aws

管理指南

AWS Wickr

AWS Wickr: 管理指南

Table of Contents

什么是 AWS Wickr？

AWS Wickr 是一项 end-to-end加密服务，可帮助组织和政府机构通过 one-to-one群组消息、语音和视频通话、文件共享、屏幕共享等进行安全通信。Wickr 可以帮助客户克服与消费级消息传递应用程序相关的数据留存义务，并安全地促进协作。先进的安全和管理控制措施可帮助组织满足法律和监管要求，并针对数据安全挑战构建定制解决方案。

可以将信息记录到客户控制的私有数据存储中，以便保留和审计。用户可以对数据进行全面的管理控制，包括设置权限、配置临时消息选项和定义安全组。Wickr 与其他服务集成，例如 Active Directory (AD)、带有 OpenID Connect 的单点登录 (SSO) (OIDC) 等。您可以通过快速创建和管理 Wickr 网络 AWS 管理控制台，并使用 Wickr 机器人安全地自动执行工作流程。要开始使用，请参阅设置 AWS Wickr。

主题

Wickr 功能

加强的安全性和隐私性

Wickr 对每项功能都使用 256 位高级加密标准 (AES) end-to-end 加密。通信在用户设备上进行本地加密，在传输给除发送方和接收方之外的任何人时，通信仍无法被破解。每条消息、通话和文件都使用新的随机密钥加密，除了预期的收件人（甚至不是 AWS）之外，任何人都无法解密它们。无论他们是在共享敏感和受监管的数据、讨论法律或人力资源事务，还是进行战术军事行动，客户都可以在安全和隐私至关重要的时候使用 Wickr 进行沟通。

数据留存

灵活的管理功能不仅可以保护敏感信息，还可以根据合规义务、法律保留和审计目的保留数据。消息和文件可以存档在安全的、由客户控制的数据存储中。

灵活的访问

用户可以访问多设备（移动设备、台式机），并且能够在低带宽环境中工作，包括断开连接和 out-of-band通信。

管理控制

用户可以对数据进行全面的管理控制，包括设置权限、配置负责任的临时消息选项和定义安全组。

强大的集成和机器人

Wickr 与其他服务集成，例如 Active Directory、带有 OpenID Connect 的单点登录 (SSO) (OIDC) 等。客户可以通过快速创建和管理 Wickr 网络 AWS 管理控制台，并使用 Wickr Bots 安全地自动执行工作流程。

以下是 Wickr 协作服务的详细介绍：

- 1:1 和群组消息：在最多可容纳 500 名成员的房间中与您的团队安全聊天
- 音频和视频通话：与最多 70 人进行电话会议
- 屏幕共享和广播：最多可容纳 500 名参与者
- 文件共享和保存：GBs 使用无限存储空间传输最多 5 个文件
- 短暂：控制到期时间和计时器 burn-on-read
- 全球联合身份验证：与网络之外的 Wickr 用户建立联系

区域可用性

Wickr 在美国东部（弗吉尼亚北部）、亚太地区（马来西亚）、亚太地区（新加坡）、亚太地区（悉尼）、亚太地区（东京）、加拿大（中部）、欧洲（法兰克福）、欧洲（伦敦）、欧洲（斯德哥尔摩）和欧洲（苏黎世） AWS 区域上市。Wickr 也在 AWS GovCloud （美国西部）地区上市。每个区域都包含多个可用区，这些可用区在物理上是独立的，但通过专用、低延迟、高带宽和冗余网络连接相连。这些可用区域用于提供增强的可用性、容错能力和最小化延迟。

要了解更多信息 AWS 区域，请参阅中的指定 AWS 区域 您的账户可以使用的内容AWS 一般参考。有关每个区域可用区域数量的更多信息，请参阅AWS 全球基础设施。

访问 Wickr

管理员可在以下网址 AWS 管理控制台 访问 Wickr 的。https://console.aws.amazon.com/wickr/在开始使用 Wickr 之前，您应该完成 设置 AWS Wickr 和 AWS Wickr 入门 指南。

最终用户通过 Wickr 客户端访问 Wickr。有关更多信息，请参阅 AWS Wickr 用户指南。

定价

Wickr 有不同的套餐可供个人、小型团队和大型企业使用。有关更多信息，请参阅 AWS Wickr 定价。

Wickr 最终用户文档

如果您是 Wickr 客户端的最终用户并且需要访问其文档，请参阅 AWS Wickr 用户指南。

设置 AWS Wickr

注册获取 AWS 账户

要开始使用 AWS，你需要一个 AWS 账户。有关创建的信息 AWS 账户，请参阅《AWS 账户管理 参考指南》 AWS 账户中的入门指南。

接下来做什么

您已完成先决条件设置步骤。要开始配置 Wickr，请参阅 开始使用。

AWS Wickr 入门

在该指南中，我们将介绍如何通过创建网络、配置网络和创建用户来开始使用 Wickr。

主题

先决条件

在开始之前，请确保完成以下前提条件（如果您尚未完成）。

- 注册 Amazon Web Services (AWS)。有关更多信息，请参阅 设置 AWS Wickr。
- 确保拥有管理 Wickr 所需的权限。有关更多信息，请参阅 AWS托管策略： AWSWickrFullAccess。
- 确保允许列出 Wickr 的相应端口和域。有关更多信息，请参阅 允许列出 Wickr 网络的端口和域名。

步骤 1：创建网络

你可以创建一个 Wickr 网络。

完成以下过程为您的账户创建一个 Wickr 网络。

1. 在 f AWS 管理控制台 or Wickr 上https://console.aws.amazon.com/wickr/打开。

   > **Note**
   >
   > 如果您之前尚未创建 Wickr 网络，则会看到 Wickr 服务的信息页面。创建一个或多个 Wickr 网络后，您会看到网络页面，其中包含您创建的所有 Wickr 网络的列表视图。

2. 选择创建网络。
3. 在网络名称文本框中输入网络名称。选择您的组织成员可以识别的名称，例如公司的名称或团队的名称。
4. 选择一个计划。您可以选择以下 Wickr 网络计划之一：

- 标准- 适用于需要管理控制和灵活性的小型和大型企业团队。
- 高级版或高级版免费试用 — 适用于需要最高功能限制、精细管理控制和数据保留的企业。

管理员可以选择高级免费试用版，该试用版最多可供30个用户使用，有效期为三个月。对于 AWS WickrGov，高级免费试用选项最多允许 50 名用户，并且持续三个月。在高级版免费试用期内，管理员可以升级或降级到高级版或标准版计划。

有关可用的 Wickr 计划和定价的更多信息，请参阅 Wickr 定价页面。

5. （可选）选择添加新标签为您的网络添加一个标签。标签由一个键值对组成。您可以使用标签来搜索和筛选资源或跟踪 AWS 成本。有关更多信息，请参阅网络标签。
6. 选择 “创建网络”。

您将被重定向到 f or Wickr AWS 管理控制台 的 “网络” 页面，新网络将列在页面上。

第 2 步：配置网络

完成以下步骤以访问 Wickr AWS 管理控制台 的，您可以在其中添加用户、添加安全组、配置 SSO、配置数据保留和其他网络设置。

1. 在 “网络” 页面上，选择要导航到该网络的网络名称。

   您将被重定向到所选网络的 Wickr 管理员控制台。
2. 以下用户管理选项可用。有关配置这些设置的更多信息，请参阅 管理 AWS Wickr 网络。

   - 安全组 — 管理安全组及其设置，例如密码复杂性策略、消息传递首选项、呼叫功能、安全功能和外部联合身份验证。有关更多信息，请参阅 AWS Wickr 的安全组。
   - 单点登录 (SSO) 配置-配置 SSO 并查看 Wickr 网络的端点地址。Wickr 仅支持使用 OpenID Connect (OIDC) 的 SSO 提供者。不支持使用安全断言标记语言 (SAML) 的提供商。有关更多信息，请参阅 AWS Wickr 的单点登录配置。

步骤 3：创建并邀请用户

可以使用以下方法在 Wickr 网络中创建用户：

- 单点登录 — 如果要配置 SSO，您可通过共享您的 Wickr 公司 ID 来邀请用户。最终用户使用提供的公司 ID 和工作电子邮件地址注册 Wickr。有关更多信息，请参阅 AWS Wickr 的单点登录配置。

- 邀请 — 您可以在 Wickr 的 AWS 管理控制台 中手动创建用户，并向他们发送电子邮件邀请。最终用户可以通过选择电子邮件中的链接来注册 Wickr。

> **Note**
>
> 您还可以为 Wickr 网络启用访客用户。有关更多信息，请参阅 AWS Wickr 网络中的访客用户。

完成以下过程以创建或邀请用户。

> **Note**
>
> 管理员也被视为用户，必须邀请自己加入 SSO 或非 SSO Wickr 网络。

要创建 Wickr 用户并通过 SSO 发送邀请，请执行以下操作：

写一封电子邮件给应当注册 Wickr 的 SSO 用户。在您的电子邮件中，请包含以下信息：

- 您的 Wickr 公司账号。在配置 SSO 时，您可以为 Wickr 网络指定一个公司 ID。有关更多信息，请参阅 在 AWS Wickr 中配置 SSO。
- 他们注册时应使用的电子邮件地址。
- 下载 Wickr 客户端的 URL。用户可以从 AWS Wickr 下载页面下载 Wickr 客户端，网址为 downlo https://aws.amazon.com/wickr/ ad/。

  > **Note**
  >
  > 如果您在 AWS GovCloud （美国西部）创建了 Wickr 网络，请指导您的用户下载并安装客户端。 WickrGov 对于所有其他 AWS 区域，请指导您的用户下载并安装标准 Wickr 客户端。有关的更多信息 AWS WickrGov，请参阅《AWS GovCloud (US) 用户指南》AWS WickrGov中的。

当用户注册您的 Wickr 网络时，他们会被添加到 Wickr 团队目录，状态为活跃。

手动创建 Wickr 用户并发送邀请：

1. 在 f AWS 管理控制台 or Wickr 上https://console.aws.amazon.com/wickr/打开。
2. 在“网络”页面上，选择要导航到该网络的网络名称。

   您将被重定向到 Wickr 网络。在 Wickr 网络中，您可以添加用户、添加安全组、配置 SSO、配置数据保留以及调整其他设置。
3. 在导航窗格中，选择用户管理。
4. 在用户管理页面的团队目录选项卡下，选择邀请用户。

   您也可以通过选择邀请用户旁边的下拉箭头来批量邀请用户。在批量邀请用户页面上，选择下载模板以下载 CSV 模板，您可以编辑该模板并将其与用户列表一起上传。
5. 输入用户的名字、姓氏、国家/地区代码、电话号码和电子邮件地址。电子邮件地址是唯一必填字段。请务必为用户选择合适的安全组。
6. 选择邀请。

   Wickr 将邀请电子邮件发送到您为该用户指定的地址。电子邮件提供了 Wickr 客户端应用程序的下载链接以及注册 Wickr 的链接。有关这种最终用户体验如何的更多信息，请参阅《AWS Wickr 用户指南》中的下载 Wickr 应用程序并接受邀请。

   当用户使用电子邮件中的链接注册 Wickr 时，他们在 Wickr 团队目录中的状态将从待定变为活跃。

后续步骤

您已完成开始任务步骤。要管理 Wickr，请参阅以下内容：

- 管理 AWS Wickr 网络
- 在 AWS Wickr 中管理用户

管理 AWS Wickr 网络

在 f AWS 管理控制台 or Wickr 中，你可以管理你的 Wickr 网络名称、安全组、SSO 配置和数据保留设置。

主题

AWS Wickr 的网络详情

您可以在 for Wickr 的 “网络详情” 部分中编辑 Wickr 网络名称并查看您的网络 ID。AWS 管理控制台

主题

在 AWS Wickr 中查看网络详情

您可以查看 Wickr 网络的详细信息，包括您的网络名称和网络 ID。

完成以下过程以查看 Wickr 网络配置文件和网络 ID。

1. 在 f AWS 管理控制台 or Wickr 上https://console.aws.amazon.com/wickr/打开。
2. 在网络页面上，找到您要查看的网络。
3. 在要查看的网络的右侧，选择垂直省略号图标（三个点），然后选择查看详细信息。

   网络主页在 “网络详情” 部分中显示您的 Wickr 网络名称和网络 ID。您可以使用网络 ID 来配置联合身份验证。

在 AWS Wickr 中编辑网络名称

您可以编辑 Wickr 网络的名称。

完成以下过程以编辑 Wickr 网络名称。

1. 在 f AWS 管理控制台 or Wickr 上https://console.aws.amazon.com/wickr/打开。
2. 在 “网络” 页面上，选择网络名称以导航到该网络的 Wickr 管理控制台。
3. 在网络主页的网络详细信息部分，选择编辑。
4. 在网络名称文本框中输入新的网络名称。
5. 选择 “保存” 以保存您的新网络名称。

在 AWS Wickr 中删除网络

您可以删除您的 AWS Wickr 网络。

> **Note**
>
> 如果您删除了付费免费试用网络，则将无法再创建一个。

要在 Networks 主页上删除您的 Wickr 网络，请完成以下步骤。

1. 在 f AWS 管理控制台 or Wickr 上https://console.aws.amazon.com/wickr/打开。
2. 在 “网络” 页面上，找到要删除的网络。
3. 在要删除的网络的右侧，选择垂直省略号图标（三个点），然后选择删除网络。
4. 在弹出窗口中键入确认，然后选择删除。

删除网络可能需要几分钟。

要在网络中删除您的 Wickr 网络，请完成以下步骤。

1. 在 f AWS 管理控制台 or Wickr 上https://console.aws.amazon.com/wickr/打开。
2. 在“网络”页面上，选择要删除的网络。
3. 在网络主页右上角附近，选择删除网络。
4. 在弹出窗口中键入确认，然后选择删除。

   删除网络可能需要几分钟。

> **Note**
>
> 删除网络时，您的数据保留配置（如果启用）保留的数据不会被删除。有关更多信息，请参阅 AWS Wickr 的数据保留。

AWS Wickr 的安全组

在 for Wickr AWS 管理控制台 的“安全组”部分，您可以管理安全组及其设置，例如密码复杂性策略、消息首选项、呼叫功能、安全功能和网络联合。

主题

- 在 AWS Wickr 中查看安全组
- 在 AWS Wickr 中创建安全组
- 在 AWS Wickr 中编辑安全组
- 在 AWS Wickr 中删除安全组

在 AWS Wickr 中查看安全组

您可以查看 Wickr 安全组的详细信息。

完成以下过程以查看安全组。

1. 在 f AWS 管理控制台 or Wickr 上https://console.aws.amazon.com/wickr/打开。

2. 在“网络”页面上，选择要导航到该网络的网络名称。
3. 在导航窗格中，选择安全组。

   安全组页面显示您当前的 Wickr 安全组，并允许您选择创建新组。

   在安全组页面上，选择要查看的安全组。该页面将显示该安全组的当前详细信息。

在 AWS Wickr 中创建安全组

您可以创建新的 Wickr 安全组。

完成以下过程以创建安全组。

1. 在 f AWS 管理控制台 or Wickr 上https://console.aws.amazon.com/wickr/打开。
2. 在“网络”页面上，选择要导航到该网络的网络名称。
3. 在导航窗格中，选择安全组。
4. 在安全组页面上，选择创建安全组以创建新的安全组。

   > **Note**
   >
   > 具有默认名称的新安全组将自动添加到安全组列表。

5. 在创建安全组页面上，输入您的安全组的名称。
6. 选择创建安全组。

   有关编辑新安全组的更多信息，请参阅 在 AWS Wickr 中编辑安全组。

在 AWS Wickr 中编辑安全组

您可以编辑 Wickr 安全组的详细信息。

完成以下过程以编辑安全组。

1. 在 f AWS 管理控制台 or Wickr 上https://console.aws.amazon.com/wickr/打开。
2. 在“网络”页面上，选择要导航到该网络的网络名称。
3. 在导航窗格中，选择安全组。
4. 选择要编辑的安全组的名称。

安全组详细信息页面在不同的选项卡中显示安全组的设置。

5. 以下选项卡和相应的设置可用：

- 安全组详细信息-在安全组详细信息部分选择编辑以编辑名称。
- 消息 — 管理群组成员的消息传递功能。
  - Burn-on-read— 控制用户可以在 Wickr 客户端中为读取时刻录计时器设置的最大值。有关更多信息，请参阅在 Wickr 客户端中设置消息到期时间和刻录计时器。
  - 过期计时器 — 控制用户可以在 Wickr 客户端中为消息过期计时器设置的最大值。有关更多信息，请参阅在 Wickr 客户端中设置消息到期时间和刻录计时器。
  - 消息转发-控制用户是否可以在其 Wickr 客户端中转发消息。有关更多信息，请参阅在 Wickr 客户端中转发消息。
  - 快速回复-设置快速回复列表，供用户回复消息。
  - 安全碎纸机强度-为用户配置安全碎纸机控件的运行频率。有关更多信息，请参阅消息。
- 通话 — 管理群组成员的呼叫功能。
  - 启用音频通话-用户可以发起音频通话。
  - 启用视频通话和屏幕共享-用户可以在通话期间开始视频通话或共享屏幕。
  - TCP 呼叫 — 当组织的 IT 或安全部门不允许使用标准 VoIP UDP 端口时，通常使用启用（或强制）TCP 呼叫。如果 TCP 调用被禁用，并且无法使用 UDP 端口，Wickr 客户端将首先尝试 UDP，然后回退到 TCP。
- 媒体和链接-为群组成员管理与媒体和链接相关的设置。

  文件下载大小-选择“最佳质量传输”，允许用户以原始加密形式传输文件和附件。如果您选择低带宽传输，Wickr 文件传输服务将压缩用户在 Wickr 中发送的文件附件。
- 位置-管理群组成员的位置共享设置。

  位置共享-用户可以使用 GPS-enabled 设备共享其位置。此功能根据设备的操作系统默认值显示可视地图。用户可以选择禁用地图视图并共享包含其 GPS 坐标的链接。
- 安全 — 为群组配置其他安全功能。
  - 启用账户接管保护-当用户向其账户添加新设备时，强制执行双重身份验证。要验证新设备，用户可以从其旧设备生成 Wickr 代码，或者执行电子邮件验证。这是一层额外的安全保护，可防止未经授权访问 AWS Wickr 账户。
  - 启用始终重新身份验证-强制用户在重新进入应用程序时始终重新进行身份验证。

- 主恢复密钥-创建账户时创建主恢复密钥。如果没有其他设备可用，用户可以批准在其帐户中添加新设备。
- 非 SSO 超时 — 为要求在一段绝对时间后在应用程序中重新输入密码的非 SSO 用户配置会话超时，无论用户活动如何。

- 通知和可见性-为群组成员配置通知和可见性设置，例如通知中的消息预览。
- Wickr 开放访问权限 — 为群组成员配置 Wickr 开放访问设置。
  - 启用 Wickr 开放访问 — 启用 Wickr 开放访问将掩盖流量，以保护受限和受监控网络上的数据。根据地理位置，Wickr开放访问将连接到各种全球代理服务器，这些代理服务器为流量混淆提供了最佳路径和协议。
  - 强制 Wickr 开放访问 — 在所有设备上自动启用和强制执行 Wickr 开放访问。
- 联邦 — 控制您的用户与其他 Wickr 网络通信的能力。
  - 本地联合-能够与同一区域内其他网络中的AWS用户联合。例如，如果AWS加拿大（中部）地区有两个网络启用了本地联合，则它们将能够相互通信。
  - 全球联合 — 能够与 Wickr Enterprise AWS 用户或不同网络中属于其他区域的用户进行联合。例如，AWS加拿大（中部）地区的 Wickr 网络上的用户和AWS欧洲（伦敦）区域的网络中的一个用户在两个网络上都开启了全球联合后，将能够相互通信。
  - 受限联合 — 允许列出用户可以联合的特定 AWS Wickr 或 Wickr Enterprise 网络。配置后，用户只能在允许列出的网络中与外部用户通信。两个网络必须允许相互列出才能使用受限联合。

    有关访客联合的信息，请参阅在 AWS Wickr 网络中启用或禁用访客用户。
- ATAK 插件配置 — 有关启用 ATAK 的更多信息，请参阅什么是 ATAK？ 。

6. 选择 “保存” 以保存您对安全组详细信息所做的编辑。

在 AWS Wickr 中删除安全组

您可以删除您的 Wickr 安全组。

完成以下过程以删除安全组。

1. 在 f AWS 管理控制台 or Wickr 上https://console.aws.amazon.com/wickr/打开。
2. 在 “网络” 页面上，选择要导航到该网络的网络名称。
3. 在导航窗格中，选择安全组。
4. 在安全组页面上，找到要删除的安全组。

5. 在要删除的安全组的右侧，选择垂直省略号图标（三个点），然后选择删除。
6. 在弹出窗口中键入确认，然后选择删除。

   删除已分配用户的安全组时，这些用户会自动添加到默认安全组。要修改分配给用户的安全组，请参阅在 AWS Wickr 网络中编辑用户。

AWS Wickr 的单点登录配置

在 f AWS 管理控制台 or Wickr 中，您可以将 Wickr 配置为使用单点登录系统进行身份验证。SSO 与适当的多重身份验证（MFA）系统配对时可提供一层额外的安全。Wickr 仅支持使用 OpenID Connect (OIDC) 的 SSO 提供者。不支持使用安全断言标记语言 (SAML) 的提供商。

主题

在 AWS Wickr 中查看 SSO 详情

您可以查看 Wickr 网络和网络端点的单点登录配置的详细信息。

完成以下过程以查看 Wickr 网络的当前单点登录配置（若有）。

1. 在 f AWS 管理控制台 or Wickr 上https://console.aws.amazon.com/wickr/打开。
2. 在“网络”页面上，选择要导航到该网络的网络名称。
3. 在导航窗格中，选择用户管理。

   在“用户管理”页面上，“单个” Sign-on 部分显示您的 Wickr 网络端点和当前的 SSO 配置。

在 AWS Wickr 中配置 SSO

为确保安全访问您的 Wickr 网络，您可以设置当前的单点登录配置。详细的指南可帮助您完成此过程。

Important

- 配置 SSO 时，需要为 Wickr 网络指定一个公司 ID。请务必记录此公司 ID。在发送邀请电子邮件时，您必须将其提供给最终用户。最终用户在注册您的 Wickr 网络时必须指定该公司 ID。
- 2025 年 9 月，AWS Wickr 推出了经过改进、更安全的单点登录连接系统。要利用这些安全增强功能，使用 SSO 的组织必须在 2026 年 3 月 9 日之前迁移到新的重定向 URI。有关迁移说明，请参阅以下AWS re:Post文章：迁移到 AWS Wickr 的新 SSO 重定向 URI。

有关配置 SSO 的更多信息，请参阅以下指南：

- 使用微软 Entr Sign-on a (Azure AD) 设置 AWS Wickr Single (SSO)
- 使用 Okta 设置 AWS Wickr Single Sign-on (SSO)
- 使用 Amazon Cognito 设置 AWS Wickr Single Sign-on (SSO)

使用微软 Entra (Azure AD) 单点登录配置 AWS Wickr

AWS Wickr 可以配置为使用微软 Entra (Azure AD) 作为身份提供商。为此，请在 Microsoft Entra 和 AWS Wickr 管理控制台中完成以下程序。

Warning

在网络上启用 SSO 后，它将让活跃用户退出 Wickr，并强制他们使用 SSO 提供商重新进行身份验证。

第 1 步：在 Microsoft Entra 中将 AWS Wickr 注册为应用程序

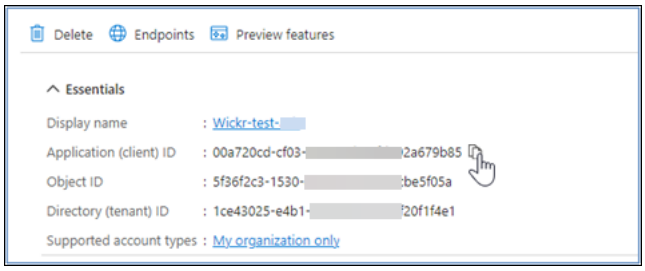
完成以下步骤，在 Microsoft Entra 中将 AWS Wickr 注册为应用程序。

Note

有关详细的屏幕截图和疑难解答，请参阅 Microsoft Entra 文档。有关更多信息，请参阅在 Microsoft 身份平台上注册应用程序

1. 在导航窗格中，选择 “应用程序”，然后选择 “应用程序注册”。

2. 在 “应用程序注册” 页面上，选择 “注册应用程序”，然后输入应用程序名称。
3. 仅选择此组织目录中的帐户（仅限默认目录-单租户）。
4. 在 “重定向 URI” 下，选择 Web，然后在 W AWS ickr 管理员控制台中输入 SSO 配置设置中可用的重定向 URI
5. 选择注册。
6. 注册后， copy/save 将生成应用程序（客户端）ID。

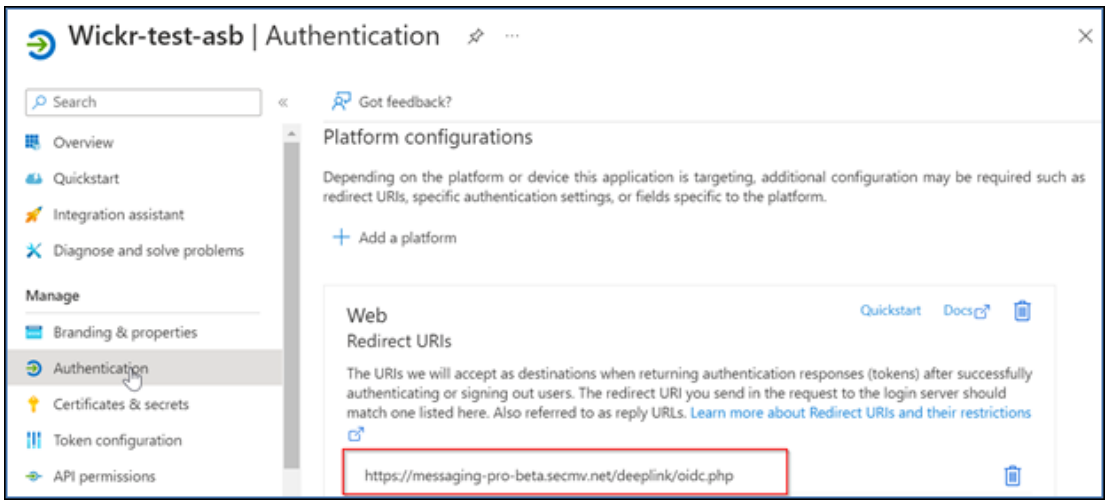


7. 选择 “端点” 选项卡，记下以下内容：
    1. Oauth 2.0 授权端点 (v2)：例如：`https://login.microsoftonline.com/1ce43025-e4b1-462d-a39f-337f20f1f4e1/oauth2/v2.0/authorize`
    2. 编辑此值以删除 “oauth2/” 和 “授权”。例如，固定网址将如下所示：`https://login.microsoftonline.com/1ce43025-e4b1-462d-a39f-337f20f1f4e1/v2.0/`
    3. 这将被称为 SSO 发行者。

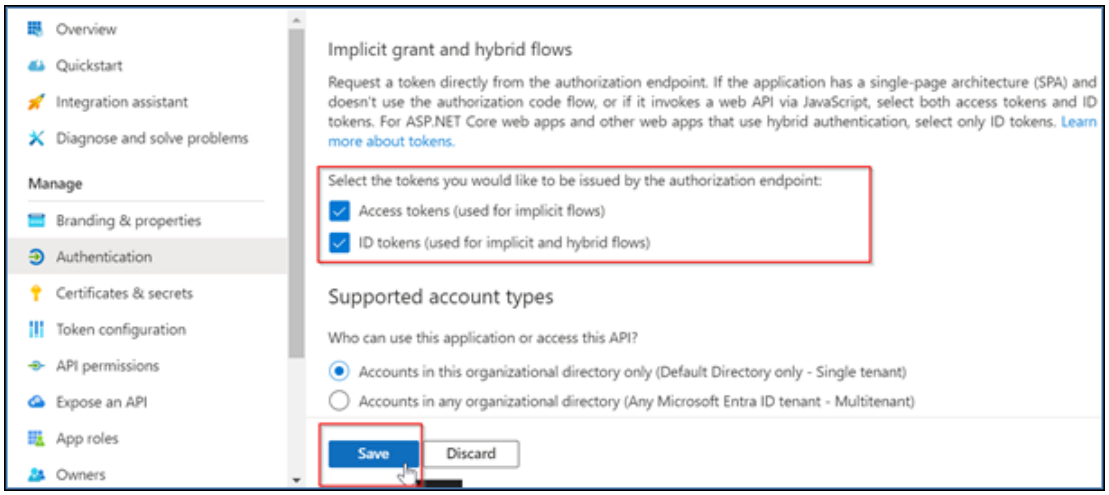
步骤 2：设置身份验证

完成以下步骤以在 Microsoft Entra 中设置身份验证。

1. 在导航窗格中，选择 “身份验证”。
2. 在身份验证页面上，确保 Web 重定向 URI 与之前输入的相同（在将 AWS Wickr 注册为应用程序中）。



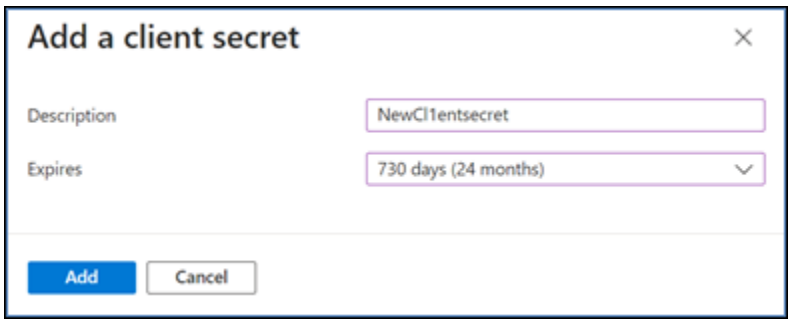
3. 选择用于隐式流程的访问令牌和用于隐式和混合流程的 ID 令牌。
4. 选择保存。



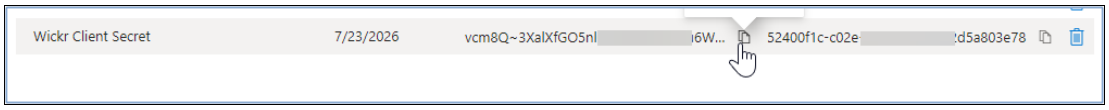
第 3 步：设置证书和密钥

完成以下步骤在 Microsoft Entra 中设置证书和密钥。

1. 在导航窗格中，选择 “证书和机密”。
2. 在 “证书和密钥” 页面上，选择 “客户机密” 选项卡。
3. 在 “客户机密钥” 选项卡下，选择 “新建客户机密”。
4. 输入描述并选择密钥的到期时间。
5. 选择添加。



6. 创建证书后，复制客户机密值。

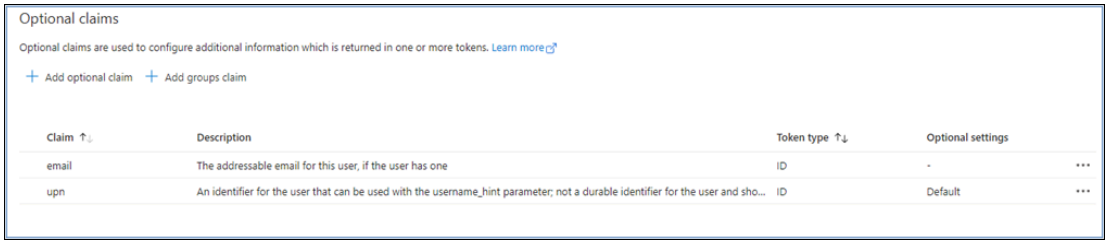


> **Note**
>
> 您的客户端应用程序代码将需要客户端密钥值（不是密钥 ID）。离开此页面后，您可能无法查看或复制密钥值。如果您现在不复制，则必须返回创建新的客户机密钥。

步骤 4：设置令牌配置

完成以下步骤在 Microsoft Entra 中设置令牌配置。

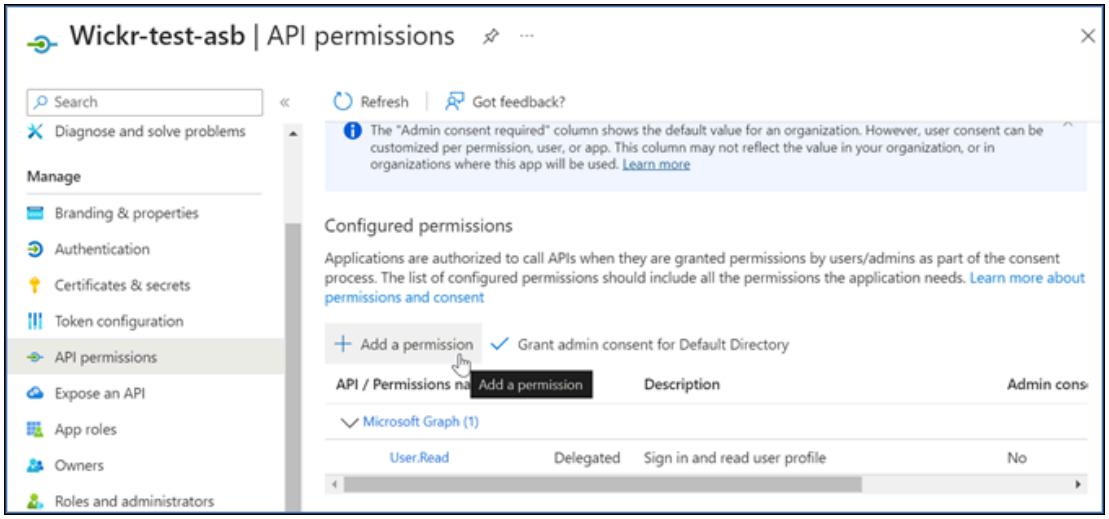
1. 在导航窗格中，选择令牌配置。
2. 在令牌配置页面上，选择添加可选声明。
3. 在 “可选声明” 下，选择令牌类型作为 ID。
4. 选择 ID 后，在 “声明” 下，选择 “电子邮件” 和 “upn”。
5. 选择添加。



第 5 步：设置 API 权限

完成以下步骤，在 Microsoft Entra 中设置 API 权限。

1. 在导航窗格中，选择 API permissions（API 权限）。
2. 在 API 权限页面上，选择添加权限。

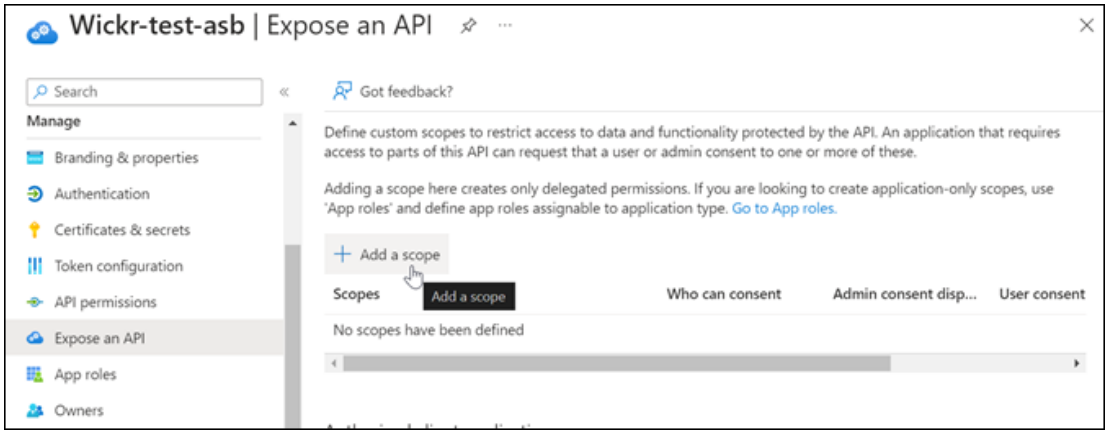


3. 选择 Microsoft Graph，然后选择委派权限。
4. 选中电子邮件、O ffline_access、o pen id、个人资料的复选框。
5. 选择添加权限。

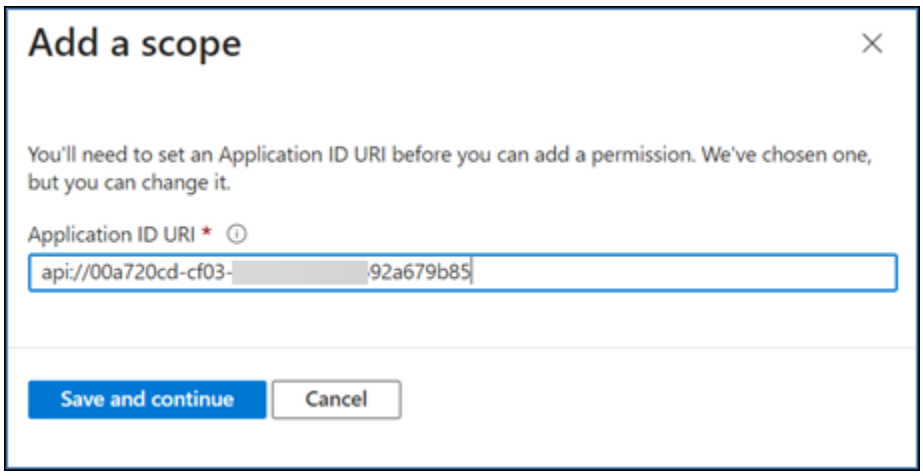
第 6 步：公开 API

完成以下步骤，在 Microsoft Entra 中为 4 个作用域中的每个作用域公开一个 API。

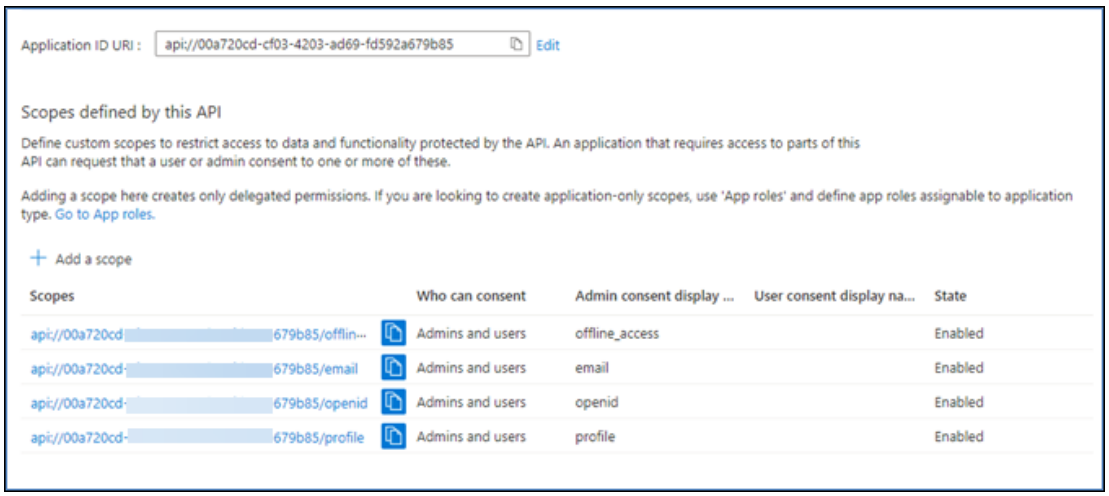
1. 在导航窗格中，选择 “公开 API”。
2. 在 “公开 API” 页面上，选择 “添加范围”。



应用程序 ID URI 应自动填充，URI 后面的 ID 应与应用程序 ID 相匹配（在将 AWS Wickr 注册为应用程序中创建）。



3. 选择 保存并继续。
4. 选择 “管理员和用户” 标签，然后将范围名称输入为 o ff line_access。
5. 选择 “状态”，然后选择 “启用”。
6. 选择 “添加范围”。
7. 重复本节的步骤 1-6，添加以下范围：电子邮件、openid 和个人资料。



8. 在 “授权的客户端应用程序” 下，选择 “添加客户端应用程序”。
9. 选择在上一步中创建的所有四个作用域。
10. 输入或验证应用程序（客户端）ID。
11. 选择添加应用程序。

第 7 步：AWS Wickr 单点登录配置

在 AWS Wickr 控制台中完成以下配置过程。

1. 在 f AWS 管理控制台 or Wickr 上https://console.aws.amazon.com/wickr/打开。
2. 在 “网络” 页面上，选择要导航到该网络的网络名称。
3. 在导航窗格中，选择用户管理，然后选择配置 SSO。
4. 输入以下详细信息：

   - 颁发者-这是之前修改过的端点（例如`https://login.microsoftonline.com/1ce43025-e4b1-462d-a39f-337f20f1f4e1/v2.0/`）。
   - 客户端 ID-这是 “概览” 窗格中的应用程序（客户端）ID。
   - 客户机密钥（可选）-这是证书和密钥窗格中的客户机密钥。
   - 范围 — 这些是 “公开 API” 窗格上显示的范围名称。输入电子邮件、个人资料、离线访问权限和 openID。
   - 自定义用户名范围（可选）-输入 upn。
   - 公司 ID — 这可以是一个唯一的文本值，包括字母数字和下划线字符。这句话是您的用户在新设备上注册时要输入的内容。

   其他字段是可选的。
5. 选择下一步。
6. 在 “查看并保存” 页面中验证详细信息，然后选择 “保存更改”。

SSO 配置已完成。要进行验证，您现在可以在 Microsoft Entra 中将用户添加到应用程序中，然后使用 SSO 和公司 ID 使用该用户登录。

有关如何邀请和加入用户的更多信息，请参阅创建和邀请用户。

问题排查

以下是您可能遇到的常见问题以及解决这些问题的建议。

- SSO 连接测试失败或没有响应：
  - 确保按预期配置 SSO 颁发者。
  - 确保按预期设置配置的 SSO 中的必填字段。
- 连接测试成功，但用户无法登录：
  - 确保用户已添加到你在 Microsoft Entra 中注册的 Wickr 应用程序中。

- 确保用户使用正确的公司 ID，包括前缀。例如 UE1-DemoNetwork w_drqtva。
- 在 AWS Wickr SSO 配置中可能未正确设置客户端密钥。通过在 Microsoft Entra 中创建另一个客户端密钥来重置它，然后在 Wic kr SSO 配置中设置新的客户端密钥。

令牌刷新的宽限期

有时，身份提供商可能会遇到临时或长期中断的情况，这可能会导致用户因客户端会话刷新令牌失败而意外被注销。为防止出现此问题，您可以设置一个允许用户保持登录状态的宽限期，即使他们的客户端刷新令牌在此类中断期间失败。

以下是宽限期的可用选项：

- 无宽限期（默认）：刷新令牌失败后，用户将立即被系统退出。
- 30 分钟宽限期：刷新令牌失败后，用户最多可以保持登录状态 30 分钟。
- 60 分钟宽限期：刷新令牌失败后，用户最多可以保持登录状态 60 分钟。

AWS Wickr 的网络标签

您可以将标签应用到 Wickr 网络。然后，您可以使用这些标签来搜索和筛选您的 Wickr 网络或跟踪您的AWS费用。您可以在 Wickr 的 “网络” 主页上配置网络标记。AWS 管理控制台

标签是应用于资源的键值对，用于保存有关该资源的元数据。每个标签都是由一个键和一个值组成的。有关标签的更多信息，另请参阅什么是标签？以及标签添加用例。

主题

在 AWS Wickr 中管理网络标签

您可以管理 Wickr 网络的网络标签。

完成以下过程以管理 Wickr 网络的网络标签。

1. 在 f AWS 管理控制台 or Wickr 上https://console.aws.amazon.com/wickr/打开。
2. 在 “网络” 页面上，选择要导航到该网络的网络名称。
3. 在网络主页的标签部分，选择管理标签。
4. 在管理标签页面上，您可以完成以下选项之一：

   - 添加新标签 — 以键值对的形式输入新标签。选择添加新标签以添加多个键值对。标签区分大小写。有关更多信息，请参阅 在 AWS Wickr 中添加网络标签。
   - 编辑现有标签 — 为现有标签选择键或值文本，然后在文本框中输入修改内容。有关更多信息，请参阅 在 AWS Wickr 中编辑网络标签。
   - 移除现有标签 — 选择要删除的标签旁边列出的移除按钮。有关更多信息，请参阅 在 AWS Wickr 中移除网络标签。

在 AWS Wickr 中添加网络标签

你可以为你的 Wickr 网络添加网络标签。

完成以下过程以将标签添加到 Wickr 网络。有关管理标签的更多信息，请参阅 在 AWS Wickr 中管理网络标签。

1. 在网络主页的标签部分，选择添加新标签。
2. 在添加标签页面上，选择添加标签。
3. 在出现的空白键和值字段中，输入新的标签键和值。
4. 选择保存更改以保存新标签。

在 AWS Wickr 中编辑网络标签

您可以编辑您的 Wickr 网络的网络标签。

完成以下过程以编辑与 Wickr 网络关联的标签。有关管理标签的更多信息，请参阅 在 AWS Wickr 中管理网络标签。

1. 在管理标签页面上，编辑标签的值。

> **Note**
>
> 无法编辑标签的键。相反，可以移除键值对和使用新键添加新标签。

2. 选择保存更改以保存您的编辑。

在 AWS Wickr 中移除网络标签

您可以移除 Wickr 网络的网络标签。

完成以下过程以从 Wickr 网络中移除标签。有关管理标签的更多信息，请参阅 在 AWS Wickr 中管理网络标签。

1. 在管理标签页面上，选择要删除的标签旁的删除。
2. 选择保存更改以保存您的编辑。

阅读 AWS Wickr 的收据

AWS Wickr 的已读回执是发送给发件人的通知，用于显示他们的消息何时被读取。这些收据可以在一对一的对话中获得。已发送的邮件将出现一个复选标记，已读邮件将出现一个带有复选标记的实心圆圈。要在外部对话期间查看消息的已读回执，两个网络都应启用已读回执。

管理员可以在管理员面板中启用或禁用已读回执。此设置将应用于整个网络。

完成以下步骤以启用或禁用已读回执。

1. 在 f AWS 管理控制台 or Wickr 上https://console.aws.amazon.com/wickr/打开。
2. 在 “网络” 页面上，选择要导航到该网络的网络名称。
3. 在导航窗格中，选择网络策略。
4. 在 “网络策略” 页面的 “消息” 部分，选择 “编辑”。
5. 选中 “启用或禁用已读回执” 复选框。
6. 选择保存更改。

管理 AWS Wickr 的网络计划

在 f AWS 管理控制台 or Wickr 中，您可以根据业务需求管理您的网络计划。

要管理您的网络计划，请完成以下步骤。

1. 在 f AWS 管理控制台 or Wickr 上https://console.aws.amazon.com/wickr/打开。

2. 在“网络”页面上，选择要导航到该网络的网络名称。
3. 在网络主页的网络详细信息部分，选择编辑。
4. 在编辑网络详细信息页面上，选择所需的网络计划。您可以通过选择以下选项之一来修改当前的网络计划：

   - 标准- 适用于需要管理控制和灵活性的小型和大型企业团队。
   - 高级版或高级版免费试用 — 适用于需要最高功能限制、精细管理控制和数据保留的企业。

     管理员可以选择高级免费试用版，该试用版最多可供30个用户使用，有效期为三个月。对于 AWS WickrGov，高级免费试用选项最多允许 50 名用户，并且持续三个月。此优惠适用于新的和标准的计划。在高级版免费试用期内，管理员可以升级或降级到高级版或标准版套餐

     > **Note**
     >
     > 要停止在您的网络上使用和计费，请从您的网络中移除所有用户，包括所有已暂停的用户。

高级版免费试用限制

以下限制适用于高级免费试用：

- 如果某个计划之前注册过高级免费试用，则该计划将没有资格再试一次。
- 每个AWS账户只能注册一个网络参加高级免费试用。
- 在高级免费试用期间，访客用户功能不可用。
- 如果标准网络有超过 30 个用户（超过 50 个用户 AWS WickrGov），则无法升级到高级免费试用版。

AWS Wickr 的数据保留

AWS Wickr 数据留存可以保留网络中的所有对话。这包括网络内（内部）成员和您的网络与之进行联合身份验证的其他团队（外部）成员之间的直接消息对话以及群组或会议室中的对话。数据留存功能仅适用于选择保留数据的 AWS Wickr Premium 计划用户和企业客户。有关 Premium 计划的更多信息，请参阅 Wickr 定价。

当网络管理员为其网络配置和激活数据保留功能时，用户在其网络中共享的所有消息和文件都将存档到指定位置（E.g.、本地存储、Amazon S3 存储桶），在那里可以根据需要进行查看、处理和保留。

> **Note**
>
> AWS无法访问 Wickr 中的端到端加密消息内容。如果您的组织需要访问最终用户的消息内容，则必须部署数据保留机器人。

主题

在 AWS Wickr 中查看数据保留详情

完成以下过程以查看 Wickr 网络的数据留存详细信息。您还可以启用或禁用 Wickr 网络的数据留存功能。

1. 在 f AWS 管理控制台 or Wickr 上https://console.aws.amazon.com/wickr/打开。
2. 在“网络”页面上，选择要导航到该网络的网络名称。
3. 在导航窗格中，选择网络策略。
4. 网络策略页面显示设置数据保留的步骤以及激活或停用数据保留功能的选项。有关配置数据留存的更多信息，请参阅 为 AWS Wickr 配置数据保留。

> **Note**
>
> 数据留存功能激活后，网络中所有用户都会看到一条数据留存已开启的消息，告知他们启用了保留功能的网络。

为 AWS Wickr 配置数据保留

要为您的 AWS Wickr 网络配置数据留存，您必须将数据留存机器人 Docker 映像部署到主机上的容器，例如本地计算机或 Amazon Elastic Compute Cloud (Amazon EC2) 中的实例。部署机器人后，您

可以将其配置为将数据存储在 Amazon Simple Storage Service (Amazon S3) 存储桶中。您还可以将数据保留机器人配置为使用其他 AWS 服务，例如 AWS Secrets Manager (Secrets Manager)、亚马逊 ()、亚马逊简单通知服务 CloudWatch (Amazon SNSCloudWatch) Simple Notification Service 和 ()。AWS Key Management Service AWS KMS以下主题介绍如何为您的 Wickr 网络配置和运行数据留存机器人。

对于 Wickr 数据保留 (DR) 机器人的生产部署， AWS 建议使用存档在 Amazon S3 中的消息以及以下最低实例和存储大小进行部署到 Amazon EC2/Amazon EBS：

- 实例类型：m8i.large（ 8GiB 内存，2vCPU ）
- 存储空间：1 TB 亚马逊 EBS 容量
- 部署：每台 Amazon EC2 主机一个灾难恢复机器人实例

有关亚马逊 EBS 的更多信息，请参阅亚马逊 EBS 用户指南中的亚马逊 EBS 快照生命周期。

主题

为 AWS Wickr 配置数据保留的先决条件

这假设您已经有一个 Amazon EC2 实例正在运行，并且满足上面列出的最低存储要求，并且您的 VPC 能够访问 Wickr 消息终端节点：

`com.amazonaws.region.wickr-messaging`— 机器人接收来自 Wickr 消息服务的消息。

在开始之前，请完成以下步骤以在控制台中启用数据保留。

1. 在 f AWS 管理控制台 or Wickr 上https://console.aws.amazon.com/wickr/打开。

2. 在“网络”页面上，选择要导航到该网络的网络名称。
3. 在导航窗格中，选择网络策略。
4. 在“网络策略”页面的“数据保留”部分，选择“编辑”。
5. 在“编辑数据保留期”页面上，执行步骤 1 和 2。
6. 启动您的数据保留机器人。有关更多信息，请参阅启动您的 Wickr 网络的数据保留机器人。
7. 在“配置您的数据保留服务器”部分，复制用户名和初始密码。按照 AWS Wickr 中的数据保留机器人密码，使用用户名和初始密码配置数据保留机器人。
8. 选中“启用数据保留”复选框，然后选择“保存更改”。

> **Note**
>
> 灾难恢复机器人经过验证，可以持续处理每小时大约 11,000 封邮件（约 3 条 messages/second）。对于持续超过此吞吐量或预计在单次处理运行中将超过 150 万条消息的工作负载，应评估其他扩展策略。

对于灾难恢复，我们建议在 Amazon EBS 卷上使用快照生命周期和 Amazon S3 复制。 Cross-Region 要配置向 Amazon S3 发送消息的频率，您可以将环境变量 WICKRIO_COMP_FILESIZE 设置`WICKRIO_COMP_TIMEROTATE`为按大小或时间轮换。消息日志和文件附件将传送到同一个存储桶中的相同前缀中。有关更多信息，请参阅 在 AWS Wickr 中配置数据保留机器人的环境变量。

AWS Wickr 中数据保留机器人的密码

首次启动数据留存机器人时，您可以使用以下选项之一指定初始密码：

- 环境变量 `WICKRIO_BOT_PASSWORD` 本指南后面的 在 AWS Wickr 中配置数据保留机器人的环境变量 部分概述了数据留存机器人环境变量。
- 由 `AWS_SECRET_NAME` 环境变量标识的 Secrets Manager 中的密码值。本指南后面的 AWS Wickr 的 Secrets Manager 值 部分概述了数据留存机器人的 Secrets Manager 值。
- 当数据留存机器人提示时，请输入密码。您需要使用 `-ti` 选项以交互式 TTY 访问权限运行数据留存机器人。

首次配置数据留存机器人时，将生成一个新密码。如果您需要重新安装数据留存机器人，则使用生成的密码。初始安装数据留存机器人后，初始密码无效。您可以轮换生成的密码。要轮换生成的密码，请使用以下各节中提供的指导。

密码轮换

数据保留机器人（最低版本 6.66.01.00）可以通过设置 WICKRIO_ROTATE_PASSWORD 环境变量在启动时以编程方式轮换其 Wickr 账户密码。

用法

使用 docker 运行启动机器人时，设置环境变量 WICKRIO_ROTATE_PASSWORD：

```
-e WICKRIO_ROTATE_PASSWORD="new_password"
```

启动时，机器人使用其当前密码（来自 WICKRIO_BOT_PASSWORD 或 Secrets AWS Manager）成功登录后，它会执行以下操作：

1. 从流程环境中读取 WICKRIO_ROTATE_PASSWORD。
2. 验证新密码（至少 12 个字符，必须与当前密码不同）。
3. 调用 AWS Wickr 服务来轮换密码。

成功轮换后，在下次重启之前，将 WICKRIO_BOT_PASSWORD（或 Secr AWS ets Manager 中的密码）更新为新密码。

将显示新生成的密码，如以下示例中所示。

> **Important**
>
> 将密码保存在安全的位置。如果您丢失了密码，您将无法重新安装数据留存机器人。请勿共享此密码。它提供了开始为 Wickr 网络保留数据的功能。

```
************************************************************************
**** GENERATED PASSWORD
**** DO NOT LOSE THIS PASSWORD, YOU WILL NEED TO ENTER IT EVERY TIME
**** TO START THE BOT
 "HuEXAMPLERAW4lGgEXAMPLEn"
 ************************************************************************
```

密码要求

- 新密码必须至少为 12 个字符。
- 新密码必须与当前密码不同。

- 机器人必须能够先使用当前密码登录。

AWS Wickr 网络的存储选项

启用数据留存功能并为 Wickr 网络配置数据留存机器人后，它将捕获在您的网络中发送的所有消息和文件。消息保存在文件中，这些文件受限于特定大小或时间限制，可以使用环境变量进行配置。有关更多信息，请参阅 在 AWS Wickr 中配置数据保留机器人的环境变量。

您可以配置下列选项之一来存储这些数据：

- 将所有捕获的消息和文件存储在本地。这是默认选项。您有责任将本地文件移动到另一个系统进行长期存储，并确保主机磁盘不会耗尽内存或空间。
- 将所有捕获的消息和文件存储在 Amazon S3 存储桶中。数据留存机器人会将所有解密的消息和文件保存到您指定的 Amazon S3 存储桶中。成功保存到存储桶后，捕获的消息和文件将从主机中移除。
- 将所有已捕获消息和加密文件存储在 Amazon S3 存储桶中。数据留存机器人将使用您提供的密钥对所有捕获的消息和文件进行重新加密，并将其保存到您指定的 Amazon S3 存储桶中。成功重新加密并保存到存储桶后，捕获的消息和文件将从主机上移除。您将需要软件来解密消息和文件。

  有关用您的数据留存创建要使用的 Amazon S3 存储桶的更多信息，请参阅 Amazon Simple 用户指南中的创建存储桶。

在 AWS Wickr 中配置数据保留机器人的环境变量

您可以使用以下环境变量来配置数据留存机器人。在运行数据留存机器人 Docker 映像时，您可以使用 `-e` 选项设置这些环境变量。有关更多信息，请参阅 为你的 Wickr 网络启动数据保留机器人。

> **Note**
>
> 除非另有说明，否则这些环境变量是可选的。

使用以下环境变量来指定数据留存机器人凭证：

- `WICKRIO_BOT_NAME`：数据留存机器人的名称。运行数据留存机器人 Docker 映像时需要此变量。
- `WICKRIO_BOT_PASSWORD`：数据留存机器人的初始密码。有关更多信息，请参阅 为 AWS Wickr 配置数据保留的先决条件。如果您不打算使用密码提示启动数据留存机器人，或者您不打算使用 Secrets Manager 来存储数据留存机器人凭据，则需要使用此变量。

使用以下环境变量来配置默认数据留存流式传输功能：

- `WICKRIO_COMP_MESGDEST`：将要流式传输消息的目录的路径名。默认值为 `/tmp/<botname>/compliance/messages`。
- `WICKRIO_COMP_FILEDEST`：将流式传输文件的目录的路径名。默认值为 `/tmp/<botname>/compliance/attachments`。
- `WICKRIO_COMP_BASENAME`：收到的消息文件的基本名称。默认值为 `receivedMessages`。
- `WICKRIO_COMP_FILESIZE`：以 kibibyte (KiB) 为单位的已接收消息文件的最大文件大小。当大小达到最大时，将启动一个新文件。默认值为 `1000000000`，如 1024 GiB。
- `WICKRIO_COMP_TIMEROTATE`：数据留存机器人将收到的消息放入收到的消息文件的时间长度，以分钟为单位。默认值为`0`，因为不旋转。使用 Amazon S3 进行数据保留时需要使用此变量。如果不设置此值，则永远不会轮换消息文件，因此也永远不会传送到 Amazon S3。建议的起始值为`10`分钟。您可以根据邮件量和传送要求调整此值。

使用以下环境变量来定义 AWS 区域 要使用的默认值。

- `AWS_DEFAULT_REGION`— Secrets Manager 等 AWS 服务的默认值 AWS 区域（不用于亚马逊 S3 或 AWS KMS）。如果未定义此环境变量，则默认使用 `us-east-1` 区域。

使用以下环境变量指定在选择使用 Secrets Manager 存储数据保留机器人凭据和 AWS 服务信息时要使用的 Secrets Manager 密钥。有关可以在 Secrets Manager 中存储的值的更多信息，请参阅 AWS Wickr 的 Secrets Manager 值。

- `AWS_SECRET_NAME`— Secrets Manager 密钥的名称，其中包含数据保留机器人所需的凭据和 AWS 服务信息。
- `AWS_SECRET_REGION`— AWS 秘密所在的那个。 AWS 区域 如果您使用的是 AWS 密钥但未定义此值，则将使用该`AWS_DEFAULT_REGION`值。

> **Note**
>
> 您可以将以下所有环境变量作为值存储在 Secrets Manager 中。如果您选择使用 Secrets Manager，并将这些值存储在那里，那么在运行数据留存机器人 Docker 映像时，您无需将它们指定为环境变量。您只需要指定本指南前面描述的 `AWS_SECRET_NAME` 环境变量即可。有关更多信息，请参阅 AWS Wickr 的 Secrets Manager 值。

当您选择将消息和文件存储到存储桶时，使用以下环境变量指定 Amazon S3 存储桶。

- `WICKRIO_S3_BUCKET_NAME`：存储消息和文件的 Amazon S3 存储桶的名称。
- `WICKRIO_S3_REGION`— 用于存储消息和文件的 Amazon S3 存储桶 AWS 区域。
- `WICKRIO_S3_FOLDER_NAME`：存储邮件和文件的 Amazon S3 存储桶中的可选文件夹名称。此文件夹名称前将带有保存到 Amazon S3 存储桶中的邮件和文件的密钥。

在将文件保存到 Amazon S3 存储桶时，当您选择使用客户端加密来重新加密文件时，请使用以下环境变量来指定 AWS KMS 详细信息。

- `WICKRIO_KMS_MSTRKEY_ARN`— AWS KMS 主密钥的亚马逊资源名称 (ARN)，用于在消息文件和数据保留机器人上的文件保存到 Amazon S3 存储桶之前对其进行重新加密。
- `WICKRIO_KMS_REGION`— AWS KMS 主密钥所在的 AWS 区域。

当您选择向 Amazon SNS 主题发送数据留存事件时，使用以下环境变量指定 Amazon SNS 的详细信息。发送的事件包括启动、关闭以及错误情况。

- `WICKRIO_SNS_TOPIC_ARN`：要使用其发送数据留存事件的 Amazon SNS 主题的 ARN。

使用以下环境变量向发送数据保留指标 CloudWatch。如果指定，则将每 60 秒生成一次指标。

- `WICKRIO_METRICS_TYPE`— 将此环境变量的值设置为，`cloudwatch`以向其发送指标 CloudWatch。

AWS Wickr 的 Secrets Manager 值

你可以使用 Secrets Manager 来存储数据保留机器人凭据和 AWS 服务信息。有关创建 Secrets Manager 密钥的更多信息，请参阅 S AWS Secrets Manager ecrets Manager 用户指南中的创建密钥。

Secrets Manager 密钥可以具有以下值：

- `password`：数据留存机器人密码。
- `s3_bucket_name`：存储消息和文件的 Amazon S3 存储桶的名称。如果未设置，则将使用默认文件流式传输。
- `s3_region`— 用于存储消息和文件的 Amazon S3 存储桶 AWS 区域。

- `s3_folder_name`：存储邮件和文件的 Amazon S3 存储桶中的可选文件夹名称。此文件夹名称前将带有保存到 Amazon S3 存储桶中的邮件和文件的密钥。
- `kms_master_key_arn`— AWS KMS 主密钥的 ARN，用于在消息文件和数据保留机器人上的文件保存到 Amazon S3 存储桶之前对其进行重新加密。
- `kms_region`— AWS KMS 主密钥所在的 AWS 区域。
- `sns_topic_arn`：要使用其发送数据留存事件的 Amazon SNS 主题的 ARN。

使用数据保留的 IAM 政策 AWS 务

如果您计划在 Wickr 数据保留机器人中使用其他 AWS 服务，则必须确保主机具有相应的 AWS Identity and Access Management (IAM) 角色和策略来访问这些服务。你可以将数据保留机器人配置为使用 Secrets Manager、Amazon S3、 CloudWatch、Amazon SNS 和。 AWS KMS以下 IAM policy授予这些服务的特定操作所需的访问权限。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": [
                "s3:PutObject",
                "secretsmanager:GetSecretValue",
                "sns:Publish",
                "cloudwatch:PutMetricData",
                "kms:GenerateDataKey"
            ],
            "Resource": "*"
        }
    ]
}
```

您可以通过识别您希望允许主机上的容器访问的每项服务的特定对象来创建更严格的 IAM policy。删除您不打算使用的 AWS 服务的操作。例如，如果您打算仅使用 Amazon S3 存储桶，则使用以下策略，该策略会删除 `secretsmanager:GetSecretValue`、`sns:Publish`、`kms:GenerateDataKey` 和 `cloudwatch:PutMetricData` 操作。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Sid": "VisualEditor0",
            "Effect": "Allow",
            "Action": "s3:PutObject",
            "Resource": "*"
        }
    ]
}
```

如果您使用 Amazon Elastic Compute Cloud (Amazon EC2) 实例来托管您的数据留存机器人，请使用亚马逊 Amazon EC2 常见案例创建 IAM 角色并使用上面的策略定义分配策略。

为你的 Wickr 网络启动数据保留机器人

在运行数据留存机器人之前，应确定要如何对其进行配置。如果您计划在主机上运行该机器人：

- 将无法访问 AWS 服务，那么您的选择将受到限制。在这种情况下，您将使用默认的消息流式传输选项。您应该决定是否要将捕获的消息文件的大小限制为特定的大小或时间间隔内。有关更多信息，请参阅 在 AWS Wickr 中配置数据保留机器人的环境变量。
- 将有权访问 AWS 服务，那么您应该创建一个 Secrets Manager 密钥来存储机器人凭据和 AWS 服务配置详细信息。配置 AWS 服务后，您可以继续启动数据留存机器人 Docker 映像。有关可以存储在 Secrets Manager 密钥中的详细信息的更多信息，请参阅 AWS Wickr 的 Secrets Manager 值

以下各节显示了运行数据留存机器人 Docker 映像的示例命令。在每个示例命令中，将以下示例值替换为自己的值：

- *compliance_1234567890_bot*，上面写上您的数据留存机器人的名字。
- *password*，使用您的数据留存机器人的密码。
- *wickr/data/retention/bot*，使用您的 Secrets Manager 密钥的名称，用于您的数据留存机器人。
- *bucket-name*，使用存储消息和文件的 Amazon S3 存储桶的名称。
- *folder-name*，使用存储消息和文件的 Amazon S3 存储桶中的文件夹名称。

- *us-east-1*使用您指定的资源 AWS 区域。例如，AWS KMS 主密钥所在的区域或 Amazon S3 存储桶的区域。
- *arn:aws:kms:us-east-1:111122223333:key/12345678-1234-abcde-a617-abababababab*使用 AWS KMS 主密钥的 Amazon 资源名称 (ARN)，用于重新加密消息文件和文件。

使用密码环境变量启动机器人（否）AWS 服务）

以下 Docker 命令启动数据留存机器人。密码是使用 WICKRIO_BOT_PASSWORD 环境变量指定的。机器人开始使用默认文件流式传输，并使用本指南 在 AWS Wickr 中配置数据保留机器人的环境变量 部分中定义的默认值。

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
-e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
-e WICKRIO_BOT_PASSWORD='password' \
public.ecr.aws/x3s2s6k3/wickrio/bot-compliance-cloud:latest
```

使用密码提示启动机器人（否）AWS 服务）

以下 Docker 命令启动数据留存机器人。当数据留存机器人提示时，系统会输入密码。它将使用本指南 在 AWS Wickr 中配置数据保留机器人的环境变量 部分中定义的默认值开始使用默认文件流式传输。

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
-e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
public.ecr.aws/x3s2s6k3/wickrio/bot-compliance-cloud:latest

docker attach compliance_1234567890_bot
.
.
.
Enter the password:************
Re-enter the password:************
```

使用 -ti 选项运行机器人以接收密码提示。您还应该在启动 Docker 映像后立即运行 docker attach *<container ID or container name>* 命令，以便获得密码提示。您应该在脚本中运行这两个命令。如果您附加到 Docker 映像但没有看到提示，请按输入，您将看到提示。

以轮换 10 分钟的消息文件启动机器人（否） AWS 服务）

以下 Docker 命令使用环境变量启动数据留存机器人。它还将其配置为将收到的消息文件轮换到 10 分钟。

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
-e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
-e WICKRIO_BOT_PASSWORD='password' \
-e WICKRIO_COMP_TIMEROTATE=10 \
public.ecr.aws/x3s2s6k3/wickrio/bot-compliance-cloud:latest
```

启动机器人并使用 Secrets Manager 指定初始密码

您可以使用 Secrets Manager 来识别数据留存机器人的密码。当您启动数据留存机器人时，您需要设置一个环境变量来指定存储这些信息的 Secrets Manager。

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
-e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
-e AWS_SECRET_NAME='wickrpro/alpha/new-3-bot' \
public.ecr.aws/x3s2s6k3/wickrio/bot-compliance-cloud:latest
```

`wickrpro/compliance/compliance_1234567890_bot` 密钥里面有以下秘密值，显示为纯文本。

```
{
    "password":"password"
}
```

启动机器人并使用 Secrets Manager 配置 Amazon S3

您可以使用 Secrets Manager 来托管凭据和 Amazon S3 存储桶信息。当您启动数据留存机器人时，您需要设置一个环境变量来指定存储这些信息的 Secrets Manager。

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
 -e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
 -e AWS_SECRET_NAME='wickrpro/alpha/compliance_1234567890_bot' \
 -e WICKRIO_COMP_TIMEROTATE=10 \
public.ecr.aws/x3s2s6k3/wickrio/bot-compliance-cloud:latest
```

wickrpro/compliance/compliance_1234567890_bot 密钥里面有以下秘密值，显示为纯文本。

```
{
    "password":"password",
    "s3_bucket_name":"bucket-name",
    "s3_region":"us-east-1",
    "s3_folder_name":"folder-name"
}
```

机器人收到的消息和文件将存放在名为 network1234567890 的文件夹中的 bot-compliance 存储桶中。

启动机器人并配置 Amazon S3 然后 AWS KMS 使用 Secrets Manager

您可以使用 Secrets Manager 来托管证书、Amazon S3 存储桶和 AWS KMS 主密钥信息。当您启动数据留存机器人时，您需要设置一个环境变量来指定存储这些信息的 Secrets Manager。

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
 -e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
 -e AWS_SECRET_NAME='wickrpro/alpha/compliance_1234567890_bot' \
 -e WICKRIO_COMP_TIMEROTATE=10 \
public.ecr.aws/x3s2s6k3/wickrio/bot-compliance-cloud:latest
```

wickrpro/compliance/compliance_1234567890_bot 密钥里面有以下秘密值，显示为纯文本。

```
{
    "password":"password",
    "s3_bucket_name":"bucket-name",
    "s3_region":"us-east-1",
    "s3_folder_name":"folder-name",
    "kms_master_key_arn":"arn:aws:kms:us-east-1:111122223333:key/12345678-1234-abcde-a617-abababababab",
    "kms_region":"us-east-1"
}
```

机器人收到的消息和文件将使用由 ARN 值标识的 KMS 密钥进行加密，然后放入名为 “network1234567890” 的文件夹中的 “bot-compliance”' 存储桶中。确保您已设置适当的 IAM policy。

启动机器人并使用环境变量配置 Amazon S3

如果您不想使用 Secrets Manager 来托管数据留存机器人凭据，则可以使用以下环境变量启动数据留存机器人 Docker 映像。您必须使用 WICKRIO_BOT_NAME 环境变量标识数据留存机器人的名称。

```
docker run -v /opt/compliance_1234567890_bot:/tmp/compliance_1234567890_bot \
-d --restart on-failure:5 --name="compliance_1234567890_bot" -ti \
-e WICKRIO_BOT_NAME='compliance_1234567890_bot' \
-e WICKRIO_BOT_PASSWORD='password' \
-e WICKRIO_COMP_TIMEROTATE=10 \
-e WICKRIO_S3_BUCKET_NAME='bot-compliance' \
-e WICKRIO_S3_FOLDER_NAME='network1234567890' \
-e WICKRIO_S3_REGION='us-east-1' \
public.ecr.aws/x3s2s6k3/wickrio/bot-compliance-cloud:latest
```

您可以使用环境值来识别数据留存机器人的证书、有关 Amazon S3 存储桶的信息以及默认文件流的配置信息。

停止你的 Wickr 网络的数据保留机器人

在数据留存机器人上运行的软件将捕获 SIGTERM 信号并正常关闭。使用 `docker stop <container ID or container name>` 命令向数据留存机器人 Docker 映像发出 SIGTERM 命令，如以下示例中所示。

```
docker stop compliance_1234567890_bot
```

获取 Wickr 网络的数据保留日志

在数据留存机器人 Docker 映像上运行的软件将输出到 /tmp/<botname>/logs 目录中的日志文件。它们将旋转到最多 5 个文件。您可以通过运行以下命令来获取日志。

```
docker logs <botname>
```

示例：

```
docker logs compliance_1234567890_bot
```

Wickr 网络的数据保留指标和事件

以下是 AWS Wickr 数据保留机器人的 5.116 版本目前支持的亚马逊 CloudWatch (CloudWatch) 指标和亚马逊简单通知服务 (Amazon SNS) Simple Notification Service 事件。

主题

CloudWatch 你的 Wickr 网络的指标

指标由机器人以 1 分钟为间隔生成，并传输到与运行数据保留机器人 Docker 镜像的账户关联的 CloudWatch 服务。

以下是数据留存机器人支持的现有指标。

指标	说明
Messages_Rx	消息收到
Messages_Rx_Failed	处理收到的消息失败。
Messages_Saved	消息保存到收到的消息文件中。
Messages_Saved_Failed	将消息保存到收到的消息文件中失败。
Files_Saved	文件已收到。
Files_Saved_Bytes	已接收文件的字节数。
Files_Saved_Failed	无法保存文件。
登录名	登录（通常每个间隔为 1 次）。
Login_Failures	登录失败（通常每个间隔为 1 次）。
S3_ Post_Errors	将消息文件和文件发布到 Amazon S3 存储桶时出错。
Watchdog_Failures	看门狗故障。

指标	说明
Watchdog_Warnings	看门狗警告。

生成指标供其使用 CloudWatch。用于机器人的命名空间是 `WickrIO`。每个指标都有一个维度阵列。以下是与上述指标一起发布的维度的列表。

维度	值
Id	机器人的用户名。
设备	特定机器人设备或实例的描述。在运行多个机器人设备或实例时有用。
产品	机器人的产品。可以是附加了 `Alpha`、`Beta` 或 `Production` 的 `WickrPro_` 或 `WickrEnterprise_`。
BotType	机器人类型。合规机器人被标记为合规。
Network	关联网络的 ID。

为你的 Wickr 网络举办的亚马逊 SNS 活动

以下事件发布到由使用 `WICKRIO_SNS_TOPIC_ARN` 环境变量或 `sns_topic_arn` Secrets Manager 密钥值识别的 Amazon 资源名称（ARN）值定义的 Amazon SNS 主题。有关更多信息，请参阅[在 AWS Wickr 中配置数据保留机器人的环境变量](#)和[AWS Wickr 的 Secrets Manager 值](#)。

数据留存机器人生成的事件以 JSON 字符串的形式发送。从 5.116 版的数据留存机器人起，这些事件中包含以下值。

Name	值
complianceBot	数据留存机器人的用户名。
dataTime	事件发生时的日期和时间。

Name	值
设备	对特定机器人设备或实例的描述。在运行多个机器人实例时很有用。
dockerImage	与机器人关联的 Docker 映像。
dockerTag	Docker 映像的标签或版本。
message	事件消息。有关更多信息，请参阅关键事件和正常事件。
notificationType	这个值将是 `Bot Event`。
severity	事件的严重性。可以是 `normal` 或 `critical`。

必须订阅 Amazon SNS 主题才能接收事件。如果您使用电子邮件地址进行订阅，则系统会向您发送一封电子邮件，其中包含与以下示例类似的信息。

```
{
"complianceBot": "compliance_1234567890_bot",
 "dateTime": "2022-10-12T13:05:39",
 "device": "Desktop 1234567890ab",
 "dockerImage": "public.ecr.aws/x3s2s6k3/wickrio/bot-compliance-cloud",
 "dockerTag": "5.116.13.01",
 "message": "Logged in",
 "notificationType": "Bot Event",
 "severity": "normal"
}
```

关键事件

这些事件将导致机器人停止或重启。重启次数受到限制，以免导致其他问题。

登录失败

以下是机器人登录失败时可能生成的事件。每条消息都会指出登录失败的原因。

事件类型	事件消息
failedlogin	凭证不正确。检查密码。
failedlogin	未找到用户。
failedlogin	账户或设备已被暂停。
预置	用户退出命令。
预置	`config.wickr` 文件的密码不正确。
预置	无法读取 `config.wickr` 文件。
failedlogin	登录全部失败。
failedlogin	新用户但数据库已存在。

更多关键事件

事件类型	事件消息
账户暂停	WickrIOClientMain:: slotAdminUserSuspend: 代码 (%1)：原因：%2”
BotDevice 已暂停	设备已暂停！
WatchDog	SwitchBoard 系统停机时间超过 < *N* > 分钟
S3 失败	无法将文件 < *file-name* >> 放在 S3 存储桶上。错误：< *AWS-error* >
回退键	服务器提交的回退键：不是已识别客户端活跃回退键。请向桌面工程部门提交日志。

正常事件

以下是警告您发生正常操作的事件。在特定时间段内出现过多此类事件可能是担忧的原因。

设备已添加到账户

此事件在向数据留存机器人账户添加新设备时生成。在某些情况下，这可能是一个重要迹象，表明有人已创建数据留存机器人实例。以下是此事件的消息。

```
A device has been added to this account!
```

机器人已登录

此事件在机器人已成功登录时生成。以下是此事件的消息。

```
Logged in
```

正在关闭

此事件在机器人正在关闭时生成。如果用户没有明确发起此操作，则可能表示存在问题。以下是此事件的消息。

```
Shutting down
```

有更新可用

此事件在数据留存机器人启动时生成，它表明关联的 Docker 映像有更新的版本可用。此事件在机器人启动时生成，并且每天都会生成。此事件包括用于识别可用新版本的 `versions` 数组字段。以下为此事件具体形式的示例。

```
{
  "complianceBot": "compliance_1234567890_bot",
  "dateTime": "2022-10-12T13:05:55",
  "device": "Desktop 1234567890ab",
  "dockerImage": "public.ecr.aws/x3s2s6k3/wickrio/bot-compliance-cloud",
  "dockerTag": "5.116.13.01",
  "message": "There are updates available",
  "notificationType": "Bot Event",
  "severity": "normal",
  "versions": [
    "5.116.10.01"
  ]
}
```

安全注意事项

仔细评估在何处以及如何部署数据保留机器人。这些机器人集中收集和解密用户发送或接收的所有端到端加密消息，整合以前只能在个人设备上访问的内容。因此，该组件及其数据存储具有极高的安全价值。

如果您部署了数据保留机器人，请确保其符合最高安全标准并符合组织的安全政策。对于使用AWS服务的部署，请遵循我们的 AWS Wickr 安全最佳实践和AWS云安全责任共担模型中的其他指导。

什么是 ATAK？

安卓团队感知套件（ATAK）或军用安卓战术攻击套件（ATAK），是一款智能手机地理空间基础设施和态势感知应用程序，可实现跨地域的安全协作。虽然 ATAK 最初是为在战区使用而设计，但经过调整，可承担地方、州和联邦机构的任务。

主题

- 在 Wickr 网络控制面板中启用 ATAK
- 有关 ATAK 的其他信息
- 安装并配对适用于 ATAK 的 Wickr 插件
- 取消配对 ATAK 的 Wickr 插件
- 在 ATAK 中拨打和接听电话
- 在 ATAK 中发送文件
- 在 ATAK 中发送安全的语音留言 (Push-to-talk)
- 适用于 ATAK 的 Pinwheel（快速访问）
- ATAK 的导航

在 Wickr 网络控制面板中启用 ATAK

AWS Wickr 支持许多使用安卓战术攻击套件 (ATAK) 的机构。但是，到目前为止，使用 Wickr 的 ATAK 操作员必须离开应用程序才能进行这些操作。为了帮助减少中断和运营风险，Wickr 开发了一种插件，该插件通过安全的通信功能增强了 ATAK。使用适用于 ATAK 的 Wickr 插件，用户可以在 ATAK 应用程序中在 Wickr 上发送消息、协作和传输文件。这消除了中断以及 ATAK 聊天功能配置的复杂性。

在 Wickr 网络控制面板中启用 ATAK

完成以下过程以在 Wickr Network Dashboard 中启用 ATAK。

1. 在 f AWS 管理控制台 or Wickr 上https://console.aws.amazon.com/wickr/打开。
2. 在“网络”页面上，选择要导航到该网络的网络名称。
3. 在导航窗格中，选择安全组。
4. 在安全组页面上，选择要为其启用 ATAK 的所需安全组。
5. 在“集成”选项卡上的“ATAK 插件”部分，选择“编辑”。
6. 在“编辑 ATAK 插件”页面上，选中“启用 ATAK 插件”复选框。
7. 选择“添加新套餐”
8. 在软件包文本框中输入软件包名称。您可以选择以下值之一，具体取决于用户将安装和使用的 ATAK 版本：

   - `com.atakmap.app.civ`：如果您的 Wickr 最终用户要在其 Android 设备上安装和使用民用版 ATAK 应用程序，请在软件包文本框中输入此值。
   - `com.atakmap.app.mil`：如果您的 Wickr 最终用户要在其 Android 设备上安装和使用军用版 ATAK 应用程序，请在软件包文本框中输入此值。
9. 选择保存。

   现在，已为选定的 Wickr 网络和选定的安全组启用 ATAK。您应该要求安全组中为其启用了 ATAK 功能的 Android 用户安装适用于 ATAK 的 Wickr 插件。有关更多信息，请参阅安装并配对 Wickr ATAK 插件。

有关 ATAK 的其他信息

有关 ATAK 的 Wickr 插件的更多信息，请参阅以下内容：

- Wickr ATAK 插件概述
- 其他 Wickr ATAK 插件信息

安装并配对适用于 ATAK 的 Wickr 插件

安卓战术突击套件 (ATAK) 是美国军方、州和政府机构使用的安卓解决方案，这些机构需要态势感知能力来进行任务规划、执行和事件响应。ATAK 的插件架构能让开发者添加功能。它使用户能够使用 GPS 和地理空间地图数据进行导航，再加上对正在发生的事件的实时态势感知。在本文档中，我们将向您展示如何在安卓设备上安装适用于 ATAK 的 Wickr 插件并将其与 Wickr 客户端配对。这让您无需退出 ATAK 应用程序就能在 Wickr 上发送消息和进行协作。

安装 ATAK 的 Wickr 插件

完成以下过程以在安卓设备上安装 ATAK 用的 Wickr 插件。

1. 前往 Google Play 商店，安装 ATAK 用的 Wickr 插件。
2. 在安卓设备上打开 ATAK 应用程序。
3. 在 ATAK 应用程序中，选择屏幕右上角的菜单图标（ ），然后选择插件。
4. 选择导入。
5. 在选择导入类型弹出窗口中，选择本地 SD，然后导航到保存“适用于 ATAK 的 Wickr 插件”.apk 文件的位置。
6. 选择插件文件并按照提示进行安装。

   > **Note**
   >
   > 如果系统要求您发送插件文件进行扫描，请选择否。

7. ATAK 应用程序将询问您是否要加载该插件。选择确定。

ATAK 的 Wickr 插件现已安装。继续按照“将 ATAK 与 Wickr 配对”一节进行操作以完成此过程。

将 ATAK 与 Wickr 配对

成功安装用于 ATAK 的 Wickr 插件后，完成以下过程将 ATAK 应用程序与 Wickr 配对。

1. 在 ATAK 应用程序中，选择屏幕右上角的菜单图标（ ），然后选择 Wickr 插件。

2. 选择 Wickr 配对。

   将出现一条通知提示，要求您查看用于 ATAK 的 Wickr 插件的权限。如果没有出现通知提示，请打开 Wickr 客户端，转到设置，然后转到已连接的应用程序。可在屏幕的待处理部分下面看到这个插件。
3. 选择批准进行配对。
4. 选择打开 Wickr ATAK 插件按钮以返回到 ATAK 应用程序。

   现在，您已成功将 ATAK 插件与 Wickr 配对，而且无需退出 ATAK 应用程序便可使用该插件来发送消息和使用 Wickr 进行协作。

取消配对 ATAK 的 Wickr 插件

你可以取消与 ATAK 的 Wickr 插件的配对。

完成以下过程以取消 ATAK 插件与 Wickr 的配对。

1. 在本机应用程序中，选择设置，然后选择连接的应用程序。
2. 在连接的应用程序屏幕上，选择 Wickr ATAK 插件。
3. 在 Wickr ATAK 插件屏幕上，选择屏幕底部的删除。

   现在，你已经成功取消了 ATAK 的 Wickr 插件的配对。

在 ATAK 中拨打和接听电话

您可以使用适用于 ATAK 的 Wickr 插件拨打和接听电话。

完成以下过程以拨打和接听电话。

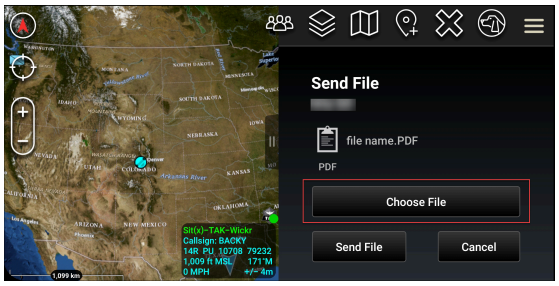
1. 打开聊天窗口。
2. 在地图视图中，选择要呼叫的用户图标。
3. 选择屏幕右上角的电话图标。
4. 连接后，您可以返回 ATAK 插件视图并接听电话。

在 ATAK 中发送文件

您可以使用适用于 ATAK 的 Wickr 插件发送文件。

完成以下过程以发送文件。

1. 打开聊天窗口。
2. 在地图视图中，搜索要向其发送文件的用户。
3. 找到要向其发送文件的用户时，请选择用户名称。
4. 在发送文件屏幕上，选择选择文件，然后导航至要发送的文件。



5. 在浏览器窗口中，选择所需的文件。
6. 在发送文件屏幕上，选择发送文件。

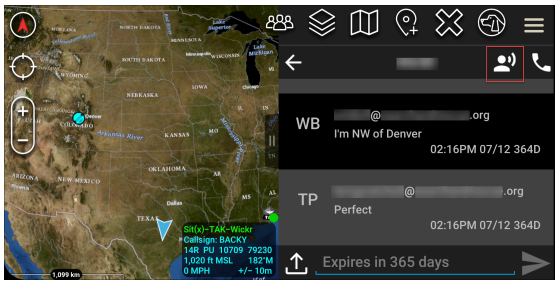
   此时将显示下载图标，表示您选择的文件正在下载。

在 ATAK 中发送安全的语音留言 (Push-to-talk)

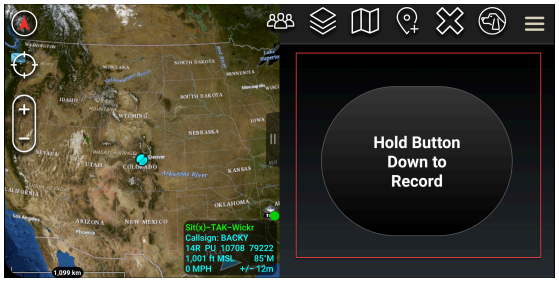
你可以在 ATAK 的 Wickr 插件中发送安全的语音消息 (Push-to-talk)。

完成以下过程以发送安全语音消息。

1. 打开聊天窗口。
2. 选择屏幕顶部的 Push-to-Talk图标，该图标由一个人说话的图标表示。



3. 选择并按住按住按钮录制按钮。



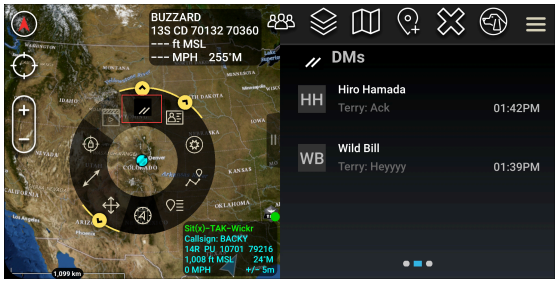
4. 录制消息。
5. 录制消息后，释放按钮即可发送。

适用于 ATAK 的 Pinwheel（快速访问）

风车或快速访问功能用于 one-one-one对话或私信。

完成以下过程以使用风车。

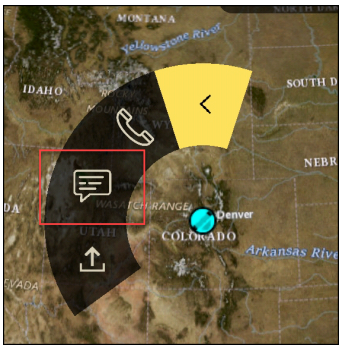
1. 同时打开 ATAK 地图和适用于 ATAK 的 Wickr 插件分屏视图。地图会在地图视图上显示您的队友或资产。
2. 选择用户图标以打开风车。
3. 选择 Wickr 图标，查看所选用户的可用选项。



4. 在风车上，请选择下列图标之一：

   - 电话：选择以呼叫。

- 消息：选择以聊天。



- 文件发送：选择以发送文件。

ATAK 的导航

插件 UI 包含三个插件视图，这些视图由屏幕右下角的蓝色和白色形状表示。向左和向右滑动可在不同的视图之间导航。

- 联系人视图：创建私信群组或房间对话。
- DMs 查看：创建 one-to-one对话。聊天功能与 Wickr 本机应用程序一样。此功能允许您保留在地图视图中，并通过插件与其他人通信。
- 房间视图：本机应用程序中的现有房间会移植过来。插件中的任何操作都会反映在 Wickr 本机应用程序中。

> **Note**
>
> 某些功能（例如删除房间）只能在本机应用程序中手动执行，以防用户意外修改和现场设备造成干扰。

允许列出 Wickr 网络的端口和域名

允许列出以下端口以确保 Wickr 正常运行：

端口

- TCP 端口 443（用于消息和附件）
- UDP 端口 16384-16584（用于呼叫）

按地区列出的允许列入许可名单的域名和地址

如果您需要将所有可能的主叫域和服务器 IP 地址列入许可名单，请参阅以下按区域列出的可能 CIDR 列表。请定期查看此列表，因为它可能会发生变化。

> **Note**
>
> 注册和验证电子邮件由no-reply@amazonaws.com和发送donotreply@wickr.email。

美国东部（弗吉尼亚州北部）

域名：	• gw-pro-prod.wickr.com • api.messaging。wickr.us-east-1.amazonaws.com • ingress.prod.calling.wickr.com
呼叫 CIDR 地址：	• 44.211.195。 0/27 • 44.213.83。 32/28
呼叫 IP 地址：	• 44.211.195.0 • 44.211.195.1 • 44.211.195.2 • 44.211.195.3 • 44.211.195.4 • 44.211.195.5 • 44.211.195.6

- 44.211.195.7
- 44.211.195.8
- 44.211.195.9
- 44.211.195.10
- 44.211.195.11
- 44.211.195.12
- 44.211.195.13
- 44.211.195.14
- 44.211.195.15
- 44.211.195.16
- 44.211.195.17
- 44.211.195.18
- 44.211.195.19
- 44.211.195.20
- 44.211.195.21
- 44.211.195.22
- 44.211.195.23
- 44.211.195.24
- 44.211.195.25
- 44.211.195.26
- 44.211.195.27
- 44.211.195.28
- 44.211.195.29
- 44.211.195.30
- 44.211.195.31
- 44.213.83.32
- 44.213.83.33
- 44.213.83.34
- 44.213.83.35
- 44.213.83.36

	• 44.213.83.37 • 44.213.83.38 • 44.213.83.39 • 44.213.83.40 • 44.213.83.41 • 44.213.83.42 • 44.213.83.43 • 44.213.83.44 • 44.213.83.45 • 44.213.83.46 • 44.213.83.47

亚太地区（马来西亚）

域名：	• gw-pro-prod.wickr.com • api.messaging。wickr.ap-southeast-5.amazonaws.com • ingress.prod.calling。wickr.ap-southeast-5.amazonaws.com
呼叫 CIDR 地址：	• 43.216.226。 160/28
呼叫 IP 地址：	• 43.216.226.160 • 43.216.226.161 • 43.216.226.162 • 43.216.226.163 • 43.216.226.164 • 43.216.226.165 • 43.216.226.166 • 43.216.226.167 • 43.216.226.168 • 43.216.226.169

	• 43.216.226.170 • 43.216.226.171 • 43.216.226.172 • 43.216.226.173 • 43.216.226.174 • 43.216.226.175

亚太地区（新加坡）

域:	• gw-pro-prod.wickr.com • api.messaging。wickr.ap-southeast-1.amazonaws.com • ingress.prod.calling。wickr.ap-southeast-1.amazonaws.com
呼叫 CIDR 地址：	• 47.129.23。 144/28
呼叫 IP 地址：	• 47.129.23.144 • 47.129.23.145 • 47.129.23.146 • 47.129.23.147 • 47.129.23.148 • 47.129.23.149 • 47.129.23.150 • 47.129.23.151 • 47.129.23.152 • 47.129.23.153 • 47.129.23.154 • 47.129.23.155 • 47.129.23.156 • 47.129.23.157 • 47.129.23.158

	• 47.129.23.159

亚太地区（悉尼）

域:	• gw-pro-prod.wickr.com • api.messaging。wickr.ap-southeast-2.amazonaws.com • ingress.prod.calling。wickr.ap-southeast-2.amazonaws.com
呼叫 CIDR 地址：	• 3.27.180。 208/28
呼叫 IP 地址：	• 3.27.180.208 • 3.27.180.209 • 3.27.180.210 • 3.27.180.211 • 3.27.180.212 • 3.27.180.213 • 3.27.180.214 • 3.27.180.215 • 3.27.180.216 • 3.27.180.217 • 3.27.180.218 • 3.27.180.219 • 3.27.180.220 • 3.27.180.221 • 3.27.180.222 • 3.27.180.223

亚太地区（东京）

域:	• gw-pro-prod.wickr.com

	• api.messaging。wickr.ap-northeast-1.amazonaws.com • ingress.prod.calling。wickr.ap-northeast-1.amazonaws.com
呼叫 CIDR 地址：	• 57.181.142。 240/28
呼叫 IP 地址：	• 57.181.142.240 • 57.181.142.241 • 57.181.142.242 • 57.181.142.243 • 57.181.142.244 • 57.181.142.245 • 57.181.142.246 • 57.181.142.247 • 57.181.142.248 • 57.181.142.249 • 57.181.142.250 • 57.181.142.251 • 57.181.142.252 • 57.181.142.253 • 57.181.142.254 • 57.181.142.255

加拿大（中部）

域:	• gw-pro-prod.wickr.com • api.messaging。wickr.ca-central-1.amazonaws.com • ingress.prod.calling。wickr.ca-central-1.amazonaws.com
呼叫 CIDR 地址：	• 15.156.152。 96/28

呼叫 IP 地址：	• 15.156.152.96 • 15.156.152.97 • 15.156.152.98 • 15.156.152.99 • 15.156.152.100 • 15.156.152.101 • 15.156.152.102 • 15.156.152.103 • 15.156.152.104 • 15.156.152.105 • 15.156.152.106 • 15.156.152.107 • 15.156.152.108 • 15.156.152.109 • 15.156.152.110 • 15.156.152.111

欧洲地区（法兰克福）

域:	• gw-pro-prod.wickr.com • api.messaging。wickr.eu-central-1.amazonaws.com • ingress.prod.calling。wickr.eu-central-1.amazonaws.com
呼叫 CIDR 地址：	• 3.78.252。 32/28
呼叫 IP 地址：	• 3.78.252.32 • 3.78.252.33 • 3.78.252.34 • 3.78.252.35 • 3.78.252.36

	• 3.78.252.37 • 3.78.252.38 • 3.78.252.39 • 3.78.252.40 • 3.78.252.41 • 3.78.252.42 • 3.78.252.43 • 3.78.252.44 • 3.78.252.45 • 3.78.252.46 • 3.78.252.47

消息 IP 地址：	• 3.163.236.183 • 3.163.238.183 • 3.163.251.183 • 3.163.232.183 • 3.163.241.183 • 3.163.245.183 • 3.163.248.183 • 3.163.234.183 • 3.163.237.183 • 3.163.243.183 • 3.163.247.183 • 3.163.240.183 • 3.163.242.183 • 3.163.244.183 • 3.163.246.183 • 3.163.249.183 • 3.163.252.183 • 3.163.235.183 • 3.163.250.183 • 3.163.239.183 • 3.163.233.183

欧洲地区（伦敦）

域:	• gw-pro-prod.wickr.com • api.messaging。wickr.eu-west-2.amazonaws.com • ingress.prod.calling。wickr.eu-west-2.amazonaws.com
呼叫 CIDR 地址：	• 13.43.91。 48/28

呼叫 IP 地址：	• 13.43.91.48 • 13.43.91.49 • 13.43.91.50 • 13.43.91.51 • 13.43.91.52 • 13.43.91.53 • 13.43.91.54 • 13.43.91.55 • 13.43.91.56 • 13.43.91.57 • 13.43.91.58 • 13.43.91.59 • 13.43.91.60 • 13.43.91.61 • 13.43.91.62 • 13.43.91.63

欧洲地区（斯德哥尔摩）

域:	• gw-pro-prod.wickr.com • api.messaging。wickr.eu-north-1.amazonaws.com • ingress.prod.calling。wickr.eu-north-1.amazonaws.com
呼叫 CIDR 地址：	• 13.60.1。 64/28
呼叫 IP 地址：	• 13.60.1.64 • 13.60.1.65 • 13.60.1.66 • 13.60.1.67 • 13.60.1.68

	• 13.60.1.69 • 13.60.1.70 • 13.60.1.71 • 13.60.1.72 • 13.60.1.73 • 13.60.1.74 • 13.60.1.75 • 13.60.1.76 • 13.60.1.77 • 13.60.1.78 • 13.60.1.79

欧洲（苏黎世）

域:	• gw-pro-prod.wickr.com • api.messaging。wickr.eu-central-2.amazonaws.com • ingress.prod.calling。wickr.eu-central-2.amazonaws.com
呼叫 CIDR 地址：	• 16.63.106。 224/28
呼叫 IP 地址：	• 16.63.106.224 • 16.63.106.225 • 16.63.106.226 • 16.63.106.227 • 16.63.106.228 • 16.63.106.229 • 16.63.106.230 • 16.63.106.231 • 16.63.106.232 • 16.63.106.233

	• 16.63.106.234 • 16.63.106.235 • 16.63.106.236 • 16.63.106.237 • 16.63.106.238 • 16.63.106.239

AWS GovCloud (US-West)

域:	• gw-pro-prod.wickr.com • api.messaging。wickr.us-gov-west-1.amazonaws.com • ingress-prod-calling。wickr.us-gov-west-1.amazonaws.com • s3.us-gov-west-1.amazonaws.com • s3-fips.us-gov-west-1.amazonaws.com • s3.amazonaws.com • 注册。wickr.us-gov-west-1.amazonaws.com • 管理员。wickr.us-gov-west-1.amazonaws.com • admin.messagy。wickr.us-gov-west-1.amazonaws.com • cognito-identity.us-gov-west-1.amazonaws.com • kinesis.us-gov-west-1.amazonaws.com • 消息传递。wickr.us-gov-west-1.amazonaws.com
呼叫 CIDR 地址：	• 3.30.186。 208/28 • 3.31.11。 216/29
呼叫 IP 地址：	• 3.30.186.208 • 3.30.186.209

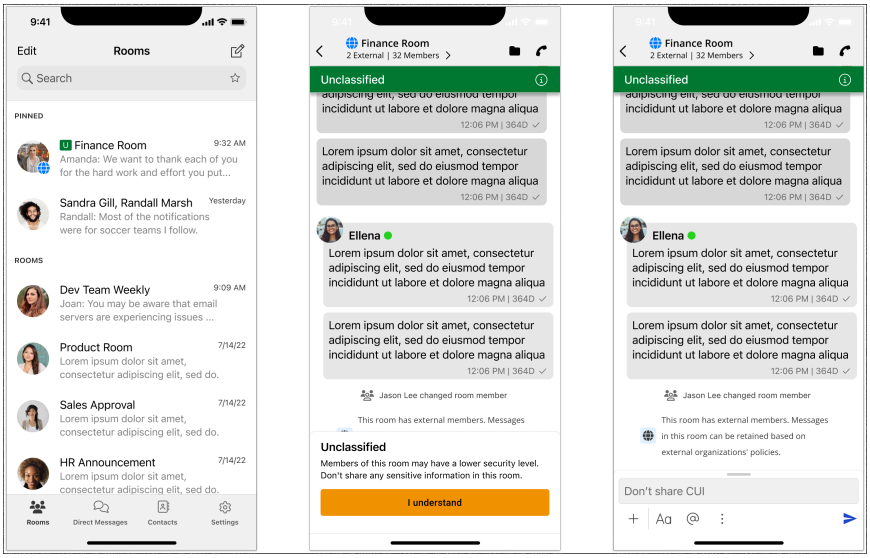
	• 3.30.186.210 • 3.30.186.211 • 3.30.186.212 • 3.30.186.213 • 3.30.186.214 • 3.30.186.215 • 3.30.186.216 • 3.30.186.217 • 3.30.186.218 • 3.30.186.219 • 3.30.186.220 • 3.30.186.221 • 3.30.186.222 • 3.30.186.223 • 3.31.11.216 • 3.31.11.217 • 3.31.11.218 • 3.31.11.219 • 3.31.11.220 • 3.31.11.221 • 3.31.11.222 • 3.31.11.223

GovCloud 跨界分类和联合

AWS Wickr 提供专为 GovCloud 用户量身定制的 WickrGov 客户端。 GovCloud 联合会允许 GovCloud 用户和商业用户之间进行通信。跨界分类功能允许用户更改对话的 GovCloud 用户界面。作为 GovCloud 用户，您必须遵守有关政府定义的分类的严格指导方针。当 GovCloud 用户与商业用户（企业用户、AWS Wickr、访客用户）进行对话时，他们将看到显示以下未保密的警告：

- 房间列表中有 U 标签
- 消息屏幕上显示未保密的确认

- 对话顶部有一面未保密的横幅



> **Note**
>
> 只有当用户与外部 GovCloud 用户进行对话或在会议室的一部分时，才会显示这些警告。如果外部用户退出对话，它们就会消失。 GovCloud 用户之间的对话中不会显示任何警告。

AWS Wickr 的文件预览

使用 Wickr Premium 级别（包括高级免费试用）的组织现在可以在安全组级别管理文件下载权限。

默认情况下，安全组中的文件下载处于启用状态。管理员可以通过管理员面板启用或禁用文件下载。此设置适用于整个 Wickr 网络。

要启用或禁用文件下载，请完成以下步骤。

1. 在 f AWS 管理控制台 or Wickr 上https://console.aws.amazon.com/wickr/打开。
2. 在“网络”页面上，选择要导航到该网络的网络名称。
3. 在导航窗格中，选择安全组。
4. 选择要编辑的安全组的名称。

   安全组详细信息页面在不同的选项卡中显示安全组的设置。
5. 在“消息”选项卡下的“媒体和链接”部分，选择“编辑”。

6. 在 “编辑媒体和链接” 页面上，选中或取消选中文件下载选项。
7. 选择保存更改。

为安全组启用文件下载功能后，用户可以下载私信和聊天室中共享的文件。如果禁用下载，他们只能预览这些文件并上传到 “文件” 选项卡，但不能下载它们。用户也被限制拍摄屏幕截图；尝试屏幕截图会导致黑屏。

> **Note**
>
> 禁用文件下载后，该安全组中的所有用户都必须使用 Wickr 6.54 及更高版本才能应用此文件设置。

> **Note**
>
> 在有来自不同网络（由于联合）和安全组的用户所在的房间中，每个用户预览或下载文件的能力取决于其特定的安全组设置。因此，有些用户可以在房间里下载文件，而其他用户只能预览文件。

AWS Wickr 的同意弹出窗口

您可以为网络配置同意弹出窗口，以便在用户登录 Wickr 时向他们显示条款、政策或组织要求。用户必须先确认弹出窗口，然后才能访问应用程序。当用户注销并重新登录或更新弹出窗口内容时，弹出窗口会再次显示。

要启用同意弹出窗口，请完成以下步骤。

1. 在 f AWS 管理控制台 or Wickr 上https://console.aws.amazon.com/wickr/打开。
2. 在 “网络” 页面上，选择要导航到该网络的网络名称。
3. 在导航窗格中，选择网络策略。
4. 在 “网络政策” 页面的 “同意” 弹出窗口部分，选择 “编辑”。
5. 在 “编辑用户同意” 弹出式页面的 “同意弹出窗口” 部分中，开启启用。
6. 填写以下字段：

    - 标题-输入显示在同意弹出窗口顶部的标题。使用标题提供向用户提供的信息或操作的摘要。

- 正文内容-输入同意弹出窗口中显示的主消息。使用正文内容传达条款、政策、组织要求或其他信息，用户在访问应用程序之前必须查看这些信息。
- 关闭按钮标签（可选）-输入按钮上显示的文本，用户选择该文本以确认和关闭同意弹出窗口。例如，您可以使用 “确认”、“接受” 或 “继续”。

7. 要预览您的同意弹出窗口，请选择右上角的 “预览”。预览后，选择 “关闭预览”。
8. 选择保存更改。

在 AWS Wickr 中管理用户

在 for Wickr 的 AWS 管理控制台 “用户管理” 部分，您可以查看当前的 Wickr 用户和机器人，并修改他们的详细信息。

主题

AWS Wickr 网络中的团队名录

您可以在 for Wickr 的 “用户管理” 部分中查看当前 Wickr 用户并修改他们的详细信息。 AWS 管理控制台

主题

查看 AWS Wickr 网络中的用户

您可以查看注册到您的 Wickr 网络的用户的详细信息。

完成以下过程以查看注册到 Wickr 网络的用户。

1. 在 f AWS 管理控制台 or Wickr 上https://console.aws.amazon.com/wickr/打开。
2. 在 “网络” 页面上，选择要导航到该网络的网络名称。
3. 在导航窗格中，选择用户管理。

   “团队目录” 选项卡显示注册到您的 Wickr 网络的用户，包括他们的姓名、电子邮件地址、分配的安全组和当前状态。对于当前用户，您可以查看他们的设备、编辑其详细信息、暂停、删除设备以及将其切换到其他 Wickr 网络。

邀请用户加入 AWS Wickr 网络

您可以邀请您的 Wickr 网络中的用户。

完成以下步骤邀请您的 Wickr 网络中的用户。

1. 在 f AWS 管理控制台 or Wickr 上https://console.aws.amazon.com/wickr/打开。
2. 在 “网络” 页面上，选择要导航到该网络的网络名称。
3. 在导航窗格中，选择用户管理。
4. 在 “团队目录” 选项卡中，选择 “邀请用户”。
5. 在邀请用户页面上，输入用户的电子邮件地址和安全组。电子邮件地址和安全组是唯一必填字段。请务必为用户选择合适的安全组。Wickr 将向用户指定的地址发送邀请电子邮件。
6. 选择 Invite user。

   向用户发送电子邮件。电子邮件提供了 Wickr 客户端应用程序的下载链接以及注册 Wickr 的链接。当用户使用电子邮件中的链接注册 Wickr 时，他们在 Wickr 团队目录中的状态将从待定变为活跃。

在 AWS Wickr 网络中编辑用户

您可以编辑 Wickr 网络中的用户。

完成以下过程以编辑用户。

1. 在 f AWS 管理控制台 or Wickr 上https://console.aws.amazon.com/wickr/打开。
2. 在 “网络” 页面上，选择要导航到该网络的网络名称。
3. 在导航窗格中，选择用户管理。
4. 在 “团队目录” 选项卡中，选择要编辑的用户的垂直省略号（三个点）图标。
5. 选择编辑。
6. 编辑用户信息，然后选择保存更改。

删除 AWS Wickr 网络中的用户

您可以删除 Wickr 网络中的用户。

完成以下过程以删除用户。

1. 在 f AWS 管理控制台 or Wickr 上https://console.aws.amazon.com/wickr/打开。
2. 在 “网络” 页面上，选择要导航到该网络的网络名称。
3. 在导航窗格中，选择用户管理。
4. 在 “团队目录” 选项卡中，选择要删除的用户的垂直省略号（三个点）图标。
5. 选择删除以删除用户。

   当您删除用户时，该用户将无法再在 Wickr 客户端中登录您的 Wickr 网络。
6. 在弹出窗口中，选择删除。

批量删除 AWS Wickr 网络中的用户

您可以在 for Wickr 的 “用户管理” 部分中批量删除 Wickr 网络用户。 AWS 管理控制台

> **Note**
>
> 批量删除用户的选项仅在未启用 SSO 时适用。

要使用 CSV 模板批量删除您的 Wickr 网络用户，请完成以下步骤。

1. 在 f AWS 管理控制台 or Wickr 上https://console.aws.amazon.com/wickr/打开。
2. 在 “网络” 页面上，选择要导航到该网络的网络名称。
3. 在导航窗格中，选择用户管理。
4. “团队目录” 选项卡显示注册到您的 Wickr 网络的用户。
5. 在 “团队目录” 选项卡中，选择 “管理用户”，然后选择 “批量删除”。
6. 在批量删除用户页面上，下载示例 CSV 模板。要下载示例模板，请选择下载模板。
7. 通过添加要从网络中批量删除的用户的电子邮件来完成模板。
8. 上传已完成的 CSV 模板。您可以将文件拖放到上传框中，也可以选择选择一个文件。
9. 选中该复选框，我知道删除用户是不可逆的。
10. 选择 “删除用户”。

> **Note**
>
> 此操作将立即开始删除用户，可能需要几分钟。已删除的用户将无法再在 Wickr 客户端中登录您的 Wickr 网络。

要通过下载团队目录的 CSV 来批量删除 Wickr 网络用户，请完成以下步骤。

1. 在 f AWS 管理控制台 or Wickr 上https://console.aws.amazon.com/wickr/打开。
2. 在 “网络” 页面上，选择要导航到该网络的网络名称。
3. 在导航窗格中，选择用户管理。
4. “团队目录” 选项卡显示注册到您的 Wickr 网络的用户。
5. 在 “团队目录” 选项卡中，选择 “管理用户”，然后选择 “下载为 CSV”。
6. 下载团队目录 CSV 模板后，移除不需要删除的用户行。
7. 在 “团队目录” 选项卡中，选择 “管理用户”，然后选择 “批量删除”。
8. 在批量删除用户页面上，上传团队目录 CSV 模板。您可以将文件拖放到上传框中，也可以选择选择文件。
9. 选中该复选框，我知道删除用户是不可逆的。
10. 选择 “删除用户”。

> **Note**
>
> 此操作将立即开始删除用户，可能需要几分钟。已删除的用户将无法再在 Wickr 客户端中登录您的 Wickr 网络。

批量暂停 AWS Wickr 网络中的用户

您可以在 for Wickr 的 “用户管理” 部分中批量暂停 Wickr 网络用户。 AWS 管理控制台

> **Note**
>
> 批量暂停用户的选项仅在未启用 SSO 时适用。

要批量暂停 Wickr 网络用户，请完成以下过程。

1. 在 f AWS 管理控制台 or Wickr 上https://console.aws.amazon.com/wickr/打开。
2. 在“网络”页面上，选择要导航到该网络的网络名称。
3. 在导航窗格中，选择用户管理。
4. “团队目录”选项卡显示注册到您的 Wickr 网络的用户。
5. 在“团队目录”选项卡中，选择“管理用户”，然后选择“批量暂停”。
6. 在批量暂停用户页面上，下载示例 CSV 模板。要下载示例模板，请选择下载模板。
7. 通过添加要从网络中批量暂停的用户的电子邮件来完成模板。
8. 上传已完成的 CSV 模板。您可以将文件拖放到上传框中，也可以选择选择一个文件。
9. 选择“暂停用户”。

> **Note**
>
> 此操作将立即开始暂停用户，可能需要几分钟。被暂停的用户无法在 Wickr 客户端中登录您的 Wickr 网络。当您在客户端暂停当前登录您的 Wickr 网络的用户时，该用户将自动注销。

AWS Wickr 网络中的访客用户

Wickr 访客用户功能允许个人访客用户登录 Wickr 客户端并与 Wickr 网络用户协作。Wickr 管理员可以为其 Wickr 网络启用或禁用访客用户。

该功能启用后，受邀加入 Wickr 网络的访客用户可以与 Wickr 网络中的用户互动。 AWS 账户 对于访客用户功能，将向您收取费用。有关访客用户功能定价的更多信息，请参阅定价附加组件下的 Wickr 定价页面。

主题

- 在 AWS Wickr 网络中启用或禁用访客用户
- 查看 AWS Wickr 网络中的访客用户数量
- 查看 AWS Wickr 网络中的每月使用量
- 查看 AWS Wickr 网络中的访客用户
- 在 AWS Wickr 网络中屏蔽访客用户

在 AWS Wickr 网络中启用或禁用访客用户

您可以在 Wickr 网络中启用或禁用访客用户。

完成以下步骤为 Wickr 网络启用或禁用访客用户。

1. 在 f AWS 管理控制台 or Wickr 上https://console.aws.amazon.com/wickr/打开。
2. 在 “网络” 页面上，选择要导航到该网络的网络名称。
3. 在导航窗格中，选择安全组。
4. 选择特定安全组的名称。

> **Note**
>
> 只能为单个安全组启用访客用户。要为 Wickr 网络中的所有安全组启用访客用户，必须为网络中的每个安全组启用此功能。

5. 在安全组中选择 “联合” 选项卡。
6. 在两个位置可以选择启用访客用户：
   - 本地联邦- 对于美国东部（弗吉尼亚北部）的网络，请在该页面的 “本地联邦” 部分选择 “编辑”。
   - 全球联合- 对于其他区域的所有其他网络，请在该页面的 “全球联合” 部分选择 “编辑”。
7. 在 “编辑联合” 页面上，选择 “启用联合”。
8. 选择保存更改以保存更改并使其对安全组生效。

   Wickr 网络中特定安全组的注册用户现在可以与访客用户交互。有关更多信息，请参阅《Wickr 用户指南》中的访客用户。

查看 AWS Wickr 网络中的访客用户数量

您可以在 Wickr 网络中查看访客用户数。

完成以下过程以查看 Wickr 网络的访客用户计数。

1. 在 f AWS 管理控制台 or Wickr 上https://console.aws.amazon.com/wickr/打开。
2. 在 “网络” 页面上，选择要导航到该网络的网络名称。
3. 在导航窗格中，选择用户管理。

   用户管理页面显示您的 Wickr 网络中的访客用户数量。

查看 AWS Wickr 网络中的每月使用量

您可以查看您的网络在计费周期内与之通信的访客用户数。

完成以下步骤以查看 Wickr 网络的每月使用量。

1. 在 f AWS 管理控制台 or Wickr 上https://console.aws.amazon.com/wickr/打开。
2. 在“网络”页面上，选择要导航到该网络的网络名称。
3. 在导航窗格中，选择用户管理。
4. 选择“访客用户”选项卡。

   访客用户选项卡显示访客用户的每月使用量。

> **Note**
>
> 访客账单数据每 24 小时更新一次。

查看 AWS Wickr 网络中的访客用户

您可以查看网络用户在特定账单周期内与之通信的访客用户。

完成以下步骤，查看网络用户在特定计费周期内与之通信的访客用户。

1. 在 f AWS 管理控制台 or Wickr 上https://console.aws.amazon.com/wickr/打开。
2. 在“网络”页面上，选择要导航到该网络的网络名称。
3. 在导航窗格中，选择用户管理。
4. 选择“访客用户”选项卡。

   访客用户选项卡显示您网络中的访客用户。

在 AWS Wickr 网络中屏蔽访客用户

您可以屏蔽和解除封锁您的 Wickr 网络中的访客用户。被屏蔽的用户无法与您网络中的任何人通信。

屏蔽访客用户

1. 在 f AWS 管理控制台 or Wickr 上https://console.aws.amazon.com/wickr/打开。

2. 在 “网络” 页面上，选择要导航到该网络的网络名称。
3. 在导航窗格中，选择用户管理。
4. 选择 “访客用户” 选项卡。

   访客用户选项卡显示您网络中的访客用户。
5. 在访客用户部分，找到您要屏蔽的访客用户的电子邮件。
6. 在访客用户名的右侧，选择三个点，然后选择屏蔽访客用户。
7. 选择弹出窗口中的屏蔽。
8. 要查看 Wickr 网络中被屏蔽的用户列表，请选择状态下拉菜单，然后选择已屏蔽。

解除对访客用户的屏蔽

1. 在 f AWS 管理控制台 or Wickr 上https://console.aws.amazon.com/wickr/打开。
2. 在 “网络” 页面上，选择要导航到该网络的网络名称。
3. 在导航窗格中，选择用户管理。
4. 选择 “访客用户” 选项卡。

   访客用户选项卡显示您网络中的访客用户。
5. 选择 “状态” 下拉菜单，然后选择 “已阻止”。
6. 在 “已屏蔽” 部分中，找到您要取消屏蔽的访客用户的电子邮件。
7. 在访客用户名的右侧，选择三个点，然后选择取消屏蔽用户。
8. 在弹出窗口中选择 “解除封锁”。

AWS Wickr 中的安全性

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

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

- 云安全 — AWS 负责保护在云中运行AWS服务的基础架构AWS Cloud。 AWS还为您提供可以安全使用的服务。 Third-party 作为AWS合规计划合规计划合规计划合的一部分，审计师定期测试和验证我们安全的有效性。要了解适用于 AWS Wickr 的合规计划，请参阅AWS按合规计划划分的范围内AWS服务按合规计划。
- 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、您公司的要求以及适用的法律法规。

此文档将帮助您了解如何在使用 Wickr 时应用责任共担模式。以下主题说明如何配置 Wickr 以实现您的安全性和合规性目标。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 Wickr 资源。

主题

AWS Wickr 中的数据保护

责任AWS共担模式适用于 AWS Wickr 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解答AWS条款。 有关欧洲数据保护的信息，请参阅通用数据保护条例（GDPR）中心。

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）。
- 用于 SSL/TLS 与AWS资源通信。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》https://aws.amazon.com/compliance/fips/。

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）。这包括你AWS 服务使用控制台、API 或 AWS SDK 与 Wickr 或其他人合作时。AWS CLI在用于名称的标签或自由格式文本字段中输入的任何数据都可能会用于计费或诊断日志。如果您向外部服务器提供 URL，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。

适用于 AWS Wickr 的 Identity and Access Management

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 管理员控制可以通过身份验证（登录）和授权（具有权限）使用 Wickr 资源的人员。您可以使用 IAMAWS 服务，无需支付额外费用。

主题

- 对 AWS Wickr 身份和访问进行故障排除

AWS Wickr 的受众

您的使用方式 AWS Identity and Access Management (IAM) 因您的角色而异：

- 服务用户：如果您无法访问功能，请从管理员处请求权限（请参阅对 AWS Wickr 身份和访问进行故障排除）
- 服务管理员：确定用户访问权限并提交权限请求（请参阅AWS Wickr 如何与 IAM 协同工作）
- IAM 管理员：编写用于管理访问权限的策略（请参阅Identity-based AWS Wickr 的策略示例）

使用 AWS Wickr 的身份进行身份验证

身份验证是您AWS使用身份凭证登录的方式。您必须以 IAM 用户身份进行身份验证AWS 账户根用户，或者通过担任 IAM 角色进行身份验证。

您可以使用来自身份源的证书AWS IAM Identity Center（例如（IAM Identity Center）、单点登录身份验证或 Google/Facebook 证书，以联合身份登录。有关登录的更多信息，请参阅《AWS 登录 用户指南》中的如何登录您的 AWS 账户。

对于编程访问，AWS提供 SDK 和 CLI 来对请求进行加密签名。有关更多信息，请参阅《IAM 用户指南》中的适用于 API 请求的 AWS 签名版本 4。

AWS 账户根用户

创建时AWS 账户，首先会有一个名为 AWS 账户 root 用户的登录身份，该身份可以完全访问所有资源AWS 服务和资源。我们强烈建议不要使用根用户进行日常任务。有关需要根用户凭证的任务，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，要求人类用户使用与身份提供商的联合身份验证才能AWS 服务使用临时证书进行访问。

联合身份是指来自您的企业目录、Web 身份提供商的用户Directory Service，或者AWS 服务使用来自身份源的凭据进行访问的用户。联合身份代入可提供临时凭证的角色。

要集中管理访问权限，建议使用。AWS IAM Identity Center有关更多信息，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

IAM 用户是对某个人员或应用程序具有特定权限的一个身份。建议使用临时凭证，而非具有长期凭证的 IAM 用户。有关更多信息，请参阅 IAM 用户指南中的要求人类用户使用身份提供商的联合身份验证才能AWS使用临时证书进行访问。

IAM 组指定一组 IAM 用户，便于更轻松地对大量用户进行权限管理。有关更多信息，请参阅《IAM 用户指南》中的 IAM 用户使用案例。

IAM 角色

IAM 角色是具有特定权限的身份，可提供临时凭证。您可以通过从用户切换到 IAM 角色（控制台）或调用AWS CLI或 AWS API 操作来代入角色。有关更多信息，请参阅《IAM 用户指南》中的担任角色的方法。

IAM 角色对于联合用户访问、临时 IAM 用户权限、跨账户访问、跨服务访问以及在 Amazon EC2 上运行的应用程序非常有用。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。

使用 AWS Wickr 的策略管理访问权限

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。策略定义了与身份或资源关联时的权限。 AWS在委托人提出请求时评估这些政策。大多数策略都以 JSON 文档的AWS形式存储在中。有关 JSON 策略文档的更多信息，请参阅《IAM 用户指南》中的 JSON 策略概述。

管理员使用策略，通过定义哪个主体可以在什么条件下对哪些资源执行哪些操作来指定谁有权访问什么。

默认情况下，用户和角色没有权限。IAM 管理员创建 IAM 策略并将其添加到角色中，然后用户可以担任这些角色。IAM 策略定义权限，与执行操作所用的方法无关。

Identity-based 政策

Identity-based 策略是您附加到身份（用户、组或角色）的 JSON 权限策略文档。这些策略控制身份可以执行什么操作、对哪些资源执行以及在什么条件下执行。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。

Identity-based 策略可以是内联策略（直接嵌入到单个身份中）或托管策略（附加到多个身份的独立策略）。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。

Resource-based 政策

Resource-based 策略是您附加到资源的 JSON 策略文档。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。您必须在基于资源的策略中指定主体。

Resource-based 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（ACL）

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

Amazon S3 和 Amazon VPC 就是支持 ACL 的服务示例。AWS WAF要了解有关 ACL 的更多信息，请参阅《Amazon Simple Storage Service 开发人员指南》中的访问控制列表（ACL）概览。

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。由此产生的权限是实体的基于身份的策略及其权限边界的交集。 Resource-based 在`Principal`字段中指定用户或角色的策略不受权限边界的限制。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。
- 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。

AWSAWS Wickr 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。这些策略涵盖常见使用案例，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。服务偶尔会向 AWS 托管式策略添加额外权限以支持新特征。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。

AWS托管策略： AWSWickrFullAccess

您可以将 `AWSWickrFullAccess` 策略附加到 IAM 身份。此策略向 Wickr 服务授予完全的管理权限，包括 AWS 管理控制台 中的 AWS 管理控制台 的权限。有关将策略添加到身份的更多信息，请参阅 AWS Identity and Access Management 用户指南中的添加和删除 IAM 身份权限。

权限详细信息

该策略包含以下权限。

- `wickr` — 向 Wickr 服务授予完全管理权限。

JSON

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

Wickr 更新至AWS托管策略

查看自该服务开始跟踪这些更改以来 Wickr AWS 托管策略更新的详细信息。有关此页面更改的自动提示，请订阅 Wickr 文档历史记录页面上的 RSS 源。

更改	描述	日期
AWSWickrFullAccess - 新策略	Wickr 添加了一项新策略，向 Wickr 服务（包括 AWS 管理控制台 中的 Wickr 管理员控制台）授予完全管理权限。	2022 年 11 月 28 日
Wickr 已开启跟踪更改	Wickr 开始跟踪其AWS托管策略的更改。	2022 年 11 月 28 日

AWS Wickr 如何与 IAM 协同工作

在使用 IAM 管理对 Wickr 的访问之前，您应该了解哪些 IAM 功能可用于 Wickr。

您可以与 AWS Wickr 搭配使用的 IAM 特征

IAM 功能	Wickr 支持
Identity-based 政策	是
Resource-based 政策	否
策略操作	是
策略资源	否
策略条件密钥	否
ACL	否
ABAC（策略中的标签）	否
临时凭证	否
主体权限	否
服务角色	否
Service-linked 角色	否

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

Identity-based Wickr 的政策

支持基于身份的策略：是

Identity-based 策略是您可以附加到身份（例如 IAM 用户、用户组或角色）的 JSON 权限策略文档。这些策略控制用户和角色可在何种条件下对哪些资源执行哪些操作。要了解如何创建基于身份的策略，请参阅《IAM 用户指南》中的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。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。

Identity-based Wickr 的策略示例

要查看 Wickr 基于身份的策略的示例，请参阅 Identity-based AWS Wickr 的策略示例。

Resource-based Wickr 内部的政策

支持基于资源的策略：否

Resource-based 策略是您附加到资源的 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它账户中的 IAM 实体指定为基于资源的策略中的主体。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。

适用于 Wickr 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。在策略中包含操作以授予执行关联操作的权限。

要查看 Wickr 操作的列表，请参阅服务授权参考中的 AWS Wickr 定义的操作。

Wickr 中的策略操作在操作前使用以下前缀：

```
wickr
```

要在单个语句中指定多项操作，请使用逗号将它们隔开。

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

要查看 Wickr 基于身份的策略的示例，请参阅 Identity-based AWS Wickr 的策略示例。

Wickr 的策略资源

支持策略资源：否

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。作为最佳实践，请使用其 Amazon 资源名称（ARN）指定资源。对于不支持资源级权限的操作，请使用通配符 (*) 指示语句应用于所有资源。

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

要查看 Wickr 的资源类型及其 ARN 的列表，请参阅《服务授权参考》中的 AWS Wickr 定义的资源。要了解您可以在哪些操作中指定每个资源的 ARN，请参阅 AWS Wickr 定义的操作。

要查看 Wickr 基于身份的策略的示例，请参阅 Identity-based AWS Wickr 的策略示例。

Wickr 的策略条件键

支持特定于服务的策略条件键：否

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。

Condition 元素根据定义的条件指定语句何时执行。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。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。

有关 Wickr 条件密钥的列表，请参阅《服务授权参考》中的 AWS Wickr 的条件密钥。要了解您可以对哪些操作和资源使用条件键，请参阅 AWS Wickr 定义的操作。

要查看 Wickr 基于身份的策略的示例，请参阅 Identity-based AWS Wickr 的策略示例。

Wickr 中的 ACL

支持 ACL：否

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

ABAC 与 Wickr

支持 ABAC（策略中的标签）：否

Attribute-based 访问控制 (ABAC) 是一种授权策略，它根据称为标签的属性来定义权限。您可以将标签附加到 IAM 实体和AWS资源，然后设计 ABAC 策略以允许在委托人的标签与资源上的标签匹配时进行操作。

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）。

将临时凭证用于 Wickr

支持临时凭证：否

临时证书提供对AWS资源的短期访问权限，并且是在您使用联合身份或切换角色时自动创建的。 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 用户指南》中的 IAM 中的临时安全凭证和使用 IAM 的。AWS 服务

Cross-service Wickr 的委托人权限

支持转发访问会话（FAS）：否

转发访问会话 (FAS) 使用调用主体的权限AWS 服务，再加上AWS 服务向下游服务发出请求的请求。有关发出 FAS 请求时的策略详情，请参阅转发访问会话。

Wickr 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 Wickr 的功能。仅当 Wickr 提供相关指导时才编辑服务角色。

Service-linked Wickr 的角色

支持服务相关角色：否

服务相关角色是一种链接到的服务角色。AWS 服务该服务可以代替您执行操作。 Service-linked 角色出现在您的，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关联角色的权限。

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Service-linked 角色列Yes中包含的服务。选择是链接以查看该服务的服务相关角色文档。

Identity-based AWS Wickr 的策略示例

默认情况下，全新的 IAM 用户没有执行任何操作的权限。IAM 管理员必须创建并分配 IAM policy以向用户授予管理 AWS Wickr 服务的权限。下面介绍权限策略示例。

JSON

```
{
    "Version":"2012-10-17",
    "Statement": [
        {
            "Effect": "Allow",
```

```
            "Action": [
                "wickr:CreateAdminSession",
                "wickr:ListNetworks"
            ],
            "Resource": "*"
        }
    ]
}
```

此示例策略允许用户使用 for Wickr 列出 Wick AWS 管理控制台 r 网络。要了解有关 IAM policy 语句中的元素的更多信息，请参阅 Identity-based Wickr 的政策。要了解如何使用这些示例 JSON 策略文档创建 IAM policy，请参阅《IAM 用户指南》中的在 JSON 选项卡上创建策略。

您还可以创建 IAM 策略以允许用户访问特定的 API 操作。对 API 操作的访问是与 AWS Wickr 控制台分开管理的。以下是向特定 API 操作授予只读访问权限的策略示例。有关 API 操作的更多信息，请参阅欢迎使用 AWS Wickr API 参考。

```
{
   "Version":"2012-10-17",
   "Statement":[
      {
         "Sid": "WickrAPIReadOnlyAccess",
            "Effect": "Allow",
            "Action": [
                "wickr:ListNetworks",
                "wickr:ListUsers",
                "wickr:GetNetworkSettings",
                "wickr:GetNetwork",
                "wickr:GetUser",
                "wickr:ListTagsForResource"
            ],
            "Resource": "*"
        }
    ]
}
```

主题

- 策略最佳实践
- 使用AWS 管理控制台适用于 Wickr
- 允许用户查看他们自己的权限

策略最佳实践

Identity-based 策略决定是否有人可以在您的账户中创建、访问或删除 Wickr 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 托管策略或工作职能的 AWS 托管策略。
- 应用最低权限：在使用 IAM 策略设置权限时，请仅授予执行任务所需的权限。为此，您可以定义在特定条件下可以对特定资源执行的操作，也称为最低权限许可。有关使用 IAM 应用权限的更多信息，请参阅《IAM 用户指南》中的 IAM 中的策略和权限。
- 使用 IAM 策略中的条件进一步限制访问权限：您可以向策略添加条件来限制对操作和资源的访问。例如，您可以编写策略条件来指定必须使用 SSL 发送所有请求。如果服务操作是通过特定的方式使用的，则也可以使用条件来授予对服务操作的访问权限AWS 服务，例如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AWS 管理控制台适用于 Wickr

将`AWSWickrFullAccess`AWS托管策略附加到您的 IAM 身份，以授予他们对 Wickr 服务的完全管理权限，包括中的 Wickr 管理员控制台。AWS 管理控制台有关更多信息，请参阅 AWS托管策略：AWSWickrFullAccess。

允许用户查看他们自己的权限

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

```
{
```

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

对 AWS Wickr 身份和访问进行故障排除

有关诊断和修复 IAM 常见问题的帮助，请参阅AWS Identity and Access Management用户指南中的 IAM 故障排除。

合规性验证

有关特定合规计划范围内的AWS服务列表，请参阅按合规计划划分的范围内的AWSAWS服务按合规计划。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。

您使用 Wickr 的合规性责任取决于您数据的敏感度、贵公司的合规性目标以及适用的法律法规。AWS 提供以下资源来帮助满足合规性：

- 安全与合规性快速入门指南 — 这些部署指南讨论了架构注意事项，并提供了在上部署以安全性和合规性为重点的基准环境的步骤。AWS
- 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。
- 使用AWS Config开发人员指南中的规则评估资源 —AWS Config; 评估您的资源配置在多大程度上符合内部实践、行业准则和法规。
- AWS Security Hub CSPM— 此AWS服务可全面了解您的安全状态AWS，帮助您检查是否符合安全行业标准和最佳实践。

AWS Wickr 中的故障恢复能力

AWS全球基础设施是围绕AWS 区域可用区构建的。 AWS 区域提供多个物理分隔和隔离的可用区，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设施相比，可用区具有更高的可用性、容错能力和可扩展性。

有关AWS 区域和可用区的更多信息，请参阅AWS全球基础设施。

除了AWS全球基础架构外，Wickr 还提供多项功能来帮助支持您的数据弹性和备份需求。有关更多信息，请参阅 AWS Wickr 的数据保留。

AWS PrivateLink适用于 AWS Wickr

借AWS PrivateLink助 AWS Wickr，您可以使用接口 VPC 终端节点在您的虚拟私有云 (VPC) 和 AWS Wickr 中的部分终端节点之间建立私有连接。接口 VPC 终端节点由AWS PrivateLink一种AWS技术提供支持，您可以使用该技术AWS通过私有 IP 地址访问在其上运行的服务。

对于移动客户端或其他本地设备，请使用 VPN 将您的设备连接到 VPC，以实现端到端的私有连接。有关更多信息，请参阅 AWS Virtual Private Network 文档。

有关AWS PrivateLink和 AWS VPC 的更多信息，请参阅什么是AWS PrivateLink？ 在《AWS PrivateLink指南》和《什么是 AWS VPC？》中 在《亚马逊虚拟私有云 Virtual Private Cloud 用户指南》中。

支持的 AWS Wickr 服务

以下 AWS Wickr 服务支持AWS PrivateLink：

服务	端点格式
AWS Wickr 管理员	com.amazonaws. *your-region* .wickr-admin
AWS Wickr 消息传递	com.amazonaws. *your-region* .wickr-messaging
AWS Wickr 通话	com.amazonaws. *your-region* .wickr-calling

目前，所有 Wickr VPC 终端节点都需要启用私有 DNS 名称。有关更多信息，请参阅启用私有 DNS 名称。

在公共 Wickr 终端节点支持 FIPS 的区域，Wickr VPC 终端节点支持 FIPS。有关更多信息，请参阅《联邦信息处理标准》。

目前不支持

- 消息和呼叫终端节点的 VPC 终端节点策略
- 消息和呼叫端点在中不可用us-east-1。

主题

先决条件

在创建 VPC 终端节点之前，请确保满足以下先决条件：

1. VPC 配置：正确配置的 VPC，其子网位于多个可用区
2. 安全组：允许 HTTPS 流量的相应安全组（端口 443）
3. DNS 解析：在 VPC 中启用了 DNS 主机名和 DNS 解析
4. IAM 权限：创建和管理 VPC 终端节点的必要权限

创建 VPC 端点

您可以为 AWS Wickr 管理员、消息和呼叫创建 VPC 终端节点。

完成以下过程，使用AWS控制台创建 VPC 终端节点。

步骤 1：导航到 VPC 控制台

1. 登录亚马逊 VPC 控制台。
2. 在左侧导航窗格中，选择端点。
3. 选择创建端点。

步骤 2：配置端点设置

1. 在服务类别下，选择AWS服务。
2. 在 “服务名称” 下，搜索wickr并选择相应的服务：
   - 对于管理员：com.amazonaws.*your-region*.wickr-admin
   - 对于消息传递：com.amazonaws.*your-region*.wickr-messaging
   - 致电：com.amazonaws.*your-region*.wickr-calling

步骤 3：网络配置

1. 在 VPC 下，选择您的目标 VPC。
2. 在 “子网” 下，选择多个可用区域中的子网以实现高可用性。
3. 在 “启用私有 DNS 名称” 下，选中复选框。这样可以支持私有 DNS 名称。

4. 在“安全组”下，选择或创建要与端点网络接口关联的安全组。

步骤 4：创建终端节点

1. 审核 配置。
2. 您可以选择添加或删除标签。标签是用于与端点关联的名称-值对。
3. 选择创建端点。

完成以下步骤以使用创建 VPC 终端节点AWS CLI。

1. 查看您所在地区的服务可用性：

   查看 Wickr 管理员的可用性

   ```
   aws ec2 describe-vpc-endpoint-services --service-names com.amazonaws.your-region.wickr-admin
   ```

   查看 Wickr 消息的可用性

   ```
   aws ec2 describe-vpc-endpoint-services --service-names com.amazonaws.your-region.wickr-messaging
   ```

   查看 Wickr 通话的可用性

   ```
   aws ec2 describe-vpc-endpoint-services --service-names com.amazonaws.your-region.wickr-calling
   ```

2. 创建 VPC 终端节点。

   Wickr 管理员端点：

   ```
   aws ec2 create-vpc-endpoint \
     --vpc-endpoint-type Interface \
     --service-name com.amazonaws.your-region.wickr-admin \
     --subnet-ids subnet-12345678 subnet-87654321 subnet-11223344 \
     --vpc-id vpc-12345678 \
     --security-group-ids sg-12345678 \
     --private-dns-enabled \
   ```

Wickr 消息传递端点

```
aws ec2 create-vpc-endpoint \
  --vpc-endpoint-type Interface \
  --service-name com.amazonaws.your-region.wickr-messaging \
  --subnet-ids subnet-12345678 subnet-87654321 subnet-11223344 \
  --vpc-id vpc-12345678 \
  --security-group-ids sg-12345678 \
  --private-dns-enabled \
```

Wickr 呼叫端点

```
aws ec2 create-vpc-endpoint \
  --vpc-endpoint-type Interface \
  --service-name com.amazonaws.your-region.wickr-calling \
  --subnet-ids subnet-12345678 subnet-87654321 subnet-11223344 \
  --vpc-id vpc-12345678 \
  --security-group-ids sg-12345678 \
  --private-dns-enabled \
```

限制

以下功能不受支持AWS PrivateLink，需要互联网连接：

- Wickr 开放存取 (WOA)
- 客户端应用程序更新
  - 移动应用程序 (iOS/Android)
    - 来源：App P Store/Google lay 商店
    - 要求：需要上网
  - 桌面应用程序
    - Windows/Mac: 使用全局 S3 端点（不AWS PrivateLink兼容）
    - Linux：使用 Snap Store（需要访问互联网）
- 调试和遥测
  - 崩溃报告

- 调试指标
- Client-side 分析链接
- 移动推送通知

  这些服务需要互联网连接，不能使用AWS PrivateLink：

  - 苹果推送通知
    - 要求：直接上网
    - 端口：443、2195、2196、5223
    - 参考：Apple Support 文档
  - Google/Android 通知
    - 要求：Firebase 云消息访问权限
    - 参考：Firebase 文档
- AWS Wickr 控制台目前不支持私有访问。有关更多信息，请参阅支持的AWS 区域、服务控制台和私有访问的功能。

所需的最低客户端版本AWS PrivateLink

以下客户端版本已经过验证AWS PrivateLink：

- iOS 6.64（如果适用）
- 安卓 6.60（如果适用）
- 桌面客户端 6.60
- Bots 6.60

需要额外配置的功能

Wickr Bots

- 要求： Customer-managed 基础设施
- 操作：为机器人依赖项配置网络路径
- 注意事项：确保机器人能够通过 VPC 终端节点访问所需的AWS服务

文件下载

- S3 连接：文件操作所必需的（法兰克福地区除外）
- 解决方案：创建 S3 VPC 网关终端节点
- 参考：AWS PrivateLink适用于亚马逊 S3

AWS Wickr 中的基础设施安全性

作为一项托管服务，AWS Wickr 受亚马逊网络服务：安全流程概述白皮书中描述的AWS全球网络安全程序的保护。

AWS Wickr 中的配置和漏洞分析

配置和 IT 控制由您（我们的客户）共同AWS负责。有关更多信息，请参阅责任AWS共担模型。

您有责任根据规格和指南配置 Wickr，定期指导您的用户下载最新版本的 Wickr 客户端，确保您运行的是最新版本的 Wickr 数据留存机器人，并监控您用户的 Wickr 使用情况。

AWS Wickr 的安全最佳实践

Wickr 提供了在您开发和实施自己的安全策略时需要考虑的大量安全功能。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。

为避免使用 Wickr 时可能会出现的安全事件，请遵循以下最佳实践：

- 实施最低权限访问权限并创建用于 Wickr 操作的特定角色。使用 IAM 模板创建一个角色。有关更多信息，请参阅 AWSAWS Wickr 的托管策略。
- 通过AWS 管理控制台对第一个进行身份验证即可访问 Wickr 的。AWS 管理控制台不要共享您的个人控制台凭证。互联网上的任何人都可以浏览到控制台，但除非他们拥有有效的控制台凭证，否则他们无法登录或启动会话。

监控 AWS Wickr

监控是维护 AWS Wickr 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 提供了以下监控工具，用于监视 Wickr、报告出现问题并在适当时自动采取措施：

- 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 AWS CloudTrail 《用户指南》。有关使用记录 Wickr API 调用的更多信息 CloudTrail，请参阅使用记录 AWS Wickr API 调用 AWS CloudTrail。

使用记录 AWS Wickr API 调用 AWS CloudTrail

AWS Wickr 与 AWS CloudTrail一项服务集成，该服务提供用户、角色或 AWS 服务在 Wickr 中执行的操作的记录。 CloudTrail 将 Wickr 的所有 API 调用捕获为事件。捕获的调用包括来自 for Wickr AWS 管理控制台 的调用和对 Wickr 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 Wickr 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。使用收集的信息 CloudTrail，您可以确定向 Wickr 发出的请求、发出请求的 IP 地址、谁发出了请求、何时发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》。

Wickr 中的信息 CloudTrail

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

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

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

所有 Wickr 操作都由记录。 CloudTrail例如，调用和ListNetworks操作会在 CloudTrail 日志文件中生成条目。CreateAdminSession

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

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

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

了解 Wickr 日志文件条目

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

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

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "<principal-id>",
        "arn": "<arn>",
        "accountId": "<account-id>",
        "accessKeyId": "<access-key-id>",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "<principal-id>",
                "arn": "<arn>",
                "accountId": "<account-id>",
                "userName": "<user-name>"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-03-10T07:53:17Z",
                "mfaAuthenticated": "false"
            }
```

```
        }
    },
    "eventTime": "2023-03-10T08:19:24Z",
    "eventSource": "wickr.amazonaws.com",
    "eventName": "CreateAdminSession",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "<ip-address>",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/110.0.0.0 Safari/537.36",
    "requestParameters": {
        "networkId": 56019692
    },
    "responseElements": {
        "sessionCookie": "***",
        "sessionNonce": "***"
    },
    "requestID": "39ed0e6f-36e9-460d-8a6e-f24be0ec11c5",
    "eventID": "98ccb633-0e6c-4325-8996-35c3043022ac",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "<account-id>",
    "eventCategory": "Management"
}
```

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

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "<principal-id>",
        "arn": "<arn>",
        "accountId": "<account-id>",
        "accessKeyId": "<access-key-id>",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "<principal-id>",
                "arn": "<arn>",
                "accountId": "<account-id>",
                "userName": "<user-name>"
            },
```

```
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-03-10T07:53:17Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-03-10T07:54:09Z",
    "eventSource": "wickr.amazonaws.com",
    "eventName": "CreateNetwork",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "<ip-address>",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/110.0.0.0 Safari/537.36",
    "requestParameters": {
        "networkName": "BOT_Network",
        "accessLevel": "3000"
    },
    "responseElements": null,
    "requestID": "b83c0b6e-73ae-45b6-8c85-9910f64d33a1",
    "eventID": "551277bb-87e0-4e66-b2a0-3cc1eff303f3",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "<account-id>",
    "eventCategory": "Management"
}
```

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

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "<principal-id>",
        "arn": "<arn>",
        "accountId": "<account-id>",
        "accessKeyId": "<access-key-id>",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "<principal-id>",
                "arn": "<arn>",
```

```
                "accountId": "<account-id>",
                "userName": "<user-name>"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-03-10T12:19:39Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-03-10T12:29:32Z",
    "eventSource": "wickr.amazonaws.com",
    "eventName": "ListNetworks",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "<ip-address>",
    "userAgent": "Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML,
 like Gecko) Chrome/110.0.0.0 Safari/537.36",
    "requestParameters": null,
    "responseElements": null,
    "requestID": "b9800ba8-541a-43d1-9c8e-efd94d5f2115",
    "eventID": "5fbc83d7-771b-457d-9329-f85163a6a428",
    "readOnly": true,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "<account-id>",
    "eventCategory": "Management"
}
```

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

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "<principal-id>",
        "arn": "<arn>",
        "accountId": "<account-id>",
        "accessKeyId": "<access-key-id>",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "<principal-id>",
                "arn": "<arn>",
```

```
                "accountId": "<account-id>",
                "userName": "<user-name>"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-03-08T22:42:15Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-03-08T22:42:58Z",
    "eventSource": "wickr.amazonaws.com",
    "eventName": "UpdateNetworkDetails",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "<ip-address>",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/110.0.0.0 Safari/537.36",
    "requestParameters": {
        "networkName": "CloudTrailTest1",
        "networkId": <network-id>
    },
    "responseElements": null,
    "requestID": "abced980-23c7-4de1-b3e3-56aaf0e1fdbb",
    "eventID": "a4dc3391-bdce-487d-b9b0-6f76cedbb198",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "<account-id>",
    "eventCategory": "Management"
}
```


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


```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "<principal-id>",
        "arn": "<arn>",
        "accountId": "<account-id>",
        "accessKeyId": "<access-key-id>",
        "sessionContext": {
            "sessionIssuer": {
```

```
                "type": "Role",
                "principalId": "<principal-id>",
                "arn": "<arn>",
                "accountId": "<account-id>",
                "userName": "<user-name>"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-03-08T22:42:15Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-03-08T23:06:04Z",
    "eventSource": "wickr.amazonaws.com",
    "eventName": "TagResource",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "<ip-address>",
    "userAgent": "Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36
 (KHTML, like Gecko) Chrome/110.0.0.0 Safari/537.36",
    "requestParameters": {
        "resource-arn": "<arn>",
        "tags": {
            "some-existing-key-3": "value 1"
        }
    },
    "responseElements": null,
    "requestID": "4ff210e1-f69c-4058-8ac3-633fed546983",
    "eventID": "26147035-8130-4841-b908-4537845fac6a",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "<account-id>",
    "eventCategory": "Management"
}
```

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

```
{
    "eventVersion": "1.08",
    "userIdentity": {
        "type": "AssumedRole",
        "principalId": "<principal-id>",
```

```
        "arn": "<arn>",
        "accountId": "<account-id>",
        "accessKeyId": "<access-key-id>",
        "sessionContext": {
            "sessionIssuer": {
                "type": "Role",
                "principalId": "<access-key-id>",
                "arn": "<arn>",
                "accountId": "<account-id>",
                "userName": "<user-name>"
            },
            "webIdFederationData": {},
            "attributes": {
                "creationDate": "2023-03-08T18:50:37Z",
                "mfaAuthenticated": "false"
            }
        }
    },
    "eventTime": "2023-03-08T18:50:37Z",
    "eventSource": "wickr.amazonaws.com",
    "eventName": "ListTagsForResource",
    "awsRegion": "us-east-1",
    "sourceIPAddress": "<ip-address>",
    "userAgent": "axios/0.27.2",
    "errorCode": "AccessDenied",
    "requestParameters": {
        "resource-arn": "<arn>"
    },
    "responseElements": {
        "message": "User: <arn> is not authorized to perform: wickr:ListTagsForResource
 on resource: <arn> with an explicit deny"
    },
    "requestID": "c7488490-a987-4ca2-a686-b29d06db89ed",
    "eventID": "5699d5de-3c69-4fe8-b353-8ae62f249187",
    "readOnly": false,
    "eventType": "AwsApiCall",
    "managementEvent": true,
    "recipientAccountId": "<account-id>",
    "eventCategory": "Management"
}
```

AWS Wickr 中的分析控制面板

您可以使用分析控制面板来查看您的组织如何使用 AWS Wickr。以下过程说明了如何使用 AWS Wickr 控制台访问分析控制面板。

访问分析仪表板

1. 在 f AWS 管理控制台 or Wickr 上https://console.aws.amazon.com/wickr/打开。
2. 在“网络”页面上，选择要导航到该网络的网络名称。
3. 在导航窗格中，选择分析。

   Analytics（分析）页面在不同的选项卡中显示您的网络的指标。

在“分析”页面上，您将在每个选项卡的右上角找到一个时间范围筛选器。此过滤器适用于整个页面。此外，在每个选项卡的右上角，您可以通过选择可用的“导出”选项来导出所选时间范围内的数据点。

> **Note**
>
> 所选时间采用 UTC（协调世界时）。

可以看到以下选项卡：

- 概述显示：
  - 已注册- 所选时间内网络上的注册用户总数，包括处于活动状态和暂停状态的用户。它不包括待处理或已邀请的用户。
  - 待处理- 所选时间内网络上的待处理用户总数。
  - 用户注册- 该图表显示所选时间范围内注册的用户总数。
  - 设备- 应用程序处于活动状态的设备数量。
  - 客户端版本- 按其客户端版本分类的活动设备数量。

- 成员显示：
  - 状态- 所选时间段内网络上的活跃用户。
  - 活跃用户 —
    - 该图表显示一段时间内的活跃用户数，可以按每天、每周或每月（在上述选定时间范围内）进行汇总。

    - 活跃用户数可以按平台、客户端版本或安全组进行细分。如果删除了安全组，则总计数将显示为 Deleted#。

- 消息显示：
    - 已发送的消息- 在所选时间段内，网络上所有用户和机器人发送的唯一消息的数量。
    - 呼叫- 网络中所有用户发出的唯一呼叫数。
    - 文件- 网络中用户发送的文件数（包括语音备忘录）。
    - 设备- 饼图显示按操作系统分类的活动设备数量。
    - 客户端版本- 按其客户端版本分类的活动设备数量。

对 AWS Wickr 的问题进行故障排除

以下程序和提示可以帮助您解决 AWS Wickr 的问题。

如果您无法使用本指南中的步骤解决问题，请在 AWS Support Center 中提交支持案例。

主题

解决 AWS Wickr 的一般问题

以下是疑难解答技巧，可帮助您解决 AWS Wickr 的一般问题。如果本节中的步骤无法解决您的问题，请在 Support Cent er 中AWS 提交案例。

主题

开始前的准备工作

在进行故障排除之前，请验证以下内容：

- 您使用的是适合您组织的 Wickr 产品：AWS Wickr、AWS WickrGov(GovCloud) 或 Wickr E nterpris e（自托管）。如果您不确定，请联系您的网络管理员。
- 您正在运行支持的客户端版本。AWS Wickr 支持当前版本和之前的 2-3 版本。要查看您的版本，请打开 Wickr，然后选择 “设置”、“关于”。要更新，请参阅检查更新。
- 您的组织采用了正确的身份验证方法（SSO 或非 SSO）。
- 您已将用户密码和 Wickr 恢复密钥保存在安全的位置。

- 您的网络允许与所需的 Wickr 域和端口进行通信。
- 您的设备符合系统要求。

收集诊断信息

客户机日志

要解决大多数 AWS Wickr 问题，客户端日志是必不可少的。

完成以下过程以收集客户机日志。

1. 登录 Wickr 客户端。
2. 在导航窗格中，选择菜单（三行或三点），然后选择 Su pport。
3. 选择 Su pport 日志记录。
4. 选择 “保存日志”。
5. 记下日志的保存位置。

按平台记录位置：

- Windows：`C:\Users\<USERNAME>\AppData\Local\Wickr, LLC\Wickr Pro\logs\`
- macOS：`~/Library/Application Support/Wickr, LLC/Wickr Pro/logs/`
- Linux：`~/.local/share/Wickr, LLC/Wickr Pro/logs/`
- iOS：通过 Support Logging 菜单导出
- Android：通过 Support 日志菜单导出

要收集的信息

进行故障排除或联系支持人员时，请收集：

- 设备信息：型号、操作系统版本
- 客户端版本：在 “设置” 中的 “关于” 下找到
- 网络 ID：可在管理员控制台的 “网络设置” 下找到
- 错误消息：精确的文字或屏幕截图
- 时间戳：问题发生的时间

- 复制步骤：如何重现问题
- 客户端日志：从 Support Logging 菜单

常见错误消息

无法连接到 Wickr 服务器。

可能的原因：

- 网络连接问题
- 防火墙阻止 Wickr 流量
- VPN 或代理干扰

解决方法

1. 对蜂窝数据与企业数据进行测试 WiFi ，以隔离网络问题。
2. 查看网络要求。
3. 请联系您的 IT 团队，将所需的域和端口列入许可名单。

此用户属于不同的网络。

可能的原因：用户账号存在于其他 Wickr 网络上

解决方法

1. 验证您使用的 AWS Wickr 客户端版本是否正确。
2. 请联系您的网络管理员。
3. 如果问题仍然存在，请使用用户电子邮件和网络 ID 与 Su AWS pport 联系。

账户已暂停

可能的原因：多次登录尝试失败或管理员操作失败

解决方法

1. 请联系您的网络管理员解除可能的暂停权限。

2. 如果您是唯一的管理员，请联系 Supp AWS ort。

需要电子邮件验证

可能的原因：注册期间未完成电子邮件验证。

解决方法

1. 检查 spam/junk 文件夹中是否有验证电子邮件。
2. 验证电子邮件地址是否正确。
3. 请咨询您的 IT 团队有关电子邮件过滤的信息。
4. 从登录屏幕申请新的验证电子邮件。

解决登录和注册问题

本部分可帮助您解决 AWS Wickr 的登录和注册问题。如果本节中的步骤无法解决您的问题，请在 Support Cent er 中AWS提交案例。

主题

- 开始前的准备工作
- 常见登录问题
- 注册问题
- 密码重置
- 账户暂停
- 收集日志

开始前的准备工作

在对登录或注册问题进行故障排除之前，请验证以下内容：

- 您使用的是适合您组织的 Wickr 产品：AWS Wickr、AWSWickrGov(GovCloud) 或 Wickr E nterpris e（自托管）。如果您不确定，请联系您的网络管理员。
- 您正在运行支持的客户端版本。AWS Wickr 支持当前版本和之前的 2-3 版本。要查看您的版本，请打开 Wickr，然后选择 “设置”、“关于”。要更新，请参阅检查更新。

- 您的组织采用了正确的身份验证方法（SSO 或非 SSO）。
- 您已将用户密码和 Wickr 恢复密钥保存在安全的位置。
- 您的网络允许与所需的 Wickr 域和端口进行通信。
- 您的设备符合系统要求。

> **Tip**
>
> 如果您在登录或注册过程中遇到错误，请在进行故障排除之前捕获错误消息的屏幕截图。这可以帮助您的管理员或 Su AWS pport 更快地诊断问题。

常见登录问题

登录失败时，错误消息将决定故障排除路径。首先确定您看到的是哪个错误。

“密码不正确” 或凭据被拒绝

1. 验证您输入的密码是否正确。检查是否有错别字、多余的空格和大写锁定。
2. 如果你使用 SSO（Okta、Microsoft Entra ID、Amazon Cognito），请通过身份提供商重置密码，而不是通过 Wickr 重置密码。
3. 如果您使用 Wickr-managed 证书，请参阅the section called “密码重置”。

“无法访问服务器” 或连接错误

这表示网络问题，而不是账户问题。

1. 验证您的互联网连接是否处于活动状态。
2. 切换网络 — 改用蜂窝数据 WiFi，反之亦然。
3. 如果在公司网络上，请您的 IT 团队确认是否允许使用所需的 Wickr 域和端口。
4. 如果使用 VPN，请尝试暂时断开连接。
5. 如果问题仍然存在，请收集日志并联系您的网络管理员。

“未找到账户” 或 “未找到用户”

1. 确认您登录的是正确的 Wickr 产品（AWS Wickr WickrGov vs Enterprise）。

2. 验证输入的用户名或电子邮件是否正确。
3. 您的账户可能已从网络中删除。请联系您的网络管理员。

“账户已暂停”

请参阅the section called “账户暂停”。

“此用户属于不同的网络”

1. 您可能不小心在另一个 Wickr 网络上创建了一个帐户（请参阅the section called “访客用户问题”）。
2. 确认您的组织使用的是正确的 Wickr 客户端。
3. 请联系您的网络管理员。管理员可能需要使用您的电子邮件地址和网络 ID 与 Su AWS pport 联系，以解决冲突。

在移动设备上登录失败，但在台式机上却能正常工作

1. 验证您输入的密码是否正确。
2. 测试蜂窝数据-禁用 WiFi 并重试。如果蜂窝网络正常工作但 WiFi 不行，则问题出在您的网络配置上。请联系您的 IT 团队。
3. 检查 Wickr 应用程序是否具有必要的设备权限。
4. 从您的应用商店卸载并重新安装 AWS Wickr。

> **Note**
>
> 重新安装会删除本地消息历史记录。

其他登录错误

如果您的错误未在上面列出：

1. 验证您输入的密码是否正确。
2. 截取错误消息的屏幕截图。
3. 为你的平台@@ 收集日志。
4. 请联系您的网络管理员获取屏幕截图和日志。

注册问题

访客用户问题

症状：注册后，您会看到 “访客网络” 屏幕，并且在组织的联系人中看不到其他用户。

原因：您直接启动了注册，而不是通过管理员的邀请完成注册。这将创建一个访客用户帐户，而不是加入您组织的网络。

解决方法：

1. 请联系您的网络管理员。
2. 管理员必须删除访客用户帐户，然后重新邀请您进入正确的网络。
3. 使用管理员提供的邀请链接或代码完成注册。

“此用户属于不同的网络”

原因：你不小心在不同的 Wickr 网络上创建了一个账户，或者你使用了错误的客户端。

1. 确认您使用的是正确的客户端：用于商业网络的 AWS Wickr，WickrGov或用于自托管的 W ickr Enterpris e。 GovCloud
2. 从 AWS Wickr 下载页面下载正确的客户端。
3. 请联系您的网络管理员。管理员可能需要使用您的电子邮件地址和网络 ID 与 Su AWS pport 联系。

用户名格式错误

AWS Wickr 中的用户名需要满足以下要求：

- 用户名是永久性的，创建后不能更改。
- 电子邮件地址是注册的主要标识符。
- 用户名不得包含不支持的特殊字符。通常支持字母数字字符、句点、连字符和下划线。
- 对于 SSO-enabled 网络，用户创建由身份提供商 (IdP) 处理。在登录 Wickr 客户端之前，用户必须存在于身份端。

未收到电子邮件验证

1. 检查您的垃圾邮件或垃圾文件夹。

2. 验证您输入的电子邮件地址是否正确。
3. 请联系您的 IT 团队，确保来自 AWS Wickr 的电子邮件不会被电子邮件筛选器屏蔽。
4. 返回登录屏幕并选择重新发送验证电子邮件的选项。

密码重置

> **Note**
>
> 对于 SSO-enabled 账户，密码重置由你的身份提供商（微软 Entra ID、Okta、Amazon Cognito 或）进行管理，而不是通过 Wickr 进行管理。

密码重置流程（非 SSO）：

> **Important**
>
> 重置 Wickr 密码即完全重置账户。这将永久删除所有本地消息历史记录，将用户从所有房间中移除，并清除设备注册。必须重新邀请用户进入他们之前参与的房间。此操作无法撤消。建议用户在继续操作之前用尽所有其他选项（验证大写锁定、检查已保存的密码、尝试其他设备）。

1. 在 Wickr 登录屏幕上，选择忘记密码？
2. 输入与您的 AWS Wickr 账户关联的电子邮件地址。
3. 检查您的收件箱中是否有密码重置电子邮件。如果几分钟内没有收到，请检查 spam/junk 文件夹。
4. 选择电子邮件中的密码重置链接。密码重置链接将在 24 小时后过期。
5. 输入并确认您的新密码。您的密码必须符合网络管理员配置的复杂性要求。

密码复杂性要求

密码要求由管理员在管理员控制台的 “安全组设置” 下配置。要求可能包括：

- 最小长度（至少 8 个字符；管理员可以设置得更高）
- 必填的小写字母数
- 所需的大写字母数

- 所需的数字数量
- 所需的特殊字符数

从客户端版本 6.70 开始，在 Android 和 iOS 上创建账户和更改密码期间，密码复杂度要求会以内联方式显示。

账户暂停

症状：您在登录时看到 “账户已暂停” 错误。

对于普通用户：

1. 请联系您的网络管理员。
2. 管理员可以在 “管理员控制台” > “团队目录” > “定位用户” > “取消暂停” 中解除暂停。

对于单个管理员（没有其他管理员可以取消暂停）：

请联系 Support，并AWS提供您的电子邮件地址、网络 ID 和管理员身份验证信息。

由于登录尝试失败而导致账户被封锁：

- 等待 24 小时自动解锁，或者
- 请联系您的网络管理员手动解锁您的帐户，或者
- 使用the section called “密码重置”流程重置您的凭证并解锁您的帐户。

如果您在取消暂停后无法登录：

请联系 Su AWS pport，告知您的电子邮件地址、网络 ID、客户端版本（Wickr > 设置 > 关于）和操作系统版本。

收集日志

日志收集方法因平台而异。在联系您的管理员或 Su AWS pport 之前，请收集日志。

桌面

如果你能访问 Wickr 菜单：

1. 打开 Wickr 并选择汉堡菜单 (☰)，然后选择 Support、Su pp ort L o gging。
2. 开启允许 Support 日志记录。要进行调查，还要启用 “扩展日志记录详细信息”。
3. 重现问题。
4. 返回 Su ppor t 并选择 “保存日志”。与您的管理员共享该文件。

如果您无法访问 Wickr 菜单（例如，客户端在登录屏幕上崩溃），请启动带有该`-logging`标志的客户端以生成日志：

- macOS：打开终端并运行：

  ```
  /Applications/AWS\ Wickr.app/Contents/MacOS/AWS\ Wickr -logging
  ```

  日志已保存到`~/Library/Application Support/Wickr, LLC/Wickr Pro/logs/`。
- Windows：打开 AWS Wickr 快捷方式的快捷菜单，选择 “属性”，然后选择 “快捷方式” 选项卡。附加`-logging`到目标路径（引号外）。启动快捷方式。

  日志已保存到`C:\Users\<USERNAME>\AppData\Local\Wickr, LLC\Wickr Pro\logs\`。
- Linux：从带有`-logging`标志的终端启动。

  日志已保存到`~/.local/share/Wickr, LLC/Wickr Pro/logs/`。

移动

1. 打开 Wickr 并选择 “设置”、“关于”、“导出所有日志”。
2. 与管理员共享导出的日志文件。

如果您无法访问 “设置”（例如，您停留在登录屏幕上）：

- iOS：将您的设备连接到 Mac，打开 Console.app，筛选 “Wickr”，然后重现问题。
- 安卓：启用 USB 调试，连接到计算机并运行`adb logcat | grep -i wickr`。

对 SSO 和身份验证问题进行故障排除

本部分可帮助管理员解决 AWS Wickr 的单点登录 (SSO) 和身份验证问题。如果本节中的步骤无法解决您的问题，请在 Support Cent er 中AWS 提交案例。

> **Important**
>
> Wickr 仅支持 Op enID Connect (O IDC)。 SAML-based 不支持身份提供者。如果您的组织使用 SAML-only 身份提供商，则必须配置 OIDC-compatible 替代方案或实施 OIDC 网桥。

主题

开始前的准备工作

在进行故障排除之前，请验证以下内容：

- 您拥有对 Wickr 管理控制台的管理员访问权限。
- 您可以访问组织的身份提供商 (IdP) 配置。
- 您的 Wickr 网络设置中已启用 SSO。
- 您的身份提供者是 OIDC-compliant。Wickr 不支持 SAML。

常见的 SSO 问题

支持的身份提供商

Wickr 为以下 OIDC-compliant身份提供商提供配置指导：

- 微软 Entra ID（前身为 Azure AD）
- Okta
- Amazon Cognito
- AWS Identity and Access Management 身份中心

任何 OIDC-compliant 身份提供者都可以与 Wickr 一起使用。对于上面未列出的提供商，请使用配置 SSO 文档中的常规 OIDC 配置参数。

用户无法使用 SSO 登录

当用户报告无法使用 SSO 登录时，请仔细检查以下内容。

验证 Wickr SSO 配置

1. 在 Wickr 管理员控制台中，选择网络设置，然后选择单个 Sign-On。
2. 确认已启用 SSO。
3. 验证颁发者 URL、客户端 ID 和客户端密钥是否与您的身份提供商配置相匹配。
4. 验证身份提供商中的重定向 URI 是否与 Wickr 管理控制台中显示的值相匹配。

常见的 SSO 错误

“未找到用户”

您的身份提供商中不存在该用户，或者该用户尚未被分配到 Wickr 应用程序。验证用户是否存在于您的 IdP 中，并且小组分配正确。

“响应无效” 或 “配置错误”

OIDC 元数据或端点配置错误。验证 Wickr 和您的身份提供商之间的发行者网址、客户端 ID 和重定向 URI 是否匹配。

“访问被拒绝”

用户在您的身份提供商中缺少所需的群组成员资格或应用程序分配。检查您的 IdP 的应用程序分配设置。

未提示用户输入公司 ID

如果在 SSO 注册期间没有提示用户输入公司 ID，请在 Wickr 管理员控制台的 “网络设置”、“网络配置文件” 中验证公司 ID 是否已配置。

确定问题出在 Wickr 还是您的身份提供商身上

使用以下问题来确定问题出在哪里：

- 用户能否使用同一 IdP 向其他应用程序进行身份验证？ 如果不是，则问题在于您的身份提供商，而不是 Wickr。
- 是所有用户都受到影响，还是只有特定用户受到影响？ 如果只有特定用户，请在您的 IdP 中查看他们的群组分配和应用程序访问权限。

- 您的 IdP 配置最近有变化吗？ 证书轮换、策略更改或端点更新可能会中断 OIDC 连接。
- 错误发生在 Wickr 客户端还是 IdP 登录页面中？ 如果错误出现在IdP登录页面上，则问题出在您的身份提供商身上。

其他资源

- 在 AWS Wickr 中配置 SSO
- 微软 Entra ID 单点登录设置（包括 Entra-specific 故障排除）

解决身份和访问问题

本部分帮助管理员解决使用 AWS Wickr 的身份和访问问题。如果本节中的步骤无法解决您的问题，请在 Support Cent er 中AWS 提交案例。

主题

- 开始前的准备工作
- 常见的身份和访问问题

开始前的准备工作

在进行故障排除之前，请验证以下内容：

- 您拥有对包含您的 Wickr 网络 AWS 账户 的管理员访问权限。
- 您可以访问 IAM 控制台或查看 IAM 策略。
- 您知道哪个 IAM 用户或角色遇到了访问问题。

常见的身份和访问问题

我无权在中执行操作 AWS 管理控制台 适用于 Wickr

如果 AWS 管理控制台 for Wickr 告诉您无权执行某项操作，则必须联系管理员寻求帮助。管理员是向您提供登录凭证的人。

当 `mateojackson` IAM 用户尝试使用 for Wickr 创建、管理或查看 Wickr 网络但没有`wickr:CreateAdminSession`和`wickr:ListNetworks`权限时，就会发生以下示例错误。 AWS 管理控制台

```
User: arn:aws:iam::123456789012:user/mateojackson is not authorized to perform:
 wickr:ListNetworks
```

在这种情况下，Mateo 要求管理员更新其策略，允许他使用`wickr:CreateAdminSession`和`wickr:ListNetworks`操作访问 Wickr 的。 AWS 管理控制台 有关更多信息，请参阅Identity-based AWS Wickr 的策略示例和AWS托管策略：AWSWickrFullAccess。

对网络和连接问题进行故障排除

本部分帮助管理员解决使用 AWS Wickr 的网络和连接问题。最终用户报告的大多数连接问题是由企业网络配置（防火墙、代理、VPN）阻塞所需的 Wickr 流量造成的。如果本节中的步骤无法解决您的问题，请在 Support Cent er 中AWS提交案例。

主题

开始前的准备工作

在进行故障排除之前，请验证以下各项：

- 您可以访问组织的网络配置（防火墙规则、代理设置、VPN 配置）。
- 您已经查看了 Wickr 网络要求（必需的域和端口）。
- 您已确认问题是否影响到所有用户、特定用户或特定位置。
- 您已确认受影响的用户是否可以在非公司网络（蜂窝网络或家庭网络 WiFi）上进行连接。

> **Important**
>
> 如果用户可以通过蜂窝数据或家庭网络进行连接， WiFi 但不能通过公司网络进行连接，则问题在于您的网络配置，而不是 Wickr 服务。

常见的网络问题

防火墙阻止 Wickr 流量

这是导致连接失败的最常见原因。Wickr 需要访问特定的域和端口。

症状

用户无法在公司上连接 WiFi ，但可以通过蜂窝数据进行连接。同一位置的多个用户会受到影响。Wickr 以前工作过，但在网络变更后停了下来。

解决方案

1. 在 Wickr 的网络要求中查看所需域和端口的完整列表。
2. 将防火墙中所有必需的域名列入白名单。Wickr 需要 HTTPS (TCP 443) 来发送消息和信令，需要使用 UDP 端口进行语音和视频通话。
3. 在公司网络中验证所需域的 DNS 解析。使用`nslookup`或`dig`确认域名已解析。
4. 进行更改后测试连通性。让受影响的用户重启 Wickr 并尝试连接。

> **Note**
>
> 如果只有语音和视频通话失败但消息传递正常，那么 UDP 流量可能会被阻止。默认情况下，Wickr 使用 UDP 进行通话。请参阅the section called “UDP 已阻止（通话失败，消息正常）”。

代理服务器干扰

公司代理服务器可能会干扰 Wickr 连接，尤其是在它们不支持 WebSocket 连接的情况下。

症状

只有在配置代理时才会出现连接问题。绕过代理时，Wickr 可以正常工作。间歇性断开连接。

解决方案

1. 验证您的代理是否支持 WebSocket 连接（Wickr 消息传递所必需的）。
2. 为网络要求中列出的 Wickr 域配置代理绕过（PAC 文件例外或直接连接规则）。
3. 查看代理日志，了解与 Wickr 域的连接是否受阻或失败。

4. 如果您的代理需要身份验证，请确认 Wickr 流量没有因为缺少凭据而被拒绝。Wickr 不支持在 SaaS 部署上进行代理身份验证。

SSL/TLS 检查断开连接

企业 SSL 检查（也称为 HTTPS 检查或 TLS 拦截）破坏了 Wickr 所期望的证书链，从而导致连接失败。

症状

Wickr 中的证书错误。“安全连接失败” 错误。Wickr 可以在没有 SSL 检查的网络上运行。

解决方案

1. 首选：绕过 Wickr 域名的 SSL 检查。将 SSL 检查设备配置为排除网络要求中列出的域。这样可以维持 Wickr 的端到端加密。
2. 备选方案：在用户设备上安装组织的根 CA 证书。这允许 Wickr 信任截获的证书链。请联系您的 IT 安全团队获取证书和安装说明。

要验证 SSL 检查是否是原因，请在受影响的设备上运行以下命令，并将证书颁发者与预期的AWS证书进行比较：

```
openssl s_client -showcerts -connect ingress-prod-calling.wickr.us-
east-1.amazonaws.com:443
```

如果证书颁发者显示的是贵组织的 CA 而不是AWS或 Amazon 证书，则会对 Wickr 流量进行 SSL 检查。

VPN 封锁 Wickr

VPN 配置通常会阻止 Wickr 流量，尤其是呼叫所需的 UDP 端口。

症状

Wickr 在没有 VPN 的情况下工作，但在连接 VPN 的情况下却无法运行。VPN 连接时连接中断。通话失败，但通过 VPN 可以发送消息。

解决方案

1. 配置分割隧道以直接路由 Wickr 流量（绕过 VPN 隧道）网络要求中列出的域。
2. 如果不允许分割隧道，请确保 VPN 同时允许 TCP 443 和网络要求中列出的 UDP 端口。

3. 如果只有呼叫通过 VPN 进行故障转移，则 VPN 可能会阻止 UDP。请参阅the section called “UDP 已阻止（通话失败，消息正常）”。

UDP 已阻止（通话失败，消息正常）

默认情况下，Wickr 使用 UDP 进行语音和视频通话，然后回退到 TCP。如果您的网络阻止 UDP，则呼叫将无法立即连接，并且会回退到 TCP，性能可能会降低，同时消息传递将继续正常工作。您可以在 Wickr 网络安全组中启用（强制）TCP 调用以完全跳过 UDP，从而强制所有调用 TCP。

诊断

要求受影响的用户启用 TCP 呼叫作为测试（或者通过控制台为所有用户启用 enable/force TCP）：设置、呼叫、启用 TCP 呼叫。如果在启用 TCP 的情况下呼叫成功，则会阻止 UDP。

解决方案

将防火墙和 VPN 配置中网络要求中列出的 UDP 端口列入许可名单。

TCP 调用是一种诊断工具，而不是永久的解决方案。使用 TCP 时，通话质量会降低。

DNS 解析失败

如果您的 DNS 服务器无法解析 Wickr 域，则客户端将无法连接。

诊断

在受影响网络上的设备上，验证所需 Wickr 域的 DNS 解析：

```
nslookup gw-pro-prod.wickr.com
```

如果域名无法解析，则问题出在 DNS 配置上。

解决方案

1. 验证您的 DNS 服务器能否解析网络要求中列出的域。
2. 如果使用 DNS 过滤或 DNS 防火墙，请为 Wickr 域名添加例外情况。
3. 使用备用 DNS 服务器（例如`8.8.8.8`）进行测试，以确认问题是否出在您的内部 DNS 上。

确定问题的范围

使用以下问题来缩小原因范围：

- Wickr 能处理蜂窝数据还是家庭 WiFi数据？ 如果是，则问题出在您的公司网络配置上。
- 是所有用户都受到影响，还是只有特定用户受到影响？ 如果某个地点的所有用户都受到影响，则问题出在整个网络范围内。如果只有特定用户，请检查他们的设备或 VPN 配置。
- 这是在网络变更之后开始的？ 防火墙规则更新、代理更改或 VPN 配置更改通常会中断 Wickr 连接。
- 消息可以正常工作但通话失败了吗？ 这表示 UDP 已被阻止。请参阅the section called “UDP 已阻止（通话失败，消息正常）”。
- 用户会看到证书错误吗？ 这表明 SSL 检查正在拦截 Wickr 流量。请参阅the section called “SSL/TLS 检查断开连接”。

其他资源

- AWS Wickr 的网络要求（必需的域和端口）
- End-user 网络疑难解答（与受影响的用户共享）

文档历史记录

下表介绍了 Wickr 的文档版本。

变更	说明	日期
文件预览现已可用	Wickr 管理员现在可以启用或禁用文件下载。有关更多信息，请参阅 AWS Wickr 的文件预览。	2025 年 5 月 29 日
全新设计的 Wickr 管理员控制台现已上市	Wickr 增强了 Wickr 管理员控制台，以实现更好的导航，并改善了管理员的可访问性。	2025 年 3 月 13 日
Wickr 现已在亚太地区（马来西亚）上市 AWS 区域	Wickr 现已在亚太地区（马来西亚）AWS 区域上市。有关更多信息，请参阅区域可用性。	2024 年 11 月 20 日
删除网络现已可用	Wickr 管理员现在可以删除 AWS Wickr 网络。有关更多信息，请参阅在 AWS Wickr 中删除网络。	2024 年 10 月 4 日
使用微软 Entra (Azure AD) SSO 配置 AWS Wickr 现已上线	AWS Wickr 可以配置为使用微软 Entra (Azure AD) 作为身份提供商。有关更多信息，请参阅使用微软 Entra (Azure AD) 单点登录配置 AWS Wickr。	2024 年 9 月 18 日
Wickr 现已在欧洲（苏黎世）上市 AWS 区域	Wickr 现已在欧洲（苏黎世）AWS 区域上市。有关更多信息，请参阅区域可用性。	2024 年 8 月 12 日
跨境分类和联合现已推出	跨界分类功能允许用户更改对话的 GovCloud 用户界面。有	2024 年 6 月 25 日

	关更多信息，请参阅GovCloud跨界分类和联合。	
已读回执功能现已推出	Wickr 管理员现在可以在管理员控制台中启用或禁用已读回执功能。有关更多信息，请参阅已读回执。	2024 年 4 月 23 日
全局联合现在支持受限联合，管理员可以在管理员控制台中查看使用情况分析	全局联合现在支持受限联合。这适用于其他 AWS 区域网络中的 Wickr 网络。有关更多信息，请参阅安全组。此外，管理员现在可以在管理员控制台的 Analytics 控制面板上查看其使用情况分析。有关更多信息，请参阅 “分析” 控制面板。	2024 年 3 月 28 日
AWS Wickr 高级版套餐现已推出三个月免费试用	Wickr 管理员现在可以为多达 30 名用户选择三个月的免费试用高级套餐。在免费试用期间，标准版和高级版计划的所有功能都可用，包括无限的管理员控制和数据保留。在高级版免费试用期间，访客用户功能不可用。有关更多信息，请参阅管理套餐。	2024 年 2 月 9 日
访客用户功能现已正式启用，并已添加更多管理员控件	Wickr 管理员现在可以访问一系列新功能，包括访客用户列表、批量删除或暂停用户的功能以及阻止访客用户在 Wickr 网络中通信的选项。有关更多信息，请参阅用户指南。	2023 年 11 月 8 日
Wickr 现已在欧洲（法兰克福）上市 AWS 区域	Wickr 现已在欧洲（法兰克福） AWS 区域上市。有关更多信息，请参阅区域可用性。	2023 年 10 月 26 日

Wickr 网络现在可以跨界联合了 AWS 区域	Wickr 网络现在可以在 AWS 区域进行联合身份验证。有关更多信息，请参阅安全组。	2023 年 9 月 29 日
Wickr 现已在欧洲（伦敦）上市 AWS 区域	Wickr 现已在欧洲（伦敦）AWS 区域上市。有关更多信息，请参阅区域可用性。	2023 年 8 月 23 日
Wickr 现已在加拿大（中部）上市 AWS 区域	Wickr 现已在加拿大（中部）AWS 区域上市。有关更多信息，请参阅区域可用性。	2023 年 7 月 3 日
访客用户功能现已可供预览	访客用户可以登录到 Wickr 客户端并连接 Wickr 网络用户。有关更多信息，请参阅访客用户（预览）。	2023 年 5 月 31 日
AWS Wickr 现已与（美国西部）集成 AWS CloudTrail，现已在 AWS GovCloud （美国西部）上市 WickrGov	AWS Wickr 现已与集成。AWS CloudTrail有关更多信息，请参阅使用 AWS CloudTrail记录 AWS Wickr API 调用。此外，Wickr 现已在 AWS GovCloud （美国西部）上市。 WickrGov有关更多信息，请参阅《AWS GovCloud (US) 用户指南》中的 AWS WickrGov。	2023 年 3 月 30 日
标记和多网络创建	AWS Wickr 现在支持添加标签。有关更多信息，请参阅网络标签。现在可以在 Wickr 中创建多个网络。有关更多信息，请参阅创建网络。	2023 年 3 月 7 日
初始版本	《Wickr 管理指南》初始版本	2022 年 11 月 28 日

发行说明

为了帮助您跟踪 Wickr 正在进行的更新和改进，我们发布了描述最近更改的发布说明。

2026 年 6 月

- 会话超时-管理员现在可以配置非活动超时，在指定时间后自动锁定 Wickr 客户端。系统会提示用户重新进行身份验证以恢复会话。
- 意见征求横幅-管理员现在可以配置用户登录时显示的同意横幅。用户在访问应用程序之前必须确认横幅。

2026 年 3 月

- 整个管理控制台的可访问性已得到改进，包括对 ATAK 帮助面板、SSO 配置和网络创建流程的更新。

2025 年 12 月

- 设备暂停和取消暂停操作已从管理员控制台中删除。管理员可以继续重置用户设备。

2025 年 11 月

- 改进了网络和安全组表的 UI 和 UX，以及页面加载和 API 调用监控的控制台指标。

2025 年 8 月

- AWS Wickr 的电子邮件模板AWSWickrGov 已更新，以改善用户入门体验。发件人的电子邮件地址已从更改`donotreply@wickr.email`为`no-reply@amazonaws.com`。

2025 年 5 月

- 文件预览现已可用。当管理员在管理员控制台中为安全组禁用文件下载时，用户只能在 “消息” 和 “文件” 选项卡中查看支持的文件列表。

2025 年 3 月

- 重新设计的 Wickr 管理员控制台现已推出。

2024 年 10 月

- Wickr 现在支持删除网络。有关更多信息，请参阅在 AWS Wickr 中删除网络。

2024 年 9 月

- 管理员现在可以使用微软 Entra (Azure AD) 单点登录配置 AWS Wickr。有关更多信息，请参阅使用微软 Entra (Azure AD) 单点登录配置 AWS Wickr。

2024 年 8 月

- 增强功能
  - Wickr 现已在欧洲（苏黎世）AWS 区域上市。

2024 年 6 月

- 跨境分类和联合现在可供 GovCloud用户使用。有关更多信息，请参阅GovCloud 跨界分类和联合。

2024 年 4 月

- Wickr 现在支持已读回执。有关更多信息，请参阅已读回执。

2024 年 3 月

- 全局联合现在支持受限联合，只有在受限联合下添加的选定网络才能启用全局联合。这适用于其他 AWS 区域网络中的 Wickr 网络。有关更多信息，请参阅安全组。
- 管理员现在可以在管理员控制台的 Analytics 控制面板上查看其使用情况分析。有关更多信息，请参阅 “分析” 控制面板。

2024 年 2 月

- AWS Wickr现在为多达30名用户提供为期三个月的高级套餐免费试用。更改和限制包括：
  - 高级版免费试用版现已提供所有标准版和高级版套餐功能，例如无限制的管理员控制和数据保留。在 Premium 免费试用期间，访客用户功能不可用。
  - 之前的免费试用版不再可用。如果您尚未使用高级免费试用版，则可以将现有的免费试用版或标准版升级为高级版免费试用版。有关更多信息，请参阅管理套餐。

2023 年 11 月

- 访客用户功能现已正式推出。更改和新增内容包括：
  - 能够举报其他 Wickr 用户的滥用行为。
  - 管理员可以查看网络与之交互的访客用户列表以及每月使用计数。
  - 管理员可以阻止访客用户与其网络通信。
  - Add-on 访客用户的定价。

- 管理控制增强功能
  - 能够批量 delete/suspend 使用用户。
  - 用于配置令牌刷新宽限期的其他 SSO 设置。

2023 年 10 月

- 增强功能
  - Wickr 现已在欧洲地区（法兰克福）AWS 区域 发布。

2023 年 9 月

- 增强功能
  - Wickr 网络现在可以在 AWS 区域 进行联合身份验证。有关更多信息，请参阅安全组。

2023 年 8 月

- 增强功能
  - Wickr 现已在欧洲地区（伦敦）AWS 区域 发布。

2023 年 7 月

- 增强功能
  - Wickr 现已在加拿大（中部）AWS 区域 发布 。

2023 年 5 月

- 增强功能
  - 增加了对访客用户的支持。有关更多信息，请参阅 AWS Wickr 网络中的访客用户。

2023 年 3 月

- Wickr 现已与集成。AWS CloudTrail有关更多信息，请参阅 使用记录 AWS Wickr API 调用 AWS CloudTrail。
- Wickr 现已在 AWS GovCloud (US-West) 中推出。 WickrGov有关更多信息，请参阅《AWS GovCloud (US) 用户指南》中的 AWSWickrGov。
- Wickr 现在支持标记。有关更多信息，请参阅 AWS Wickr 的网络标签。现在可以在 Wickr 中创建多个网络。有关更多信息，请参阅 步骤 1：创建网络。

2023 年 2 月

- Wickr 现在支持安卓战术攻击套件 (ATAK)。有关更多信息，请参阅 在 Wickr 网络控制面板中启用 ATAK。

2023 年 1 月

- 现在可以在所有套餐中配置单点登录 (SSO)，包括免费试用版和标准版。

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。