 选择 “创建数据保护设置”。

4. 输入设置的显示名称（必填）和描述（可选）。
5. 选择内嵌密文的默认设置。您可以设置以下内容：
   - 所有数据类型的严格程度
   - 应强制执行密文的域名
6. 从支持的类型中选择您的基本内联密文数据类型，或者创建自定义数据类型。您可以为每种数据类型设置替代，包括严格级别和域异常。
7. 为报告添加任何标签（可选）。
8. 完成此操作后，选择Save（保存）。

## 在 Amazon WorkSpaces 安全浏览器中关联数据保护设置

您可以在 WorkSpaces 安全浏览器中关联数据保护设置。

将数据保护设置与现有门户关联

1. 打开 WorkSpaces 安全浏览器控制台，网址为https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/。
2. 在左侧导航窗格中，选择 Web 门户。
3. 选择 Web 门户，然后选择编辑。
4. 在数据保护设置下，选择门户的设置。
5. 选择保存。

要在创建新门户时关联数据保护设置，请执行以下步骤。

在创建新入口时关联数据保护设置

1. 按照中的the section called “Web 门户创建”说明创建门户，直到进入数据保护设置。
2. 从下拉菜单中选择您的数据保护设置。
3. 完成中的步骤the section called “Web 门户创建”以完成门户的创建。

要在创建新门户时创建数据保护设置，请执行以下步骤。

在创建新入口时创建数据保护设置

1. 按照中的the section called “Web 门户创建”说明创建门户，直到进入数据保护设置。

2. 从下拉菜单中选择数据保护设置。
3. 输入设置的显示名称（必填）和描述（可选）。
4. 选择内嵌密文的默认设置。您可以设置以下内容：
   - 所有数据类型的严格程度
   - 应强制执行密文的域名
5. 从支持的类型中选择您的基本内联密文数据类型，或者创建自定义数据类型。您可以为每种数据类型设置替代，包括严格级别和域异常。
6. 为报告添加任何标签（可选）。
7. 完成此操作后，选择Save（保存）。
8. 选择 “数据保护设置” 下的 “刷新” 按钮，然后从下拉菜单中选择您的数据保护设置。
9. 继续按照创建门户说明完成门户的创建。

## 在 Amazon WorkSpaces 安全浏览器中编辑数据保护设置

您可以在 WorkSpaces 安全浏览器中编辑数据保护设置。

编辑数据保护设置

1. 打开 WorkSpaces 安全浏览器控制台，网址为https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/。
2. 从列表视图中选择要编辑的数据保护设置和数据保护设置。
3. 您可以更新名称、描述、默认设置、数据类型（支持或自定义），并应用置信度或域覆盖。
4. 选择保存。

## 删除 Amazon WorkSpaces 安全浏览器中的数据保护设置

您可以在 WorkSpaces 安全浏览器中删除数据保护设置。

删除数据保护设置

1. 如果您的入口与数据保护设置关联，则必须先移除关联，然后才能删除数据保护设置。
2. 打开 WorkSpaces 安全浏览器控制台，网址为https://console.aws.amazon.com/workspaces-web/home?region=us-east-1#/。
3. 从列表视图中选择数据保护设置和要删除的数据保护设置。

4. 选择删除。

# 在 Amazon WorkSpaces 安全浏览器中管理工具栏控件

使用工具栏控件，您可以为最终用户会话配置工具栏显示方式，包括以下选项：

- 功能
  - 剪贴板：启用后，允许使用精细控件进行复制/粘贴（仅限复制、仅粘贴或两者兼而有之）。禁用后，将隐藏图标并禁止在工具栏上使用。
  - 文件传输：启用后，允许使用精细控制进行文件操作（仅上传、仅下载或两者兼而有之）。禁用后，隐藏图标并阻止传输。
  - 麦克风：启用后，允许使用麦克风。禁用后，隐藏图标。
  - 摄像头：启用后，允许使用摄像头。禁用后，隐藏图标。
  - 双显示器：启用后，允许使用双显示器。禁用后，隐藏图标。
  - 全屏：启用后，允许全屏模式。禁用后，隐藏图标。
  - Windows：启用后，允许在窗口之间移动。禁用后，隐藏图标。
- 设置
  - 工具栏主题：控制浅色或深色模式的显示。配置会移除最终用户主题控件。
  - 工具栏状态：设置工具栏的停靠或分离状态。配置取消了最终用户对工具栏状态的控制。
  - 最大分辨率：定义允许的最高显示分辨率。用户只能选择不超过此定义限制的分辨率。

# Amazon WorkSpaces 安全浏览器中的安全

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。责任共担模式将此描述为云的安全性和云中的安全性：

- 云安全 — AWS 负责保护在 AWS 云中运行 AWS 服务的基础架构。 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。要了解适用于亚马逊 WorkSpaces 安全浏览器的合规计划，请参阅按合规计划划分的 AWS 范围内的服务 AWS 按合规计划。
- 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、您公司的要求以及您的数据适用的任何法律法规。

本文档可帮助您了解在使用 Amazon WorkSpaces 安全浏览器时如何应用责任共担模型。它向您展示了如何配置 Amazon WorkSpaces 安全浏览器以实现您的安全和合规目标。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 WorkSpaces 安全浏览器资源。

内容


- Amazon WorkSpaces 安全浏览器中的数据保护
- 适用于亚马逊 WorkSpaces 安全浏览器的身份和访问管理
- Amazon WorkSpaces 安全浏览器中的事件响应
- Amazon WorkSpaces 安全浏览器的合规性验证
- Amazon WorkSpaces 安全浏览器的弹性
- Amazon 安全浏览器中的基础设施 WorkSpaces 安全
- Amazon WorkSpaces 安全浏览器中的配置和漏洞分析
- APIs 使用接口 VPC 终端节点进行访问 (AWS PrivateLink)
- Amazon 安全浏览器的 WorkSpaces 安全最佳实践


## Amazon WorkSpaces 安全浏览器中的数据保护

责任 AWS 共担模式适用于亚马逊 WorkSpaces 安全浏览器中的数据保护。如本模型所述 AWS ，负责保护运行所有内容的全球基础架构 AWS Cloud。您负责维护对托管在此基础结构上的内容的控制。

您还负责您所使用的 AWS 服务 的安全配置和管理任务。有关数据隐私的更多信息，请参阅数据隐私常见问题。有关欧洲数据保护的信息，请参阅 AWS Security Blog 上的 AWS Shared Responsibility Model and GDPR 博客文章。

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

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

强烈建议您切勿将机密信息或敏感信息（如您客户的电子邮件地址）放入标签或自由格式文本字段（如名称字段）。这包括您使用控制台、 AWS CLI API 或 AWS 服务 使用 WorkSpaces 安全浏览器或其他浏览器时 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。如果您向外部服务器提供网址，强烈建议您不要在网址中包含凭证信息来验证对该服务器的请求。

主题


- Amazon WorkSpaces 安全浏览器中的数据加密
- Amazon WorkSpaces 安全浏览器中的网络间流量隐私
- 在 Amazon WorkSpaces 安全浏览器中登录用户访问权限


## Amazon WorkSpaces 安全浏览器中的数据加密

Amazon S WorkSpaces ecure Browser 收集门户自定义数据，例如浏览器设置、用户设置、网络设置、身份提供者信息、信任存储数据和信任存储证书数据。 WorkSpaces 安全浏览器还收集浏览器策

略数据、用户首选项（用于浏览器设置）和会话日志。收集的数据存储在亚马逊 DynamoDB 和亚马逊 S3 中。 WorkSpaces 安全浏览器 AWS Key Management Service 用于加密。

要保护您的内容，请遵循以下指南进行操作：

- 实现最低权限访问权限并创建用于 WorkSpaces 安全浏览器操作的特定角色。使用 IAM 模板创建完全访问权限角色或只读角色。有关更多信息，请参阅 AWS WorkSpaces 安全浏览器的托管策略。
- 通过提供客户管理的密钥来端到端地保护数据，这样 WorkSpaces Secure Browser 就可以使用您提供的密钥对您的静态数据进行加密。
- 请谨慎共享门户域和用户凭证：
  - 管理员需要登录 Amazon WorkSpaces 控制台，用户必须登录 WorkSpaces 安全浏览器门户。
  - Internet 上的任何人都可以访问 Web 门户，但除非他们拥有有效的门户用户凭证，否则他们无法启动会话。
- 用户可以通过选择结束会话来明确结束自己的会话。这会丢弃托管浏览器会话的实例，从而导致浏览器隔离。

WorkSpaces 默认情况下，Secure Browser 通过加密所有敏感数据来保护内容和元数据。 AWS KMS 它收集浏览器策略和用户首选项，以便在 WorkSpaces 安全浏览器会话期间强制执行策略和设置。如果应用现有设置时出现错误，则用户无法访问新会话，也无法访问公司的内部网站和 SaaS 应用程序。

## Amazon WorkSpaces 安全浏览器的静态加密

静态加密是默认配置的， WorkSpaces 安全浏览器中使用的所有客户数据（例如，浏览器策略声明、用户名、日志记录或 IP 地址）均使用 AWS KMS进行加密。默认情况下， WorkSpaces 安全浏览器启用使用 AWS自有密钥进行加密。您也可以通过在创建资源时指定您的 CMK 来使用客户托管密钥 (CMK)。这是当前唯一通过 CLI 支持的类型。

如果您选择传递 CMK，则提供的密钥必须是对称加密 AWS KMS 密钥，并且作为管理员，您必须具有以下权限：

```
kms:DescribeKey

kms:GenerateDataKey

kms:GenerateDataKeyWithoutPlaintext

kms:Decrypt

kms:ReEncryptTo
```

```
kms:ReEncryptFrom
```

如果您使用 CMK，则需要将 WorkSpaces 安全浏览器外部服务主体列入许可名单才能访问密钥。有关更多信息，请参阅 aw s 的作用域 CMK 密钥策略示例：SourceAccount

只要有可能， WorkSpaces 安全浏览器就会使用正向访问会话 (FAS) 凭据来访问您的密钥。有关 FAS 的更多信息，请参阅转发访问会话。
在某些情况下， WorkSpaces 安全浏览器可能需要异步访问您的密钥。通过在密钥策略中列入 WorkSpaces 安全浏览器外部服务主体许可名单， WorkSpaces 安全浏览器将能够使用您的密钥执行列入许可名单的一组加密操作。

创建资源后，无法再删除或更改密钥。如果您使用了 CMK，则作为访问该资源的管理员，您必须具有以下权限：

```
kms:GenerateDataKey
kms:GenerateDataKeyWithoutPlaintext
kms:Decrypt

kms:ReEncryptTo
kms:ReEncryptFrom
```

如果您在使用控制台时看到访问被拒绝错误，则可能表明访问控制台的用户不具备针对正在利用的密钥使用 CMK 所需的权限。

WorkSpaces 安全浏览器的关键策略和范围界定示例

CMKs 需要以下密钥策略：

```
{
  "Version": "2012-10-17",
  "Statement": [
  ...,
    {
      "Sid": "Allow WorkSpaces Secure Browser to encrypt/decrypt",
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces-web.amazonaws.com"
      },
      "Action": [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
```

```
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
       ],
      "Resource": "*",
      }
    ]
}
```

WorkSpaces 安全浏览器需要以下权限：

- `kms:DescribeKey`— 验证提供的 AWS KMS 密钥配置是否正确。
- `kms:GenerateDataKeyWithoutPlaintext`和 `kms:GenerateDataKey` — 请求 AWS KMS 密钥以创建用于加密对象的数据密钥。
- `kms:Decrypt`— 请求 AWS KMS 密钥以解密加密的数据密钥。这些数据密钥用于加密您的数据。
- `kms:ReEncryptTo`和 `kms:ReEncryptFrom` — 请求 AWS KMS 密钥以允许从 KMS 密钥重新加密或向 KMS 密钥重新加密。

为您的密钥设定 WorkSpaces 安全浏览器的 AWS KMS 权限范围

当密钥策略声明中的委托人是AWS 服务委托人时，除了加密上下文之外，我们强烈建议您使用 a ws: SourceArn 或 aws: SourceAccount 全局条件密钥。

用于资源的加密上下文将始终包含 `aws:workspaces-web:RESOURCE_TYPE:id` 格式的条目和相应的资源 ID。

只有当请求 AWS KMS 来自其他 AWS 服务时，来源 ARN 和来源账户值才会包含在授权上下文中。这种条件的组合实施最低权限，避免了潜在的混淆代理情况。有关更多信息，请参阅密钥策略中的 AWS 服务权限。

```
   "Condition": {
        "StringEquals": {
          "aws:SourceAccount": "AccountId",
          "kms:EncryptionContext:aws:workspaces-web:resourceType:id": "resourceId"
        },
        "ArnEquals": {
          "aws:SourceArn": [
            "arn:aws:workspaces-web:Region:AccountId:resourceType/resourceId"
          ]
        },
```

```
    }
```

> **Note**
>
> 在创建资源之前，密钥策略应仅使用 `aws:SourceAccount` 条件，因为完整的资源 ARN 尚不存在。创建资源后，可以更新密钥策略以包含 `aws:SourceArn` 和 `kms:EncryptionContext` 条件。

### 带有 **`aws:SourceAccount`** 的范围限定的 CMK 密钥策略示例

```
{
  "Version": "2012-10-17",
  "Statement": [
  ...,
    {
      "Sid": "Allow WorkSpaces Secure Browser to encrypt/decrypt",
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces-web.amazonaws.com"
      },
      "Action": [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
       ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "<AccountId>"
        }
      }
    }
  ]
}
```

### 带 **`aws:SourceArn`** 和资源通配符的范围限定的 CMK 密钥策略示例

```
{
```

```
  "Version": "2012-10-17",
  "Statement": [
  ...,
    {
      "Sid": "Allow WorkSpaces Secure Browser to encrypt/decrypt",
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces-web.amazonaws.com"
      },
      "Action": [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
       ],
      "Resource": "*",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": "arn:aws:workspaces-web:<Region>:<AccountId>:*/*"
        }
      }
    }
  ]
}
```

### 带有 **aws:SourceArn** 的范围限定的 CMK 密钥策略示例

```
{
  "Version": "2012-10-17",
  "Statement": [
  ...,
    {
      "Sid": "Allow WorkSpaces Secure Browser to encrypt/decrypt",
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces-web.amazonaws.com"
      },
      "Action": [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
```

```
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
       ],
      "Resource": "*",
      "Condition": {
        "ArnLike": {
          "aws:SourceArn": [
            "arn:aws:workspaces-web:<Region>:<AccountId>:portal/*",
            "arn:aws:workspaces-web:<Region>:<AccountId>:browserSettings/*",
            "arn:aws:workspaces-web:<Region>:<AccountId>:userSettings/*",
            "arn:aws:workspaces-web:<Region>:<AccountId>:ipAccessSettings/*"
          ]
        }
    }
  ]
}
```

> **Note**
>
> 创建资源后，您可以在 SourceArn 中更新其通配符。如果您使用 WorkSpaces 安全浏览器创建需要 CMK 访问权限的新资源，请确保相应地更新其密钥策略。

### 带 **aws:SourceArn** 和资源特定的 **EncryptionContext** 的范围限定的 CMK 密钥策略示例

```
{
  "Version": "2012-10-17",
  "Statement": [
  ...,
    {
      "Sid": "Allow WorkSpaces Secure Browser to encrypt/decrypt portal",
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces-web.amazonaws.com"
      },
      "Action": [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:ReEncryptTo",
```

```
        "kms:ReEncryptFrom"
       ],
      "Resource": "*",
      "Condition": {
        "StringEquals": {
            "aws:SourceAccount": "<AccountId>",
            "kms:EncryptionContext:aws:workspaces-web:portal:id": "<portalId>>"
        }
      }
    },
    {
      "Sid": "Allow WorkSpaces Secure Browser to encrypt/decrypt userSettings",
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces-web.amazonaws.com"
      },
      "Action": [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
       ],
      "Resource": "*",
      "Condition": {
         "StringEquals": {
            "aws:SourceAccount": "<AccountId>",
            "kms:EncryptionContext:aws:workspaces-web:userSetttings:id":
 "<userSetttingsId>"
        }
      }
    },
    {
      "Sid": "Allow WorkSpaces Secure Browser to encrypt/decrypt browserSettings",
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces-web.amazonaws.com"
      },
      "Action": [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
```

```
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
       ],
      "Resource": "*",
      "Condition": {
         "StringEquals": {
            "aws:SourceAccount": "<AccountId>",
            "kms:EncryptionContext:aws:workspaces-web:browserSettings:id":
 "<browserSettingsId>"
        }
      }
    },
    {
      "Sid": "Allow WorkSpaces Secure Browser to encrypt/decrypt ipAccessSettings",
      "Effect": "Allow",
      "Principal": {
        "Service": "workspaces-web.amazonaws.com"
      },
      "Action": [
        "kms:DescribeKey",
        "kms:GenerateDataKey",
        "kms:GenerateDataKeyWithoutPlaintext",
        "kms:Decrypt",
        "kms:ReEncryptTo",
        "kms:ReEncryptFrom"
       ],
      "Resource": "*",
      "Condition": {
         "StringEquals": {
            "aws:SourceAccount": "<AccountId>",
            "kms:EncryptionContext:aws:workspaces-web:ipAccessSettings:id":
 "<ipAccessSettingsId>"
        }
      }
    },
  ]
}
```

> **Note**
>
> 在针对同一密钥策略包含资源特定的 `EncryptionContext` 时，请确保创建单独的语句。有关更多信息，请参阅 context-key 下 kms:EncryptionContext的 “使用多个加密上下文对” 部分。

### Amazon WorkSpaces 安全浏览器正在进行加密

WorkSpaces 安全浏览器对通过 HTTPS 和 TLS 1.2 传输的数据进行加密。您可以使用控制台向发送请求，也可以直接调用 API。 WorkSpaces 通过 HTTPS 或 TLS 连接发送所有内容，以此对传输的请求数据进行加密。请求数据可以从 AWS 控制台或 AWS SDK 传输到 WorkSpaces 安全浏览器。 AWS Command Line Interface

默认配置传输中的加密，默认配置安全连接（HTTPS、TLS）。

### Amazon WorkSpaces 安全浏览器的密钥管理

您可以提供自己的客户管理 AWS KMS 密钥来加密您的客户信息。如果您不提供密钥， WorkSpaces 安全浏览器将使用 AWS 自有密钥。您可以使用 AWS SDK 设置密钥。

## Amazon WorkSpaces 安全浏览器中的网络间流量隐私

为了保护 WorkSpaces 安全浏览器和本地应用程序之间的连接，您可以使用 WorkSpaces 安全浏览器在自己的 VPC 内启动浏览器会话。与本地应用程序的连接是在您自己的 VPC 中配置的，不受 WorkSpaces 安全浏览器控制。

为了保护账户之间的连接， WorkSpaces Secure Browser 使用与服务相关的角色来安全地连接到客户帐户并代表客户运行操作。有关更多信息，请参阅 在 Amazon WorkSpaces 安全浏览器中使用服务相关角色。

## 在 Amazon WorkSpaces 安全浏览器中登录用户访问权限

管理员可以记录 WorkSpaces 安全浏览器会话事件，包括开始、停止和 URL 访问。这些日志经过加密，并通过 Amazon Kinesis Data Streams 安全地传送给客户。来自用户访问日志记录的浏览信息不会由未配置日志记录的会话存储 AWS，也不会从会话中获取。隐身模式下的 URL 访问或 URLs 从浏览器历史记录中删除的 URL 访问不会记录在用户访问日志中。

# 适用于亚马逊 WorkSpaces 安全浏览器的身份和访问管理

AWS Identity and Access Management (IAM) AWS 服务 可帮助管理员安全地控制对 AWS 资源的访问权限。IAM 管理员控制谁可以进行身份验证（登录）和授权（有权限）使用 WorkSpaces 安全浏览器资源。您可以使用 IAM AWS 服务 ，无需支付额外费用。

主题

- 受众
- 使用身份进行身份验证
- 使用策略管理访问
- Amazon WorkSpaces 安全浏览器如何与 IAM 配合使用
- Ama WorkSpaces zon 安全浏览器的基于身份的策略示例
- AWS WorkSpaces 安全浏览器的托管策略
- 对 Amazon WorkSpaces 安全浏览器身份和访问进行故障排除
- 在 Amazon WorkSpaces 安全浏览器中使用服务相关角色


## 受众

您的使用方式 AWS Identity and Access Management (IAM) 会有所不同，具体取决于您在 WorkSpaces 安全浏览器中所做的工作。

服务用户-如果您使用 WorkSpaces 安全浏览器服务完成工作，则您的管理员会为您提供所需的凭据和权限。当你使用更多的 WorkSpaces 安全浏览器功能来完成工作时，你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。如果您无法在 WorkSpaces 安全浏览器中访问某项功能，请参阅对 Amazon WorkSpaces 安全浏览器身份和访问进行故障排除。

服务管理员-如果您负责公司的 WorkSpaces 安全浏览器资源，则可能拥有对 WorkSpaces 安全浏览器的完全访问权限。您的工作是确定您的服务用户应访问哪些 WorkSpaces 安全浏览器功能和资源。然后，您必须向 IAM 管理员提交请求以更改服务用户的权限。请查看该页面上的信息以了解 IAM 的基本概念。要详细了解贵公司如何将 IAM 与 WorkSpaces 安全浏览器一起使用，请参阅Amazon WorkSpaces 安全浏览器如何与 IAM 配合使用。

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对 WorkSpaces 安全浏览器的访问权限。要查看您可以在 IAM 中使用的基于身份 WorkSpaces 的安全浏览器策略示例，请参阅。Ama WorkSpaces zon 安全浏览器的基于身份的策略示例

## 使用身份进行身份验证

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

您可以使用通过身份源提供的凭据以 AWS 联合身份登录。 AWS IAM Identity Center （IAM Identity Center）用户、贵公司的单点登录身份验证以及您的 Google 或 Facebook 凭据就是联合身份的示例。

当您以联合身份登录时，您的管理员以前使用 IAM 角色设置了身份联合验证。当你使用联合访问 AWS 时，你就是在间接扮演一个角色。

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

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

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

## AWS 账户 root 用户

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

## 联合身份

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

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

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

## IAM 用户和群组

I AM 用户是您 AWS 账户 内部对个人或应用程序具有特定权限的身份。在可能的情况下，我们建议使用临时凭证，而不是创建具有长期凭证（如密码和访问密钥）的 IAM 用户。但是，如果您有一些特定

的使用场景需要长期凭证以及 IAM 用户，建议您轮换访问密钥。有关更多信息，请参阅《IAM 用户指南》中的对于需要长期凭证的用例，应在需要时更新访问密钥。

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

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

## IAM 角色

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

具有临时凭证的 IAM 角色在以下情况下很有用：

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

AWS 服务 或资源交互才能完成的请求时，才会发出 FAS 请求。在这种情况下，您必须具有执行这两项操作的权限。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。

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

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

## 使用策略管理访问

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

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

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

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

### 基于身份的策略

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

基于身份的策略可以进一步归类为内联策略或托管式策略。内联策略直接嵌入单个用户、组或角色中。托管策略是独立的策略，您可以将其附加到中的多个用户、群组和角色 AWS 账户。托管策略包括 AWS 托管策略和客户托管策略。要了解如何在托管策略和内联策略之间进行选择，请参阅《IAM 用户指南》中的在托管策略与内联策略之间进行选择。

## 基于资源的策略

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

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

## 访问控制列表 (ACLs)

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

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

## 其他策略类型

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

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

可能影响身份（包括身份）的有效权限 AWS 账户根用户，无论这些身份是否属于您的组织。有关 Organizations 的更多信息 RCPs，包括 AWS 服务 该支持的列表 RCPs，请参阅《AWS Organizations 用户指南》中的资源控制策略 (RCPs)。

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

### 多个策略类型

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

## Amazon WorkSpaces 安全浏览器如何与 IAM 配合使用

在使用 IAM 管理 WorkSpaces 安全浏览器的访问权限之前，请先了解 WorkSpaces 安全浏览器可以使用哪些 IAM 功能。

您可以在 Amazon WorkSpaces 安全浏览器中使用的 IAM 功能

| IAM 特征 | WorkSpaces 安全浏览器支持 |
| --- | --- |
| 基于身份的策略 | 是 |
| 基于资源的策略 | 否 |
| 策略操作 | 是 |
| 策略资源 | 是 |
| 策略条件键 | 是 |
| ACLs | 否 |
| ABAC（策略中的标签） | 部分 |
| 临时凭证 | 是 |
| 主体权限 | 是 |

| IAM 特征 | WorkSpaces 安全浏览器支持 |
| --- | --- |
| 服务角色 | 否 |
| 服务相关角色 | 是 |

要全面了解 WorkSpaces 安全浏览器和其他 AWS 服务如何与大多数 IAM 功能配合使用，请参阅 IAM 用户指南中的与 IAM 配合使用的AWS 服务。

主题


- 安全浏览器的基于身份的 WorkSpaces 策略
- WorkSpaces 安全浏览器中基于资源的策略
- WorkSpaces 安全浏览器的策略操作
- WorkSpaces 安全浏览器的策略资源
- WorkSpaces 安全浏览器的策略条件密钥
- WorkSpaces 安全浏览器中的访问控制列表 (ACLs)
- 使用安全浏览器进行基于属性的访问控制 (ABAC) WorkSpaces
- 在 WorkSpaces 安全浏览器中使用临时证书
- WorkSpaces 安全浏览器的跨服务主体权限
- WorkSpaces 安全浏览器的服务角色
- WorkSpaces 安全浏览器的服务相关角色


## 安全浏览器的基于身份的 WorkSpaces 策略

支持基于身份的策略：是

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

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

安全浏览器的基于身份的 WorkSpaces 策略示例

要查看基于身份 WorkSpaces 的安全浏览器策略的示例，请参阅。Ama WorkSpaces zon 安全浏览器的基于身份的策略示例

## WorkSpaces 安全浏览器中基于资源的策略

支持基于资源的策略：否

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

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

## WorkSpaces 安全浏览器的策略操作

支持策略操作：是

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

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

在策略中包含操作以授予执行关联操作的权限。

要查看 WorkSpaces 安全浏览器操作列表，请参阅《服务授权参考》中的 Amazon WorkSpaces 安全浏览器定义的操作。

WorkSpaces 安全浏览器中的策略操作在操作前使用以下前缀：

```
workspaces-web
```

要在单个语句中指定多项操作，请使用逗号将它们隔开。

```
"Action": [
      "workspaces-web:action1",
      "workspaces-web:action2"
         ]
```

要查看基于身份 WorkSpaces 的安全浏览器策略的示例，请参阅。Ama WorkSpaces zon 安全浏览器的基于身份的策略示例

## WorkSpaces 安全浏览器的策略资源

支持策略资源：是

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

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

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

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

要查看 WorkSpaces 安全浏览器资源类型及其列表 ARNs，请参阅《服务授权参考》中的 Amazon WorkSpaces 安全浏览器定义的资源。要了解您可以使用哪些操作来指定每种资源的 ARN，请参阅 Amazon WorkSpaces 安全浏览器定义的操作。

要查看基于身份 WorkSpaces 的安全浏览器策略的示例，请参阅。Ama WorkSpaces zon 安全浏览器的基于身份的策略示例

## WorkSpaces 安全浏览器的策略条件密钥

支持特定于服务的策略条件键：是

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

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

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

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

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

要查看 WorkSpaces 安全浏览器条件密钥列表，请参阅《服务授权参考》中的 Amazon WorkSpaces 安全浏览器的条件密钥。要了解您可以使用条件键的操作和资源，请参阅 Amazon WorkSpaces 安全浏览器定义的操作。

要查看基于身份 WorkSpaces 的安全浏览器策略的示例，请参阅。Ama WorkSpaces zon 安全浏览器的基于身份的策略示例

## WorkSpaces 安全浏览器中的访问控制列表 (ACLs)

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。

## 使用安全浏览器进行基于属性的访问控制 (ABAC) WorkSpaces

支持 ABAC（策略中的标签）：部分支持

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

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

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

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

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

## 在 WorkSpaces 安全浏览器中使用临时证书

支持临时凭证：是

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

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

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

## WorkSpaces 安全浏览器的跨服务主体权限

支持转发访问会话（FAS）：是

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

## WorkSpaces 安全浏览器的服务角色

支持服务角色：否

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

> **Warning**
>
> 更改服务角色的权限可能会破坏 WorkSpaces 安全浏览器的功能。只有当 WorkSpaces 安全浏览器提供相关指导时，才能编辑服务角色。

## WorkSpaces 安全浏览器的服务相关角色

支持服务相关角色：是

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

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

# Ama WorkSpaces zon 安全浏览器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 WorkSpaces 安全浏览器资源。他们也无法使用 AWS Management Console、 AWS Command Line Interface (AWS CLI) 或 AWS API 执行任务。要授予用户对所需资源执行操作的权限，IAM 管理员可以创建 IAM 策略。管理员随后可以向角色添加 IAM 策略，用户可以代入角色。

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

有关 WorkSpaces 安全浏览器定义的操作和资源类型（包括每种资源类型的格式）的 ARNs 详细信息，请参阅《服务授权参考》中的 Amazon WorkSpaces 安全浏览器的操作、资源和条件密钥。

主题


- Ama WorkSpaces zon 安全浏览器的基于身份的策略最佳实践
- 使用 Amazon WorkSpaces 安全浏览器控制台
- 允许用户查看自己对 Amazon WorkSpaces 安全浏览器的权限


## Ama WorkSpaces zon 安全浏览器的基于身份的策略最佳实践

基于身份的策略决定了某人是否可以在您的账户中创建、访问或删除 WorkSpaces 安全浏览器资源。这些操作可能会使 AWS 账户产生成本。创建或编辑基于身份的策略时，请遵循以下指南和建议：

- 开始使用 AWS 托管策略并转向最低权限权限 — 要开始向用户和工作负载授予权限，请使用为许多常见用例授予权限的AWS 托管策略。它们在你的版本中可用 AWS 账户。我们建议您通过定义针对您的用例的 AWS 客户托管策略来进一步减少权限。有关更多信息，请参阅《IAM 用户指南》中的 AWS 托管式策略或工作职能的AWS 托管式策略。

- 应用最低权限：在使用 IAM 策略设置权限时，请仅授予执行任务所需的权限。为此，您可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用 IAM 应用权限的更多信息，请参阅《IAM 用户指南》中的 IAM 中的策略和权限。
- 使用 IAM 策略中的条件进一步限制访问权限：您可以向策略添加条件来限制对操作和资源的访问。例如，您可以编写策略条件来指定必须使用 SSL 发送所有请求。如果服务操作是通过特定 AWS 服务的（例如）使用的，则也可以使用条件来授予对服务操作的访问权限 AWS CloudFormation。有关更多信息，请参阅《IAM 用户指南》中的 IAM JSON 策略元素：条件。
- 使用 IAM Access Analyzer 验证您的 IAM 策略，以确保权限的安全性和功能性 – IAM Access Analyzer 会验证新策略和现有策略，以确保策略符合 IAM 策略语言（JSON）和 IAM 最佳实践。IAM Access Analyzer 提供 100 多项策略检查和可操作的建议，以帮助您制定安全且功能性强的策略。有关更多信息，请参阅《IAM 用户指南》中的使用 IAM Access Analyzer 验证策略。
- 需要多重身份验证 (MFA)-如果 AWS 账户您的场景需要 IAM 用户或根用户，请启用 MFA 以提高安全性。若要在调用 API 操作时需要 MFA，请将 MFA 条件添加到您的策略中。有关更多信息，请参阅《IAM 用户指南》中的使用 MFA 保护 API 访问。

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

## 使用 Amazon WorkSpaces 安全浏览器控制台

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

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

为确保用户和角色仍然可以使用 WorkSpaces 安全浏览器控制台，还要将 WorkSpaces 安全浏览器`ConsoleAccess`或`ReadOnly` AWS 托管策略附加到实体。有关更多信息，请参阅《IAM 用户指南》中的为用户添加权限。

## 允许用户查看自己对 Amazon WorkSpaces 安全浏览器的权限

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

```
{
```

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

## AWS WorkSpaces 安全浏览器的托管策略

要向用户、群组和角色添加权限，使用 AWS 托管策略比自己编写策略要容易得多。创建仅为团队提供所需权限的 IAM 客户管理型策略需要时间和专业知识。要快速入门，您可以使用我们的 AWS 托管策略。这些政策涵盖常见用例，可在您的 AWS 账户中使用。有关 AWS 托管策略的更多信息，请参阅 IAM 用户指南中的AWS 托管策略。

AWS 服务维护和更新 AWS 托管策略。您无法更改 AWS 托管策略中的权限。服务偶尔可能会向 AWS 托管策略添加其他权限以支持新功能。此类更新会影响附加策略的所有身份（用户、组和角色）。当启动新特征或新操作可用时，服务最有可能会更新 AWS 托管式策略。服务不会从 AWS 托管策略中移除权限，因此策略更新不会破坏您的现有权限。

此外，还 AWS 支持跨多个服务的工作职能的托管策略。例如，`ReadOnlyAccess` AWS 托管策略提供对所有 AWS 服务和资源的只读访问权限。当服务启动一项新功能时， AWS 会为新操作和资源添加只读权限。有关工作职能策略的列表和说明，请参阅 IAM 用户指南中的适用于工作职能的AWS 托管式策略。

主题


- AWS 托管策略： AmazonWorkSpacesWebServiceRolePolicy
- AWS 托管策略： AmazonWorkSpacesSecureBrowserReadOnly
- AWS 托管策略： AmazonWorkSpacesWebReadOnly
- WorkSpaces AWS 托管策略的安全浏览器更新


## AWS 托管策略： AmazonWorkSpacesWebServiceRolePolicy

无法将 `AmazonWorkSpacesWebServiceRolePolicy` 策略附加到 IAM 实体。此策略附加到服务相关角色，允许 WorkSpaces 安全浏览器代表您执行操作。有关更多信息，请参阅 the section called “使用服务相关角色”。

此策略授予管理权限，允许访问 WorkSpaces 安全浏览器使用或管理的 AWS 服务和资源。

权限详细信息

该策略包含以下权限：

- `workspaces-web`— 允许访问 WorkSpaces 安全浏览器使用或管理的 AWS 服务和资源。

- `ec2`— 允许委托人描述 VPCs、子网和可用区；创建、标记、描述和删除网络接口；关联或取消关联地址；以及描述路由表、安全组和 VPC 终端节点。
- `CloudWatch` – 允许委托人放入指标数据。
- `Kinesis` – 允许委托人描述 Kinesis 数据流的摘要，并将记录放入用户访问日志记录的 Kinesis 数据流中。有关更多信息，请参阅 the section called “设置用户访问日志记录”。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeAvailabilityZones",
                "ec2:DescribeNetworkInterfaces",
                "ec2:AssociateAddress",
                "ec2:DisassociateAddress",
                "ec2:DescribeRouteTables",
                "ec2:DescribeSecurityGroups",
                "ec2:DescribeVpcEndpoints"
            ],
            "Resource": "*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface"
            ],
            "Resource": [
                "arn:aws:ec2:*:*:subnet/*",
                "arn:aws:ec2:*:*:security-group/*"
            ]
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateNetworkInterface"
            ],
            "Resource": "arn:aws:ec2:*:*:network-interface/*",
            "Condition": {
```

```
                "StringEquals": {
                    "aws:RequestTag/WorkSpacesWebManaged": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:CreateTags"
            ],
            "Resource": "arn:aws:ec2:*:*:network-interface/*",
            "Condition": {
                "StringEquals": {
                    "ec2:CreateAction": "CreateNetworkInterface"
                },
                "ForAllValues:StringEquals": {
                    "aws:TagKeys": [
                        "WorkSpacesWebManaged"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DeleteNetworkInterface"
            ],
            "Resource": "arn:aws:ec2:*:*:network-interface/*",
            "Condition": {
                "StringEquals": {
                    "aws:ResourceTag/WorkSpacesWebManaged": "true"
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "cloudwatch:PutMetricData"
            ],
            "Resource": "*",
            "Condition": {
                "StringEquals": {
                    "cloudwatch:namespace": [
                        "AWS/WorkSpacesWeb",
```

```
                        "AWS/Usage"
                    ]
                }
            }
        },
        {
            "Effect": "Allow",
            "Action": [
                "kinesis:PutRecord",
                "kinesis:PutRecords",
                "kinesis:DescribeStreamSummary"
            ],
            "Resource": "arn:aws:kinesis:*:*:stream/amazon-workspaces-web-*"
        }
    ]
}
```

## AWS 托管策略： AmazonWorkSpacesSecureBrowserReadOnly

您可以将 `AmazonWorkSpacesSecureBrowserReadOnly` 策略附加到 IAM 身份。

此策略授予只读权限，允许通过 AWS 管理控制台、SDK 和 CLI 访问 WorkSpaces 安全浏览器及其依赖项。此策略不包括使用 `IAM_Identity_Center` 作为身份验证类型与门户进行交互所需的权限。要获得这些权限，请将此策略与 `AWSSSOReadOnly` 相结合。

权限详细信息

该策略包含以下权限。

- `workspaces-web`— 通过 AWS 管理控制台、SDK 和 CLI 提供对 WorkSpaces 安全浏览器及其依赖项的只读访问权限。
- `ec2`— 允许委托人描述 VPCs子网和安全组。它用于 WorkSpaces 安全浏览器的 AWS 管理控制台中 VPCs，向您显示可用于该服务的子网和安全组。
- `Kinesis` – 允许委托人列出 Kinesis 数据流。它用于 WorkSpaces 安全浏览器的 AWS 管理控制台中，向您显示可用于该服务的 Kinesis 数据流。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "workspaces-web:GetBrowserSettings",
                "workspaces-web:GetIdentityProvider",
                "workspaces-web:GetNetworkSettings",
                "workspaces-web:GetPortal",
                "workspaces-web:GetPortalServiceProviderMetadata",
                "workspaces-web:GetTrustStore",
                "workspaces-web:GetTrustStoreCertificate",
                "workspaces-web:GetUserSettings",
                "workspaces-web:GetUserAccessLoggingSettings",
                "workspaces-web:ListBrowserSettings",
                "workspaces-web:ListIdentityProviders",
                "workspaces-web:ListNetworkSettings",
                "workspaces-web:ListPortals",
                "workspaces-web:ListTagsForResource",
                "workspaces-web:ListTrustStoreCertificates",
                "workspaces-web:ListTrustStores",
                "workspaces-web:ListUserSettings",
                "workspaces-web:ListUserAccessLoggingSettings"
            ],
            "Resource": "arn:aws:workspaces-web:*:*:*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeSecurityGroups",
                "kinesis:ListStreams"
            ],
            "Resource": "*"
        }
    ]
}
```

## AWS 托管策略： AmazonWorkSpacesWebReadOnly

您可以将 AmazonWorkSpacesWebReadOnly 策略附加到 IAM 身份。

此策略授予只读权限，允许通过 AWS 管理控制台、SDK 和 CLI 访问 WorkSpaces 安全浏览器及其依赖项。此策略不包括使用 IAM_Identity_Center 作为身份验证类型与门户进行交互所需的权限。要获得这些权限，请将此策略与 AWSSSOReadOnly 相结合。

> **Note**
>
> 如果您当前正在使用此策略，请切换到新 AmazonWorkSpacesSecureBrowserReadOnly 策略。

权限详细信息

该策略包含以下权限。

- workspaces-web— 通过 AWS 管理控制台、SDK 和 CLI 提供对 WorkSpaces 安全浏览器及其依赖项的只读访问权限。
- ec2— 允许委托人描述 VPCs子网和安全组。它用于 WorkSpaces 安全浏览器的 AWS 管理控制台中 VPCs，向您显示可用于该服务的子网和安全组。
- Kinesis – 允许委托人列出 Kinesis 数据流。它用于 WorkSpaces 安全浏览器的 AWS 管理控制台中，向您显示可用于该服务的 Kinesis 数据流。

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
            "Action": [
                "workspaces-web:GetBrowserSettings",
                "workspaces-web:GetIdentityProvider",
                "workspaces-web:GetNetworkSettings",
                "workspaces-web:GetPortal",
                "workspaces-web:GetPortalServiceProviderMetadata",
                "workspaces-web:GetTrustStore",
                "workspaces-web:GetTrustStoreCertificate",
                "workspaces-web:GetUserSettings",
```

```
                "workspaces-web:GetUserAccessLoggingSettings",
                "workspaces-web:ListBrowserSettings",
                "workspaces-web:ListIdentityProviders",
                "workspaces-web:ListNetworkSettings",
                "workspaces-web:ListPortals",
                "workspaces-web:ListTagsForResource",
                "workspaces-web:ListTrustStoreCertificates",
                "workspaces-web:ListTrustStores",
                "workspaces-web:ListUserSettings",
                "workspaces-web:ListUserAccessLoggingSettings"
            ],
            "Resource": "arn:aws:workspaces-web:*:*:*"
        },
        {
            "Effect": "Allow",
            "Action": [
                "ec2:DescribeVpcs",
                "ec2:DescribeSubnets",
                "ec2:DescribeSecurityGroups",
                "kinesis:ListStreams"
            ],
            "Resource": "*"
        }
    ]
}
```

## WorkSpaces AWS 托管策略的安全浏览器更新

查看有关 WorkSpaces 安全浏览器的 AWS 托管策略自该服务开始跟踪这些更改以来这些更新的详细信息。要获得有关此页面更改的自动提示，请订阅 文档历史记录 页面上的 RSS 源。

| 更改 | 描述 | 日期 |
| --- | --- | --- |
| AmazonWorkSpacesSecureBrowserReadOnly - 新策略 | WorkSpaces 安全浏览器添加了一项新策略，允许通过 AWS 管理控制台、软件开发工具包和 CLI 对 WorkSpaces 安全浏览器及其依赖项进行只读访问。 | 2024 年 6 月 24 日 |

| 更改 | 描述 | 日期 |
| --- | --- | --- |
| AmazonWorkSpacesWebServiceRolePolicy - 更新的策略 | WorkSpaces 安全浏览器更新了政策，仅限使用 aw CreateNetworkInterface s:RequestTag/WorkSpacesWebManaged: true and act on subnet and security group resources, as well as restrict DeleteNetworkInterface to ENIs tagged with aws:ResourceTag/WorkSpacesWebManaged: true 进行标记。 | 2022 年 12 月 15 日 |
| AmazonWorkSpacesWebReadOnly - 更新的策略 | WorkSpaces 安全浏览器更新了政策，增加了用户访问记录和列出 Kinesis 数据流的读取权限。有关更多信息，请参阅 the section called “设置用户访问日志记录”。 | 2022 年 11 月 2 日 |
| AmazonWorkSpacesWebServiceRolePolicy - 更新的策略 | WorkSpaces 安全浏览器更新了政策，描述了 Kinesis 数据流的摘要，并将记录放入 Kinesis 数据流中以供用户访问记录。有关更多信息，请参阅 the section called “设置用户访问日志记录”。 | 2022 年 10 月 17 日 |
| AmazonWorkSpacesWebServiceRolePolicy - 更新的策略 | WorkSpaces 安全浏览器更新了在创建 ENI 期间创建标签的策略。 | 2022 年 9 月 6 日 |

| 更改 | 描述 | 日期 |
| --- | --- | --- |
| AmazonWorkSpacesWebServiceRolePolicy - 更新的策略 | WorkSpaces 安全浏览器更新了政策，将 AWS/Usage 命名空间添加到 PutMetricData API 权限中。 | 2022 年 4 月 6 日 |
| AmazonWorkSpacesWebReadOnly：新策略 | WorkSpaces 安全浏览器添加了一项新策略，允许通过 AWS 管理控制台、软件开发工具包和 CLI 对 WorkSpaces 安全浏览器及其依赖项进行只读访问。 | 2021 年 11 月 30 日 |
| AmazonWorkSpacesWebServiceRolePolicy：新策略 | WorkSpaces 安全浏览器添加了一项新政策，允许访问 WorkSpaces 安全浏览器使用或管理的 AWS 服务和资源。 | 2021 年 11 月 30 日 |
| WorkSpaces 安全浏览器开始跟踪更改 | WorkSpaces 安全浏览器开始跟踪其 AWS 托管策略的更改。 | 2021 年 11 月 30 日 |

# 对 Amazon WorkSpaces 安全浏览器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 WorkSpaces 安全浏览器和 IAM 时可能遇到的常见问题。

主题


- 我无权在 WorkSpaces 安全浏览器中执行操作
- 我无权执行 iam：PassRole
- 我想允许 AWS 账户以外的用户访问我的 WorkSpaces 安全浏览器资源


## 我无权在 WorkSpaces 安全浏览器中执行操作

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

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

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 workspaces-web: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 `workspaces-web:`*`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。

## 我无权执行 iam：PassRole

如果您收到错误消息，指出您无权执行该`iam:PassRole`操作，则必须更新您的策略以允许您将角色传递给 WorkSpaces 安全浏览器。

有些 AWS 服务 允许您将现有角色传递给该服务，而不是创建新的服务角色或服务相关角色。为此，您必须具有将角色传递到服务的权限。

当名为的 IAM 用户`marymajor`尝试使用控制台在 WorkSpaces 安全浏览器中执行操作时，会出现以下示例错误。但是，服务必须具有服务角色所授予的权限才可执行此操作。Mary 不具有将角色传递到服务的权限。

```
User: arn:aws:iam::123456789012:user/marymajor is not authorized to perform:
 iam:PassRole
```

在这种情况下，必须更新 Mary 的策略以允许她执行 `iam:PassRole` 操作。

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 AWS 账户以外的用户访问我的 WorkSpaces 安全浏览器资源

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

要了解更多信息，请参阅以下内容：

- 要了解 WorkSpaces 安全浏览器是否支持这些功能，请参阅Amazon WorkSpaces 安全浏览器如何与 IAM 配合使用。

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

## 在 Amazon WorkSpaces 安全浏览器中使用服务相关角色

Amazon WorkSpaces 安全浏览器使用 AWS Identity and Access Management (IAM) 服务相关角色。服务相关角色是一种独特的 IAM 角色，直接链接到 WorkSpaces 安全浏览器。服务相关角色由 WorkSpaces Secure Browser 预定义，包括该服务代表您调用其他 AWS 服务所需的所有权限。

与服务相关的角色可以更轻松地设置 WorkSpaces 安全浏览器，因为您不必手动添加必要的权限。WorkSpaces 安全浏览器定义其服务相关角色的权限，除非另有定义，否则只有 WorkSpaces 安全浏览器才能担任其角色。定义的权限包括信任策略和权限策略。不能将该权限策略附加到任何其他 IAM 实体。

只有在首先删除服务相关角色的相关资源后，才能删除该角色。这可以保护您的 WorkSpaces 安全浏览器资源，因为您不会无意中删除访问这些资源的权限。

有关支持服务相关角色的其他服务的信息，请参阅使用 IAM 的AWS 服务并查找服务相关角色列中显示为是的服务。选择是和链接，查看该服务的服务相关角色文档。

主题


- WorkSpaces 安全浏览器的服务相关角色权限
- 为 WorkSpaces 安全浏览器创建服务相关角色
- 编辑 WorkSpaces 安全浏览器的服务相关角色
- 删除 WorkSpaces 安全浏览器的服务相关角色
- WorkSpaces 安全浏览器服务相关角色支持的区域

## WorkSpaces 安全浏览器的服务相关角色权限

WorkSpaces 安全浏览器使用名为的服务相关角色 `AWSServiceRoleForAmazonWorkSpacesWeb` —— WorkSpaces 安全浏览器使用此服务相关角色访问客户账户的亚马逊 EC2 资源以获取流媒体实例和 CloudWatch 指标。

`AWSServiceRoleForAmazonWorkSpacesWeb` 服务相关角色信任以下服务代入该角色：

- `workspaces-web.amazonaws.com`

名为的角色权限策略`AmazonWorkSpacesWebServiceRolePolicy`允许 WorkSpaces Secure Browser 对指定资源完成以下操作。有关更多信息，请参阅 the section called “AmazonWorkSpacesWebServiceRolePolicy”。

- 操作：`all AWS resources` 上的 `ec2:DescribeVpcs`
- 操作：`ec2:DescribeSubnets` 上的 `all AWS resources`
- 操作：`ec2:DescribeAvailabilityZones` 上的 `all AWS resources`
- 操作：针对子网和安全组资源的 `ec2:CreateNetworkInterface` 操作（通过 `aws:RequestTag/WorkSpacesWebManaged: true`）
- 操作：`all AWS resources` 上的 `ec2:DescribeNetworkInterfaces`
- 操作：针对网络接口的 `ec2:DeleteNetworkInterface` 操作（通过 `aws:ResourceTag/WorkSpacesWebManaged: true`）
- 操作：`all AWS resources` 上的 `ec2:DescribeSubnets`
- 操作：`ec2:AssociateAddress` 上的 `all AWS resources`
- 操作：`ec2:DisassociateAddress` 上的 `all AWS resources`
- 操作：`ec2:DescribeRouteTables` 上的 `all AWS resources`
- 操作：`ec2:DescribeSecurityGroups` 上的 `all AWS resources`
- 操作：`ec2:DescribeVpcEndpoints` 上的 `all AWS resources`
- 操作：针对 `ec2:CreateNetworkInterface` 的 `ec2:CreateTags` 操作（通过 `aws:TagKeys: ["WorkSpacesWebManaged"]`）
- 操作：`all AWS resources` 上的 `cloudwatch:PutMetricData`
- 操作：针对名称以 `amazon-workspaces-web-` 开头的 Kinesis 数据流的 `kinesis:PutRecord` 操作

- 操作：针对名称以 `amazon-workspaces-web-` 开头的 Kinesis 数据流的 `kinesis:PutRecords` 操作
- 操作：针对名称以 `amazon-workspaces-web-` 开头的 Kinesis 数据流的 `kinesis:DescribeStreamSummary` 操作

您必须配置权限，允许 IAM 实体（如用户、组或角色）创建、编辑或删除服务相关角色。有关更多信息，请参阅《IAM 用户指南》中的服务相关角色权限。

## 为 WorkSpaces 安全浏览器创建服务相关角色

您无需手动创建服务相关角色。当您在 AWS Management Console、或 AWS API 中创建第一个门户时， WorkSpaces 安全浏览器会为您创建服务相关角色。 AWS CLI

> **Important**
>
> 如果您在其他使用此角色支持的功能的服务中完成某个操作，此服务相关角色可以出现在您的账户中。

如果您删除了此服务相关角色，而后需要再次创建它，则可以使用相同的流程在您的账户中重新创建此角色。当您创建第一个门户时， WorkSpaces 安全浏览器会再次为您创建服务相关角色。

您还可以使用 IAM 控制台通过WorkSpaces 安全浏览器用例创建服务相关角色。在 AWS CLI 或 AWS API 中，使用服务名称创建服务相关角色。`workspaces-web.amazonaws.com`有关更多信息，请参阅《IAM 用户指南》中的创建服务相关角色。如果您删除了此服务相关角色，可以使用同样的过程再次创建角色。

## 编辑 WorkSpaces 安全浏览器的服务相关角色

WorkSpaces 安全浏览器不允许您编辑`AWSServiceRoleForAmazonWorkSpacesWeb`服务相关角色。在创建服务相关角色后，您将无法更改角色的名称，因为可能有多种实体引用该角色。不过，您可以使用 IAM 编辑角色的说明。有关更多信息，请参阅《IAM 用户指南》中的编辑服务相关角色。

## 删除 WorkSpaces 安全浏览器的服务相关角色

如果不再需要使用某个需要服务相关角色的功能或服务，我们建议您删除该角色。这样就没有未被主动监控或维护的未使用实体。但是，必须先清除服务相关角色的资源，然后才能手动删除它。

> **Note**
>
> 如果您尝试删除资源时， WorkSpaces 安全浏览器服务正在使用该角色，则删除可能会失败。如果发生这种情况，请等待几分钟后重试。

删除使用的 WorkSpaces 安全浏览器资源 AWSService RoleForAmazonWorkSpacesWeb

- 请选择以下选项之一：
  - 如果您使用控制台，请删除控制台上的所有门户。
  - 如果您使用 CLI 或 API，请取消所有资源（包括浏览器设置、网络设置、用户设置、信任存储和用户访问日志记录设置）与门户的关联，删除这些资源，然后删除这些门户。

使用 IAM 手动删除服务相关角色

使用 IAM 控制台 AWS CLI、或 AWS API 删除 AWSServiceRoleForAmazonWorkSpacesWeb服务相关角色。有关更多信息，请参见《IAM 用户指南》中的删除服务相关角色。

### WorkSpaces 安全浏览器服务相关角色支持的区域

WorkSpaces Secure Browser 支持在提供服务的所有地区使用服务相关角色。有关更多信息，请参阅 AWS 区域和端点。

## Amazon WorkSpaces 安全浏览器中的事件响应

您可以通过监控 `SessionFailure` Amazon CloudWatch 指标来检测事件。要接收事件警报，请使用`SessionFailure`指标 CloudWatch 警报。有关更多信息，请参阅 使用亚马逊监控亚马逊 WorkSpaces 安全浏览器 CloudWatch。

## Amazon WorkSpaces 安全浏览器的合规性验证

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：

- Security Compliance & Governance：这些解决方案实施指南讨论了架构考虑因素，并提供了部署安全性和合规性功能的步骤。
- 符合 HIPAA 要求的服务参考：列出符合 HIPAA 要求的服务。并非所有 AWS 服务 人都符合 HIPAA 资格。
- AWS 合规资源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、行业指导方针和法规。
- 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 通过安全控制措施评估您的 AWS 资源并检查其是否符合安全行业标准和最佳实践。有关受支持服务及控制措施的列表，请参阅 Security Hub 控制措施参考。
- Amazon GuardDuty — 它通过监控您的 AWS 账户环境中是否存在可疑和恶意活动，来 AWS 服务 检测您的工作负载、容器和数据面临的潜在威胁。 GuardDuty 通过满足某些合规性框架规定的入侵检测要求，可以帮助您满足各种合规性要求，例如 PCI DSS。
- AWS Audit Manager— 这 AWS 服务 可以帮助您持续审计 AWS 使用情况，从而简化风险管理以及对法规和行业标准的合规性。

## Amazon WorkSpaces 安全浏览器的弹性

AWS 全球基础设施是围绕 AWS 区域 可用区构建的。 AWS 区域 提供多个物理隔离和隔离的可用区，这些可用区通过低延迟、高吞吐量和高度冗余的网络连接。利用可用区，您可以设计和操作在可用区之间无中断地自动实现失效转移的应用程序和数据库。与传统的单个或多个数据中心基础结构相比，可用区具有更高的可用性、容错性和可扩展性。

有关 AWS 区域 和可用区的更多信息，请参阅AWS 全球基础设施。

WorkSpaces 安全浏览器目前不支持以下内容：

- 跨 AZs 区域备份内容
- 加密备份
- 加密或区域之间 AZs 传输的内容

- 默认备份或自动备份

要配置较高的 Internet 可用性，可以调整您的 VPC 配置。为了获得高 API 可用性，您可以请求适量的 TPS。

## Amazon 安全浏览器中的基础设施 WorkSpaces 安全

作为一项托管服务，Amazon WorkSpaces 安全浏览器受 AWS 全球网络安全的保护。有关 AWS 安全服务以及如何 AWS 保护基础设施的信息，请参阅AWS 云安全。要使用基础设施安全的最佳实践来设计您的 AWS 环境，请参阅 S AWS ecurity Pillar Well-Architected Fram ework 中的基础设施保护。

您可以使用 AWS 已发布的 API 调用通过网络访问 Amazon WorkSpaces 安全浏览器。客户端必须支持以下内容：

- 传输层安全性协议（TLS）。我们要求使用 TLS 1.2，建议使用 TLS 1.3。
- 具有完全向前保密（PFS）的密码套件，例如 DHE（临时 Diffie-Hellman）或 ECDHE（临时椭圆曲线 Diffie-Hellman）。大多数现代系统（如 Java 7 及更高版本）都支持这些模式。

此外，必须使用访问密钥 ID 和与 IAM 主体关联的秘密访问密钥来对请求进行签名。或者，您可以使用 AWS Security Token Service（AWS STS）生成临时安全凭证来对请求进行签名。

WorkSpaces 安全浏览器通过对所有服务应用标准 AWS Sigv4 身份验证和授权来隔离服务流量。客户资源端点（或 Web 门户端点）受您的身份提供者保护。您可以使用身份提供者（IdP）中的多因素授权和其他安全机制来进一步隔离流量。

可以通过配置网络设置（例如 VPC、子网或安全组）来控制所有 Internet 访问。目前不支持多租户和 VPC 终端节点 (PrivateLink)。

## Amazon WorkSpaces 安全浏览器中的配置和漏洞分析

WorkSpaces 安全浏览器代表您根据需要更新和修补应用程序和平台，包括 Chrome 和 Linux。您无需修补或重建。但是，您有责任根据规格和指南配置 WorkSpaces 安全浏览器，并监控用户对 WorkSpaces 安全浏览器的使用情况。所有与服务相关的配置和漏洞分析均由 WorkSpaces 安全浏览器负责。

您可以请求提高 WorkSpaces 安全浏览器资源的限制，例如门户网站的数量和用户数量。WorkSpaces 安全浏览器可确保服务和 SLA 的可用性。

# APIs 使用接口 VPC 终端节点进行访问 (AWS PrivateLink)

您可以直接从私有云 (VPC) 内部调用 Amazon S WorkSpaces ecure Browser API 终端节点，而不必通过互联网进行连接。您无需使用互联网网关、NAT 设备、VPN 连接或 AWS Direct Connect 连接即可执行此操作。

您可以通过创建由提供支持的接口 VPC 终端节点来建立此私有连接AWS PrivateLink。对于您在 VPC 中指定的每个子网，我们都会在子网中创建一个终端节点网络接口。终端节点网络接口是请求者管理的网络接口，可用作 Amazon S WorkSpaces ecure Browser API 流量的入口点。

有关更多信息，请参阅通过访问 AWS 服务 AWS PrivateLink。

主题


- Amazon WorkSpaces 安全浏览器的注意事项
- 为 Amazon WorkSpaces 安全浏览器创建接口 VPC 终端节点
- 为您的接口 VPC 终端节点创建终端节点策略
- 故障排除


## Amazon WorkSpaces 安全浏览器的注意事项

在为 Amazon WorkSpaces 安全浏览器设置接口 VPC 终端节点之前 APIs，请务必通过查看访问 AWS 服务中的 “先决条件” AWS PrivateLink。Amazon WorkSpaces 安全浏览器支持通过接口 VPC 终端节点调用其所有 API 操作。

默认情况下，允许通过终端节点完全访问 Amazon WorkSpaces 安全浏览器。有关更多信息，请参阅《Amazon VPC User Guide》中的 Controlling access to services with VPC endpoints。

## 为 Amazon WorkSpaces 安全浏览器创建接口 VPC 终端节点

您可以使用 Amazon VPC 控制台或 AWS Command Line Interface (AWS CLI) 为亚马逊 WorkSpaces 安全浏览器服务创建接口 VPC 终端节点。有关更多信息，请参阅《Amazon VPC User Guide》中的 Creating an interface endpoint。

使用以下服务名称为 Amazon WorkSpaces 安全浏览器创建接口 VPC 终端节点：

- com.amazonaws。*region*.workspaces-Web

对于支持 FIPS 的区域，请使用以下服务名称为 Amazon WorkSpaces 安全浏览器创建接口 VPC 终端节点：

- com.amazonaws。 *region*。 workspaces-web-fips

## 为您的接口 VPC 终端节点创建终端节点策略

终端节点策略是一种 IAM 资源，您可以将其附加到接口 VPC 终端节点。默认终端节点策略允许您 APIs 通过接口 VPC 终端节点完全访问亚马逊 WorkSpaces 安全浏览器。要控制从您的 VPC 授予亚马逊 WorkSpaces 安全浏览器的访问权限，请将自定义终端节点策略附加到接口 VPC 终端节点。

端点策略指定以下信息：

- 可执行操作的主体（AWS 账户、IAM 用户和 IAM 角色）。
- 可执行的操作。
- 可对其执行操作的资源。

有关更多信息，请参阅《Amazon VPC 用户指南》中的使用 VPC 端点控制对服务的访问。

示例：Amazon WorkSpaces 安全浏览器操作的 VPC 终端节点策略

以下是自定义端点策略的示例。当您将此策略附加到您的接口 VPC 终端节点时，它会向所有委托人授予所有资源上列出的亚马逊 WorkSpaces 安全浏览器操作的访问权限。

```
{
     "Statement": [
         {
             "Action": "workspaces-web:*",
             "Effect": "Allow",
             "Resource": "*",
             "Principal": "*"
         }
     ]
}
```

## 故障排除

如果您对 Amazon WorkSpaces 安全浏览器的调用挂起， APIs 则您的 VPC 终端节点服务安全组或 IAM 角色设置可能存在配置错误。要解决这个问题，请尝试以下方法：

- 在创建接口 VPC 终端节点时，它可能已自动连接到您的 AWS 账户默认安全组。尝试使用其他安全组，并确保入站和出站权限允许您正确传输数据。
- 确保您使用的 IAM 角色允许您调用 Amazon WorkSpaces 安全浏览器 APIs。

有关更多信息，请参阅什么是 AWS PrivateLink？ 在《亚马逊 VPC 用户指南》中。

# Amazon 安全浏览器的 WorkSpaces 安全最佳实践

Amazon S WorkSpaces ecure Browser 提供了许多安全功能，供您在制定和实施自己的安全策略时使用。以下最佳实践是一般指导原则，并不代表完整安全解决方案。这些最佳实践可能不适合环境或不满足环境要求，请将其视为有用的考虑因素而不是惯例。

Amazon WorkSpaces 安全浏览器的最佳实践包括以下内容：

- 要检测与您使用安全浏览器相关的潜在安全事件，请使用 AWS CloudTrail 或 Amazon CloudWatch 来检测和跟踪访问历史记录和处理日志。 WorkSpaces 有关更多信息，请参阅使用亚马逊监控亚马逊 WorkSpaces 安全浏览器 CloudWatch 和使用记录 WorkSpaces 安全浏览器 API 调用 AWS CloudTrail。
- 要实施侦探控制并识别异常，请使用 CloudTrail 日志和指标。 CloudWatch有关更多信息，请参阅使用亚马逊监控亚马逊 WorkSpaces 安全浏览器 CloudWatch 和使用记录 WorkSpaces 安全浏览器 API 调用 AWS CloudTrail。
- 您可以设置用户访问日志记录来记录用户事件。有关更多信息，请参阅 the section called “设置用户访问日志记录”。

为防止与您使用安全浏览器相关的潜在 WorkSpaces 安全事件，请遵循以下最佳实践：

- 实现最低权限访问权限并创建用于 WorkSpaces 安全浏览器操作的特定角色。使用 IAM 模板创建完全访问权限角色或只读角色。有关更多信息，请参阅 AWS WorkSpaces 安全浏览器的托管策略。
- 请谨慎共享门户域和用户凭证。Internet 上的任何人都可以访问 Web 门户，但除非他们拥有有效的门户用户凭证，否则他们无法启动会话。请注意您共享 Web 门户凭证的方式、时间以及对象。

# 监控 Amazon WorkSpaces 安全浏览器

监控是维护 Amazon WorkSpaces 安全浏览器和其他 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，用于监视您的 WorkSpaces 安全浏览器门户及其资源，在出现问题时进行报告，并在适当时自动采取措施：

- Amazon 会实时 CloudWatch监控您的 AWS 资源和您运行 AWS 的应用程序。您可以收集和跟踪指标，创建自定义的控制面板，以及设置警报以在指定的指标达到指定阈值时通知您或采取措施。例如，您可以 CloudWatch 跟踪您的 Amazon EC2 实例的 CPU 使用率或其他指标，并在需要时自动启动新实例。有关更多信息，请参阅 Amazon CloudWatch 用户指南。
- Amazon Lo CloudWatch g s 允许您监控、存储和访问来自亚马逊 EC2 实例和其他来源的日志文件。 CloudTrail CloudWatch 日志可以监视日志文件中的信息，并在达到特定阈值时通知您。您还可以在高持久性存储中检索您的日志数据。有关更多信息，请参阅 Amazon CloudWatch 日志用户指南。
- AWS CloudTrail捕获由您的账户或代表您的 AWS 账户进行的 API 调用和相关事件，并将日志文件传输到您指定的 Amazon S3 存储桶。您可以识别哪些用户和帐户拨打了电话 AWS、发出呼叫的源 IP 地址以及呼叫发生的时间。有关更多信息，请参阅 用户指南。AWS CloudTrail

主题


- 使用亚马逊监控亚马逊 WorkSpaces 安全浏览器 CloudWatch
- 使用记录 WorkSpaces 安全浏览器 API 调用 AWS CloudTrail
- 在 Amazon WorkSpaces 安全浏览器中登录用户访问权限


## 使用亚马逊监控亚马逊 WorkSpaces 安全浏览器 CloudWatch

您可以使用监控 Amazon WorkSpaces Secure Browser CloudWatch，该浏览器收集原始数据并将其处理为可读的近乎实时的指标。这些统计数据会保存 15 个月，从而使您能够访问历史信息，并能够更好地了解您的 Web 应用程序或服务的执行情况。此外，可以设置用于监测特定阈值的警报，并在达到相应阈值时发送通知或执行操作。有关更多信息，请参阅 Amazon CloudWatch 用户指南。

`AWS/WorkSpacesWeb` 命名空间包括以下指标。

CloudWatch Amazon WorkSpaces 安全浏览器的指标

| 指标 | 描述 | 维度 | 统计信息 | 单位 |
| --- | --- | --- | --- | --- |
| SessionAttempt | Amazon WorkSpaces 安全浏览器会话尝试次数。 | PortalId | 平均值、总数、最大值、最小值 | 计数 |
| SessionSuccess | 成功启动的 Amazon WorkSpaces 安全浏览器会话次数。 | PortalId | 平均值、总数、最大值、最小值 | 计数 |
| SessionFailure | 启动失败的 Amazon WorkSpaces 安全浏览器会话次数。 | PortalId | 平均值、总数、最大值、最小值 | 计数 |
| GlobalCpuPercent | Amazon WorkSpaces 安全浏览器会话实例的 CPU 使用率。 | PortalId | 平均值、总数、最大值、最小值 | 百分比 |
| GlobalMemoryPercent | Amazon WorkSpaces 安全浏览器会话实例的内存 (RAM) 使用情况。 | PortalId | 平均值、总数、最大值、最小值 | 百分比 |

> **Note**
>
> 您可以查看 “SampleCount” 指标统计信息`GlobalCpuPercent`或`GlobalMemoryPercent`确定门户上活跃的并发会话数量。每个会话每分钟发出一次数据点。

# 使用记录 WorkSpaces 安全浏览器 API 调用 AWS CloudTrail

WorkSpaces 安全浏览器与一项服务集成 AWS CloudTrail，该服务可记录用户、角色或 AWS 服务在 Amazon WorkSpaces 安全浏览器中执行的操作。 CloudTrail 将 Amazon WorkSpaces 安全浏览器的所有 API 调用捕获为事件。其中包括来自亚马逊 WorkSpaces 安全浏览器控制台的调用和对亚马逊 WorkSpaces 安全浏览器 API 操作的代码调用。如果您创建跟踪，则可以允许将 CloudTrail 事件持续传输到 Amazon S3 存储桶，包括亚马逊 WorkSpaces 安全浏览器的事件。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，您可以识别向 Amazon S WorkSpaces ecure Browser 发出的请求、发出请求的 IP 地址、发出请求的人、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。

主题

- WorkSpaces 中的安全浏览器信息 CloudTrail
- 了解 WorkSpaces 安全浏览器日志文件条目

## WorkSpaces 中的安全浏览器信息 CloudTrail

CloudTrail 在您创建 AWS 账户时已在您的账户上启用。当 Amazon WorkSpaces 安全浏览器中发生活动时，该活动会与其他 AWS 服务 CloudTrail 事件一起记录在事件历史记录中。在活动历史记录中，您可以查看、搜索和下载 AWS 账户中的近期事件。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 AWS 账户中的事件，包括亚马逊 WorkSpaces 安全浏览器的事件，您可以创建跟踪。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时，此跟踪应用于所有 AWS区域。跟踪记录 AWS 分区中所有区域的事件，并将日志文件传送到您指定的 Amazon S3 存储桶。此外，您可以配置其他 AWS 服务，以进一步分析和处理 CloudTrail 日志中收集的事件数据。有关更多信息，请参阅下列内容：

- 创建跟踪记录概述
- CloudTrail 支持的服务和集成
- 配置 Amazon SNS 通知 CloudTrail
- 接收来自多个地区的 CloudTrail 日志文件和接收来自多个账户的 CloudTrail 日志文件

所有亚马逊 WorkSpaces 安全浏览器操作均由《亚马逊 WorkSpaces API 参考》记录 CloudTrail 并记录在案。例如，调用`DeleteUserSettings`和`ListBrowserSettings`操作会在 CloudTrail 日志文件中生成条目。`CreatePortal`

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

- 请求是使用根用户凭证还是 IAM 用户凭证发出的。
- 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 WorkSpaces 安全浏览器日志文件条目

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、请求参数以及其他详细信息的信息。 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`ListBrowserSettings`操作的 CloudTrail 日志条目。

```
{
   "Records": [{
       "eventVersion": "1.08",
       "userIdentity": {
           "type": "IAMUser",
           "principalId": "111122223333",
           "arn": "arn:aws:iam::111122223333:user/myUserName",
           "accountId": "111122223333",
           "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
           "userName": "myUserName"
       },
       "eventTime": "2021-11-17T23:44:51Z",
       "eventSource": "workspaces-web.amazonaws.com",
       "eventName": "ListBrowserSettings",
       "awsRegion": "us-west-2",
       "sourceIPAddress": "127.0.0.1",
       "userAgent": "[]",
       "requestParameters": null,
       "responseElements": null,
```

```
        "requestID": "159d5c4f-c8c8-41f1-9aee-b5b1b632e8b2",
        "eventID": "d8237248-0090-4c1e-b8f0-a6e8b18d63cb",
        "readOnly": true,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "111122223333",
        "eventCategory": "Management"
    },
    {
        "eventVersion": "1.08",
        "userIdentity": {
            "type": "IAMUser",
            "principalId": "111122223333",
            "arn": "arn:aws:iam::111122223333:user/myUserName",
            "accountId": "111122223333",
            "accessKeyId": "AKIAIOSFODNN7EXAMPLE",
            "userName": "myUserName"
        },
        "eventTime": "2021-11-17T23:55:51Z",
        "eventSource": "workspaces-web.amazonaws.com",
        "eventName": "CreateUserSettings",
        "awsRegion": "us-west-2",
        "sourceIPAddress": "5127.0.0.1",
        "userAgent": "[]",
        "requestParameters": {
            "clientToken": "some-token",
            "copyAllowed": "Enabled",
            "downloadAllowed": "Enabled",
            "pasteAllowed": "Enabled",
            "printAllowed": "Enabled",
            "uploadAllowed": "Enabled"
        },
        "responseElements": "arn:aws:workspaces-web:us-
west-2:111122223333:userSettings/04a35a2d-f7f9-4b22-af08-8ec72da9c2e2",
        "requestID": "6a4aa162-7c1b-4cf9-a7ac-e0c8c4622117",
        "eventID": "56f1fbee-6a1d-4fc6-bf35-a3a71f016fcb",
        "readOnly": false,
        "eventType": "AwsApiCall",
        "managementEvent": true,
        "recipientAccountId": "111122223333",
        "eventCategory": "Management"
    }]
}
```

# 在 Amazon WorkSpaces 安全浏览器中登录用户访问权限

Amazon WorkSpaces 安全浏览器允许客户记录会话事件，包括开始、停止和 URL 访问。这些日志将传送到您为 Web 门户指定的 Amazon Kinesis Data Streams。有关更多信息，请参阅 the section called “设置用户访问日志记录”。

# Amazon WorkSpaces 安全浏览器用户指南

管理员使用 WorkSpaces 安全浏览器创建连接到公司网站（例如内部网站、 software-as-a-service (SAAS) Web 应用程序或互联网）的 Web 门户。最终用户使用其现有的 Web 浏览器来访问这些 Web 门户，以便启动会话和访问内容。

以下内容有助于指导想要详细了解如何访问 WorkSpaces 安全浏览器、启动和配置会话以及使用工具栏和 Web 浏览器的终端用户。

主题


- Amazon WorkSpaces 安全浏览器的浏览器和设备兼容性
- Amazon WorkSpaces 安全浏览器的门户网站访问权限
- Amazon WorkSpaces 安全浏览器的会话指南
- 在 Amazon WorkSpaces 安全浏览器中解决用户问题
- Amazon WorkSpaces 安全浏览器的单点登录扩展程序


## Amazon WorkSpaces 安全浏览器的浏览器和设备兼容性

Amazon WorkSpaces Secure Browser 由 Amazon DCV 网络浏览器客户端提供支持，该客户端在网络浏览器中运行，因此无需安装。常见的 Web 浏览器（例如 Chrome 和 Firefox）以及主要的桌面操作系统（例如 Windows、macOS 和 Linux）都支持 Web 浏览器客户端。

有关 Web 浏览器客户端支持的 up-to-date更多详细信息，请参阅 Web 浏览器客户端。

> **Note**
>
> 目前，只有基于 Chromium 的浏览器（例如 Google Chrome 和 Microsoft Edge）才支持摄像头。目前，苹果 Safari 和 Mozilla FireFox 不支持网络摄像头。

## Amazon WorkSpaces 安全浏览器的门户网站访问权限

您的管理员可以通过以下选项提供对您的 Web 门户的访问权限：

- 您可以从电子邮件或网站中选择链接，然后使用您的 SAML 身份凭证登录。

- 您可以登录您的 SAML 身份提供者（例如 Okta、Ping 或 Azure），然后在 SAML 提供者的应用程序主页（例如 Okta 最终用户控制面板或 Azure Myapps 门户）上单击一下即可启动会话。

# Amazon WorkSpaces 安全浏览器的会话指南

登录 Web 门户后，您可以启动会话并在会话期间执行各种操作。

主题


- 在 Amazon WorkSpaces 安全浏览器中启动会话
- 使用 Amazon WorkSpaces 安全浏览器中的工具栏
- 在 Amazon WorkSpaces 安全浏览器中使用浏览器
- 在 Amazon WorkSpaces 安全浏览器中结束会话


## 在 Amazon WorkSpaces 安全浏览器中启动会话

登录并启动会话后，您将看到启动会话消息和进度条。这表明 Amazon WorkSpaces 安全浏览器正在为您创建会话。在幕后，Amazon WorkSpaces Secure Browser 正在创建实例、启动托管 Web 浏览器以及应用管理员设置和浏览器策略。

如果这是您首次登录 Web 门户，您将在工具栏中看到蓝色 + 图标。此图标表示有教程可用，该教程将引导您浏览工具栏中的可用功能。您可以使用这些图标来了解如何执行以下操作：

- 通过选择本地浏览器旁边的锁图标，然后将剪贴板、麦克风和摄像头旁边的开关设置为开，为浏览器授予麦克风、摄像头和剪贴板权限。

> **Note**
>
> 如果您在首次会话启动时启用摄像头权限，摄像头会短暂启用，计算机上的指示灯将会闪烁。这将授予本地浏览器访问您摄像头的权限。

- 选择浏览器中的锁定图标并设置为 “始终允许弹出窗口”，即可启用 Amazon S WorkSpaces ecure Browser 启动其他监视窗口。

如果您想重新启动教程，可以从工具栏中选择个人资料，然后选择帮助和启动教程。

# 使用 Amazon WorkSpaces 安全浏览器中的工具栏

要了解如何使用工具栏，请按照以下步骤操作。

要移动工具栏，请选择工具栏顶部亮显的栏，将其拖动到所需位置，然后松开将其放下。

要折叠工具栏，请将鼠标指针悬停在工具栏上并选择向上箭头按钮，或者双击顶部亮显的栏。折叠视图可为您提供更多的屏幕空间，并且可以一键访问最常用的图标。

要增加显示大小，请选择浏览器窗口并放大。要增加工具栏图标和文本的显示大小，请选择工具栏并放大。

要在 Windows 设备上放大或缩小，请按照以下步骤操作：

1. 选择工具栏或 Web 内容。
2. 按 Ctrl + + 放大，或按 Ctrl + - 缩小。

要在 Mac 设备上放大或缩小，请按照以下步骤操作：

1. 选择工具栏或 Web 内容。
2. 按 Cmd + + 放大，或按 Cmd + - 缩小。

要将工具栏停靠在屏幕顶部，请在工具栏模式下选择首选项、常规和停靠。

下表介绍了工具栏中所有可用的图标：

| Icon | Title | Description |
| --- | --- | --- |
| | **Windows** | Move between windows or launch additional browser windows. |
| | **Launch additional monitor window** | Launch an additional monitor window with a separate browser window. Then drag to your secondary monitor. |
| | **Full screen** | Launch a full screen experience view. |
| | **Microphone** | Activate mic input for the session. Use the down arrow to select from a list of available microphones. |
| | **Webcam** | Activate webcam for the session. Use the down arrow to select from a list of available webcams. |
| | **Preferences** | Access the **General** and **Keyboard** menus. From the **General** menu, toggle between light and dark mode, activate the keyboard input selector (for changing the keyboard language), and switch between streaming mode or display resolution. From the **Keyboard** menu, change the option and command key settings (on Mac devices), or activate **Functions** (see below). |
| | **Profile** | End your session, view performance metrics, access **Feedback** and **Help**, and learn about Amazon WorkSpaces Web. **End Session** ends the Amazon WorkSpaces Web session.<br><br>**Performance metrics** displays the frame rate, network latency, and bandwidth usage graph. This information is useful for administrators when investigating issues with the service.<br><br>**Feedback** provides you with an email address to share feedback to the Amazon WorkSpaces Web team.<br><br>**Help** provides you with access to Frequently Asked Questions, such as how to use the clipboard, microphone, and webcam during the session, or how to troubleshoot launching an additional monitor window. From help, you can also launch the tutorial or user guide.<br><br>**About** provides more information about Amazon WorkSpaces Web. |
| | **Notifications** | Get one-click access to session notifications. |
| | **Clipboard** | Access clipboard shortcut descriptions, links to set the command key preference, and troubleshoot clipboard permissions from the local web browser. You can use the content preview text box to test clipboard functionality. This icon only displays if clipboard permission is granted by your administator. |
| | **Files** | From the files menu, you can upload content to the remote browser. Once uploaded, you can rename, download, or delete, as well as create folders in the temporary file menu. All files and data in **Files** are deleted at the end of the session. This icon only displays if **Files** permission is granted by your administator. |

> **Note**
>
> 剪贴板和文件图标默认处于隐藏状态，除非管理员授予这些权限。只有管理员才能在 Web 门户上启用或禁用剪贴板和文件。如果这些图标已隐藏，而您需要访问它们，请联系您的管理员。

## 在 Amazon WorkSpaces 安全浏览器中使用浏览器

启动会话时，浏览器会显示启动 URL，这是管理员选择的 URL。如果管理员未选择启动 URL，您将会在 Google Chrome 中看到默认新选项卡体验。

在浏览器中，您可以打开选项卡、启动其他浏览器窗口（从 Windows 工具栏图标或浏览器的三点菜单）、输入 URL 或在 URL 栏中搜索，或者通过管理的书签进入网站。要访问 Web 门户的书签，请打开书签栏（URL 栏下方）上的管理的书签文件夹，或者从 URL 栏右侧的三点菜单中打开书签管理器。

要调整或移动浏览器窗口，请向下拖动 Chrome 页框。这将允许在会话期间针对多个浏览器窗口提供更多的屏幕空间。

> **Note**
>
> 如果管理员已将浏览器功能（例如无痕模式）关闭，则这些功能可能在您的会话期间不可用。

## 在 Amazon WorkSpaces 安全浏览器中结束会话

要结束会话，请选择配置文件和结束会话。会话结束后，Amazon WorkSpaces 安全浏览器会删除会话中的所有数据。会话结束后，浏览器数据不可用，例如打开的网站或历史记录，或者文件资源管理器中的文件或数据。

如果您在会话活动期间关闭选项卡，则会话将在管理员设置的一段时间后结束。如果您在此超时生效之前关闭选项卡并重新访问 Web 门户，则可以加入当前会话并查看之前的所有会话数据，例如打开的网站和文件。

# 在 Amazon WorkSpaces 安全浏览器中解决用户问题

如果您在使用 WorkSpaces 安全浏览器时遇到以下任何问题，请尝试以下解决方案。

我 WorkSpaces 的 Amazon 安全浏览器门户不允许我登录。我收到了一条错误消息，显示“您的 Web 门户尚未设置。如需帮助，请联系您的 IT 管理员。”

您的管理员需要使用 SAML 2.0 身份提供者完成门户创建才能让您登录。如需帮助，请联系您的管理员。

我的门户无法启动会话。我收到了一条错误消息，显示“无法预约会话。发生内部错误。请重试。”

您的 Web 门户会话启动出现问题。请尝试再次启动会话。如果仍然存在问题，请联系您的管理员寻求帮助。

我无法使用剪贴板、麦克风或摄像头。

要允许浏览器权限，请选择 URL 旁边的锁图标，然后切换剪贴板、麦克风、摄像头、弹出窗口和重定向旁边的蓝色开关，以开启这些功能。

> **Note**
>
> 如果您的 Web 浏览器不支持视频或音频输入，则这些选项将不会显示在工具栏上。

Amazon WorkSpaces Secure Browser 实时音频-视频 (AV) 将您的本地网络摄像头视频和麦克风音频输入重定向到浏览器直播会话。如此一来，您就可以使用本地设备通过基于 Chromium 的 Web 浏览器（例如 Google Chrome 或 Microsoft Edge），在流会话中进行视频和音频会议。非 Chromium 浏览器目前不支持网络摄像头。

有关如何配置 Google Chrome 的信息，请参阅使用摄像头和麦克风。

我的 Web 门户不启动其他显示器窗口。

如果您尝试启动双显示器并在顶部浏览器的地址栏末尾看到弹出窗口被阻止图标，请选择始终允许弹出窗口和重定向旁边的图标和单选按钮。允许弹出窗口后，选择工具栏上的双显示器图标以启动新窗口，在显示器上重新定位窗口，然后将浏览器选项卡拖到窗口中。

我尝试从文件窗格下载文件时，没有任何反应。

如果您尝试从文件窗格中下载文件并在顶部浏览器的地址栏末尾看到弹出窗口被阻止图标，请选择始终允许弹出窗口和重定向旁边的图标和单选按钮。允许弹出窗口后，请尝试再次下载文件。

我怎样才能知道正在使用哪个麦克风和/或摄像头，以及如何进行更改？

单击麦克风或摄像头旁边的向下箭头图标。菜单显示可用设备，并带有复选标记，表示您当前的设备。选择其他设备来更改要用于会话的设备。

# Amazon WorkSpaces 安全浏览器的单点登录扩展程序

Amazon WorkSpaces Secure Browser 提供了在台式电脑上使用 Chrome 和 Firefox 浏览器进行单点登录的扩展程序。如果您的管理员启用了该扩展，则 Web 门户将在您登录时要求您安装该扩展。

Amazon WorkSpaces Secure Browser 构建的扩展程序是为了在您的会话期间启用网站的单点登录。例如，如果您使用 SAML 2.0 身份提供者（例如 Okta 或 Ping）登录您的门户，并且在会话期间访问使用相同身份提供者的网站，则该扩展可以通过删除其他登录提示来简化网站的访问。

您无需安装扩展即可访问您的 Web 门户，但它可以减少要求您输入用户名和密码的次数，从而改善您的使用体验。

当您登录时，扩展会找到您的管理员为您的会话列出的 Cookie。扩展找到的所有数据在静态和传输过程中都经过加密。这些数据都不会存储在您的本地浏览器中。当您结束会话时，您的所有会话数据（例如打开的选项卡、下载的文件以及会话期间发送或创建的 Cookie）都将被删除。

主题


- Amazon WorkSpaces 安全浏览器的单点登录扩展兼容性
- 为 Amazon WorkSpaces 安全浏览器安装单点登录扩展程序
- Amazon WorkSpaces 安全浏览器的单点登录扩展程序疑难解答


## Amazon WorkSpaces 安全浏览器的单点登录扩展兼容性

单点登录扩展适用于以下设备和浏览器：

- 设备
  - 笔记本电脑
  - 台式电脑
- 浏览器
  - Google Chrome
  - Mozilla Firefox

## 为 Amazon WorkSpaces 安全浏览器安装单点登录扩展程序

要安装单点登录扩展，请按照以下步骤操作。

登录门户时，请按照提示安装适用于您的 Chrome 或 Firefox 浏览器的扩展。对于每个 Web 浏览器，您只需要执行一次此操作。

如果您切换设备，在同一设备上切换到其他浏览器，或者从本地浏览器中删除扩展，则在启动下一次会话时，您会看到安装扩展的提示。

为确保扩展按预期运行，请在普通浏览窗口上使用该扩展，不要以无痕模式（Chrome）或私密浏览模式（Firefox）使用。

## Amazon WorkSpaces 安全浏览器的单点登录扩展程序疑难解答

在使用单点登录扩展时，您可能会遇到以下问题。

如果您已安装扩展，但在会话期间仍被要求登录，请按照以下步骤操作：

1. 确保您的浏览器上安装了 Amazon WorkSpaces 安全浏览器扩展程序。如果您删除了浏览器数据，则可能意外删除了扩展。
2. 确保您未使用无痕模式（Chrome）或私密浏览模式（Firefox）。这些模式可能会导致扩展出现问题。
3. 如果问题仍然存在，请联系您的门户管理员以获取更多帮助。

# 《Amazon WorkSpaces 安全浏览器管理指南》的文档历史记录

下表描述了 Amazon WorkSpaces 安全浏览器的文档版本。

| 变更 | 说明 | 日期 |
| --- | --- | --- |
| 工具栏控件 | 使用工具栏控件，您可以为最终用户会话配置工具栏的显示方式。 | 2025年2月21日 |
| APIs 使用接口 VPC 终端节点进行访问 (AWS PrivateLink) | 直接从私有云 (VPC) 内调用 Amazon WorkSpaces 安全浏览器 API 终端节点，而不是通过互联网进行连接。 | 2025 年 1 月 10 日 |
| 数据保护设置 | 添加数据保护设置以帮助保护数据在会话期间不被共享。 | 2024 年 11 月 20 日 |
| FIPS 端点 | 使用 FIPS 端点保护传输中数据 | 2024 年 10 月 7 日 |
| 会话管理控制面板 | 使用会话管理控制面板可监控和管理活动会话与已完成的会话。 | 2024 年 9 月 19 日 |
| 支持使用深层链接 | 支持门户在会话期间接收将用户连接到特定网站的深层链接。 | 2024 年 6 月 25 日 |
| 托管式策略更新 | 添加了 AmazonWorkSpacesSecureBrowserReadOnly 托管策略 | 2024 年 6 月 24 日 |
| 使用工具栏进行缩放 | 您可以使用工具栏增加显示、图标和文本的大小。 | 2024 年 5 月 1 日 |

| | | |
|---|---|---|
| 新 Web 门户设置 | 现在，您可以为 Web 门户指定实例类型和最大并发用户限制。 | 2024 年 4 月 22 日 |
| CloudWatch 指标 | 添加了 GlobalCpuPercent 和 GlobalMemoryPercent 指标。 | 2024 年 2 月 26 日 |
| 设置 URL 筛选 | 您可以使用 Chrome 政策来筛选哪些 URLs 用户可以通过远程浏览器进行访问。 | 2024 年 2 月 21 日 |
| IdP 身份验证类型 | 您可以选择标准身份验证类型或 IAM Identity Center 身份验证类型。 | 2024 年 2 月 5 日 |
| 启用单点登录扩展 | 您可以为最终用户启用扩展，以获得更好的门户登录体验。 | 2023 年 8 月 28 日 |
| Amazon WorkSpaces 安全浏览器的用户指南 | 添加了帮助指导想要详细了解如何访问 Amazon S WorkSpaces ecure Browser、启动和配置会话以及使用工具栏和网络浏览器的终端用户的内容。 | 2023 年 7 月 17 日 |
| IP 访问控制 | WorkSpaces 安全浏览器允许您控制可以从哪些 IP 地址访问您的门户网站。 | 2023 年 5 月 31 日 |
| 托管式策略更新 | 更新了 AmazonWor kSpacesWebReadOnly 托管策略 | 2023 年 5 月 15 日 |
| 配置身份提供者更新 | WorkSpaces 安全浏览器提供两种身份验证类型：标准和 AWS IAM Identity Center | 2023 年 3 月 15 日 |
| 浏览器策略更新 | 更新并调整了浏览器策略部分 | 2023 年 1 月 31 日 |

| | | |
|---|---|---|
| 托管式策略更新 | 更新了 AmazonWorkSpacesWebServiceRolePolicy 托管策略 | 2022 年 12 月 15 日 |
| 允许列表和阻止列表 | 指定允许列表和阻止列表，以指定您的用户可以或无法访问的域列表。 | 2022 年 11 月 14 日 |
| 托管式策略更新 | 更新了 AmazonWorkSpacesWebReadOnly 托管策略 | 2022 年 11 月 2 日 |
| 托管式策略更新 | 更新了 AmazonWorkSpacesWebServiceRolePolicy 托管策略 | 2022 年 10 月 24 日 |
| 用户访问日志记录 | 设置用户访问日志记录以记录用户事件 | 2022 年 10 月 17 日 |
| 联网更新 | 对“联网和访问”部分进行的各种更新 | 2022 年 9 月 22 日 |
| 托管式策略更新 | 更新了 AmazonWorkSpacesWebServiceRolePolicy 托管策略 | 2022 年 9 月 6 日 |
| 配置用户会话 | 配置输入法编辑器（IME）和会话内本地化 | 2022 年 7 月 28 日 |
| 联网更新 | 对“联网和访问”部分进行的各种更新 | 2022 年 7 月 7 日 |
| 超时值 | 指定断开连接超时(分钟)和空闲断开连接超时(分钟) | 2022 年 5 月 16 日 |

| | | |
|---|---|---|
| 更新了托管策略 | 更新了 AmazonWorkSpacesWebServiceRolePolicy 托管策略，将 AWS/Usage 命名空间添加到 API 权限中 PutMetricData | 2022 年 4 月 6 日 |
| 服务相关角色 | 新的 AWSServiceRoleForAmazonWorkSpacesWeb 服务相关角色 | 2021 年 11 月 30 日 |
| 托管式策略 | 新的 AmazonWorkSpacesWebReadOnly 托管策略 | 2021 年 11 月 30 日 |
| 托管式策略 | 新的 AmazonWorkSpacesWebServiceRolePolicy 托管策略 | 2021 年 11 月 30 日 |
| 初始版本 | 《WorkSpaces 安全浏览器管理指南》的初始版本 | 2021 年 11 月 30 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。