Splashtop On-Prem

系统管理员手册

2025年8月

目录

公司信息

Splashtop Inc. 总部位于加利福尼亚州圣何塞，成立于 2006 年，致力于提供全球领先的远程访问、远程支持、跨屏幕生产和协作体验，让您能轻松远程连接智能手机、平板电脑、电脑、电视和云。

Splashtop 全球用户超过3000万，惠普、联想、戴尔、宏碁、索尼、华硕、东芝、英特尔等制造业合作伙伴已在1亿多台设备上安装使用 Splashtop 软件。

了解更多或试用 Splashtop 产品，请访问网站 www.splashtop.com**。**

Splashtop Inc.

美国加利福尼亚州库比蒂诺市沃尔夫北路
10050号SW2-S260室，邮编95014

简介

Splashtop On-Prem 是可在企业内网完全自托管的本地化解决方案。IT 管理员可以借助集中式数据库和管理控制台，轻松解决系统安全问题，同时为用户提供流畅的远程控制体验。

团队所有者可以自定义部署套件，使最终用户无需进行繁琐的安装和配置步骤。

通过 **Splashtop-Prem** 应用程序，远程控制更加简单易用。从远程电脑轻松办公，就像在现场操作一样，完全不用担心使用 VPN 会出现的连接慢和延迟问题。

Splashtop On-Prem 功能

Splashtop On-Prem 解决方案具备各种内置功能。单击功能名称可详细了解。

高清质量远程性能：Splashtop 的 Remote Access 和 Remote Support 解决方案的 On-Prem 版本使用同样的高性能引擎，为面向消费者和中端市场的产品提供核心技术，目前已荣获多个奖项，用户多达数百万。高清质量、实时快速连接和多个并发会话。

多对多显示器：从多个显示器系统同时查看多个远程显示器，包括多对一和多对多查看。甚至可查看多个 Mac 显示器！

文件传输：通过快速安全的远程连接，可以快速传输文件。可以在不同电脑之间拖放文件，也可以在不启动远程会话的情况下传输文件！

聊天：在会话中或会话外与远程电脑的用户聊天。

远程重启：从 Splashtop 应用或网络控制台重启远程电脑。选择常规或安全模式重启。

远程唤醒：远程唤醒电脑。目标电脑必须支持 Wake-on-LAN（WoL） 且通过以太网线连接。同时，必须打开同一网络的另一台电脑的电源。

远程打印：将远程电脑的文件在本地打印机上打印。无需传输文件，也无需传真打印的文件。只需从远程电脑中选择所需文件，即可立即在本地打印机上打印。

会话录制：录制远程访问会话。使用远程访问窗口中的屏幕录制按钮开始和停止录制。所有录制内容都将保存到本地电脑。

AD 集成：Microsoft Active Directory （AD） 现已与 Splashtop On-Prem 集成，团队管理中可以轻松管理权限并访问电脑和其他设备。支持 Microsoft Windows Server 2012、2016和2019。

两步验证：两步验证，也称为多因素身份验证 （MFA），通过部署另一台设备以提升用户账户的安全性，该台设备会发布时间相关的动态密码用于验证凭据。采用两步验证，账户会更安全！

远程麦克风： 通过远程麦克风功能，可以将本地电脑的麦克风输入重定向到远程电脑，就像在远程电脑前操作一样。有了这一功能，则可直接加入 Skype、Teams、Zoom、VoIP 等平台的通话，还可以通过远程会话使用语音听写或录音软件。

USB 设备重定向： 通过设备重定向，可以将本地电脑上的 USB 设备重定向到远程电脑。被重定向的设备可在远程电脑允许，就像直接插入远程电脑一样。

更多...

点击在线支持网站以详细了解新产品功能。

Splashtop On-Prem 使用场景

Splashtop On-Prem 适用于不同使用场景。Splashtop On-Prem 通常可采用以下三种模式进行部署：远程访问、无人值守支持或有人值守支持

远程访问

个人用户和团队可以随时随地从电脑、智能手机或平板电脑远程访问 Windows 和 Mac 电脑，就像在远程电脑前操作一样。如果需要 LogMeIn Pro 或 GoToMyPC 的替代方案，则可试用 Splashtop On-Prem 远程访问解决方案。

无人值守支持

适用于 IT 人员管理地理位置分散的电脑和其他设备，可从一台电脑同时远程访问多台电脑以及其他设备，可以极大地提高 IT 工作效率。

仅需在每个远程设备中安装并预配置一个代理 （Streamer 应用程序），即可随时远程连接。

有人值守支持 （SOS）

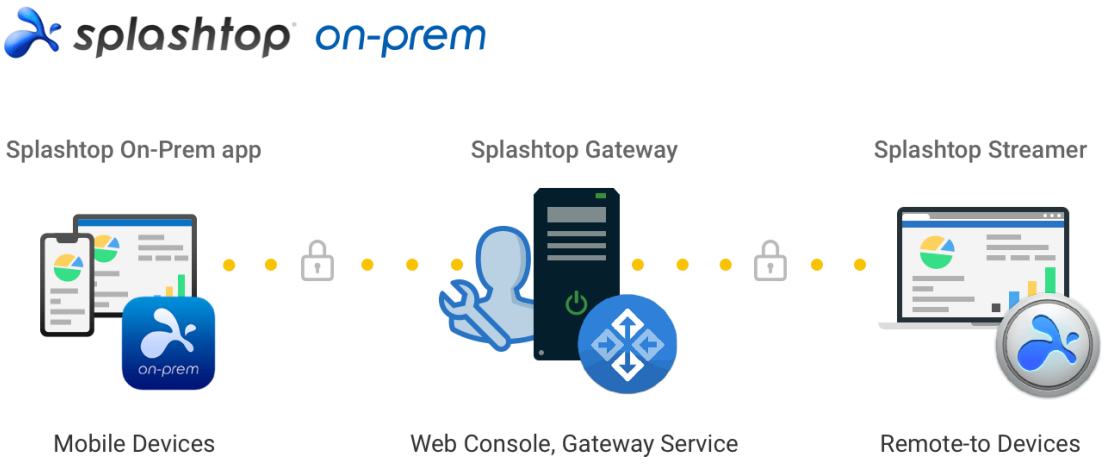
适用于 Service Desk 和 MSP 的完美解决方案，技术人员可以快速建立临时远程会话，无需最终用户在电脑中安装任何软件或插件。不过，最终用户需要下载并启动独立应用程序 SOS，并将显示的会话码提供给技术人员。

这是最具成本效益的解决方案。仅需购买一个许可证，技术人员即可远程连接无限数量的电脑，以确保妥善处理每个支持请求。

如果需要 TeamViewer、LogMeIn Rescue 或 GoToAssist 的替代方案，则可试用 Splashtop On-Prem 有人值守支持解决方案。

安装

关键组件



- Splashtop Gateway：执行 Gateway、中继、用户和设备管理功能。这是对用户和设备进行身份验证、保护和连接的中央服务器。可提供网络控制台以配置（和报告）用户和设备。安装在 Windows 服务器上。
- **Splashtop On-Prem 应用程序**：可以在本地设备和运行 Splashtop Streamer 的目标远程设备之间建立远程会话。
- Splashtop Streamer 应用程序：需要在要访问的远程设备上安装并运行。可将音频和视频流式传输到安装 On-Prem 的设备。

下载安装包

作为本地托管解决方案，大多数组件都打包到 **Splashtop Gateway** 安装包中，并支持各种平台。Gateway 初始设置成功后，用户就能下载并安装 **Splashtop Streamer** 和 **Splashtop On-Prem** 应用程序。

- *关于 Splashtop Gateway 安装包*，请参阅 Splashtop Gateway 发布公告页面
- *关于 Splashtop Streamer 安装程序*，请参阅此文：如何获取正确的 Splashtop Streamer 安装程序
- *关于 Splashtop On-Prem 应用程序安装程序*，请参阅此文：如何获取正确的 Splashtop On-Prem 应用程序

除了带有打包组件的常规 Splashtop Gateway 版本外，Splashtop 还将发布 **Splashtop Streamer** 和 **Splashtop On-Prem** 应用程序以进行补丁，此类组件将作为 PKG 文件发布，仅供团队所有者导入 Gateway。请在用户从 Gateway 下载之前，参阅系统配置章节中的软件部分，了解如何将新组件下载并导入到 Splashtop Gateway。

请随时访问公告和下载以获取系统的最新版本。

系统要求

Splashtop Gateway Server 要求

- **操作系统（64 位版本）**
  - Windows Server 2022
  - Windows Server 2019
  - Windows Server 2016
  - Windows 11
  - Windows 10
- **软件**
  - 使用管理员权限运行。
- **最低硬件规格（少于 100 个并发会话，无集中式会话录制）**
  - 处理器： 8 Cores or above
  - 内存：16GB 或以上

  - SSD 或 HDD：已安装的驱动器上为 60GB 或更高（建议在固态驱动器上安装网关）
- **最低硬件规格（超过 100 个并发会话 + 集中式会话录制）**
  - 处理器： 16 cores or above
  - 内存：64GB 或以上
  - SSD：已安装的驱动器上为 80GB 或以上

浏览器类型要求

  - Google Chrom
  - Safari
  - Edge
  - Firefox

On-Prem 应用程序设备要求

- **iPad 或 iPhone**
  - iOS 12.x 或更高版本
- **Android**
  - Android 4.0* 或更高版本
  - ARM 32/64、X86 处理器或 nVidia Tegra
  - Chromebook
- **Windows**
  - Windows XP*、Vista*、Windows 7、8、10或11
- **Mac**
  - macOS 10.10 或更高版本

*如果从 Gateway 安全选项卡禁用TLS 1.0 and 1.1 are disabled（仅 TLS 1.2），则不支持 Windows XP/Vista、Windows Server 2003和 Android 4.0。

Streamer 设备要求

- **操作系统**

  - Windows 11
  - Windows 10
  - Windows 8/8.1
  - Windows 7
  - Windows Server 2022
  - Windows Server 2019

- Windows Server 2016
- Windows Server 2012
- Mac OS 10.10或更高版本
- Android 5.0或更高版本
- iOS 12.x 或更高版本（适用于 SOS on-prem 版）
- Linux
    - Ubuntu desktop 16.04和18.04
    - CentOS 7和8
    - Red Hat Enterprise Linux （RHEL） 7.3-8.1
    - Fedora 29-31

- iOS 12.x 或更高版本（适用于 SOS 本地部署版）
- Linux
    - Ubuntu desktop 16.04和18.04
    - CentOS 7和8
    - Red Hat Enterpr
    - Fedora 29-31

- 硬件

    - 处理器： 1.6 GHz 或速度更快的双核中央处理器
    - 内存：2GB 或以上
    - 网络连接

*如果从“Gateway 安全”选项卡禁用 TLS 1.0 和 1.1（仅限 TLS 1.2），则不支持 Windows XP/Vista、Windows Server 2003 和 Android 4.0。

网络要求

基于 Internet 的远程会话

Splashtop On-Prem 是可在办公室局域网完全自托管的本地化解决方案。但有时需要从家里或其他地方访问办公室电脑，并且必须通过 Internet 建立连接。

要在 Splashtop On-Prem 中启用基于 Internet 的远程会话，可通过以下几个选项设置系统：

- 在 DMZ 网络中部署 Splashtop Gateway Server
- 为 Splashtop Gateway Server 分配公共 IP 地址
- 设置端口转发，从公共 IP 到分配给 Splashtop Gateway Server 的私有 IP
- 在云上托管 Splashtop Gateway Server
- 在客户端设备中安装 VPN 应用程序

防火墙端口

默认情况下，Splashtop Gateway 使用端口443与 Streamer 和客户端设备通信，因此必须确保端口443未被网络防火墙或操作系统防火墙阻止，也没有被其他应用程序占用。

此外，以下端口因为被本地电脑上的 Gateway 使用，也不能被占用。

- 端口号：9080
- 端口号：5432
- 端口号：7080
- 端口号：7081

快速安装指南

启动并运行 Splashtop 软件的基本步骤通常如下所示。前5个步骤由您（团队所有者或管理员）完成，其余2个步骤由用户完成。

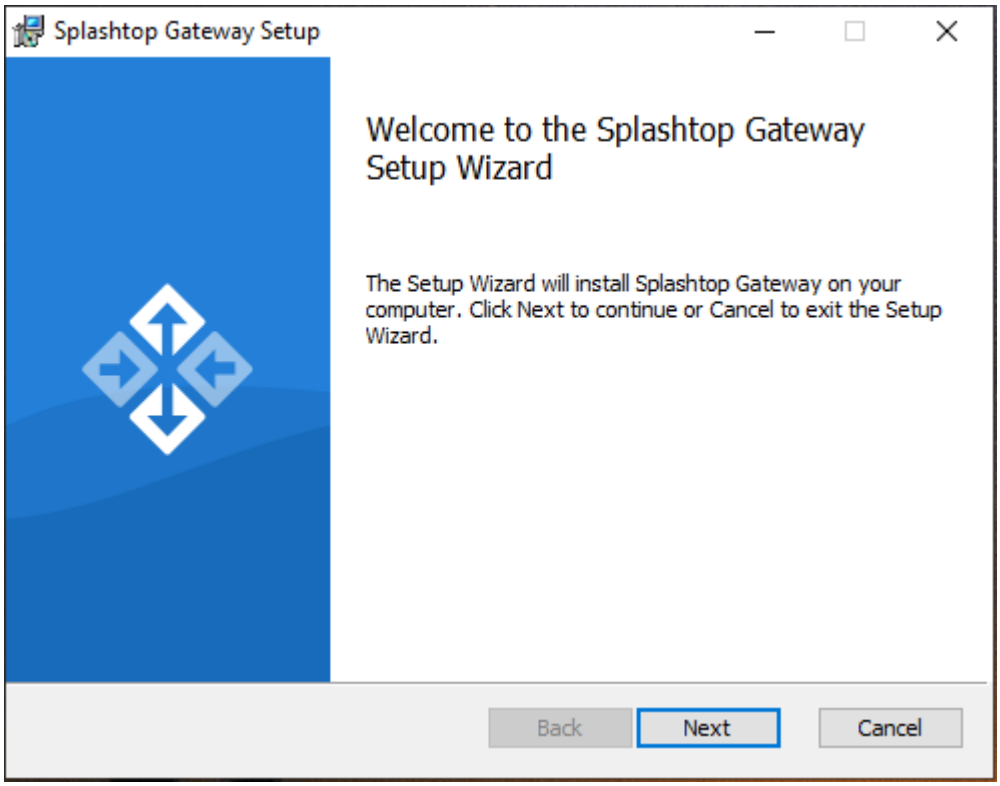
1. 团队所有者在公司网络上设置 Splashtop Gateway。

2. 团队所有者根据需要对电脑进行分组，并设置相应权限。
3. 团队所有者创建用户账户。
4. 团队所有者通知用户其已被添加到 Splashtop Gateway，并向用户提供特定凭据，例如激活码和密码。
5. 团队所有者或管理员部署 Streamer 并将其安装在可供用户远程访问的所有目标电脑上。
6. 用户通过 Splashtop Gateway 网络控制台将 Splashtop On-Prem 客户端应用程序下载并安装到其设备上。
7. 用户启动 Splashtop On-Prem 客户端应用程序并输入团队所有者或管理员提供的网关 IP 地址、账户名和密码。完成后，用户即可安全访问工作环境中的电脑。

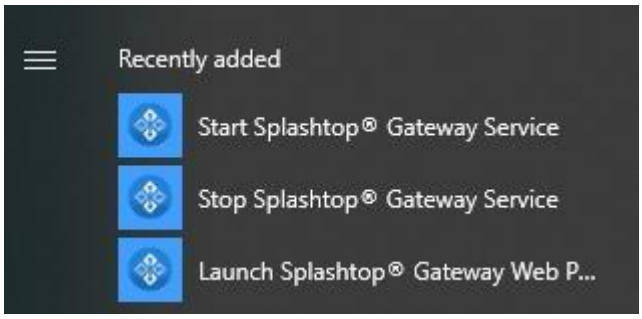
Splashtop Gateway 和 Splashtop Steamer 可以安装在同一个 Windows 服务器上。建议采用这种做法，因为在团队所有者需要配置 Splashtop Gateway 设置或重启 Splashtop Gateway 服务时，就能远程访问该服务器。

1. 安装 Splashtop Gateway

a) 下载程序并双击 EXE 文件，通过 Windows 安装向导开始安装。



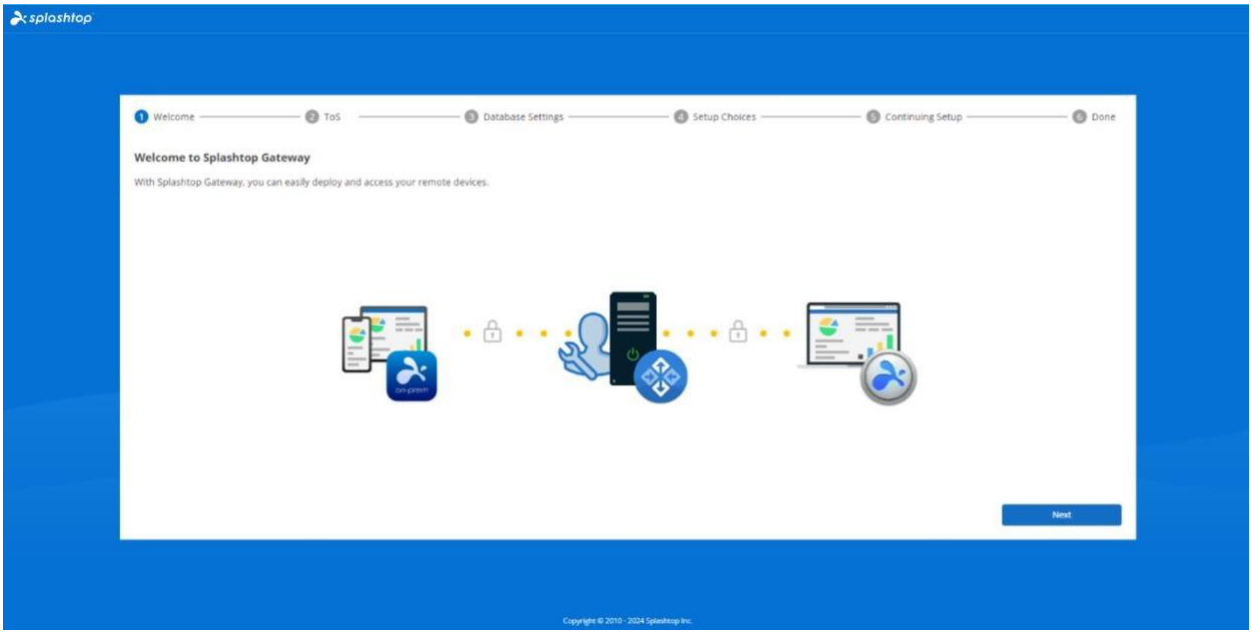
b) 安装完成后，打开 Windows 启动菜单，找到刚刚创建的3个启动快捷方式。单击启动 Splashtop Gateway Web 门户，在默认浏览器中启动网关网络控制台。



注意：我们强烈建议使用 Google Chrome、新版 Microsoft Edge、Safari、Firefox 等现代浏览器打开 Splashtop Gateway 网络控制台。

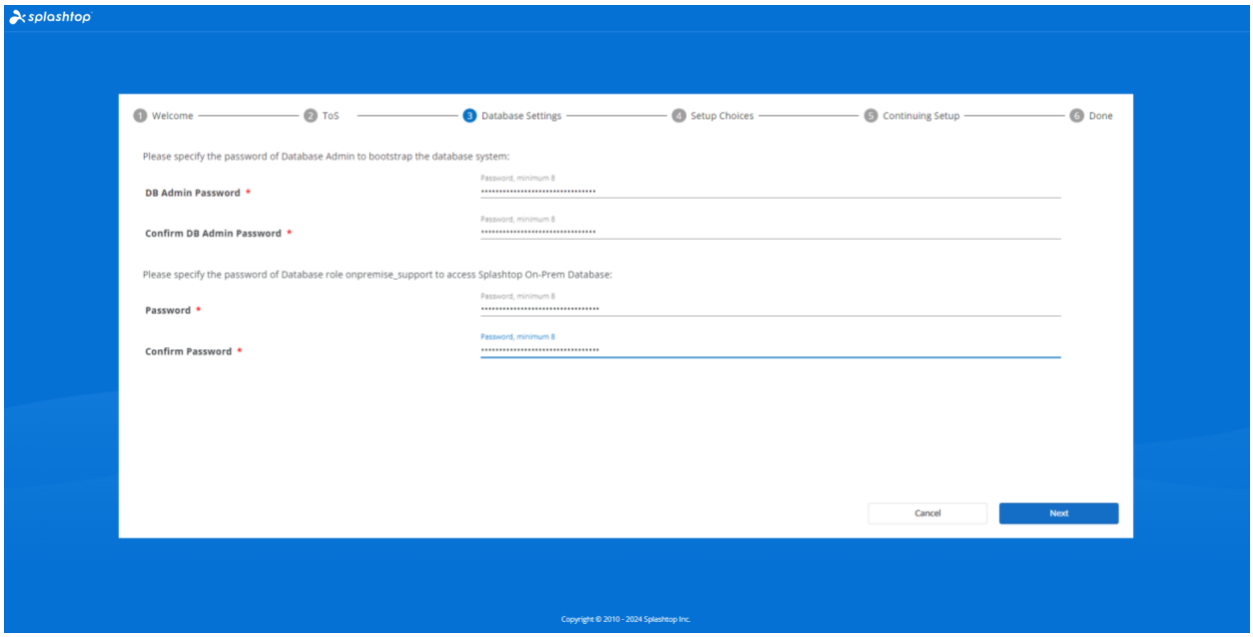
2. Splashtop Gateway OOBE 设置

a) 首次从浏览器启动网络控制台后，将显示包含服务条款的 OOBE 设置过程。单击下一步继续。

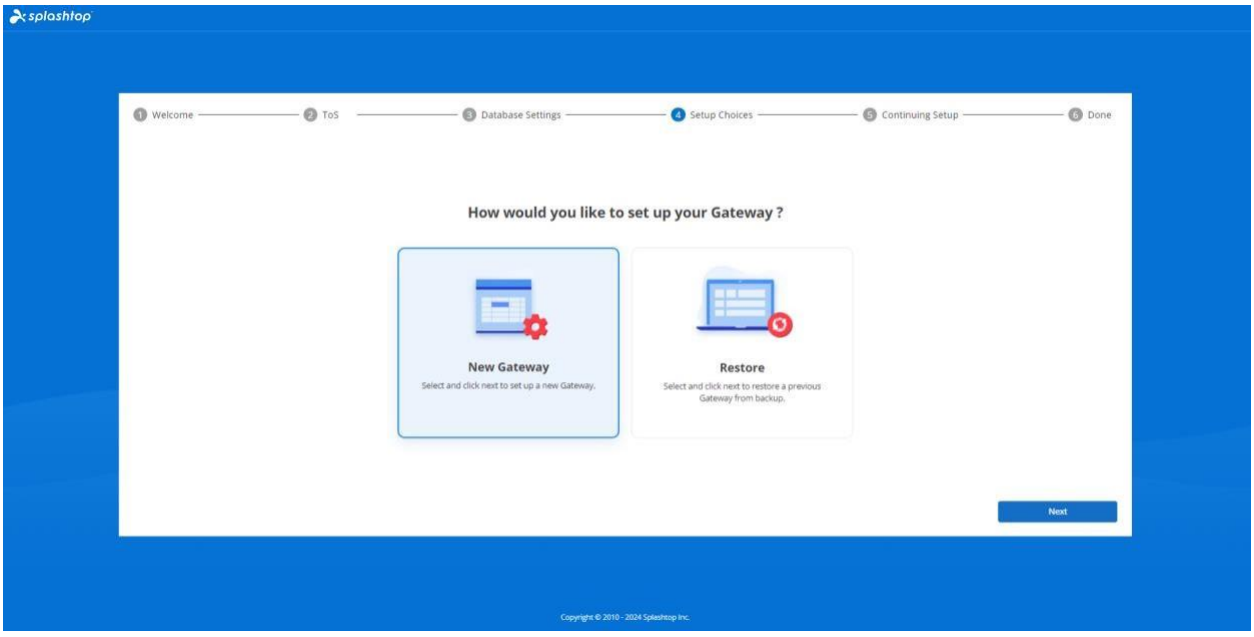


b) 设置 Splashtop Gateway 数据库管理和访问密码。此步需等待30秒以进行数据库初始化。

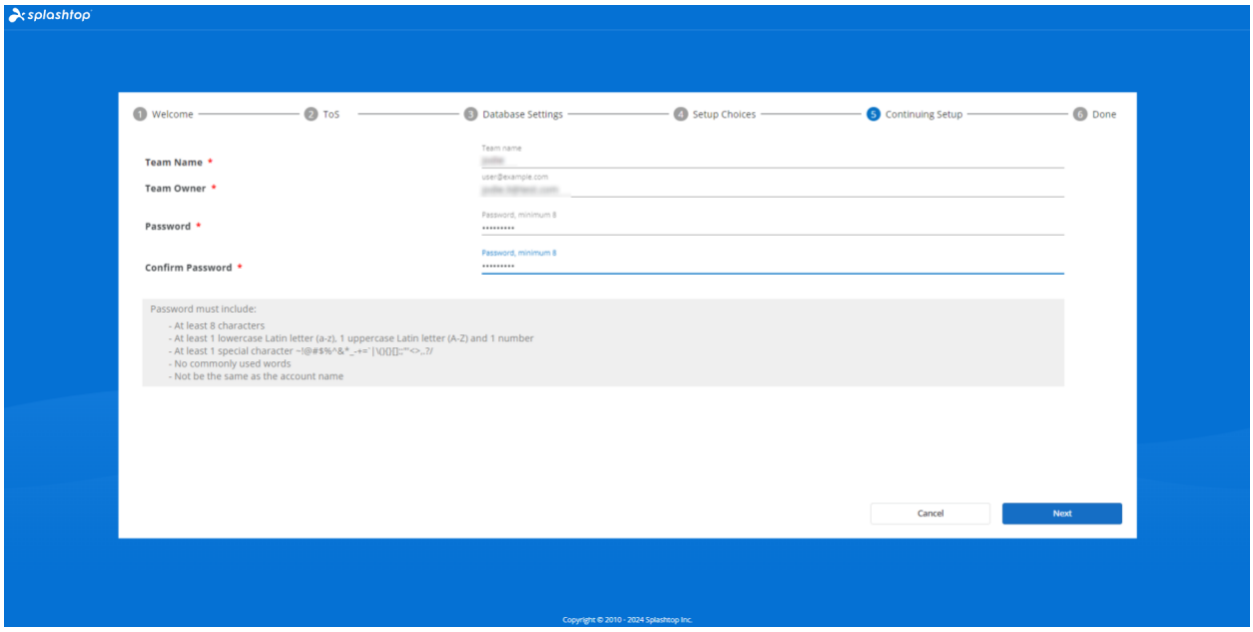
注意：请记住您的数据库密码并妥善保存，因为数据库密码无法更改。



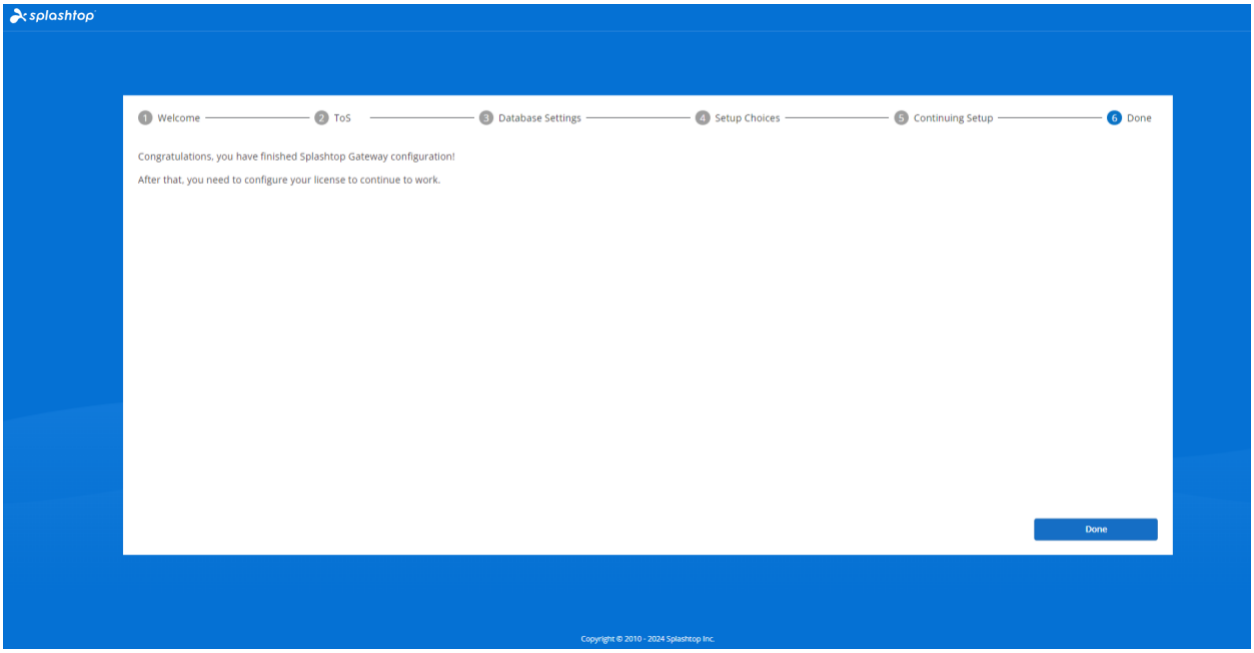
c) 选择 Gateway 设置首选项。



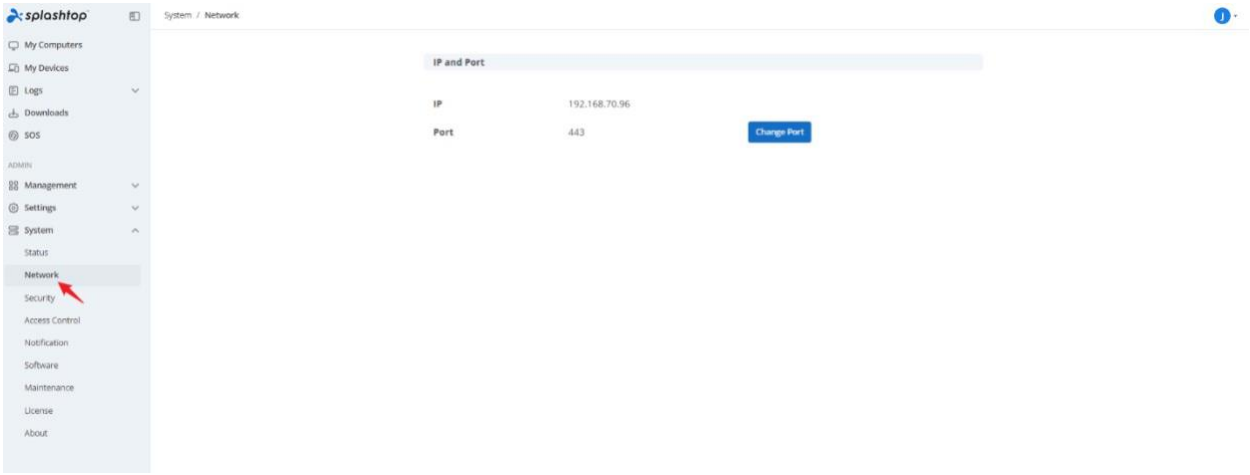
d) 通过输入电子邮件账户和凭据来建立首个团队和所有者，以完成 OOBE 设置。



e) OOBE 设置完成后， 使用刚刚创建的凭据登录到网络控制台。需要根据定制的许可证模式激活在线或离线许可证。



f) 激活 Splashtop On-Prem 后，则可登录到 Splashtop Gateway – 系统 – 网络以查看以太网/无线 IP 地址和端口号，如下图所示。此页面中显示的 IP 地址即为 **Gateway IP 地址**，使用 **On-Prem 客户端应用程序**或 **Splashtop Streamer** 登录时，该地址将与**端口号**（默认为 443）一同填写。



3. 通过许可证激活 Splashtop Gateway

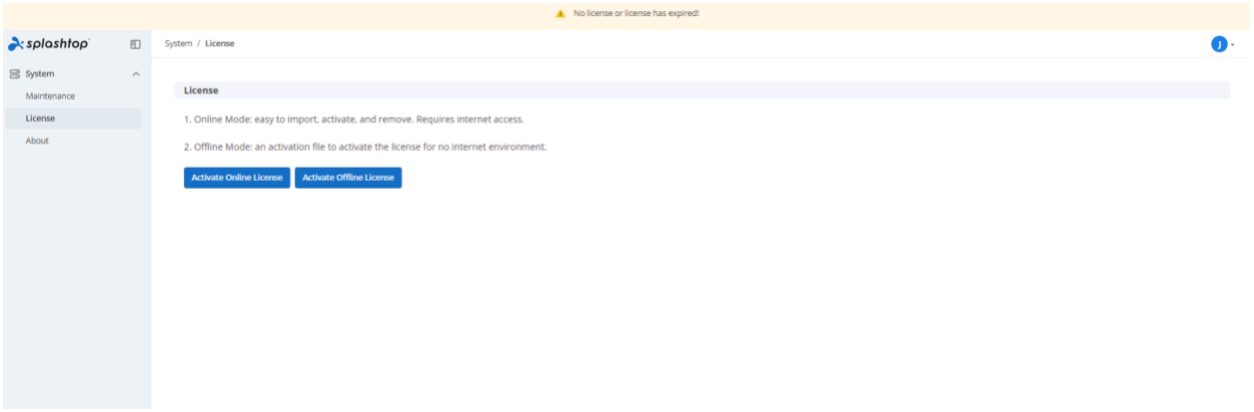
Splashtop Gateway **必须**通过有效的许可证激活才能使用。

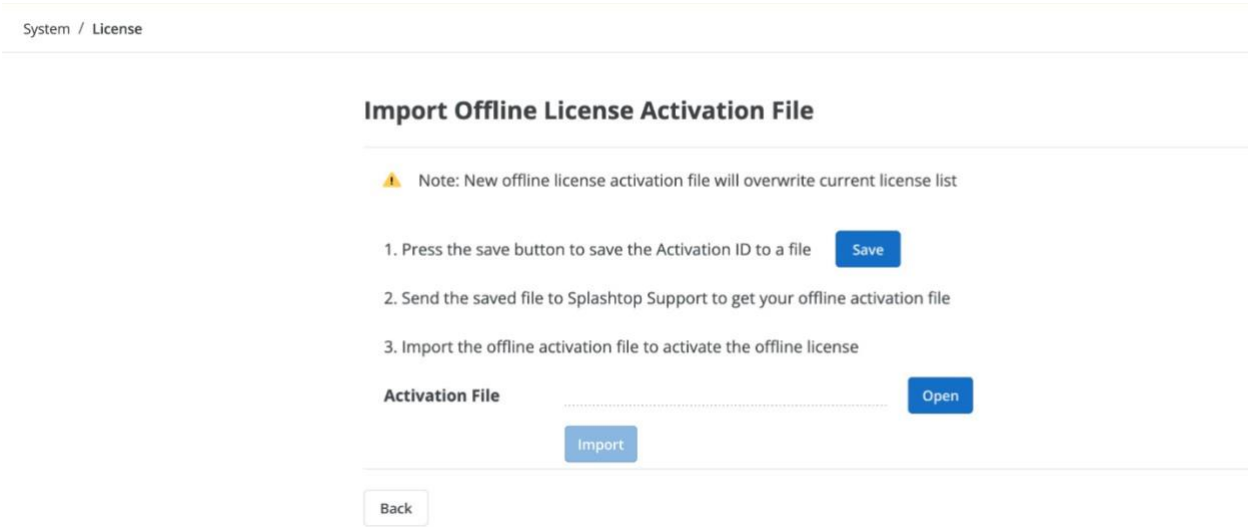
注意：请联系 Splashtop 销售人员或 Splashtop 支持部门，申请试用许可证或获取订购的许可证。

使用系统所有者登录 https://{gatewayaddress}，导航到**系统 > 许可证**页面以导入要激活的许可证。

Splashtop Gateway 提供在线和离线许可证激活。

- **在线激活：**激活在线许可证需要 Internet 访问，一旦 Gateway 激活，就可以将其移动到离线环境。
- **离线激活：**单击**保存** 以下载激活 ID 并将其发送给我们的支持人员。收到激活文件即可继续激活。请按照网络控制台的说明进行操作。（见下图）



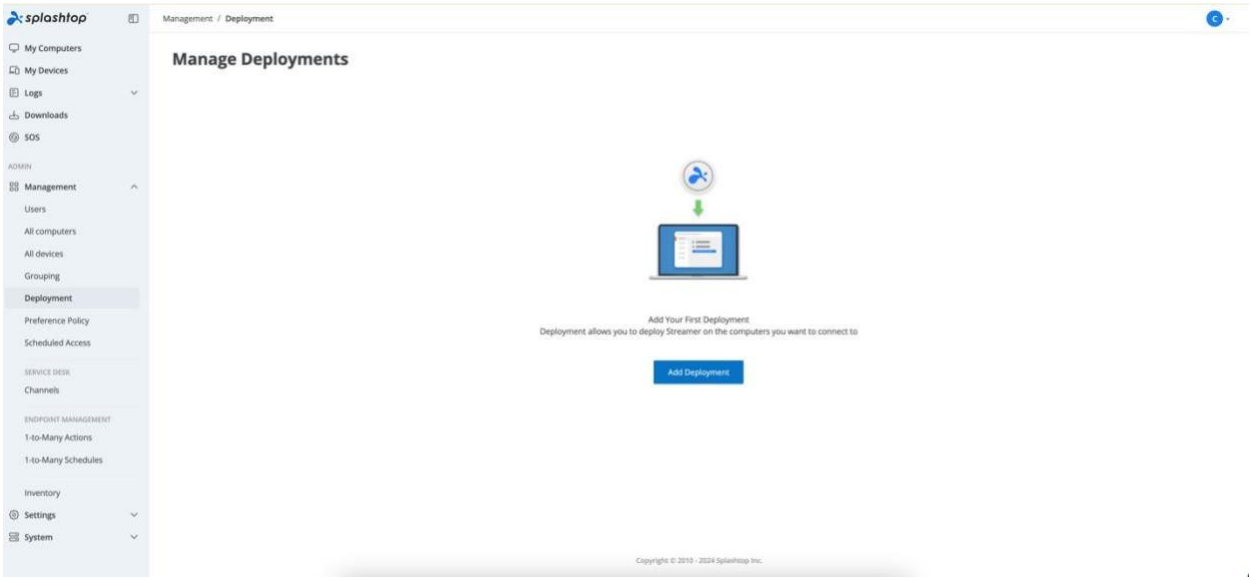


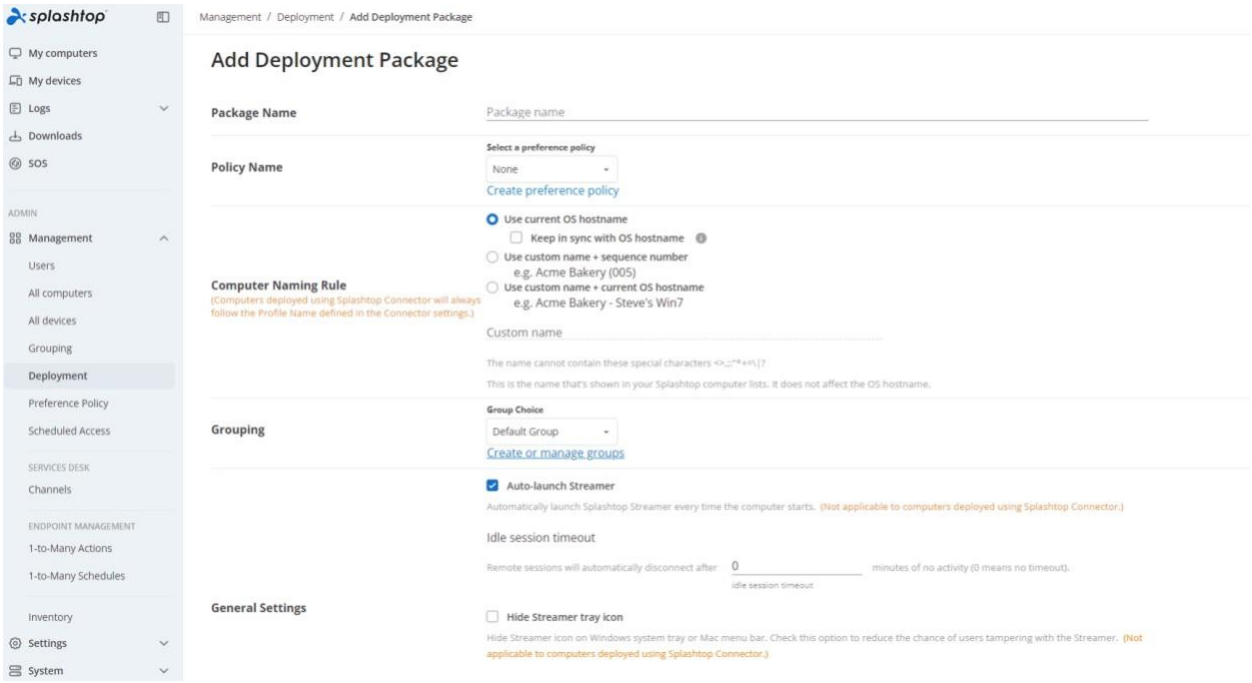
4. 部署 Splashtop Streamer

以下说明将以在 Windows 上部署 Splashtop Streamer 为例。

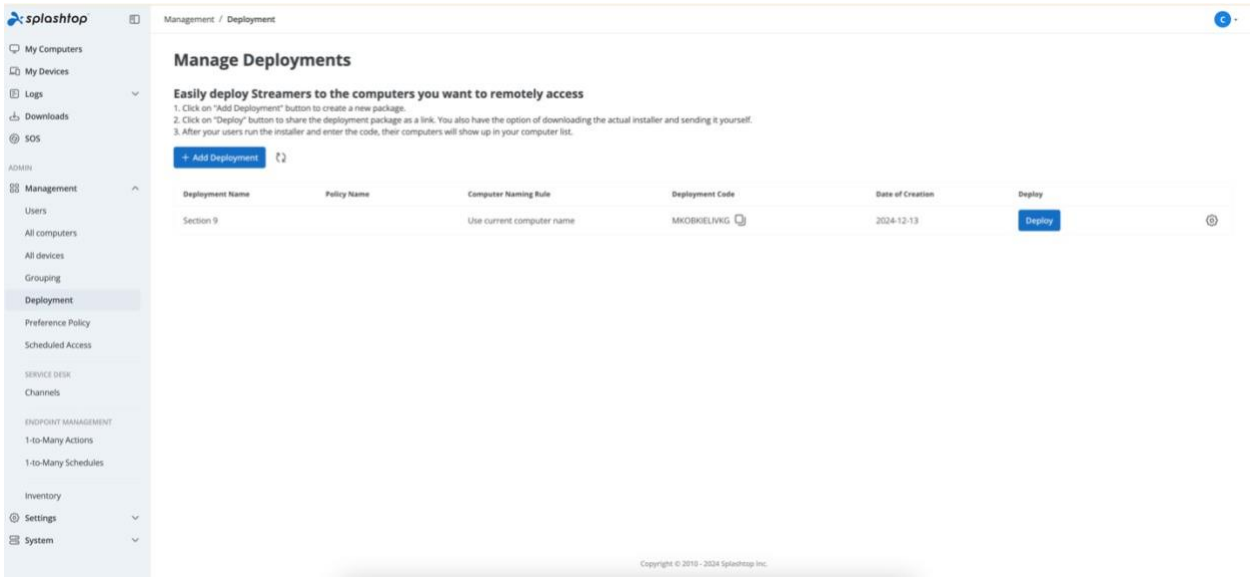
必须在要远程连接的电脑上安装 Splashtop Streamer。简单3步骤即可完成。

1. 打开 Splashtop Gateway 网络控制台 > 管理 > *部署*。单击***+添加部署***按钮创建新的部署套件。部署套件包括一个 Deployment Streamer 和唯一的12位部署码。

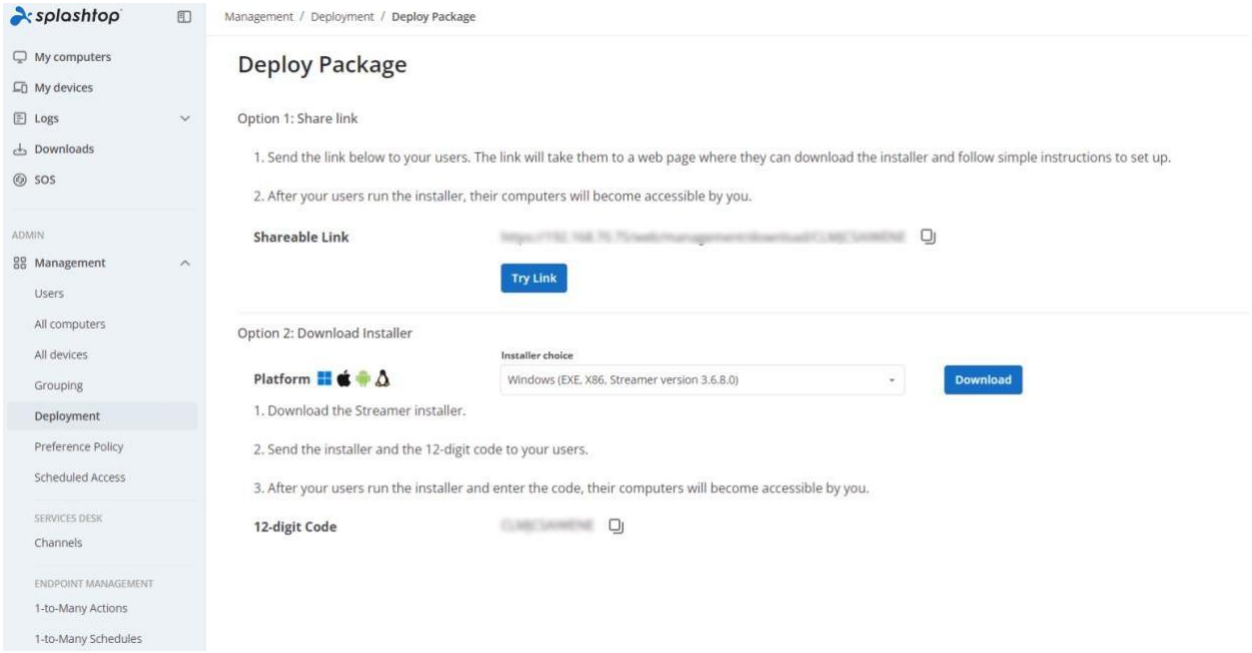




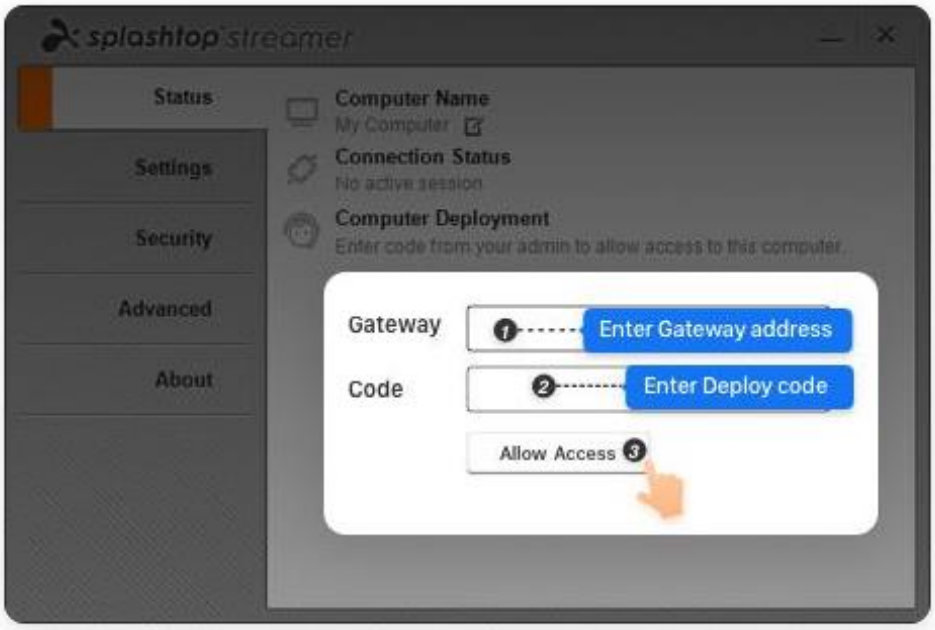
2. 为刚刚创建的部署套件选择***部署***。



3. **让用户安装 streamer。**可以将部署套件链接发送给用户。通过单击该链接，用户可以下载 streamer 安装程序并运行该文件。也可以将 Streamer 安装程序文件及其关联的部署码直接发送给用户，可使用 Dropbox、电子邮件等方式发送。



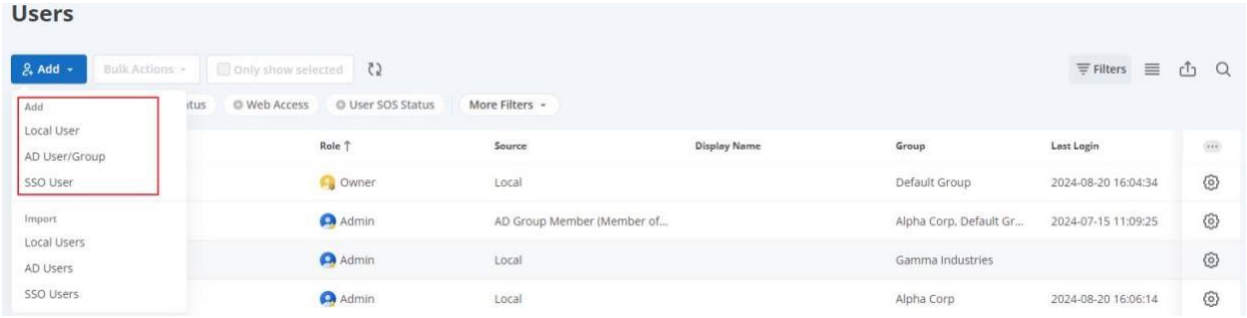
4. **Splashtop Streamer** 应用程序安装完成后，用户可以输入默认**端口号443**的 **Splashtop Gateway 服务器的 IP 地址**，以及从团队所有者或管理员处获得的部署码进行登录。未收到此信息的用户需联系 IT 部门。



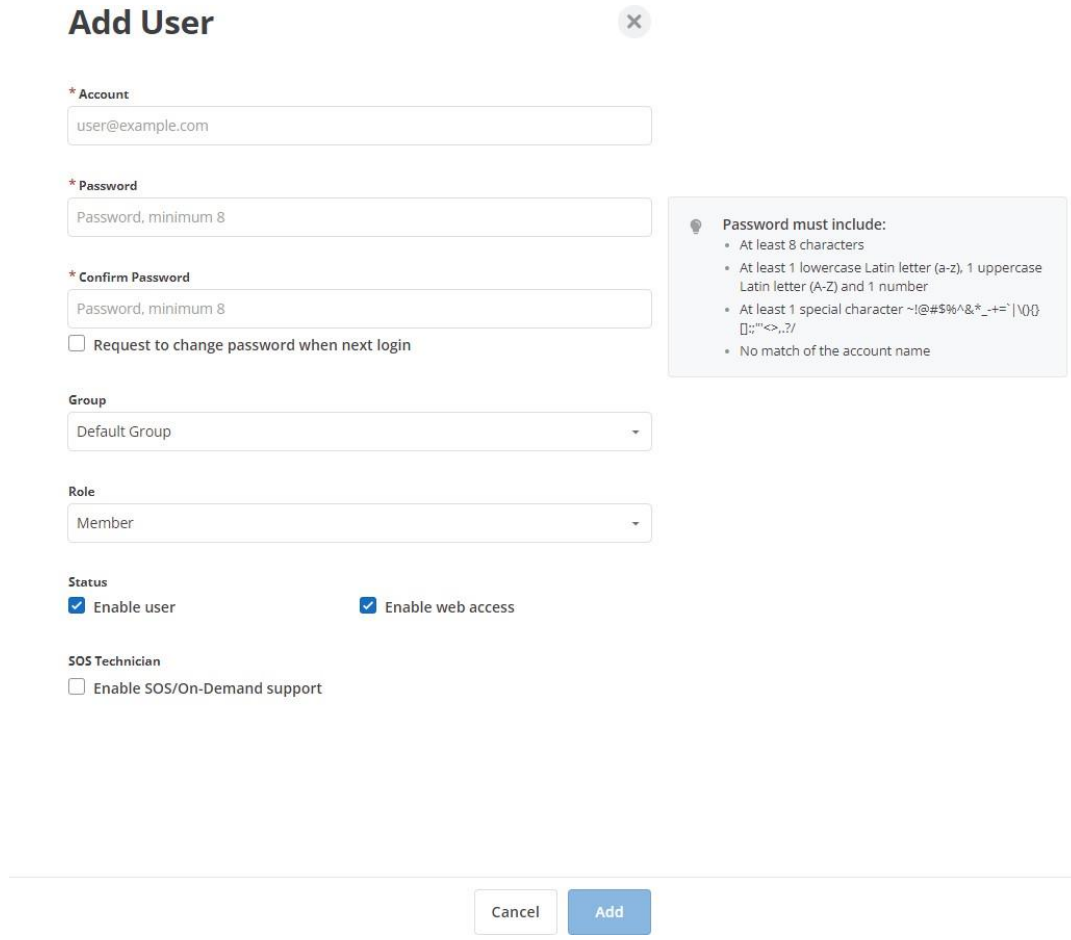
5. 创建用户账户

系统所有者或团队管理员可以创建用户，允许在 Splashtop Gateway 中集中管理用户。

1. 打开 Splashtop Gateway 网络控制台 > 管理 > 用户页面，点击**添加按钮**创建新用户。



2. 团队所有者或团队管理员在用户创建过程中设置用户角色和组类型。



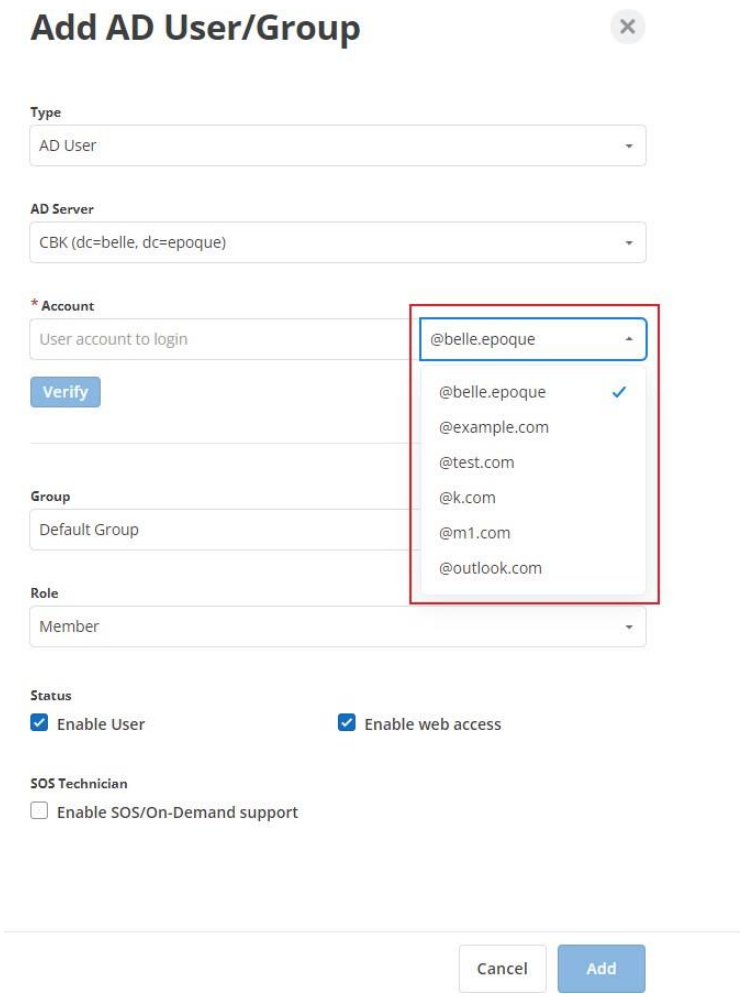
字段	含义
账户	这是用户的登录账户，是系统中是唯一的账户。
密码	复杂密码规则。
下次登录时请求更改密码	使用此选项，用户在登录系统时需要更改密码。
启用用户和 Web 访问	如果账户已启用，用户则可建立远程会话；如果账户被禁用，用户仍然可以访问 Web 门户，但远程会话被禁用。为特定账户禁用 Web 访问以限制其 Web 控制台访问功能，远程访问（远程会话）将不受影响。
分组	可将用户分到不同组中，分组功能可用于高效管理用户管理/访问权限。
角色	系统中有两种角色类型。
SOS 技术员*	如果订购内容包含 SOS 服务，则可在创建用户时启用 SOS 功能以获得按需支持。

3. 添加 AD 账户

AD 服务器成功通过身份验证后，可到系统-活动目录选项卡的 AD 服务器列表中查看。导航到管理选项卡 – 用户，单击顶部的“添加 AD 用户”按钮。

- **类型：通过选择 AD 用户，AD 个人用户将进行身份验证并添加到 Splashtop Gateway。选择 AD 组允许对 AD 组成员进行批量身份验证。（组成员必须先登录 Gateway Web 门户，然后将在用户列表显示）**
- **AD 服务器：选择包含目标 AD 用户或组的 AD 服务器。**
- **账户：填写目标 AD 用户或组的 sAMaccountName@ADDomainName（本地 AD 域名）或用户主体名称 （UPN）。**
- **组：选择 AD 用户或 AD 组添加后将自动归入的初始 Splashtop 组。**

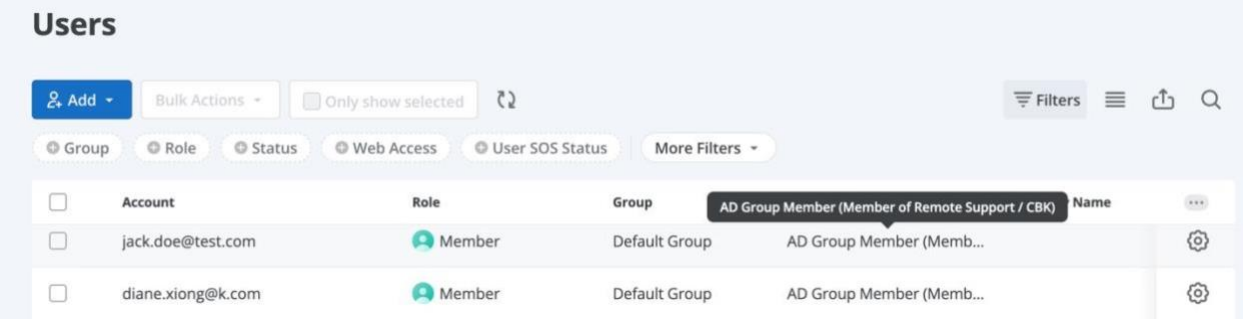
- 角色：选择管理员或成员以根据需要分配不同的访问权限。
- *SOS 技术员：启用 SOS 按需支持功能。（*基于订购方案）
- 验证：检查 AD 用户或组的可用性以进行身份验证。
- OK：将经过验证的 AD 用户或组添加到目标组。



4.添加 AD 组成员

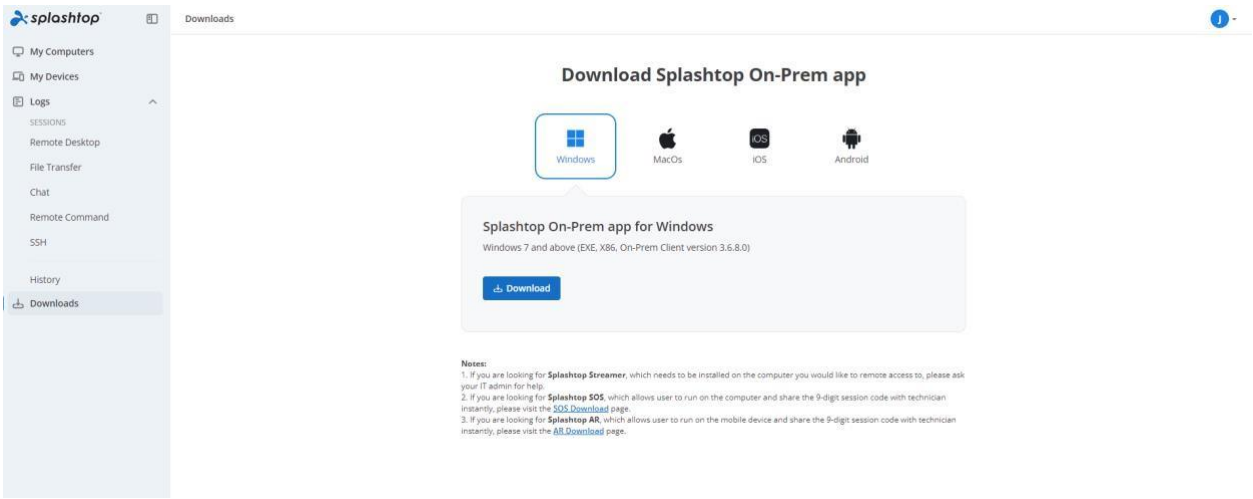
AD 账户可以根据用户列表的“来源”列来确定。如果已将 AD 组添加到 Splashtop Gateway，则表明与其关联的 AD 成员已经过身份验证，可以登录 Splashtop Gateway 以及 On-Prem 客户端应用程序。

AD 组成员中的 AD 用户将在使用其 AD 账户登录 Gateway 门户或客户端应用程序至少一次后在 AD 组成员中显示。而添加到 Gateway 的 AD 个人用户将立即显示并修改属性。

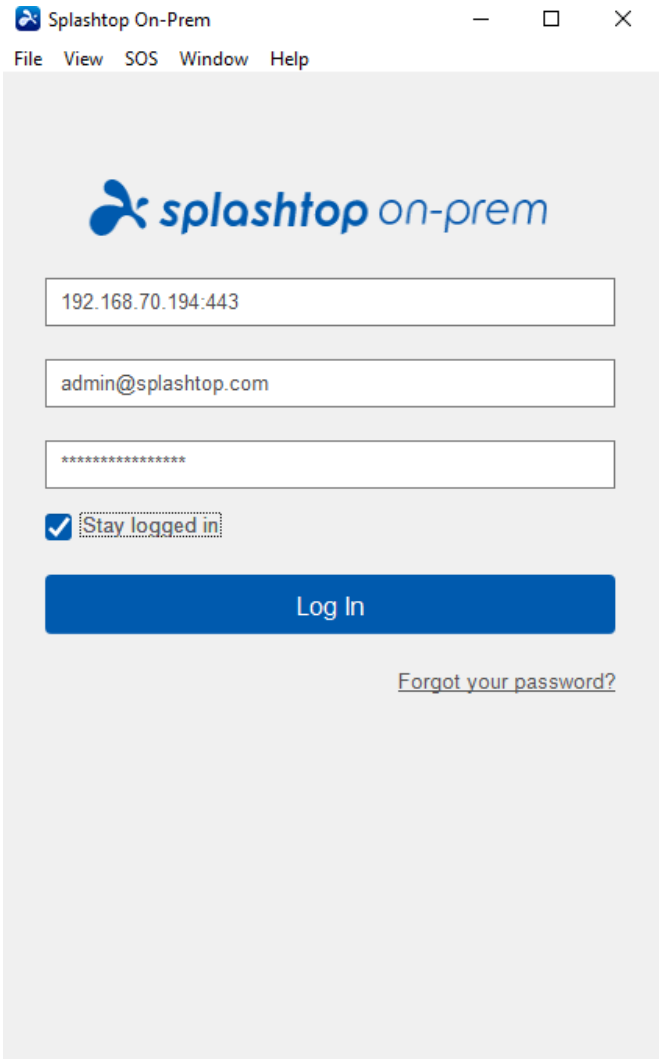


6. 安装客户端应用程序并访问

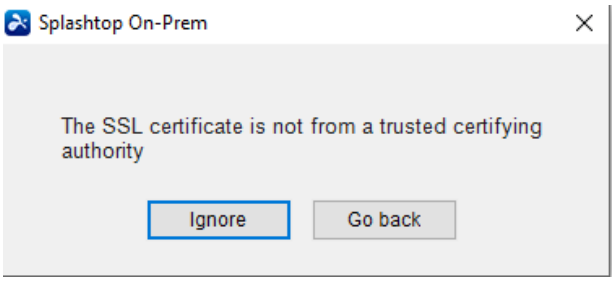
1. 与团队所有者或团队管理员相比，分配为成员的用户在登录 Splashtop Gateway 网络控制台时只能浏览有限的内容，如下图所示。成员可以登录 Splashtop Gateway 网络控制台，并通过“下载”菜单选项卡和“安装所需的客户端应用程序”下载最新的 Splashtop On-Prem 客户端。



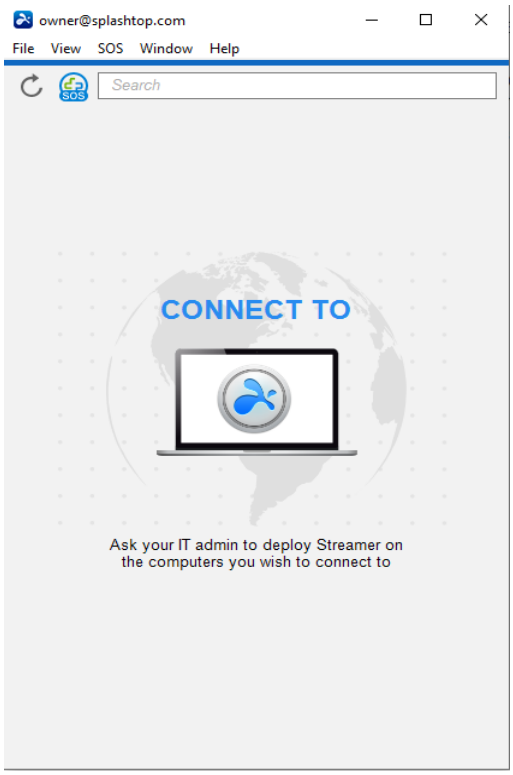
2. 安装 **Splashtop On-Prem 客户端应用程序**后，用户只需输入 Splashtop **Gateway 服务器的 IP 地址或 FQDN**（默认端口号**443**）以及从团队所有者或管理员处获取的账户名和密码即可登录。没有此类信息的用户需要咨询团队所有者或管理员。



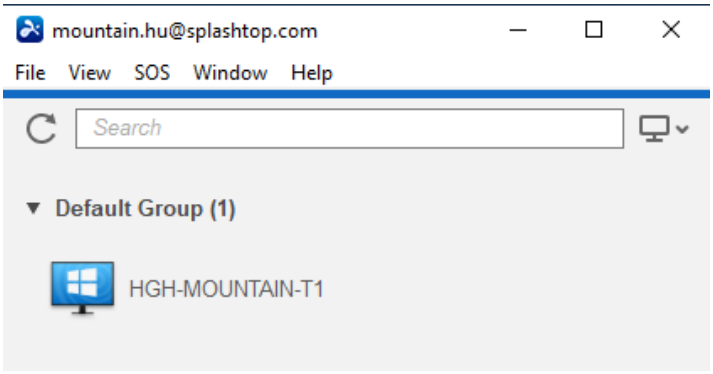
3. 如果在点击**登录**时弹出警告消息，显示 SSL 证书的认证机构不可信，则 SSL 证书可能是自行生成的，可以选择忽略。但是，我们建议弹出此消息的用户应咨询其 IT 部门，以遵守适当的准则。



4. 登录 On-Prem 应用程序后，将显示可连接的远程设备列表，或者将看到一个屏幕上没有列出任何特定电脑，如下所示。在这种情况下，请咨询您的团队所有者或管理员。



5. 下图表明已成功部署一台特定的 Windows PC，用户可以通过单击右侧的**连接**按钮或双击蓝色字段来远程访问此设备。



访问 Gateway 控制台

Splashtop Gateway 控制台是一个基于 Web 的控制台，用于配置和管理 Splashtop On-Prem 系统。可以从浏览器访问，建议使用基于 Chromium 的浏览器，例如 Google Chrome 。

Splashtop On-Prem 系统中的每个注册用户都有权访问 Gateway 控制台，但菜单显示将因用户分配的角色而不同。

配置项	团随所有者	团队管理员	成员
电脑	✓	✓	✓
设备	✓	✓	✓
日志	✓	✓	✓ (1)
管理	✓	✓	
SOS	✓	✓	✓ (2)
下载	✓	✓	✓
系统	✓		
用户配置文件	✓	✓	✓

注意：

(1) 成员仅可查看自己的日志

(2) 当在 SOS 页面上启用 SOS 功能时，用户则可看到 SOS 页面

通过打开 Web 浏览器并输入 Gateway 服务器地址，则可轻松访问 Gateway Web 门户。

地址格式定义如下：

https://(IP 地址或 FQDN):(端口号)

示例：https://192.168.1.100:443

示例地址指向 IP 地址为 192.168.1.100 的 Gateway 服务器，并且 Gateway 使用默认端口443。

注意：此处应始终使用 **https** 而不是 **http**，因为 **https** 是使用 SSL 加密的安全 **http** 连接。

服务器的 IP 地址

这是已安装 Splashtop Gateway 的服务器设备的 IP 地址。如果从位于同一局域网的电脑进行连接，则是本地 IP 地址；如果从 Internet 连接，则是公共 IP 地址。如果服务器设备有多个网卡，则可以使用任意 IP 地址访问 Gateway Web 门户。使用此功能可以在 DMZ 网络中安全部署 Gateway 服务器设备。

端口号

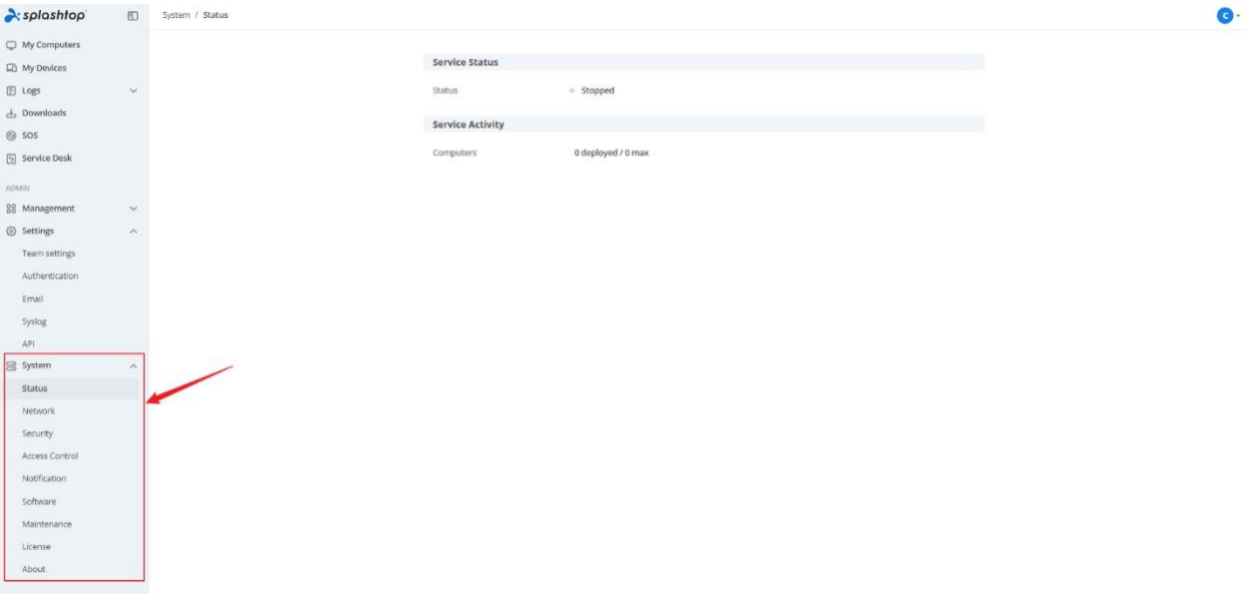
默认情况下，Splashtop On-Prem 使用端口号443，可以按照以下文章中的说明更改端口号：

系统配置

简介

Splashtop Gateway 的**系统**页面为**团队所有者**提供了配置系统设置的功能。

以团队所有者身份登录，可在顶部菜单栏找到**系统选项卡**，单击进入系统设置。



- **状态**显示 Splashtop Gateway 的当前状态
- **网络**显示 Splashtop Gateway 的网络配置
- **安全性**允许团队所有者配置安全相关设置，例如 SSL 证书、TLS 设置
- **访问控制**允许团队所有者配置访问策略，例如网络控制台、Splashtop On-Prem 客户端
- **通知**允许团队所有者设置 通知以通知用户，例如计划系统维护
- **软件**允许团队所有者配置软件组件，例如启用/禁用特定版本的 Splashtop Streamer 和 Splashtop On-Prem、上传新版本的组件

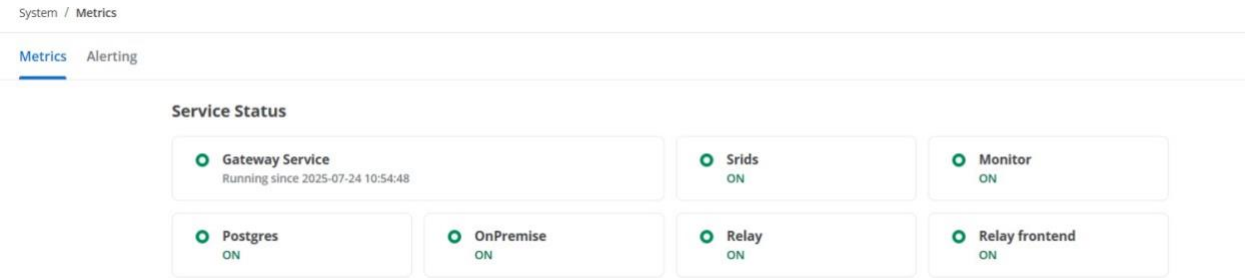
- **维护**允许团队所有者进行系统维护，例如备份和恢复
- **许可证**允许团队所有者配置许可证，例如导入/更新许可证
- **关于**显示版本、版权、服务条款、隐私和致谢

状态

指标-查看系统性能

服务状态

监控关键 Gateway 相关服务是否按预期运行。



以下是 Splashtop On-Prem Gateway 中每个服务的简要说明。

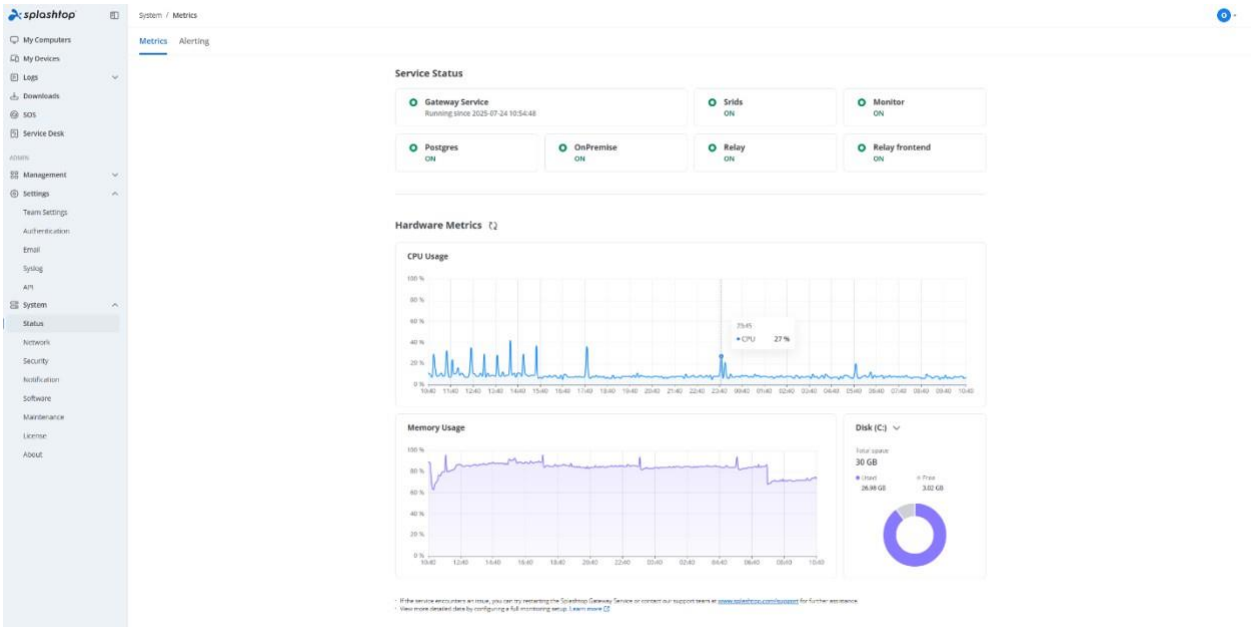
- Gateway 服务：托管和管理所有核心 Splashtop On-Prem 组件的主要 Windows 服务。
- Postgre：提供存储所有服务的配置和运行时数据的核心数据库。
- OnPremise：处理业务逻辑、身份验证请求并与数据库通信的 API 服务。
- 中继：处理远程会话期间的安全数据传输。
- 中继前端：充当中继连接的入口点，并将流量调度到后端中继实例。
- Srids：管理远程会话的唯一标识符，跟踪会话生命周期和元数据，并促进系统内的会话路由和审计。
- 监控：监控系统组件的健康状况和性能，收集 CPU 使用率、内存消耗、磁盘空间和服务状态等指标， 并对异常情况生成警报，以确保系统可靠性并及时解决问题。请完成警报配置以激活此服务。

硬件指标

硬件指标提供对系统当前健康状况的直观概览。具体包括：

- CPU 使用率：跟踪整个系统的实时 CPU 使用情况。
- 内存使用率：查看内存消耗以检测潜在的瓶颈。
- 磁盘空间：监控可用磁盘空间和使用趋势。

以上所有指标都使用直观的图形和图表显示，以实时清晰查看系统性能。

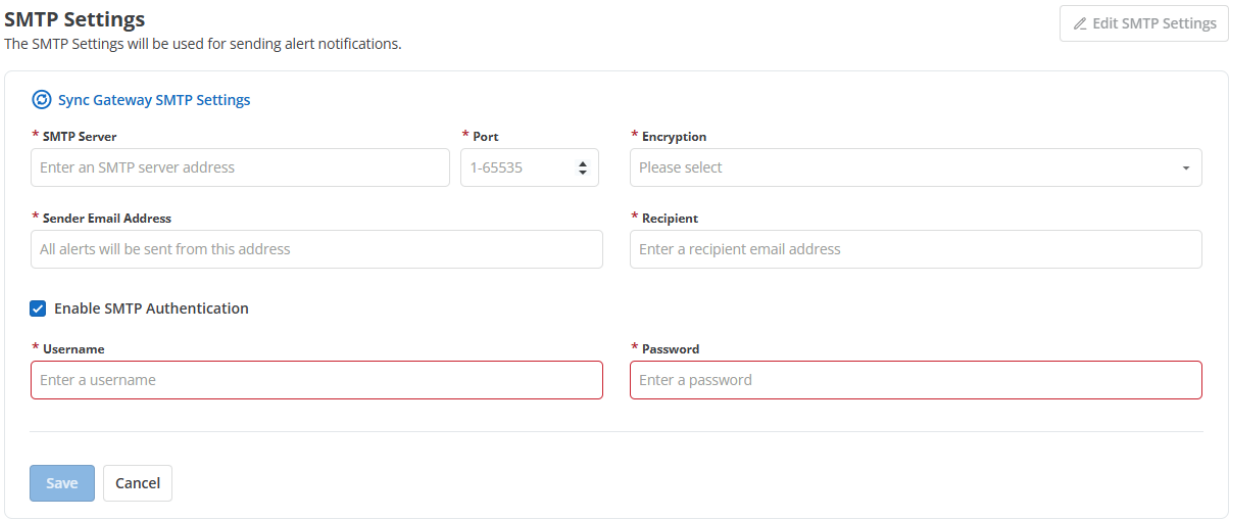


警报 - 随时关注以防止问题升级

通过警报功能可以设置自动通知，以随时了解关键系统事件。

SMTP 设置

配置 SMTP 服务器以启用基于电子邮件的警报通知。



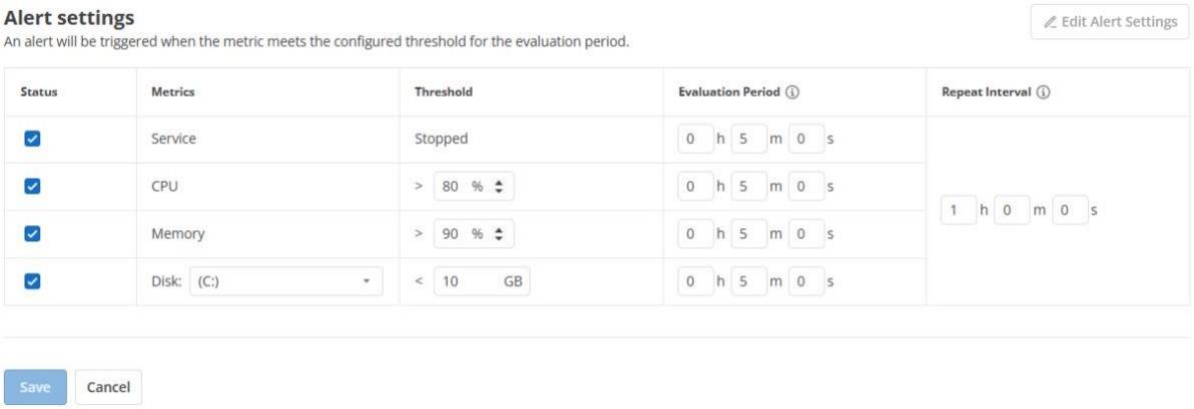
- SMTP 服务器：输入用于发送电子邮件的 SMTP 服务器的地址。
- 端口：指定 SMTP 服务器使用的端口号（通常为25、465或587）。
- 加密：选择加密方法以确保电子邮件传输的安全。
- 发件人电子邮件地址：显示为警报消息发件人的电子邮件地址。
- 收件人：接收警报通知的电子邮件地址。
- 启用 SMTP 身份验证：选中此选项则 SMTP 服务器需要登录凭据才能发送电子邮件。
  - 用户名：输入 SMTP 身份验证的用户名。
  - 密码：输入 SMTP 身份验证的密码。
- 同步 Gateway SMTP 设置：点击以从 Gateway 中的 Web/管理/电子邮件自动导入 SMTP 设置。

警报设置

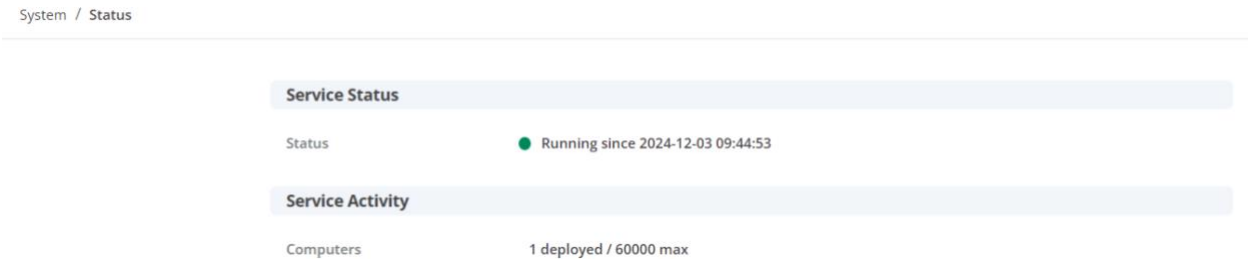
定义触发警报的具体条件。可配置警报包括：

- 服务状态发生变化（例如，服务意外停止）
- CPU 使用率高
- 内存使用率高
- 磁盘空间不足

根据配置立即发送警报，以实现快速响应并最大限度地减少停机时间。



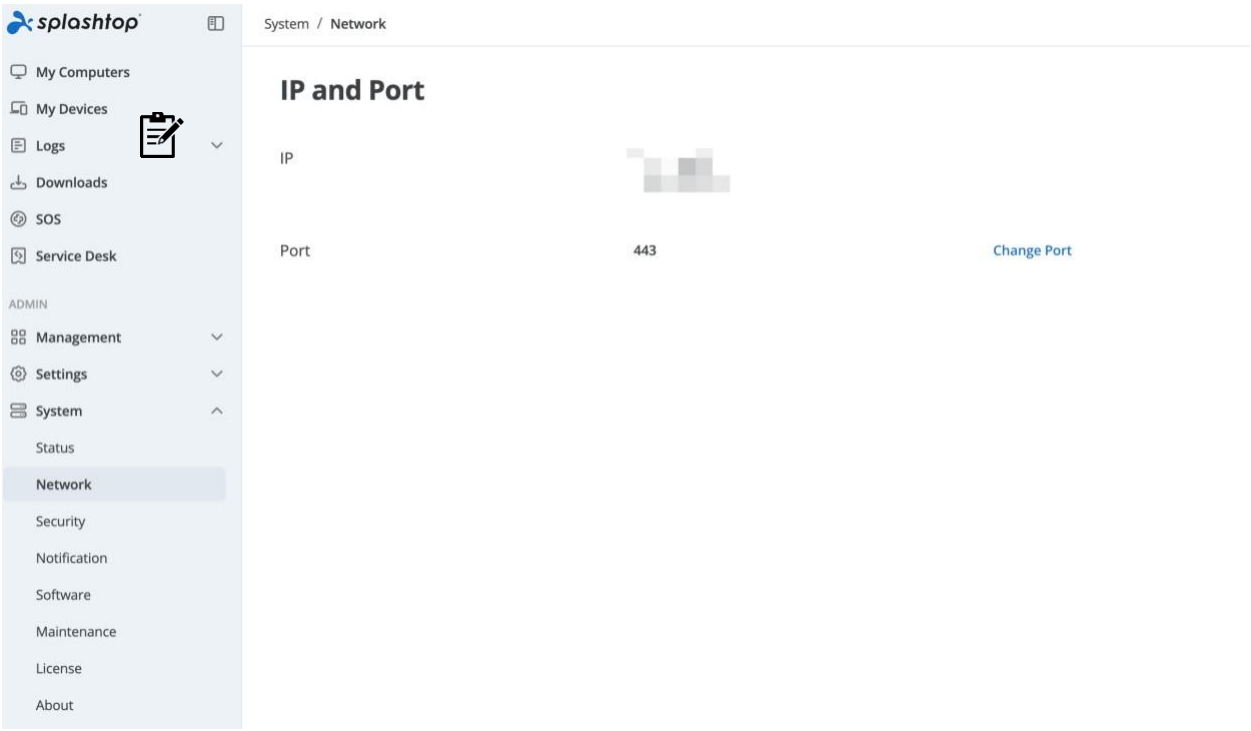
- 状态：选中此选项则可启用特定警报。
- 指标：具体的监控项，比如 CPU 使用率、内存使用率、磁盘空间等。
- 阈值：指标触发警报的具体值（例如，CPU 使用率 > 90%）。
- 评估周期：评估指标以确定其是否达到或超过阈值的时间窗口。
- 重复间隔：针对同一情况重复发出警报通知的最短时间。



网络

更改网络端口

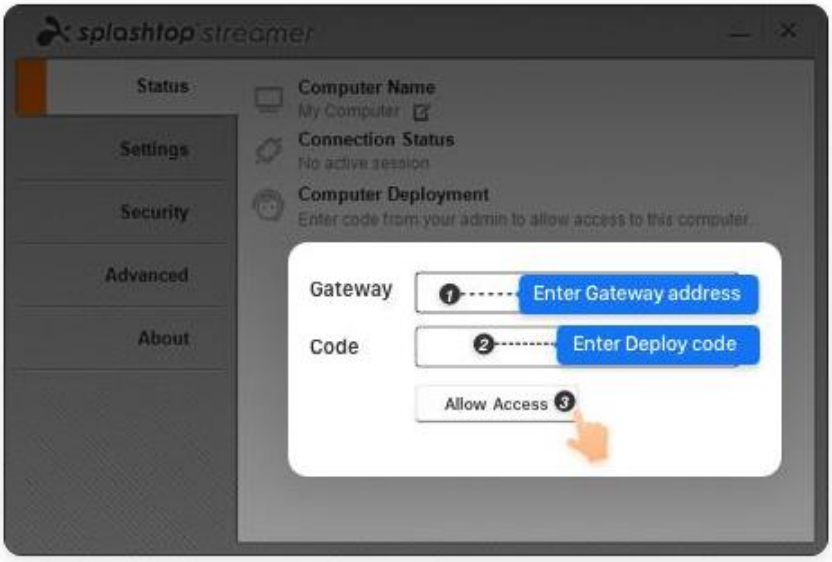
使用团队所有者身份登录 Gateway 的管理控制台，转到**系统>网络**，**端口**部分显示 Gateway 当前服务的端口，单击**更改端口**将允许用户输入新端口并应用。



注意：

1. 更改端口将自动重启 Gateway 服务，大约需要30秒才能再次准备就绪。

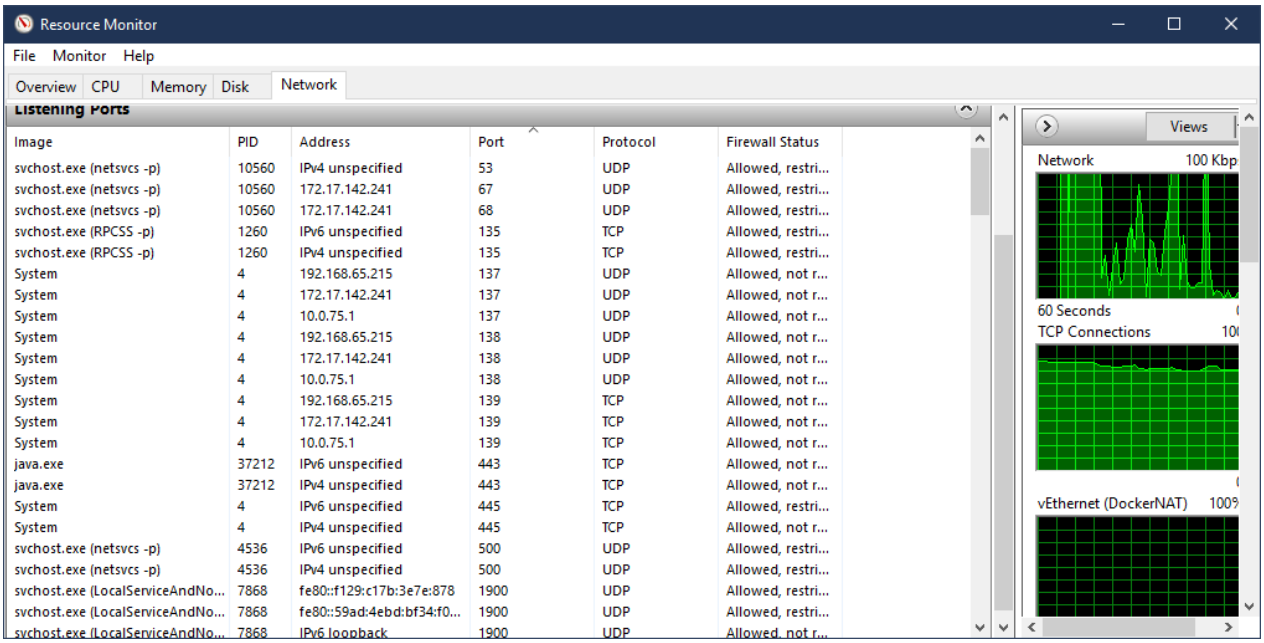
2. 已部署的 Streamer 或登录 On-Prem 应用程序将被注销，由于端口更改，需要在 Streamer 和 On-Prem 应用程序端指定正确的 *IP：Port* 才能再次登录 Gateway。443是默认端口，输入时可忽略。



（部署时在 **Gateway** 字段中输入 *IP：Port*）

（登录时在 **Gateway** 字段中输入 *IP：Port*）

3. 作为一种通用做法，我们建议 IT 管理员要确保要更改的端口**未被占用**，可以使用 Windows 内置的 **resmon** 实用程序进行检查。在 Windows 搜索框输入 resmon，运行**resmon** 工具，打开**网络**选项卡，展开**监听端口**，并检查所选端口上没有其他软件监听。



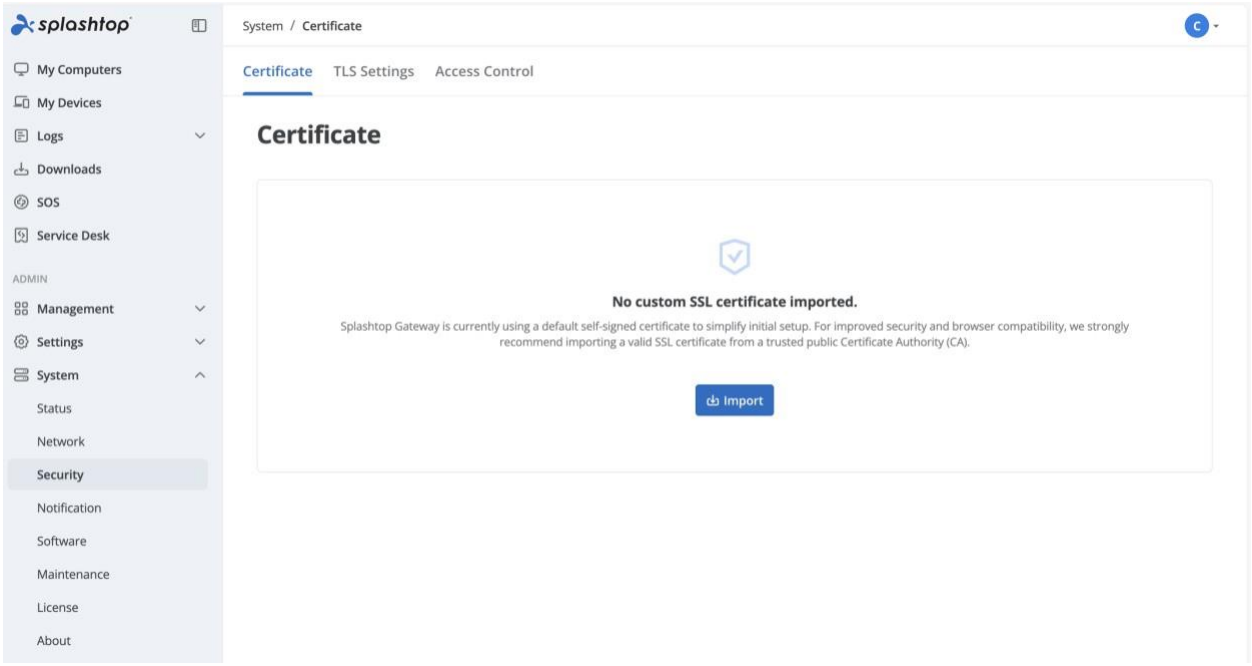
安全

导入 SSL 证书

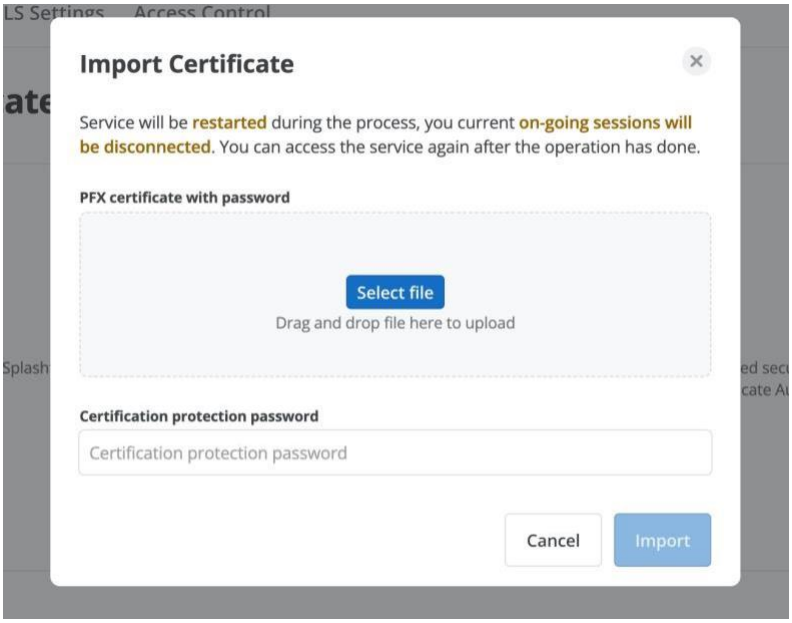
Splashtop Gateway 支持导入您自己的证书，可以是自签名证书，也可以是第三方机构颁发的证书。

Gateway 支持 **PKCS#12 (PFX)** 格式的证书。

步骤 1：要导入新证书，请以团队所有者身份登录 Gateway 的管理控制台，然后打开**系统** > **安全**页面。如果没有证书信息，则显示当前导入的证书信息；也就是说，Gateway 正在使用 Gateway 绑定的自签名证书。



步骤 2：单击**导入**，将显示导入对话框，选择 PFX 文件以及生成证书时设置的密码。



步骤 3：单击导入以完成导入，此操作将重启 Gateway 服务以使新证书生效。

将 SSL 证书转换为 PFX 格式

Windows 设备：

1. 单击**开始**，然后单击**运行**。输入 **MMC.exe**，单击**确定**。单击**文件**，然后单击**添加/删除管理单元**。
2. 单击**添加**。突出显示“证书”，然后再次单击**添加**。
3. 选择**电脑账户**，然后单击**下一步**。选择**本地电脑**，然后选择**确定**。单击**关闭**，然后单击**确定**关闭“管理单元”窗口。
4. 打开创建的**证书**（本地电脑）管理单元。打开**个人**，然后打开**证书**。
5. 右键单击要转换的服务器证书，选择**所有任务**，然后选择**导出**。
6. 在打开的向导上单击**下一步**。如果向导没有打开，请重复步骤5。如果仍然打不开，请重启电脑并返回步骤4。
7. 选择**私钥**以导出，然后单击**下一步**。
8. 选择个人信息交换 （PFX） 文件格式以创建 PFX 文件。
9. 单击**下一步**并选择文件的密码。 再次单击**下一步**。
10. 选择文件名。无需输入扩展名，因为向导会自动添加 PFX 扩展名。
11. 单击**下一步**，记住文件的保存位置，然后单击**完成**。

其他方法（以 OpenSSL 命令行和 GoDaddy 签名的证书为例）：

http://support.godaddy.com/help/article/5343/generating-a-certificate-signing-request

我们通过 OpenSSL 命令提示符生成 CSR：
http://support.godaddy.com/help/article/5269/generating-a-certificate-signing-request-csr- apache-2x
>openssl req-new-newkey rsa：2048-nodes-keyout yourdomain.key-out yourdomain.csr

请前往此网站以获取命令示例：http://www.sslshopper.com/article-most- common-openssl-commands.html

1. 将私钥、证书和 Godaddy 证书打包后转换成.PEM 文件
2. 将私钥、证书和 Godaddy 证书并置为一个单独的.PEM 文件
3. 将最终的.PEM 文件转换为.pfx 文件

要求：

创建 PFX 时，必须具备中间/中间层 CA 证书。如果 PFX 不包含直接颁发者的 CA，便携式操作系统将会出现问题。

openssl 命令行：

openssl pkcs12-export-out output.pfx-inkey private.key-in star-splashtop.com.crt-certfile int.cer
Openssl 将提示 IT 输入密码以保护输出的 PFX 文件。
Output.pfx：输出文件名。
Private.key：证书的私钥。

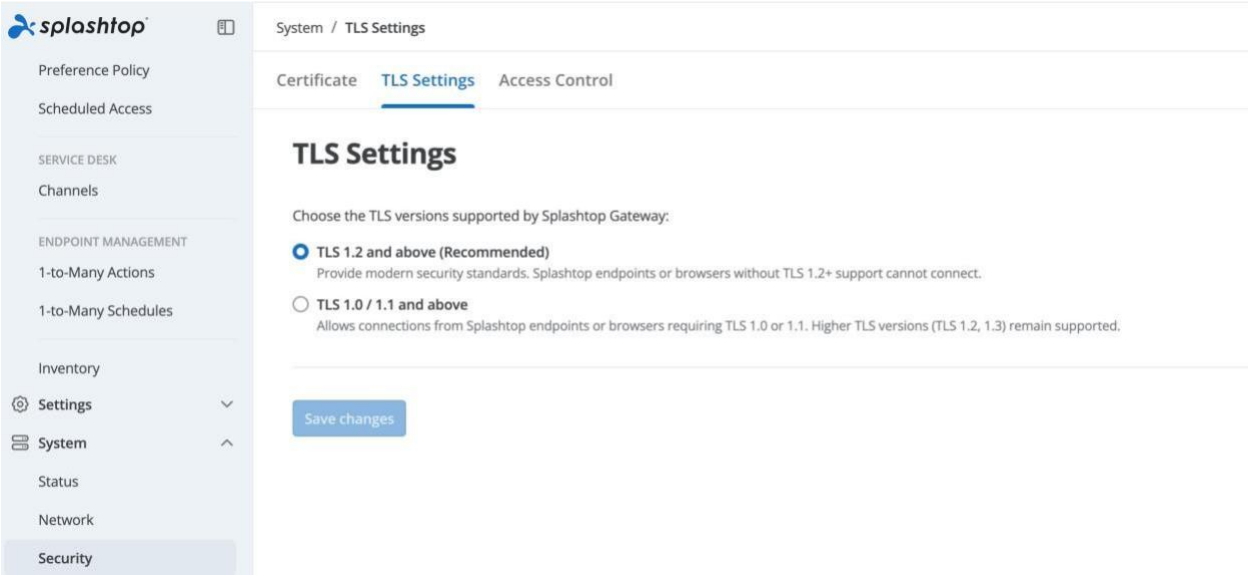
Star-splashtop.com.crt：由第三方 CA 提供的本站签名

Int.cer：第三方 CA 证书

TLS 设置

Splashtop Gateway 允许团队所有者配置客户端和浏览器连接支持的 TLS 版本。可根据安全要求和兼容性需求选择不同选项。

以团队所有者身份登录 Gateway 管理控制台，打开**系统 > 安全 > TLS 设置**。



选项 1：TLS 1.2及以上版本（推荐）

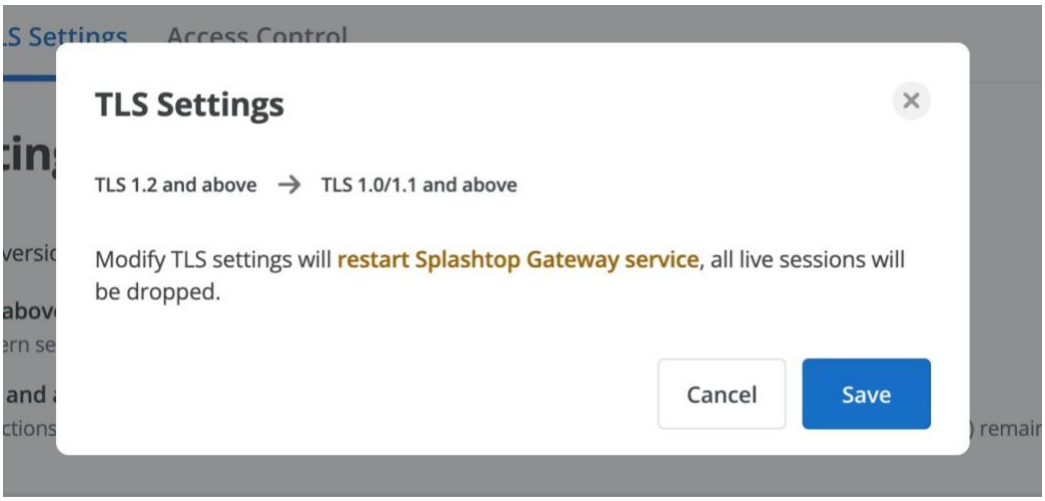
- 提供现代安全标准。
- 确保符合当前的行业和监管要求。
- 只有支持TLS 1.2或更高版本的端点或浏览器才能连接。
- 建议用于优先考虑安全性的大多数部署场景。

选项 2：TLS 1.0/1.1及以上版本

- 允许连接支持 TLS 1.0或1.1的较旧 Splashtop 端点或浏览器。
- 保持与遗留环境的向后兼容性。
- 仍支持更高的 TLS 版本（1.2和1.3），但此选项没有实施 TLS 1.2+ 安全。

应用更改

- 在切换选项并单击**保存更改**时，Splashtop Gateway 服务将重启，所有活动会话都将断开连接。



禁用 TLS 1.1和1.0后，需要在 Windows 7 和 Server 2008 上进行一些系统调整，因为这些作系统版本的默认设置是 TLS 1.0。操作说明：

1. 获取 Windows 更新以支持 TLS 1.2

请参阅此文 https://support.microsoft.com/en-us/help/3140245/ 以获取支持 TLS 1.2 的更新。

2. 注册 TLS 1.2

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Prot ocols\TLS 1.2\Client]
"Enabled"=dword:ffffffff
"DisabledByDefault"=dword:00000000

[HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Prot ocols\TLS 1.2\Server]
"Enabled"=dword:ffffffff
"DisabledByDefault"=dword:00000000

3. 将 TLS 1.1配置为默认用于 WinHTTP

对于32位 Windows 7/Server 2008

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp]
"DefaultSecureProtocols"=dword:00000200

对于64位 Windows 7/Server 2008

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp]
"DefaultSecureProtocols"=dword:00000200

4. **将 TLS 1.2 配置为默认用于 WinHTTP**

对于32位 Windows 7/Server 2008

[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\WinHttp]
"DefaultSecureProtocols"=dword:00000800

对于64位 Windows 7/Server 2008

[HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Interne t Settings\WinHttp]
"DefaultSecureProtocols"=dword:00000800

注意：

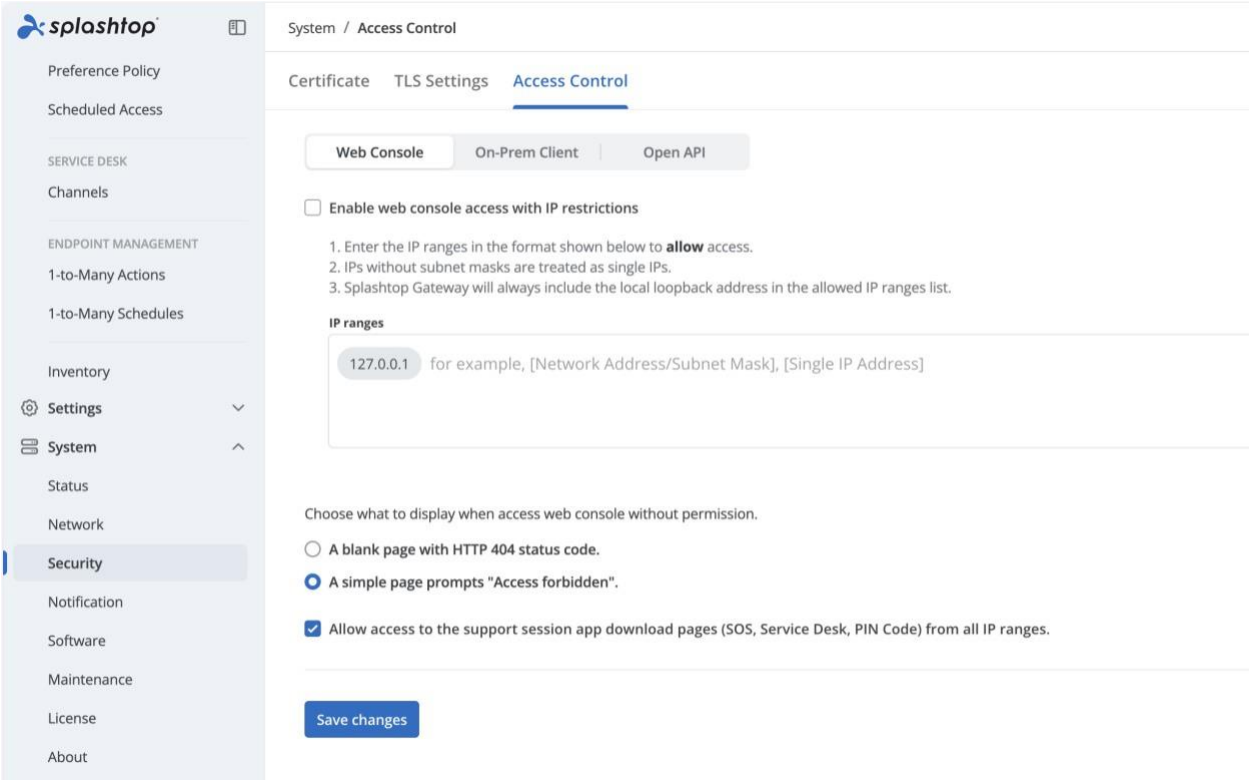
1. Windows XP 默认将 SSL v3 用于 WinHTTP。Windows 8或更高版本默认将 TLS 1.1 用于 WinHTTP。

2. 如未显示，请添加密钥：TLS 1.2\Server, TLS 1.2\Client

参考文章： Microsoft 支持

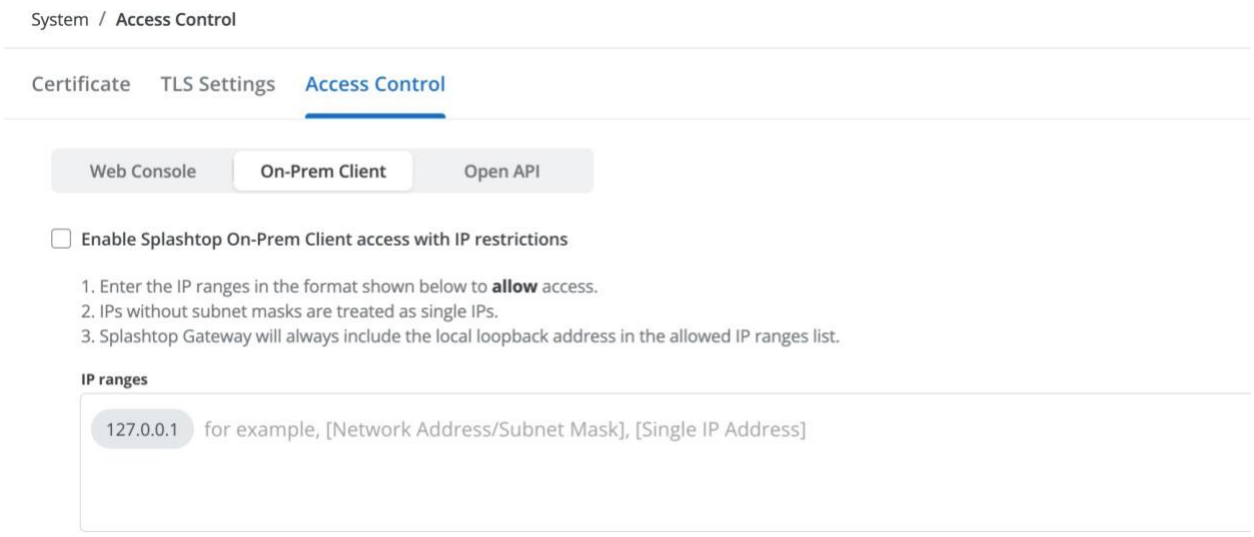
访问控制

访问控制页面允许团队所有者管理 Gateway 网络控制台、On-Prem 客户端应用程序和具有 IP 限制的 Open API 的访问。



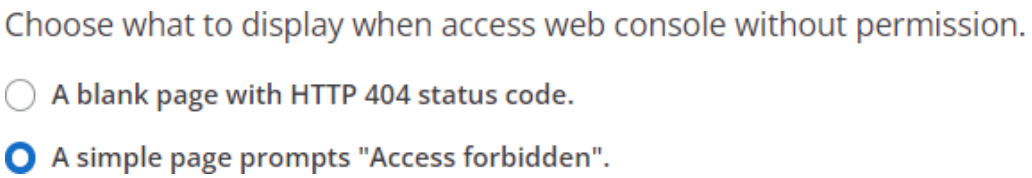
步骤 1

以所有者身份登录 Gateway 管理控制台，打开系统 > 安全 > 访问控制。Splashtop 目前支持在访问 Gateway 网络控制台、本地客户端应用程序或 Open API 时进行 IP 限制。
将允许的 IP 地址填入 IP 范围列表。IP 语法应采用 CIDR 或单个 IP 地址格式。



步骤 2

此外，所有者可以为 Web 控制台访问被拒绝选择不同的显示方法。



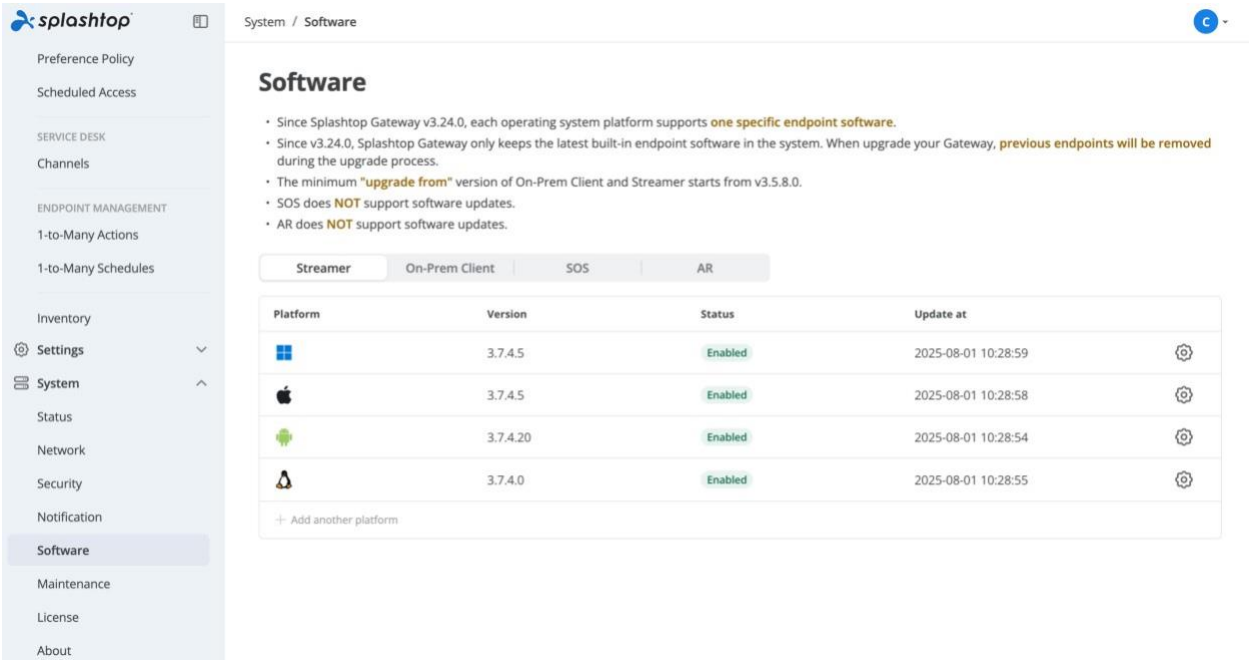
步骤 3

为 Splashtop On-Prem 客户端或 Web 控制台启用 IP 访问限制，以便阻止从列表中排除的 IP 源生成的访问。

点击保存按钮保存设置并打开该功能。

软件

Gateway 的**系统 > 软件**页面中的软件组件页面允许团队所有者管理软件组件。



团队所有者可以配置以下软件组件：

- **Splashtop Streamer**：需要在被访问的远程设备上安装并运行的软件。将音频和视频流式传输到客户端设备。
- **Splashtop On-Prem 客户端应用程序**：可以在本地设备和运行 Splashtop Streamer 或 Splashtop SOS 的目标远程设备之间建立远程会话的软件。
- **SOS**：在用户希望获得按需支持的目标设备上运行的软件，将显示9位会话码，允许技术员远程获得支持。
- **AR：一款创新应用，可为远程团队提供无缝的增强现实协作和支持。**

团队所有者可以在此页面中执行以下操作：

- 导入新版本的软件组件
- 将软件组件设置为已启用/禁用
- 删除软件组件
- 自定义软件组件

软件更新

1. 简介

Splahtop Gateway（v3.24.0 或更高版本）服务器启动的更新涉及加载了最新 Splashtop 端点软件的内置更新存储库，并根据自定义计划控制软件更新到客户端设备（Windows、Mac 和 Linux）的分发和部署。此架构有助于集中管理和部署更新，提供灵活的控制并提高安全性，以满足您的特殊维护需求。

2. 要求

- *Splashtop Gateway* **v3.24.0** 或更高版本
- Splashtop Streamer 和 *On-Prem* 客户端应用程序 **v3.5.8.3** 或更高版本。
  - ✧ v3.5.8.3是打包到 Gateway v3.24.0 中的 Windows 和 Mac 端点的默认版本
  - ✧ v3.5.8.3是支持升级的最低版本。端点软件版本低于3.5.8.3的不支持升级。

重要说明：升级 Gateway 行为更改

1. Splahtop Gateway 升级到 v3.24.0 后，将删除所有**低于 v3.5.8.3 的客户端应用程序/Streamer 版本，并将其替换为 v3.5.8.3。**服务器将仅维护给定版本的最新软件套件。

例如，在将 Gateway 从 v3.20.x 升级到 v3.24.0 后，Gateway v3.20.x 中打包的 v3.5.2.x 将被 v3.24.0 中的 v3.5.8.x 替换。

以下是 Splashtop Gateway 最新的4个主要版本中的默认端点版本。

Gateway v3.16.x -> 默认端点 v3.4.8.x

Gateway v3.18.x->默认端点 v3.5.0.x

Gateway v3.20.x->默认端点 v3.5.2.x

Gateway v3.24.x->默认端点v3.5.8.x

Gateway v3.26.x->默认端点v3.5.8.x

Gateway v3.28.x->默认端点v3.6.8.x

Gateway v3.32.x->默认端点v3.7.2.x

2. 备份 Splashtop Gateway v3.24.0 时，端点将不再包含在备份文件中。随着 Splahtop 不断推出新的兼容平台以改善跨平台体验，维护过程不应受到不断增长的安装包体积的影响。

3. 端点软件功能范围

Splashtop On-Prem 客户端

平台	支持版本
Windows	v3.5.8.3 （支持手动或自动检查更新）
macOS	v3.5.8.3 （支持手动或自动检查更新）
Android	不支持。（从 Google Play 获取新应用）
iOS	不支持。（从 App Store 获取新应用）
Linux	不支持。

Splashtop Streamer

平台	支持版本
Windows	v3.5.8.3 （支持静默更新和检查更新）
macOS	v3.5.8.3 （支持静默更新和检查更新）
Android	不支持。（从 Google Play 获取新应用）
Linux	v3.5.8.3 （支持静默更新和检查更新）

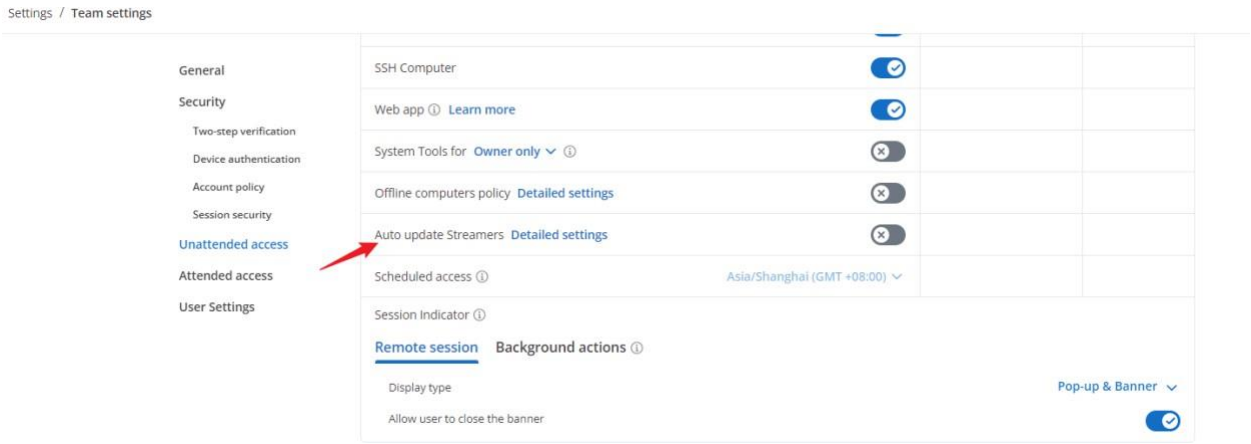
** Splashtop SOS 和 AR 不支持 Splashtop Gateway 的更新。*

4. 更新管理

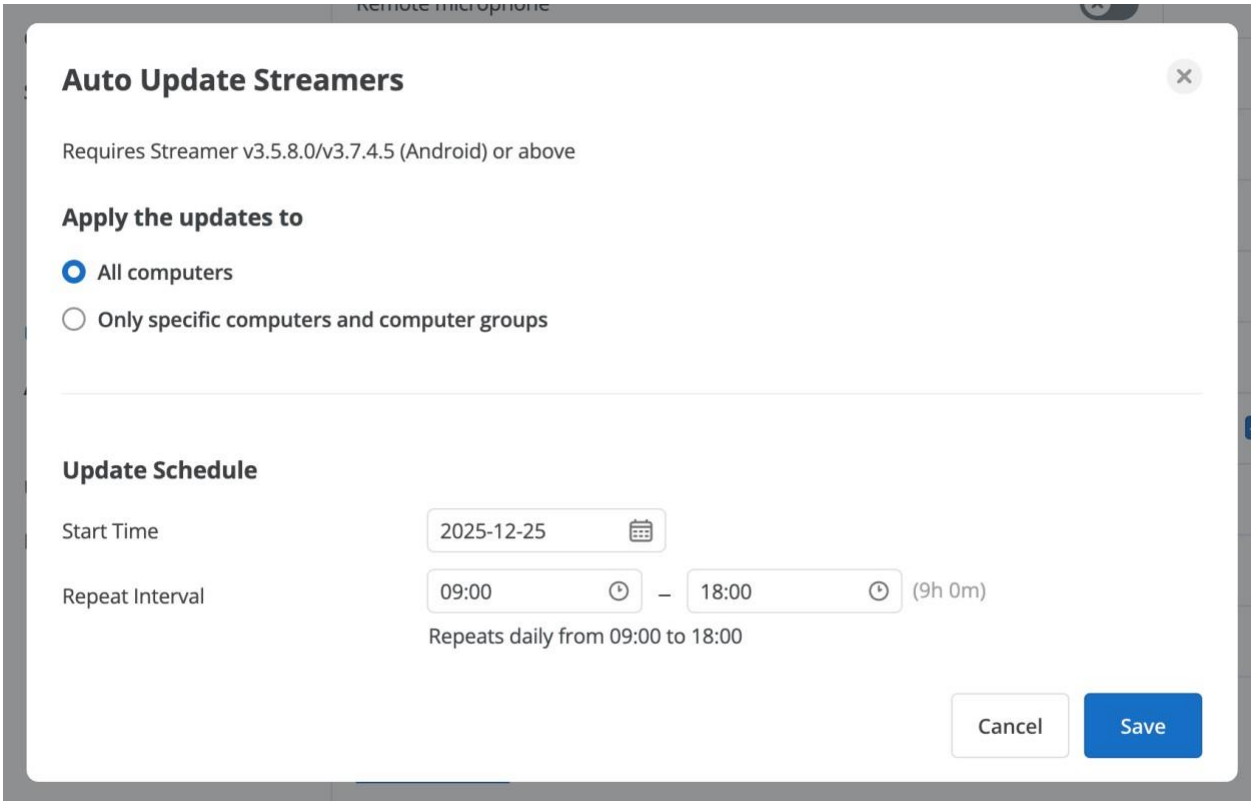
自动更新

在无人值守的情况下，可以从 Splashtop Gateway 网络控制台管理 Streamer 自动更新。

1. 以所有者身份登录，导航到设置 > 团队设置



2. 在无人值守访问部分，找到自动更新 Streamer，打开详细设置。



3. 阶段化更新和全面更新

将更新应用到 - 所有电脑

- 如果计划一次性升级所有已部署的 Streamer，请选择此选项。

将更新应用于 - 仅特定电脑和电脑组

- 选择此选项，则可通过将升级范围限定为选定的电脑组来验证公司环境中 Streamer 升级的功能。

我们强烈建议所有用户采用阶段化更新，先进行部分更新，再将更新应用于所有电脑，尤其已部署大量 Streamer 的情况。

4. 更新计划

开始时间

- 合理安排更新启动时间。注意没有结束时间，也就是说一旦启动更新，更新事件将一直进行（如果检测到较低版本）。

重复间隔

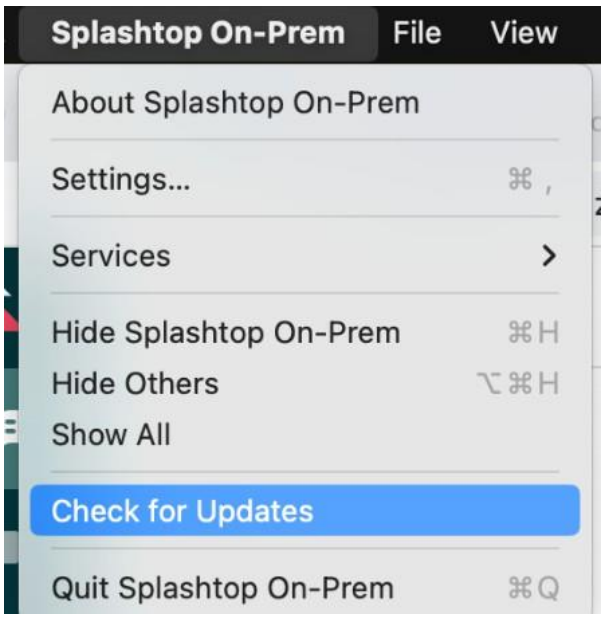
- 确定更新间隔。不存在超出计划间隔的更新事件。建议将更新间隔安排在非工作时间。

手动更新

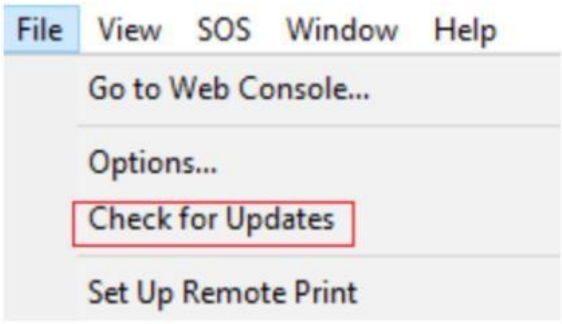
1. Splashtop On-Prem Client 应用程序

登录到客户端应用程序

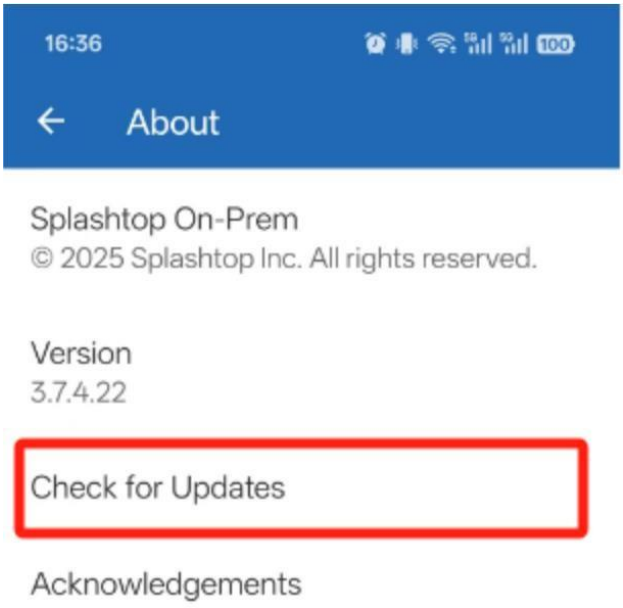
Mac：Splahtop On-Prem > 检查更新



Windows：文件 > 检查更新

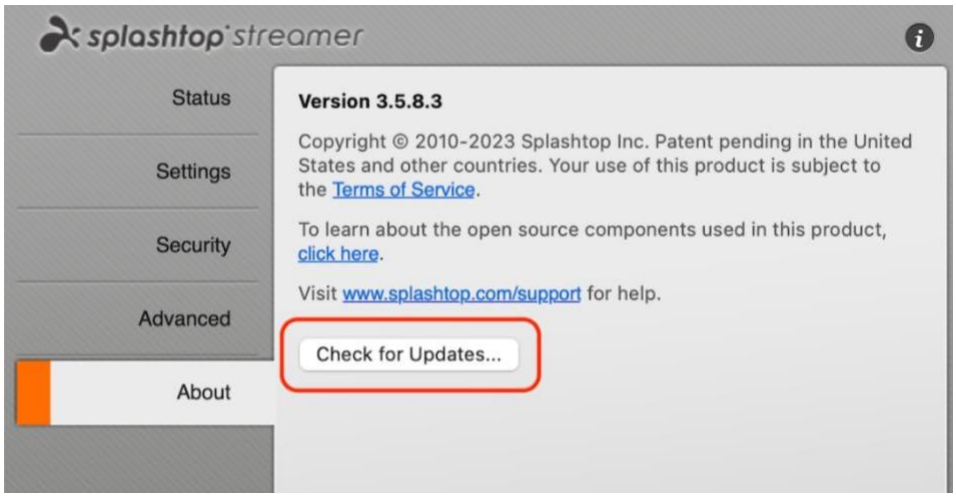


Windows：设置 > 关于 > 检查更新



注意：客户端应用程序只能通过检查更新手动更新。

2. Splashtop Streamer：关于 > 检查更新



注意：通过单击“检查更新”进行的 Streamer 更新需要与用户交互来完成整个更新过程。此更新事件与“自动更新 Streamer 间隔”无关。

导入新版本的软件组件

除了 Splashtop Gateway 中的嵌入式软件组件外，Splashtop 还将发布具有新功能和补丁的新组件。您可以导入到 Gateway，建议进行此操作以保持系统正常运行。本节将介绍如何将新版本的软件组件导入 Splashtop Gateway。

获取 PKG 文件

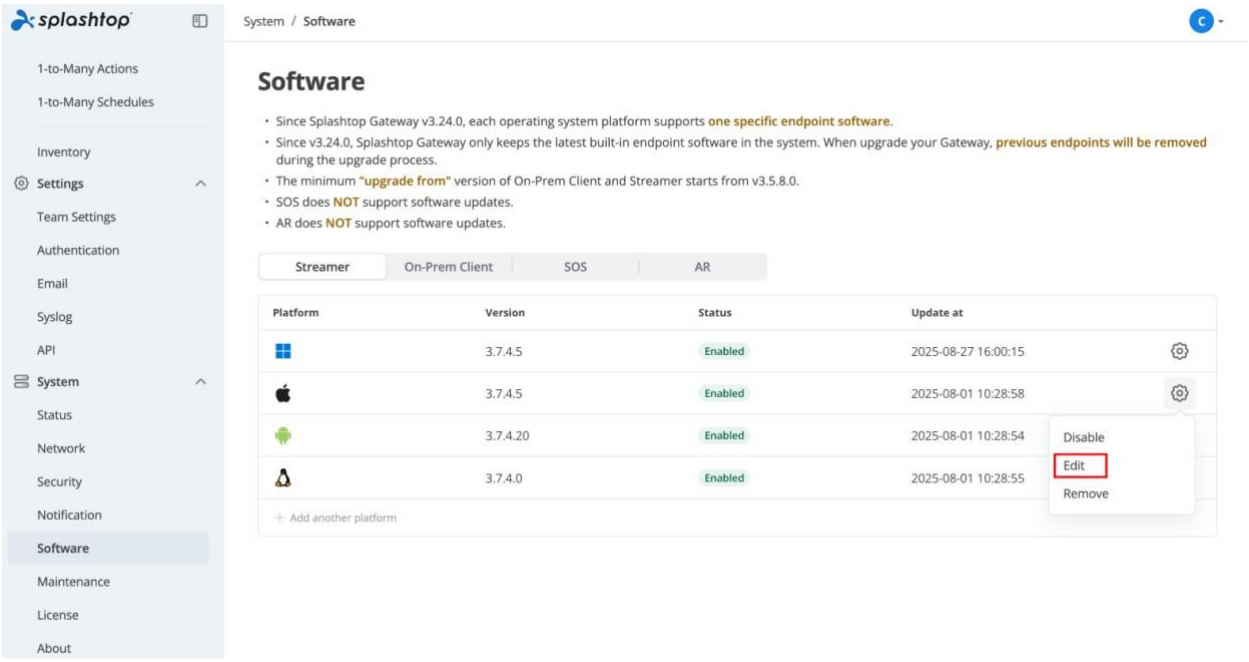
在以下新版本公告页面中，可以获取 PKG 文件格式的新版本软件组件。

- **Splashtop Gateway -** 新版本公告页面
- **Splashtop Streamer -** 新版本公告页面
- **Splashtop On-Prem 客户端应用程序 -** 新版本公告页面

> **注意：**请查看页面中的版本兼容性信息

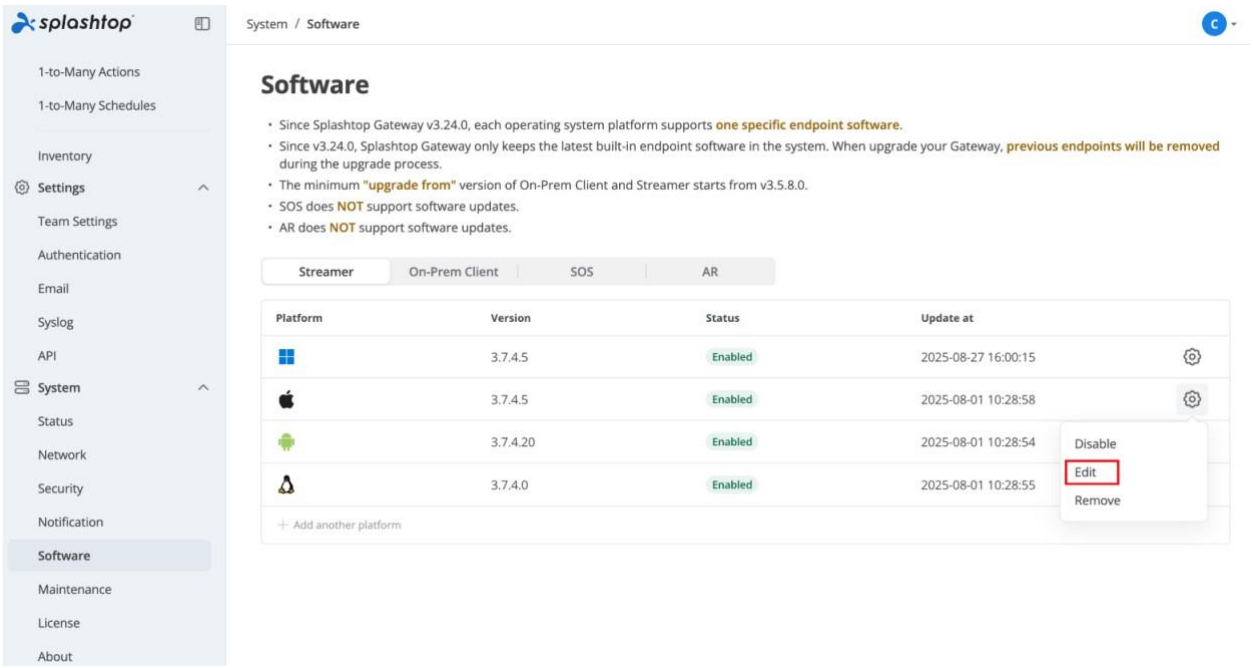
将 PKG 文件导入 Splashtop Gateway

注意：从 Gateway v3.24.0 版本开始，上传 PKG 迁至软件列表 -> 齿轮按钮 -> 编辑



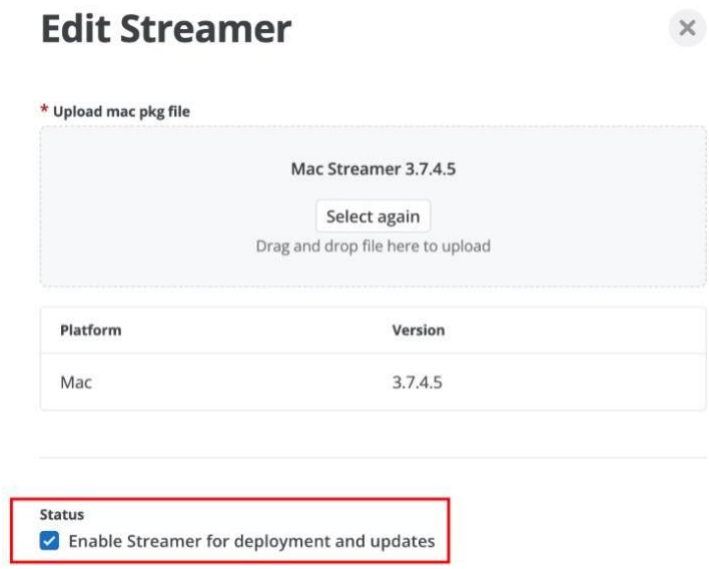
导入 Streamer

1. 以团队所有者身份登录，打开 Gateway 管理控制台 > 系统 > 软件 > Streamer，根据操作系统平台选择 Streamer，然后单击 编辑，如下所示。

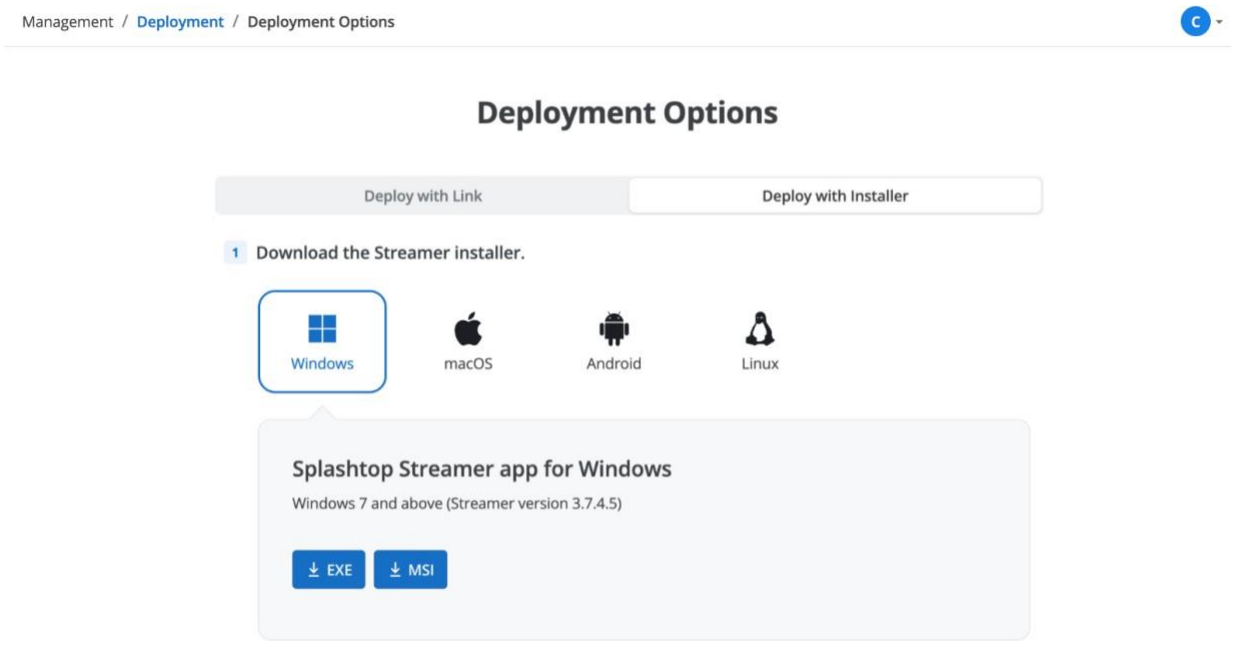


2. **选择** PKG 文件，系统将验证 PKG 是否正确打包用于 Gateway，并显示安装包信息，如 *平台*和 *版本*。最后点击**保存**以保存设置。

启用上传的 Streamer 以使其可用于部署和更新。

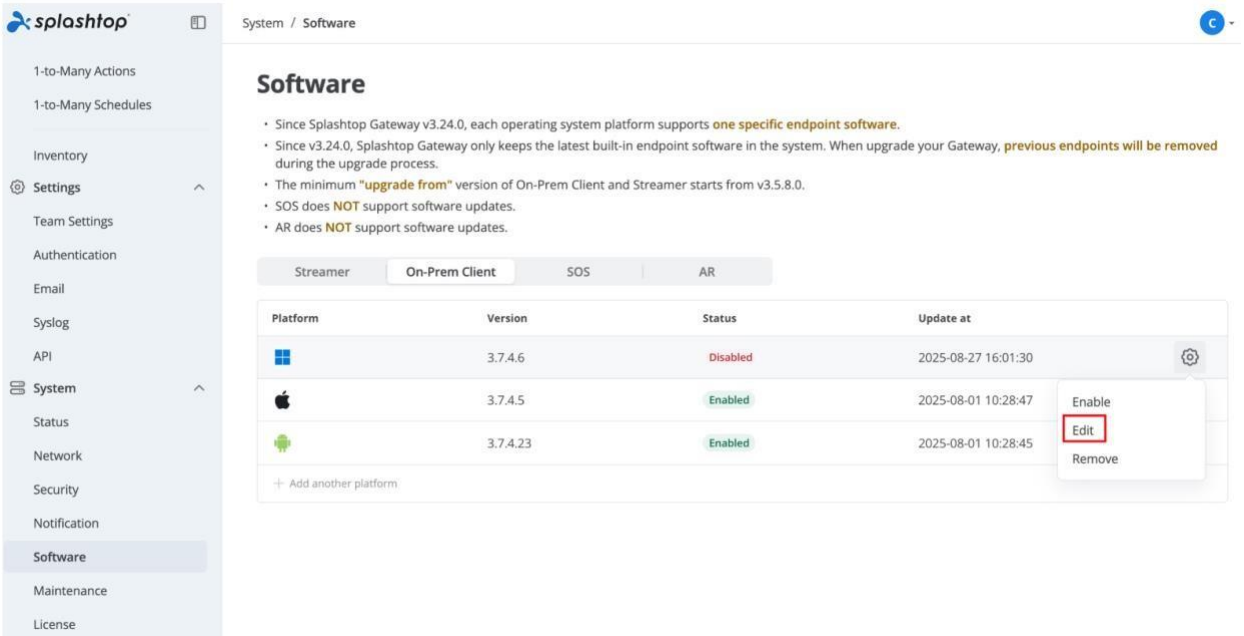


3. 完成后，新上传的软件即可用于部署和更新。



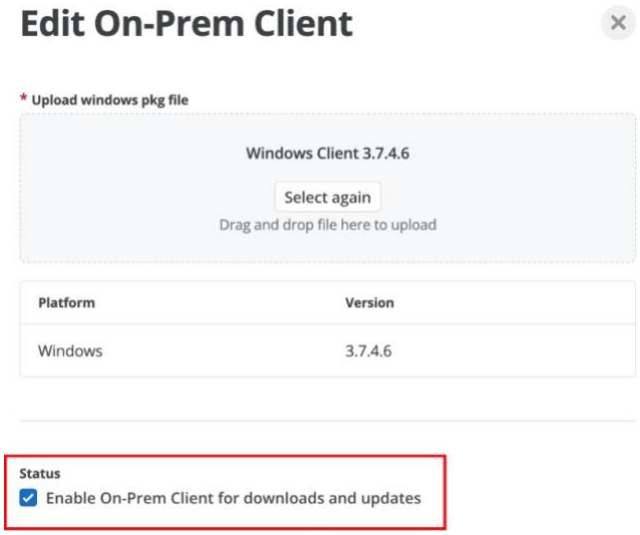
导入 Splashtop On-Prem 应用程序

1. 以团队所有者身份登录，打开 Gateway 管理控制台 > 系统 > 软件 > On-Prem 客户端，根据操作系统平台选择客户端应用程序，然后单击编辑，如下所示。

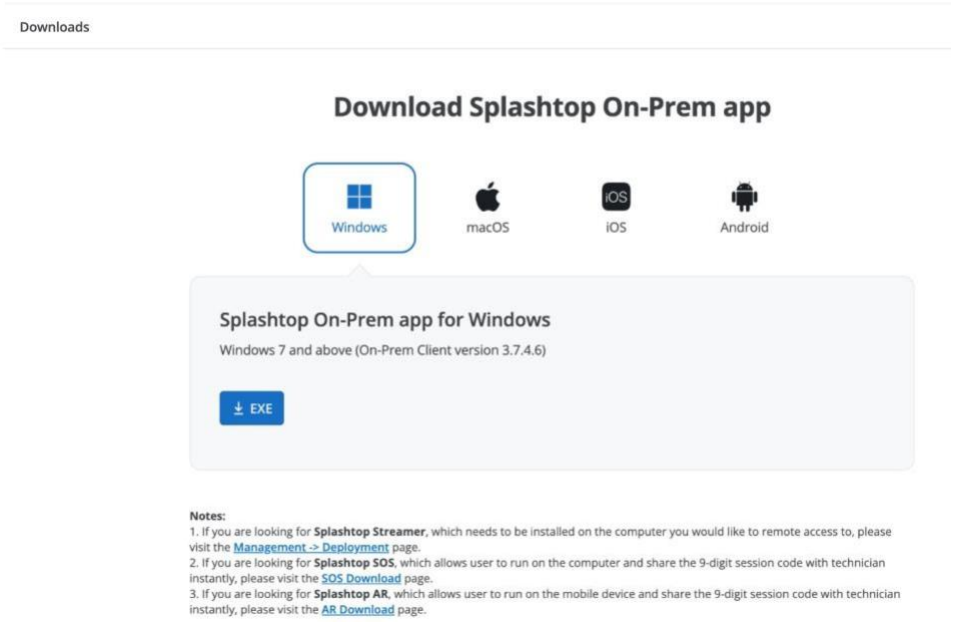


2. **选择** PKG 文件，系统将验证 PKG 是否正确打包用于 Gateway，并显示安装包信息，如 *平台*和 *版本*。最后点击**保存**以保存设置。

启用上传的客户端应用程序，使其可用于下载和更新。



3. 完成后，新上传的软件即可从 Gateway 下载和更新。

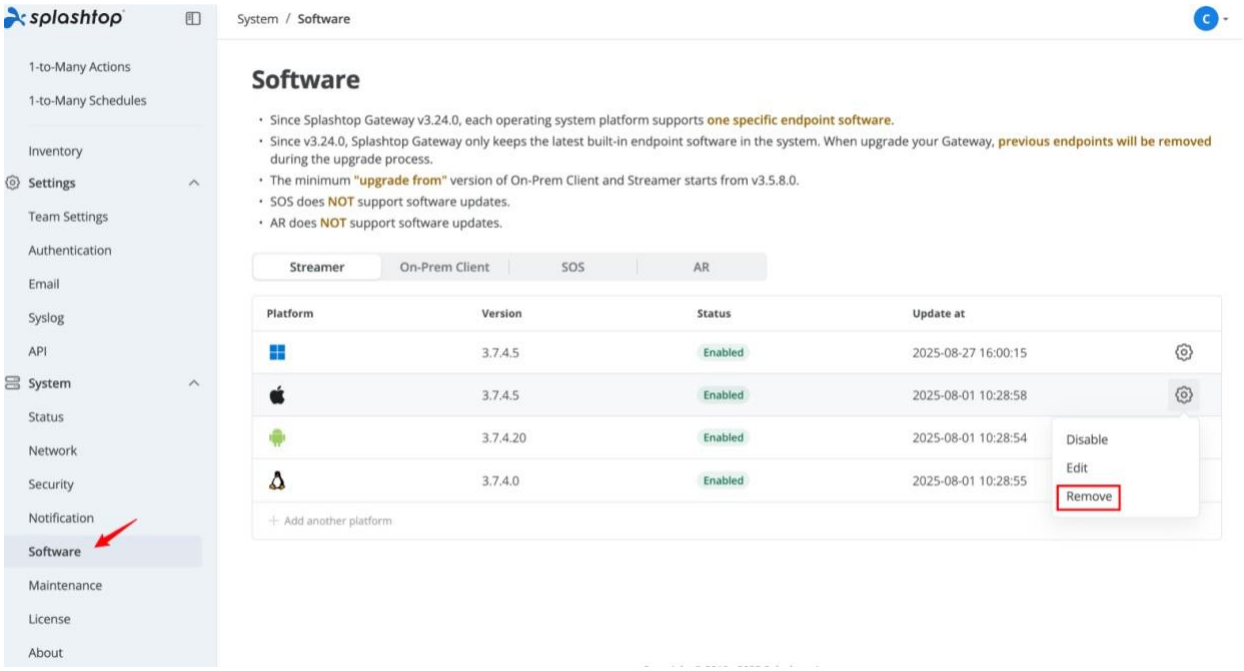


删除软件组件

团队所有者可以从 Splashtop Gateway 中删除指定的 Streamer 或 On-Prem 应用程序，已删除的组件将无法再下载，但不会影响现有安装。

删除 Streamer

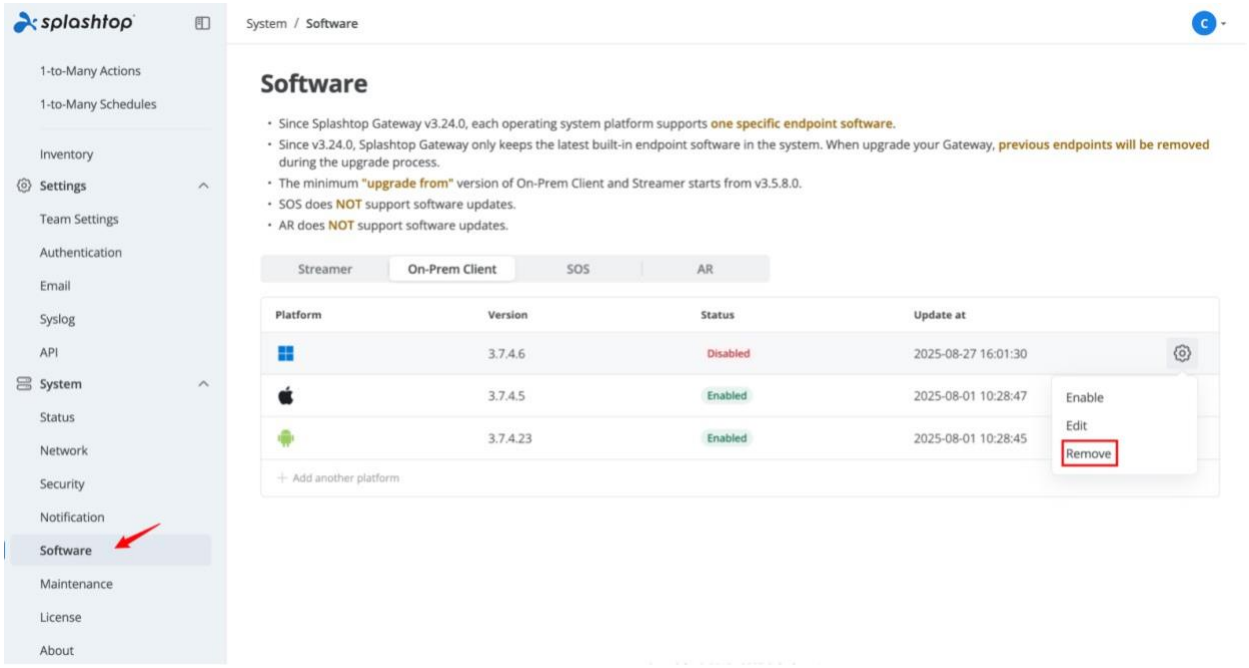
1. 以**团队所有者**身份登录，打开管理控制台 > 系统 > 软件 > Streamer，在齿轮按钮菜单中，单击*删除*以从 Gateway 中删除 Streamer。



2. Streamer 一经删除，则在**部署**页面中不可用。

删除 Splashtop On-Prem 应用程序

1. 以**团队所有者**身份登录，打开管理控制台 > *系统* > *软件* > *On-Prem 应用程序*，在齿轮按钮菜单中，单击*删除*将其从 Gateway 中删除。



2. On-Prem 客户端一经删除，则在**下载**页面中不可用。

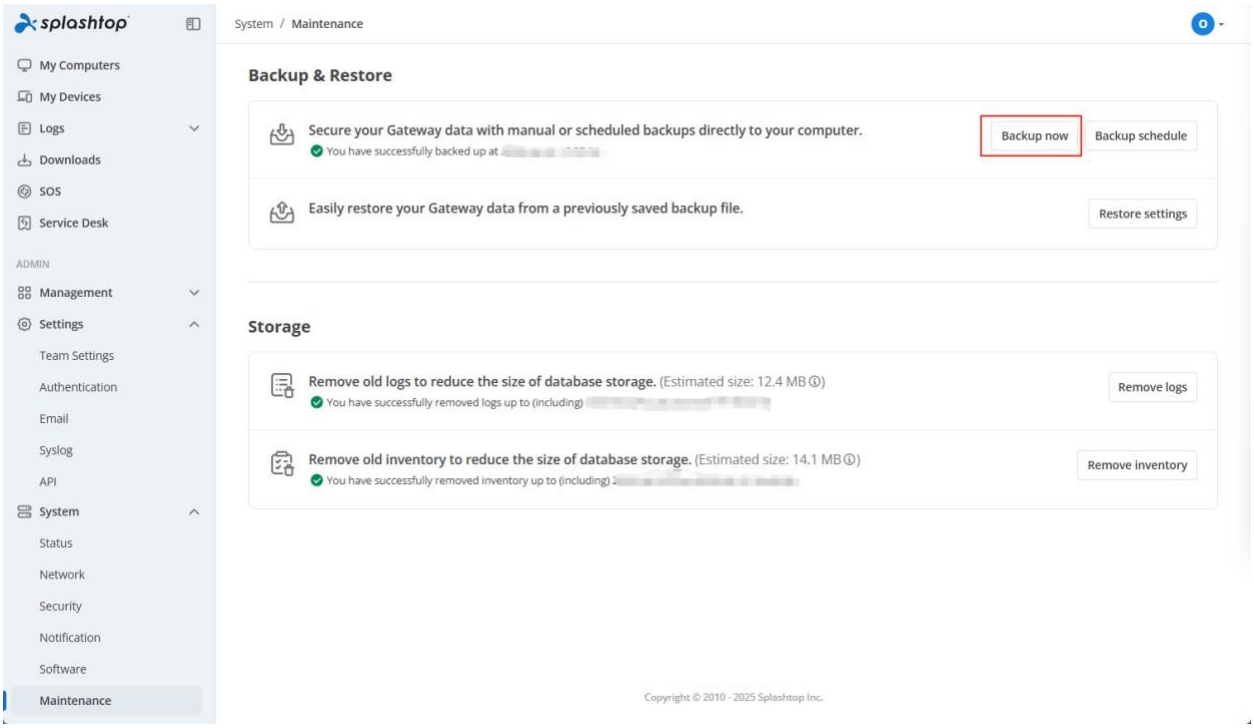
维护

定期备份系统很重要。有助于硬件/软件出现意外故障或意外删除数据后恢复 Splashtop On-Prem 系统。系统备份是防止数据丢失的关键，因为数据丢失可能会导致业务运营完全中断。

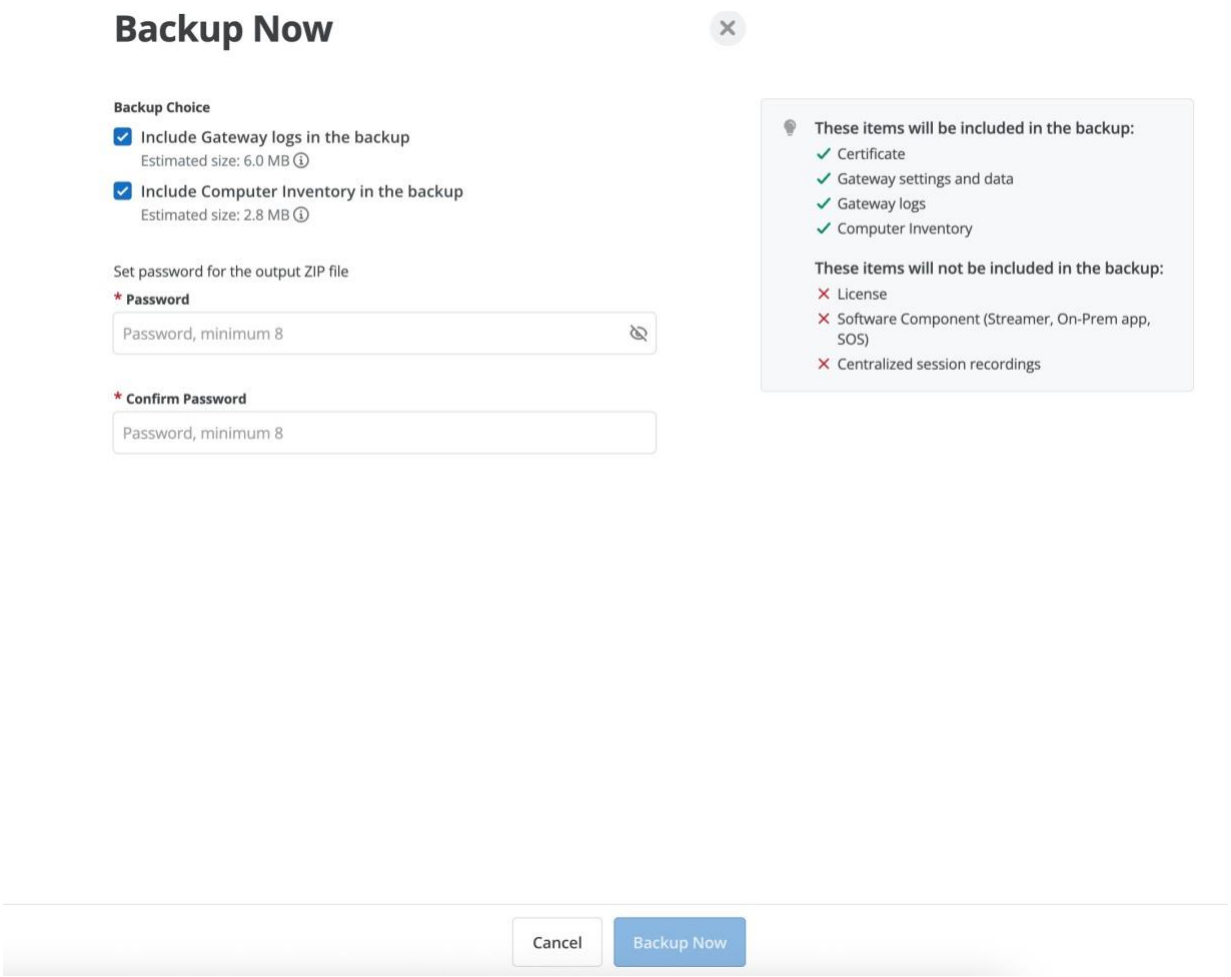
备份

要启动系统备份或恢复任务，必须使用**系统所有者账户**登录 Splashtop Gateway 门户网站。系统所有者账户是用于激活 Splashtop On-Prem 系统许可证的电子邮件地址。

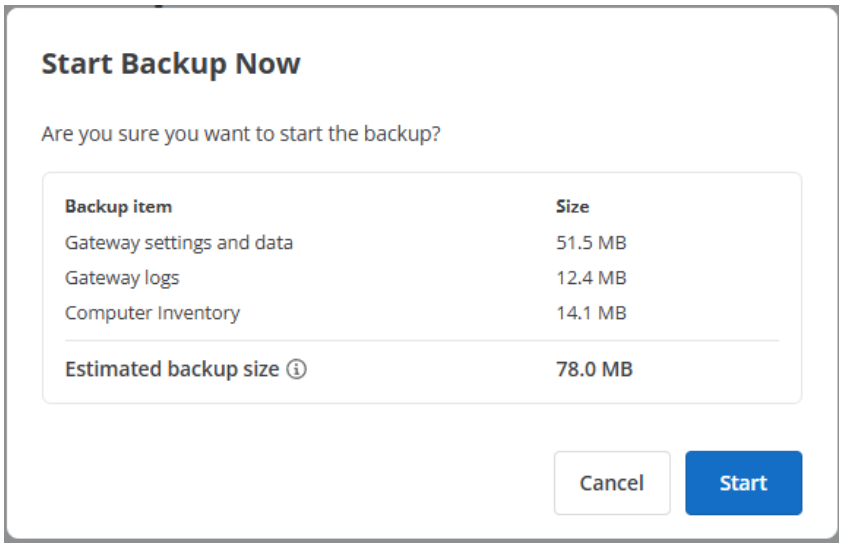
登录到 Gateway 门户网站后，转到**系统**菜单栏，然后导航到**维护**页面。



点击**立即备份**按钮。在开始整个备份过程之前，必须为要生成的 ZIP 文件设置密码。



将弹出一个确认对话框，其中列出了此备份中包含的数据库中备份项大小。



点击**开始**按钮，受密码保护的 ZIP 文件将自动保存到从浏览器下载的文件夹中。此 ZIP 文件包含一个 SQL 脚本，其中有详细的系统配置，比如系统设置、用户和组、已部署电脑和客户端设备、日志等。但是，许可证不包含在备份文件中，因此从 SQL 脚本恢复系统后需要重新激活许可证。

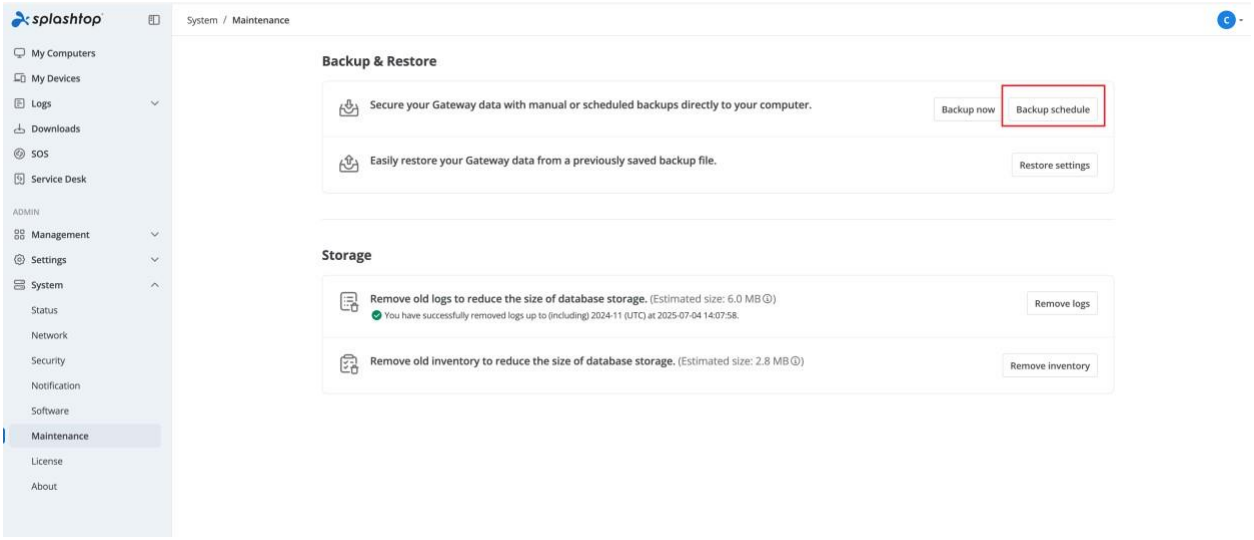
备份计划

备份计划可用于确保以一致且及时的方式完成备份。只要配置并启用备份计划，系统就可以按照计划定期进行数据备份。

如何配置备份计划？

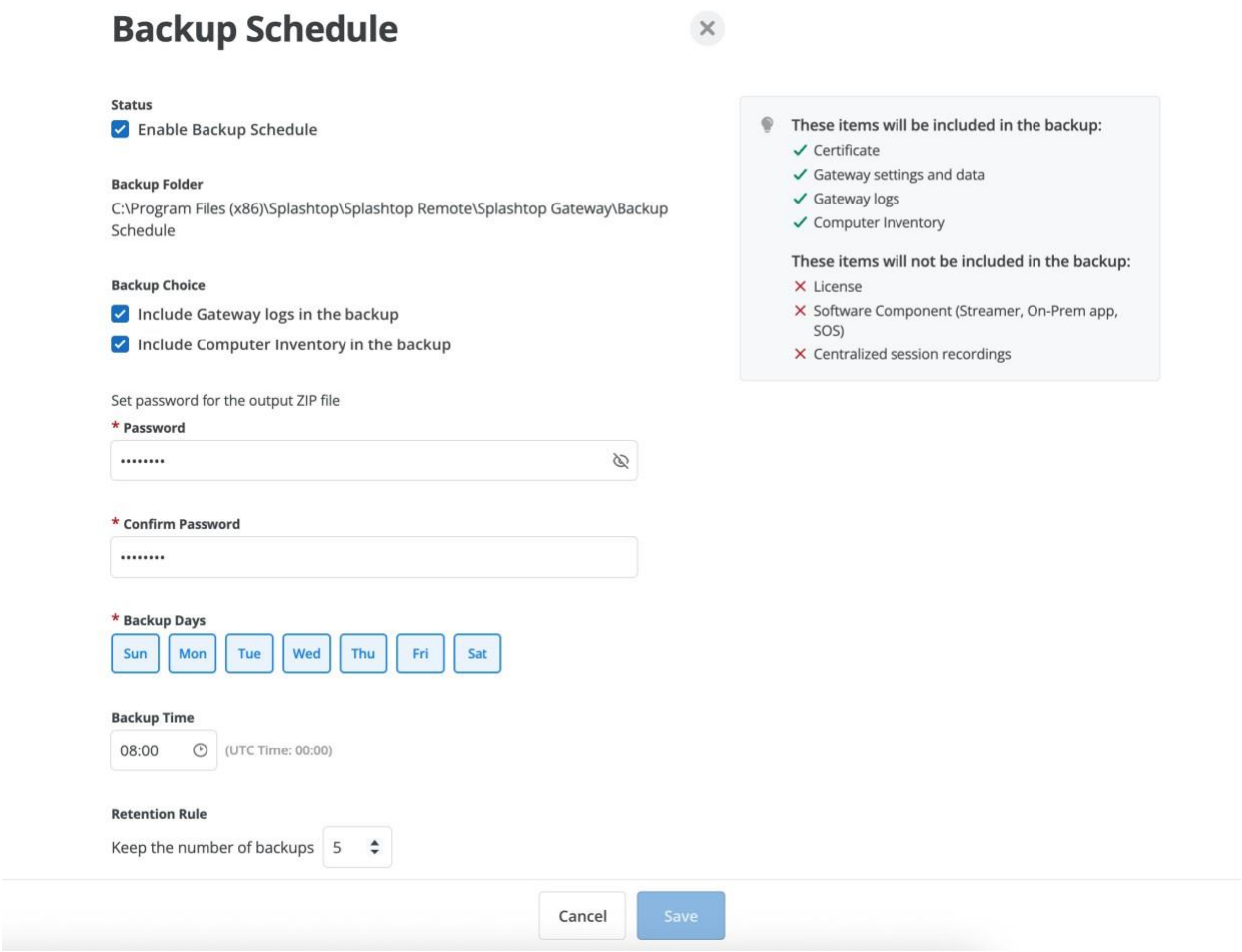
要配置备份计划，必须使用团队所有者账户登录 Splashtop Gateway 门户网站。团队所有者账户即用于激活 Splashtop On-Prem 系统许可证的电子邮件地址。

登录到 Gateway 门户网站后，转到**系统**菜单栏，然后导航到**维护**页面，单击**备份计划**按钮。



备份计划设置

配置以下选项以创建备份计划策略。

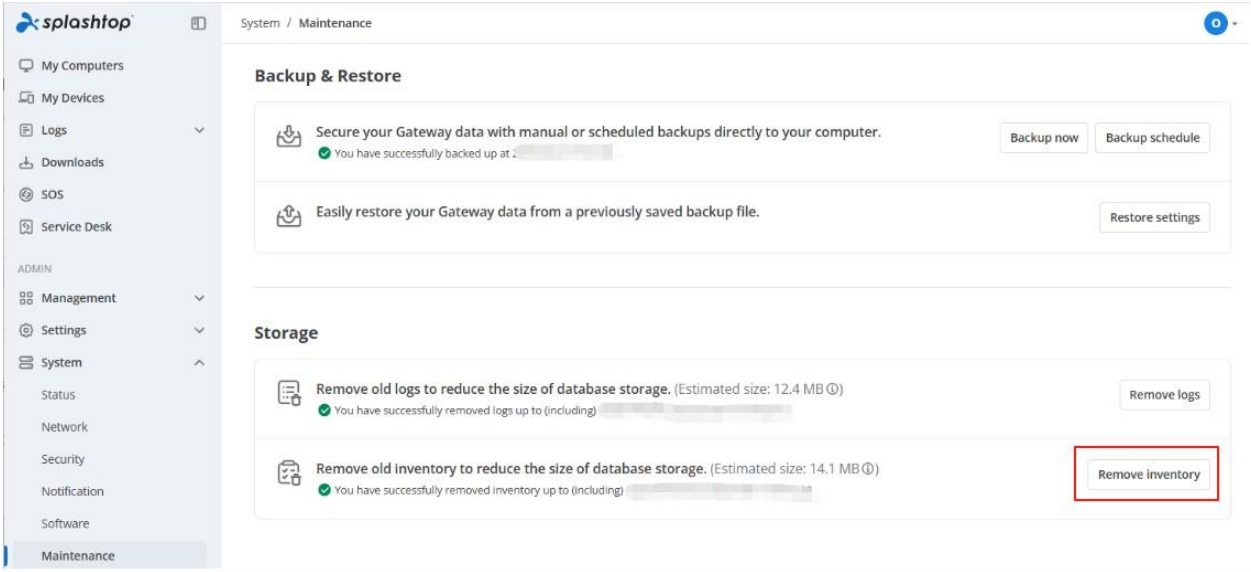


- **状态**，打开此选项以启用备份计划。如未启用此选项，则即使保存配置，备份计划也无法运行。
- **备份文件夹**，显示存储备份计划文件的路径。
- **备份选项**，选择是否在备份计划文件中包含 Gateway 日志、电脑资产清单和历史记录，页面右侧区域将根据备份选项的设置显示当前备份的确切范围。
- **输入密码**，在开始备份之前，需要为要生成的 ZIP 文件设置密码。
- **确认密码**，在开始备份之前，需要为要生成的 ZIP 文件设置密码。
- **备份天数**，选择备份计划的备份天数。
- **备份时间**，选择备份计划的备份时间。
- **保留规则**，选择需要在备份文件夹中保留的备份数量。

注意：

- 只能同时运行一个备份。
- 为确保备份计划的效率，备份计划文件将不包含端点。

从 Gateway v3.36.x 开始，团队所有者可以出于维护目的删除电脑资产清单。



以团队所有者身份登录 Splashtop Gateway，转到 web/系统/维护

找到“**删除资产清单**”并开始清理电脑资产清单以释放磁盘空间。

注意：

1. 已删除的电脑资产清单不可恢复，无法找回。如果在您的组织中定期审计是常规流程，则请在删除任何电脑资产清单前先咨询。

2. 电脑资产清单支持按月删除，最近2个月的日志无法删除。

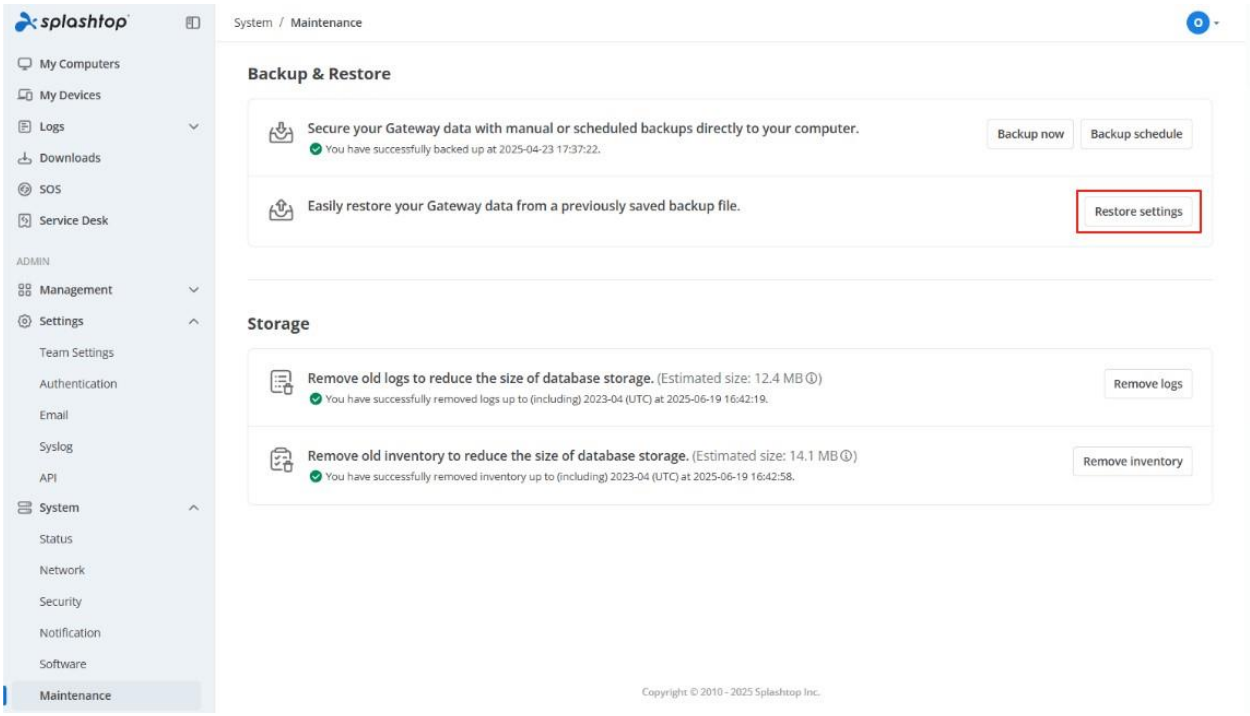
还原

在进行还原之前，请注意以下事项：

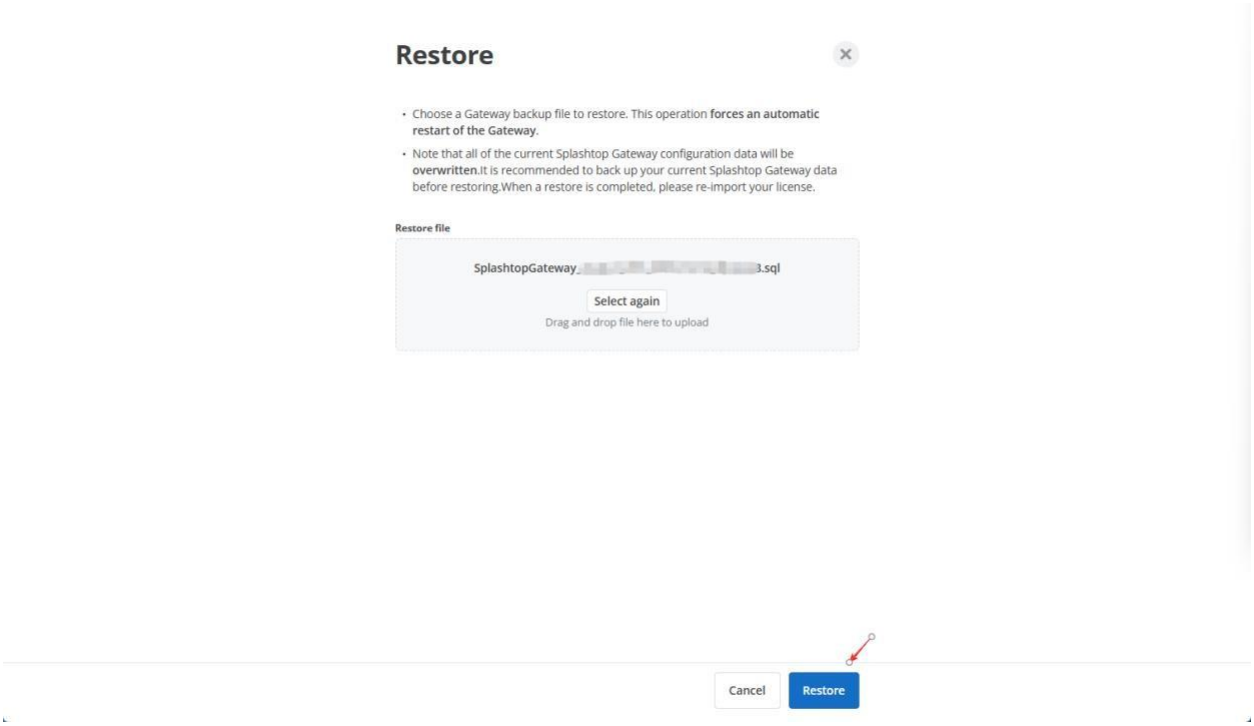
- 具备 Splashtop On-Prem 的许可证密钥。系统还原后，系统会请求再次激活许可证。
- 解压缩备份 ZIP 文件并将 SQL 脚本保存到本地文件夹，为还原文件做准备。
- 备份当前系统，因为所有现有配置都将被永久删除。

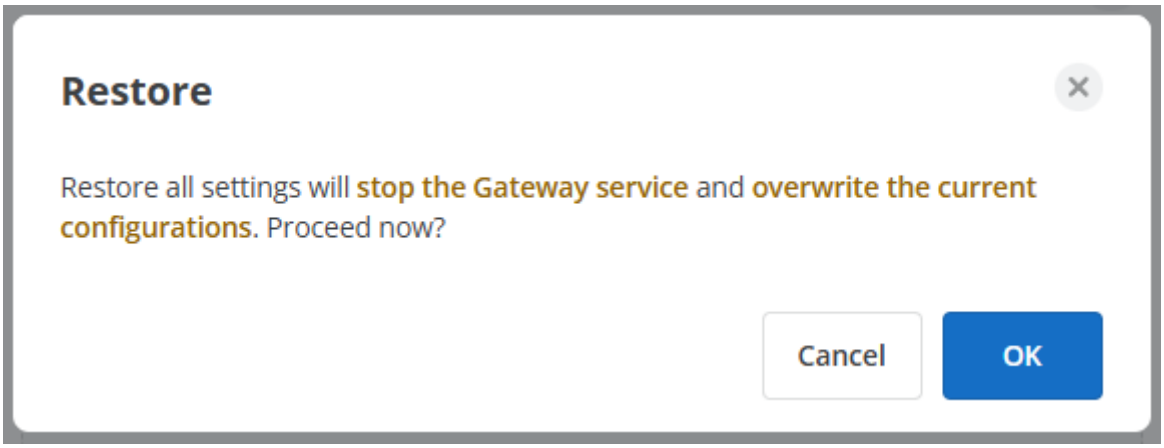
与**备份**相同，要使用系统所有者账户登录 Splashtop Gateway 门户网站，单击系统菜单并打开**维护**页面。

单击**还原设置**按钮，然后单击**选择**按钮浏览 SQL 脚本文件。

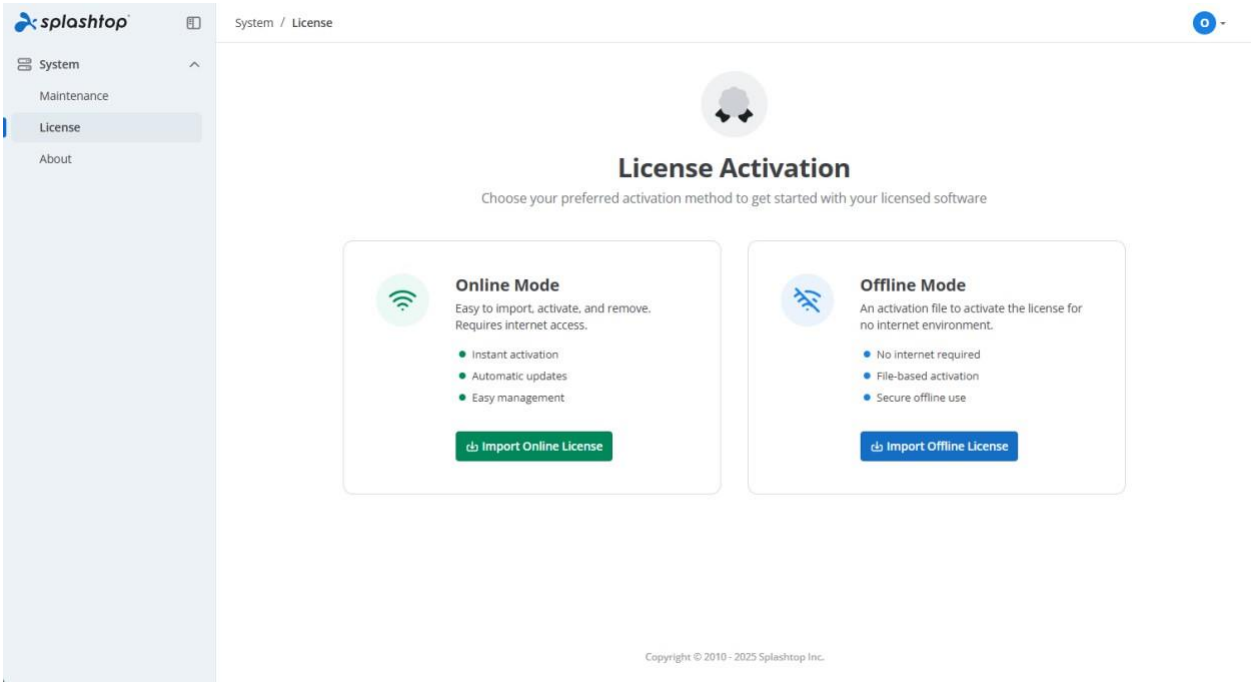


点击**还原**按钮并确认以还原系统。





成功还原 Splashtop On-Prem 系统后，该页面将自动跳转到**许可证**页面。

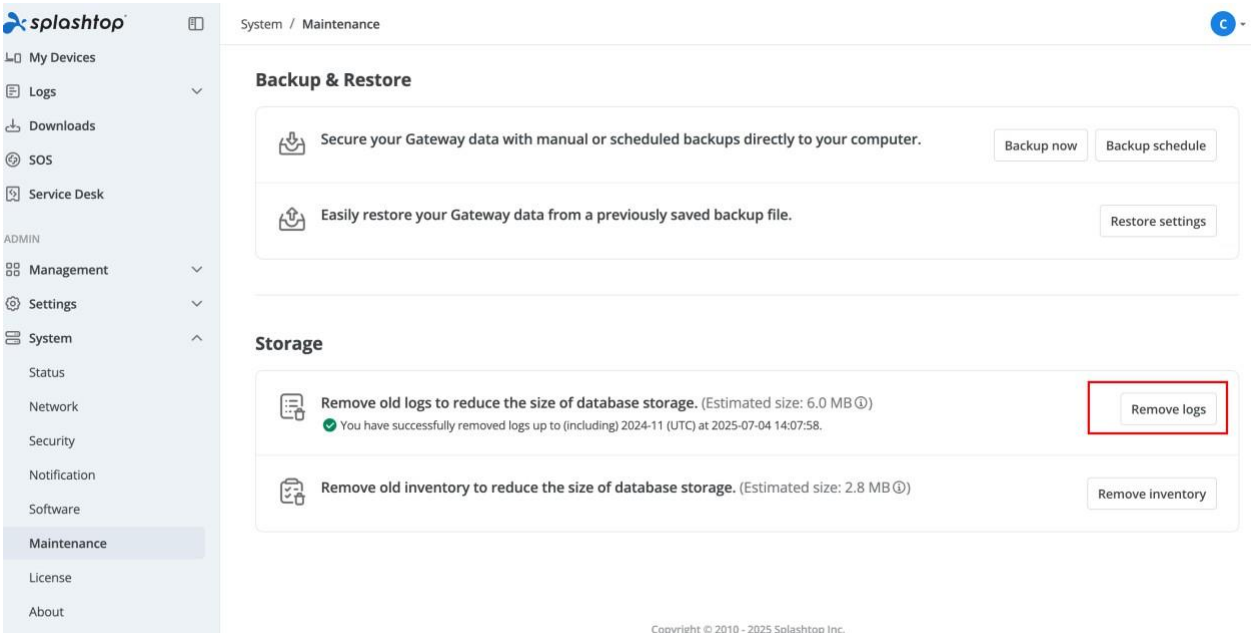


通过在线或离线模式激活许可证，具体取决于购买的许可证类型。

系统还原成功！

删除 Splashtop On-Prem 日志

系统管理员可以出于维护目的删除 Gateway 日志。



以所有者身份登录 Splashtop Gateway，导航到 web/系统/维护页面，找到“删除日志”并开始清理日志以释放磁盘空间。

注意：

1. 已删除的日志不可恢复，并且无法找回。如果在您的组织中定期审计是常规流程，则请在删除任何日志前先咨询。

2. 日志支持按月删除，最近2个月的日志无法删除。

3. 删除的日志无法在 web/日志/...中查看，也无法导出相应的 CSV。

通知

Splashtop On-Prem 团队所有者可以从通知页面发布系统通知，以通知用户是否因系统维护而导致预期停机，或可通知用户端点上是否有任何可用更新。

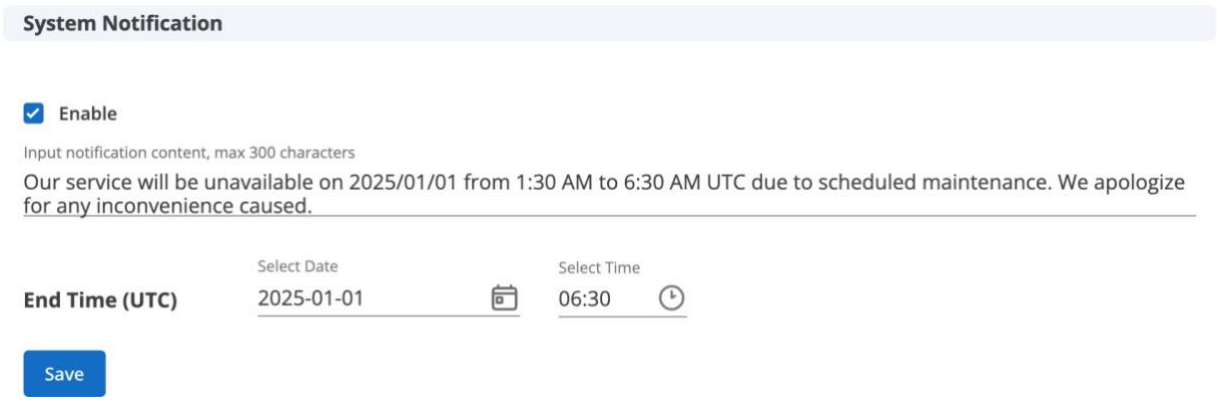
团队所有者账户可以到 **Splashtop Gateway > 系统 > 通知**中找到通知页面

要发布通知，请首先选中**启用**。

在下面的空白处输入通知内容，并设置此通知的结束时间。

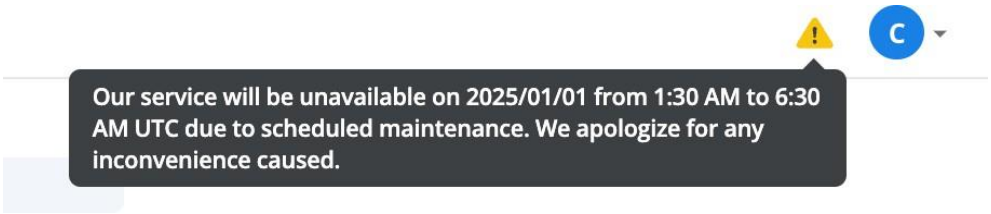
注意： 系统通知**采用 UTC 时间。请在发布通知前计算时差。**

下图以系统通知为例：

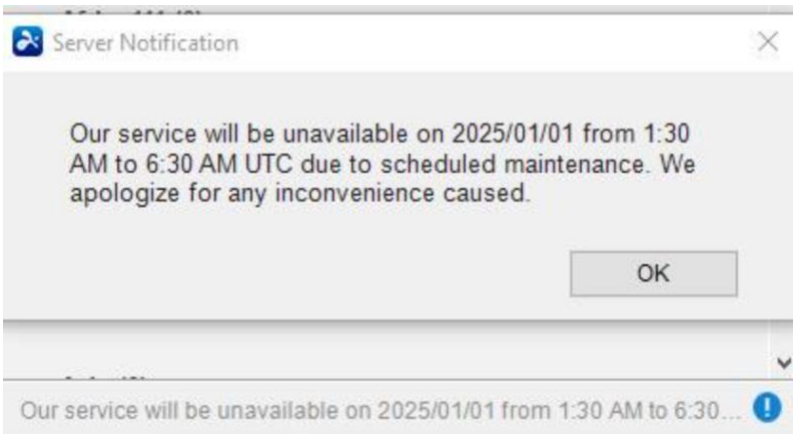


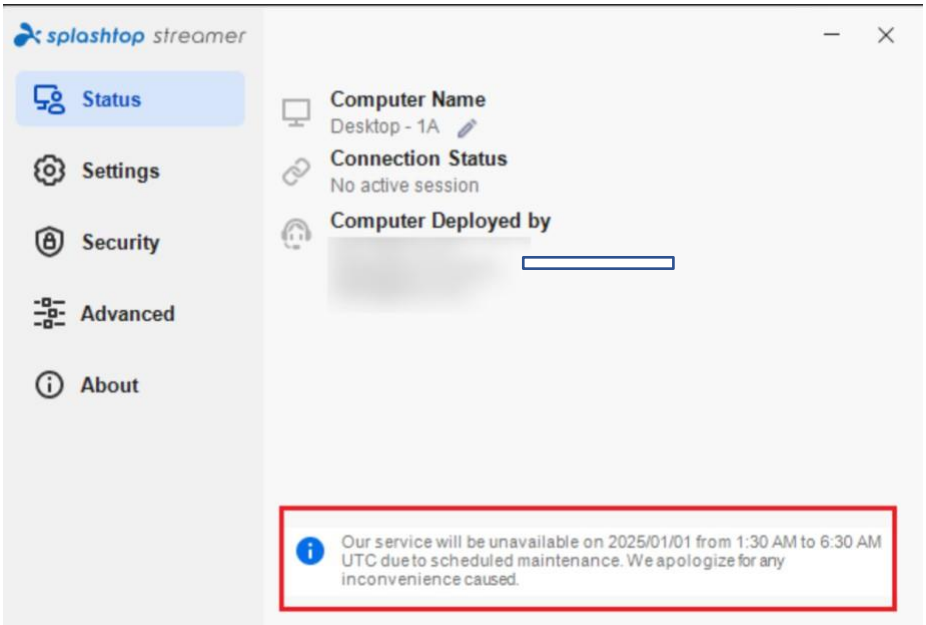
保存后，系统通知将在 Gateway 页面的右上角显示，带有一个黄色感叹号。将鼠标悬停在黄色感

叹号即可向所有登录用户显示通知。



从当前启用时间到结束时间（即2025年1月1日上午6：30），也可以在任意使用中的 On-Prem 应用程序（点击底部的蓝色感叹号以查看更多内容）或 Streamer 查看此通知。



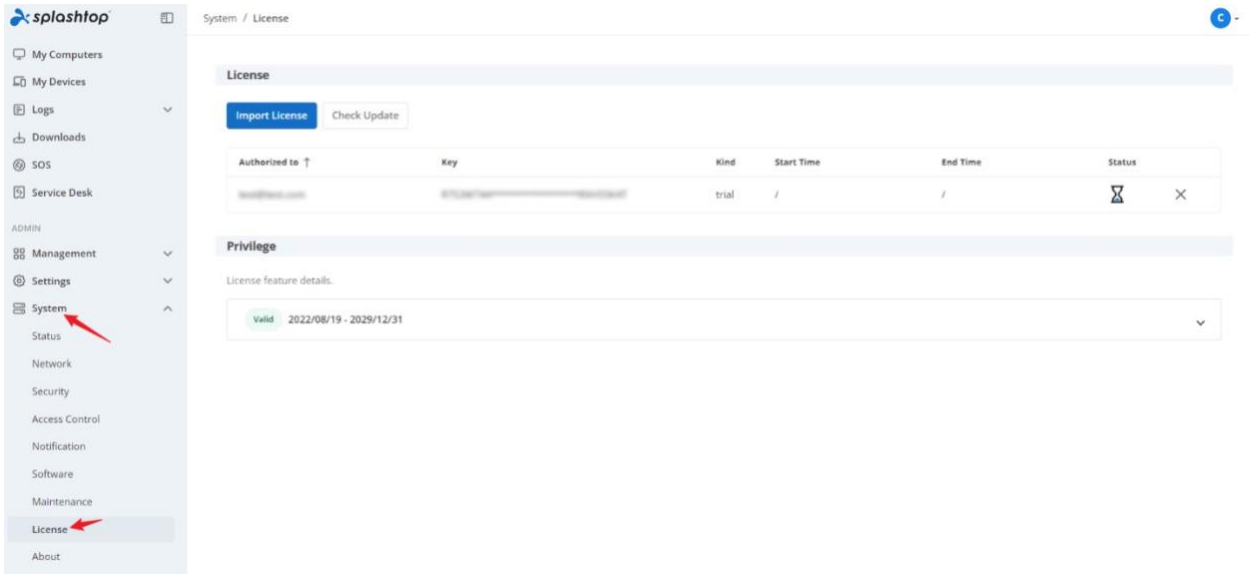


Splashtop On-Prem 许可证

了解您的许可证和权限

Splashtop Gateway 门户网站及其服务**必须** 由至少一个授权许可证（试用或付费）激活才能运行。

要查看许可证信息，请使用**团队所有者**账户在浏览器中打开Splashtop Gateway，导航到**系统 -> 许可证**。



Splashtop On-Prem 支持**多许可**，也就是说可以将两个及以上具有不同有效期和权限集的许可证应用于同一系统。许可证页面将显示每个许可证的许可证所有者、密钥编号、有效性和状态等信息。

可通过单击行尾的图标来检查特定许可证的权限，或可到权限页面单击许可证有效性以显示许可证详细信息。

许可证分为三部分：常规、无人值守功能、有人值守功能（也称为 SOS）。无人值守会话指无需远程电脑确认即可建立远程连接，而有人值守会话则需要远程电脑有人帮助设置远程连接。参考使用场景了解有关更多信息。

详见下表以了解许可证具备的权限，表中说明了许可证项目相关的功能。

有效性	含义
日期范围	以下权限集的日期范围
最大无人值守用户数量	可以启用的最大无人值守用户账户数量
最大无人值守并发用户数量	可以同时建立会话的最大无人值守用户数量
最大无人值守 Streamer 数量	可以部署的最大无人值守 Streamer 数量
最大有人值守用户数量	可以启用的具备 SOS 功能的最大用户账户数量
最大有人值守并发用户数量	可以同时建立 SOS 会话的最大有人值守用户数量
无人值守功能	
最大远程会话数量	整个系统上无人值守并发会话的最大数量，即使将其设置为无限制，仍将采用最大无人值守并发用户策略
一个 Streamer 的最大并发远程会话数量	允许同时访问一个 Streamer 的最大用户数
最大文件传输量（会话外）	可以在整个系统上建立外部会话文件传输会话的最大数量
到一个 Streamer 的最大并发文件传输量（会话外）	允许同时向一个 Streamer 传输的最大外部会话文件数

Max Chat （会话外）	整个系统上的最大外部会话聊天会话数
一个 Streamer 的最大并发聊天数（远程会话外）	可以同时为一个 Streamer 建立的最大远程会话外聊天会话数
远程打印	是否允许启用远程打印功能
远程唤醒	是否允许启用远程唤醒功能
远程重启	是否允许启用远程重启功能
远程命令	是否允许启用远程命令功能
音频	是否允许启用音频重定向功能
电脑端 Streamer	是否允许启用电脑端 Streamer，即 Windows、Mac、Linux（即将推出）
移动端 Streamer	是否允许启用移动端 Streamer，即 Android
终端会话	是否允许访问 RDP 终端会话
多对一显示	是否允许多对一屏幕显示
多对多显示	是否允许多对多屏幕显示
会话录制	是否允许启用会话录制
有人值守功能	

最大远程会话数	整个系统上的最大有人值守会话数，即使将其设置为无限制， 仍将采用**最大有人值守并发用户**策略
一个 Streamer 的最大并发远程会话数	允许同时访问一个 Streamer 的最大用户数量
电脑端 Streamer	是否允许启用电脑端 Streamer，即 Windows、Mac、Linux（即将推出）
移动端 Streamer	是否允许启用 Android Streamer
多对一显示	是否允许多对一屏幕显示
多对多显示	是否允许多对多屏幕显示
会话录制	是否允许启用会话录制

许可证过期提醒

Splashtop On-Prem 提供自动许可证到期通知功能，可以帮助管理员及时采取行动以避免服务中断。

功能详情

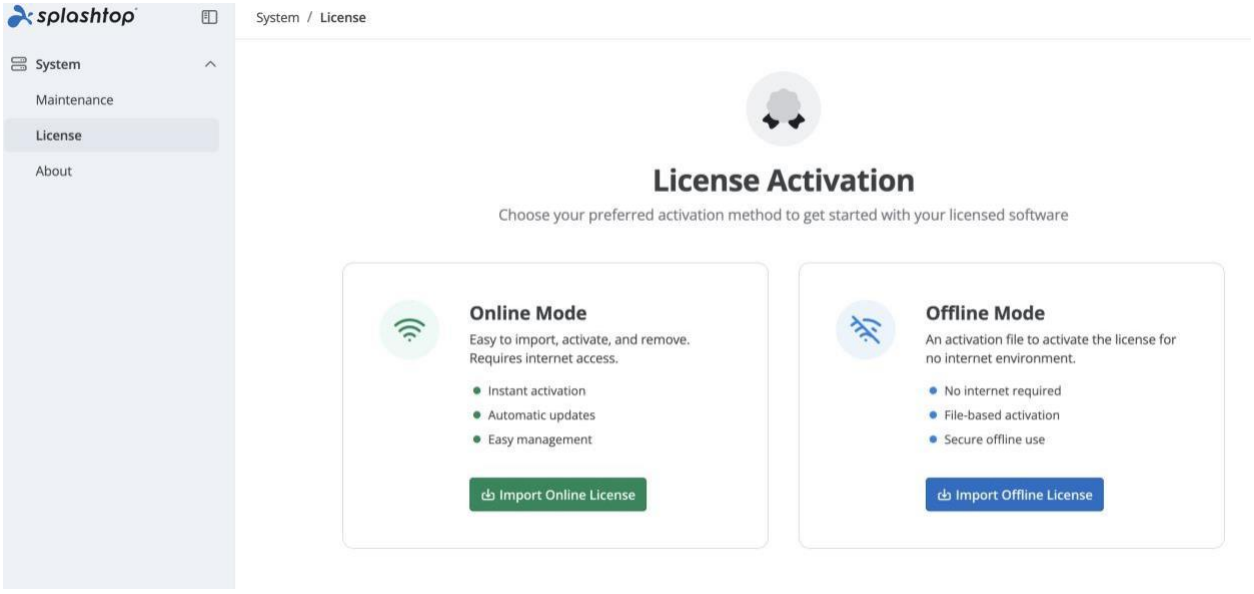
- 此功能默认启用，不需要手动设置。可在系统 -> 许可证页面查看。

- 团队所有者将在许可证到期前30、7和1天收到电子邮件通知。
- 此功能在启用 SMTP 服务器时生效。

激活许可证

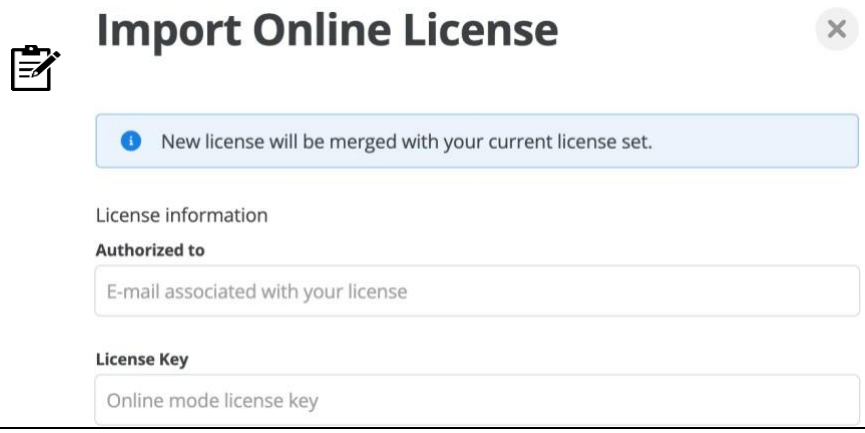
Splashtop Gateway 支持两种模式的许可证激活，即在线激活和离线激活。您需要先激活许可证，然后才能使用该系统。

只有以团队所有者身份登录才能激活许可证，可到 Gateway 的**系统 > 许可证**页面操作。



在线许可证激活

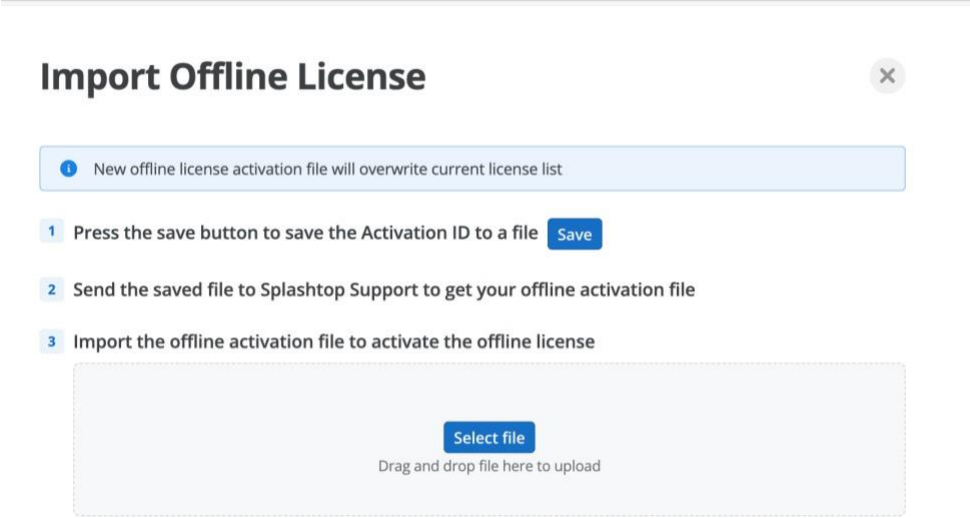
对于在线许可证激活，可以单击导入在线许可证，输入您从 Splashtop 销售人员处获取的授权和许可证密钥。



注意：Splashtop Gateway 需要连网和出站许可证。**splashtop.com:443** 不应被防火墙阻止。

离线许可证激活

如果您的 Splashtop Gateway 无法连网，则可选择离线许可证激活。



1. 在许可证页面点击**导入离线许可证**，点击**保存**下载激活 ID。

2. 将激活 ID 文件发送给 Splashtop 销售人员，他们 将生成离线激活文件并回传。

3. 单击**选择**以上传激活文件，然后单击**导入**以完成离线许可证激活

关于

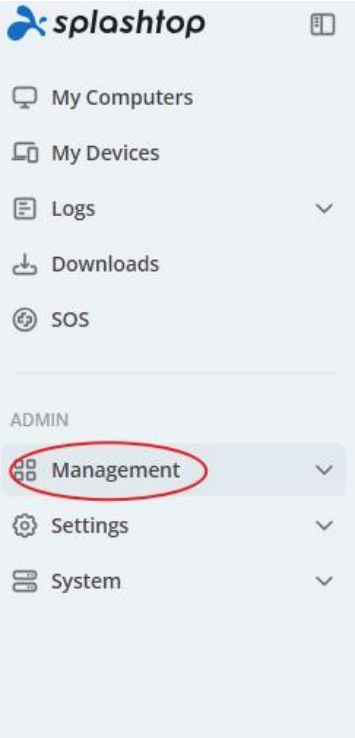
关于页面提供相关系统信息，包括：

- **版本**：Splashtop On-Prem 的版本号，版本号后面是内部版本号
- **构建时间**：构建此版本的日期和时间
- **新增功能**：此版本的新功能和增强功能
- **服务条款**：您与 Splashtop 之间关于使用 Splashtop 服务的条款和条件
- **隐私政策**：供您查阅的 Splashtop 隐私政策说明文档
- **支持网站**：Splashtop 技术支持网站的链接。如果您是 Splashtop On-Prem 用户，请在此链接页面选择 Splashtop On-Prem

管理控制台

简介

管理控制台是 Splashtop Gateway 门户网站的一个重要面板，供团队管理员和组管理员管理系统配置，例如用户和组、电脑和端点、部署套件等。



管理控制台的菜单因被分配的角色而异，角色包括团队管理员、组管理员和普通成员。

普通成员不允许访问管理控制台，因此成员菜单中没有管理和设置选项卡。

在此示例中，团队所有者和管理员可以在管理上下文菜单中查看以下选项：用户、所有电脑、所有设备、分组、部署、首选项策略、一对多操作、一对多计划、频道以及资产清单。

团队所有者独有的管理范围包括：设置 – 团队设置、身份验证、电子邮件、Syslog 和 API。

我们将从团队所有者的角度说明管理控制台每个选项的作用。

- **用户**
- **所有电脑**
- **所有设备**
- **分组**
- **计划访问**
- **部署**
- **首选项策略**
- **一对多操作**
- **一对多计划**
- **设置**

用户

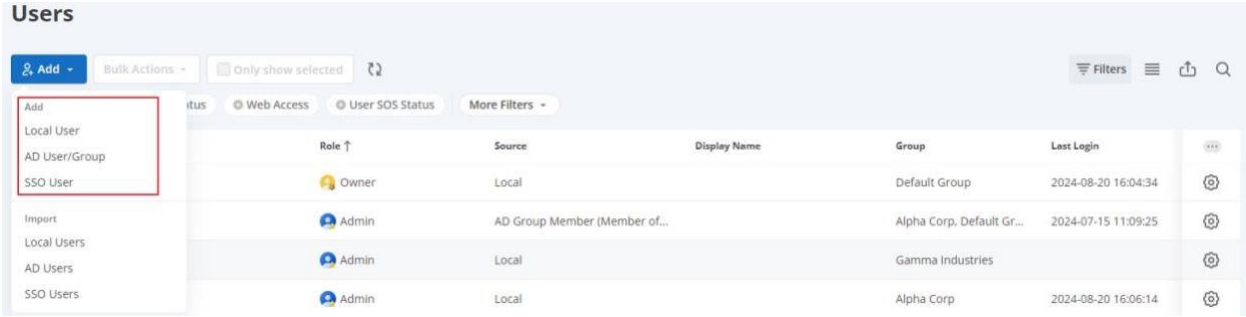
团队所有者/管理员可以使用此页面创建新用户或修改现有用户的属性。

Splashtop On-Prem 中有两种类型的用户账户：本地账户和 活动目录 （AD） 账户。要添加 AD 用户，团队所有者应首先在**系统**设置中配置活动目录服务器 。

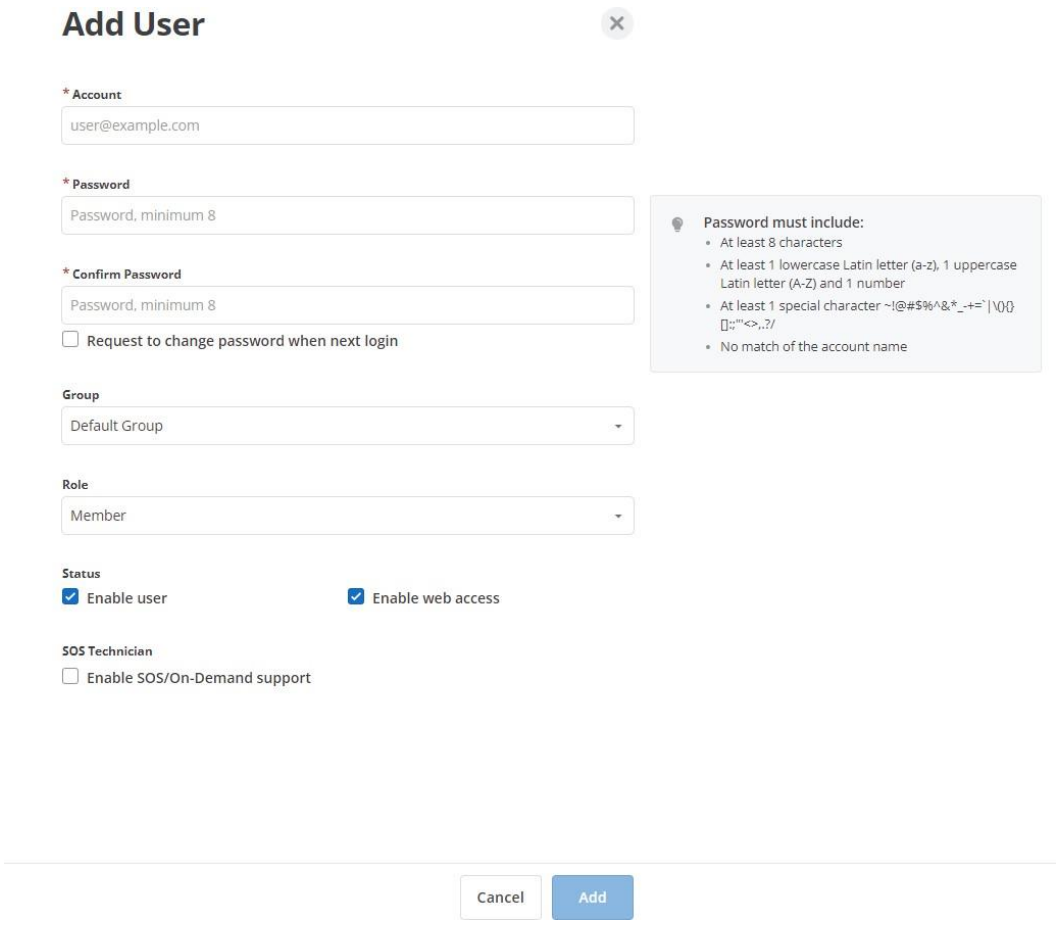
用户属性（包括角色、组、访问权限、显示名称、密码、两步验证）可在用户页面进行配置。

创建用户账户

用户管理位于 https://{gateway} > **管理** > **用户**。



创建本地账户

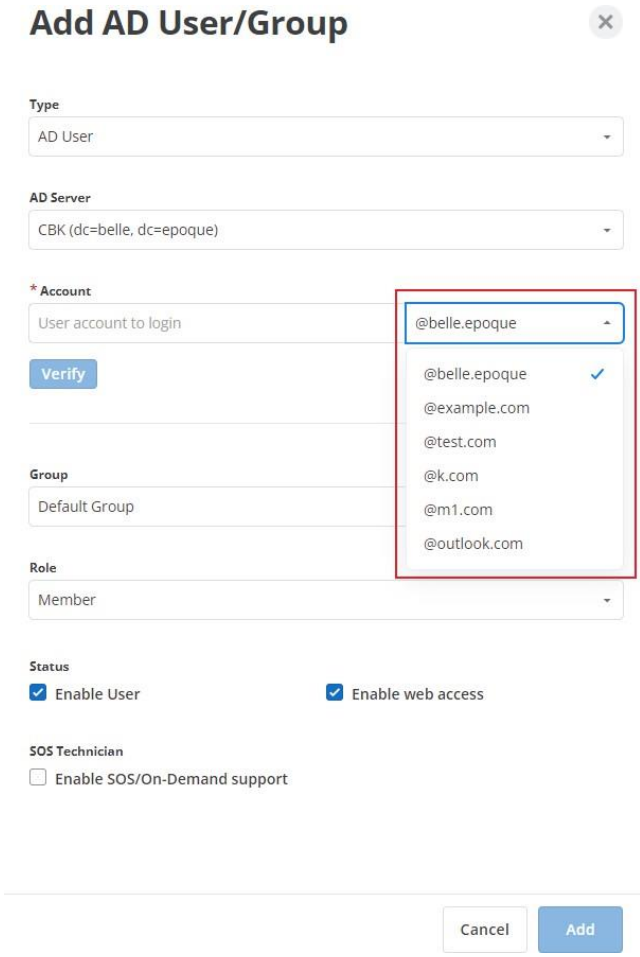


字段	*含义*
账户	此为用户的登录账户，在系统中是唯一的。
密码	至少包含8个字符。
生成密码	有助于生成更具随机性的密码以提高安全性。
下次登录时请求更改密码	选中此选项，用户登录系统时将需要更改密码。

分组	用户可以被分到不同组中，分组可以有效管理用户/访问权限。
角色	系统中有两种角色类型： 管理员： 管理员可以管理用户、电脑、授予访问权限等。管理员也可以进行远程会话。 成员：成员只能与被授予访问权限的电脑进行远程会话。
启用用户	如果账户已启用，用户则可建立远程会话；如果账户被禁用，用户仍然可以访问 Web 门户，但远程会话被禁用。
启用 Web 访问	禁用此选项将禁用此账户的 Web 访问功能。
SOS 技术员*	如果订购内容包含 SOS 服务，则可在创建用户时启用 SOS 功能以获得按需支持。

添加 AD 账户

AD 服务器成功通过身份验证后，可到系统-活动目录选项卡的 AD 服务器列表中查看。导航到**管理**选项卡 – **用户**，单击顶部的“**添加 AD 用户**”按钮。



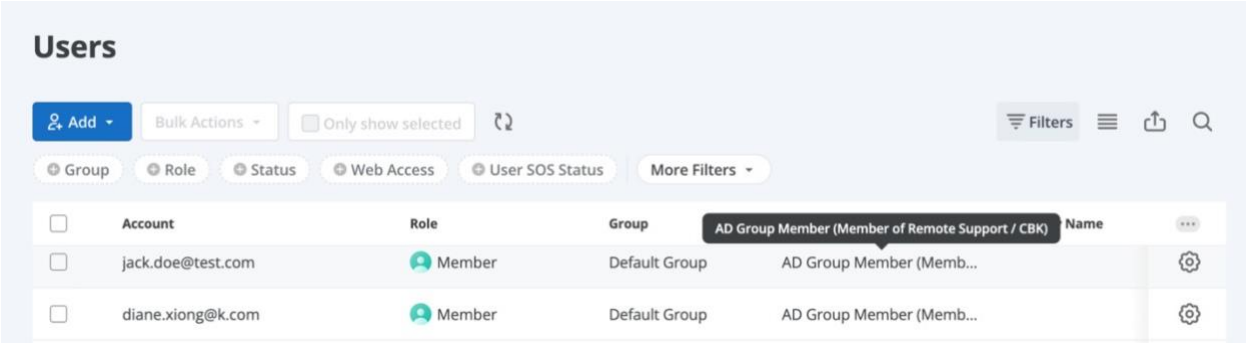
字段	*含义*
类型	通过选中 AD 用户，AD 个人用户将进行身份验证并添加到 Splashtop Gateway。选中 AD 组 允许对其 AD 组成员进行**批量身份验证**。（组成员必须先登录 Gateway Web 门户网站，然后才能在用户列表显示）
AD 服务器	选中包含目标 AD 用户或组的 AD 服务器。
账户	填写目标 AD 用户或组的 **sAMaccountName@ADDomainName（本地 AD 域名）**或**用户主体名称 （UPN）**。

分组	选择初始 Splashtop 组 AD 用户或 AD 组添加后将归入该组。
角色	用户可以被分到不同组中，分组可以有效管理用户/访问权限。
SOS 技术员	*SOS 技术员：启用 SOS 按需支持功能。（*基于订购方案）
验证	检查 AD 用户或组的可用性以进行身份验证。
添加	将经过验证的 AD 用户或组添加到目标组。

AD 组成员

绿色用户图标代表 AD 用户或 AD 组，如下图所示。如果已将 AD 组添加到 Splashtop Gateway，则表明与其关联的 AD 成员已经过身份验证，可以登录 Splashtop Gateway 以及 On-Prem 客户端应用程序。

AD 组成员中的 AD 用户将在使用其 AD 账户登录 Gateway 门户网站或客户端应用程序**至少一次**后在 AD 组成员中显示。而添加到 Gateway 的 **AD 个人用户**将立即显示并修改属性。

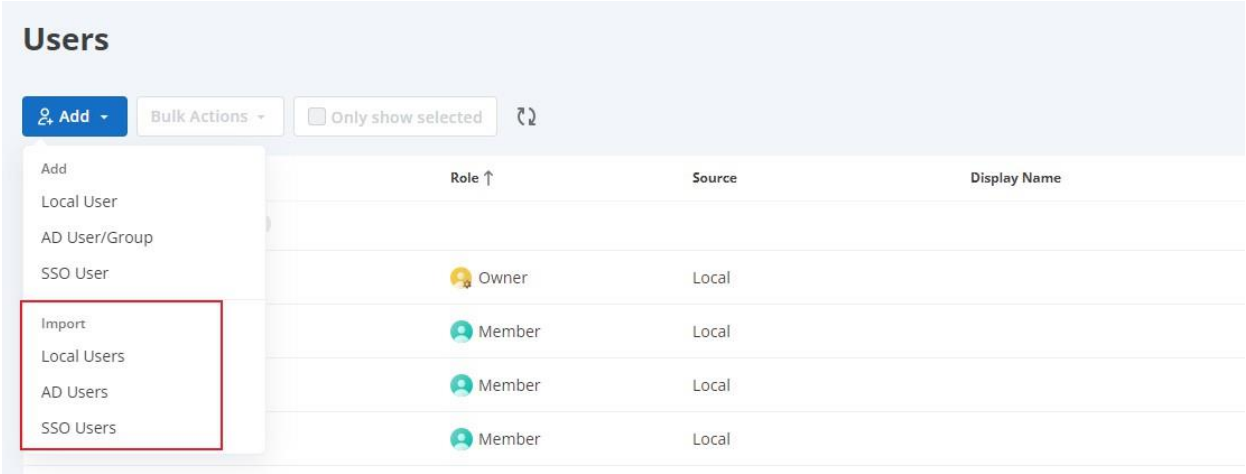


注意：通过父级 AD 组进行身份验证的 AD 账户将继承该组的用户角色和访问权限。

所有成功通过身份验证的 AD 用户都可以使用其 AD 凭据登录本地客户端应用程序，并使用 Splashtop 远程服务。

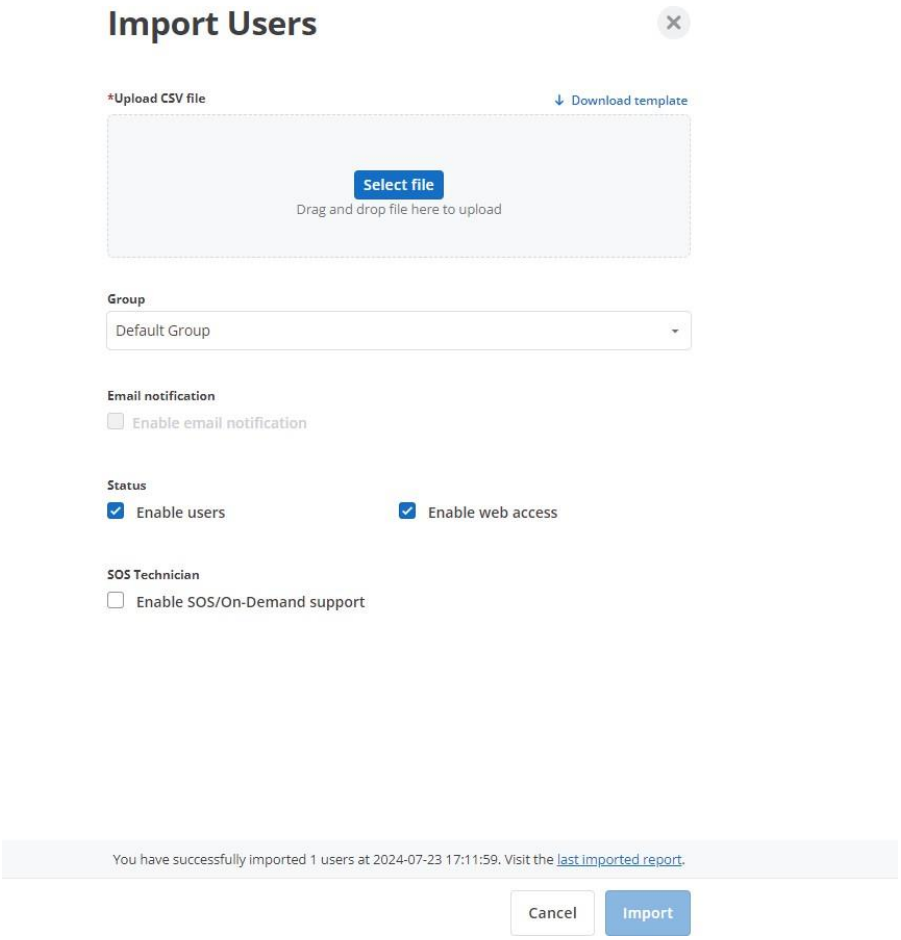
批量导入用户账户

通过批量导入，可以轻松将大量本地用户或 AD 个人用户导入到 Gateway，无需逐一添加。



导入本地用户

导入用户后，系统会为每个成功导入的本地用户账号分配一个有效期为7天的一次性密码。这些用户在重置其密码之前，将无法登录 Gateway 和 Splashtop On-Prem 应用程序。



下载 CSV 文件模板：使用 CSV 文件模板导入用户。

选择 CSV 文件：上传包含用户账户列表的 CSV 文件。

启用电子邮件通知：如果已配置 SMTP 服务器，则启用此复选框用户可以通过电子邮件接收账户和一次性密码。

状态：如果账户已启用，则用户可以建立远程会话；如果账户被禁用，则用户仍然可以访问 Web 门户网站，但远程会话被禁用。

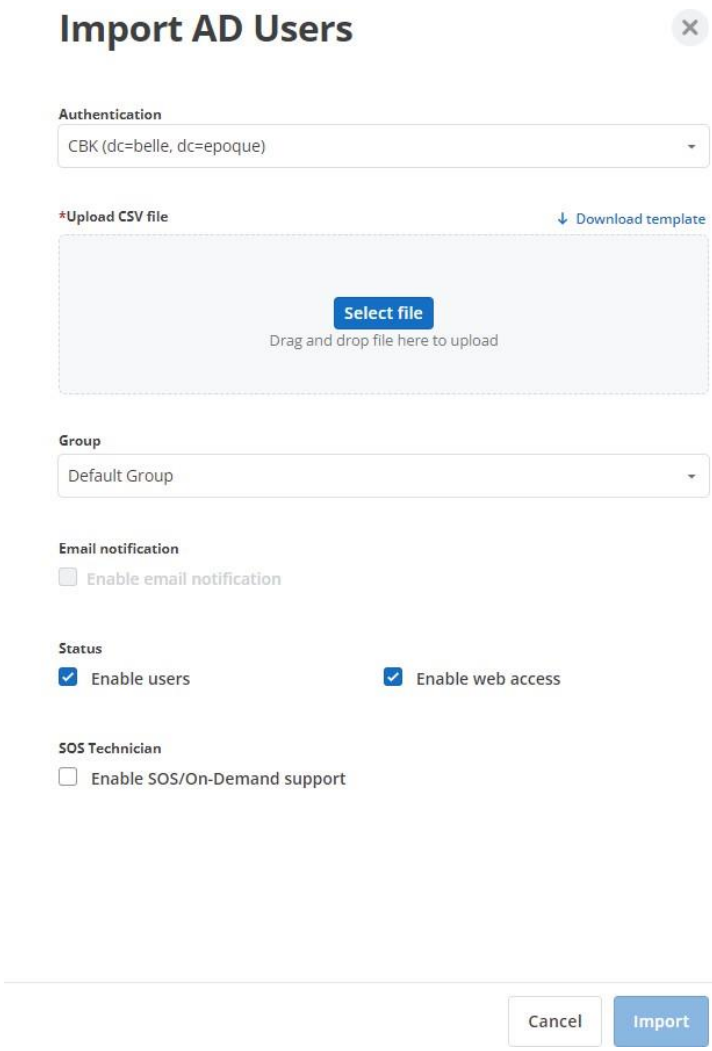
分组：用户可以被分到不同组中，分组在用户管理/访问权限方面非常有效。

SOS 技术员：启用 SOS 按需支持功能。

导入：将 CSV 文件中的本地用户导入到目标组。

导入 AD 用户

AD 服务器通过身份验证后，将出现在系统-活动目录选项卡的 AD 服务器列表中。导航到管理选项卡 – 用户，单击顶部的导入按钮，然后选择 AD 用户。所有成功通过身份验证的 AD 用户都可以使用其 AD 凭据登录 On-Prem 客户端应用程序，并使用 Splashtop 远程服务。



AD 服务器：选择包含目标 AD 用户的 AD 服务器。

下载 CSV 文件模板：使用 CSV 文件模板导入 AD 用户。

选择 CSV 文件：上传包含 AD 用户列表的 CSV 文件。

启用电子邮件通知：如果已配置 SMTP 服务器，则启用此选项用户可以通过电子邮件接收账户和一次性密码。

状态：如果账户已启用，则用户可以建立远程会话；如果账户被禁用，则用户仍然可以访问 Web 门户网站，但远程会话被禁用。

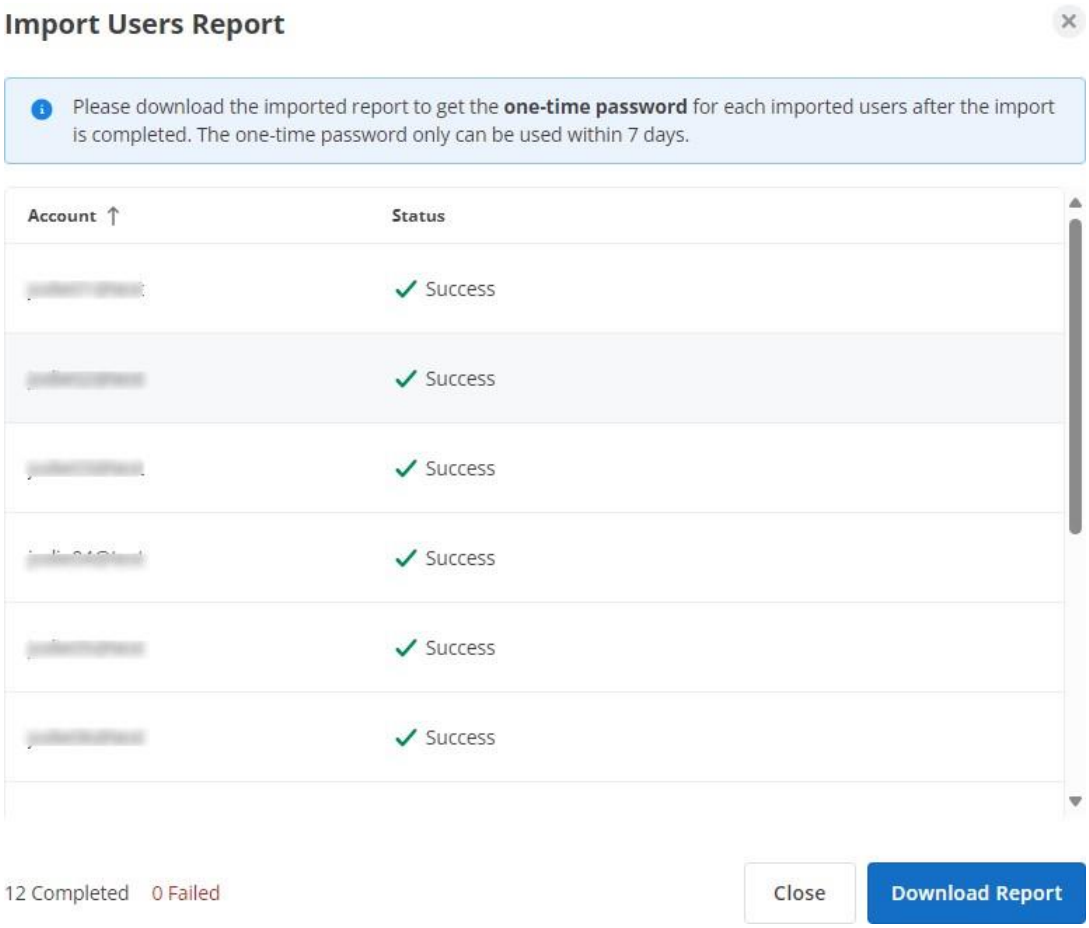
分组：用户可以被分到不同组中，分组在用户管理/访问权限方面非常有效。

SOS 技术员：启用 SOS 按需支持功能。

导入：将 CSV 文件中的 AD 用户导入到目标组。

导入的报告

用户导入完成后， **管理员**或**所有者** 可以查看导入结果并下载导入的报告。



重要说明

1. 仅支持 CSV 文件格式。
2. 文件中的数据必须遵循标准格式。可以下载下方的 example.csv 文件来检查布局/格式。
3. 在当前导入完成之前，您无法开始导入其他 CSV 文件。
4. 所有成功导入的用户都将获得成员角色。

设置访问权限

访问权限

访问权限确定哪些用户有权访问特定计算机。访问权限可以配置为：

- 没有电脑
- 所有电脑
- 仅其组中的电脑
- 仅基于组权限的电脑
- 仅特定电脑和电脑组

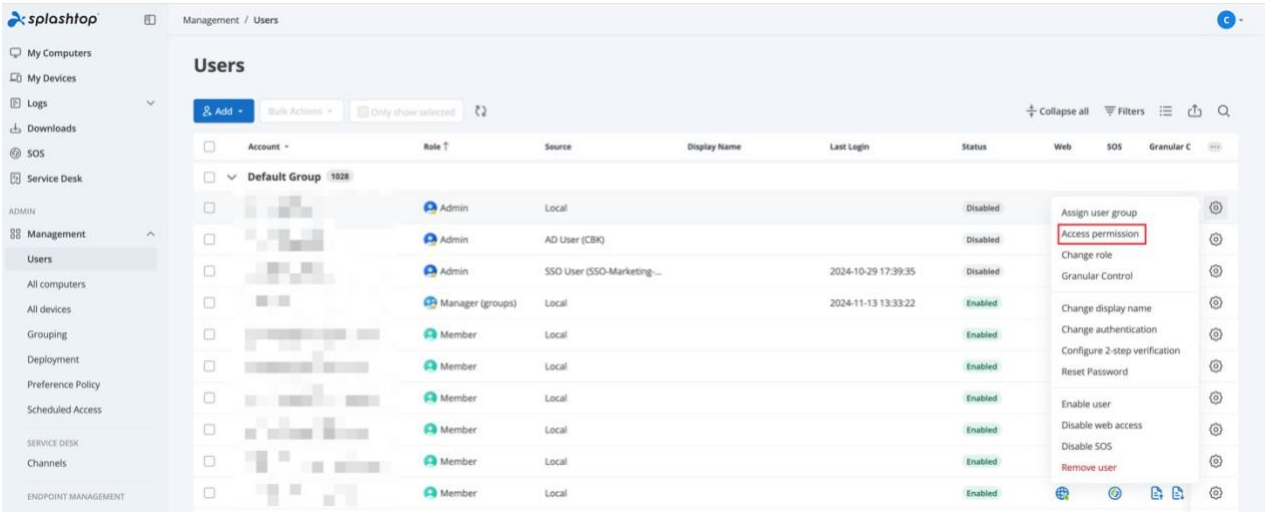
如何配置访问权限

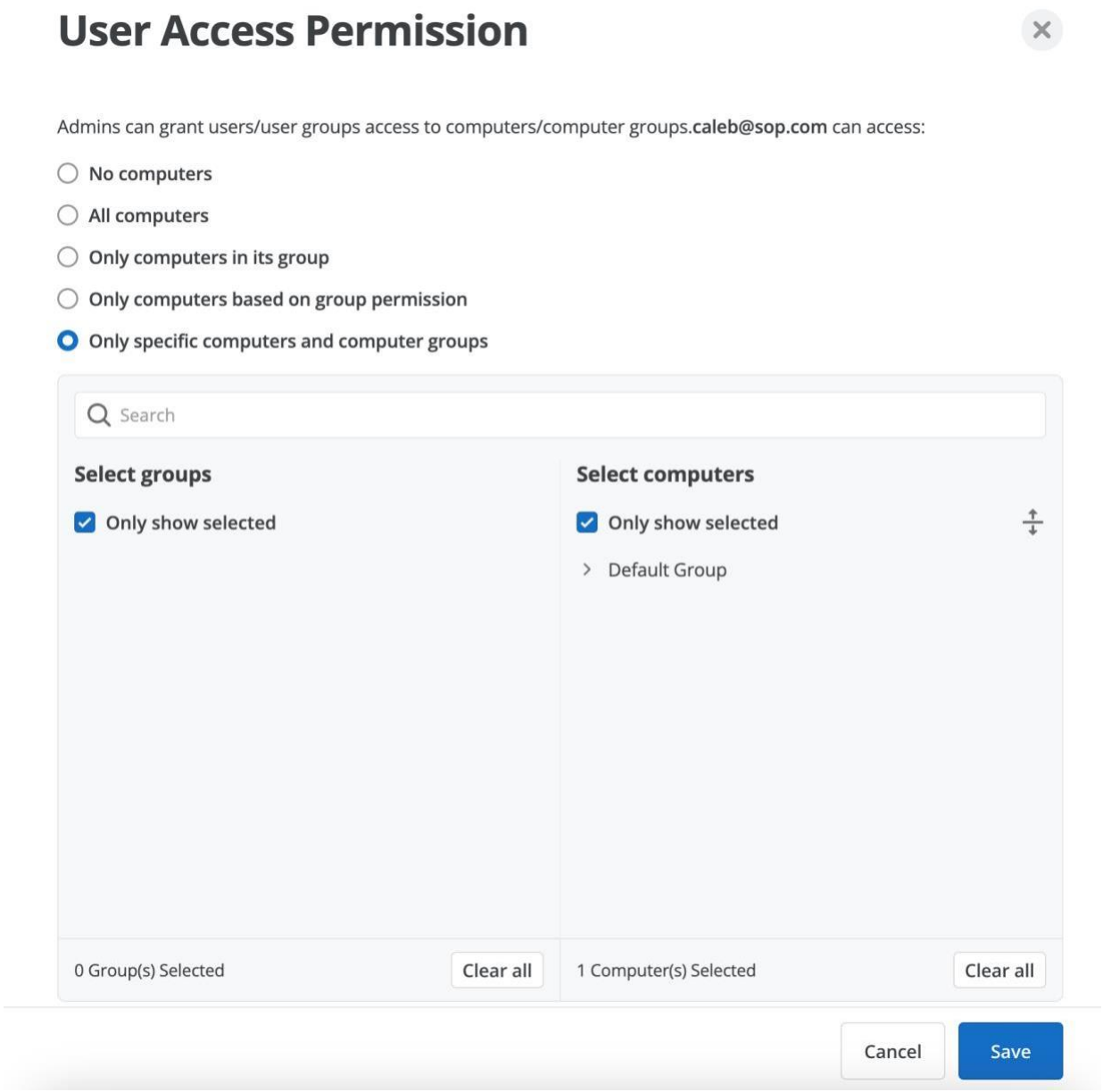
使用所有者或管理员账户登录 Gateway 网络控制台。

导航到 web/管理/管理页面，单击用户列表中每个用户旁边的齿轮图标，然后选择访问权限。然后即可设置此用户的访问权限。

用户访问权限

此外，还可以选择一个特定用户账户，并为该特定账户设置访问权限。即使已更改组权限设置，特定账户设置将覆盖任何组权限设置，除非将特定账户设置更改为跟随组访问设置。如果您希望每个最终用户只能访问其电脑，则可使用此选项。





访问权限选项

选项 1 - 无电脑

用户将无法访问任何电脑。此为新创建用户的默认选项。

选项 2 - 所有电脑

用户将能够访问所有电脑。

选项 3 - 仅组中的电脑

用户将能够访问分配到同一组的电脑。

选项 4 - 仅基于组访问权限的电脑

组访问权限包含：

- 无电脑（在此组中）
- 仅组中的电脑（在此组中）
- 仅特定电脑和电脑组（所有组）

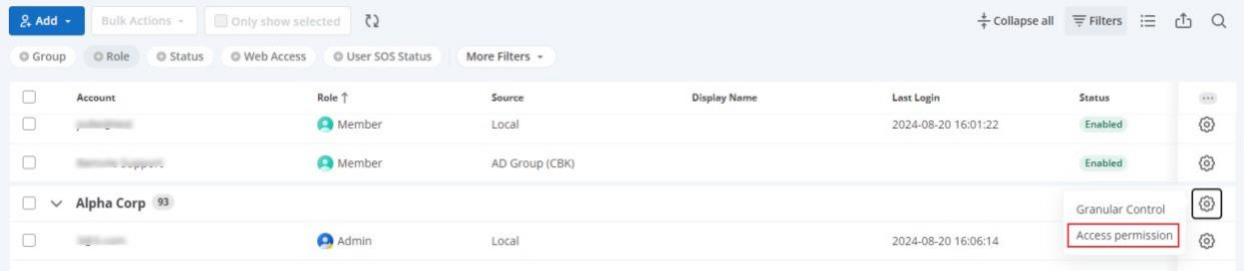
选项 5 - 仅特定电脑和电脑组

Splashtop 足够灵活，允许特定电脑或一组电脑与特定用户绑定。

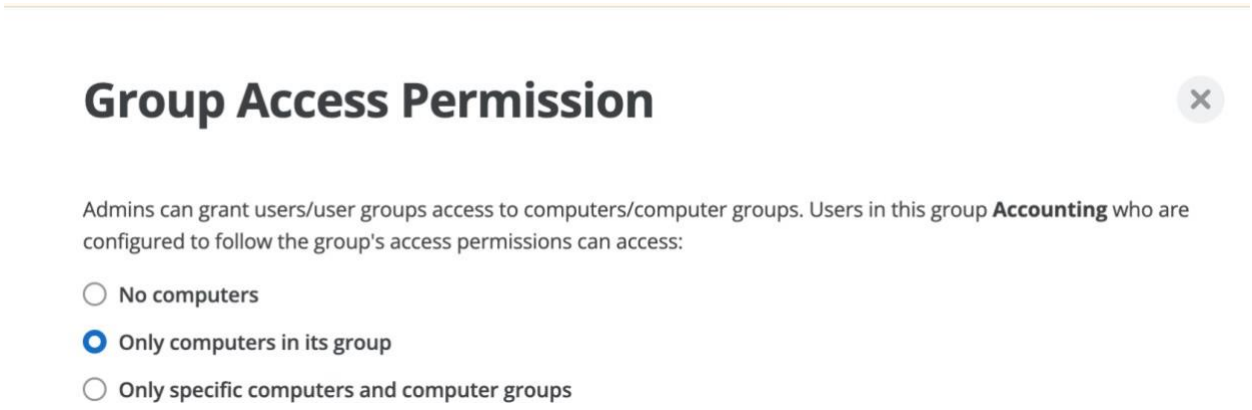
也就是说，用户可以通过精细化设置将其访问权限扩展到所有组。

组访问权限

如果您希望一组用户遵循相同的访问权限，则可创建一个组，将所有用户添加到该组，然后为该组设置访问权限。



默认情况下，用户将只能访问同一组中的电脑。您可以设置“仅特定...”以选择多组电脑或仅选择特定电脑。



通过 CSV 更新访问权限

CSV 上传功能允许管理员通过以下方式高效管理用户和组的访问权限：

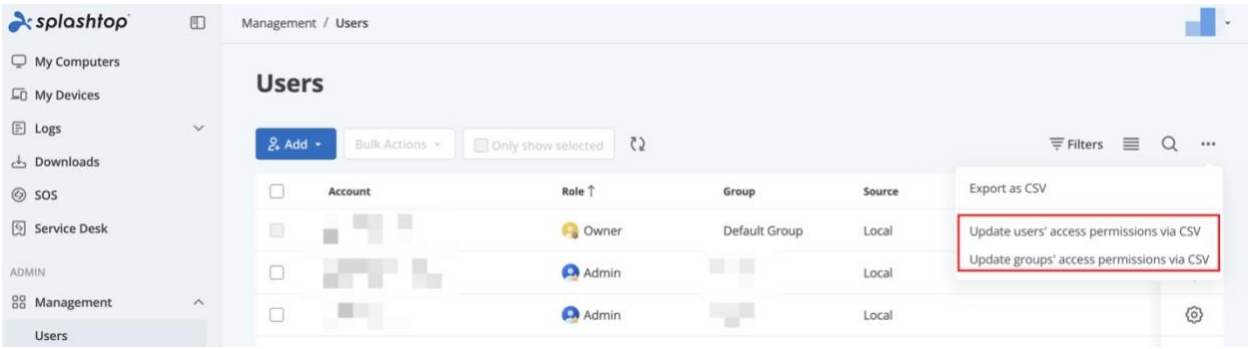
1. 将当前权限导出到 CSV 文件。
2. 编辑导出的文件以更新访问权限。
3. 重新上传已编辑的 CSV 文件以应用更改。

此功能支持批量更新、验证和详细报告，以确保权限管理的准确性。

如何更新访问权限

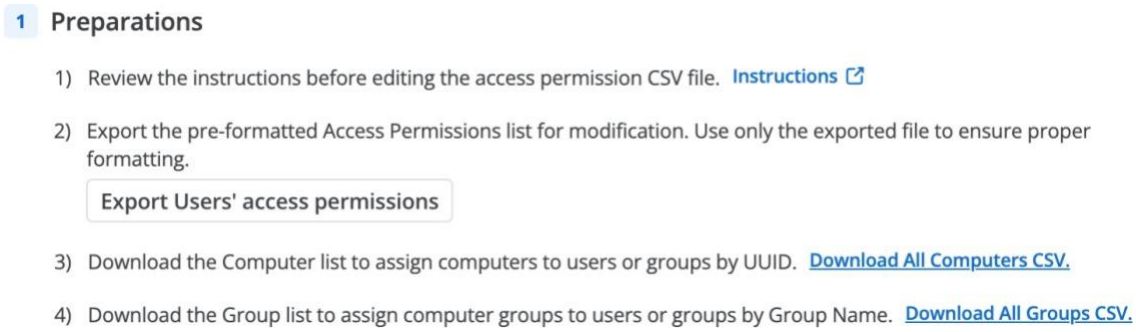
1. 访问 CSV 更新功能

- 导航到 Splashtop 网络控制台的**管理**页面。
- 根据需要，可选择**通过 CSV 更新用户的访问权限**或**通过 CSV 更新组的访问权限**。



2. 下载预先格式化的 CSV 文件

- 在**准备**步骤中，下载相关文件：
  - **用户访问权限 CSV**
  - **所有电脑 CSV**
  - **所有组 CSV**
- 通过以上文件可确保在编辑权限时采用正确的格式和引用。

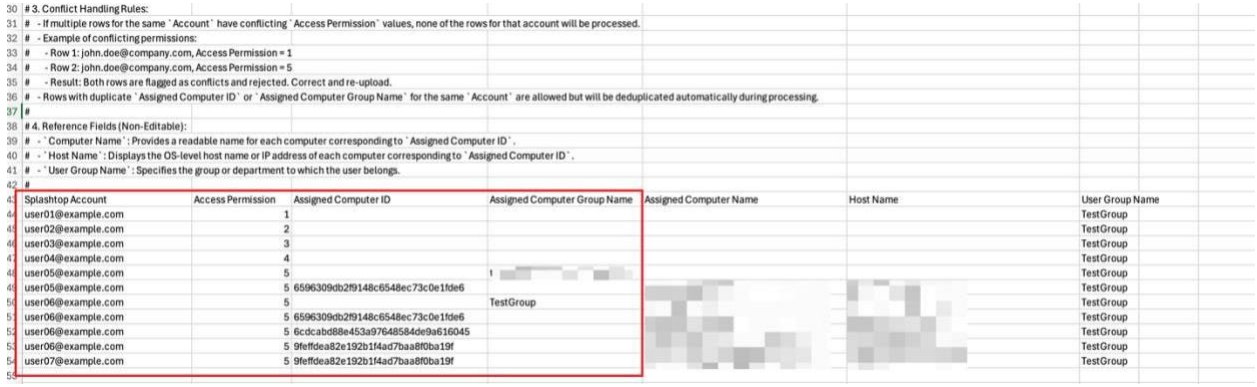


3.编辑 CSV 文件

- 使用电子表格编辑器打开下载的 CSV 文件。
- 根据需要更新以下字段：
  - **访问权限**：根据访问类型设置值（1-5）。
  - **分配的电脑 ID** 和**分配的电脑组名**：指定电脑或组的唯一标识符（如果访问权限值=5）。

验证规则：

- 确保同一账户不存在冲突的权限。
- 遵循每个字段的预定义格式。

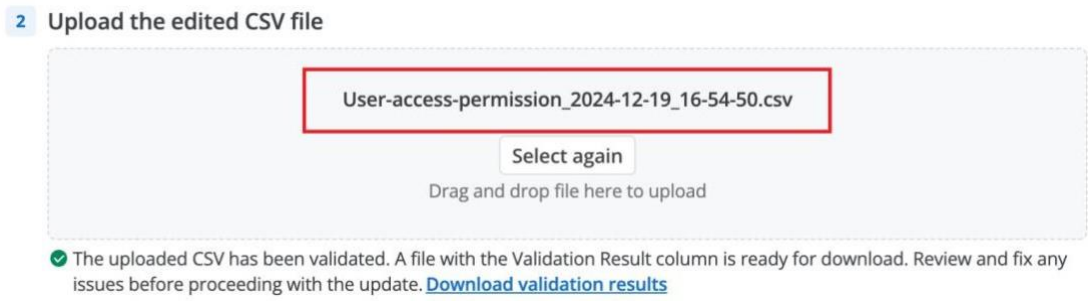


```
# 3. Conflict Handling Rules:
#  - If multiple rows for the same `Account` have conflicting `Access Permission` values, none of the rows for that account will be processed.
#  - Example of conflicting permissions:
#      - Row 1: john.doe@company.com, Access Permission = 1
#      - Row 2: john.doe@company.com, Access Permission = 5
#      - Result: Both rows are flagged as conflicts and rejected. Correct and re-upload.
#  - Rows with duplicate `Assigned Computer ID` or `Assigned Computer Group Name` for the same `Account` are allowed but will be deduplicated automatically during processing.
#
# 4. Reference Fields (Non-Editable):
#  - `Computer Name`: Provides a readable name for each computer corresponding to `Assigned Computer ID`.
#  - `Host Name`: Displays the OS-level host name or IP address of each computer corresponding to `Assigned Computer ID`.
#  - `User Group Name`: Specifies the group or department to which the user belongs.
#
```

Splashtop Account	Access Permission	Assigned Computer ID	Assigned Computer Group Name	Assigned Computer Name	Host Name	User Group Name
user01@example.com	1					TestGroup
user02@example.com	2					TestGroup
user03@example.com	3					TestGroup
user04@example.com	4					TestGroup
user05@example.com	5					TestGroup
user05@example.com	5	6596309db2f9148c6548ec73c0e1fde6				TestGroup
user06@example.com	5		TestGroup			TestGroup
user06@example.com	5	6596309db2f9148c6548ec73c0e1fde6				TestGroup
user06@example.com	5	6cdcabd88e453a97648584de9a616045				TestGroup
user06@example.com	5	9feffdea82e192b1f4ad7baa8f0ba19f				TestGroup
user07@example.com	5	9feffdea82e192b1f4ad7baa8f0ba19f				TestGroup

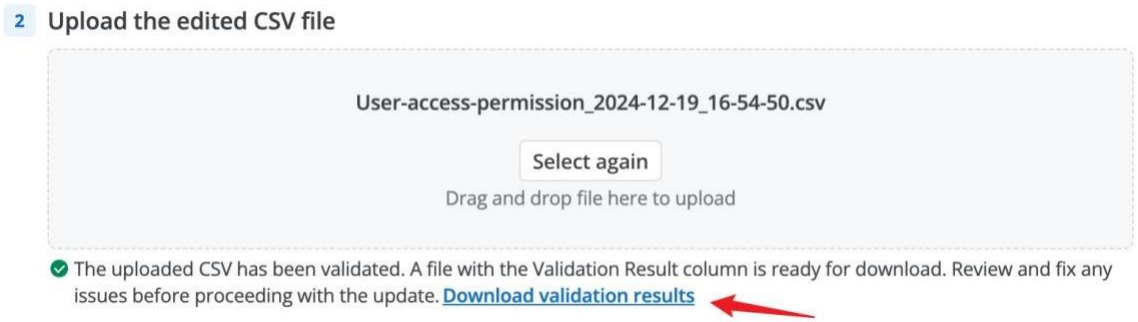
4.上传已编辑的 CSV 文件

- 将编辑后的文件拖放到**上传 CSV 文件**页面的上传区域或使用文件选择器。
- 系统将自动验证文件并生成预验证报告。



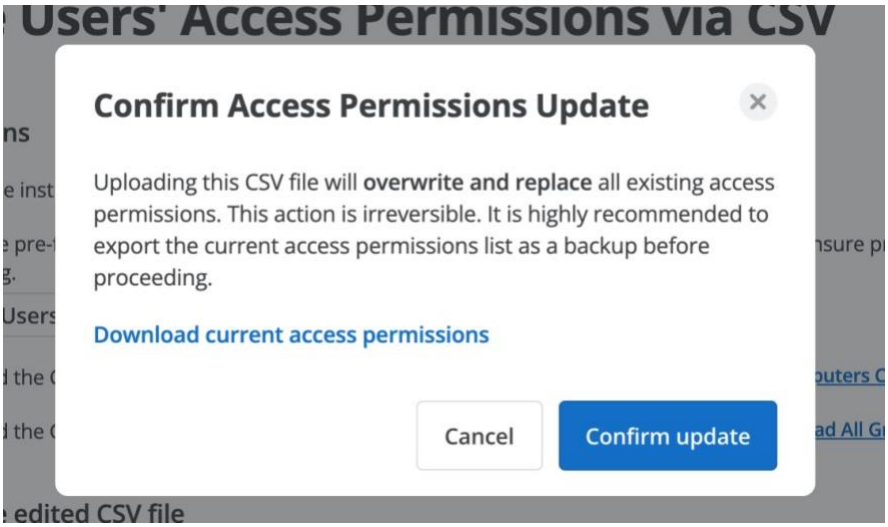
5.检查验证结果

- 下载验证报告以检查错误。
- 修改报告中突出显示的任何问题，并重新上传修改后的文件。



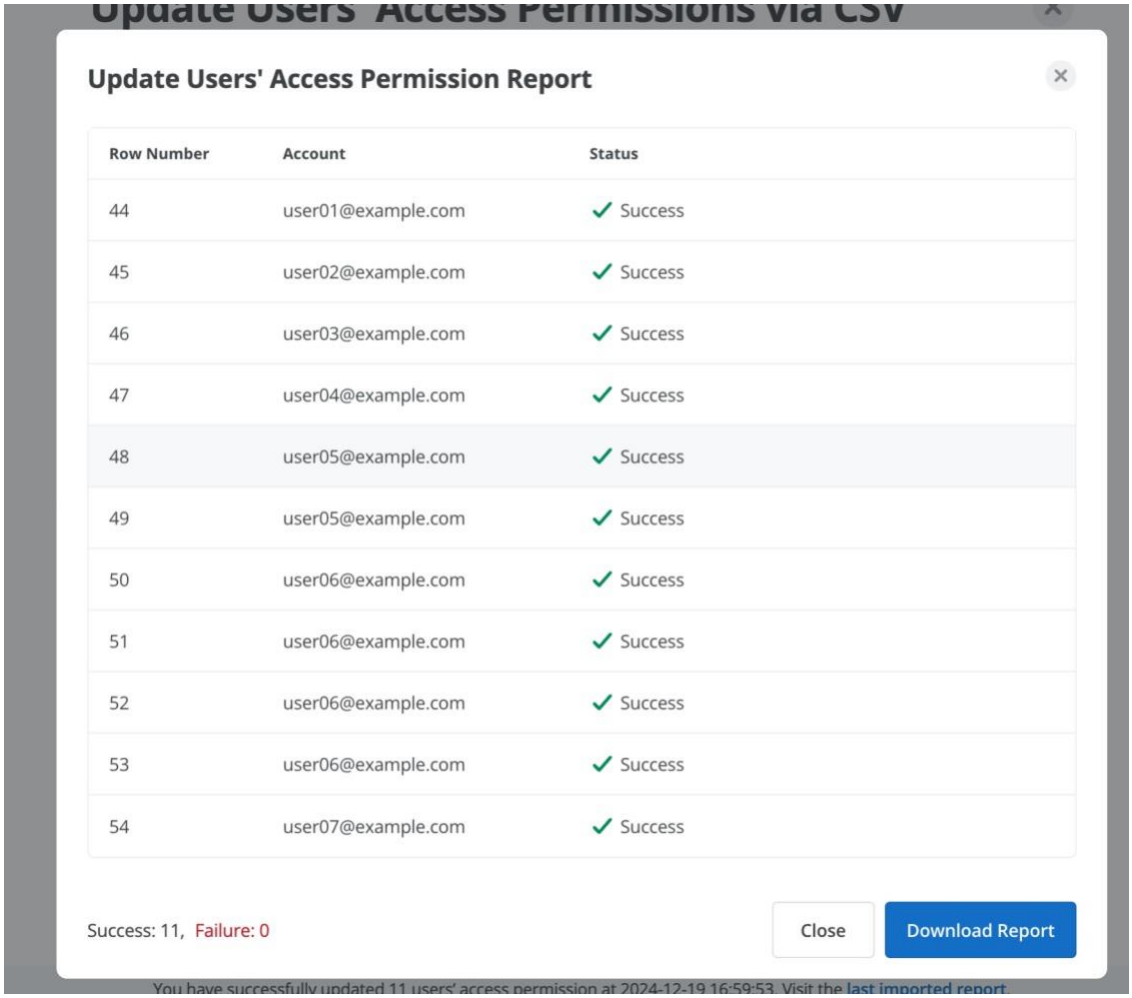
6. 确认并应用更新

- 文件通过验证后，单击**更新**按钮。
- 将弹出确认对话框：
  - 查看变更摘要。
  - 确认更新以继续。



7. 检查更新摘要

- 更新后，系统将显示操作的详细摘要：
  - 成功更新的数量
  - 发生的错误（如果有）
- 下载更新报告存档。



最佳实践

- 更改前始终导出并备份当前权限。
- 使用预先格式化的 CSV 文件以最大限度地减少错误。
- 应用更新前完全验证文件。

常见问题疑难解答

1. **文件验证错误：**
    - 检查是否缺少或格式不正确的列。
    - 确保文件采用 UTF-8 编码。
2. **权限冲突：**
    - 通过确保每个用户/组每行仅有一个权限类型以避免冲突。

3. 超过文件大小/行限制：

- 将文件拆分为更小的部分或使用过滤器以减少数据集。

精细功能控制

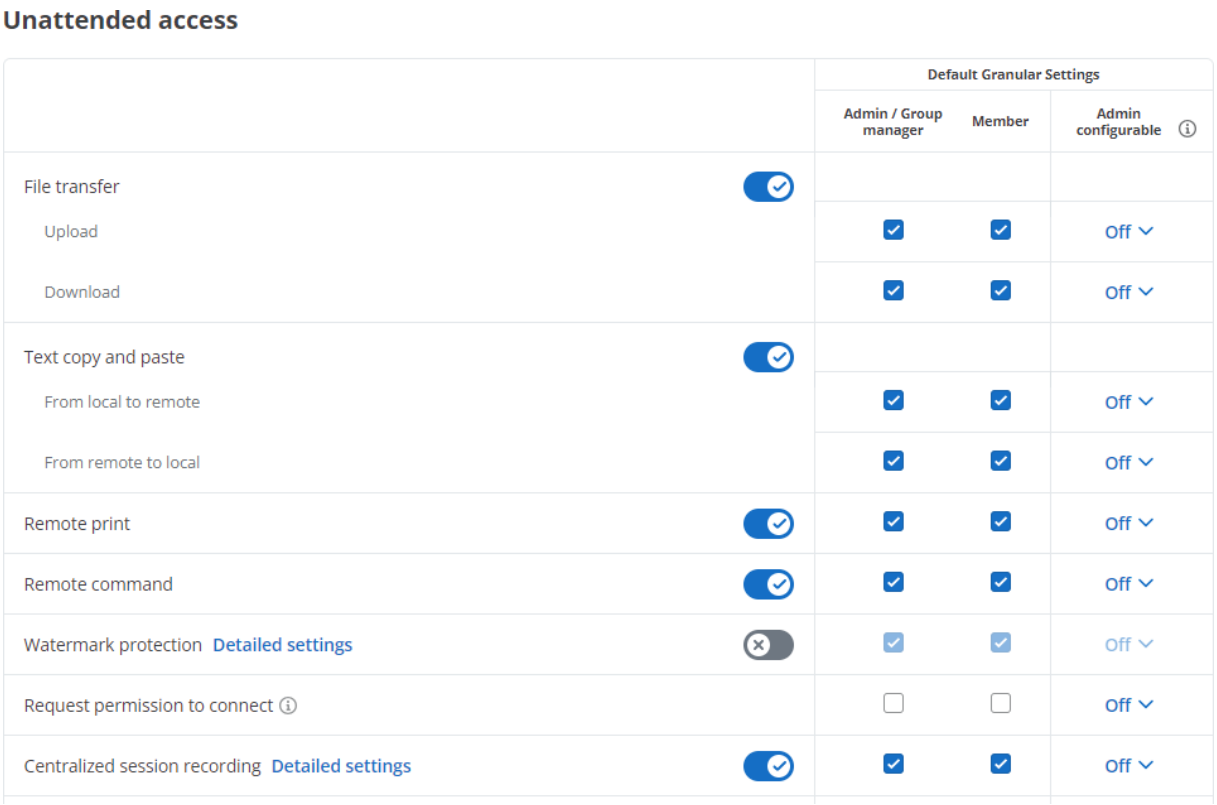
借助精细控制，可以更好地管理团队中的功能，并将某些功能设置为仅特定用户或特定用户组可用。

详细说明：

- Splashtop On-Prem 现可通过精细控制来指定团队中的特定成员使用文件传输、复制粘贴、远程打印、远程命令、水印保护、远程控制和两步验证功能。

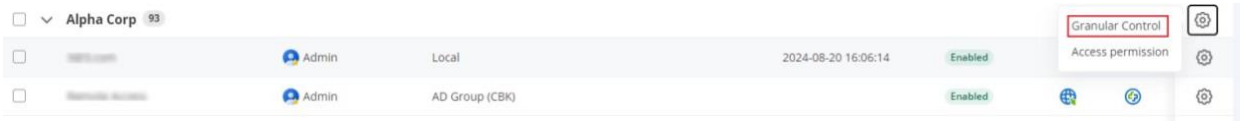
默认精细设置

- 团队所有者可以为每个用户角色配置默认功能权限，方法：**设置 → 团队设置 → 默认精细设置**。此操作可以确定用户被邀请加入团队时的默认有人值守访问权限（即，如果在有人值守访问权限旁边的默认精细设置下选中所有者和管理员，则用户在首次加入团队时将默认具有有人值守访问权限）。
- **可由管理员配置**：选择此选项将允许管理员/组管理员为特定功能配置成员权限。

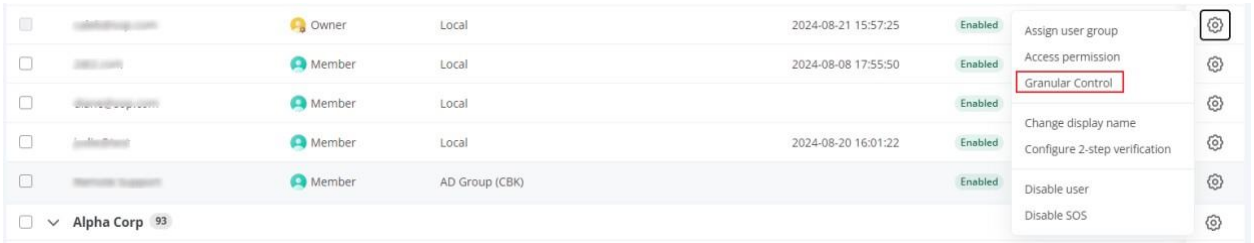


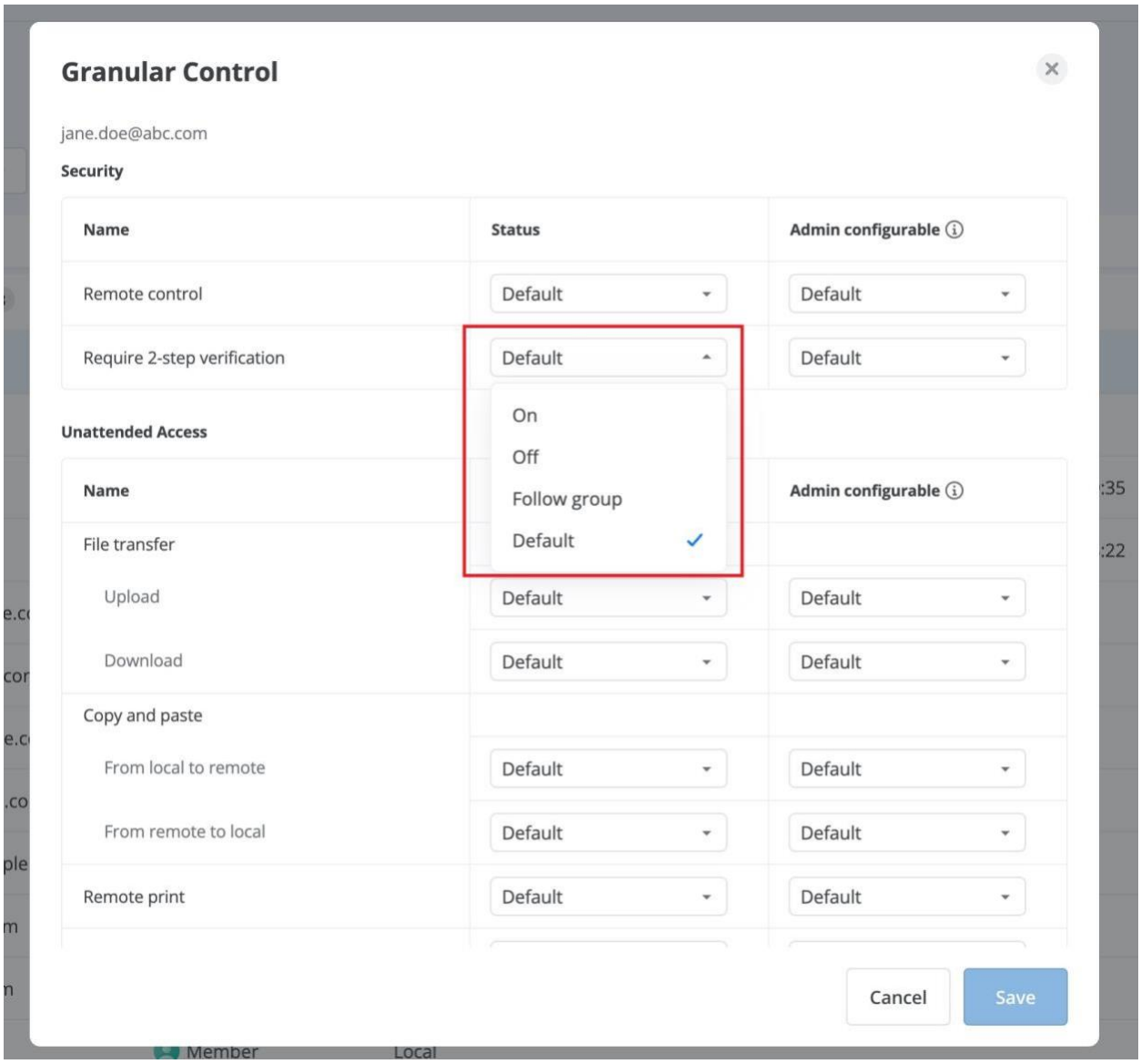
用户精细设置

在**管理** → **用户**页面还可以为每个组配置精细控制。单击组名右侧的齿轮按钮，然后单击**精细控制**。



要为每个用户配置此项，可单击用户名旁边的齿轮按钮，然后单击**精细控制**。

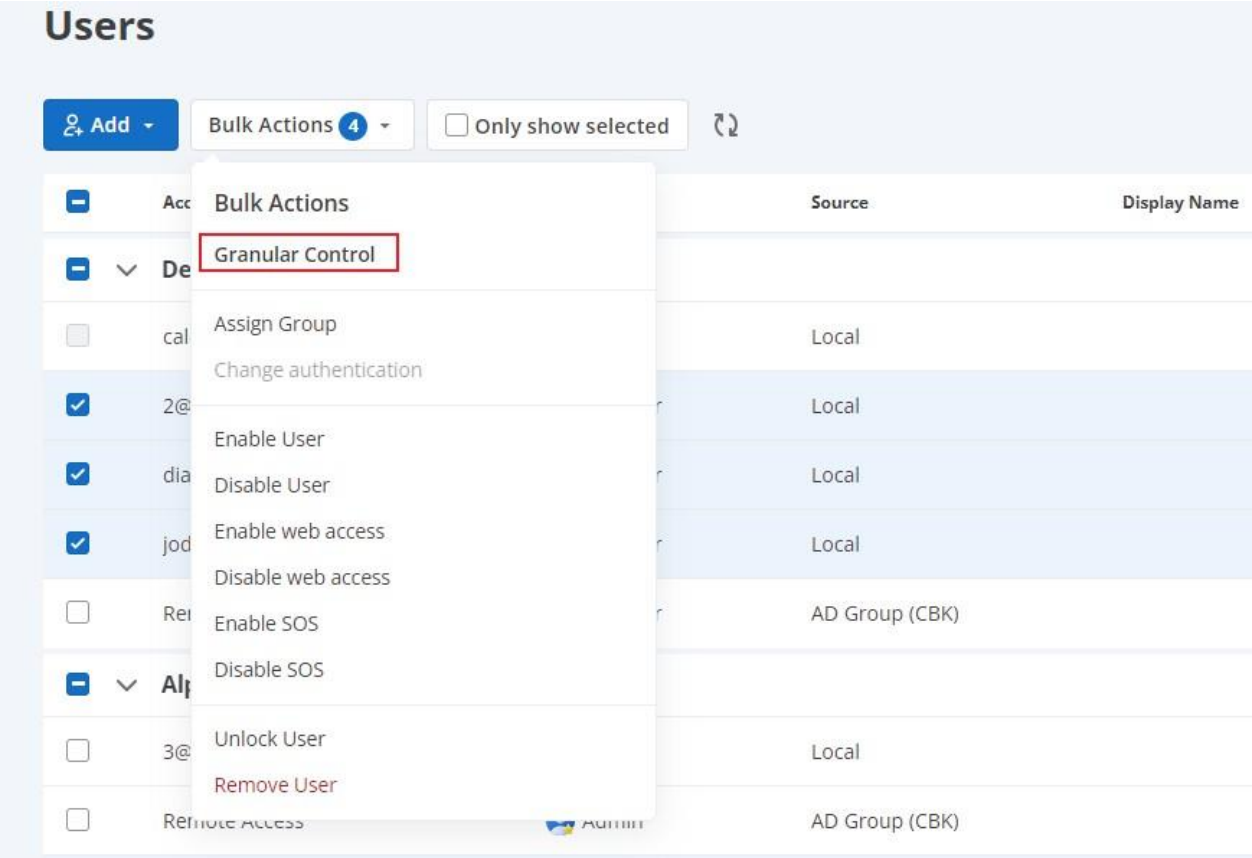


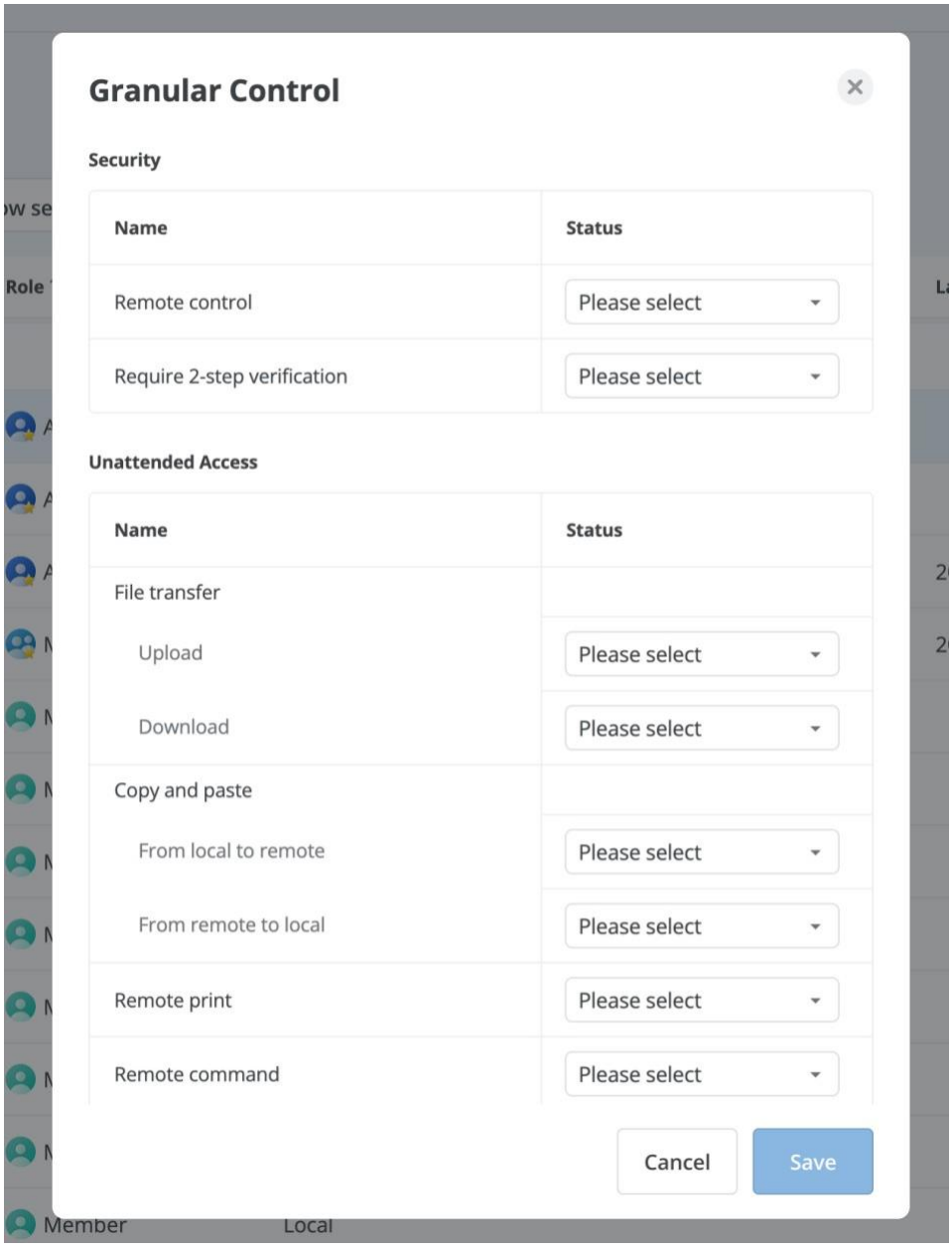


- **开**：此用户将有权访问所选功能。
- **关**：此用户将无权访问所选功能。
- **跟随组**：选择此选项将遵循组的精细设置。要设置用户组精细设置，可单击组名旁边的齿轮按钮，然后选择“**精细控制**”。
  - 调整组设置时，可以将整个组的此选项配置为开/关 或跟随团队默认设置。
- **默认**：选择此选项将遵循默认精细设置，位于**设置 → 团队设置 → 默认精细设置**

批量操作

- 在**管理** → **用户**页面，还可以通过批量操作配置精细控制。
- 通过单击账户左侧的复选框来选择账户。然后单击批量操作按钮，为所选账户配置精细控制项。
- 点击保存按钮保存设置。





设置管理员权限

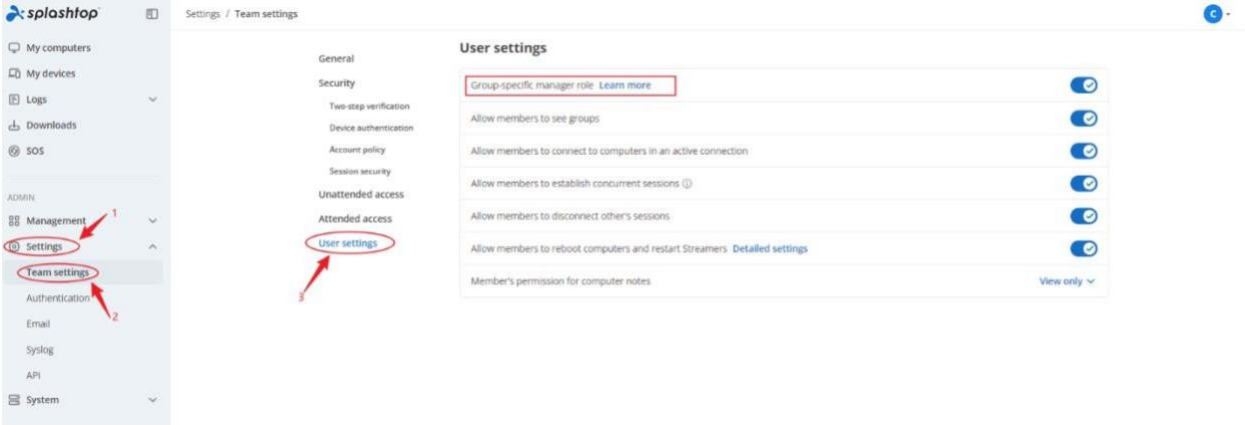
默认情况下， Splashtop On-Prem 管理员用户可以远程访问和管理所有电脑。

有时可为用户授予管理员权限，但仅允许其访问部分电脑。此选项允许用户执行添加电脑、删除电脑、创建用户等操作，**但仅限于已被授权的组。**

请参阅以下说明以启用和使用该功能。

启用组特定的管理器功能

以团队所有者身份登录 Splashtop Gateway。导航到**设置 > 团队设置 > 用户设置**。启用组特定的管理员角色。

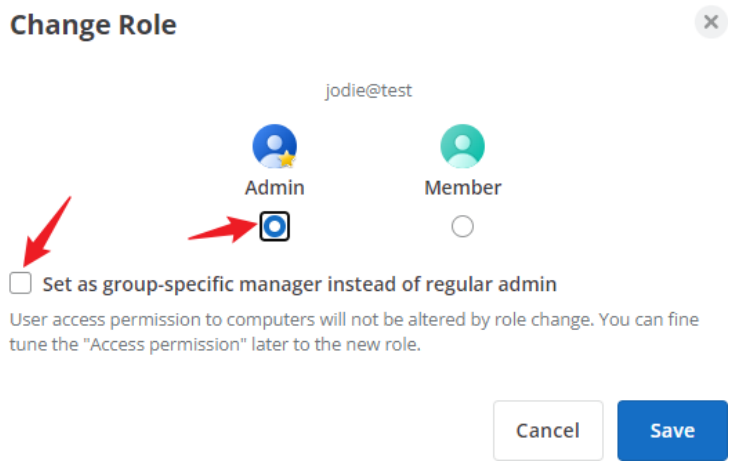


将用户设置为组特定的管理员

导航到**管理 > 用户**页面，在要将其设置为特定组管理员的用户旁点击齿轮图标。点击更改角色。

在弹出的对话框：

1. 选择“管理员”单选按钮
2. 勾选“设置为特定组管理员”复选框
3. 勾选相应的复选框，以选择您希望此用户管理的组

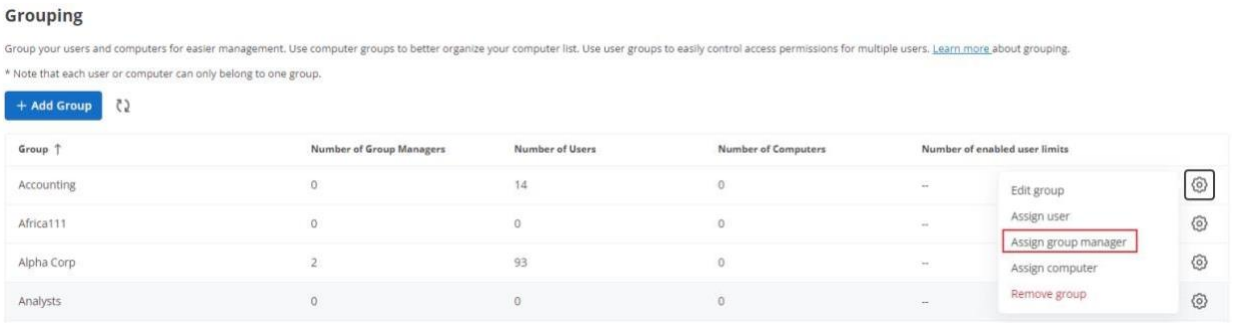


分配特定组管理员的其他方法

还可以从**分组**页面分配特定组管理员。

导航到**管理** > **分组**。在要为其设置组管理员的组旁边点击齿轮图标。点击 “分配组管理员”。

在弹出的对话框中可以选择哪些用户可以管理此组。



特定组管理员权限

特定组管理员只能在其管理的组的用户和电脑上执行这些功能。特定组管理员**无法**查看其他组的组名、用户和电脑。

- 重命名电脑
- 添加/编辑电脑注释

- 添加/删除电脑，包括创建部署套件
- 创建/启用/禁用/删除用户
- 设置访问权限
- 配置用户的 2FA（又名 MFA）和可信设备

注意：

- 管理员被分配为特定组管理员时，其管理范围将从整个团队缩小到仅特定组。
- 导航到**管理 > 用户**页面可以随时查看已为哪些用户分配了特定组管理员权限。这些用户的角色将被标记为“管理员（组）”。将鼠标悬停在标签上可以查看用户管理的组列表。
- 从 Gateway Web 门户网站删除相关组时，特定组管理员角色将更改为**成员**。

从用户列表为 AD 组成员启用 SOS

从 Gateway v3.20.0 开始，用户视图可一次显示 AD 组的所有成员。

将视图列表从组视图切换到用户视图，可以为 AD 组成员启用或禁用 SOS。

注意：AD 组成员可以同时存在于不同 AD 组中，因此 AD 组成员的精细控制设置是所属的多个 AD 组的合并结果，不支持直接从单个 AD 组成员配置精细控制设置项。

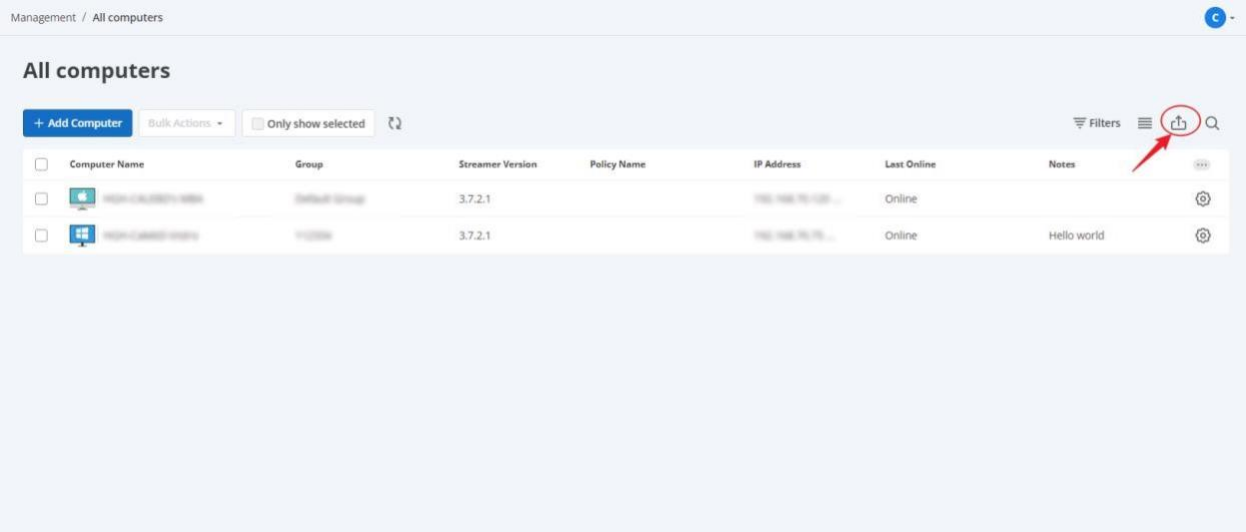
导出用户列表或访问权限列表

管理团队中的多个用户时，可能需要导出用户列表或访问权限以维护记录。用户列表和访问权限可以导出为 CSV 文件。

所需的 Gateway 版本为 v3.28.2 或更高。

登录到 Gateway Web 门户网站，单击**管理选项卡**，然后单击**用户**按钮。

单击导出图标，再单击下拉列表中的选项，则可将用户列表、用户访问权限或组访问权限下载为 CSV 文件。



用户列表的 CSV 文件包括账户、组名、状态、角色等。

	A	B	C	D	E	F
1	Splashtop Account	Group	Status (setting)	Status (result)	Source	Role
2		Default Group	enabled	enabled	Local	owner
3		a	enabled	enabled	Local	group_manager
4		c	enabled	enabled	Local	admin
5		Default Group	enabled	enabled	Local	member
6		b	enabled	enabled	Ad Group(	admin
7		Default Group	enabled	invalid	Ad Group	member

用户访问权限的 CSV 文件包括账户、角色、状态、用户组名、访问权限等。

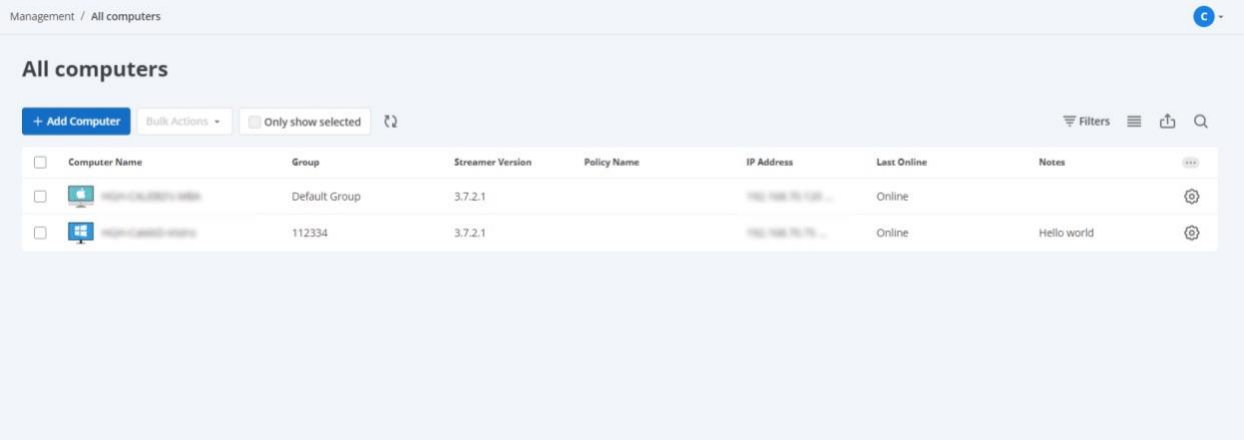
	A	B	C	D	E
1	Splashtop Account	Role	Status	User Group	Access Permission
2		admin	enabled	c	All computers
3		member	enabled	Default Group	No computers
4		admin	enabled	b	All computers
5		owner	enabled	Default Group	All computers
6		group_manager	enabled	a	All computers

组访问权限的 CSV 文件包括组名称、访问权限、电脑名称、电脑组等。

	A	B	C	D	E	F	G
1	Computer Name	Host Name	UUID	Type	Pool Size	Group Name	Operating System
2	rds - 2	rds - 2		RDP		Default Group	Microsoft Windows
3	rdp	rdp		RDP		Default Group	Microsoft Windows
4	rds - 1	rds - 1		RDP		Default Group	Microsoft Windows
5	rdspool	rdspool		RDS pool	2	Default Group	
6	Macmini	Macmini		Computer		Default Group	macOS Ventura 13.3.1

电脑

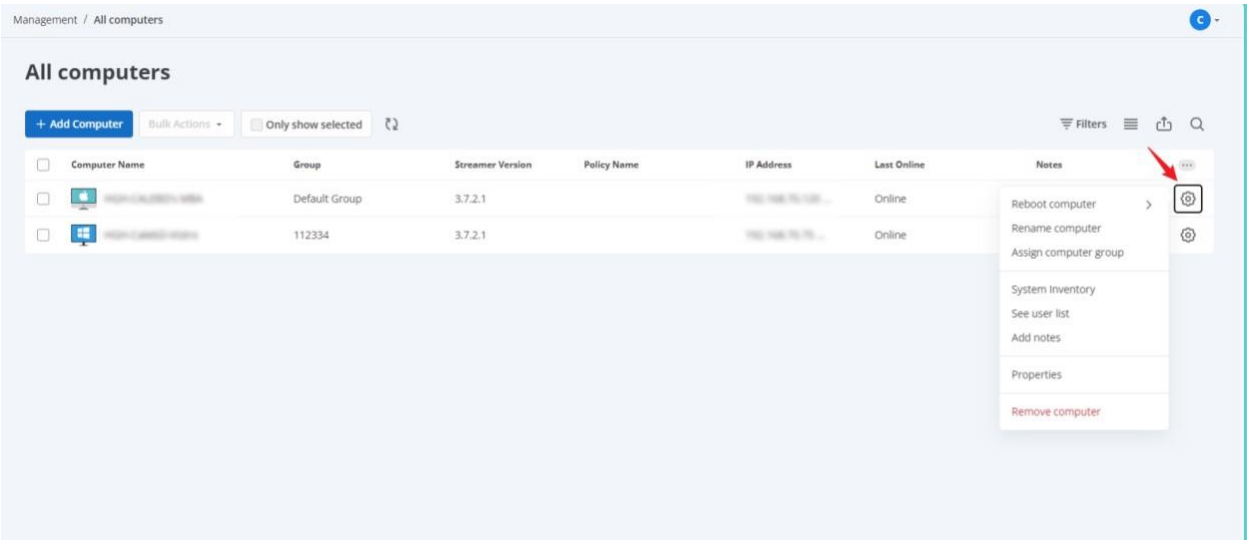
在**所有电脑**页面，管理员可以查看通过 Splashtop Gateway 注册的电脑。一台电脑在应用部署套件或手动安装 Streamer 并授予访问权限后，将在 Gateway 中被视为“已注册”。



可以选择在列表视图或组视图中显示电脑，也可以选择仅显示特定电脑组。

管理特定电脑

管理员可以通过单击特定电脑行末尾的齿轮图标来远程管理该电脑。

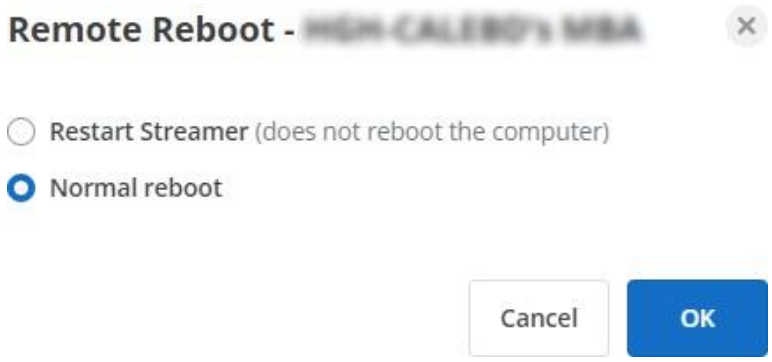


功能包括：

- 重启电脑
- 删除电脑
- 重命名电脑
- 分配电脑组
- 添加注释
- 系统清单
- 查看用户列表
- 查看属性

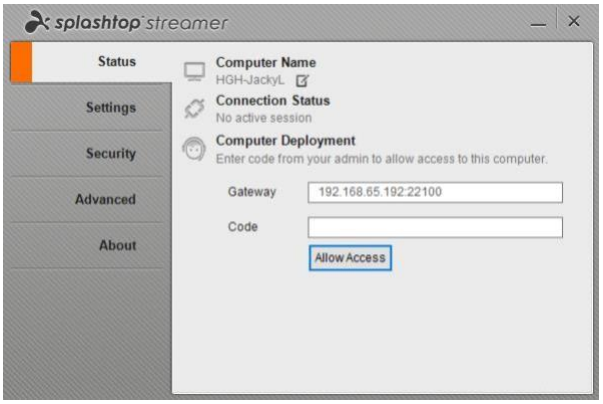
重启电脑

管理员可以远程重启 Streamer，执行常规的电脑重启或使用网络的安全模式重启。



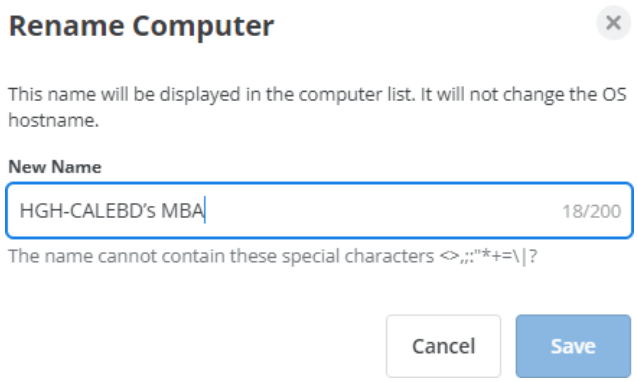
删除电脑

管理员可以通过注销 Streamer 从 Gateway 中删除电脑。删除电脑后，该电脑的 Streamer 必须使用部署码重新授予访问权限，才能在系统中再次注册。



重命名电脑

管理员可以为电脑分配自定义名称。



分配电脑组

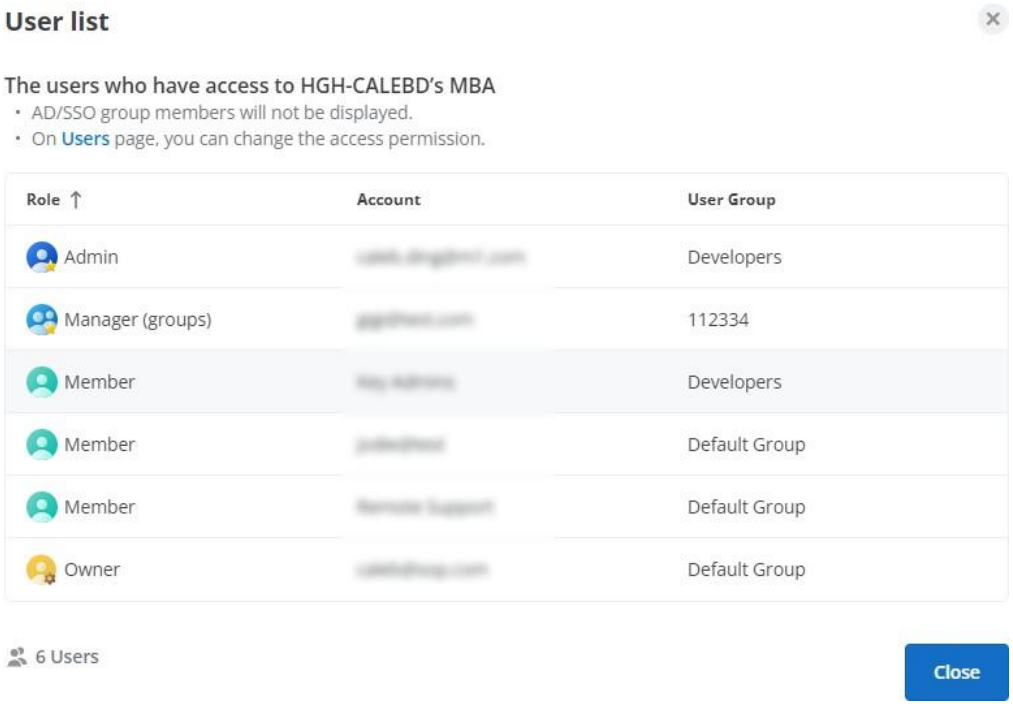
管理员可以将电脑分配到组中以继承该组的访问权限。

添加注释

注释字段可用于为电脑添加描述。

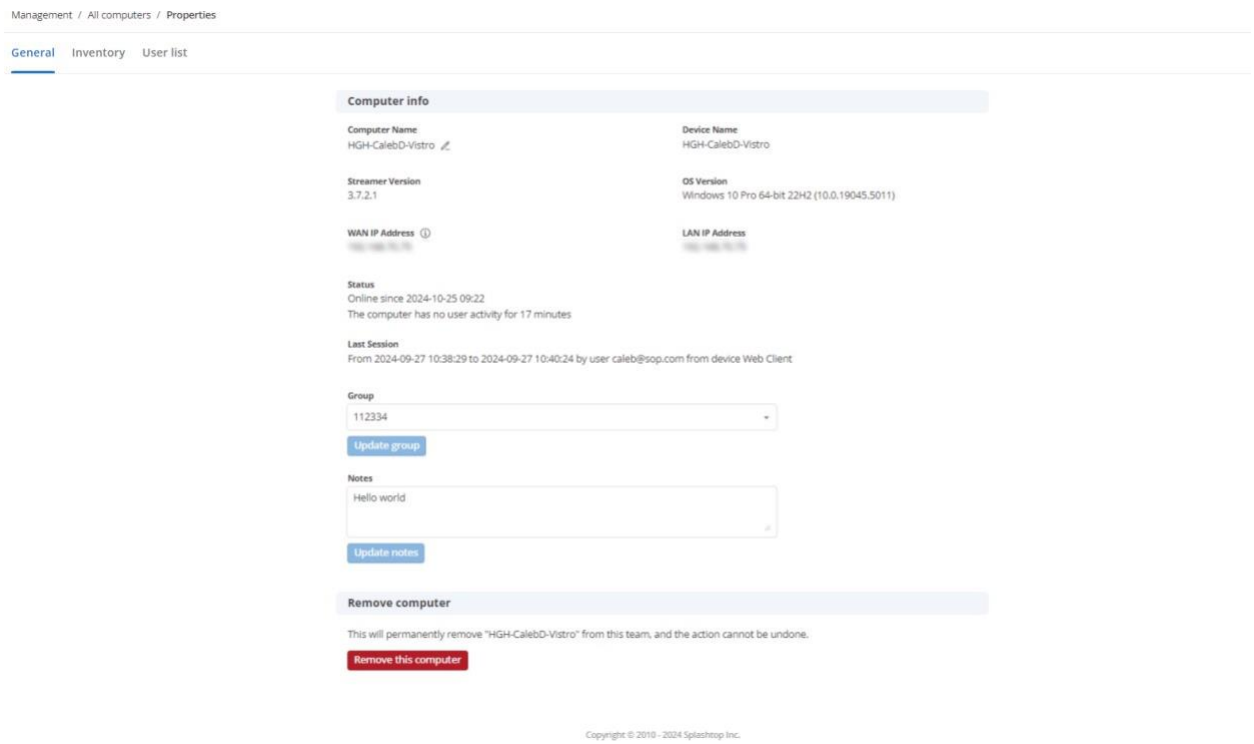
查看用户列表

管理员可以查看有权访问此电脑的用户列表。



查看属性

此页面显示电脑的属性。



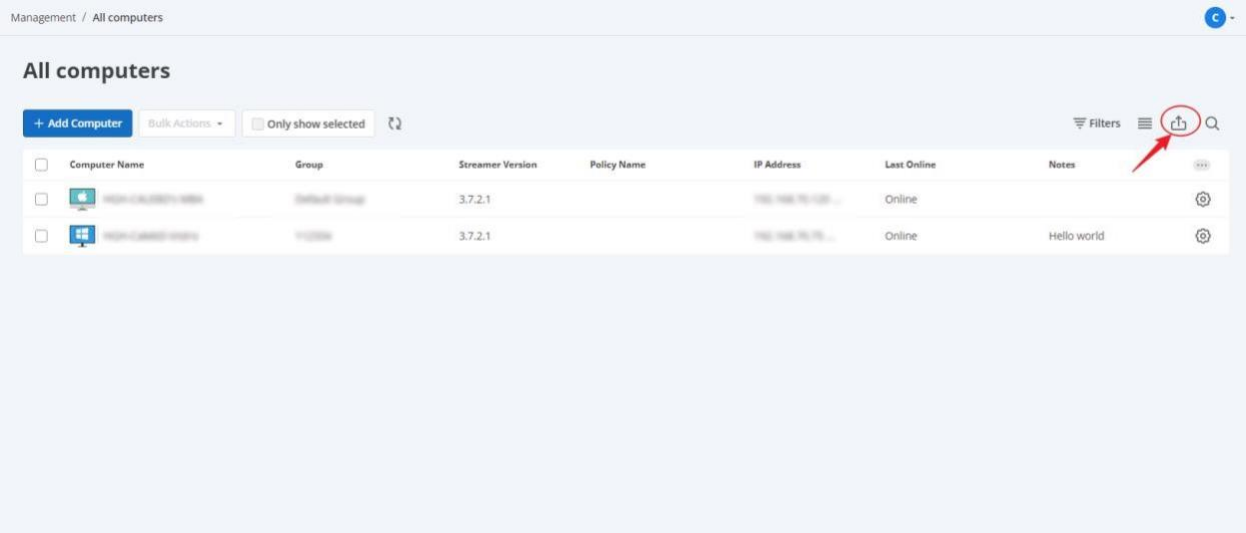
导出并保存电脑列表的副本/记录

管理团队中的多台电脑时，可能希望导出电脑列表以维护记录。电脑列表可以导出为 CSV 文件。电脑列表的 CSV 文件包括电脑名称、主机名、组名、操作系统等。

所需的 Gateway 版本为 v3.28.2 或更高。

登录到 Gateway Web 门户网站，然后单击**管理**选项卡，然后单击**所有电脑**按钮。

单击**导出**图标，可以将电脑列表下载为 CSV 文件。



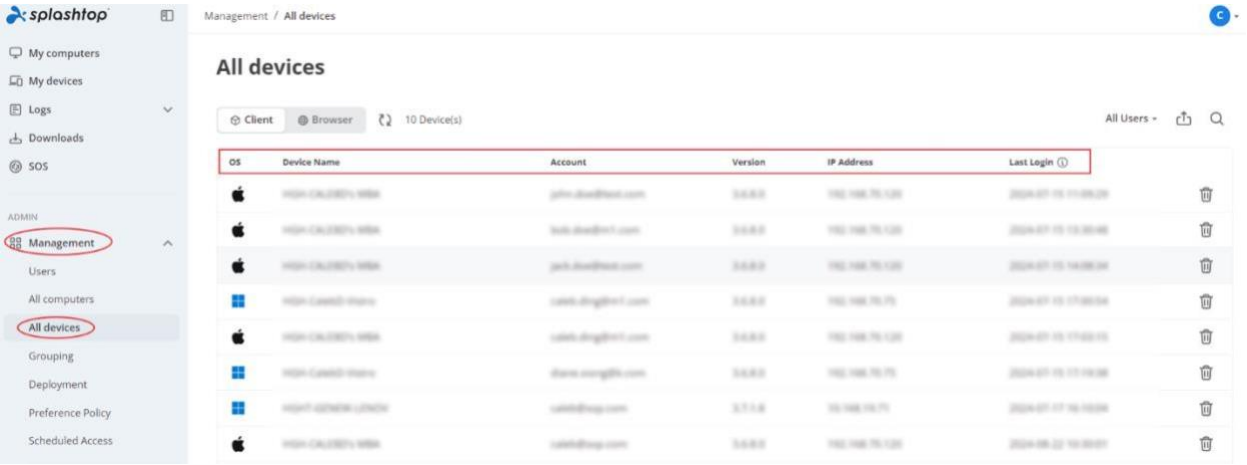
CSV 文件包括电脑名称、主机名、组名、操作系统等。

	A	B	C	D	E	F	G
1	Computer Name	Host Name	UUID	Type	Pool Size	Group Name	Operating System
2	rds - 2	rds - 2		RDP		Default Group	Microsoft Windows
3	rdp	rdp		RDP		Default Group	Microsoft Windows
4	rds - 1	rds - 1		RDP		Default Group	Microsoft Windows
5	rdspool	rdspool		RDS pool	2	Default Group	
6	Macmini	Macmini		Computer		Default Group	macOS Ventura 13.3.1

设备

管理员可以在**管理控制台**中从**所有设备**页面管理设备。设备指用户用于访问远程电脑的客户端端点。可以是电脑、智能手机或平板电脑。

单击**管理**选项卡中的**所有设备**，可以查看已注册的设备列表。



其中包括设备名称、IP 地址、客户端应用程序版本、登录的 Splashtop 账户和上次登录时间等信息。

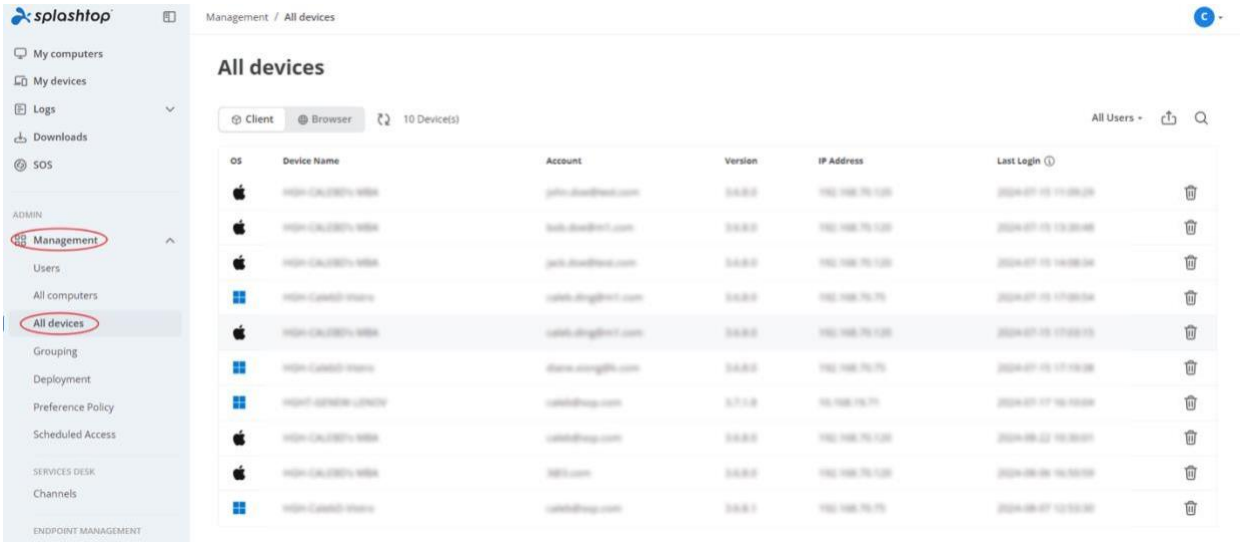
可以通过单击每行末尾的垃圾桶图标来选择删除设备。

导出设备列表

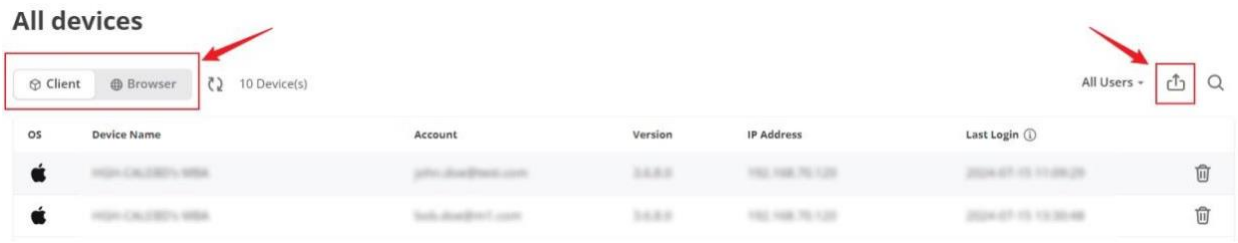
管理团队中的多台设备时，可能希望导出设备列表以维护记录。设备列表可以导出为 CSV 文件。设备列表的 CSV 文件包括设备名称、平台、账户、版本等。

所需的 Gateway 版本为 v3.28.2 或更高。

登录到 Gateway Web 门户网站，单击**管理**选项卡，然后单击**所有设备**按钮。



选择客户端选项卡或浏览器选项卡，然后单击导出图标。可以将客户端列表或浏览器列表下载为 CSV 文件。



CSV 文件包括设备名称、平台、账户、版本等。

	A	B	C	D	E	F
1	Device Name	Platform	Account	Version	IP Address	Last Login
2		Browser		3.6.8.0		2/27/2024 11:13
3		Windows		3.6.8.0		3/14/2024 15:07
4		Browser		3.6.8.0		3/7/2024 17:51
5		Browser		3.6.8.0		3/4/2024 21:48
6		Browser		3.6.8.0		3/11/2024 14:28
7		MacOS		3.6.8.0		3/22/2024 17:32

分组

管理分组

目前，Splashtop On-Prem 允许管理员创建包含特定电脑和用户的组。基于组管理访问权限很简单。

为了便于管理，可对用户和电脑进行分组。按用户或用户组分配访问权限。

登录 Gateway Web 门户网站 – 管理页面，然后单击**分组**。

注意：

- 每个用户或电脑仅能属于一个组。
- 自 Gateway v1.1.9 起支持

通用

对用户和电脑进行分组以简化管理。然后，在 Splashtop On-Prem 应用程序和网络控制台上电脑将按组进行排列。

对用户进行分组，以便轻松控制访问权限。可以为整个用户组设置访问权限。添加到组的新用户可以继承该组的访问权限设置。

创建组

通过登录到 **Gateway Web 门户网站 > 管理 > 分组**来创建组。

将用户或电脑添加到组

在分组页面可点击组右侧的齿轮图标添加用户或电脑。可以一次添加多个用户或电脑。

在电脑列表页面可点击每台电脑右侧的齿轮图标将该电脑分配到组，一次只能分配台电脑。

创建用户时，可以选择用户组。完成后，用户将自动分配到该组并继承该组的访问权限。

编辑组

在分组页面可点击组右侧的齿轮图标编辑该组的属性。可以重命名组还可以将用户和电脑添加到该组。

设置访问权限

访问权限可到用户页面的**管理 > 用户**下设置。

可以为单个用户或一组用户设置访问权限。

单击用户或用户组右侧的齿轮图标，然后选择“访问权限”。

然后选择用户或用户组可以访问的电脑和电脑组的任意组合。

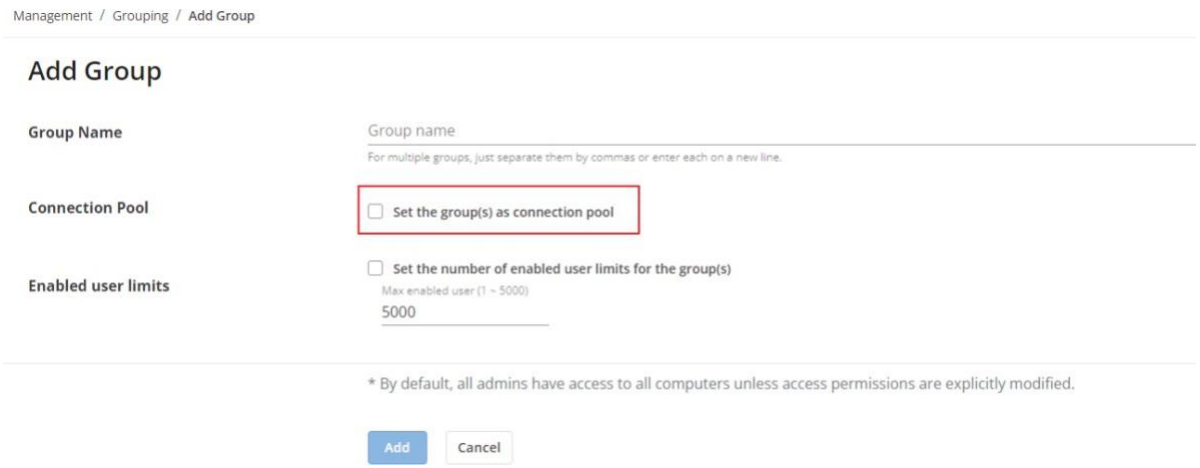
连接池

连接池允许用户通过单击组页面下的“连接”按钮以连接到远程电脑，无需展开组并选择特定电脑以连接，让用户不需要关心将连接到哪台电脑，适用以下场景：通过 Splashtop Connector 连接到 RDS 服务器时，Splashtop Connector 将根据配置文件中定义的池大小创建虚拟机。

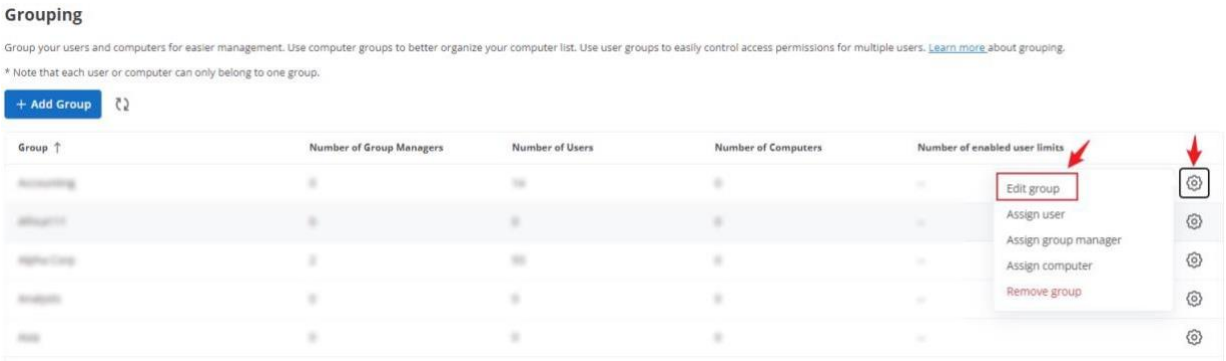
连接池不仅支持 RDS 设置，也适用于物理机设置，只要启用该组作为连接池，Gateway 就会将该组内的所有电脑作为连接池。

如何设置连接池：

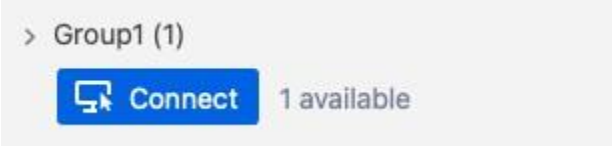
1. 前往管理 -> 分组 -> 添加组页面创建组，可以选中将该组设置为连接池选项。



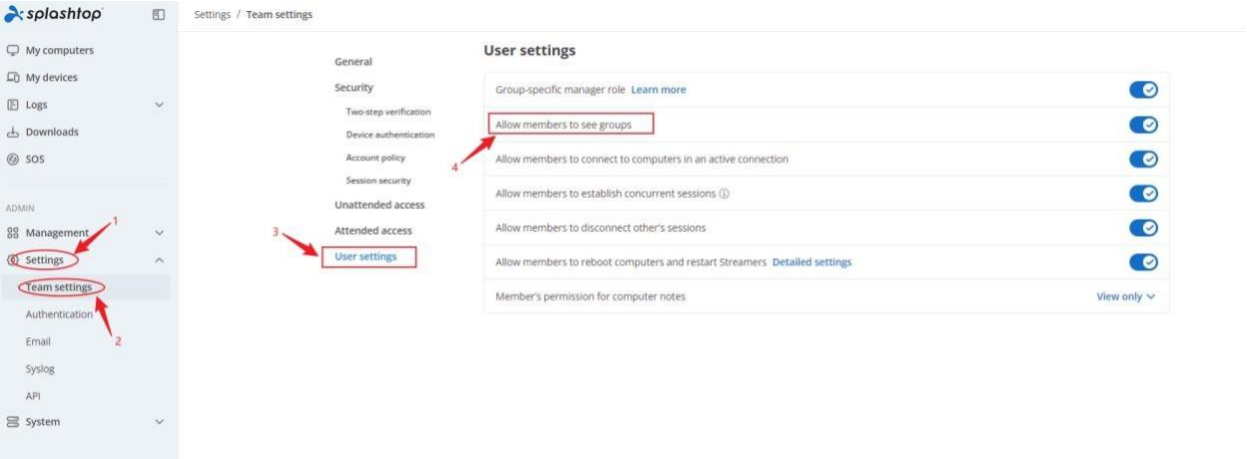
对于已有组，可以单击组列表中的齿轮按钮，选择“编辑组”并启用该选项



2. 然后在用户的 On-Prem 客户端应用程序上，该组中会出现连接 按钮，用户可以单击连接以连接 Gateway 分配的电脑



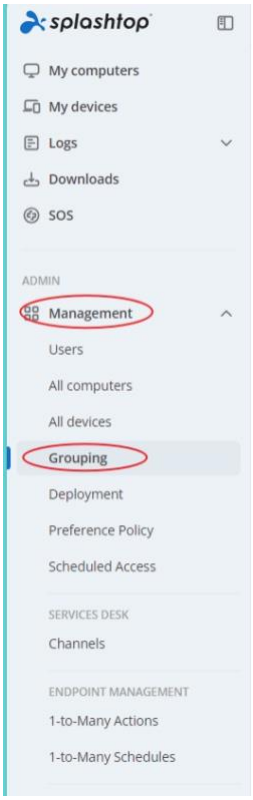
注意：请在团队设置中启用允许成员查看组选项，以确保用户可以看到该组。（设置→团队设置→用户设置）



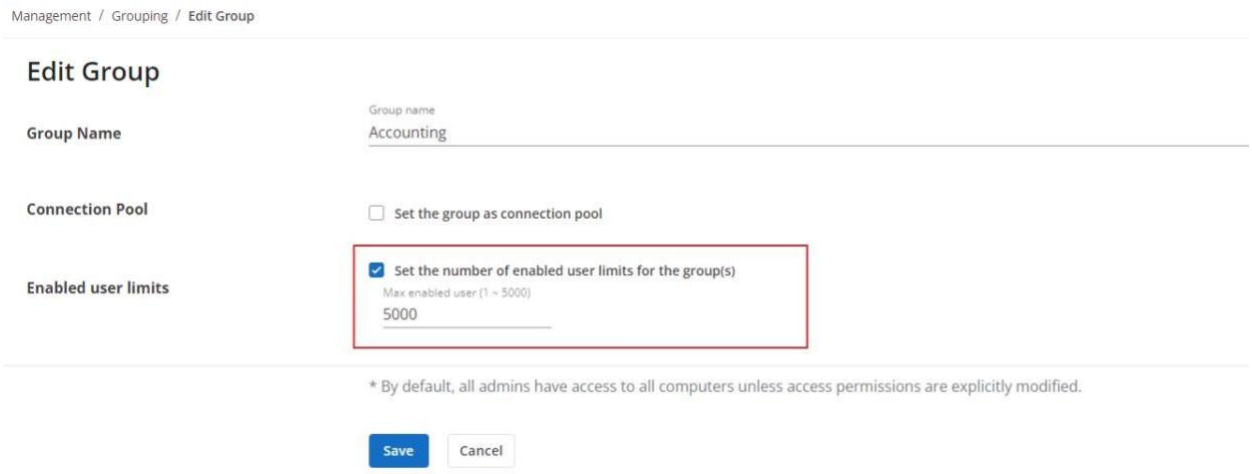
组用户限制

如果 Gateway 组相互独立，并且 IT 管理员希望优化控制许可证席位管理，则可为组设定最大用户数。

1）导航到管理/分组



2）通过启用复选框并保存，可以设置用户数量上限并应用到组。



3）如果尝试突破用户数量上限，则以下操作将被组织：

- 将新用户添加到组
- 在组之间移动用户

- 启用用户（在组中）

计划访问

简介

计划访问是一项新功能，允许管理员按时间段安排用户、组和电脑的远程访问。

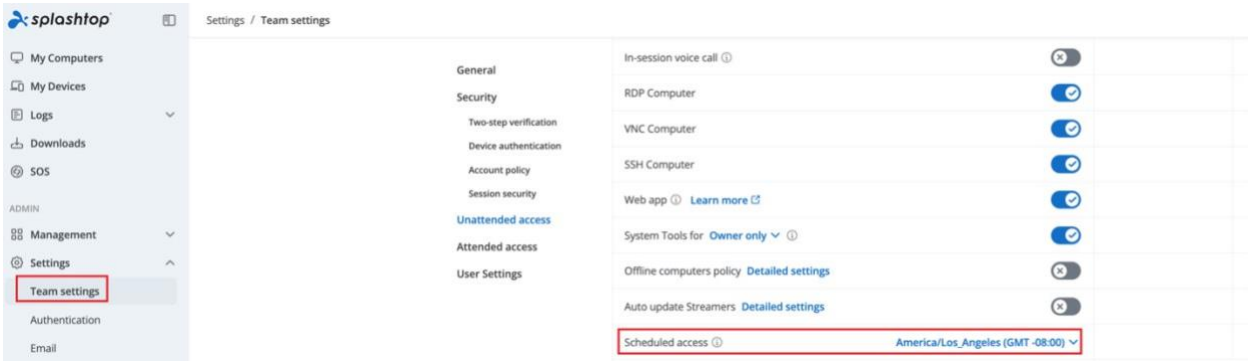
参见本文以了解计划访问示例场景。

注释和最佳实践：

- 计划访问权限*不会*覆盖现有用户/组权限，除非在 *管理 - > 用户*页面授予。
- 如果在 *管理-> 用户*页面已经配置了权限，建议取消关联这些现有权限并“迁移”以使用计划访问功能，适用于只需要计划远程访问功能的用户。
- 团队所有者和管理员可以使用计划访问功能。
- 对于开放实验室时间，可创建单独计划并为其配置时间段。例如，时间段0:00 – 9:00，包括所有成员组。另一个时间段17:00 – 23:59，包括该组成员。
- 要接收正确的断开连接警告消息，Splashtop On-Prem 应用程序 版本应为 v3.4.4.0。
- “选择电脑”页面在 IE11 上可能无法正常运行 。如果发现 IE11 有问题，请尝试使用其他浏览器或升级 IE。

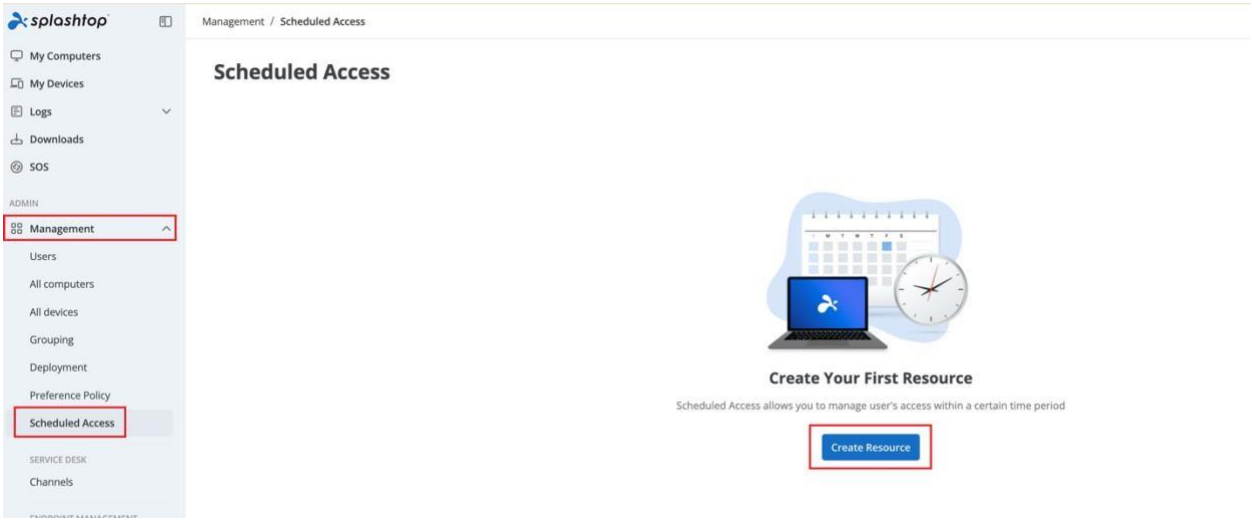
计划访问配置

1．在创建任何新日程之前，导航到 *Splashtop 网络控制台 -> 设置 -> 团队设置 -> 无人值守访问* 以配置**计划访问时区**。制定日程后，无法更改时区。只有团队所有者有权访问此设置。

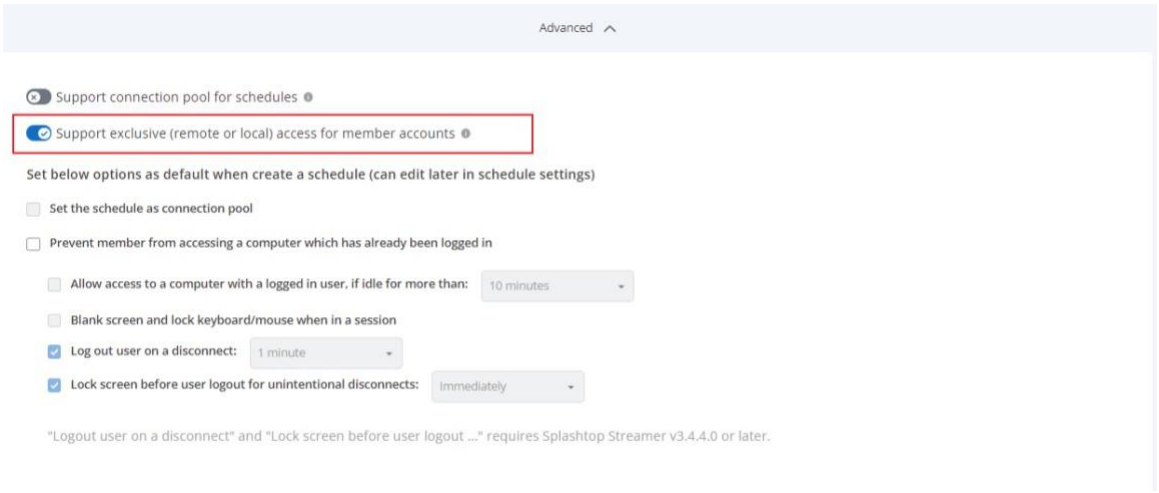


2. 打开页面 *https://{gatewayaddress}* -> *管理* -> *计划访问*

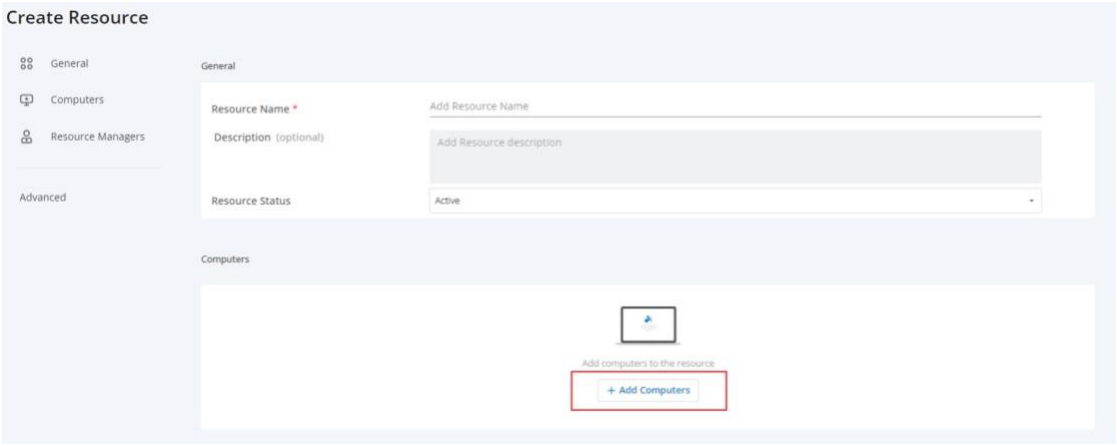
3. 单击“创建资源”并填写字段。该资源将包含哪些电脑将被安排用于访问，例如特定的电脑实验室。

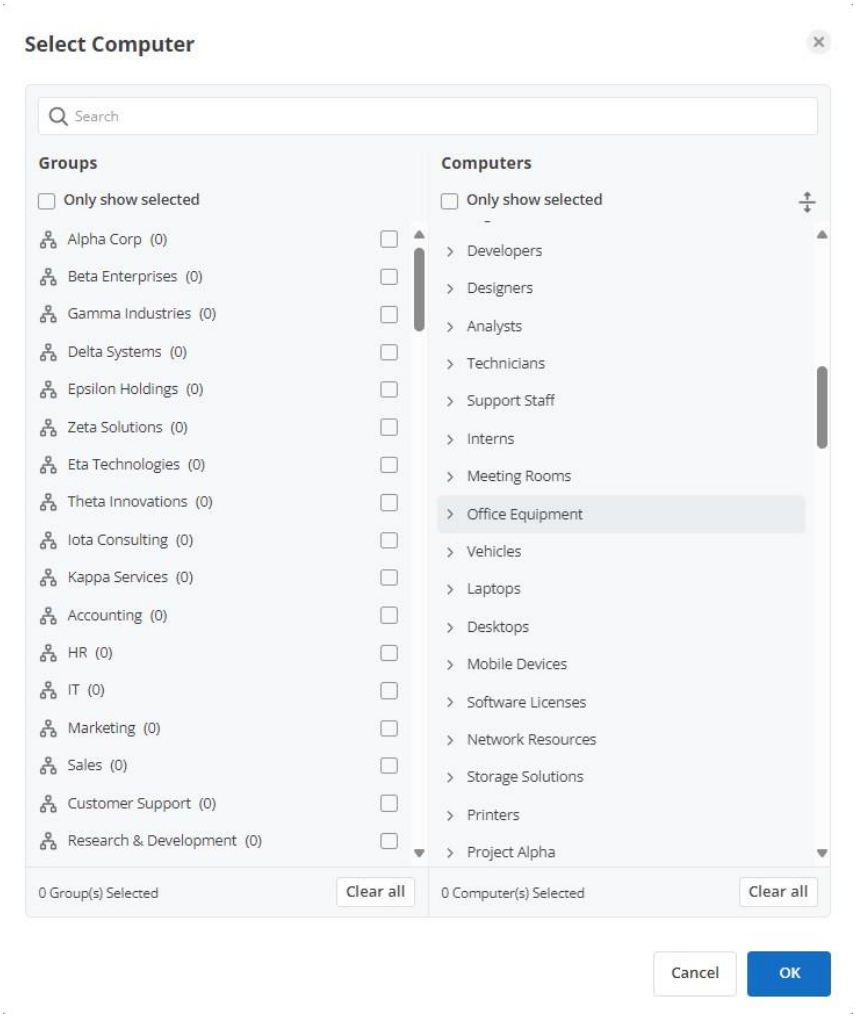


4. 单击“高级设置”以启用对独占模式。如果有用户登录到操作系统，则此设置将阻止远程用户访问电脑。有助于防止用户连接到本地使用的电脑。注销和锁屏设置还可以解决学生忘记注销操作系统账户的问题。



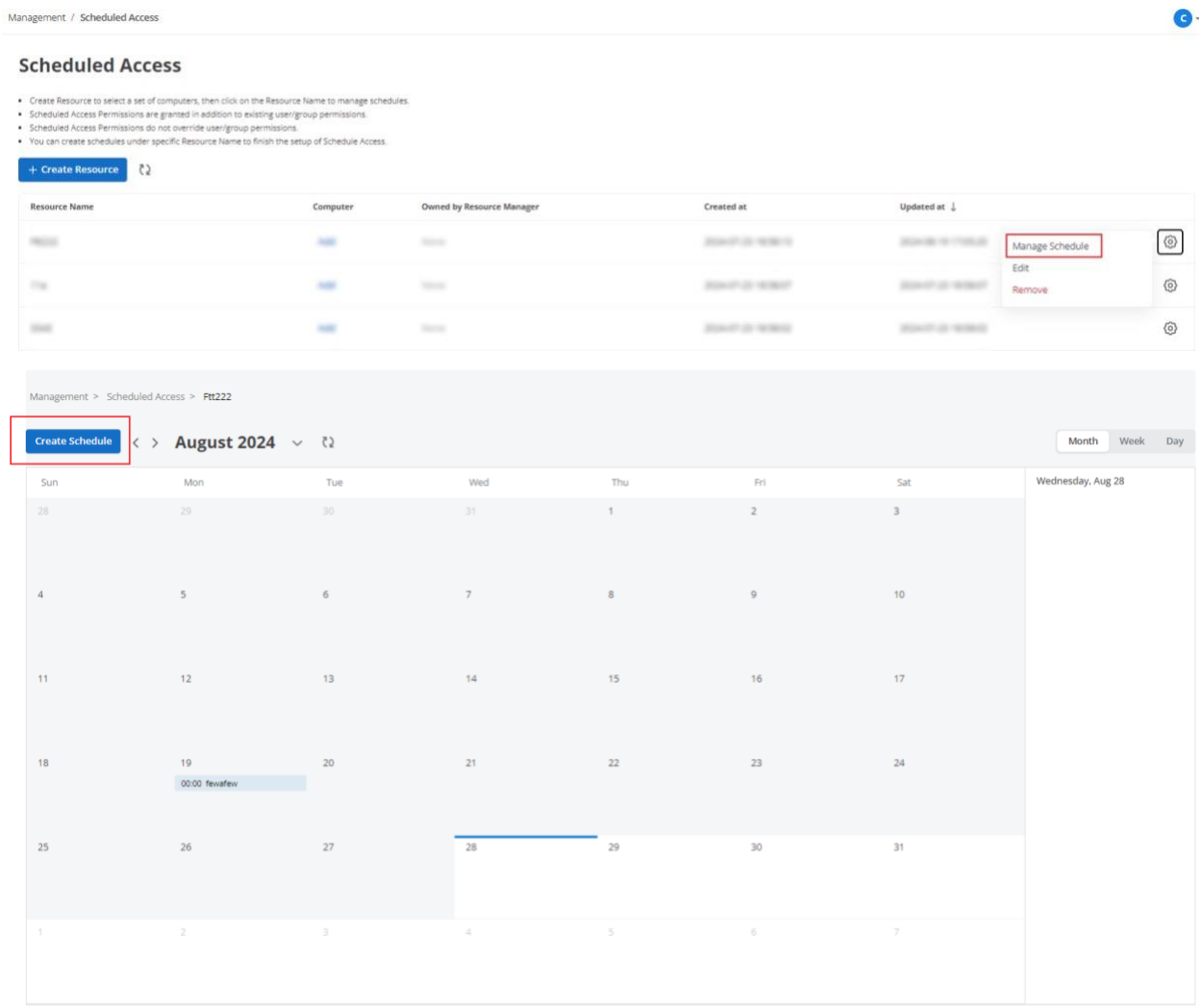
5. 选择希望在资源中可用的电脑或电脑组。



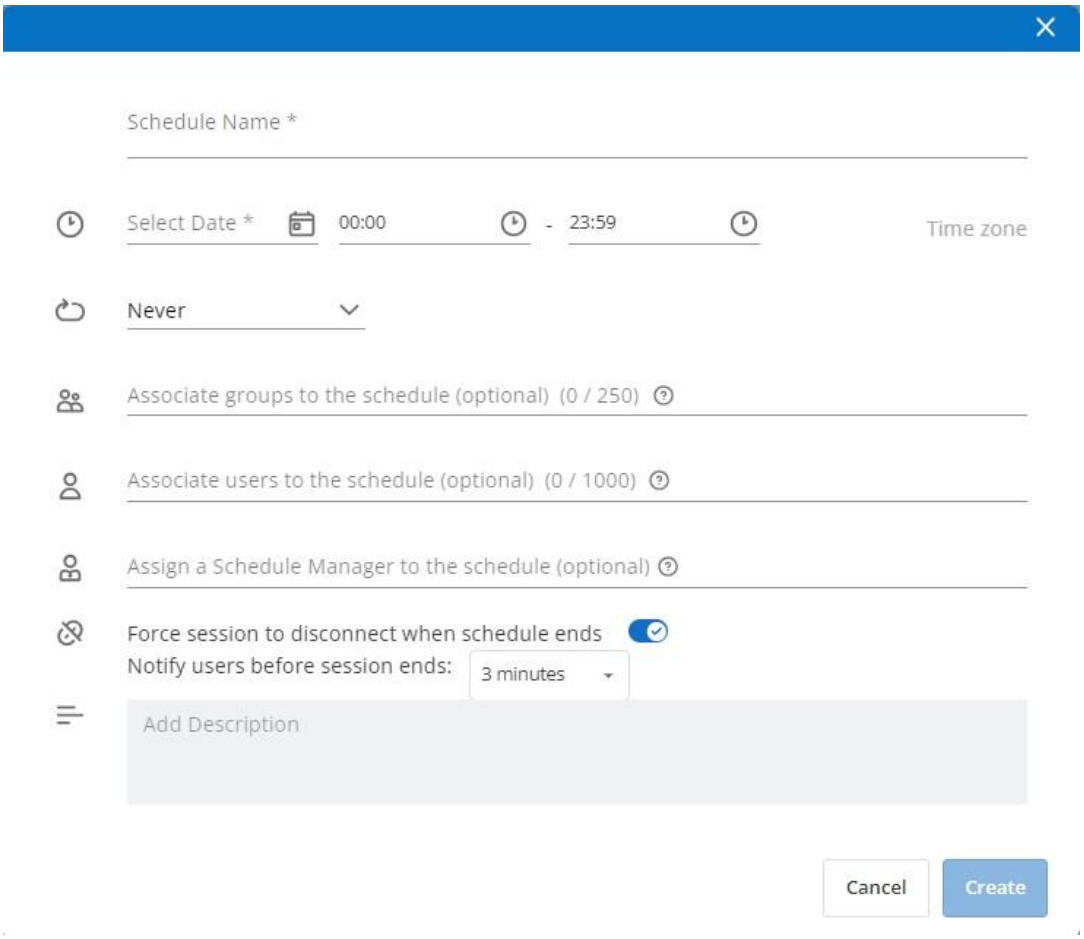


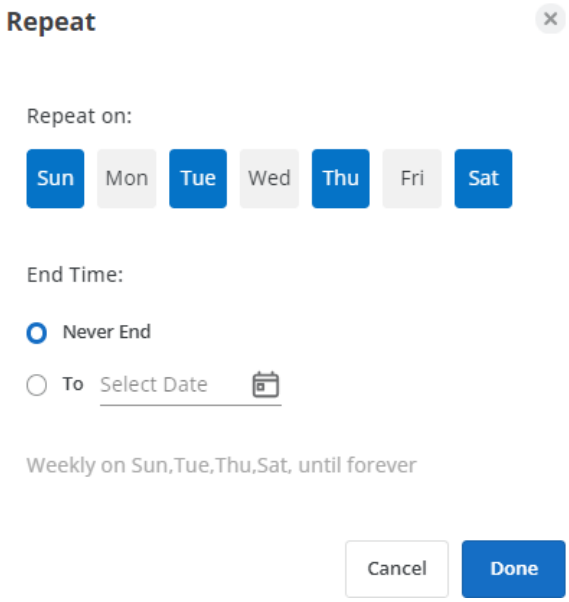
6. （非必选）分配组管理员以帮助管理资源的日程。组管理员还可以创建资源和日程。

7. 单击上下文下拉菜单（齿轮按钮）中的管理日程以将日程分配给资源。



8. 通过填写名称、开始日期和重复周期来创建该资源的日程。选择要与该日程关联的用户组或单个用户。还可以粘贴用户电子邮件列表。注意：时间下拉选项的间隔为30分钟，但可以手动输入精确到分钟的值。

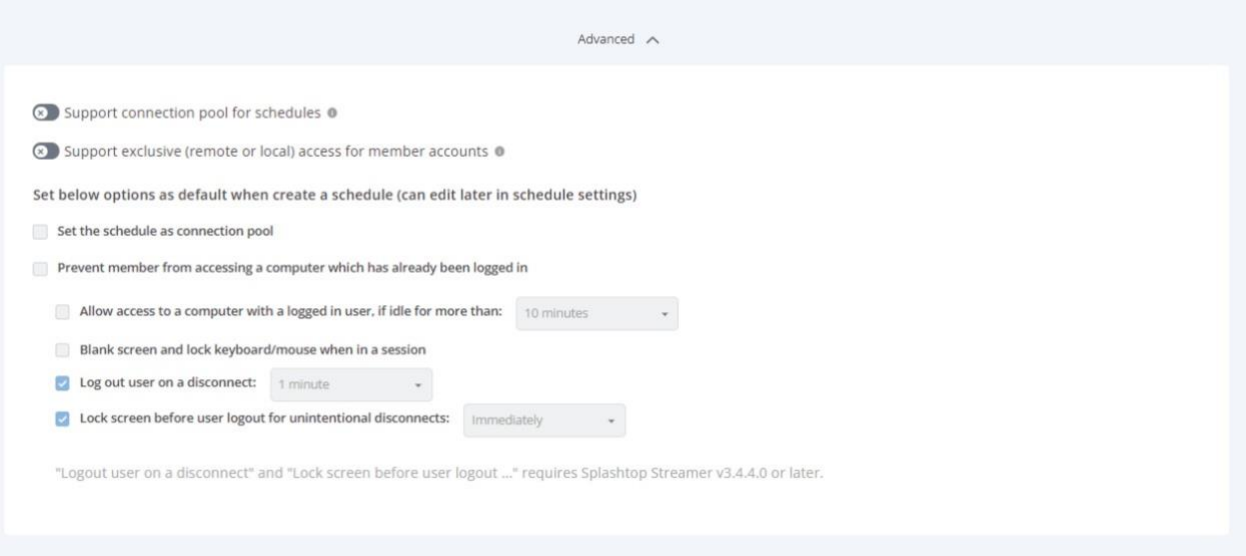




如果希望会话在时间段结束时强制断开连接，可选中选项“在日程结束时强制会话断开连接”。注意：此选项不会注销远程电脑的用户账户。

独占模式：

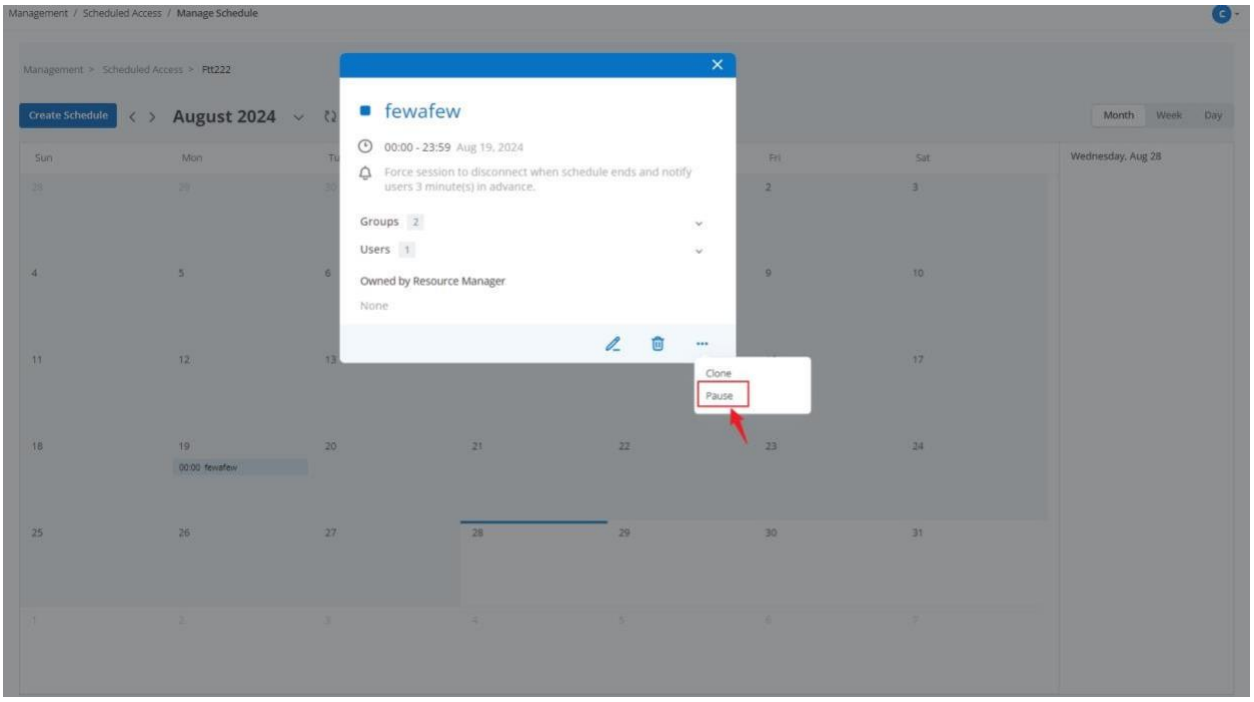
点击“高级设置”以启用/关闭独占访问

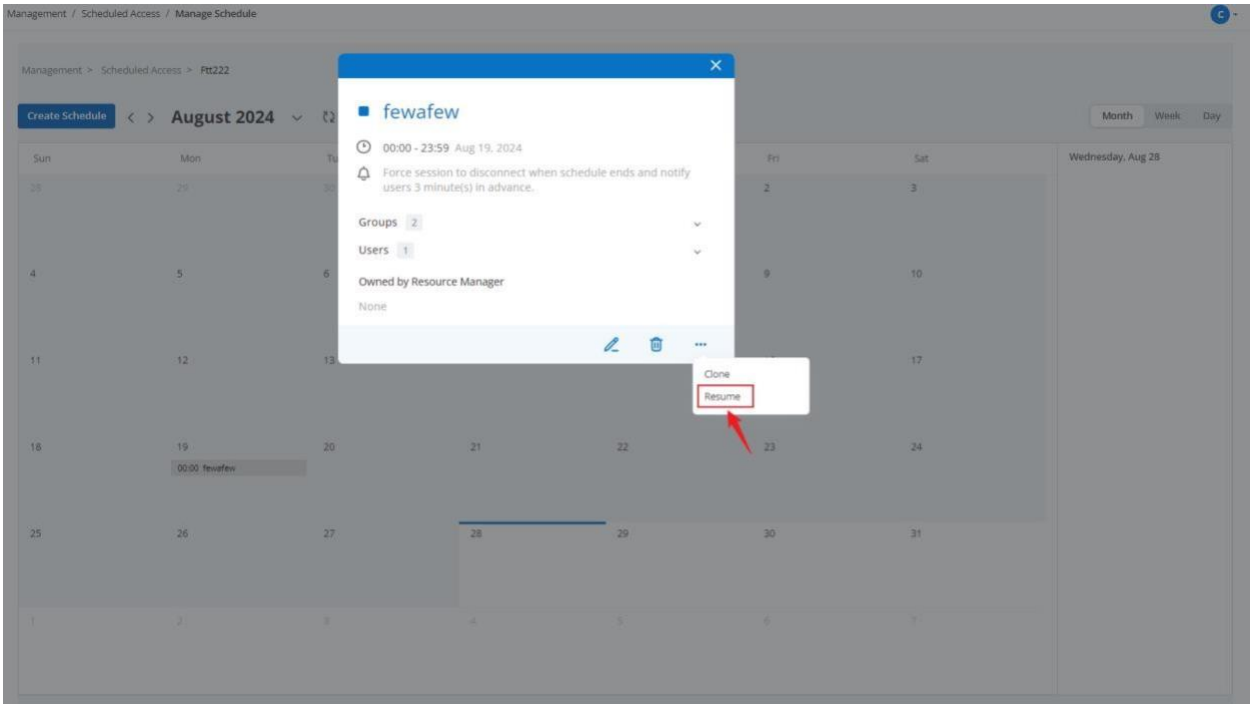


仅在当前电脑处于 Windows/Mac 登录页面时，才允许访问该日程所包含的电脑，从而使该电脑可以专供当前已登录操作系统的用户访问。适用于在实验室中或通过 Splashtop 会话远程连接的用户。

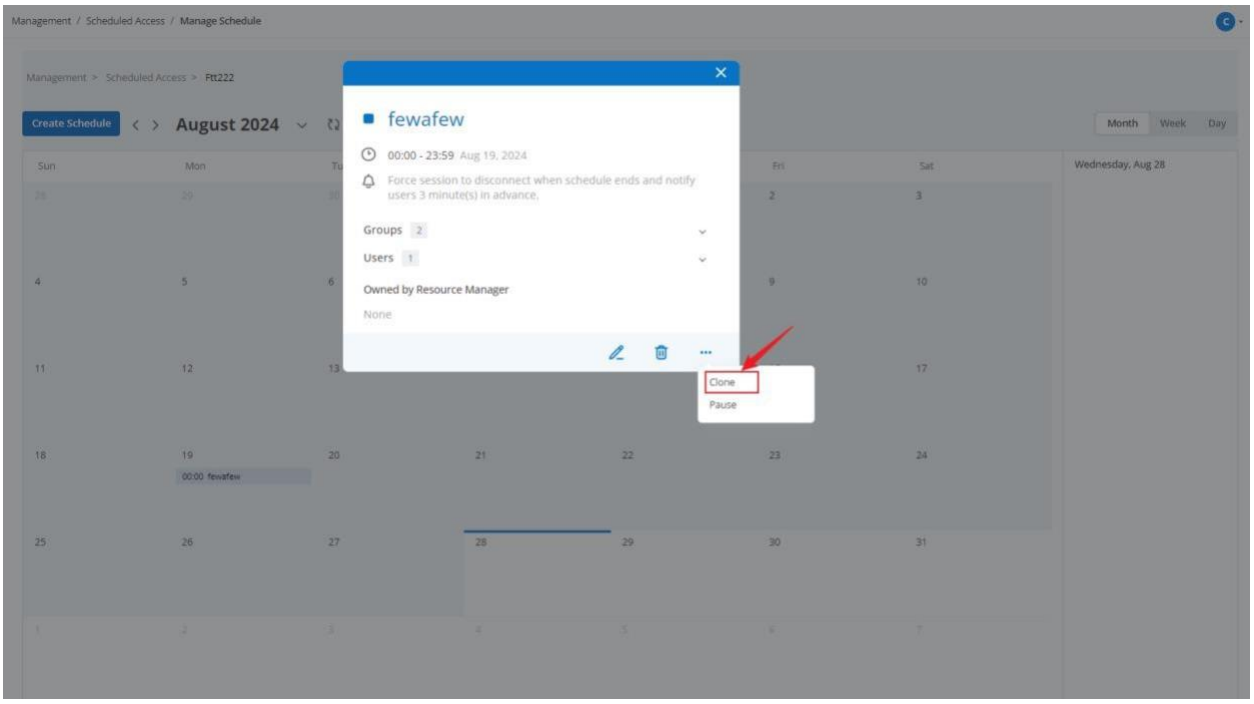
断开连接后自动注销有助于独占访问。确保 Streamer 已更新到 v3.4.4.0 以使用以上复选框选项。

9. 要暂停/恢复日程，请单击日程，然后单击暂停/恢复按钮。





10. 要克隆日程，可使用克隆按钮。



Service Desk

Service Desk – 频道

概述

Splashtop On-Prem 中的 Service Desk - 频道功能可将支持会话移动到可管理的频道中来简化 IT 支持。

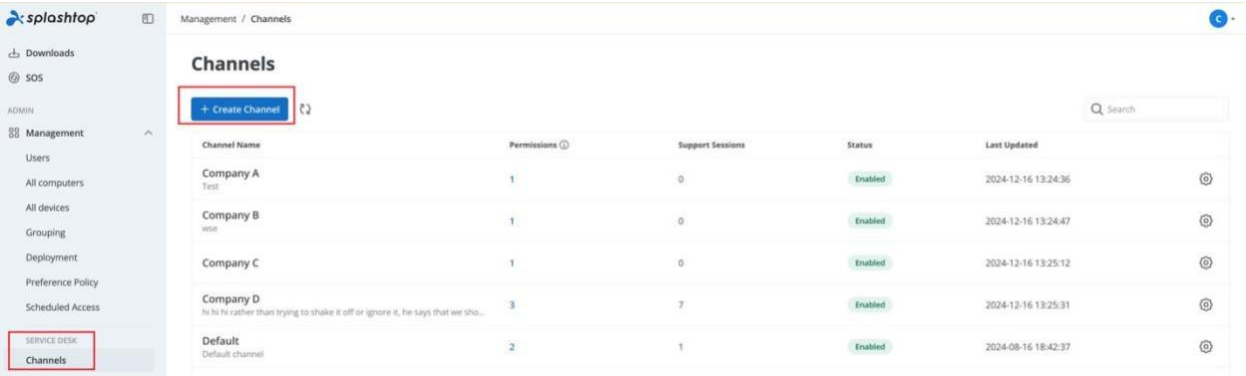
Service Desk - 频道的功能

1. 频道管理：
    a. 创建和编辑频道以有序提供支持。
    b. 将技术员和组与频道关联。
    c. 为每个频道启用精细权限。
2. 权限和角色：
    a. 分配具有不同权限的角色，例如频道管理员或技术员。
    b. 权限包括创建、传输和管理支持会话。

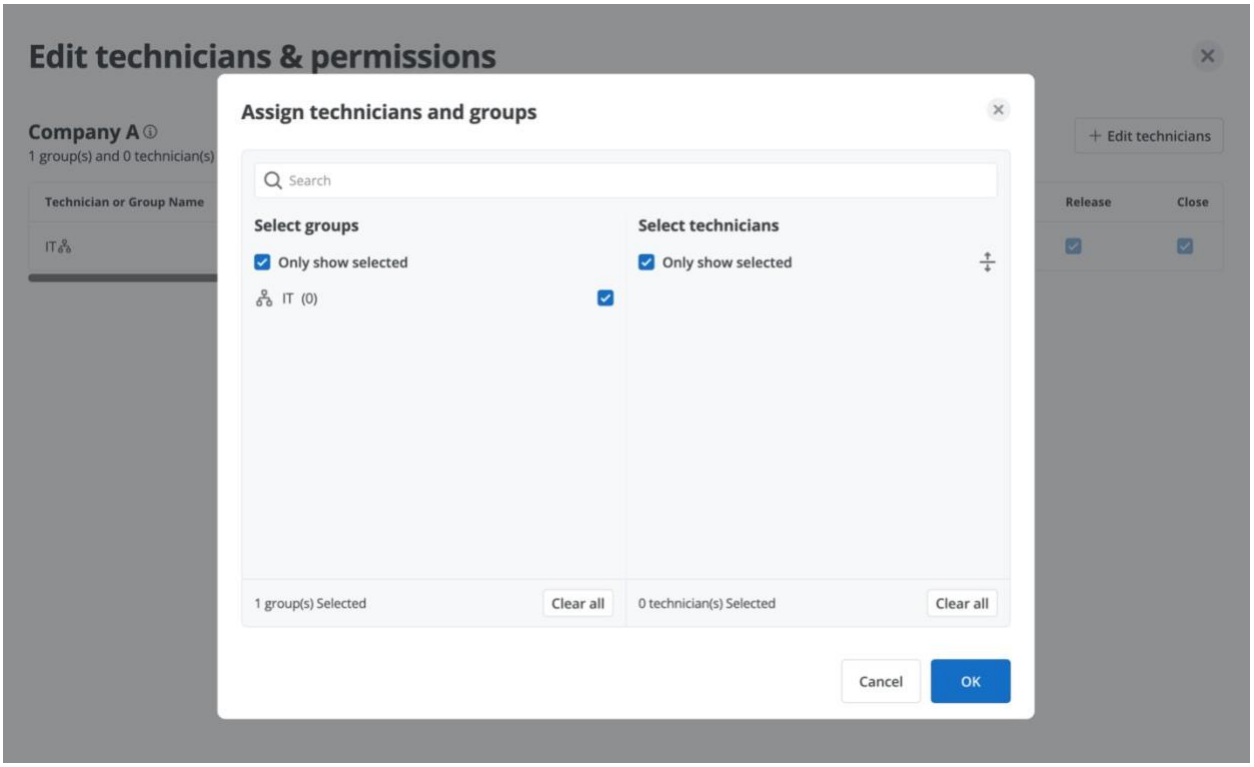
3. 支持会话：
    a. 每个频道最多可以管理100个支持会话。
    b. 可以跨频道转接、关闭或重新分配会话。
4. 默认频道：
    a. 系统创建的默认频道可确保未分配会话的无缝转接。
5. 精细控制：
    a. 针对远程访问、文件传输和命令执行等操作的微调权限。

如何使用频道

1. 创建频道
    a. 导航到管理 > Service Desk > 频道。
    b. 单击创建频道。
    c. 填写必填字段：
        1) 频道名称：必须唯一（最多64个字符）。
        2) 描述：非必选，便于识别。
        3) 会话到期时间：设置到期时间（例如，30分钟、1天）。



2. 分配技术员和组
    a. 使用分配技术员和组面板。
    b. 从可用的组或技术员中选择。
    c. 注意： 一个频道最多可以关联1000 名技术员和100个组。

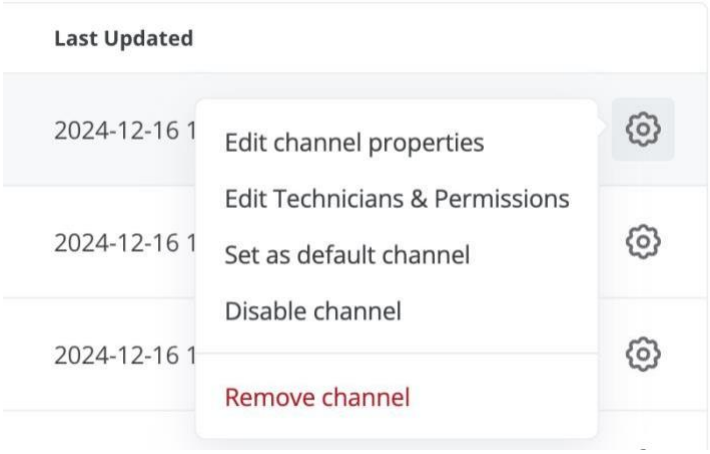


3. 编辑或删除频道

a. 访问频道名称旁边的齿轮菜单。

b. 选择编辑频道以修改属性或权限。

c. 选择删除频道以删除。请注意，此操作不可逆。



权限矩阵

角色规定了用户可以执行的操作。具体如下：

角色	权限
所有者	完全访问管理频道、权限、支持会话。
团队管理员	与所有者类似，但不能删除默认频道。
技术员	仅限于管理分配的会话。
组管理员	管理关联的组和权限，但不能创建频道。

频道行为

默认频道

- 每个团队仅存在一个默认频道。
- 来自专用频道的未分配会话会自动移动到此处。
- 无法删除或禁用。

启用/禁用频道

- 已禁用的频道在 Service Desk 控制台中会被隐藏，但数据会保留。
- 已启用的频道将在控制台显示，并允许会话管理。

错误处理

- 重复名称会触发错误提示。
- 会话限制：超过500个会话或最大活动频道数会导致错误。

最佳实践

1. 管理频道：
    a. 使用描述性名称和适当的会话到期时间来简化管理。
2. 使用默认频道：
    a. 正确配置默认通道，以确保正确处理未分配的会话。
3. 利用精细控制：
    a. 根据角色分配权限，以精确控制会话操作。

日志和报告

- 频道日志包括更改、会话活动和用户操作等详细信息。
- 每月导出日志或按日期和频道筛选以获取详细报告。

常见问题疑难解答

- 无法找到创建的频道：检查频道状态（启用/禁用）。
- 权限错误：验证角色分配和精细设置。
- 会话传输错误：确保将技术员同时分配到源频道和目标频道。

Service Desk – 控制台和一般用途

Service Desk 不仅为用户提供了监控和管理有人值守会话的新界面，而且还可以改进用户工作流程。每次启动有人值守的远程连接时，无需等待最终用户端生成新的9 位会话码。

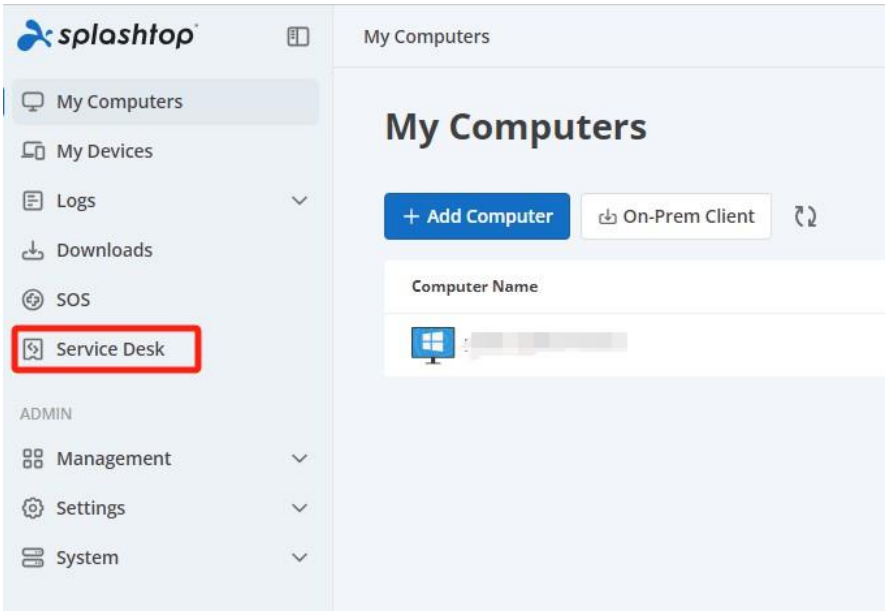
要求

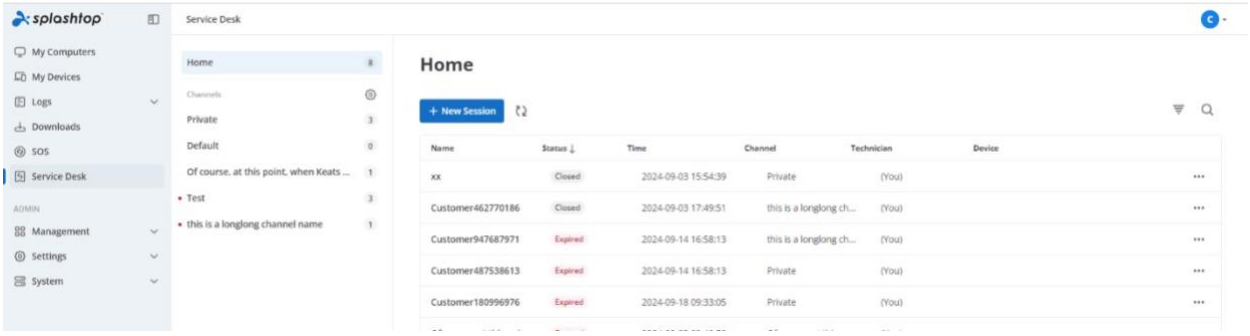
- On-Prem 应用程序和 SOS 版本为 v3.7.2.1 或更高
- 用户账户如何使用该功能：
    1) 许可证中应包含有人值守访问功能 （SOS）。
    2) 用户账户具有有人值守访问功能，例如技术员角色。

如何访问 Service Desk 控制台：

- 可以从网络控制台或 On-Prem 客户端应用程序访问 Service Desk 控制台。

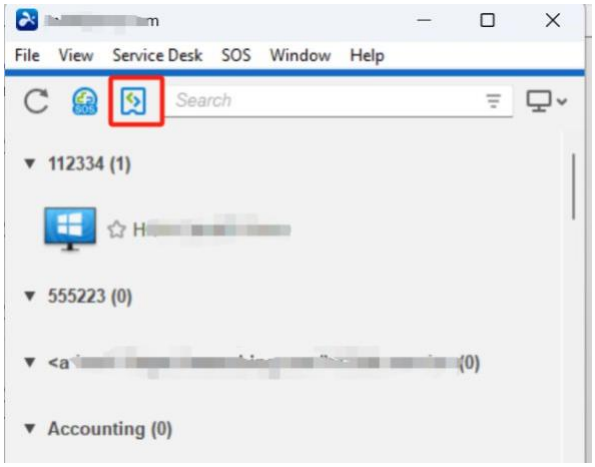
从网络控制台：

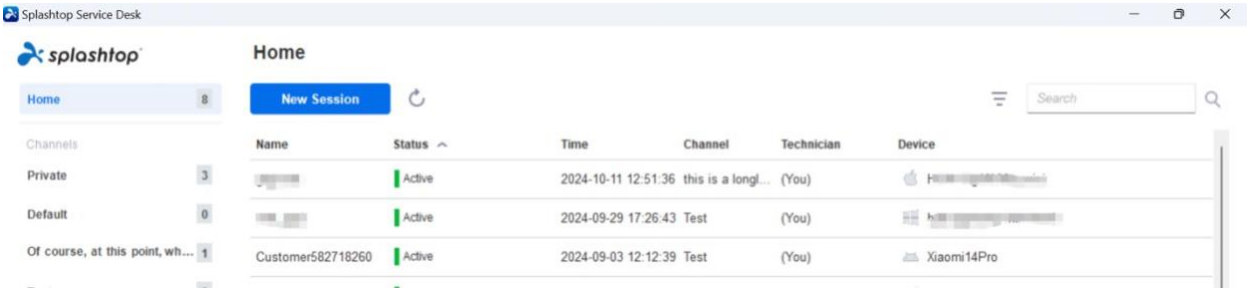




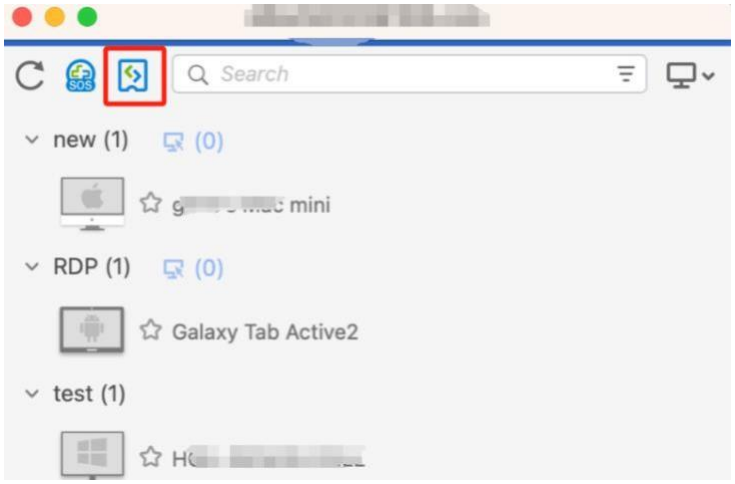
从 On-Prem 客户端应用程序

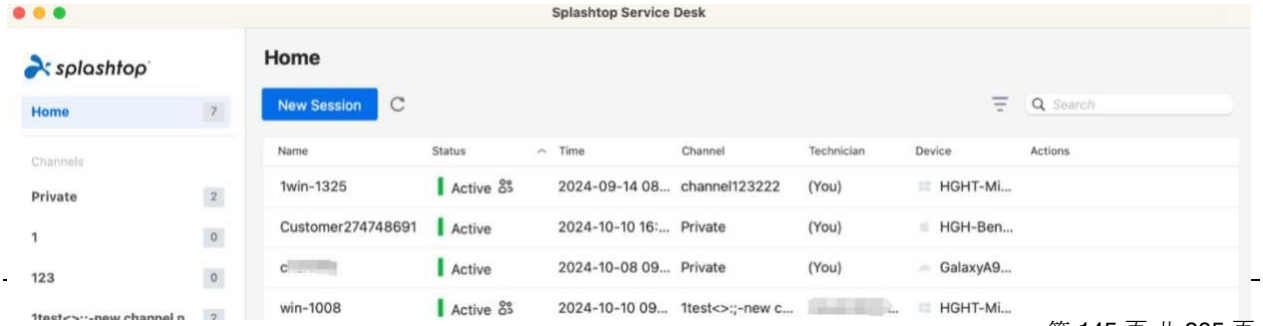
- Windows 用户



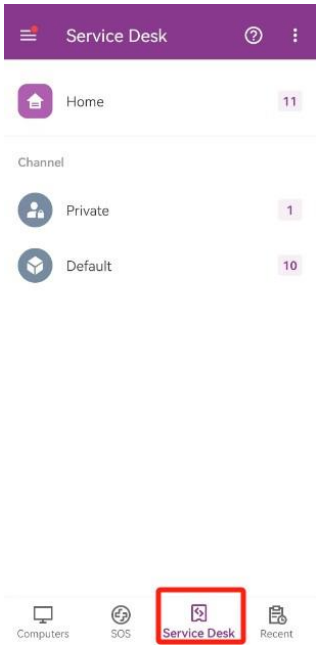


- Mac 用户





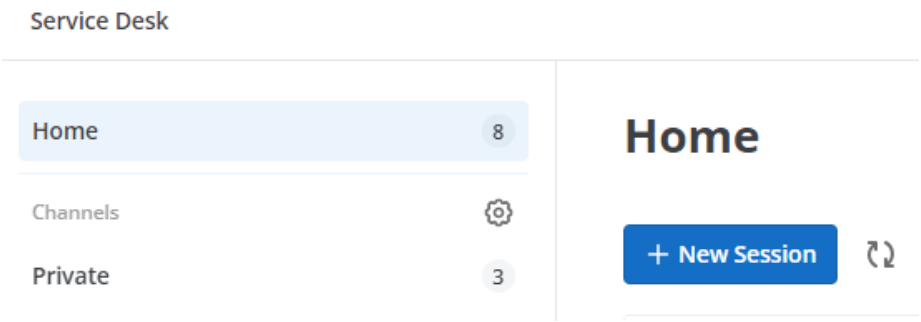
- Android 用户



如何通过 Service Desk 帮助客户

频道：在 Service Desk 中，“频道”可以理解为相关会话组。

进入 Service Desk 时，可以看到主页和频道：

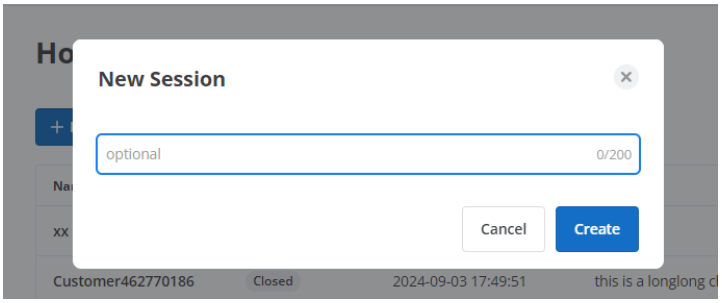


- 主页： 从主页上可以查看已分配的所有有人值守会话。
- 专用：专用频道中的会话只能由您自己查看。

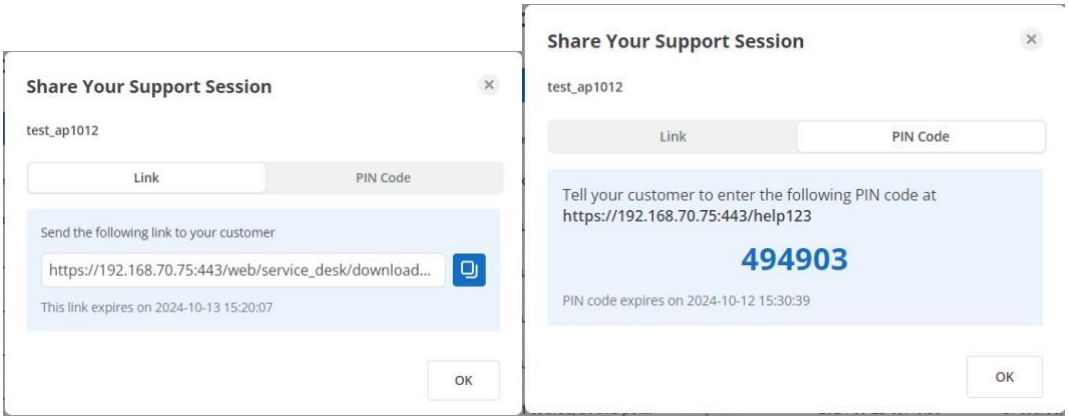
新建会话以获得支持：

步骤 1 <技术员端>：

点击所选频道的“新建会话”



通过链接或 PIN 码将此支持会话分享到客户端：

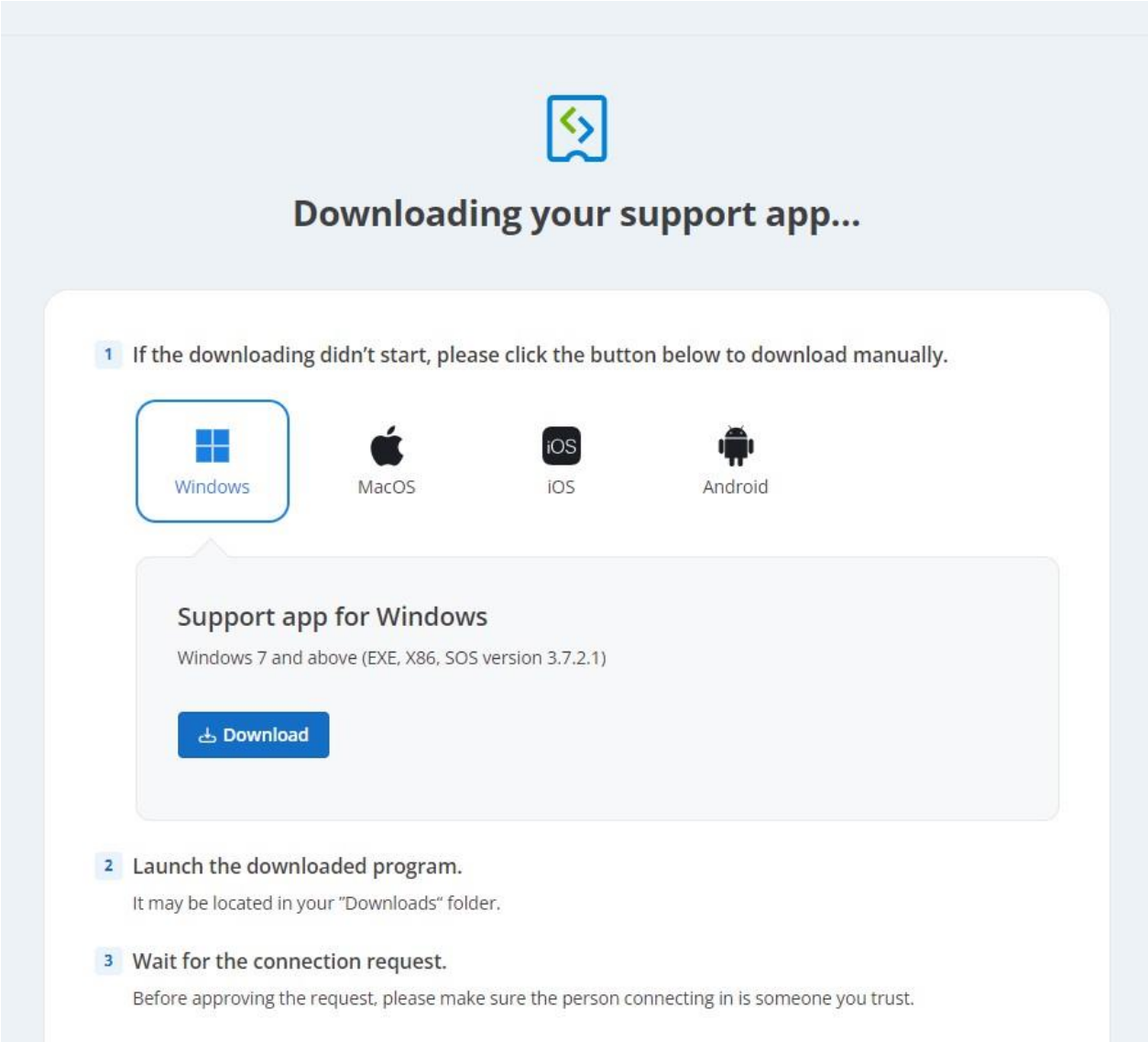


此时，会话状态显示为“等待”：

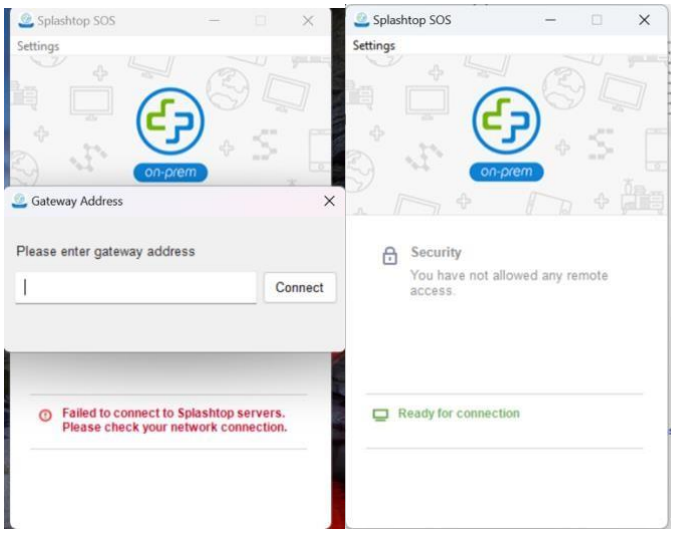
步骤 2 <客户端>：

客户端可以使用链接或 PIN 码下载并启动应用程序。

- 下载：



- 启动应用程序：输入团队 Gateway 地址并做好准备（如果想为客户端跳过此步骤，可以联系我们并使用网关地址获取 SOS 版本，然后在管理员控制台进行配置）

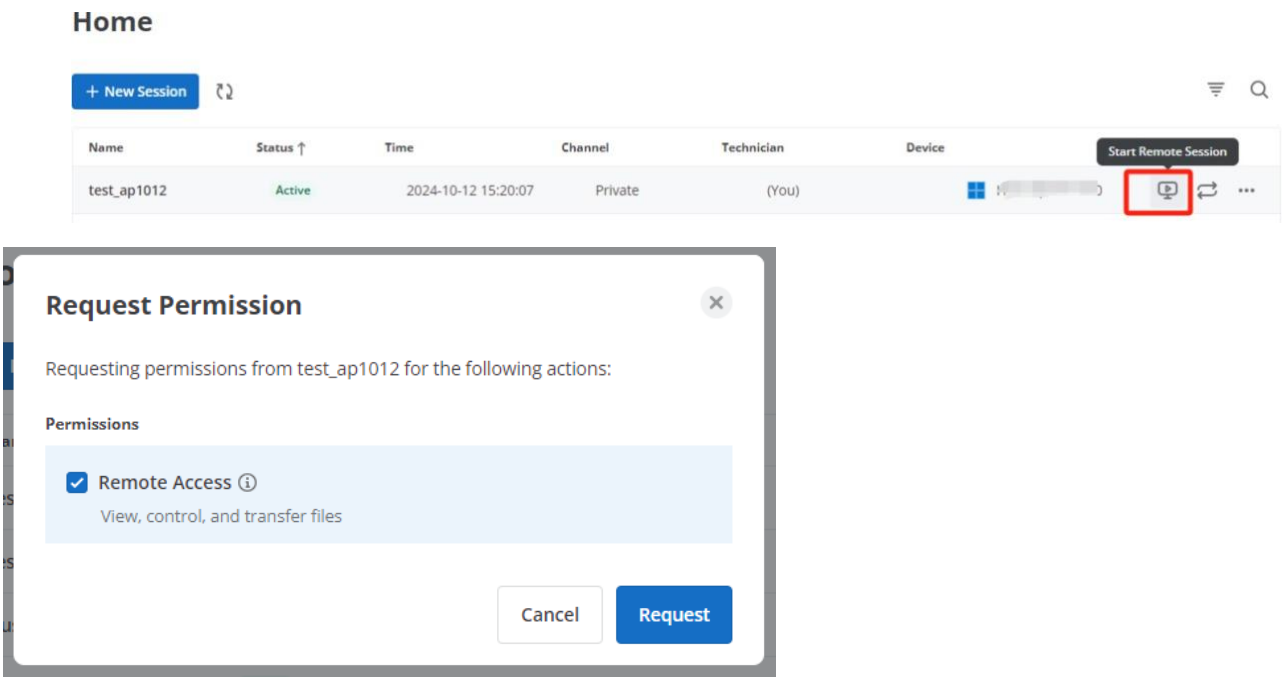


步骤 3 <技术员端>：

请求对客户端设备的访问权限

- 最终用户启动支持应用程序后，会话状态将从“等待”更改为“活动”

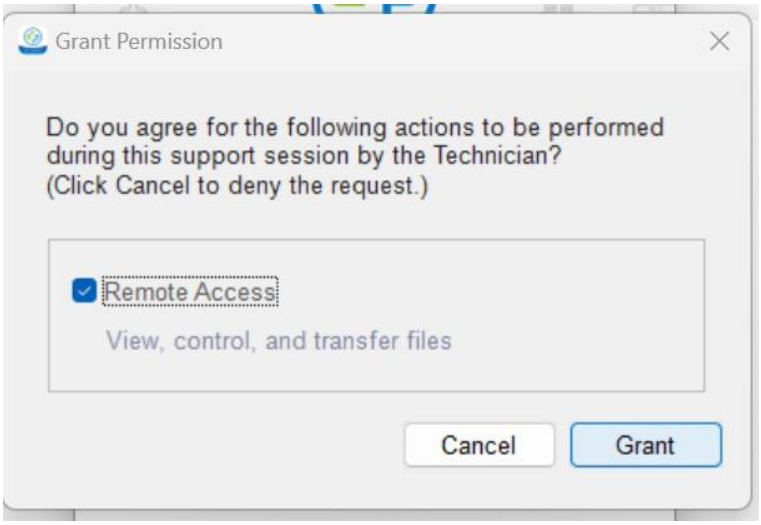
- 当会话处于活动状态时，技术员可以通过单击“启动远程会话”来请求连接权限最大远程会话数



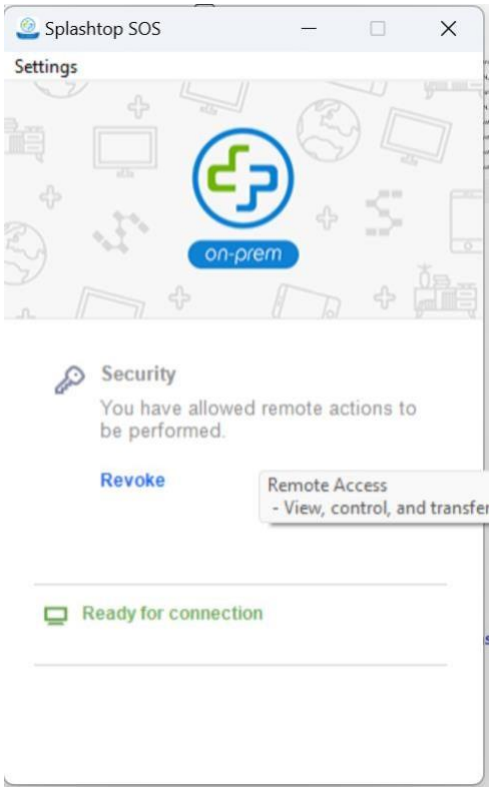
步骤 4 <客户端>：

处理技术员的权限请求

- 技术员请求权限后，最终用户将收到如下提示：拒绝或同意授权。

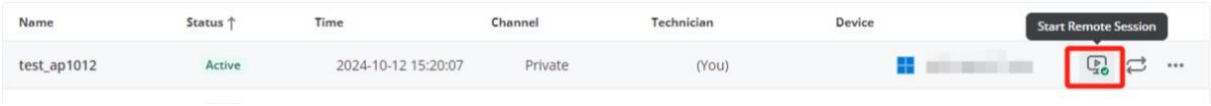


- 如果最终用户同意授权，则其端将显示以下内容：



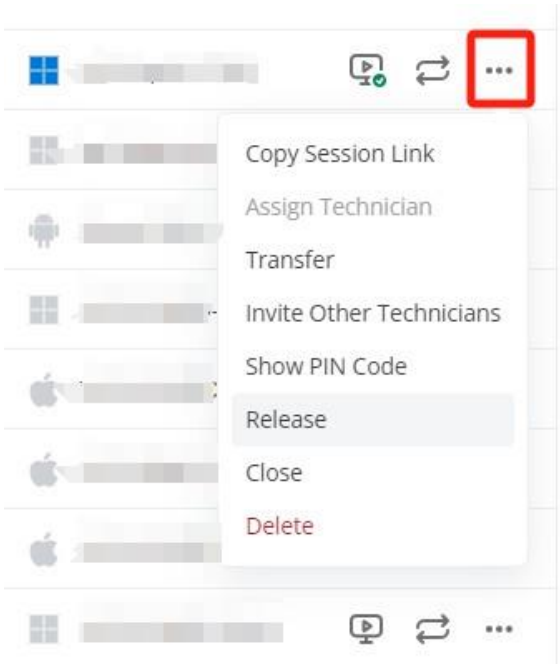
步骤 5 <技术员端>：访问要支持的目标设备

- 如果用户同意授权，“启动远程会话”图标将从 变为 ，表明技术员可以连接到用户。
- 现在，技术员可以单击“开始远程会话”以开始连接



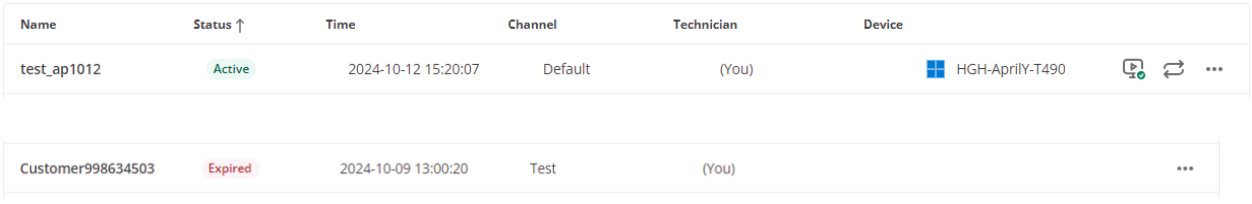
Service Desk 控制台上支持的其他操作

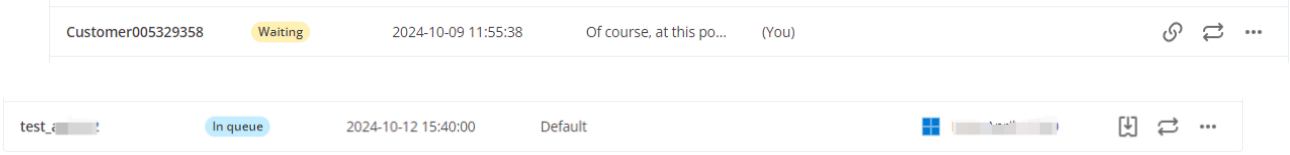
除了“开始远程会话”之外，还可以执行以下操作。



- 分配技术员：为支持会话分配或重新分配技术员
- 转接：将会话转接到其他受理人或频道
- 要转接给其他受理人，应授予释放权限
- 要转接到其他频道，应授予对该频道的访问权限
- 邀请其他技术员：最多可额外邀请2名技术员加入支持会话（最多总共3名技术员）
- 复制会话链接
- 显示 PIN 码
- 释放：从分配的技术员中释放会话
- 关闭：关闭会话
- 删除：从频道中删除会话

会话状态





- 等待：用户在生成新会话链接后立即从唯一链接下载并运行 Service Desk 支持应用程序时，状态将显示为“等待”。
- 活动：Service Desk 支持应用程序已在最终用户电脑上启动；此会话已分配技术员，并且该技术员已准备好请求连接权限。
- 排队：会话已释放，正在等待技术员加入会话。
- 已过期：会话超过了频道设置中预设的会话到期时间。
- 已关闭：技术员已手动关闭会话。无法继续连接。如果要再次连接，需要生成新会话。

Service Desk - SOS Call

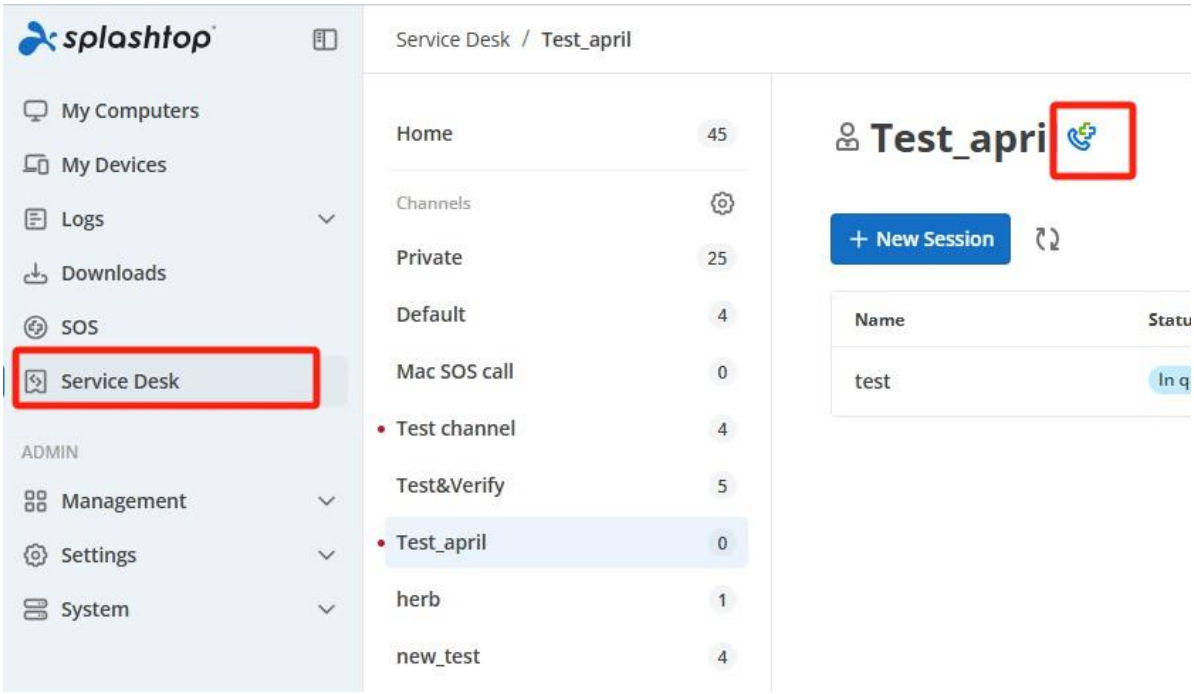
1. 要求

- On-Prem 应用程序和 SOS 版本为 v3.7.2.1 或更高
- Gateway 版本为 v3.36.0或更高。

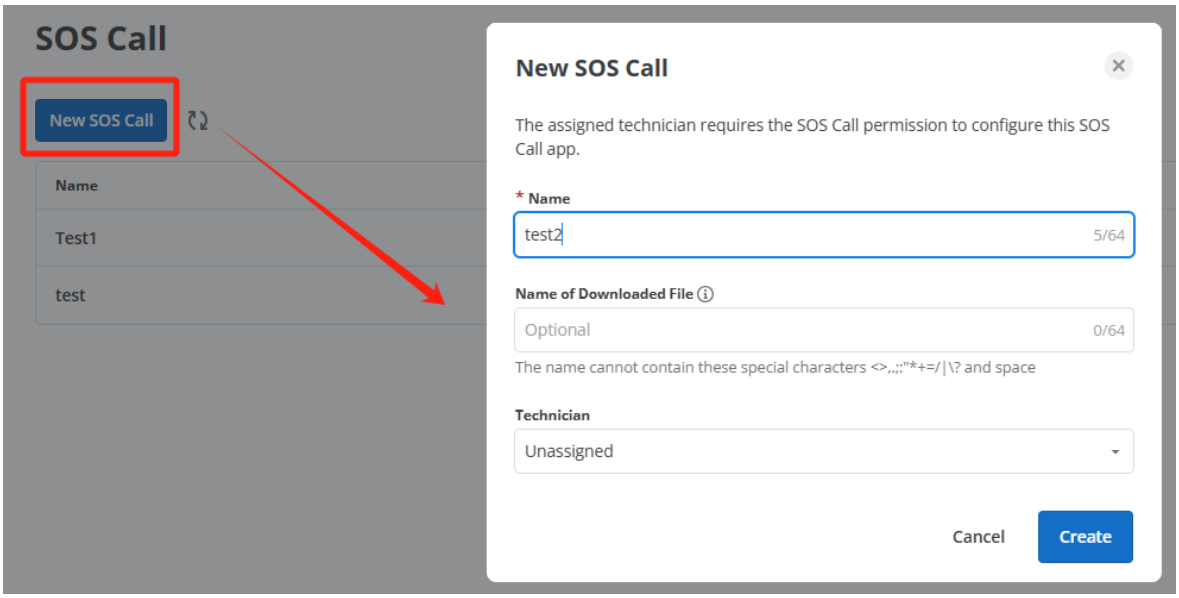
2. SOS Call 使用步骤

步骤 1 <技术员端>：创建 SOS Call

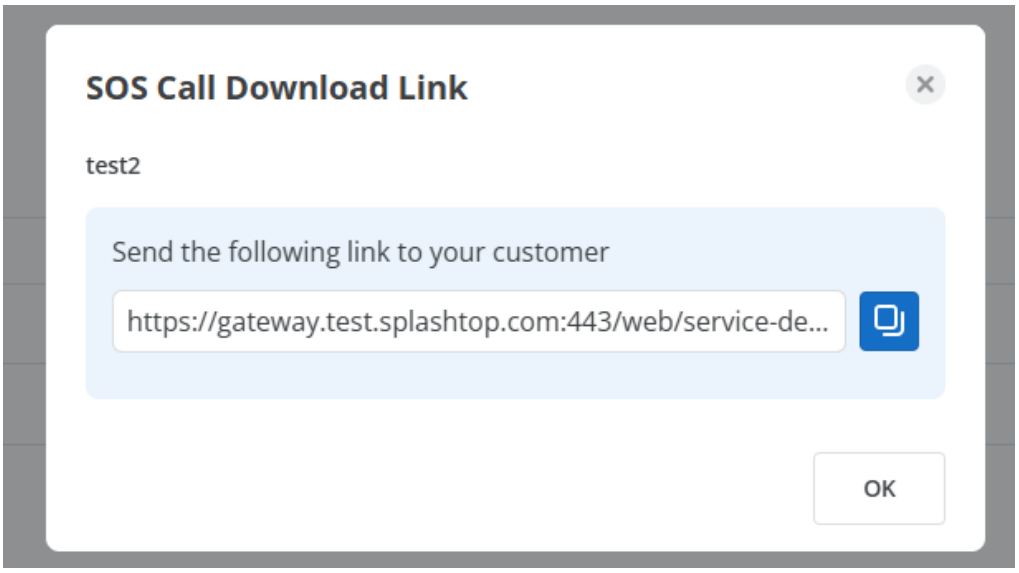
- 打开 SOS Call 管理页面：



- 新建 SOS Call：

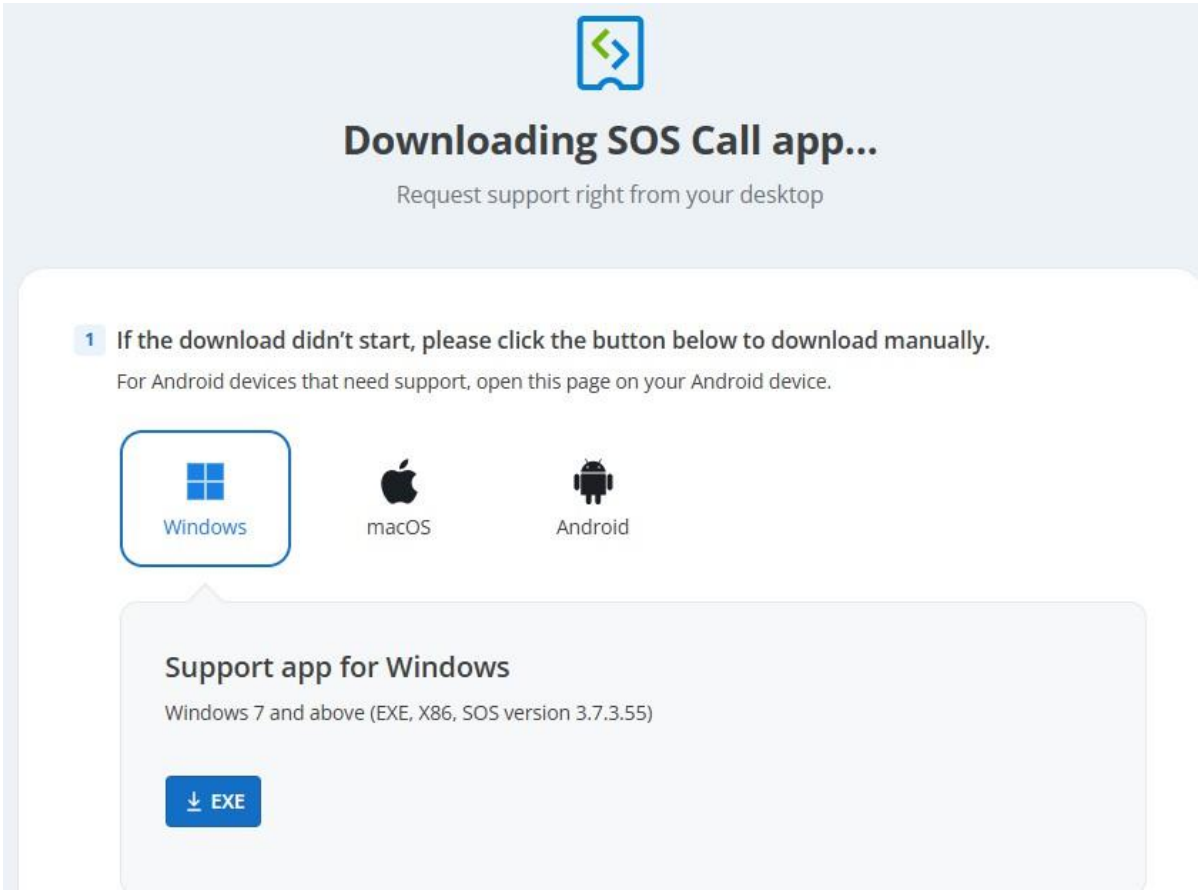


- 获取下载链接并将其发送给受支持方：
- 注意：多个用户可以同时使用一个SOS Call 链接，无需为每个用户单独创建链接。



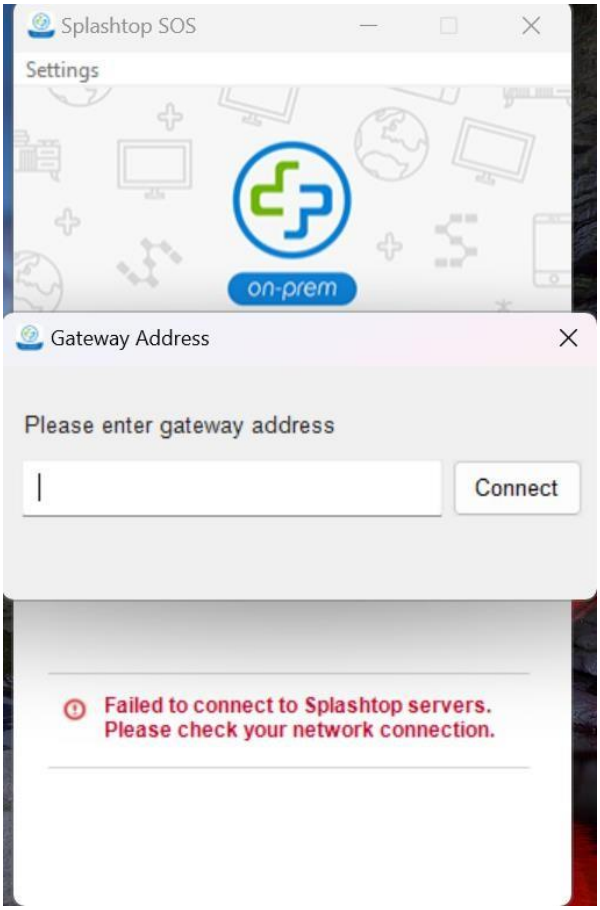
步骤 2 <受支持方>：下载并运行 SOS 应用程序

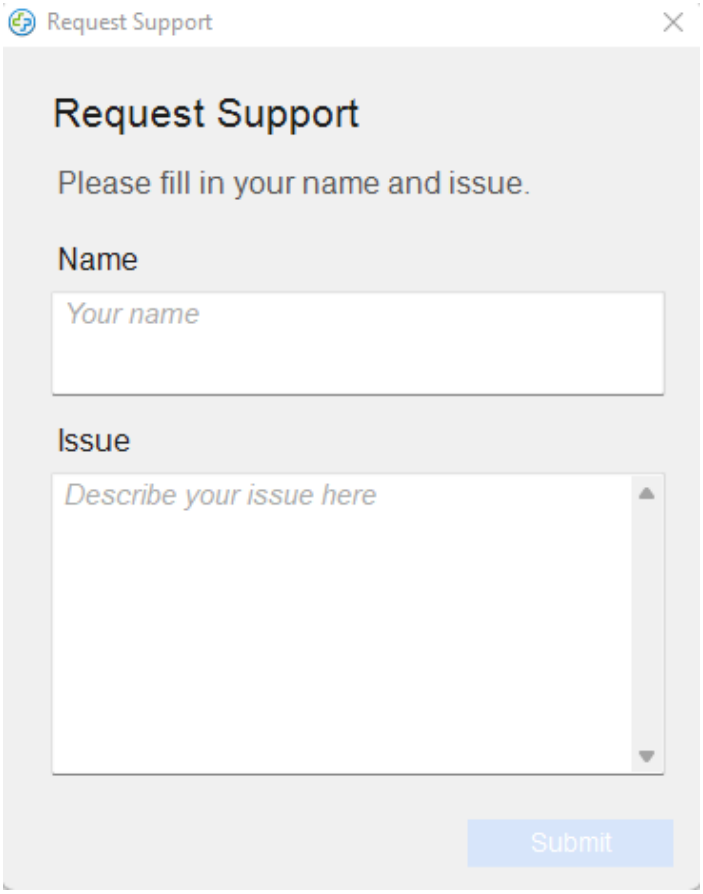
- 通过下载链接，根据使用平台下载相应的 SOS Call 应用程序：



- 如有任何问题需要技术员帮助，请启动此应用程序：

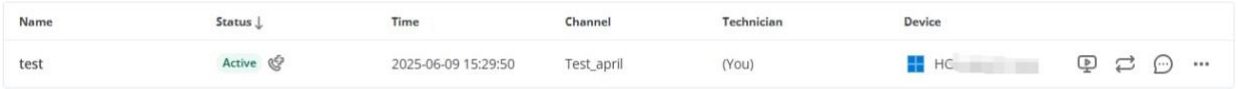
- 如果需要，请输入您的 Gateway 地址。并提交您的姓名和问题。



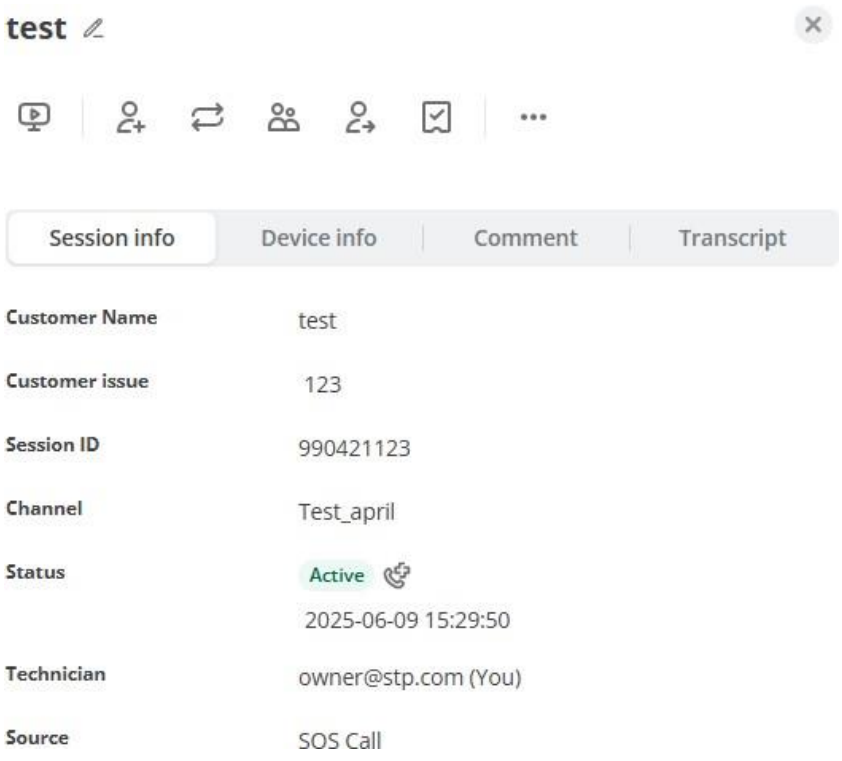


步骤 3 <技术员端>：查找请求并提供支持

- 在用户提交请求后，技术员将在 Splashtop Service Desk控制台中看到一个新条目，显示用户已请求支持。



- 通过单击新增的条目，可以查看姓名和问题详情等信息：

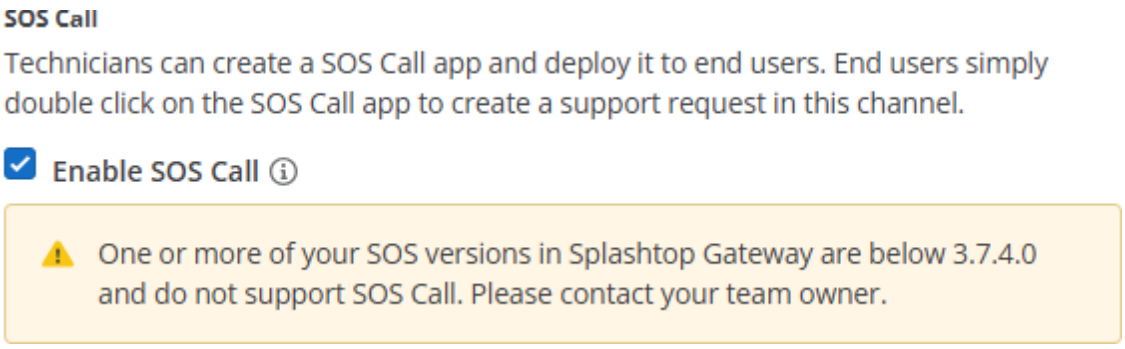


3. 在管理控制台中管理 SOS Call

3.1 为新的/现有的服务台频道启用 SOS Call

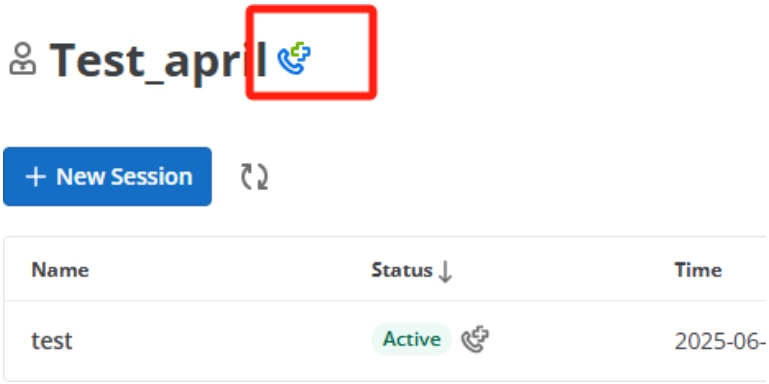
- SOS Call 是频道下设的一个设置项，可以在频道设置中进行编辑：

- 向下滚动频道编辑页面，找到启用 SOS Call：



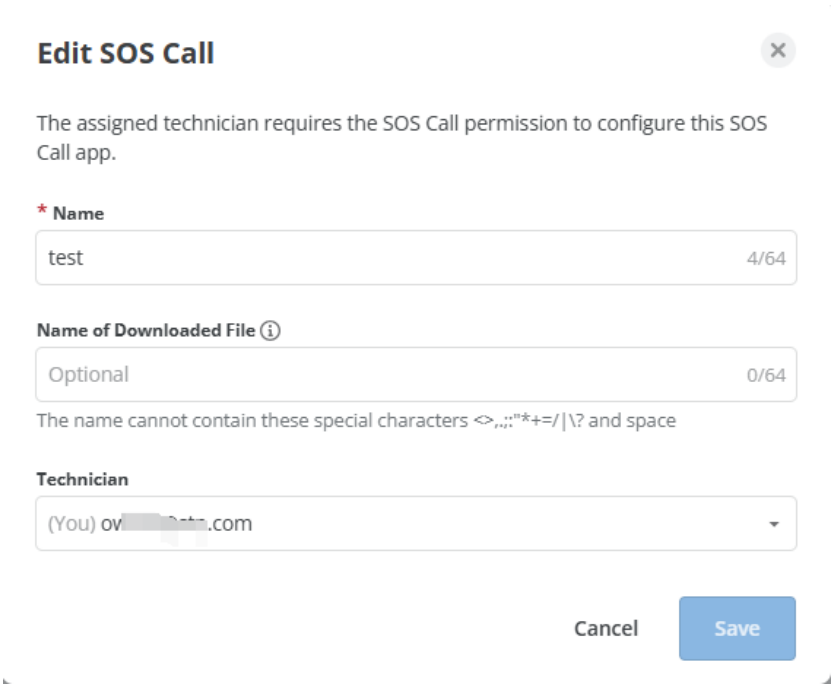
3.2 管理和创建 SOS Call 下载链接

- SOS Call 应用程序应指定为一组最终用户使用，例如某个指定公司、用户团队等，因为生成的下载链接可被重复使用。
- 在3.1中启用 SOS Call 后，则可到管理页面。管理 SOS Call 图标将出现在已启用的频道上。

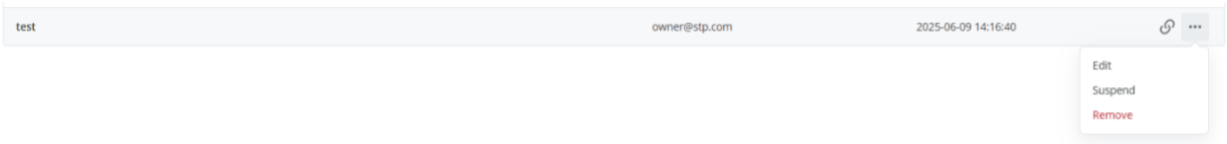


- 除了通过创建之外，已有的SOS Call 应用程序还可以通过以下方式进行管理：

- 编辑：指派新的技术员或更改应用程序的名称。

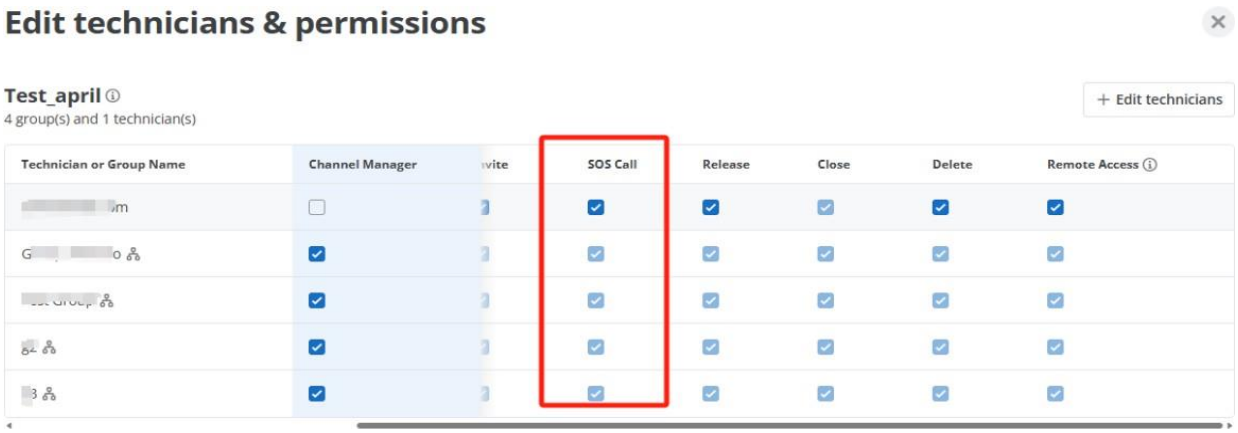


- 暂停：SOS Call应用程序链接将暂时对所有新下载以及已下载的应用程序无效。恢复应用程序不会生成新链接，链接将保持不变。
- 删除：所有已有链接或下载的应用程序将无效。



3.3 SOS Call 权限

- 如果要编辑权限，可以导航到管理 > 频道 > 编辑技术员和权限



- 如果默认受理人为“未分配”，所有技术员将能够看到新的 SOS Call应用程序
- 具备 SOS Call 权限的技术员可以创建/管理默认受理人为其本人的 SOS Call 应用程序。
- 不具备 SOS Call 权限的技术员无法创建/管理所有已有的 SOS Call 应用程序。

Service Desk - 会话记录

概述

Splashtop Service Desk 现在支持会话记录，为审计、故障排除和合规性目的提供关键会话活动的完整记录。支持会话记录包括在系统工具后台会话期间执行的聊天交互、远程控制和系统工具操作。

会话记录的具体内容？

会话元数据

- 会话开始和结束时间
- 会话 ID 和主机详细信息
- 会话转接记录。
- 会话备注。

聊天消息

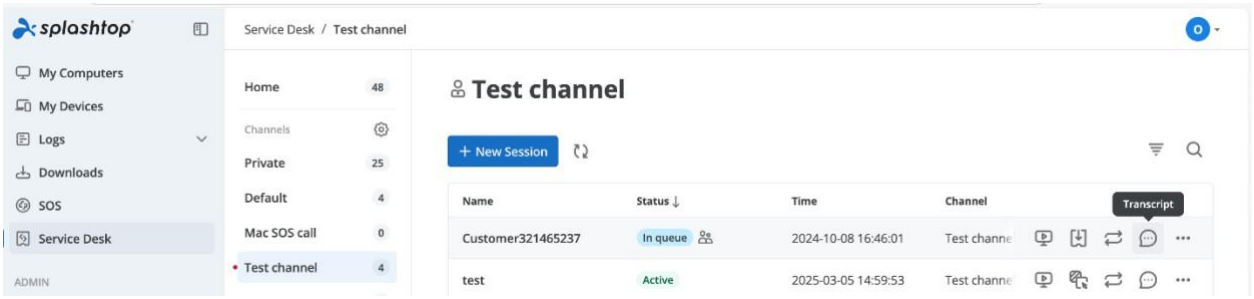
- 使用会话系统工具期间发送和收到的所有文本消息

系统工具用途（如果适用）

如何查看会话记录

查看活动会话

1. 打开 Service Desk 控制台。
2. 导航到支持会话列表。
3. 选择当前正在进行的会话。
4. 单击会话记录选项卡查看实时日志。

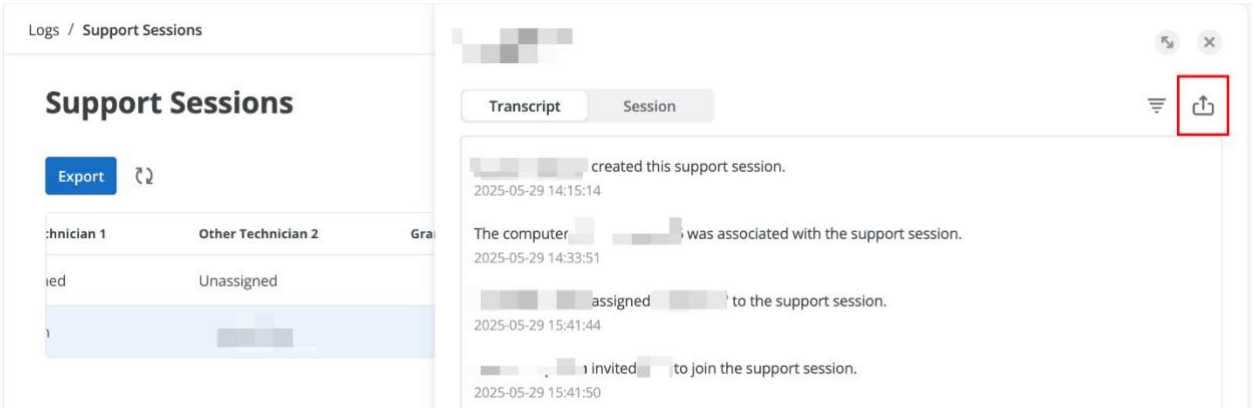


查看历史会话

1. 导航到日志→服务台→支持会话
2. 选择要查看的已完成会话。
3. 单击会话记录以显示记录的日志。

导出会话记录

- **导出格式：**会话记录可以以 CSV 格式导出，以便保存记录。
  - **如何导出：**
    - 从日志中打开所需的会话记录。
    - 单击导出，文件将下载到本地系统。



使用场景

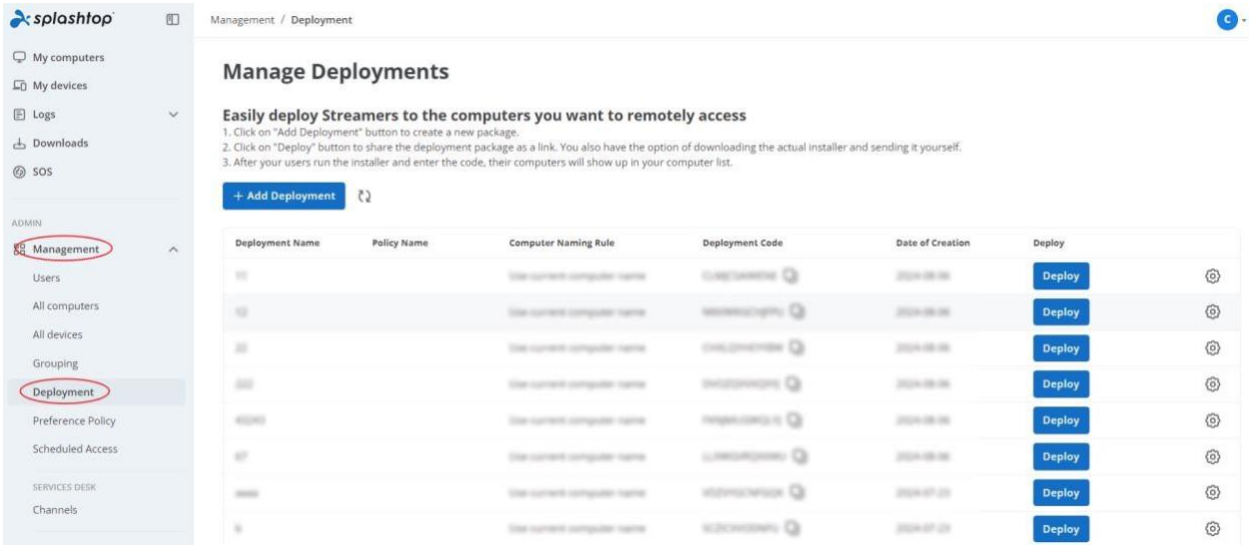
- **合规与审计：**确保支持会话符合内部 IT 或行业合规性要求。
- **故障排除：**详细查看在故障排除过程中执行的具体命令和发生的文件传输操作。
- **培训和质量控制：**使用会话记录来评估团队绩效并提供针对性指导。

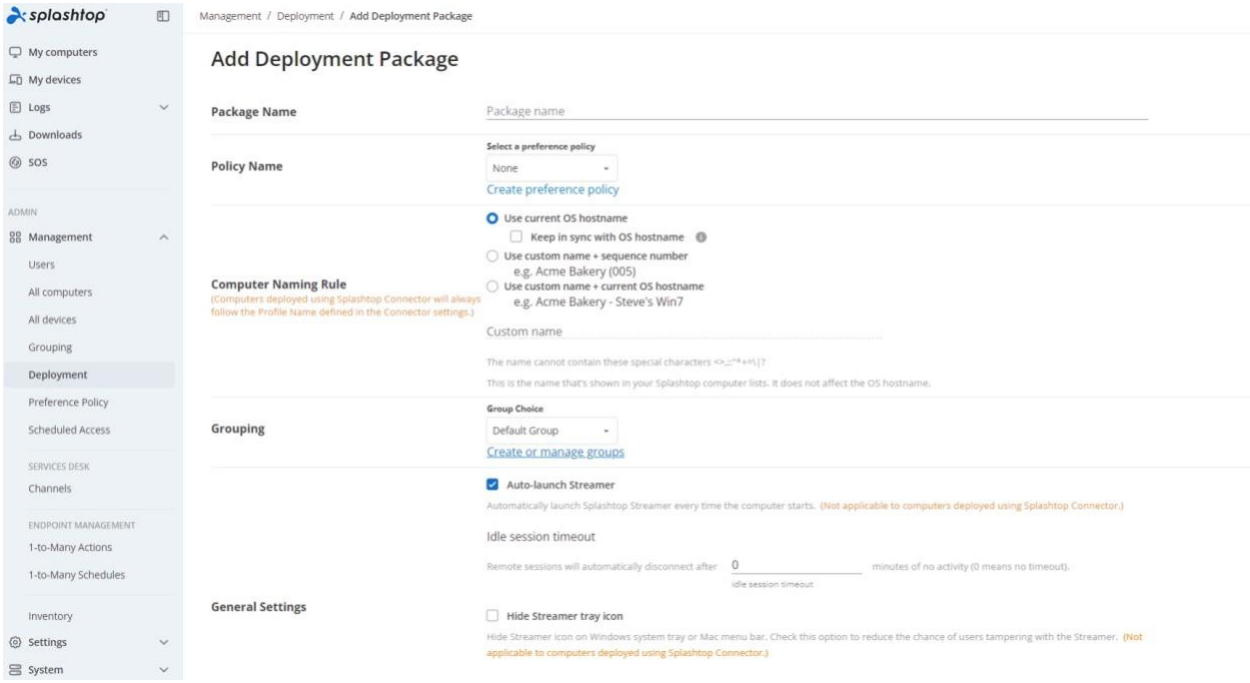
部署

部署套件可以快速轻松地在电脑中安装和配置 Streamer。管理员可以根据公司安全策略创建不同的自定义部署套件。

必须在要远程连接的电脑上安装 Splashtop Streamer。仅需4步即可完成。

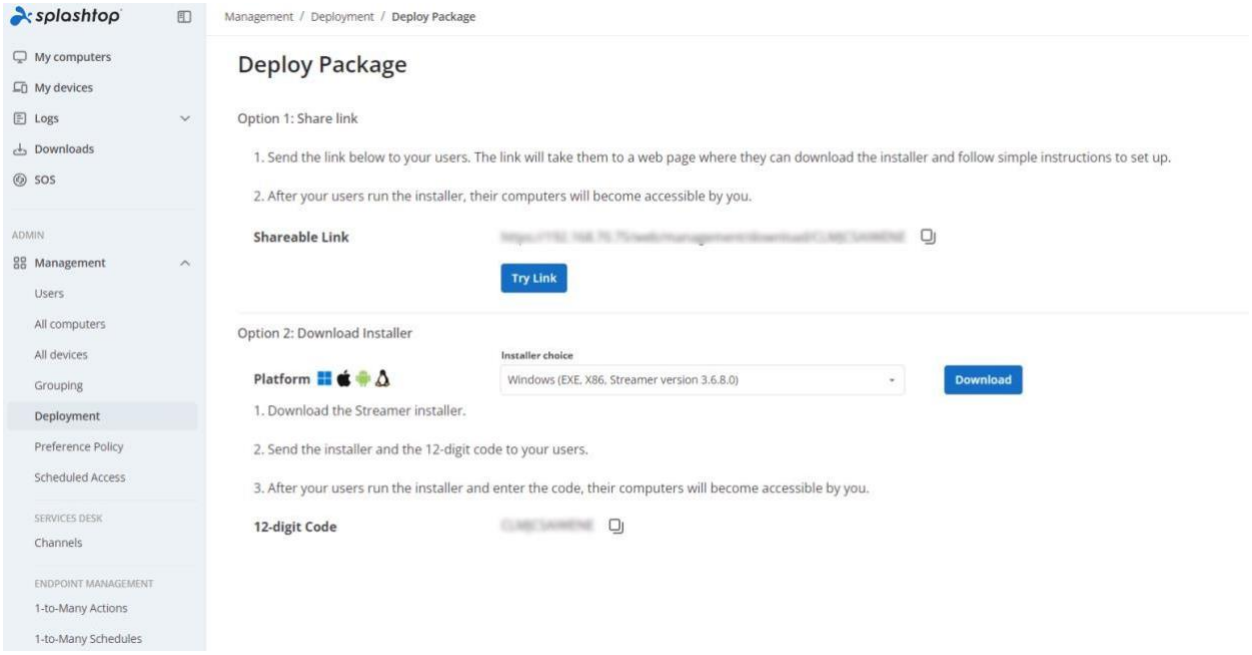
1. 创建部署套件：前往 *https://{gateway}* > *管理* > *部署*。部署套件包括部署 Streamer 和唯一的12位部署码。





2. 为新建的部署套件选择 Deploy 。

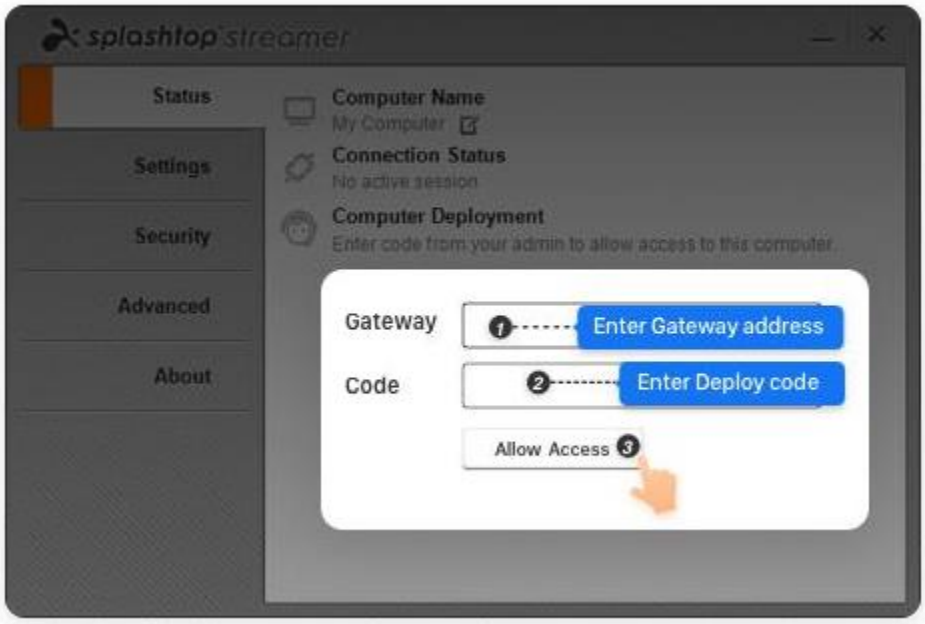
3. 让用户安装 streamer。可以将部署套件链接发送给用户。通过点击此链接，您的用户可以下载 Streamer 安装程序并运行该文件。还可以将 Streamer 安装程序文件直接发送给用户，可通 Dropbox、电子邮件等方式。



或可自行安装 Streamer。Windows 或 Mac 电脑上的 Streamer 安装可以通过命令行可执行文件或 MSI 以静默方式完成。借助 RMM 工具、Microsoft SCCM 或 Microsoft 组策略自动批量部署电脑是最简单的方法。

4. 使用部署码激活 Streamer。安装 Streamer 后， 在 Gateway 字段输入 *{Gateway IP/FDQN:Port}*，在代码字段输入部署码，然后单击**允许访问**以激活。

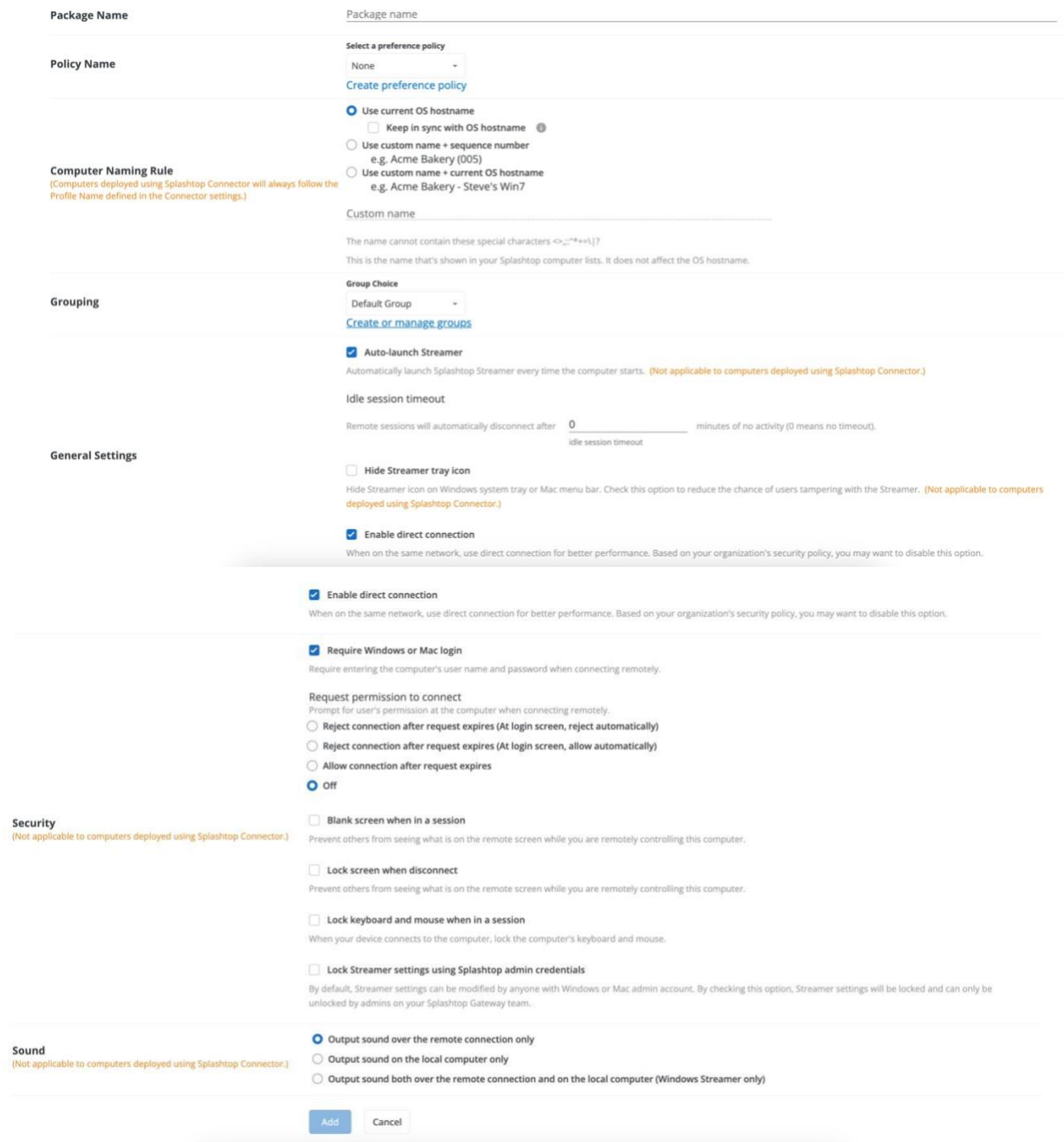
443是默认端口，在输入 Gateway 地址时可忽略。



团队管理员可以在管理控制台详细配置 Streamer 的访问权限。

部署选项

可以在创建部署套件时指定部署选项。下面是这些部署选项的含义。



选项	描述	注意
套件名称	输入唯一的名称以识别部署套件。	有助于区分不同的部署套件。
策略名称	选择首选项策略或创建新策略。	确定会话设置、质量和安全选项。
电脑命名规则	- 使用当前操作系统主机名：使电脑名称与操作系统主机名保持同步。 - 使用自定义名称 + 序列号：使用递增数字自定义电脑名称（例如，“Acme Bakery-001”）。 - 使用自定义名称或当前主机名：允许自定义名称，但如未指定，则默认使用操作系统主机名。	在 Splashtop 管理控制台中按可识别名称整理电脑。
分组	将电脑分配给特定组（例如“默认组”）。	使用“创建或管理组”链接添加/编辑组。
自动启动 Streamer	电脑启动时自动启动 Streamer。	不适用于 Splashtop Connector 部署。

空闲会话超时	在指定的非活动时间结束后自动断开会话。	设置为 '0' 表示无超时。
隐藏 Streamer 托盘图标	从系统托盘/菜单栏中删除 Streamer 图标，以防止用户篡改。	不适用于 Splashtop Connector 部署。
启用直接连接	允许直接连接，以提高同一本地网络的性能。	
需要 Windows 或 Mac 登录	远程访问需要登录凭据的选项： - 提示用户权限 - 如未授权则拒绝（自动拒绝） - 如未执行任何操作则自动允许连接（自动允许） - 完全关闭该功能。	有助于加强远程访问的安全性和控制。
隐私屏	隐藏会话期间的远程屏幕内容以保护隐私。	
断开连接时锁屏	会话结束后自动锁定远程电脑的屏幕。	
锁定键盘和鼠标	防止本地用户在会话期间与电脑交互。	

锁定 Streamer 设置	仅允许管理员更改 Streamer 设置 。	
声音	声音输出选项： - 仅远程连接 - 仅本地电脑 - 远程电脑和本地电脑（仅限 Windows Streamer）	允许在会话期间配置音频路由 。

标记为“不适用于通过 Splashtop Connector 部署的电脑”的功能可能无法按预期运行，因为 Connector 通过提供直接部署机制绕过了某些标准部署功能。

首选项策略

简介

首选项策略是一种工具，用于远程配置已部署的 Streamer 的 Streamer 设置，可从 Splashtop Gateway 网络控制台进行配置。通过将 Streamer 分配到策略，可以配置和覆盖现有的 Streamer 设置，无需重新部署 Streamer 或在本地端点手动更改设置。

所需的 Gateway 版本：v3.24.0 或更高

平台

目前，只有 **Windows** 和 **Mac** Streamer（**v3.5.2.5** 及更高版本）可以添加到首选项策略中。

用途

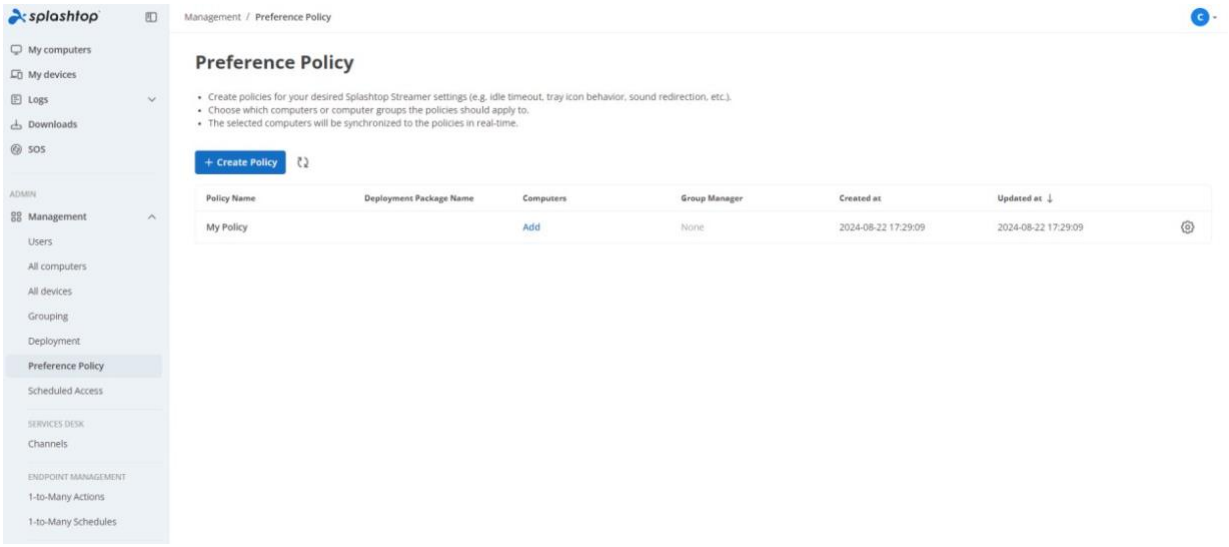
创建策略

- 概述

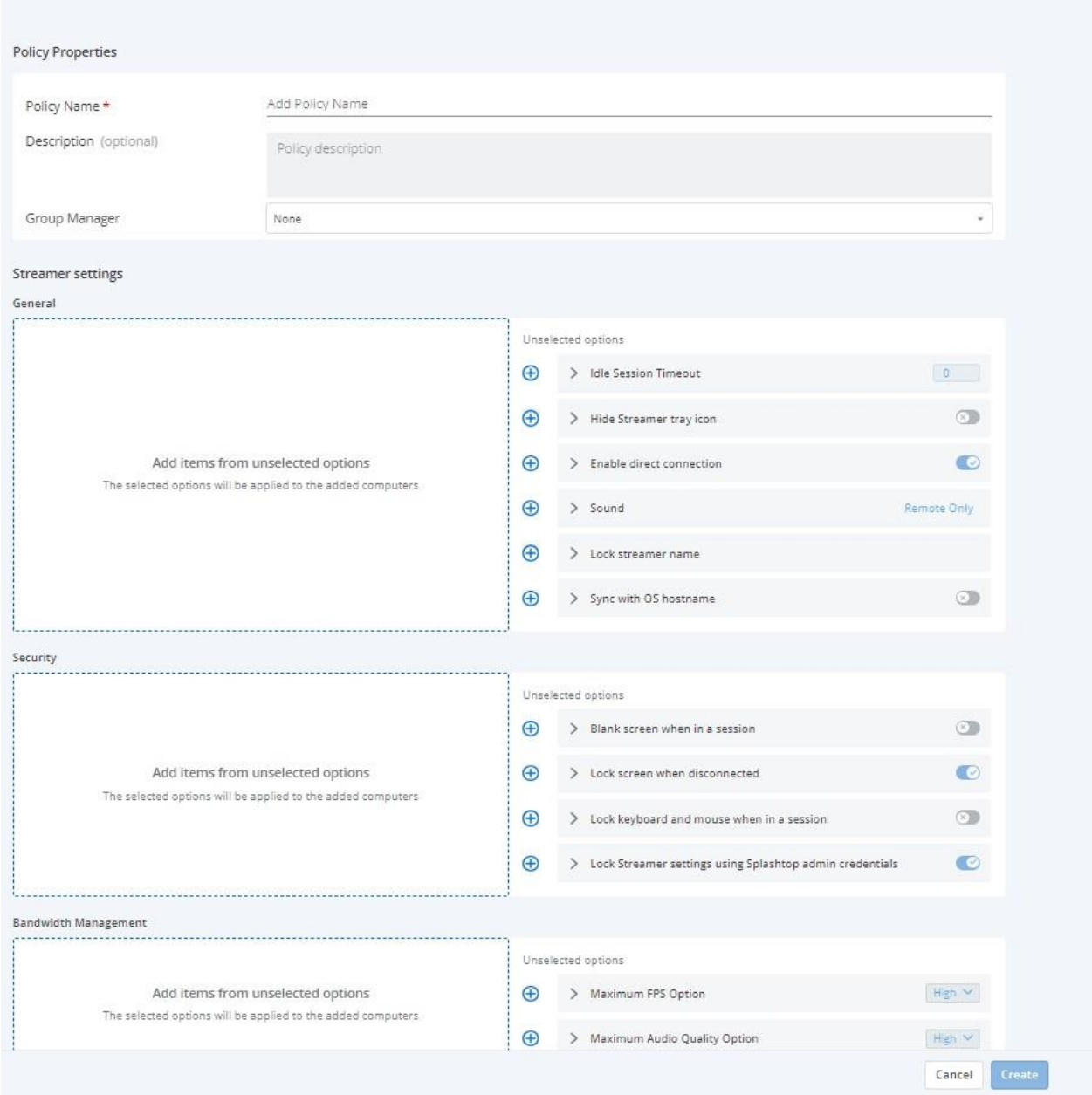
要创建新策略，先登录 Splashtop Gateway 网络控制台，将鼠标悬停在**管理**上，然后单击下拉菜单中的**首选项策略**。然后，单击**创建策略**。

如果尚未创建任何策略，则将看到以下界面。

如果已创建策略，则会看到以下页面。

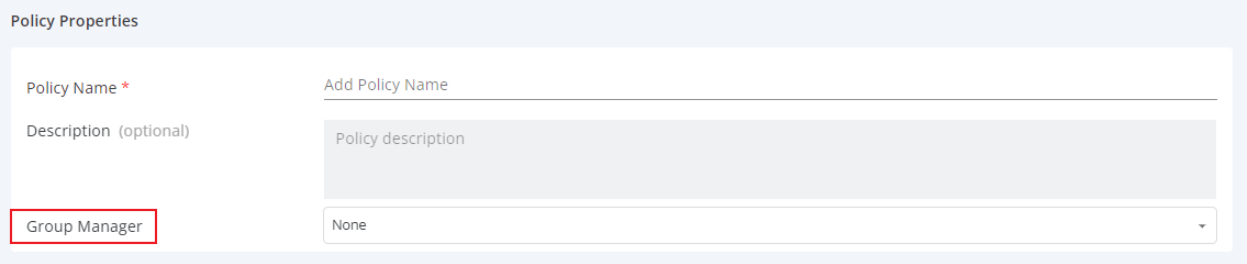


除了**名称**和**描述**，还有三个主要类别：**通用**、**安全性**和**带宽管理**。



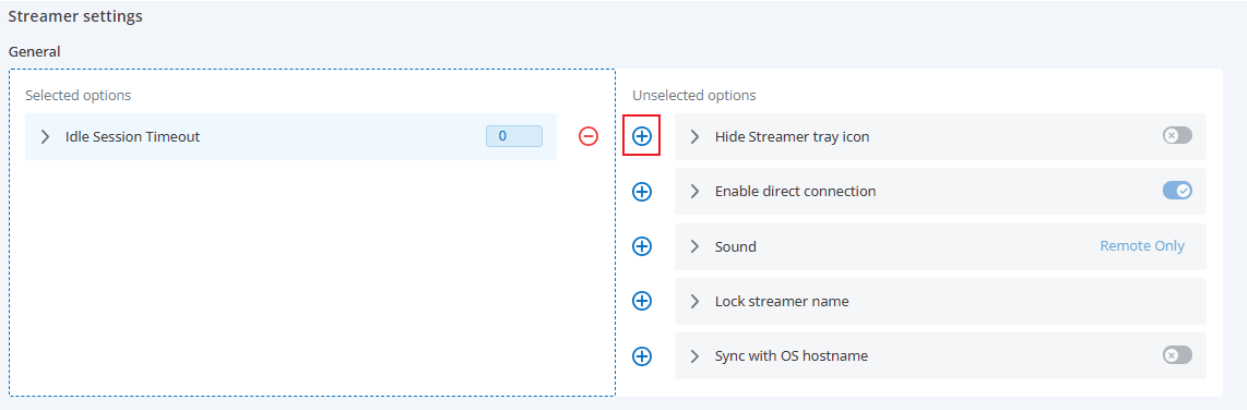
这三个类别都被分为左右两栏。左侧一栏 （已选选项） 包含已添加到策略中的设置。右侧一栏 （未选选项） 包含可以选择添加到策略中的设置。

还可以为策略分配**组管理员**。

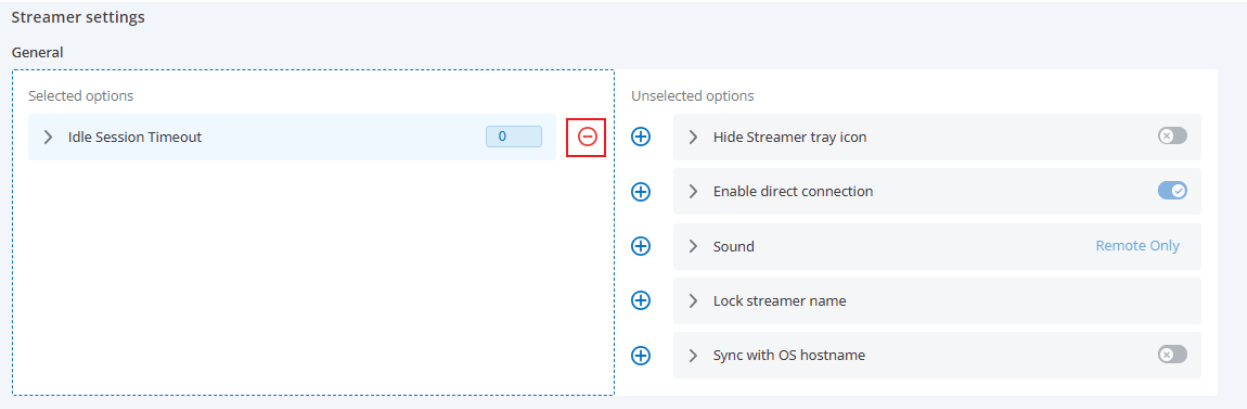


- 向策略添加和删除项目

要将项目添加到策略中，请单击蓝色加号按钮。所选项目将移动到所选选项的左侧一栏。

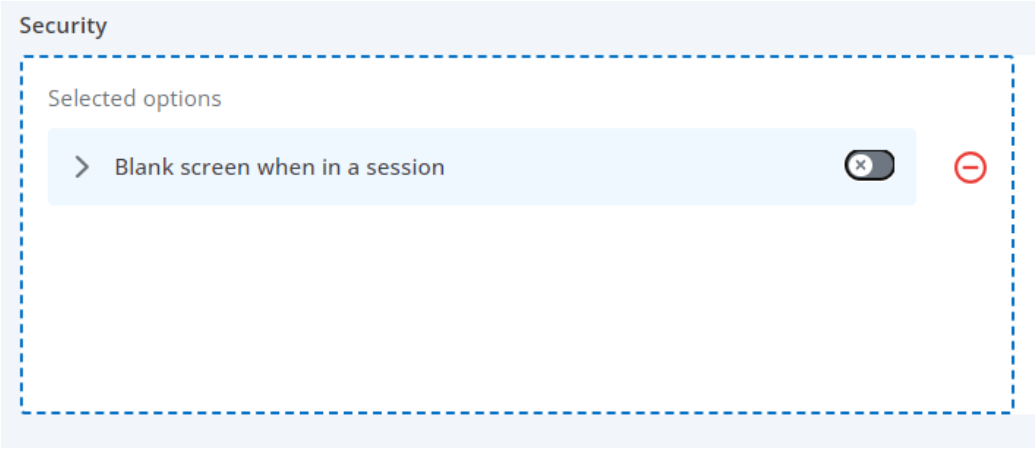


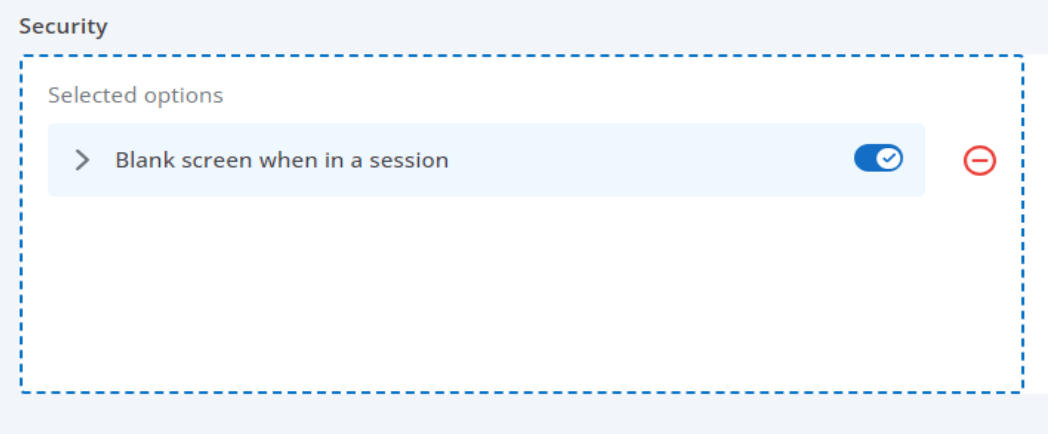
如果要从策略中删除项目，请单击红色的减号按钮。所选项目将移动到未选选项的右侧一栏。



- 配置添加项的值

将项目添加到策略后，可以配置其值。大多数项目都有可配置的开或关的二进制值。如果开关按钮显示为灰色，则该值设置为关。如果开关按钮显示为蓝色，则该值设置为开。

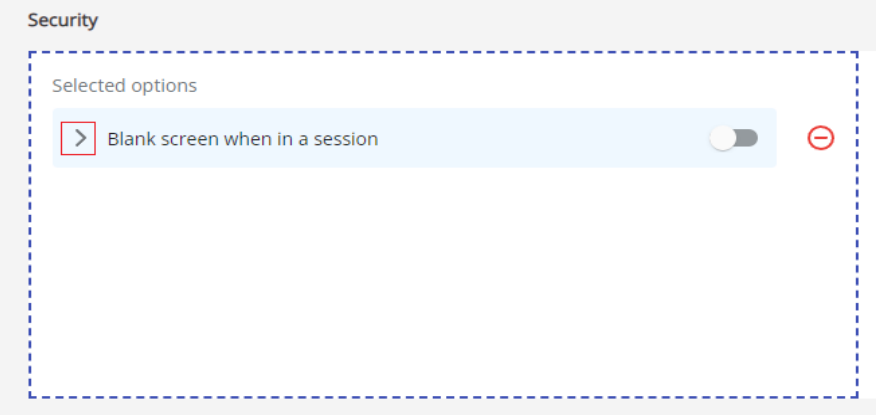


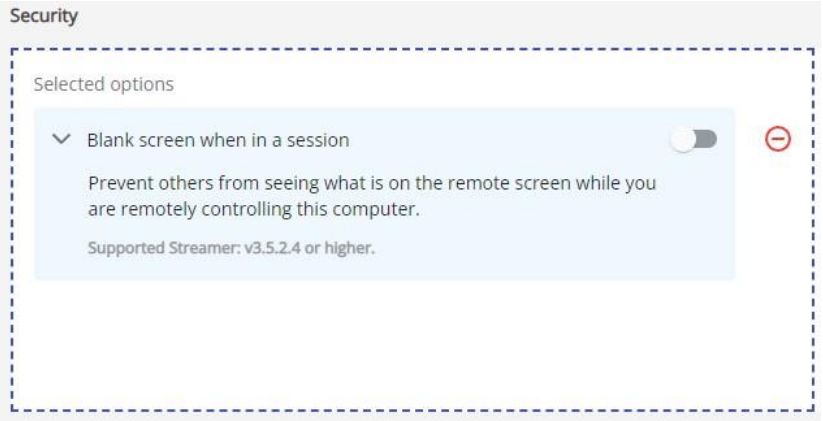


初始状态下，各项都设置为默认值。例如，上面的隐私屏设置默认处于关闭状态。

- 了解配置项

如果不确定某个配置项的功能，可以单击尖括号图标以显示简要描述。

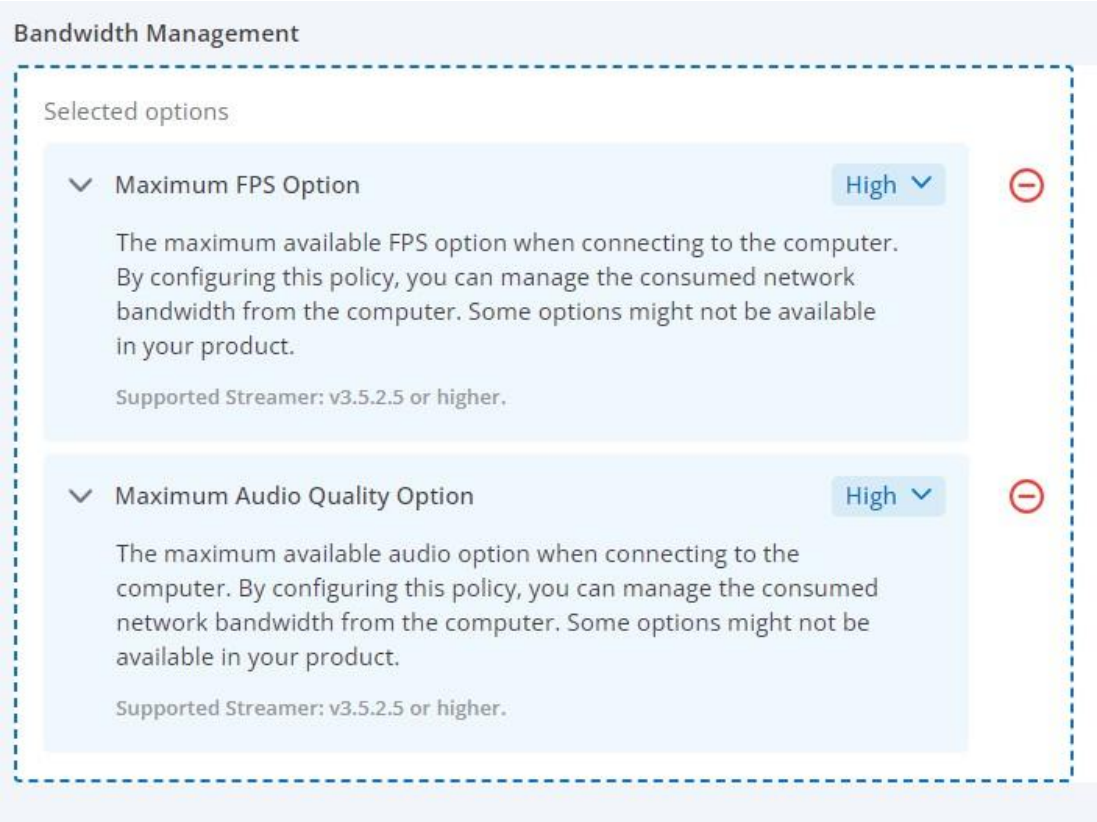




- 带宽管理

带宽管理是一个新增工具，允许根据 FPS 和音频质量参数来控制带宽。

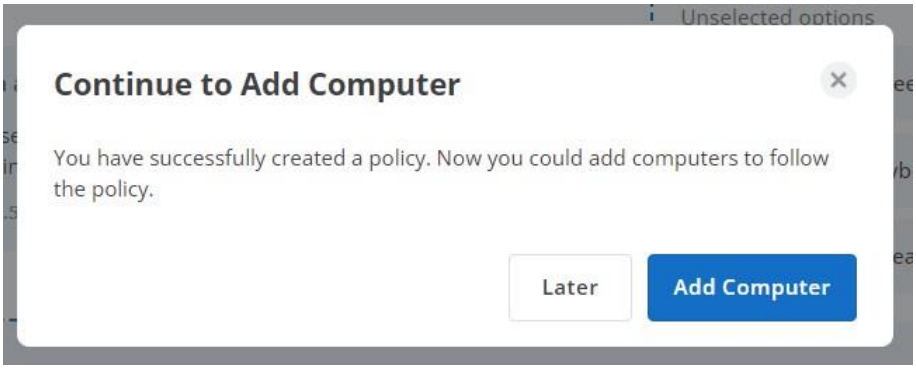
对于“**最大 FPS 选项**”和“**最高音质选项**”，如果选择最高值（最大 FPS 选项：“超高”，最高音质选项：“超高 - 384k”），则效果等同于完全不将这些项目添加到策略中：用户没有带宽限制。



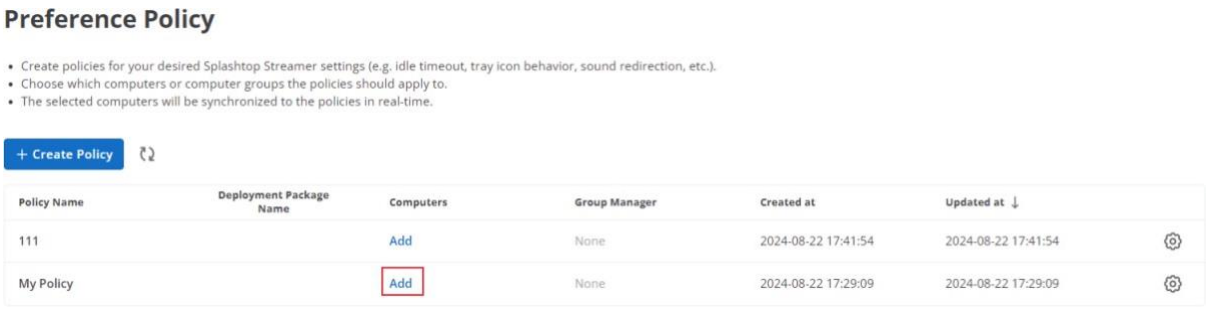
- 添加电脑

创建策略后，可以向该策略添加电脑。

直接在弹出窗口点击**添加电脑**。

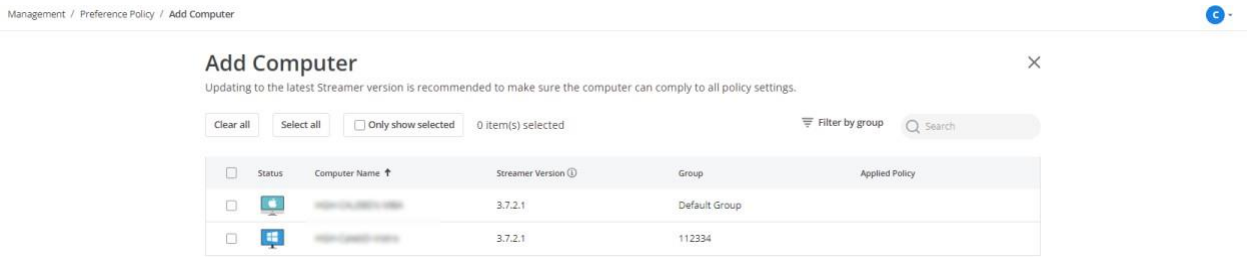


或可在首选项策略仪表盘中单击**添加**。

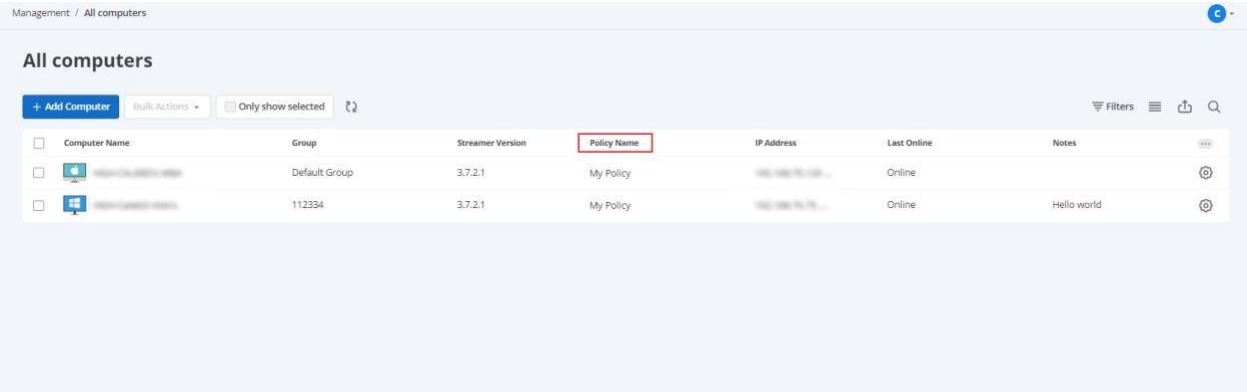


选择要应用策略的电脑或电脑组，然后单击保存。另请确保 Splashtop Streamer 已更新到最新版本。

请注意，只有 Streamers v3.5.2.5 或更高版本会在可以添加到策略的电脑列表中显示。

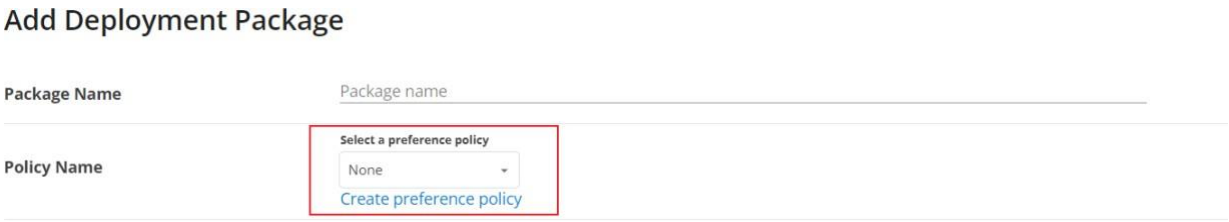


关联策略将在“管理 - 所有电脑”页面的新增列“策略名称”中显示。



将首选项策略分配到部署套件

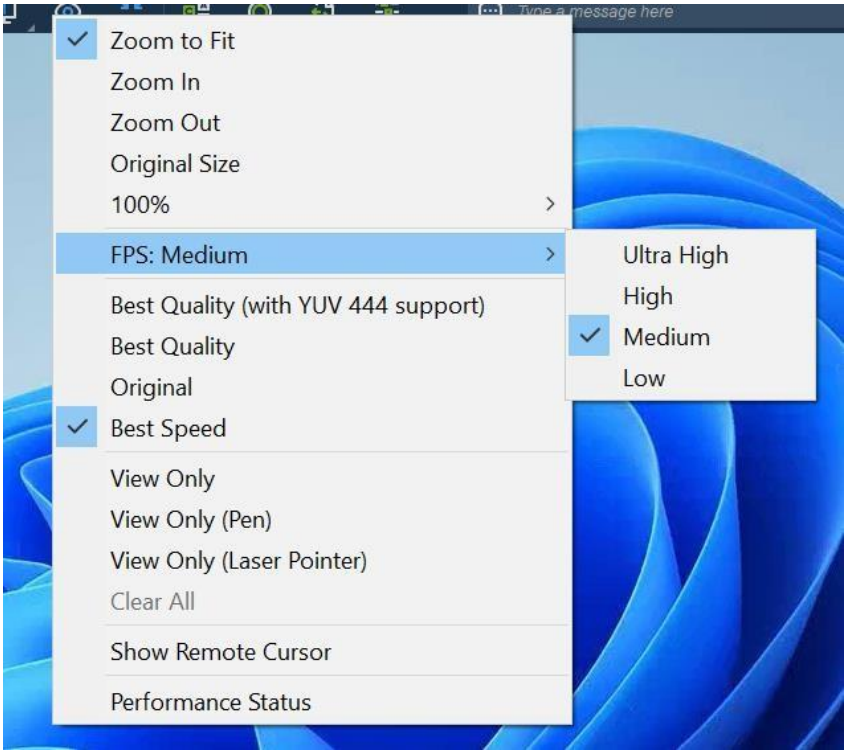
从Splashtop On-Prem Gateway v3.24.0开始，Streamer 可在部署时遵循特定的首选项策略。从部署页面创建新的部署套件时，从下图所示的下拉列表中选择已创建的首选项策略。如需详细了解如何创建新部署套件，请参阅本文：[如何设置要远程访问的电脑？]



行为

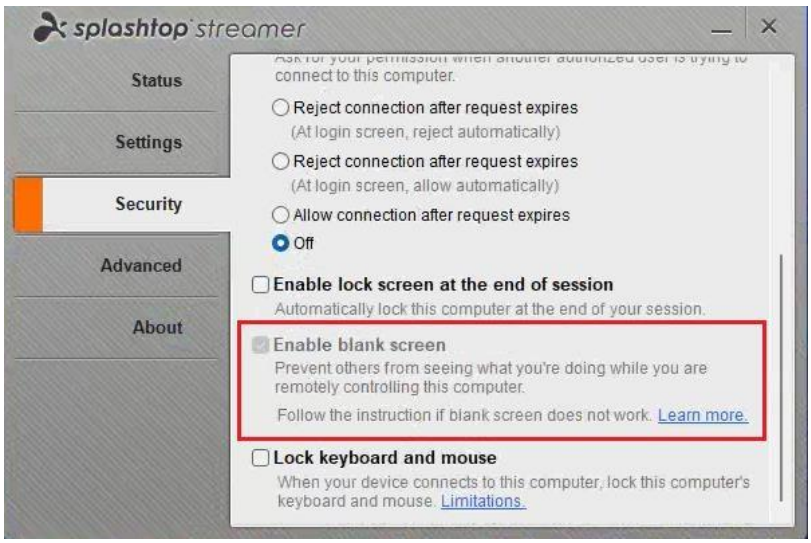
- 会话中

当用户远程访问与首选项策略关联的电脑时，已经配置的设置或限制将应用于远程会话。例如，如果首选项策略将 FPS 限制为“高”，而用户尝试将其设置为“超高”，则会弹出错误消息。

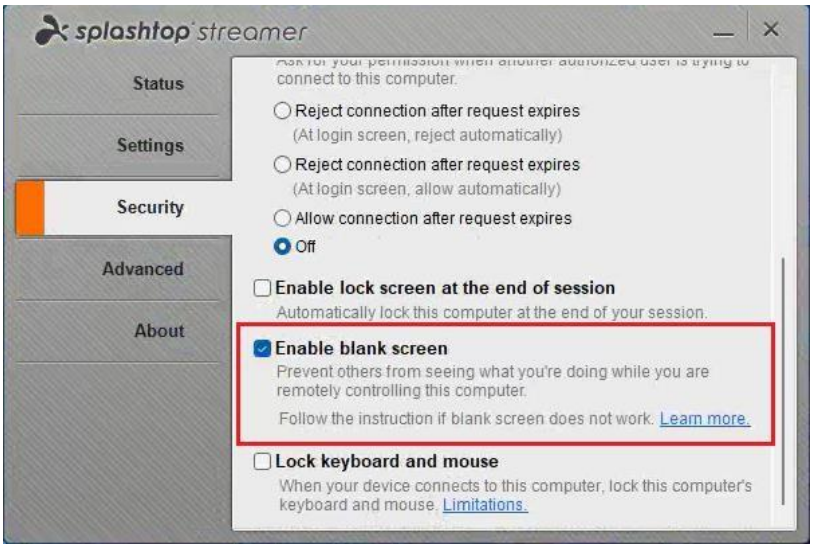


- Streamer

可在首选项策略中配置的许多配置项也可以从 Streamer 用户界面 进行配置。如果策略中配置的设置与 Streamer 设置重合，则该设置将显示为灰色，并且无法从 Streamer 用户界面进行配置，除非从该策略解除关联。例如，如果在首选项策略中启用了隐私屏设置，那么对于已应用此策略的所有电脑，隐私屏设置在 Streamer 用户界面中将处于锁定状态。



如果从策略中删除电脑，或从策略中删除此配置项（在本例中为隐私屏设置），则可再次从 Streamer 用户界面配置该设置。但是，此配置项的值不会自动切换回默认值（注意，隐私屏设置默认关闭），而是会保留之前的给定值。



单点登录 （SSO）

如何申请新的 SSO 方法？（SAML 2.0）

Splashtop 目前支持使用 SAML 2.0 身份提供商创建的凭据登录 Gateway 和 *Splashtop On-Prem 应用程序*。请按照以下说明为团队申请 SSO 方法。

要求

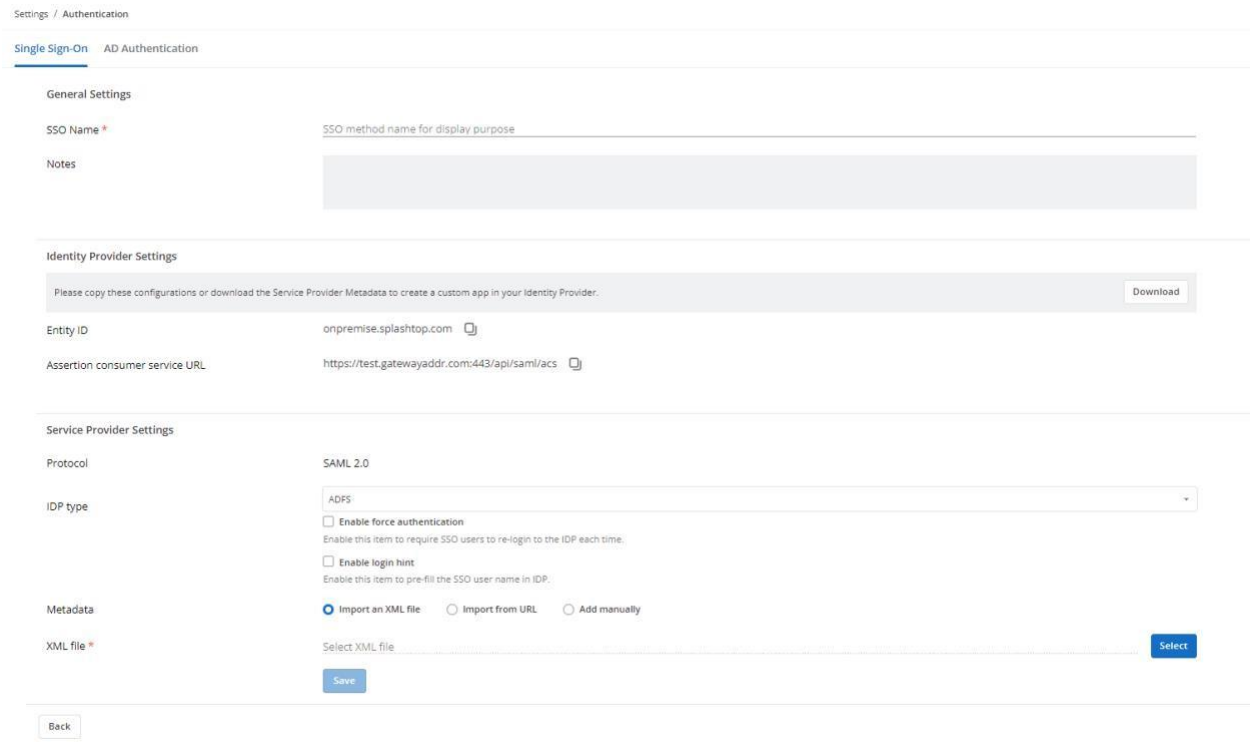
- **Splashtop Gateway v3.24.0** 或更高版本

输入 IDP/X.509 证书信息

1. 使用所有者账户登录 Gateway，然后转到管理/设置/身份验证/单点登录。

2. 单击“添加”以添加 Gateway URL。请填写正确的 Gateway URL，以确保 Gateway 和 IDP 之间的连接。

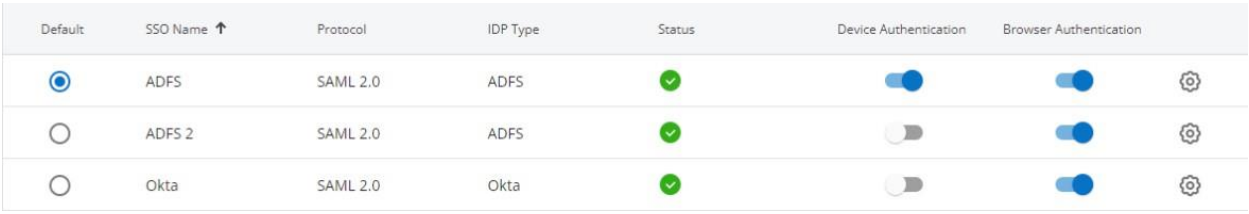
3. 点击“添加 SSO 方法”，然后输入所需信息并保存 SSO 方法的设置。



- **通用设置**
  1) **SSO 名称**：输入 SSO 方法的名称。
  2) **备注**：输入 SSO 方法的备注。
- **身份提供商设置**
  1) **实体 ID**：请从 Gateway 复制实体 ID 和断言消费者服务 URL，然后将其粘贴到 IDP。
  2) **断言消费者服务 URL**：请从 Gateway 复制实体 ID 和断言消费者服务 URL，然后将其粘贴到 IDP。
  3) **下载服务提供商元数据**：此外，我们还提供元数据下载，以便在 IDP 中导入 SP 的元数据。
- **服务提供商设置**
  1) **协议**：已修复为 SAML 2.0。
  2) **IDP 类型**：选择 IDP 类型。
  - **元数据**（输入 **IDP SSO 登录 URL**、**IDP 颁发者**和 IDP 中的 X.509 证书信息：Okta、Azure AD、JumpCloud、OneLogin 或 ADFS 或其他 IdP）

1) 使用元数据导入自动填充设置
   - 上传 XML 或从 URL 导入
2) 或手动添加
   - 对于 X.509，需要从 IdP 复制内容，并将其粘贴到以下字段。
   - 注意 http 地址与 https 地址

4. 点击“保存”将启用 SSO 方法。



- 可在齿轮按钮中启用/禁用/删除 SSO 方法。
- 可以根据不同 SSO 方法选择禁用设备身份验证，只需在“设备身份验证”列下取消选中相应的 SSO 方法即可。
- 可以根据不同 SSO 方法选择禁用浏览器身份验证，浏览器身份验证”列下取消选中相应的 SSO 方法即可。
- 还可以设置默认 SSO 方法。单击“默认”列下相应 SSO 方法的单选按钮。

注意：

- **Gateway**（v3.24.0 或更高版本）和 **Splashtop On-Prem 应用程序**（v3.5.8.0 或更高版本）支持 SSO 登录。

创建 SSO 用户

在 Gateway 上设置 SSO 方法后即可添加 SSO 用户。

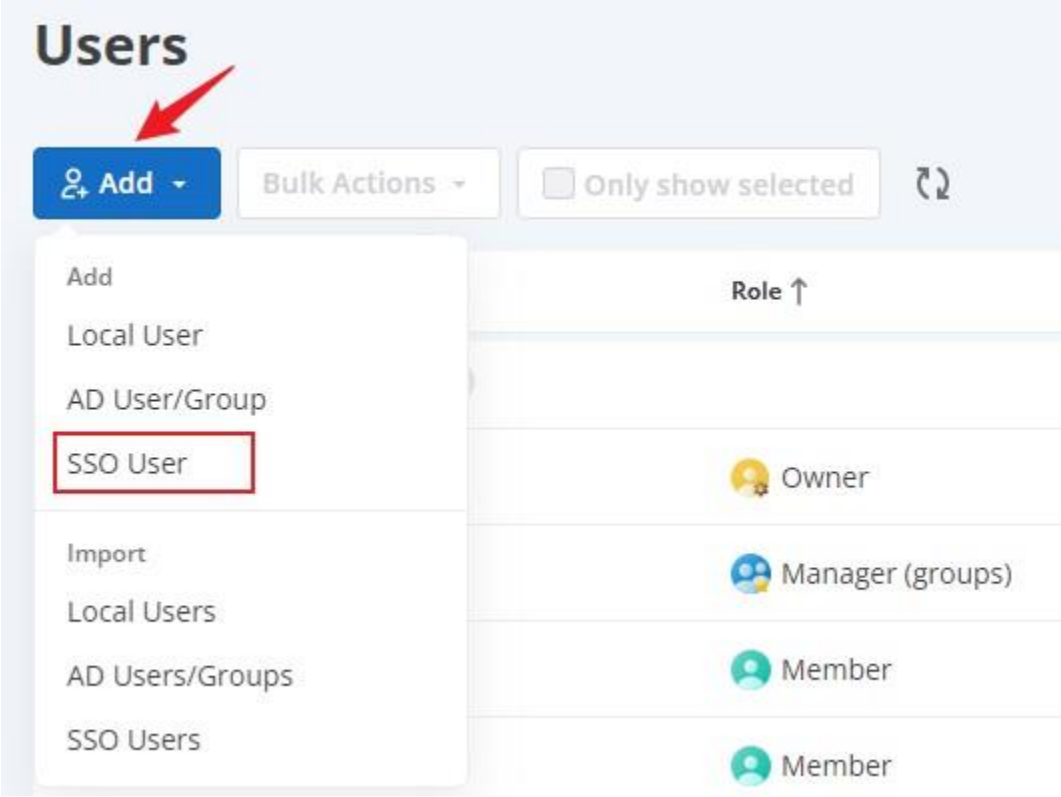
要求

- **Splashtop Gateway v3.24.0** 或更高版本

添加 SSO 用户

1. 按照说明**申请 SSO 方法**。

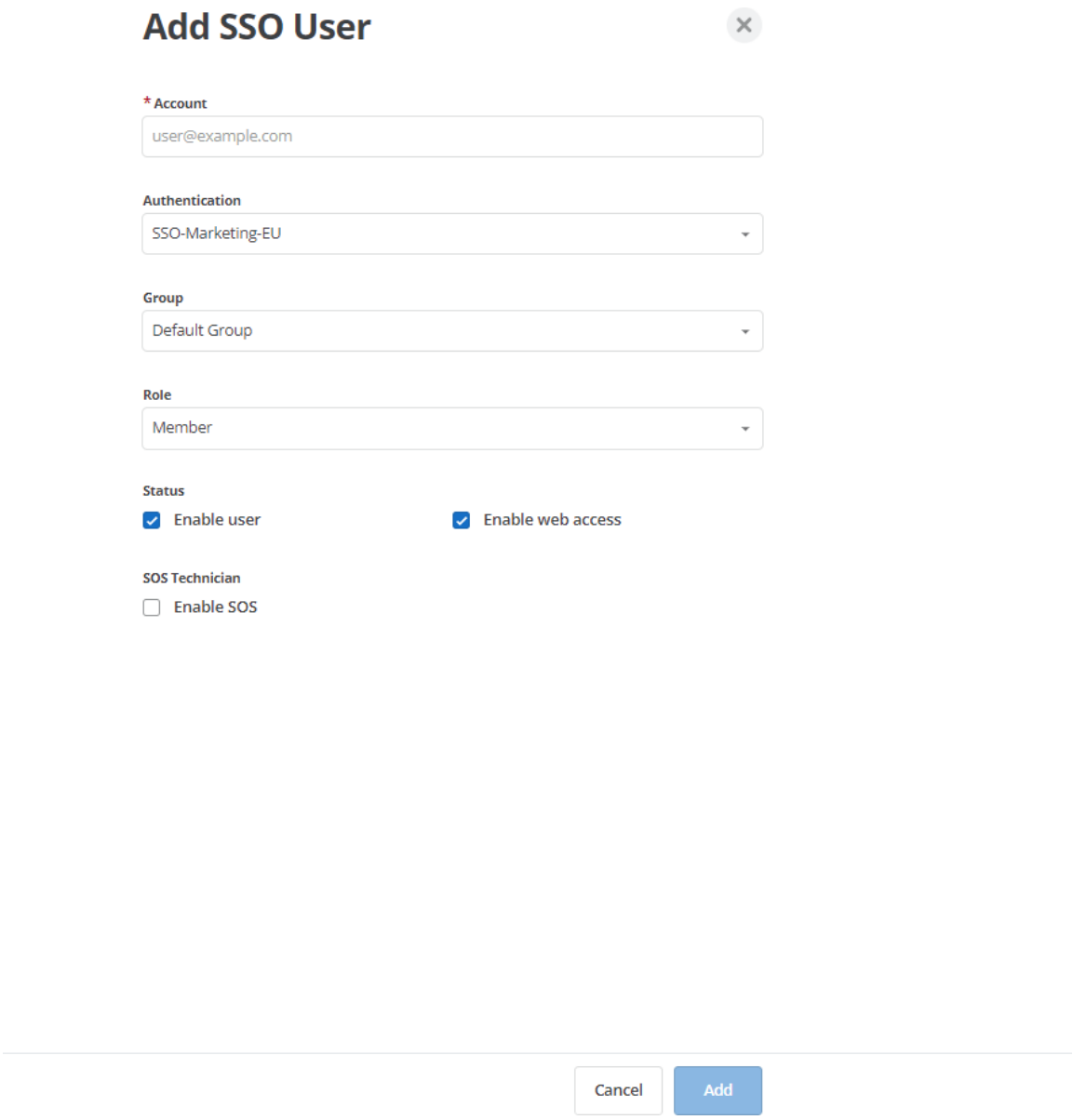
2. 导航到**管理选项卡 – 用户**，单击顶部的添加按钮，然后选择“**SSO 用户**”。



3. 输入 SSO 用户的所需信息，然后单击**添加**。

- **账户：** SSO 用户的登录账户，在 Gateway 中是唯一的。
- **身份验证：**选择要关联的 SSO 方法。
- **启用用户：**如果启用此项，则用户可以建立远程会话。否则，将禁用远程会话。
- **启用 Web 访问：** 如果启用此项，则用户可以访问 Web 门户网站。否则，将拒绝 Web 访问。
- **分组：**用户可以被分到不同组中，分组在用户管理/访问权限方面非常有效。
- **角色：**系统中有两种角色类型：
    - **管理员：** 管理员可以管理用户、电脑、授予访问权限等。管理员也可以进行远程会话。
    - **成员：**只能与被授予访问权限的电脑进行远程会话。
- **SOS 技术员：**启用 SOS 按需支持功能。

- **添加：** 将 SSO 用户添加到目标组。



添加 SSO 组/SSO 组成员

SSO 组/SSO 组成员无法手动添加，只能通过 SCIM 配置创建。

注意：SSO 组成员将继承其父级 SSO 组的用户角色和访问权限。

批量导入 SSO 用户

在 Gateway 上设置 SSO 方法并确认可以成功登录后，即可使用 CSV 文件导入用户。

要求

Splashtop Gateway v3.24.0 或更高版本

操作步骤

1. 设置 SSO 方法。（说明）

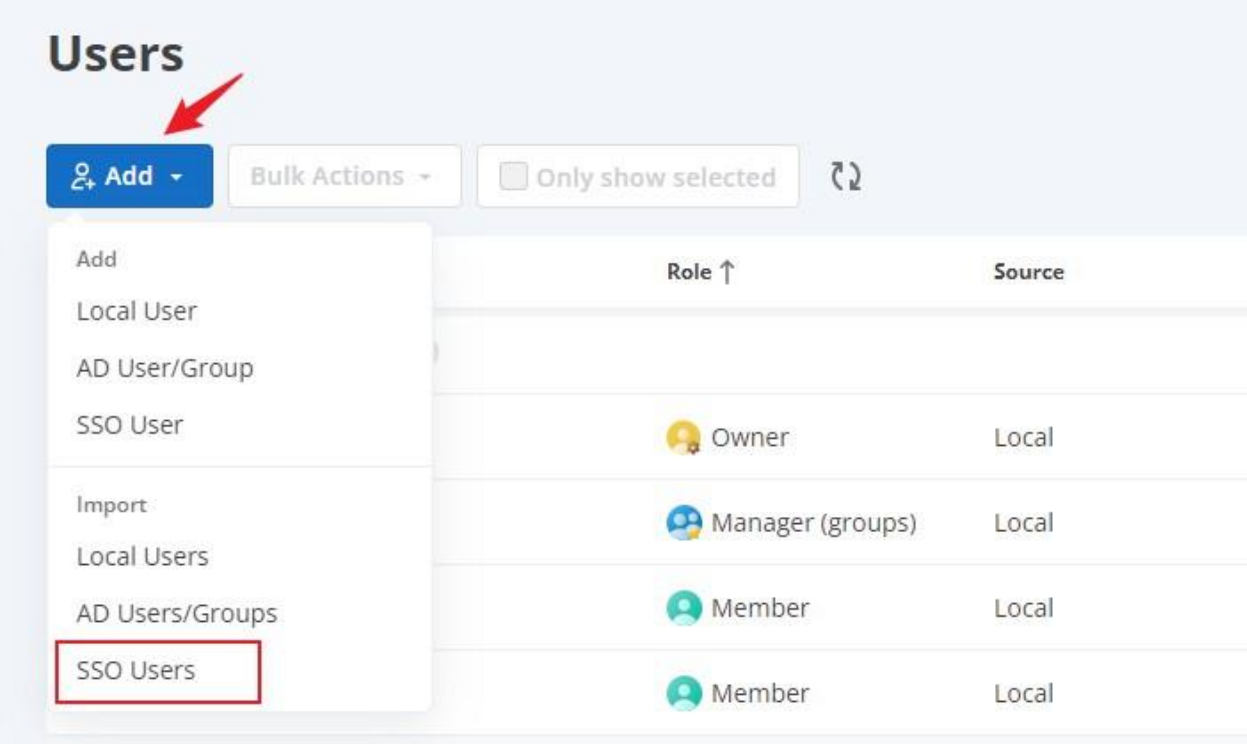
2. 使用创建的 SSO 方法创建用户（说明），或将现有用户与创建的 SSO 方法关联（说明）。

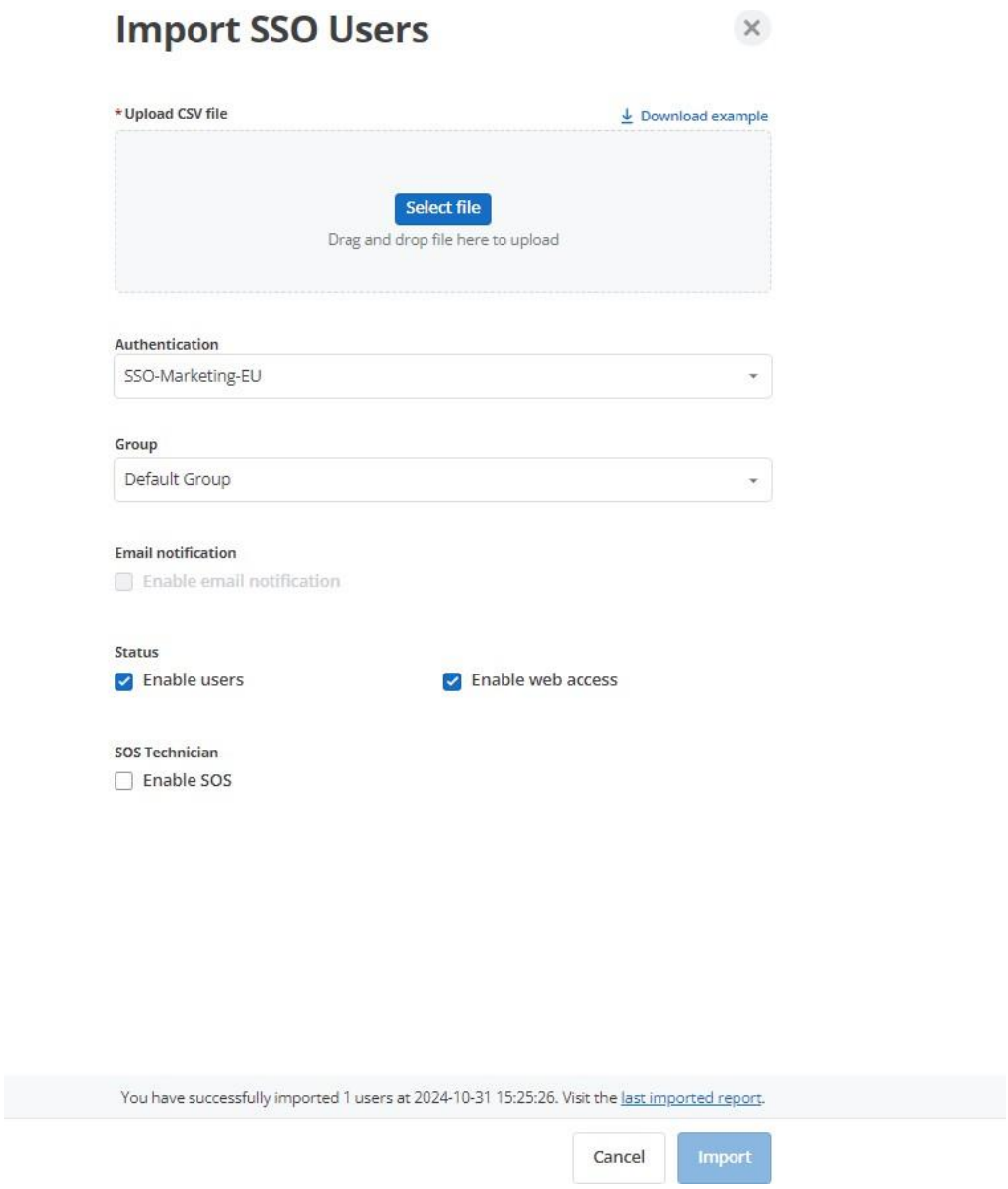
3. 使用上述用户测试登录。

4. 对于创建的 SSO 方法，可以使用 CSV 文件导入用户。

导入 SSO 用户

导航到**管理**选项卡 – **用户**，单击顶部的**导入**按钮，然后选择 **SSO 用户**。



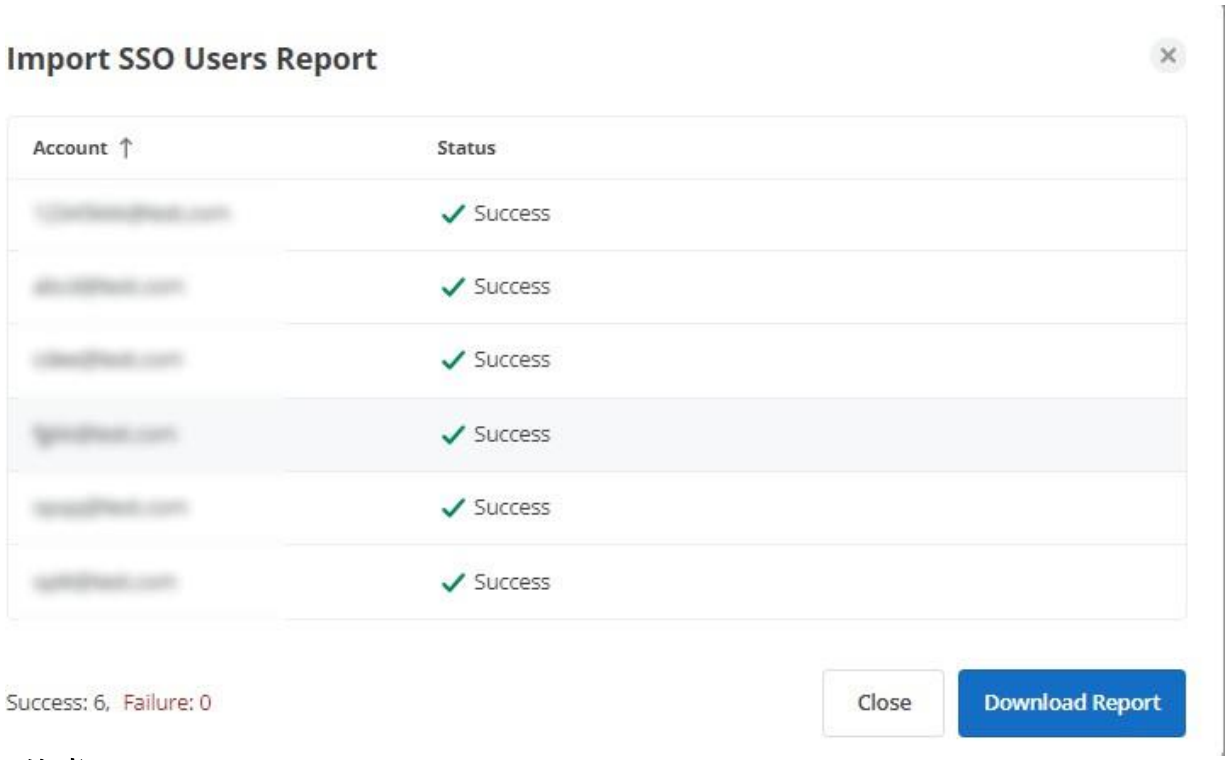


- **选择 CSV 文件**：上传包含 AD 用户列表的 CSV 文件。
- **下载 CSV 文件模板**：使用 CSV 文件模板导入 AD 用户。
- **启用邮件通知**：如果已配置 SMTP 服务器。启用此项，则用户可以收到通知邮件。
- **身份验证**：选择要关联的 SSO 方法。
- **启用用户**：如果启用此项，则用户可以建立远程会话。否则，将禁用远程会话。

- **启用 Web 访问：** 如果启用此项，则用户可以访问 Web 门户网站。否则，将拒绝 Web 访问。
- **分组**：用户可以被分到不同组中，分组在用户管理/访问权限方面非常有效。
- **SOS 技术员**：启用 SOS 按需支持功能。
- **导入**：将 CSV 文件中的 SSO 用户导入到目标组。

导入的报告

用户导入完成后， **管理员**或**所有者** 可以查看导入结果并下载导入的报告。



注意：

1. 仅支持 CSV 文件格式。
2. 文件中的数据必须采用标准格式。可以下载下方的 example.csv 文件来检查布局/格式。
3. 如果当前导入未完成，则无法导入其他 CSV 文件。

4. 所有成功导入的用户都将获得成员角色。

如何将 SSO 方法与现有团队管理员/成员关联?

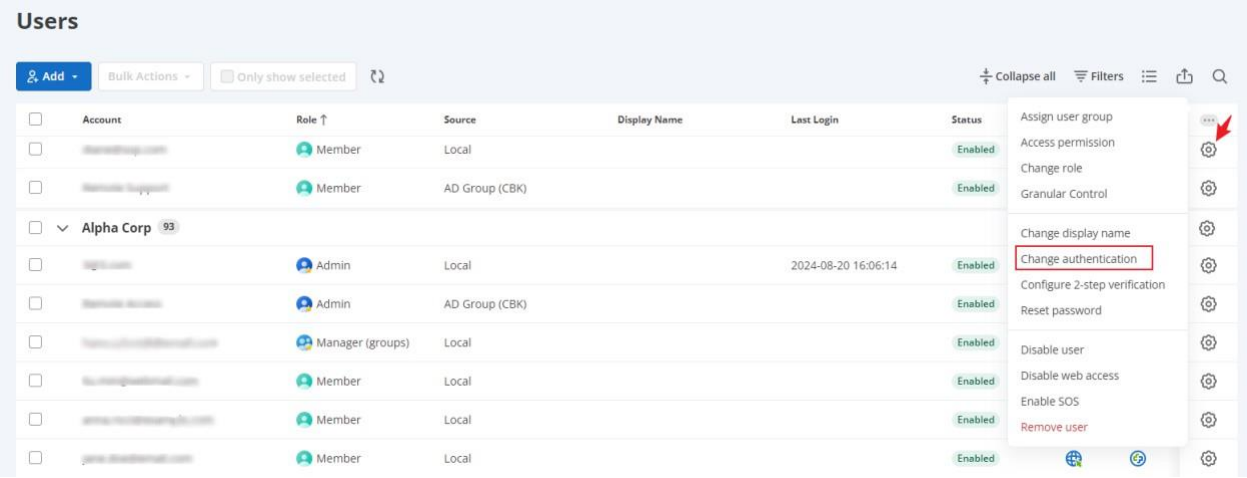
要求

- **Splashtop Gateway v3.24.0** 或更高版本

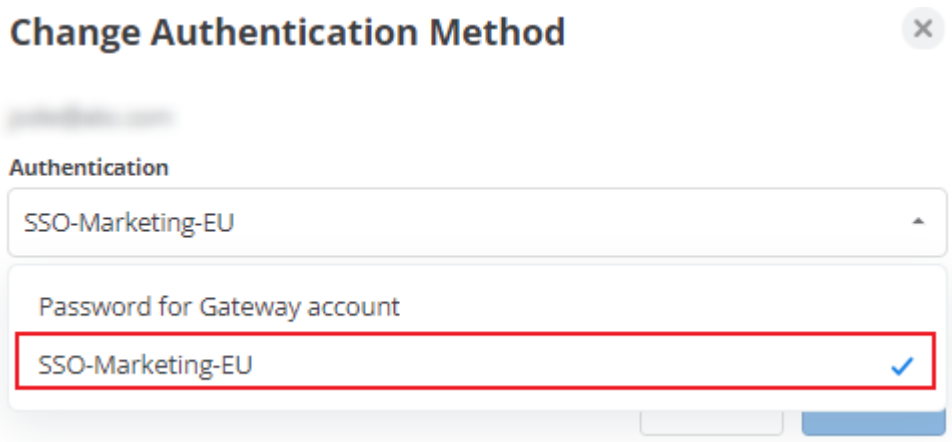
操作步骤

1. 按照说明申请 SSO 方法。

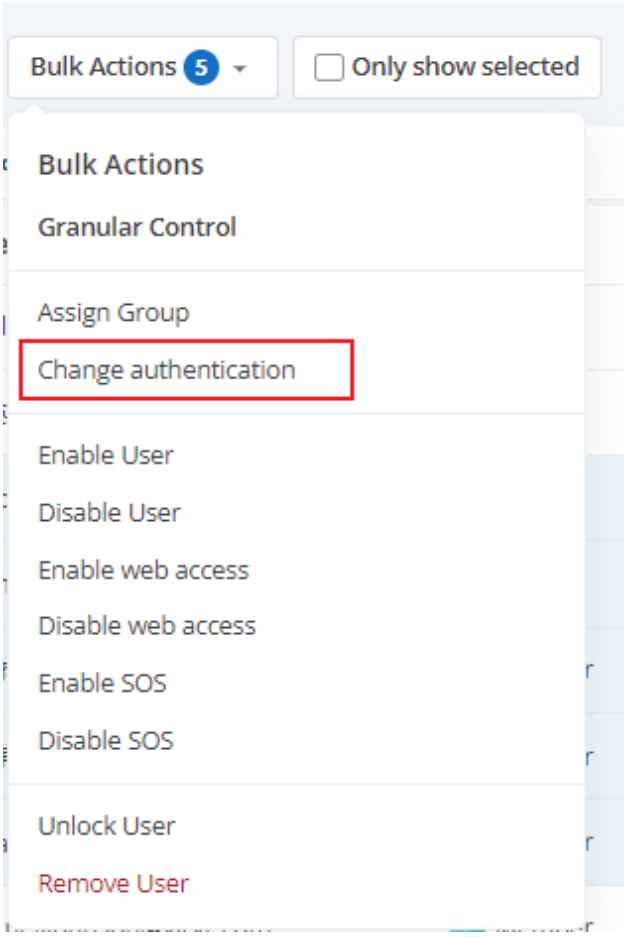
2. 登录到 Gateway → 管理 → 用户，单击要修改的用户配置文件的齿轮图标，然后选择**更改身份验证**。

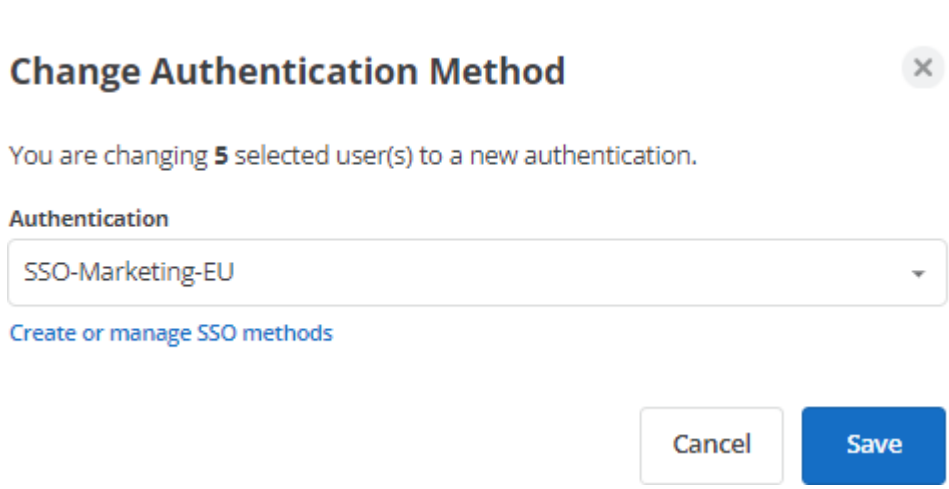


3. 选择要关联的 SSO 方法。



4. 此外，还可以通过批量操作变更用户的身份验证方式。通过单击账户左侧的复选框来选择账户。然后单击批量操作按钮进行配置更改所选账户的**身份验证**项。





注意

- 出于安全考虑，仅所有者可以更改身份验证方式。
- 所有者的身份验证方式无法更改。
- AD 用户/AD 组/AD 组成员的身份验证方式无法更改。
- 更改用户的身份验证方式后，正在进行的 Web 会话和远程/SOS 会话将中断，用户需要使用新的身份验证方式重新登录。

如何使用 SSO 账户登录?

可以使用 SSO 账户登录 Splashtop Gateway 和 Splashtop On-Prem 应用程序（v3.5.8.0 及更高版本）。

请按照以下说明使用 SSO 账户登录。

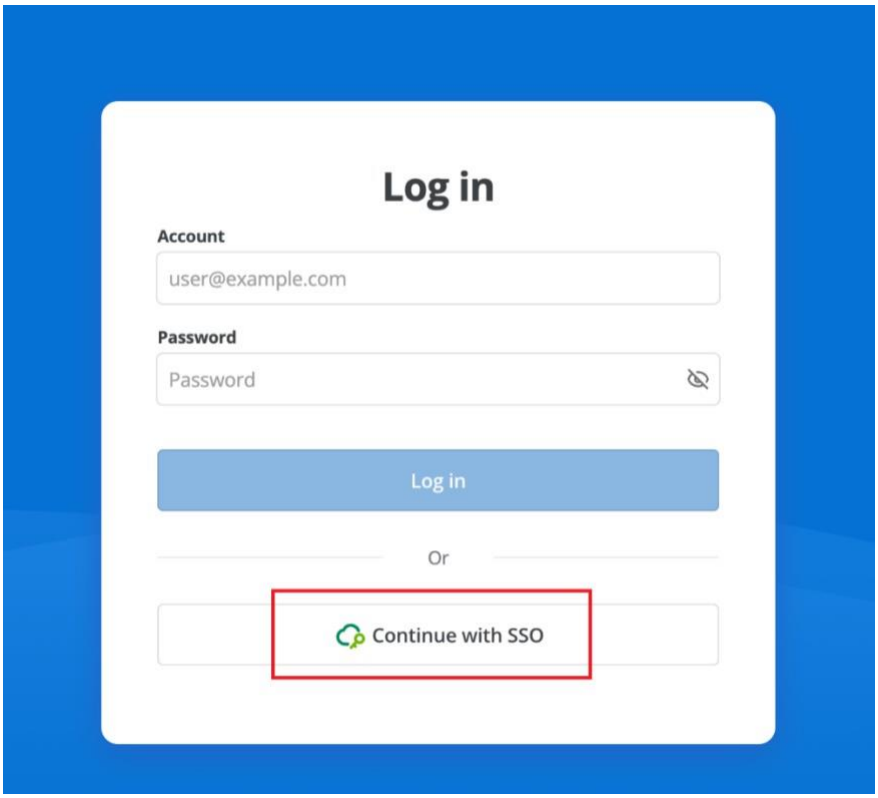
要求

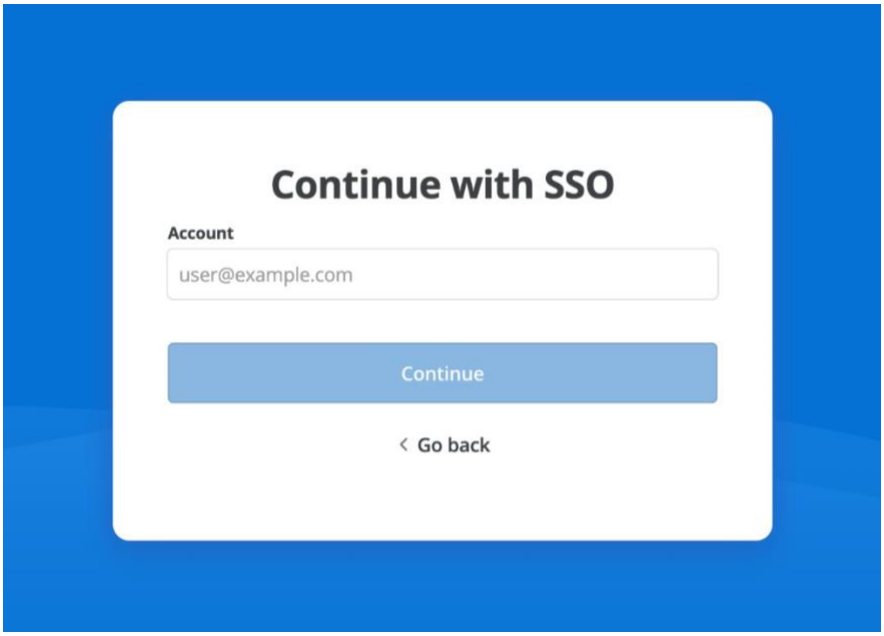
- **Splashtop Gateway v3.24.0** 或更高版本
- **On-Prem 客户端应用程序 v3.5.8.0** 或更高版本

从 Gateway 登录

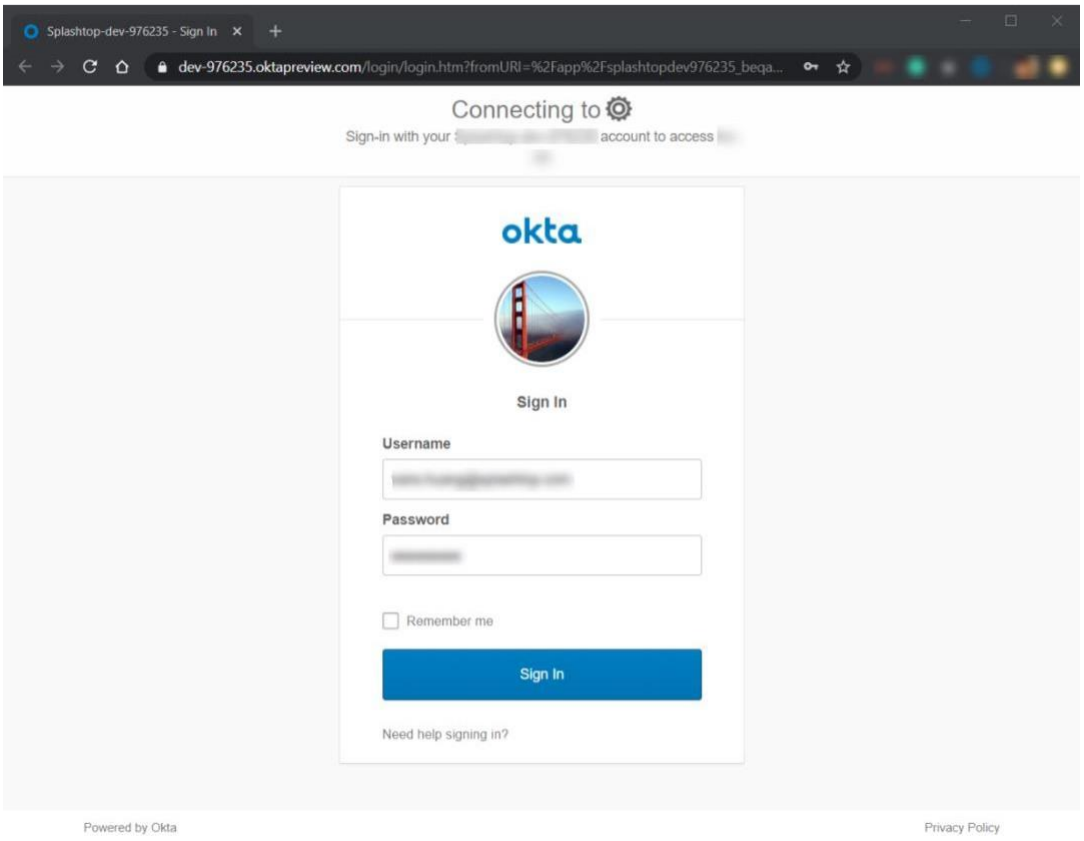
1. 输入 Gateway 地址并访问 SSO 登录页面

2. 输入 SSO 账户并登录。

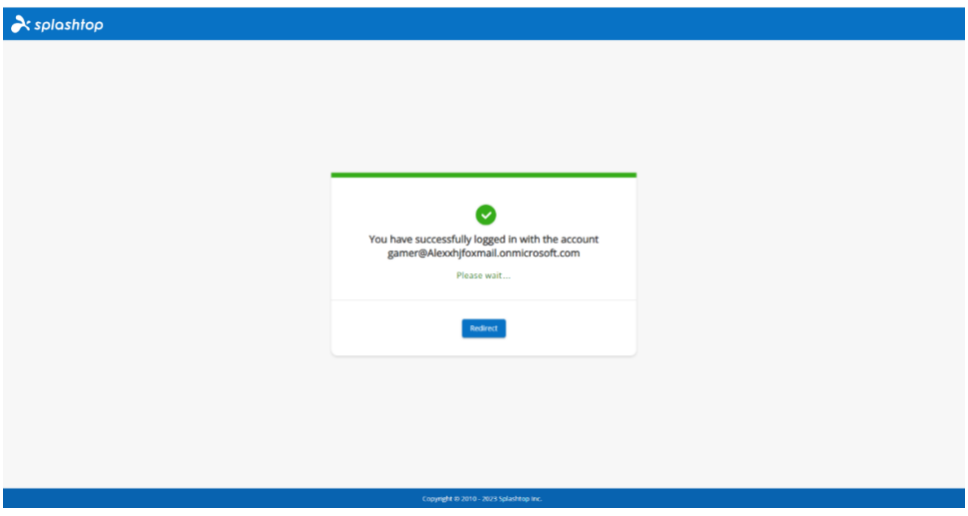




3. 单击单点登录按钮，将引导打开身份提供商门户网站。例如，Okta 门户网站。



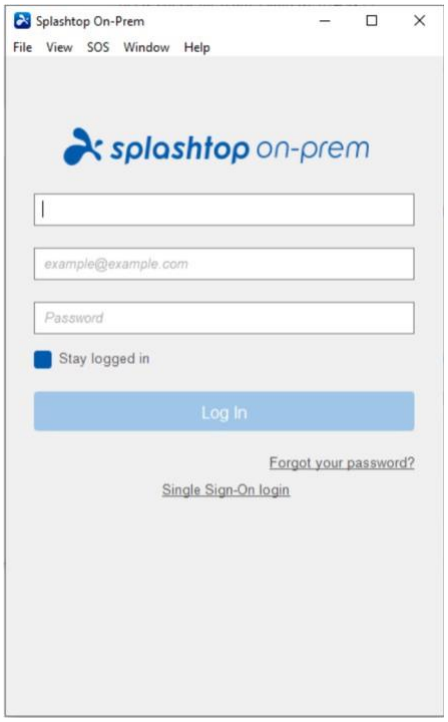
4. 登录身份提供商门户网站后，即可登录 Gateway。



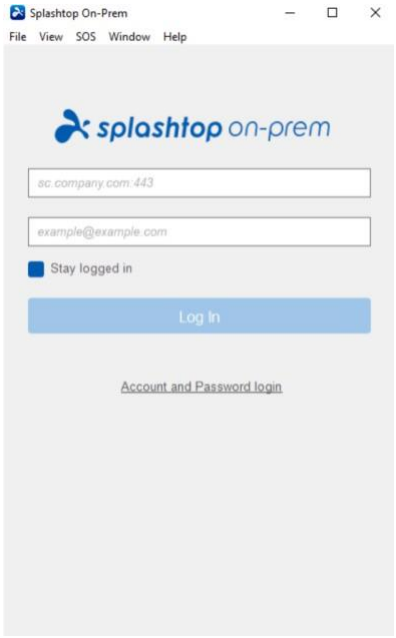
从 Splashtop On-Prem 应用程序登录

请确保使用的 Splashtop On-Prem 应用程序版本是 v3.5.8.0+。

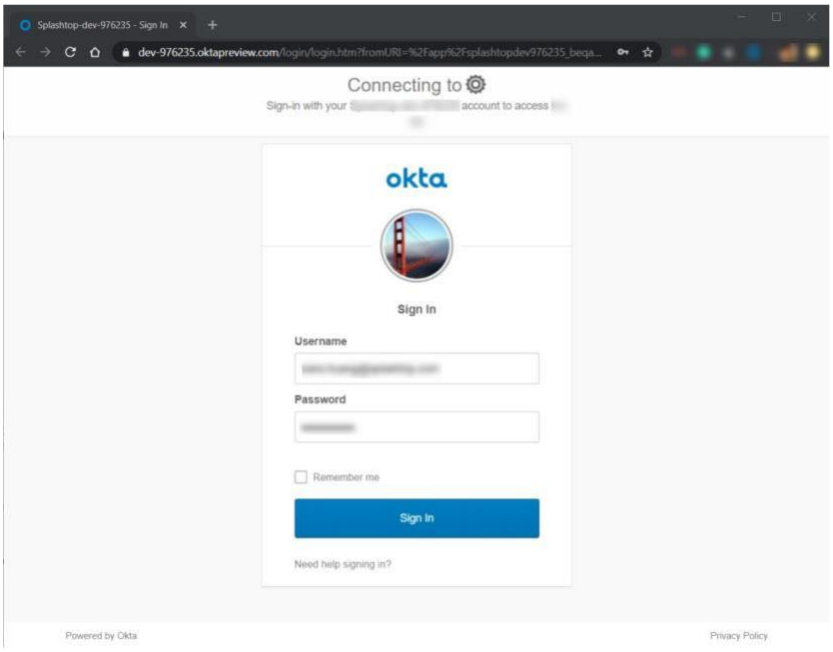
1. 在 Splashtop On-Prem 应用程序上，单击**单点登录**链接。



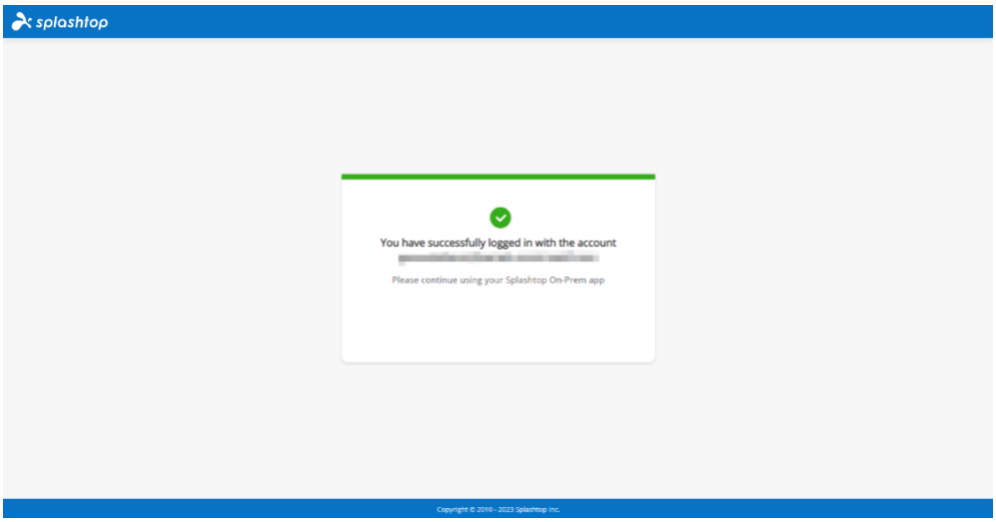
2. 在单点登录登录页面输入 Gateway 地址和 SSO 账户，然后单击登录。



3. 单击“登录”将打开 Web 浏览器并跳转到身份提供商门户网站。例如，Okta 门户网站。



4. 登录身份提供商门户网站后，即可登录应用程序。

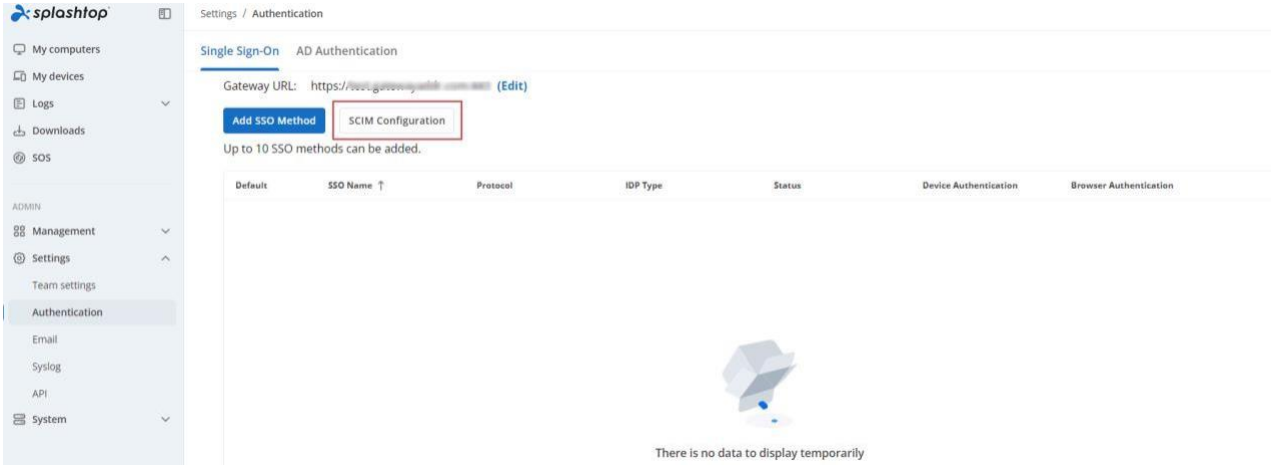


如何生成 SCIM 配置令牌?

需要在 IDP 门户网站配置密钥令牌，以确保 SCIM 配置可以正常运行。可以登录 Gateway 以生成用于 SCIM 配置的密钥令牌。

如何生成

1. 打开 Gateway，导航到*管理/团队设置/身份验证/单点登录*。添加 Gateway URL，然后单击 **SCIM 配置**。



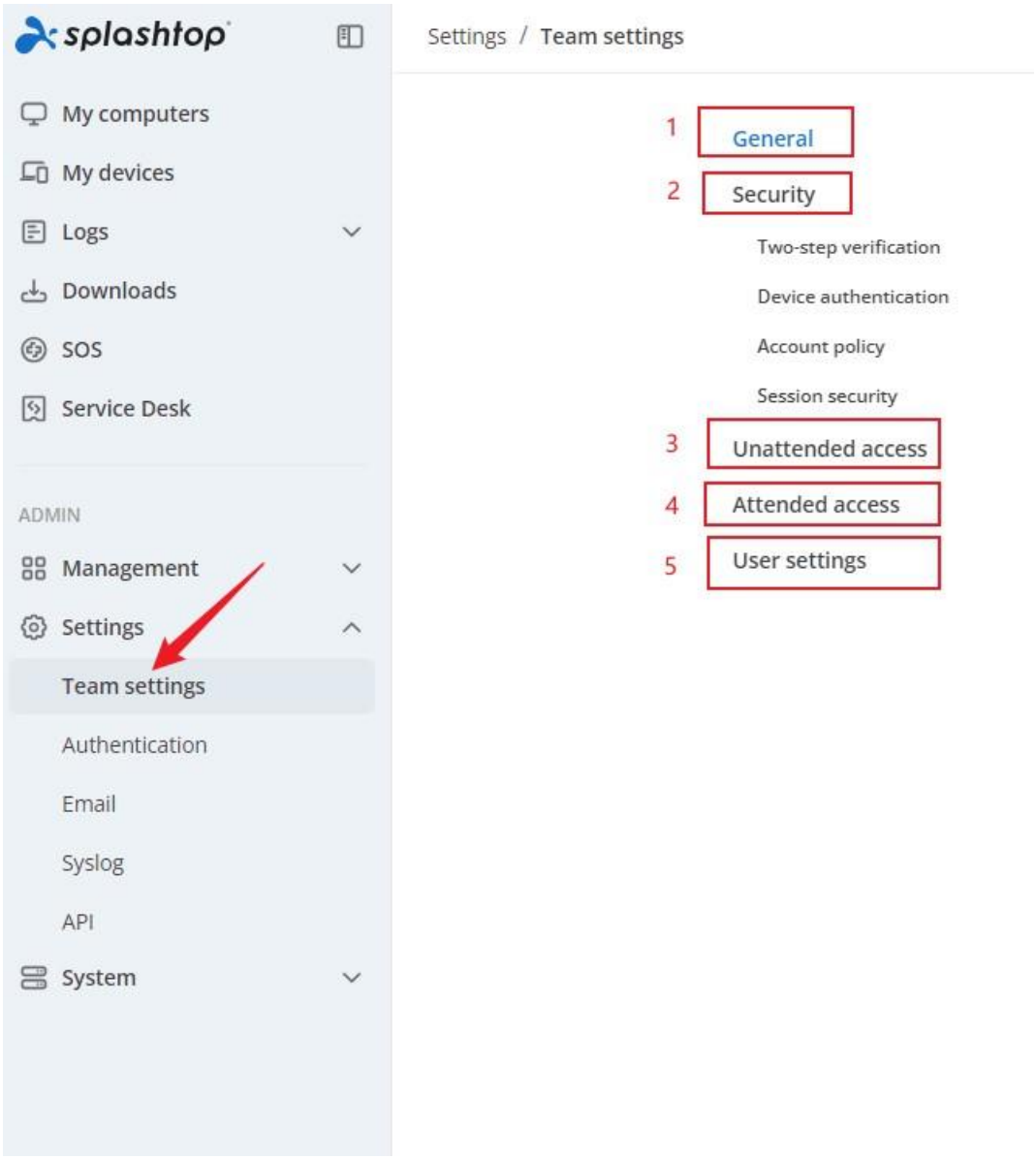
2. 单击复制图标以复制 Base URL 和 API 令牌。

3. 单击生成图标以生成新的 API 令牌。

设置

团队设置

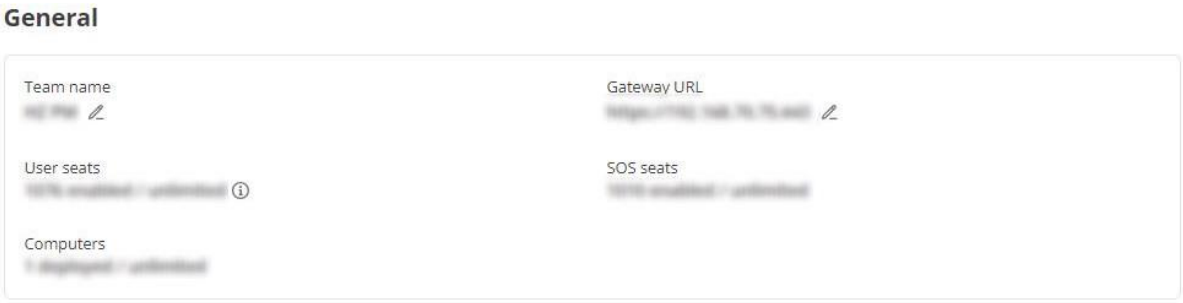
在 Splashtop On-Prem 的多租户系统中，每个租户即被视为一个团队。团队管理员可以从管理控制台访问和管理团队设置。



团队设置页面由以下5部分内容组成：

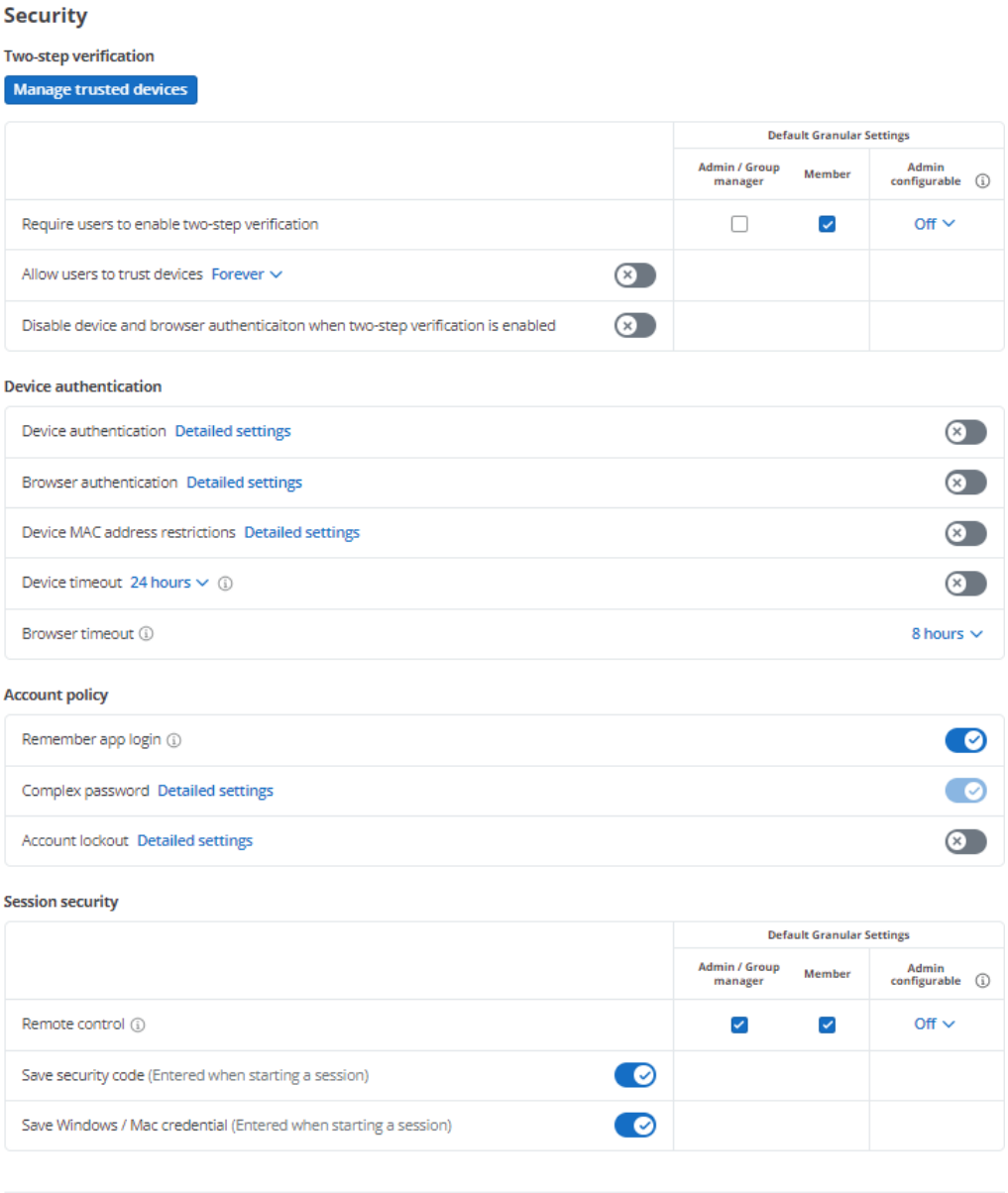
- **通用**
- **安全**
- 无人值守访问
- **有人值守访问**
- **用户设置**

通用

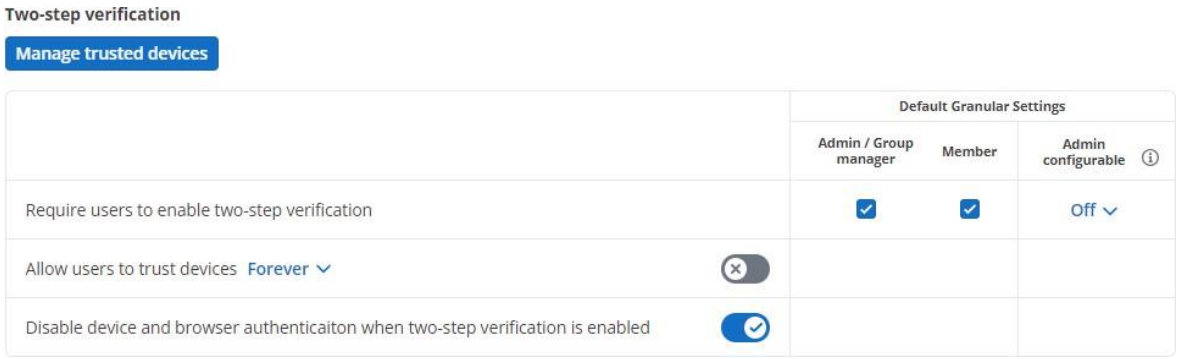


- 团队名称：可以自定义团队名称。团队名称会在所有 Streamer 和客户端设备的账户信息中显示。
- 用户席位：显示团队可用用户席位的最大数量以及已启用的用户席位数量。
- 电脑：显示团队可部署电脑的最大数量以及已部署电脑的数量。
- Gateway URL：此参数用作访问 Splashtop Gateway 服务的外部域名。
- SOS 席位：显示团队可用 SOS 席位的最大数量和已启用的 SOS 席位数量。

安全



两步验证：两步验证通过手机中主流的身份验证软件提供的基于时间的 OTP 验证提高安全性。On-Prem 客户端必须输入6位 TOTP 码才能登录设备。

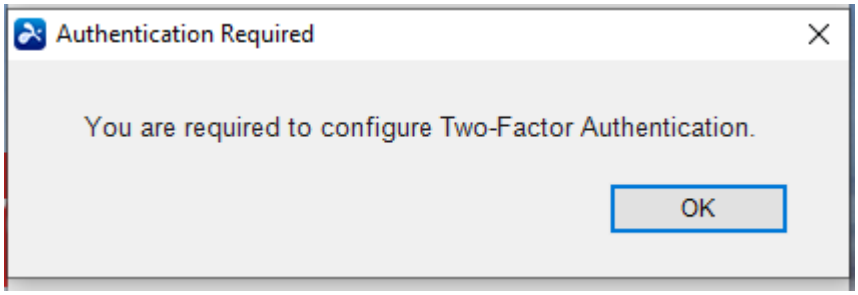


管理受信任设备：**团队管理员可以查看受信任的设备，并在必要时将其删除。**

要求用户启用两步验证： **默认精细设置列中有两个复选框，一个面向管理员/组管理员，另一个面向成员。**

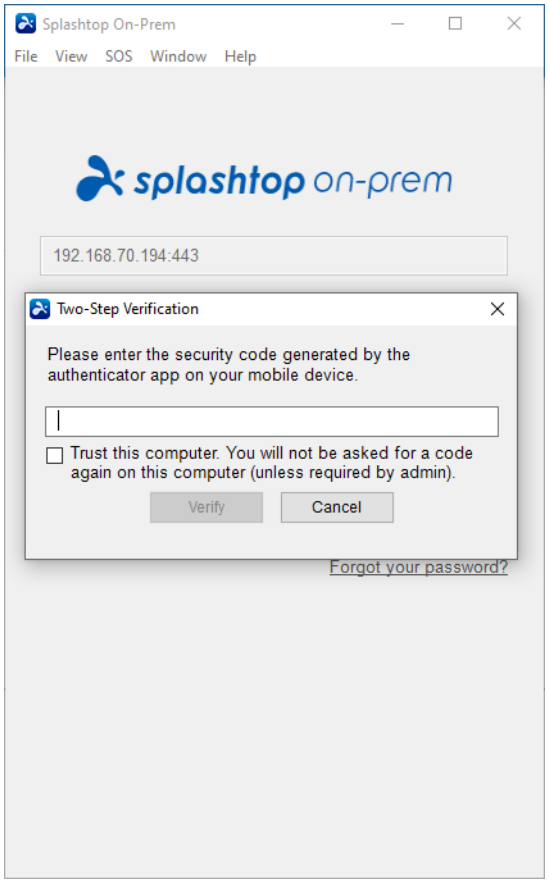
如果选中第一个复选框，则管理员用户/组管理员在首次尝试登录 On-Prem 客户端时需要设置两步验证设备。

如果选中第二个复选框，则成员用户在首次尝试登录 On-Prem 客户端时需要设置两步验证设备。



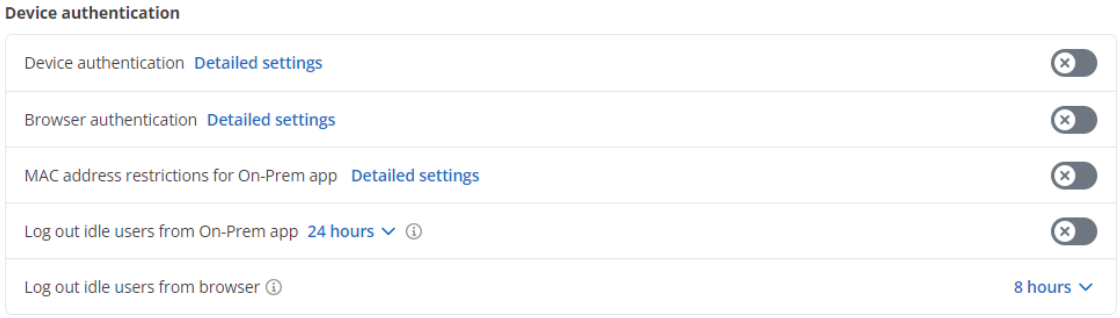
除了这两个复选框，还有一个名为管理员可配置的单独列，上面有个向下箭头。如果要允许管理员和组管理员为其他用户配置精细设置，则可单击向下箭头并选择开。

允许用户信任设备：如果选中此选项，则 Splashtop On-Prem 用户可以选择信任客户端设备，以在将来登录时无需输入 TOTP 码。可以单击向下箭头为受信任设备设置有效期（永久、1天、7天和 30天）。



启用两步验证时禁用设备和浏览器身份验证：启用此选项表明，如果已启用两步验证（可提高安全性），则将禁用设备和浏览器的身份验证。

设备身份验证：选中此选项则需先进行设备身份验证，然后才能启动远程会话。可以单击详细设置以进行精细设置。



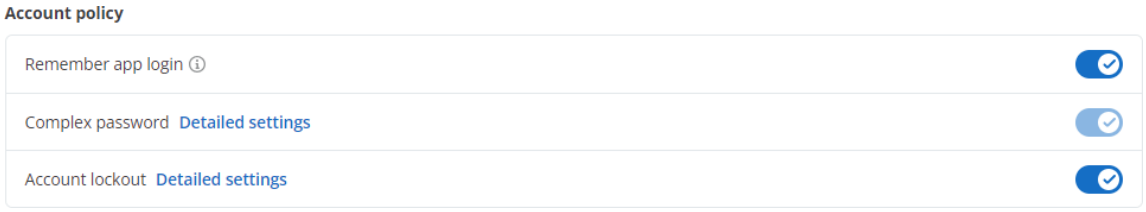
浏览器身份验证：选中此选项则需在启动远程会话前进行基于浏览器的身份验证。可以单击详细设置以进行精细设置。

On-Prem 应用程序的 MAC 地址限制：每个设备基于 MAC 的地址是唯一的，使用 MAC 地址进行身份验证更安全。如果选中此选项，则需要完成更详细的设置以忽略特定的 MAC 地址。可以逐个输入要忽略的 MAC 地址，也可以直接导入（或导出）现有的 .csv 格式文件。

从 On-Prem 应用程序注销空闲用户：选中此选项则当用户的空闲时间达到15分钟/1小时/8小时/24小时时，将其从 On-Prem 应用程序强制注销。

从浏览器注销空闲用户：通过此设置，可以在用户空闲达到一定时间（5分钟/15分钟/30分钟/1小时/4小时/8小时）时，将其从浏览器中注销

账户策略：

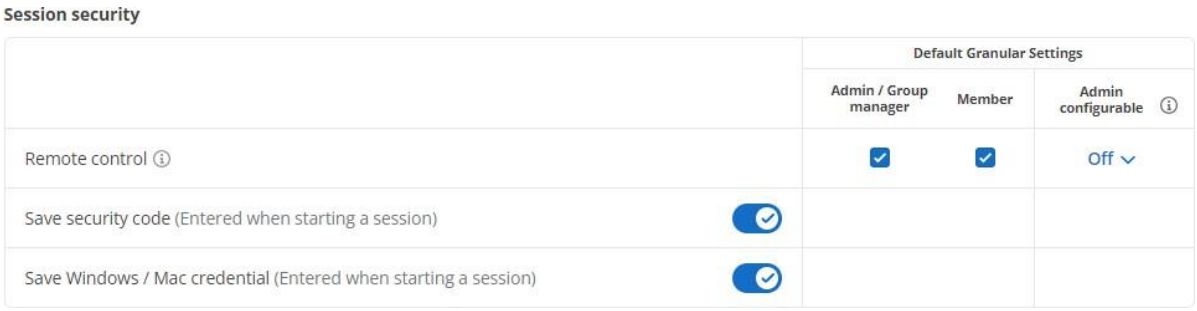


记住软件登录凭据：如果选中此选项，则用户无需在每次登录账户时重复输入凭据。

复杂密码：选中此选项则可微调复杂密码策略，包括密码最小长度、启用密码过期期限以及下次登录时强制执行密码策略。

账户锁定：选中此选项则可设置账户注销阈值并选择如何锁定账户。

会话安全：



远程控制：此选项用于限制远程会话中管理员/组管理员和/或成员的远程控制权限。如果要允许管理员和组

管理员为其他用户配置精细设置，可以单击管理员可配置 单独列中的向下箭头，然后选择开。

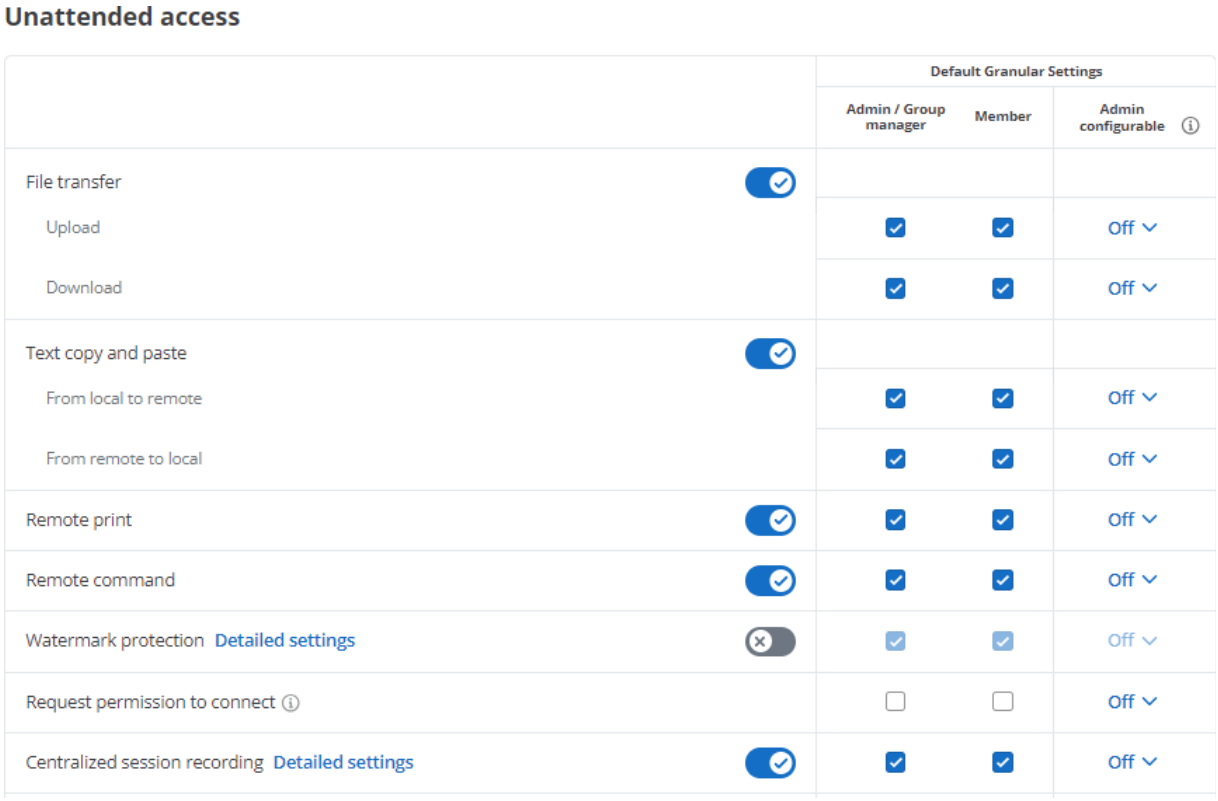
保存安全码：选中此选项则在建立远程会话时保存安全码。

保存 Windows / Mac 登录凭据：选中此选项则在建立远程会话时保存 Windows / Mac 凭据。

无人值守访问

Splashtop Remote Support 或 Splashtop Remote Access 可以通过安装相应软件端点来启用远程支持和远程控制。启动远程会话无需用户在场。

此区域支持从默认精细设置列对某些功能进行微调。



文件传输：在本地和远程电脑（仅限 Windows 和 Mac）之间启用文件传输（上传和/或下载）。

文本复制和粘贴：本地电脑和远程电脑之间的双向文本复制粘贴功能。

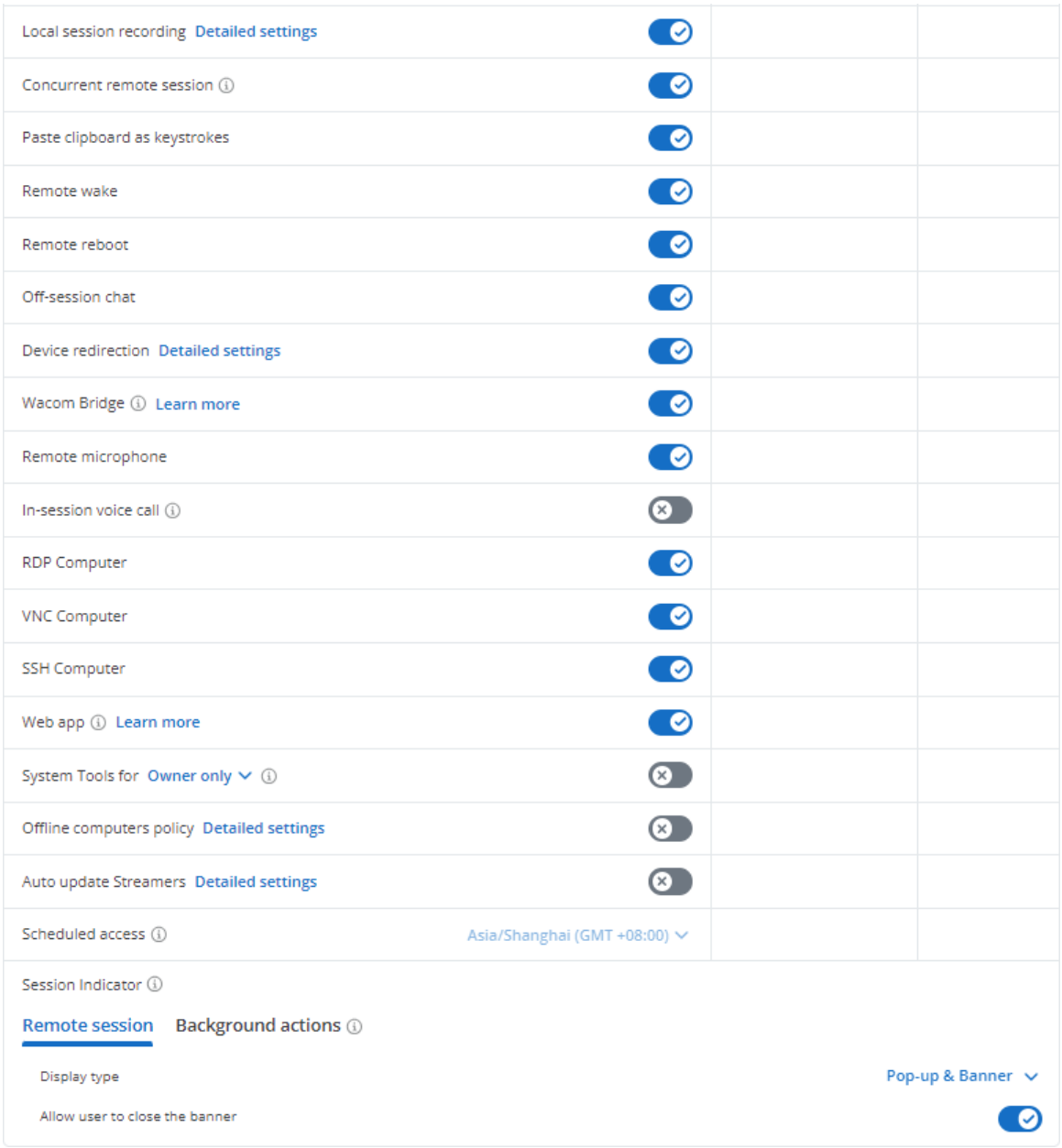
远程打印：从已安装 Streamer 的电脑（被控端）在已连接客户端电脑（主控端）的打印机上打印文档。

远程命令：从客户端电脑（主控端）向 Streamer 电脑（被控端）发送命令。

水印保护：通过勾选此选项，用户可以自定义远程会话期间显示的水印文本和布局，包括字体大小、字体颜色、字体不透明度、轮廓颜色、轮廓不透明度等。

请求连接权限：为用户提供了3个接受远程连接提示的方法选项，即请求到期后拒绝连接（在登录界面自动拒绝连接）、请求到期后允许连接（在登录界面自动允许连接）和请求到期后允许连接。

集中会话录制：通过选中此选项，录制的远程会话将自动保存到集中式云存储空间。用户可以在详细设置中指定允许播放/下载/删除录制文件的人员。



本地会话录制：启用本地会话录制，则可以根据 Windows 或操作系统平台为 SOS 应用程序的存储文件夹分配自动录制、路径和大小限制。

并发远程会话：从多个客户端设备（主控端）启动到 Streamer 电脑（被控端）的并发远程会话。

远程复制粘贴：一种特殊的粘贴方式，启用此功能可将本地剪贴板的内容以快捷键的方式粘贴到远程电脑。

远程唤醒：从客户端设备（主控端）唤醒 Streamer 电脑（被控端）。

远程重启：从客户端设备（主控端）重启 Streamer 电脑（被控端）。

会话外聊天：开启会话外聊天功能。

设备重定向：启用此功能用户可以远程重定向 USB 设备。

Wacom Bridge：启用此功能可在本地无缝使用 Wacom 压感笔技术。

远程麦克风：启用此功能可将本地麦克风的输入传输到远程电脑。

会话中语音呼叫：启用此功能可在远程访问会话期间向最终用户发起语音呼叫。

RDP 电脑：从客户端设备（主控端）远程连接 RDP 电脑（被控端）。

VNC 电脑：从客户端设备（主控端）远程连接 VNC 电脑（被控端）。

SSH 电脑：从客户端设备（主控端）远程连接 SSH 电脑（被控端）。

Web 应用：启用此功能以允许用户使用浏览器连接到远程电脑。

系统工具：输入电脑的管理员用户名和密码，可以指定允许访问系统工具的人员。

脱机电脑策略：启用此选项可设置自动删除脱机电脑的天数。

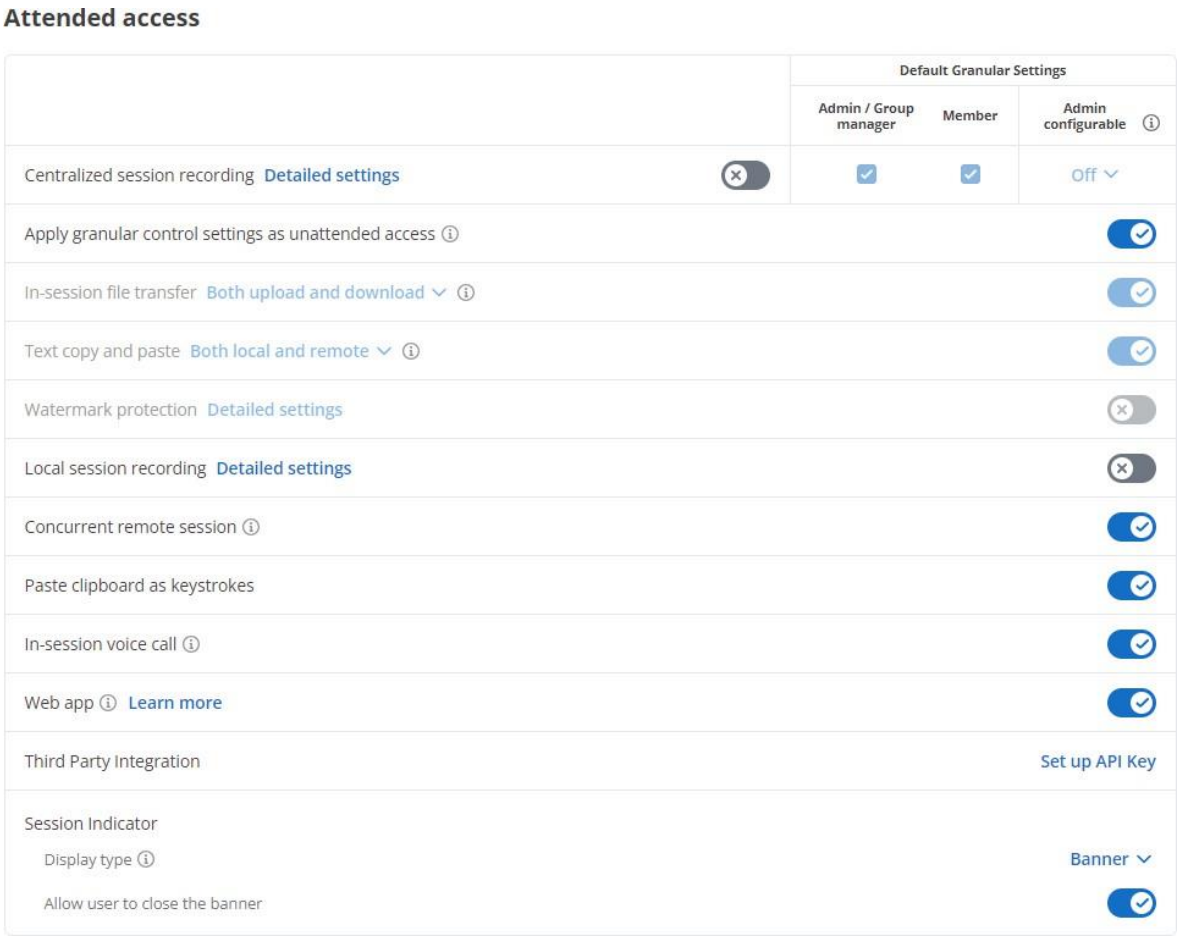
自动更新 Streamer：启用此选项可将 Streamer 更新应用于所有电脑或仅应用于特定电脑和电脑组。

计划访问：启用此选项可设置用户的远程访问时间。

会话指示器：可以在此处选择显示类型，以及是否允许用户关闭远程会话和后台操作的横幅。

有人值守访问

Splashtop 按需支持（又名 SOS）是一种远程支持方式，无需端点安装任何软件。端点需要下载并启动一个便携式 SOS 应用程序，技术员可以使用 Splashtop On-Prem 客户端连接 SOS 应用程序。



集中会话录制：启用此选项，则录制的远程会话将自动保存到集中式云存储空间。用户可以在详细设置中指定允许播放/下载/删除录制文件的人员。

将精细控制设置应用到无人值守访问：如果未勾选此选项，则两步验证和远程控制将始终遵循用户级别的精细控制设置。

会话中文件传输：在远程会话期间，在本地和远程电脑之间启用文件传输（上传和/或下载）。

文本复制和粘贴：本地电脑和远程电脑之间的双向文本复制粘贴功能。

水印保护：启用此选项，用户可以自定义远程会话期间显示的水印文本和布局，包括字体大小、字体颜色、字体不透明度、轮廓颜色、轮廓不透明度等。

本地会话录制：为 SOS 远程支持会话启用会话录制。

并发远程会话：为多个 Splashtop 客户端启用并发远程会话以连接到同一个 SOS 应用程序。

远程复制粘贴：一种特殊的粘贴方式，启用此功能可将本地剪贴板的内容以快捷键的方式粘贴到远程电脑。

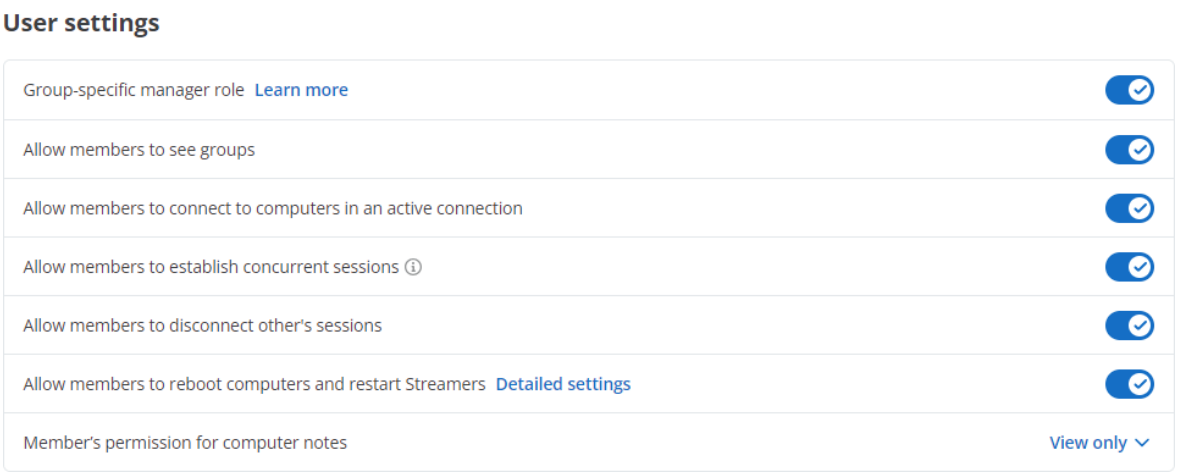
会话中语音呼叫：启用此功能可在远程访问会话期间向最终用户发起语音呼叫。

Web 应用：启用此功能以允许用户使用浏览器连接到远程电脑。

第三方集成：用户可以单击设置 API 密钥与第三方集成。

会话指示器：用户可以在此处选择显示类型，以及是否允许用户关闭横幅。

用户设置



特定组管理员角色：启用允许管理组的组管理员角色。

允许成员查看组：允许成员用户查看组中的电脑。

允许成员连接会话连接中的电脑：允许成员用户与已连接的电脑建立远程会话。

允许成员建立并发会话：允许成员用户同时远程访问多台电脑。

允许成员断开其他成员的会话连接：允许成员用户结束其他用户的远程连接。

允许成员重启电脑和 Streamer：选择成员用户可以在电脑上执行的操作，包括重启 Streamer、常规重启和安全模式重启。

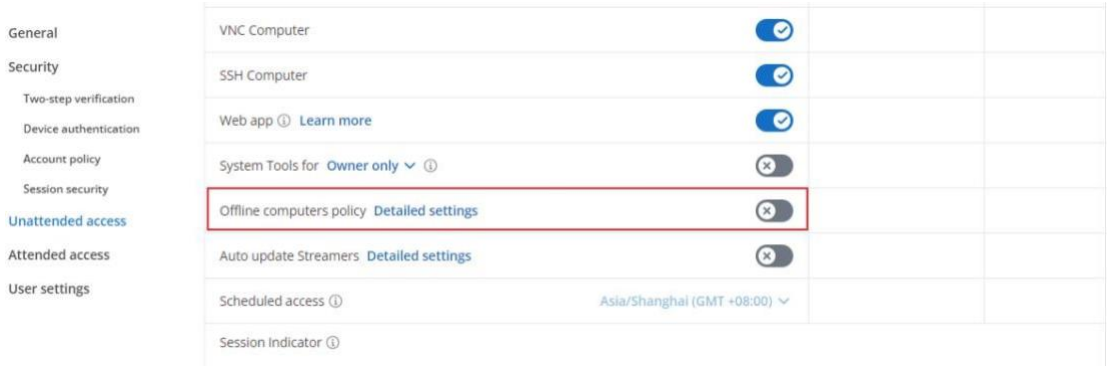
成员电脑备注权限：管理成员用户的电脑备注权限，包括不允许查看和编辑、仅查看、查看和编辑。

删除离线电脑策略

删除离线电脑策略规定了离线电脑被自动删除的天数。此功能允许团队所有者设置策略参数以自动清理过时电脑。

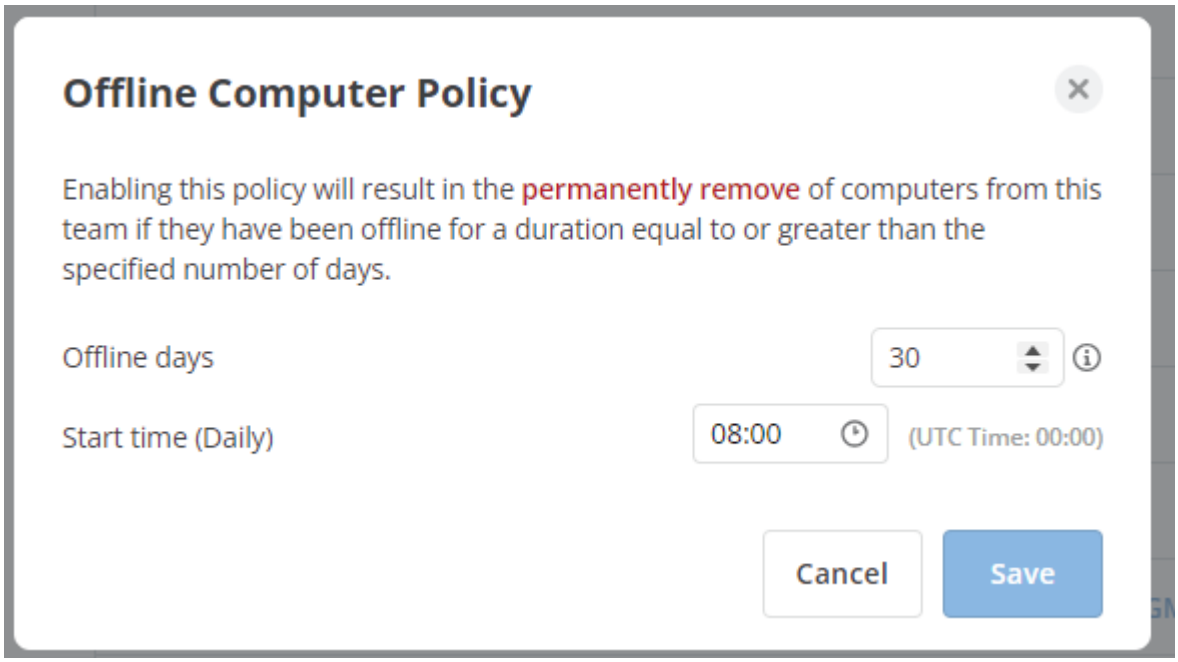
如何设置删除离线电脑策略？

1. 以所有者身份登录 Gateway 管理控制台，打开 *设置* > *团队设置* > *无人值守访问页面*，开启**离线电脑策略**。



2. 在详细设置中配置**离线天数**和**开始时间**。然后点击**保存**按钮保存设置并打开该功能。

- **离线天数**：设置离线天数，达到离线天数的电脑将被移除。
- **开始时间**：设置此策略的开始时间，每天重复一次。



3. 点击保存按钮以保存设置。

4. 此策略默认处于禁用状态。自动删除电脑时启用此选项将有助于问题解决。

如何设置 Web 访问

什么是 Web 访问

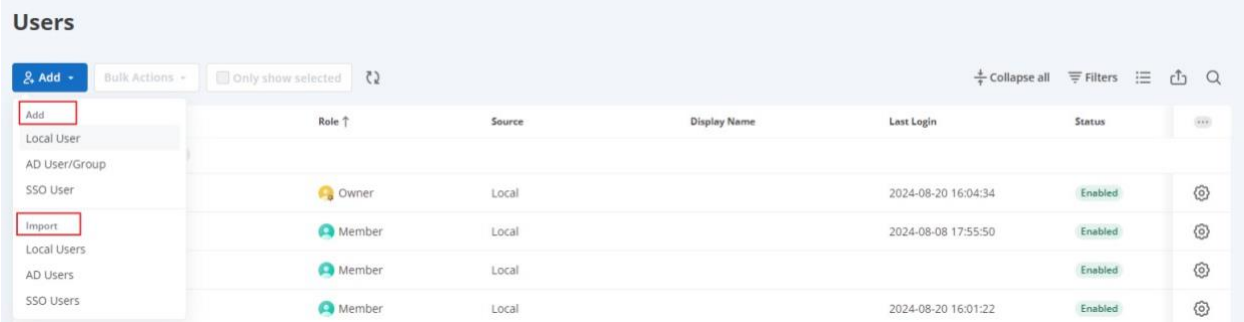
Web 访问规定了用户是否可以访问 Splashtop Gateway Web 门户网站。禁用 Web 访问后，浏览器将阻止登录尝试，但此选项不影响用户从本地客户端应用程序的远程访问功能。

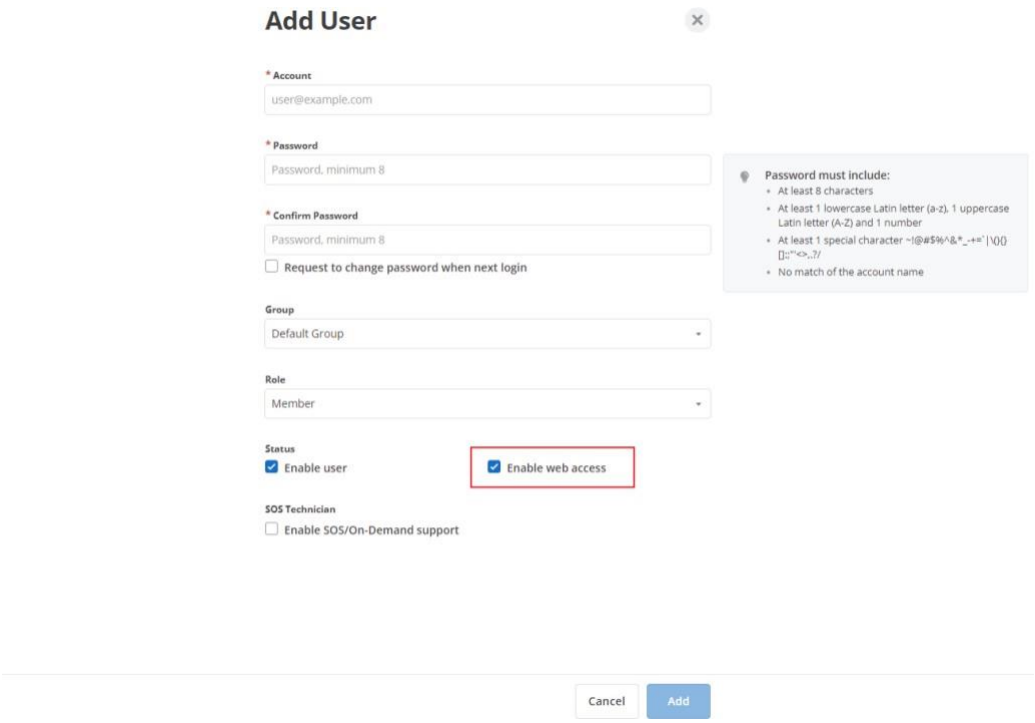
如何配置 Web 访问

使用所有者或管理员账户登录 Gateway 网络控制台。

创建用户

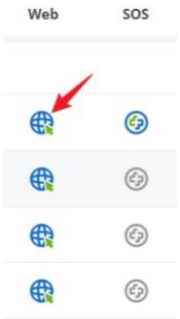
可以在创建新用户时设置 Web 访问权限。导航到 *web/管理/用户*页面，单击**添加**或**导入**。



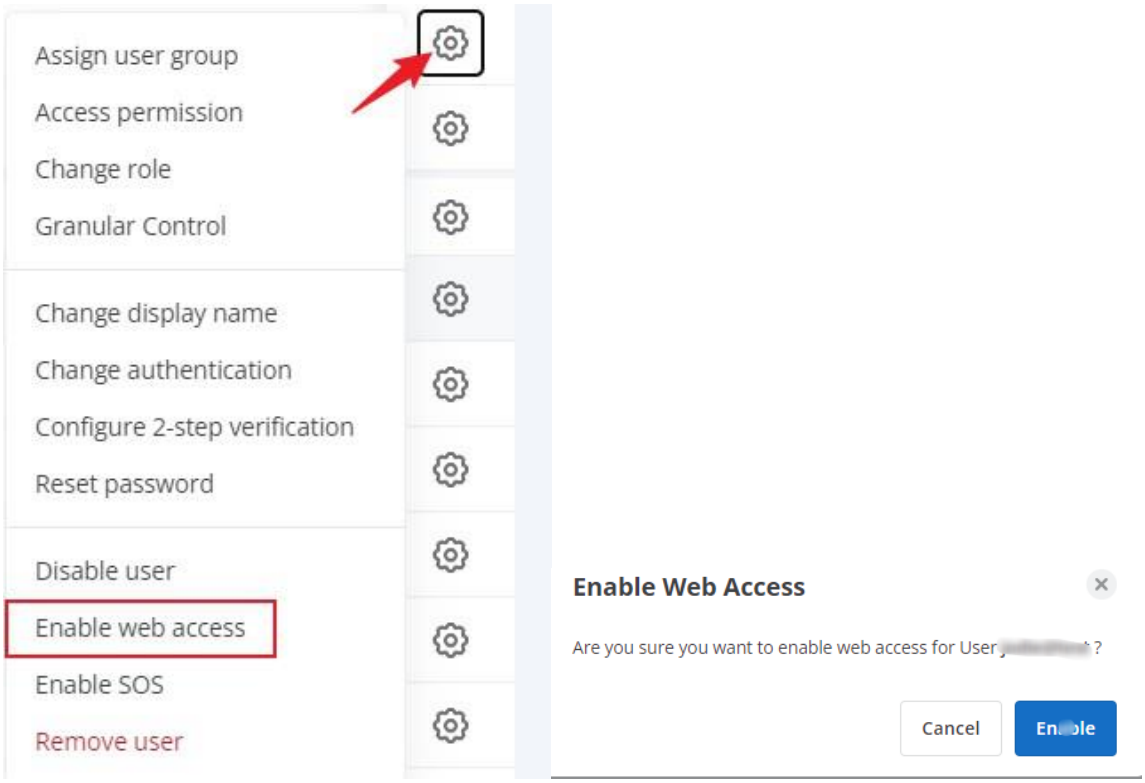


编辑用户

从管理/用户表中启用/禁用 Web 访问。

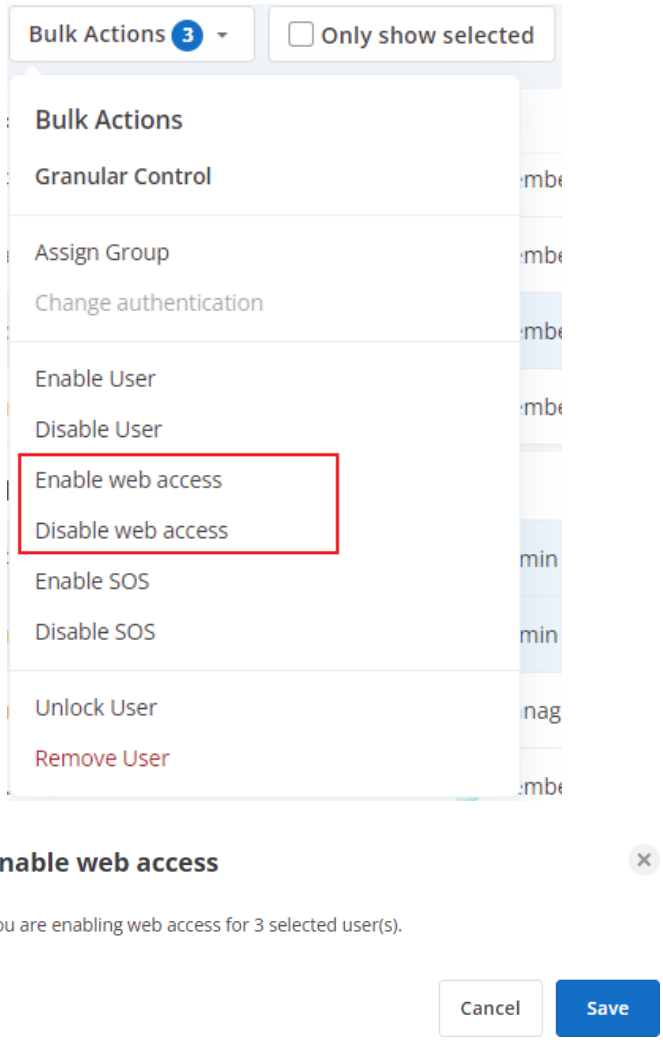


可以指定用户账户，并为其设置 Web 访问权限。导航到 *web/管理/用户*页面，在用户列表中的每个用户旁，单击齿轮图标并选择 **Web 访问**。



批量操作

还可以通过批量操作为多个账户设置 Web 访问权限。导航到 *web//管理/用户*页面，单击齿轮图标，然后选择 **Web 访问**。



设置两步验证

两步验证，也称为双因素身份验证或 2FA 或多因素身份验证 （mfa），是一个非必选但强烈推荐的安全功能。

启用后，在登录 Splashtop 时，除了账户密码外， 还需要额外输入六位安全码。安全码由移动设备的身份验证软件生成。（暂不支持短信发送安全码）

也就是说，即使 Splashtop On-Prem 账户 ID 和密码被破解或窃取，电脑也无法被登录和访问。

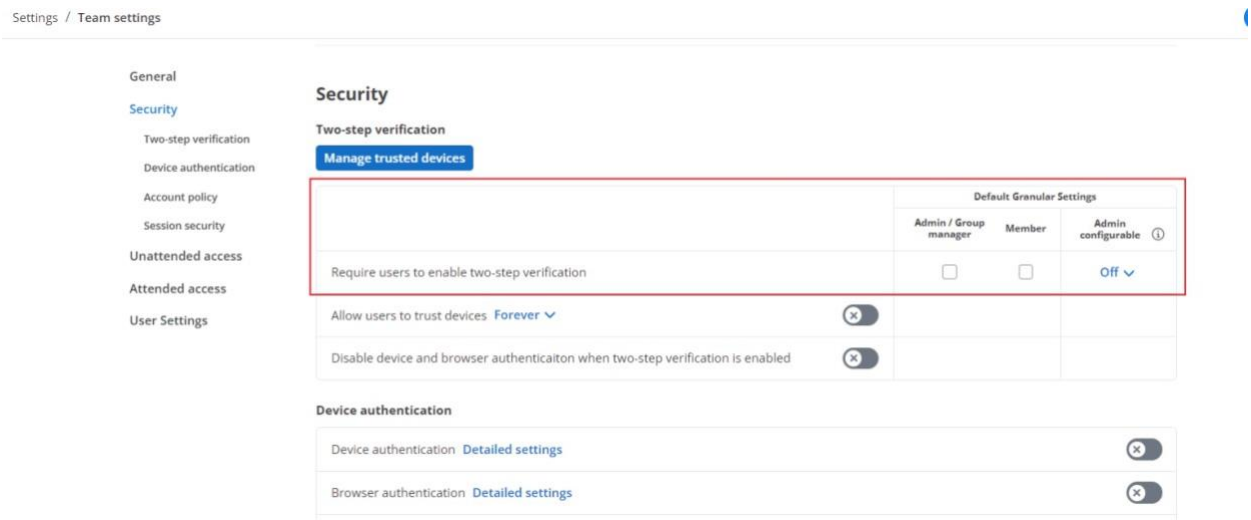
Splashtop On-Prem 支持基于 TOTP（基于时间的一次性密码性密码算法）的两步验证，并支持使用以下身份验证软件进行验证：

- Google Authenticator （安卓/iPhone/黑莓）
- Duo Mobile （安卓/iPhone）
- Microsoft Authenticator （安卓/iPhone/Windows Phone 7）
- Okta Verify （安卓/iPhone）
- 其他主流 OTP 应用程序

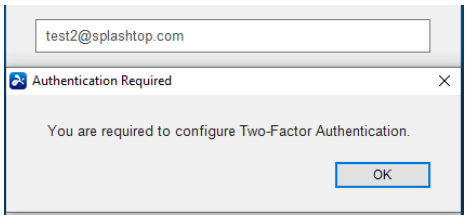
设置指南

步骤 1

以团队所有者身份登录管理控制台，导航到**设置** > **团队设置**页面，即可设置强制执行两步验证的方法和对象。

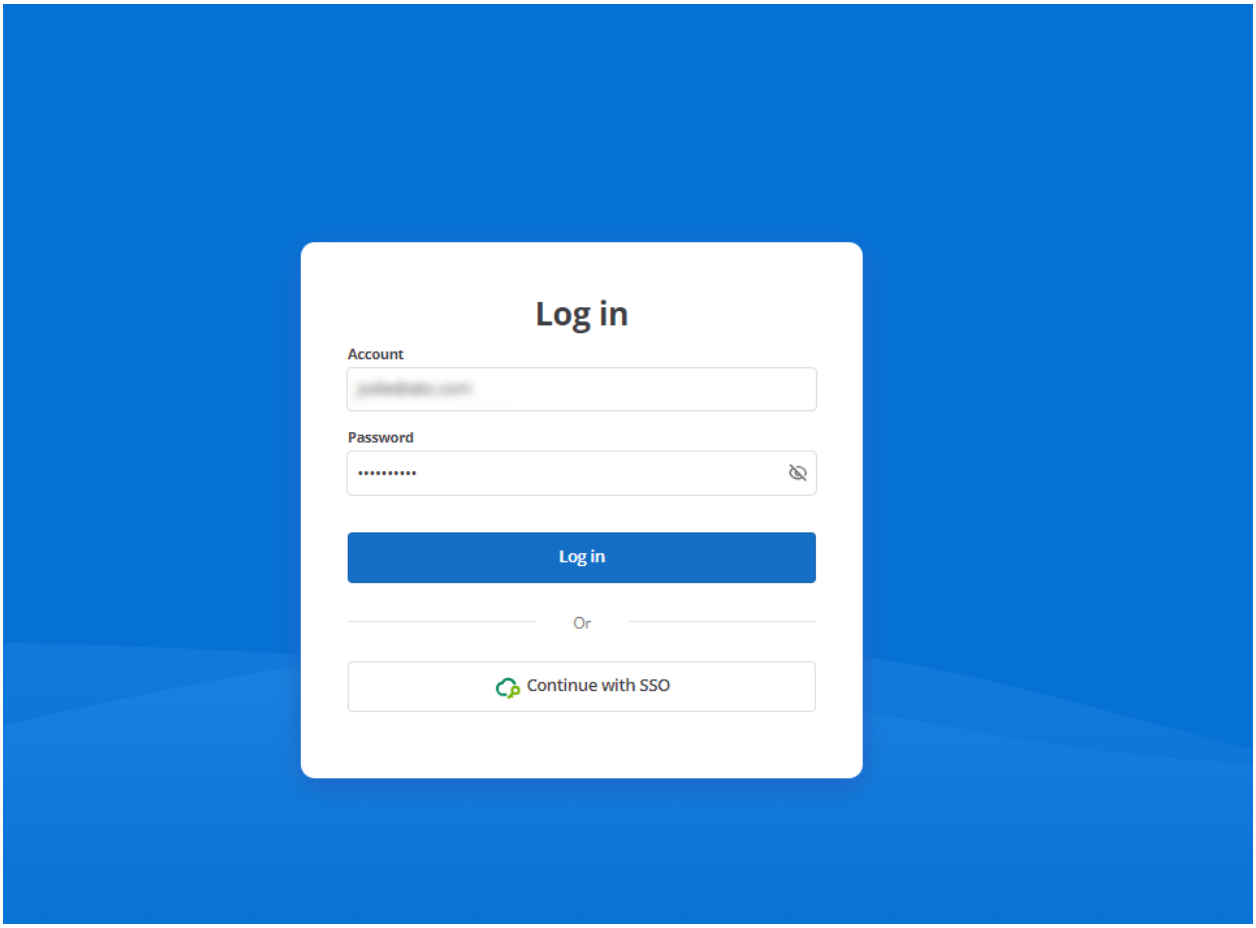


如果账户被强制启用两步验证，则用户将需要通过两步验证设置指南才能继续使用该服务，或者在用户尝试登录客户端应用程序时，将弹出下图所示的窗口。

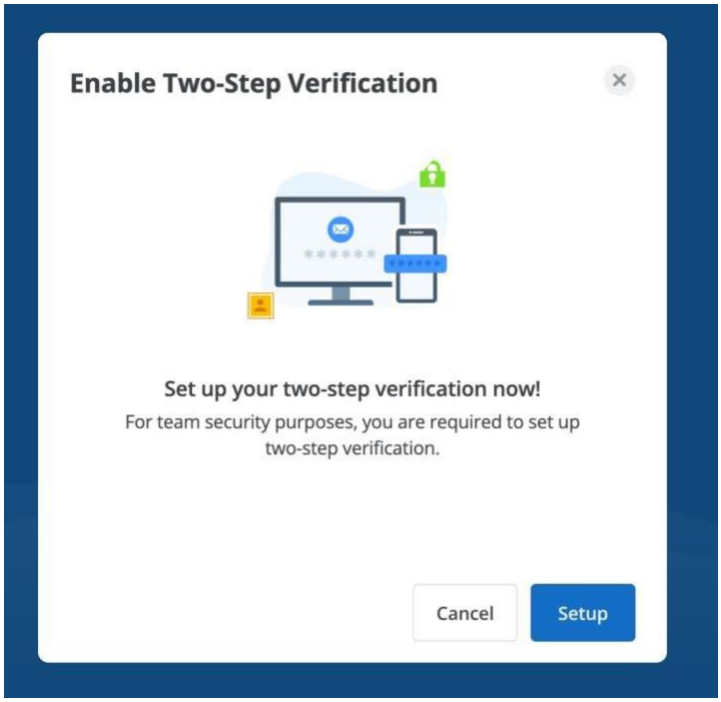


步骤 2

首次设置两步验证账户，用户需要使用个人账户登录 **Gateway**。



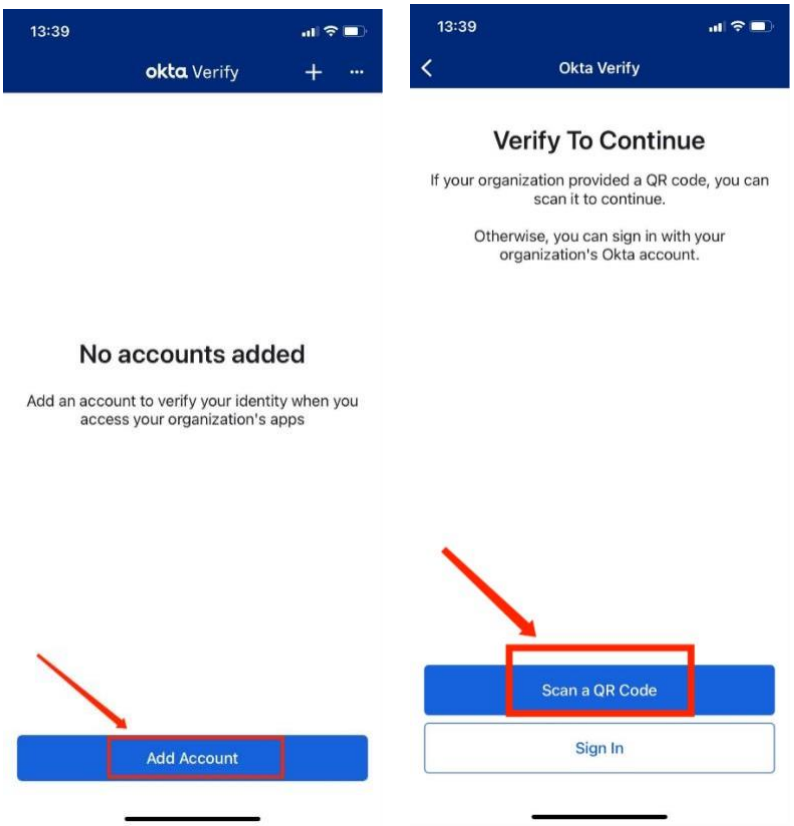
按照说明完成设置。

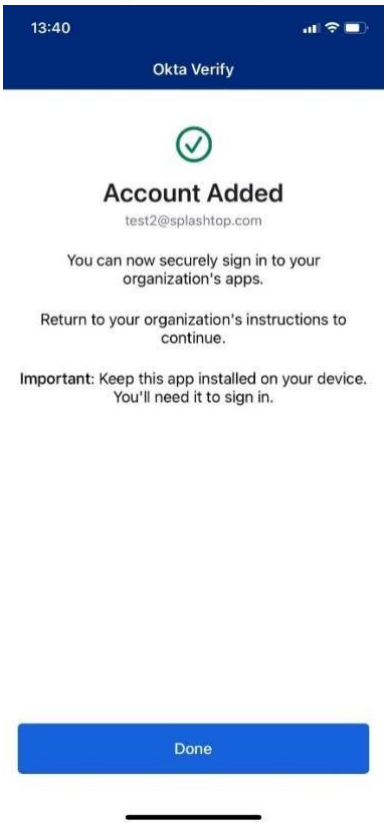


点击设置生成一个二维码，打开身份验证软件扫描该二维码。

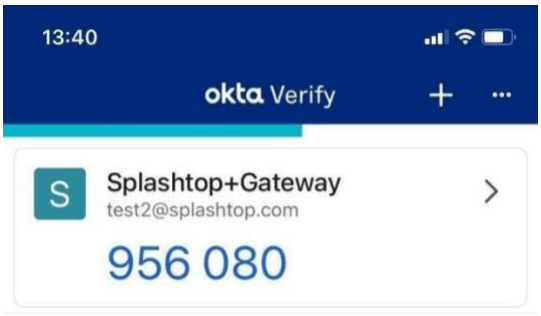
打开身份验证软件（以 okta Verify 为例）完成以下步骤。

添加账户 -> 组织 -> 扫描二维码 -> 完成。



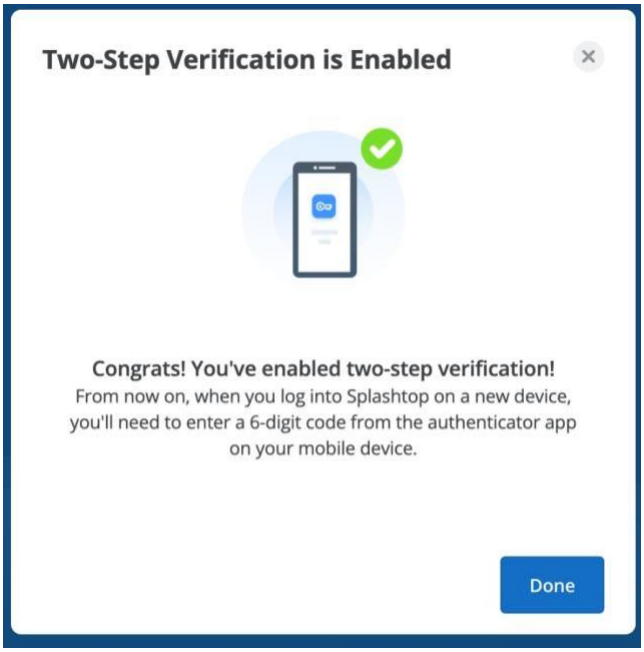


身份验证软件上会生成安全码。输入身份验证软件生成的安全码以完成配对。



单击复制或保存代码以继续下一步。

两步验证启用成功，即可在新设备上登录 Splashtop！



步骤 3 使用两步验证登录 On-Prem 应用程序和控制台

启用和设置两步验证后，用户将需要输入一次性安全码。如果团队所有者**已允许受信任设备**，则用户可以勾选信任此设备以提高便利性。

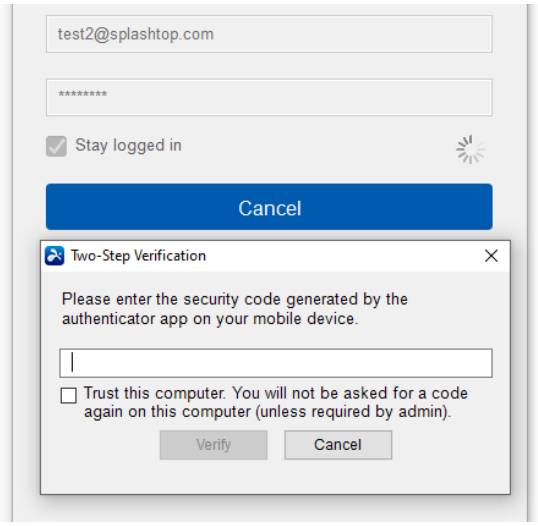


图.2-On-Prem 应用程序上的两步验证安全码输入对话框

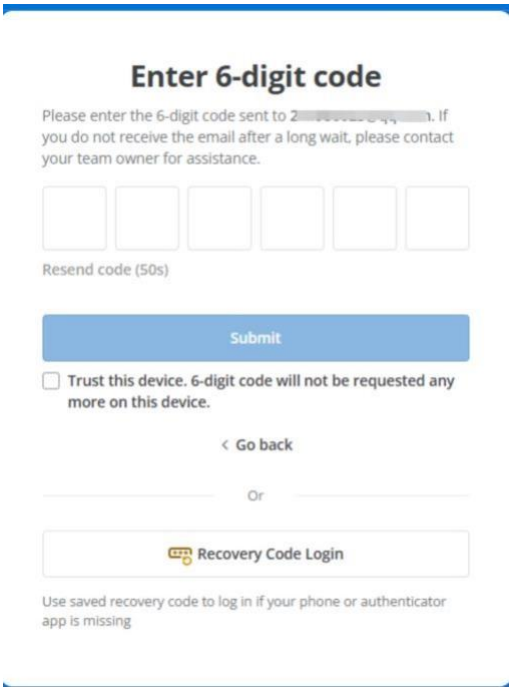


图.2-网络控制台上的两步验证安全码输入对话框

Q&A

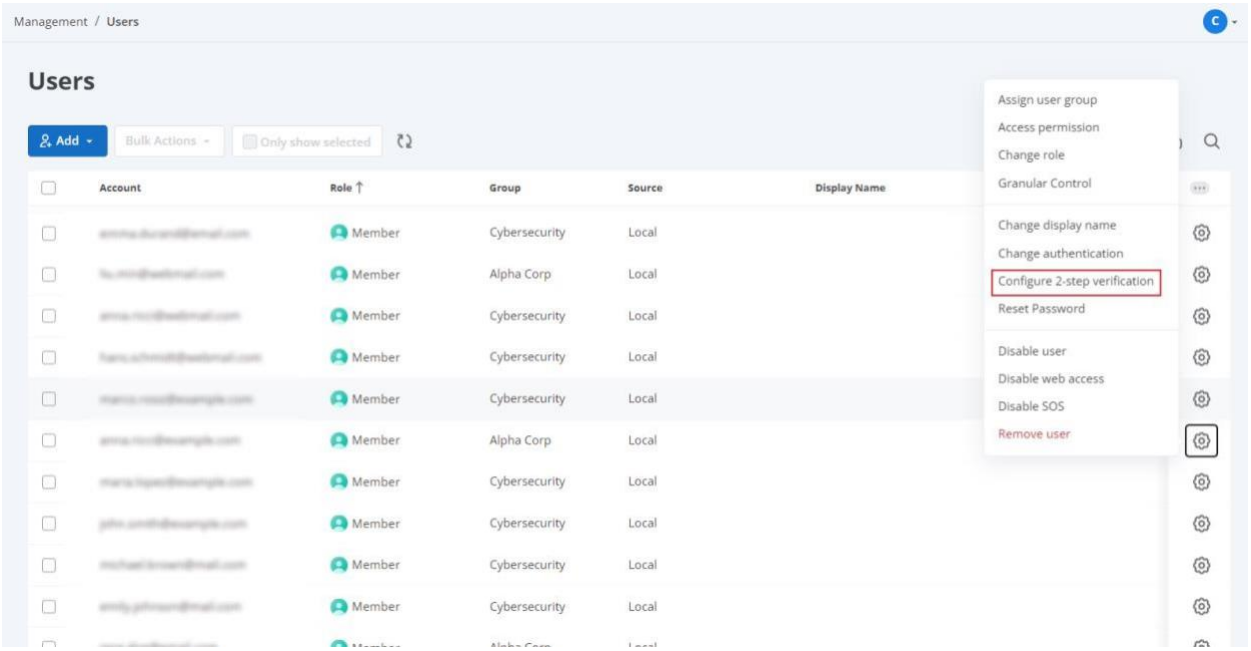
1. 为什么总是收到两步验证安全码错误？

TOTP 是一种基于时间和时钟的身份验证方式，当存在明显的系统时钟差异时（例如超过30秒），则可能会导致无法接收两步验证安全码。请确保 Gateway 服务器的系统时间和您的身份验证软件时间保持同步。

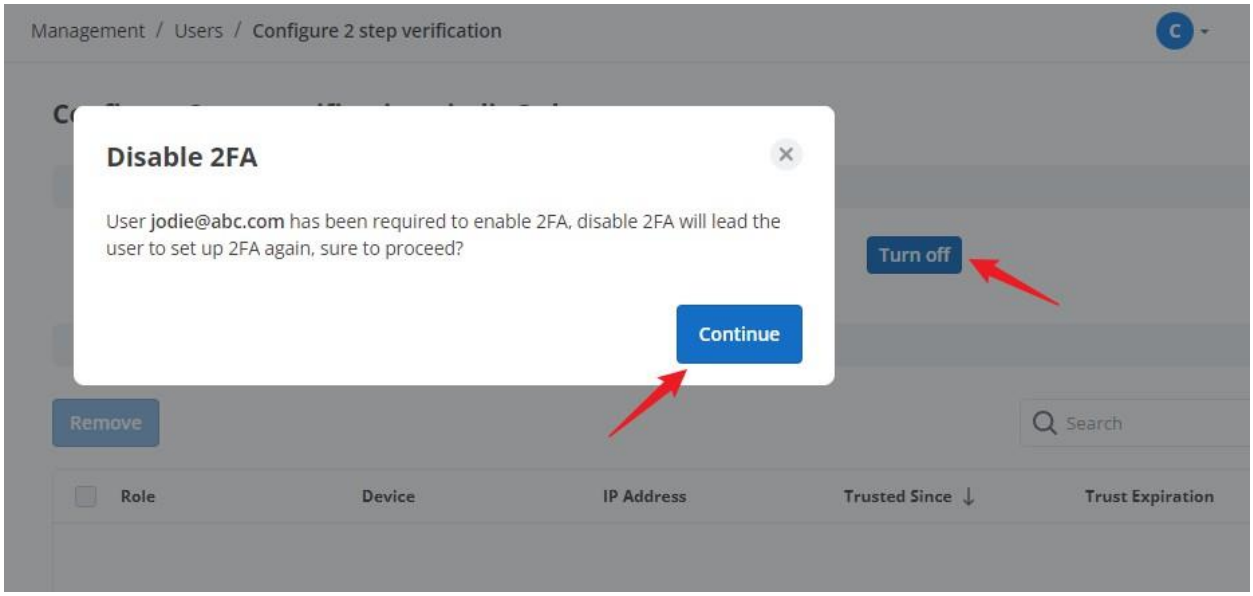
2. 如果手机丢失或忘记恢复码怎么办？

如果恢复码丢失，请联系团队管理员重置2FA 设置。
管理员重置2FA 步骤如下：
1）以管理员身份登录 Gateway

2）导航到管理 -> 用户 -> 齿轮按钮 -> 配置两步验证



3）禁用 2FA



4）用户可以再次设置2FA。

> **注意**：TOTP 是一种基于时间和时钟的身份验证方式，当存在明显的系统时钟差异时（例如超过30秒），则可能会导致无法接收两步验证安全码。请确保 Gateway 服务器的系统时间和您的身份验证软件时间保持同步。

通过电子邮件设置两步验证

两步验证，也称为双因素身份验证或 2FA 或多因素身份验证 （mfa），是一个非必选但强烈推荐的安全功能。

启用后，在登录 Splashtop 时，除了账户密码外， 还需要额外输入六位安全码。安全码将以电子邮件的形式发送到您的邮箱。

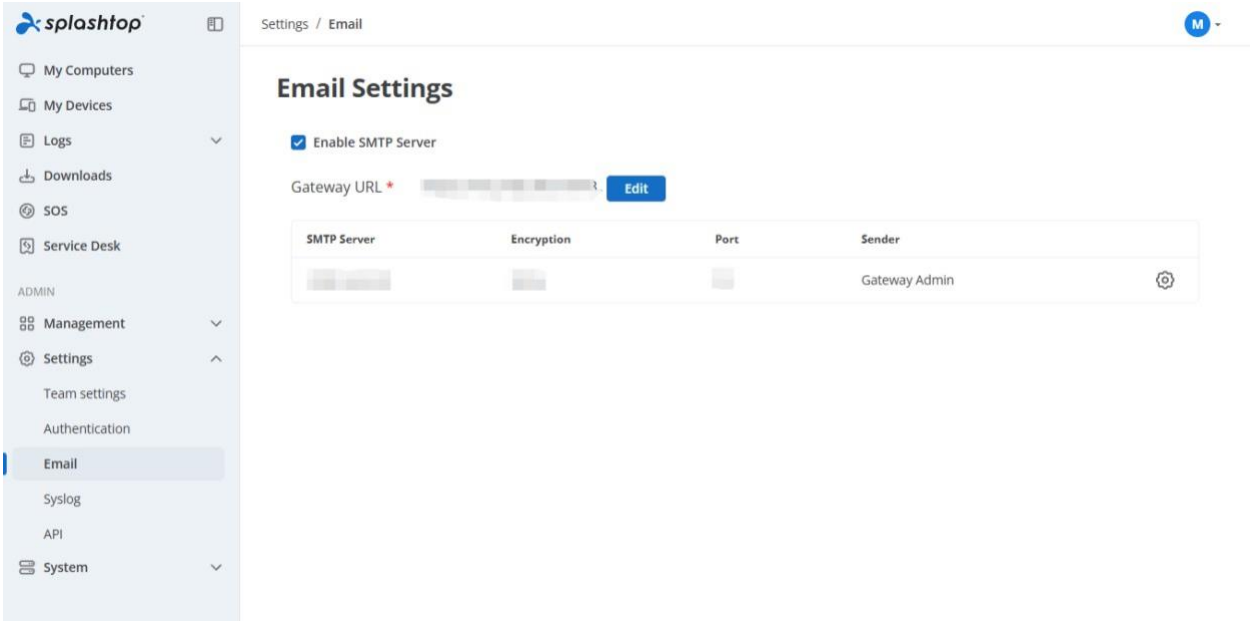
也就是说，即使 On-Prem 账户 ID 和密码被破解或窃取，电脑也无法被登录和访问。

从 Gateway v3.36.0开始，Splashtop On-Prem 支持基于电子邮件 OTP（一次性密码）的两步验证。

在 Gateway 中启用 SMTP 服务器

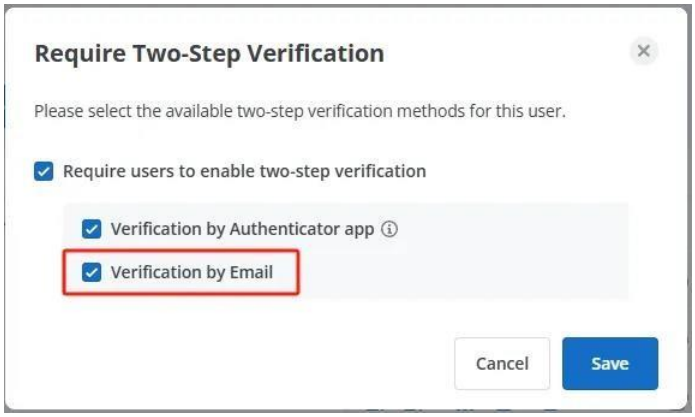
由于两步验证依赖于电子邮件，请确保 SMTP 服务器已正确配置和启用。此外，需要验证用户的电子邮件地址是否准确。否则，用户将无法收到一次性密码以完成两步验证。

以团队所有者的身份登录网络控制台，导航到**设置 > 电子邮件**，然后需要配置并启用 SMTP 服务器。



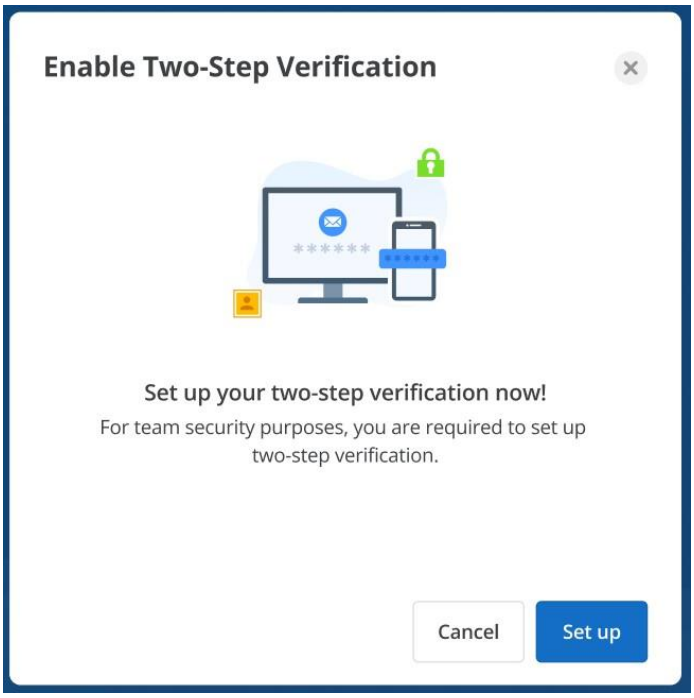
启用并选择两步验证方法

以**团队管理员**身份登录网络控制台。导航到**管理>用户**，为用户启用两步验证，并选择**通过电子邮件验证**作为两步验证方法。



设置两步验证

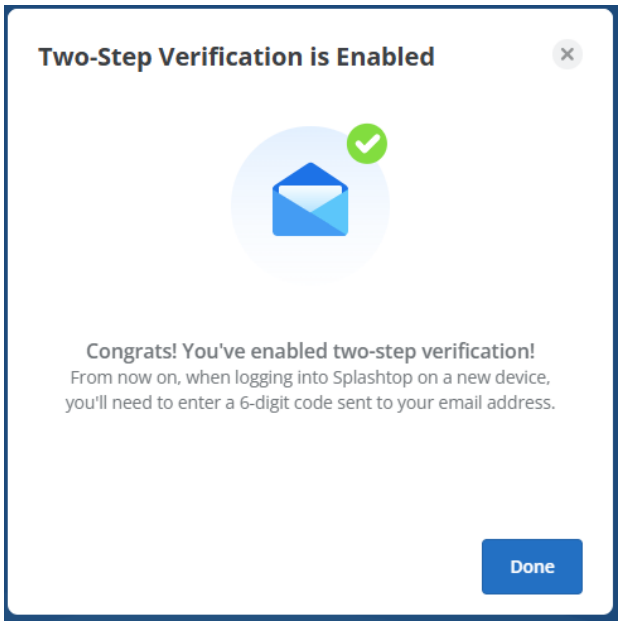
请按照说明完成两步设置流程。首先，单击**设置**进入下一步。



然后，将发送6位验证码到电子邮箱。输入6位验证码，单击**下一步**完成配对。

单击**复制恢复码**或**保存恢复码**以保存恢复码。请注意，恢复仅显示一次，请将其妥善保存。然后，单击**继续**进入下一步。

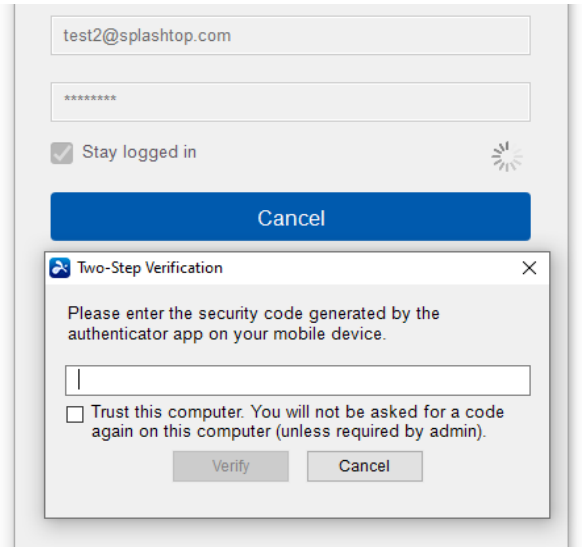
成功启用两步验证！

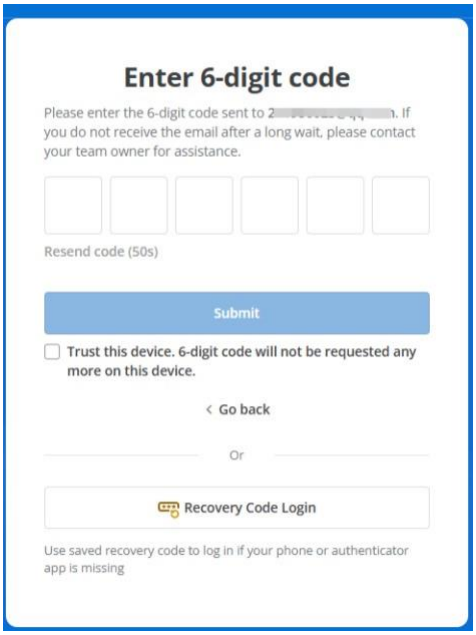


使用电子邮件登录网络控制台或 Splashtop On-Prem 应用程序

如果某个账户被强制启用两步验证，用户输入账户和密码后，需要填写邮箱中收到的6位一次性验证码，以完成登录过程。

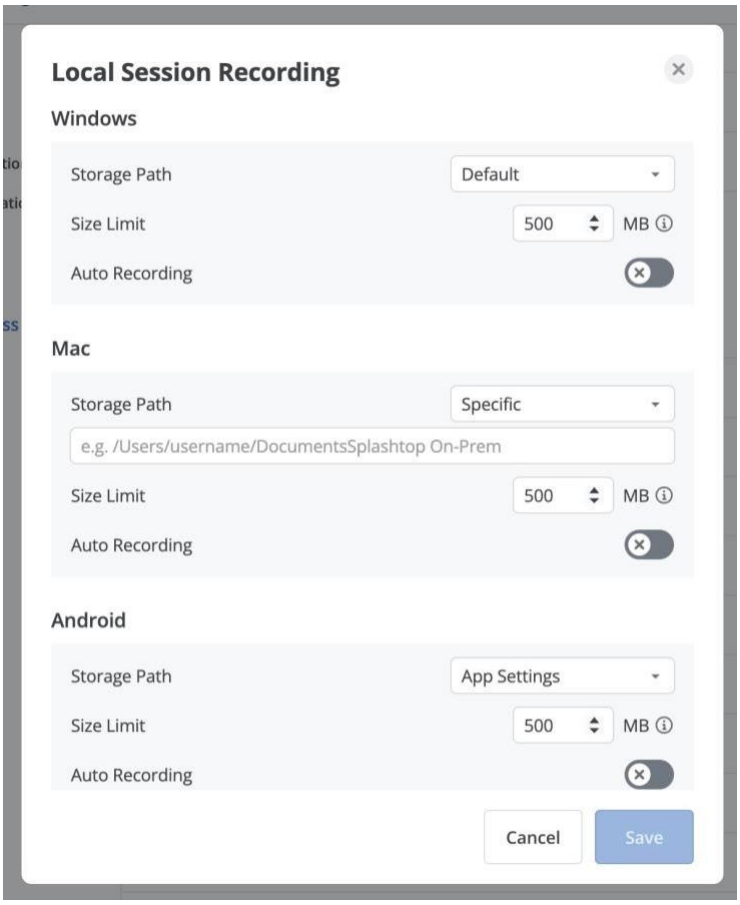
如果团队所有者**已允许受信任设备**，则用户可以勾选信任此设备以提高便利性。





Gateway 网络控制台的本地会话录制

本地会话录制详细设置



自动录制

- 保持选中自动录制选项将强制 Splashtop On-Prem 应用程序在会话开始时自动录制每个远程会话。
- 如果“选项 > 高级 > 会话录制”页面显示“会话录制由团队设置管理”，则 Splashtop Gateway Web 门户网站中的设置将会覆盖 On-Prem 应用程序设置

平台

- Windows
- macOS
- 安卓（Gateway 版本需要 v3.36.0或更高，安卓应用版本需要 v3.7.4.0或更高）

存储路径

通过映射 UNC 路径，可以将录制文件保存到 On-Prem 应用程序电脑或网络驱动器的不同位置。

- 默认路径：

1）Windows - *C:\用户\用户名\文档\Splashtop On-Prem*
2）macOS - */用户/用户名/文档/Splashtop On-Prem*
3）Android -*%device_album_path%/Splashtop On-Prem*

- *特定路径：*

12. *从安装 On-Prem 应用程序的电脑端手动输入本地文件夹路径。*
13. 手动输入 Windows UNC 路径：\\servername\path
14. 手动输入 macOS UNC 路径：//servername/path
15. 最大路径长度：256个字符。

- 应用程序设置

遵循 **Splashtop On-Prem 应用程序设置**的存储路径。

大小限制

如果录制文件大小超过大小限制，录制文件将自动删除。

- 最小值：0MB（无限制，安装 On-Prem 应用程序的电脑端的所有可用空间）
- 最大值：40000MB

集中式会话录制

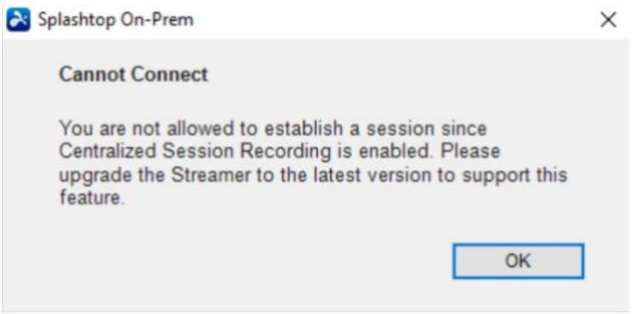
BETA 测试 - 我们目前正处于新录制功能的 Beta 测试阶段。如果您想申请测试，请联系 Splashtop 销售人员。

通过集中式会话录制，IT 管理员可以强制录制所有 Splashtop 远程桌面会话。所有会话均由 Splashtop Gateway 服务器录制，如果启用此功能，技术员就无需从客户端应用程序端手动开始或停止录制。

会话录制视频可以通过 Splashtop 网络控制台播放或下载，用于培训和审计目的。

要求

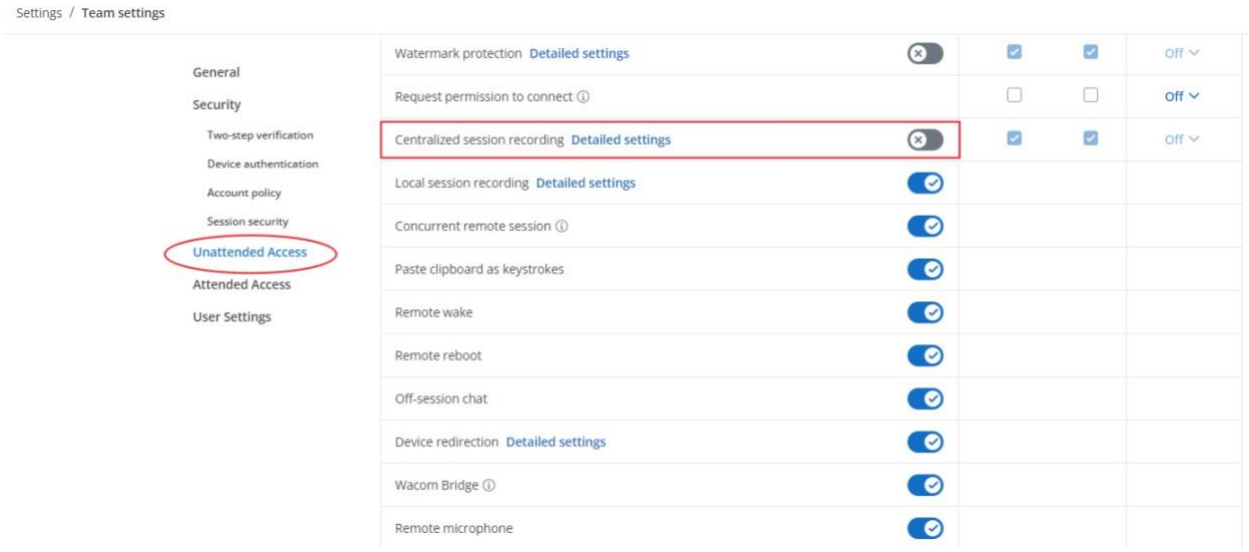
- **本地电脑**（技术员端）：仅限 Windows 和 Mac；客户端应用程序版本为 v3.5.2.2 或更高。
- **远程电脑**（端点/最终用户端）：Windows、Mac、iOS 和安卓；Streamer 版本为 v3.5.2.2 或更高。如果 Streamer 不满足版本要求，会话将被阻止，并显示以下错误消息。

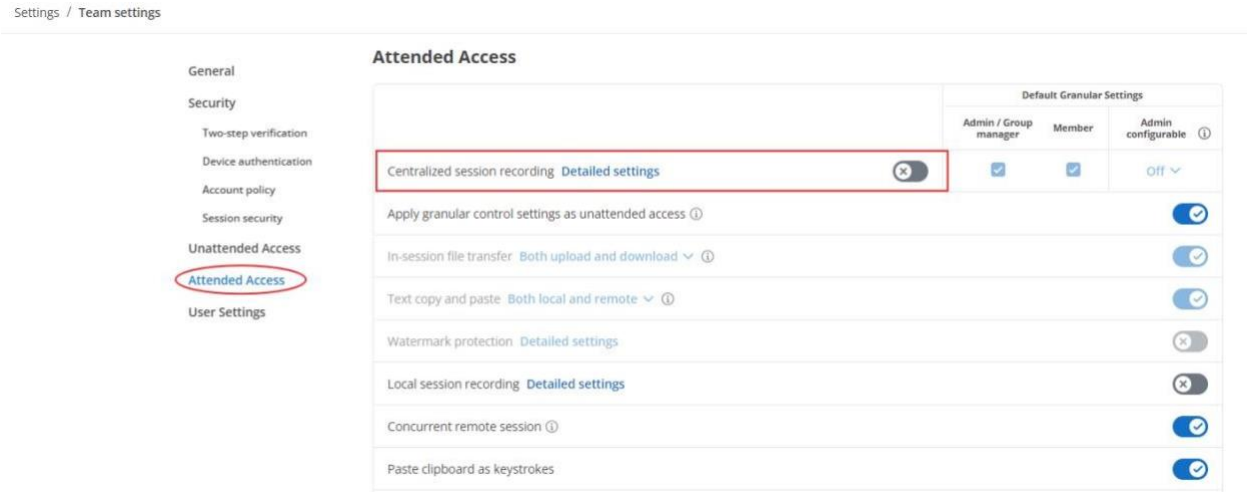


在网络控制台启用集中式会话录制

请联系 Splahtop 销售人员为您的许可证激活附加功能。

默认禁用集中式会话录制功能，可以通过 Splashtop 网络控制台启用。
（启用方法：Gateway 网络控制台->设置->团队设置->无人值守访问/有人值守访问）



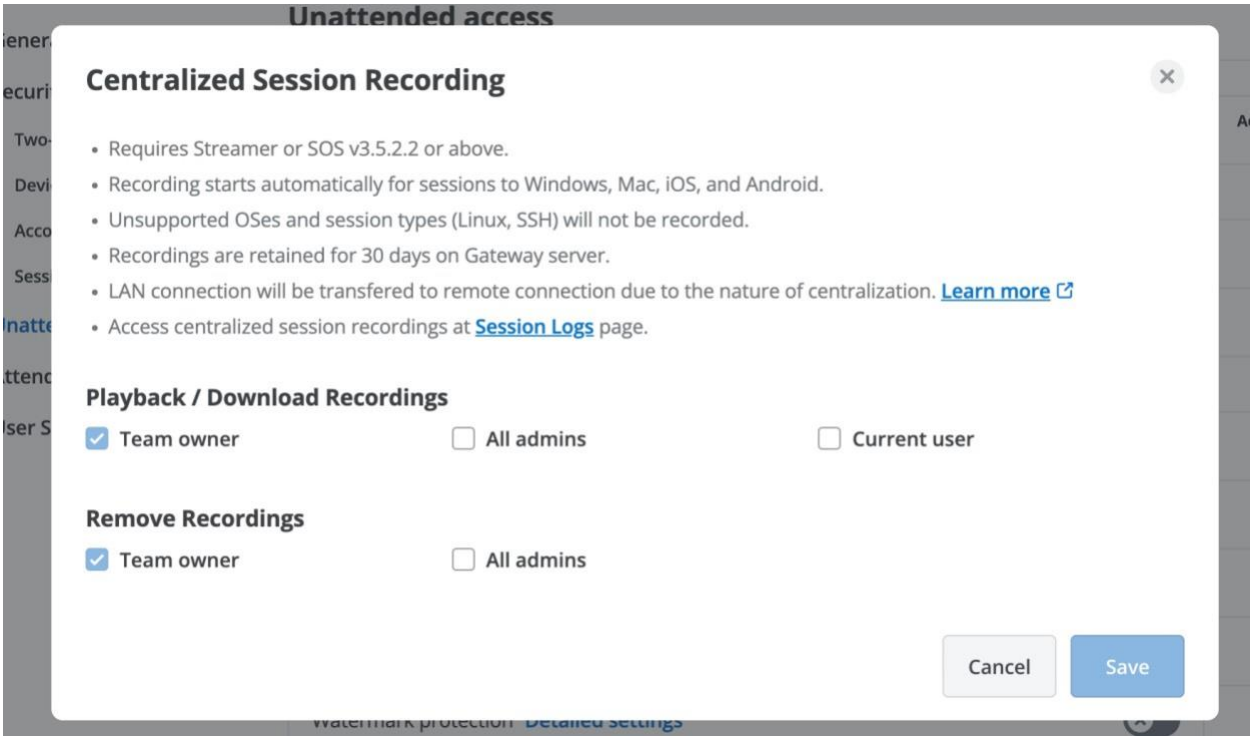


详细设置

可以根据用户角色授予播放/下载或删除录制内容的权限。默认情况下，团队所有者被授予所有权限。

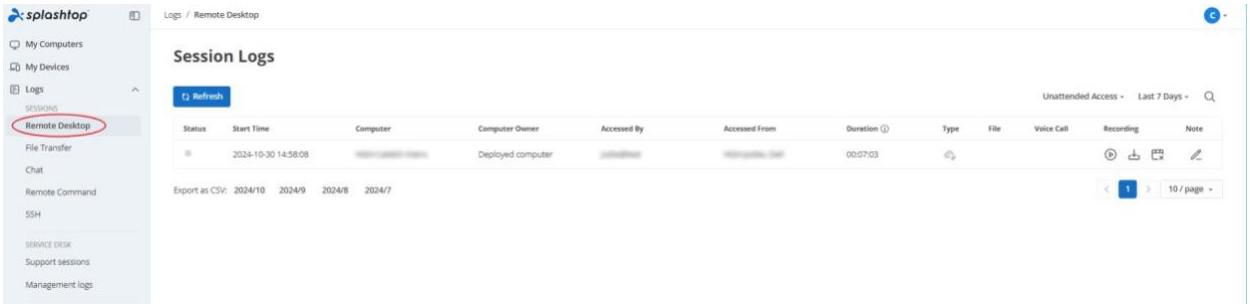
为了在处理录制文件时获得最大的安全性，加密的流数据必须存储在 Splashtop Gateway 中，以确保文件完整性。Splashtop 客户端应用程序和 Streamer 之间的 LAN 连接将被重定向到 Gateway 服务器。

录制文件将在 Gateway 服务器上保留30天。确保及时下载所有所需文件以备将来之需。



播放和下载

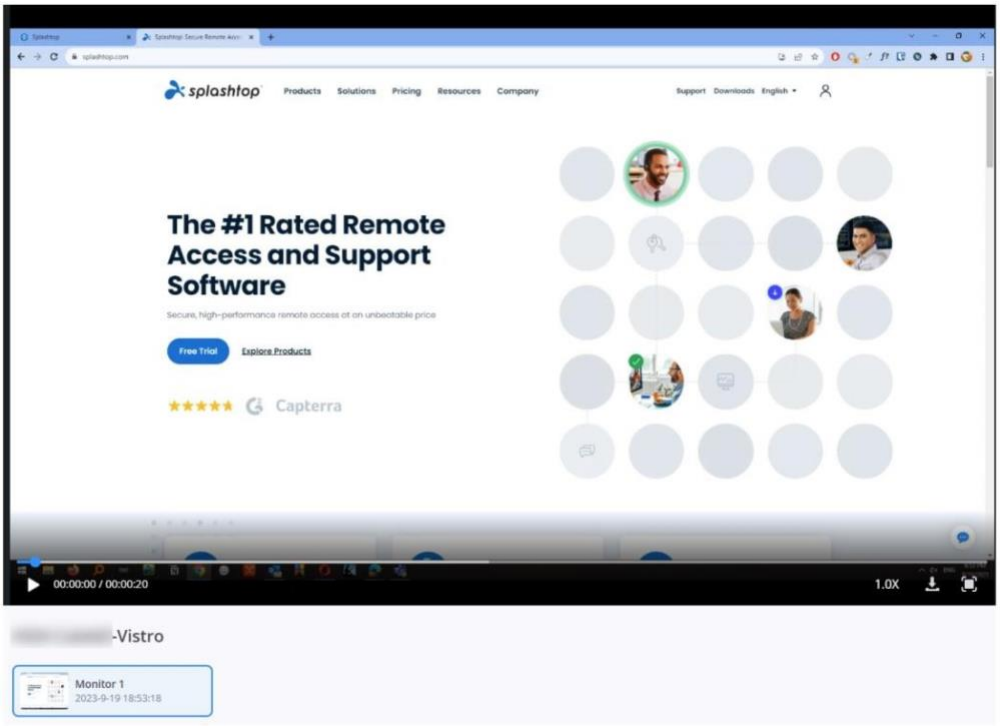
可以从 Splashtop 网络控制台中的会话日志页面访问录制内容。（方法：Gateway 网络控制台->日志->会话）



会话日志的录制一列显示特定会话的访问方式。

单击会话旁边的录制图标可查看该会话的录制内容。

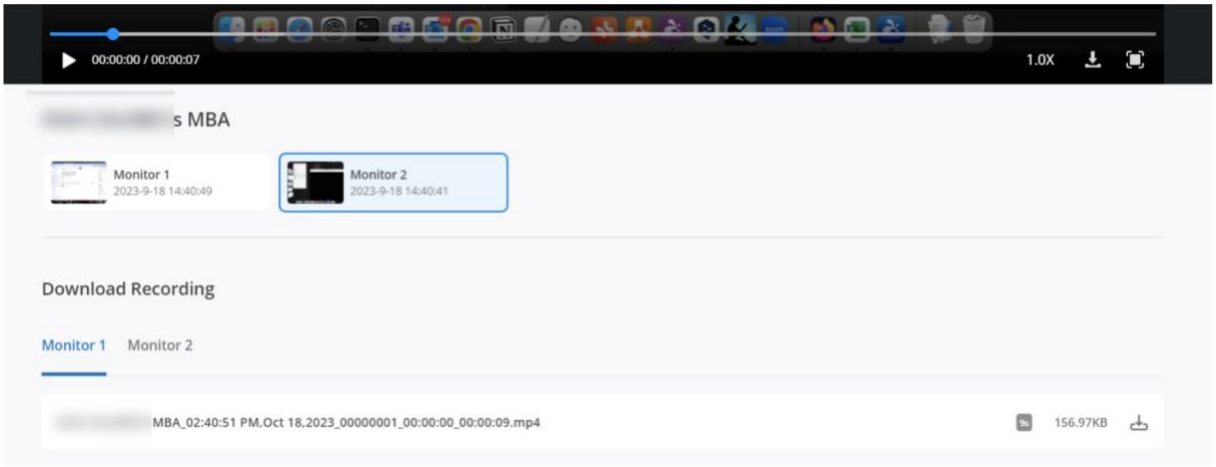
回放



在以下情况下，录制内容将被拆分为多个文件：

- 文件大小达到 512 MB（例如，如果录制内容大小为 3GB，将被拆分为6个文件）。
- 技术员将视图切换到其他显示器。
- 技术员更改帧率。
- 最终用户的设备切换方向（纵向/横向）。

下载录制视频



单击会话日志页面或播放器工具栏的下载按钮，从下载界面并选择要下载的.mp4。

注意

- 录制操作由 Splashtop Gateway 执行，因为远程会话均通过该服务器传输。所有会话都将通过 Splashtop Gateway 进行代理，以确保任何一方都无法访问录制文件。
- 录制文件的时间戳基于会话日志的时区。
- 录制内容不包含鼠标光标和音频。
- 如果一个会话有多个录制文件（例如技术员切换了显示器视图），则录制文件将按显示器和文件名中的时间戳排序（详见上图）。

将 Splashtop On-Prem 与 FreshService 集成

如果使用 FreshService 来支持客户或同事，现在则可以远程访问最终用户的电脑，可直接从支持工单启动远程连接，简单高效地排除故障。Splashtop On-Prem 是领先的本地部署版远程桌面解决方案，目前可与 FreshService 账户无缝集成。

本文将指导您完成集成设置，并介绍如何使用 Splashtop 来支持您的 FreshService 最终用户。

设置 Splashtop On-Prem 与 FreshService 的集成

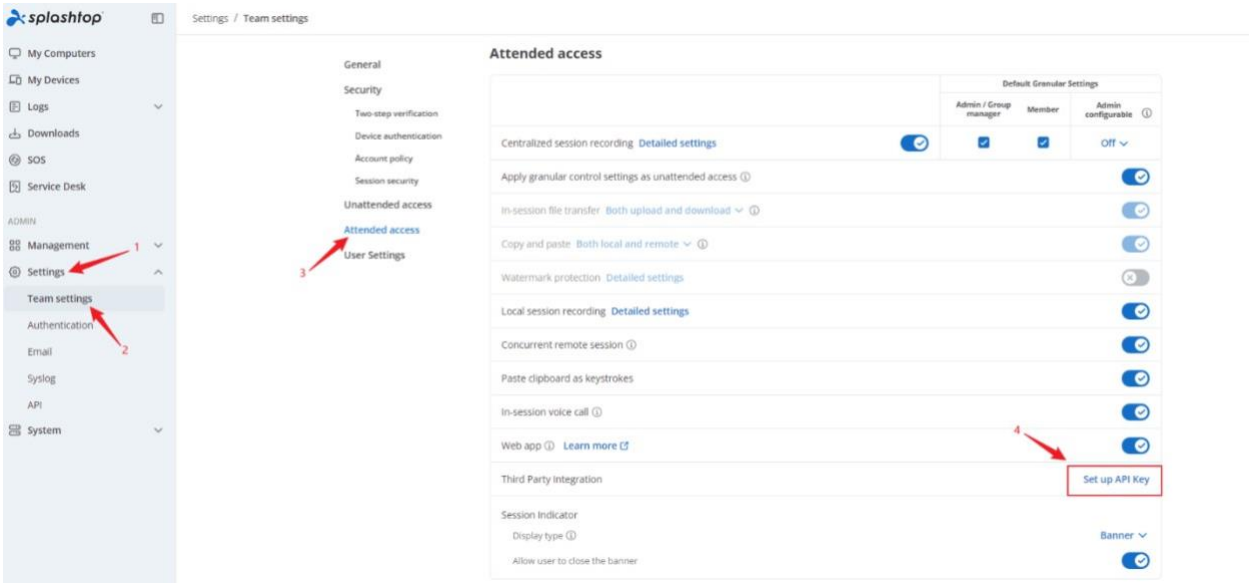
Splashtop On-Prem 与 Freshservice 集成的设置是一次性操作，可使用 API 密钥连接两个系统。需具备 Splashtop On-Prem 和 FreshService 的管理员账户才能执行该任务。

从 Splashtop Gateway 生成 API 密钥

只有团队所有者才能从 Splashtop Gateway 生成 API 密钥。

使用团队所有者账户登录 Splashtop Gateway，然后导航到**设置 > 团队设置 > 有人值守 > 第三方集成** 。

单击**设置 API 密钥**按钮。



在弹出窗口中，选中 FreshService 所在行开头的复选框。将在密钥字段中生成 API 密钥。

单击**获取新密钥**按钮，以将 API 密钥替换为新密钥 。然后，前一个密钥将被替换。

设备/浏览器身份验证

为了提高安全性，运行 Splashtop On-Prem 应用程序并使用 Splashtop 账户登录的所有设备现在都需要通过电子邮件或网络 控制台进行身份验证。

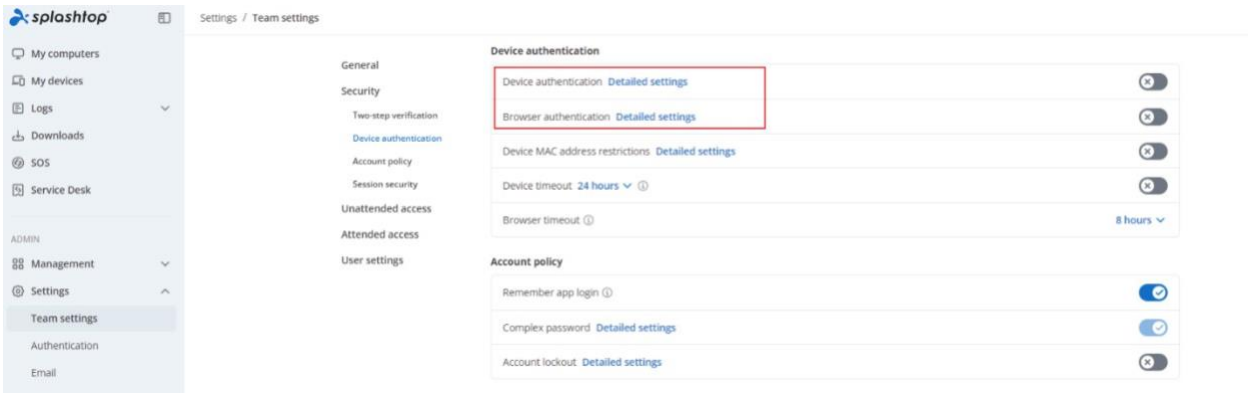
每台电脑上的每个应用程序/浏览器仅应触发一次电子邮件。也就是说，首次登录 On-Prem 应用程序会触发一次电子邮件，在新浏览器中登录网站会触发一次电子邮件。

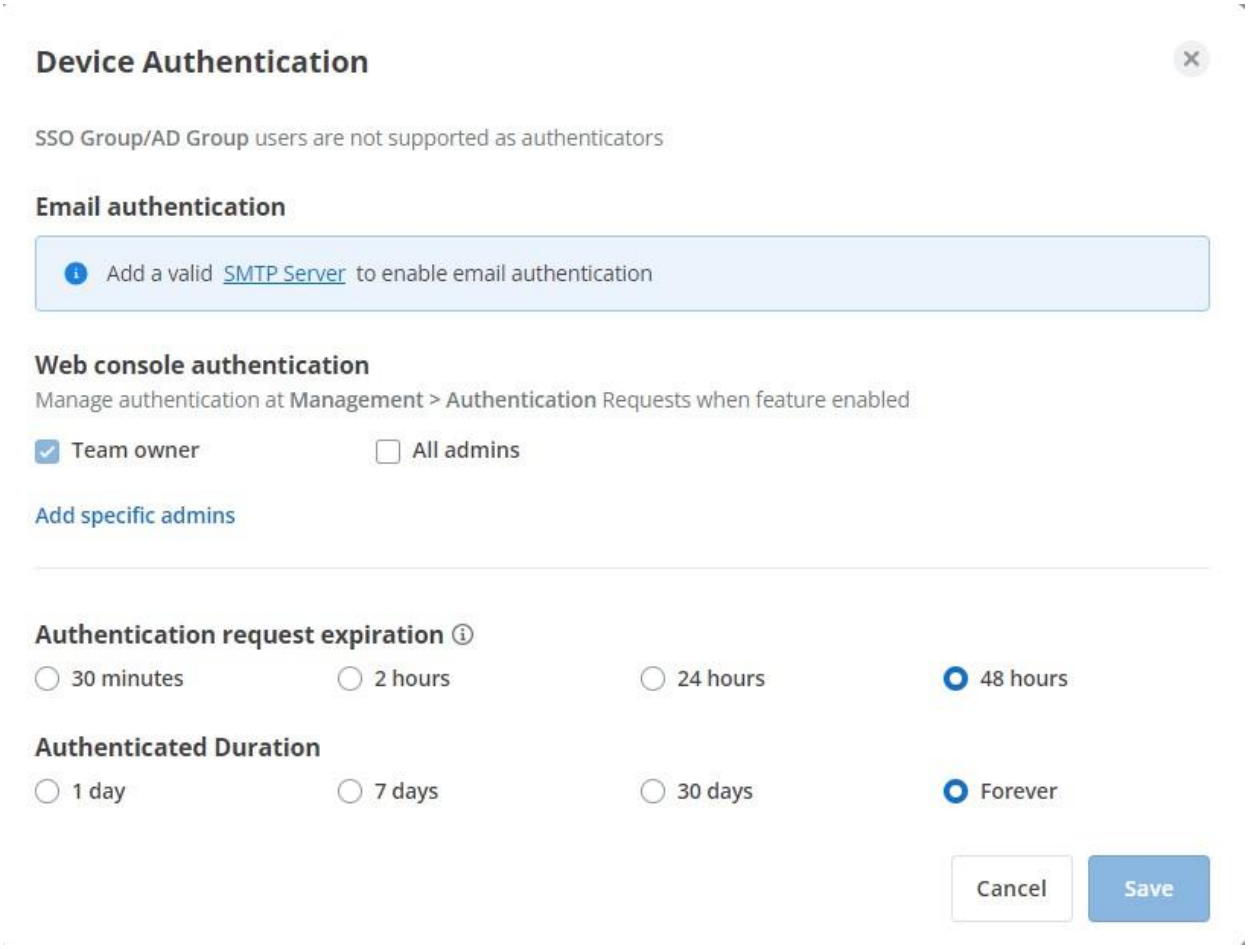
首次登录新设备时，如果系统管理员要使用电子邮件身份验证，我们将通过电子邮件向您发送身份验证链接。您需要先单击身份验证链接，然后才能成功登录并在该设备上使用 Splashtop On-Prem 应用程序。（等待5分钟后尝试登录，系统将再次发送邮件）。

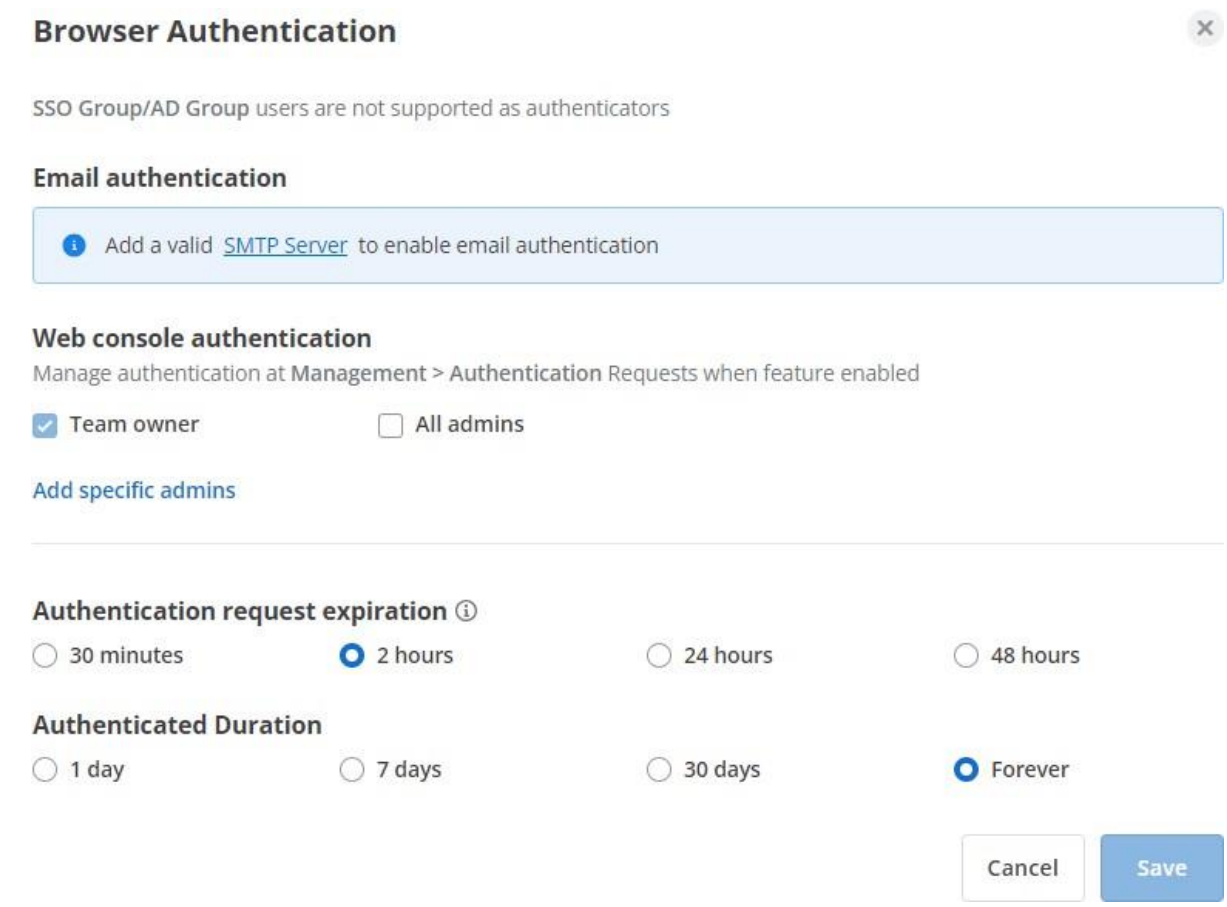
系统管理员可以通过登录 Splashtop Gateway 网络控制台顶部菜单 - >设置 -> 团队设置，使用所有者账户配置详细设置。

- 身份验证软件：选定用户可以通过验证电子邮件或网络控制台，对从 Splashtop On-Prem 应用程序或 Splashtop 网络控制台生成的每次登录尝试进行身份验证。

- 身份验证请求过期：如果身份验证请求的待处理时间超过已配置的到期时间，而未被响应以进行验证，则最终用户需要重新发送身份验证请求。
- 身份验证持续时间：通过身份验证后，用户无需在已配置持续时间内对同一设备/浏览器进行身份验证。







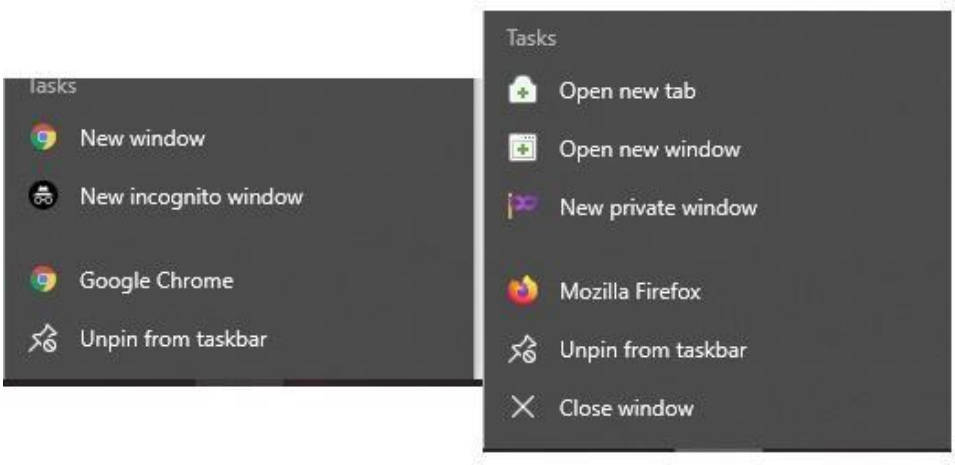
为什么收不到验证电子邮件？

如果您没有收到电子邮件，请检查以下内容：

- 请在几分钟后检查，邮件路由可能延迟
- 请检查垃圾邮件和文件夹
- 您的电子邮件服务（即 Outlook）有黑名单或白名单，请检查是否被该列表阻止/尚未获得批准。
    - 在 Outlook 2010/2013中，单击功能区的**垃圾邮件**按钮，然后选择**垃圾电子邮件**选项。您可以在**安全发件人**和**安全收件人**选项卡上找到白名单。黑名单位于**阻止的发件人**选项卡。
- 您的网络/域已阻止并自动删除来自 Splashtop 的所有电子邮件
    - 如果是这种情况，请联系您的本地网络/IT 管理员，以允许接收 Splashtop 电子邮件。

点击验证链接没有反应？

有时会收到验证电子邮件，但单击身份验证链接却没有反应。浏览器上保存的 cookie 偶尔会产生干扰，则可能会发生这种情况。最简单的解决方法是打开一个新的私密浏览器/隐身窗口。



然后重新接收身份验证电子邮件，并在使用隐身窗口/私密窗口时打开电子邮件进行身份验证。

注意

1. 请在使用电子邮件设备/浏览器身份验证之前添加有效的 SMTP 服务器并测试该功能。
2. 如果您无法再访问用作 Splashtop ID 的电子邮件地址，请将您的 Splashtop ID 更改为新的电子邮件地址，然后再次尝试登录。身份验证电子邮件将发送到您的新电子邮件地址。
3. 更改 Splashtop ID 将清除所有此前已通过身份验证的设备。

Splashtop On-Prem 密码策略

创建或更新密码时，请务必选择满足密码复杂性要求的密码。

复杂密码策略：

- 至少8个字符（最小长度由系统管理员定义）
- 至少1个大写字母 （a-z）、1个小写字母 （A-Z）、1个数字 （0-9）
- 至少1个特殊字符 ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/

- 没有常用词
- 账户名称或最后5个密码不匹配

账户锁定策略

账户锁定策略设置**规定了登录尝试失败的次数，登录尝试失败会导致用户账户被锁定，**只有管理员或所有者重置锁定账户，或账户锁定时间策略设置中规定的分钟数到期，该锁定账户才能再次被使用。

简介

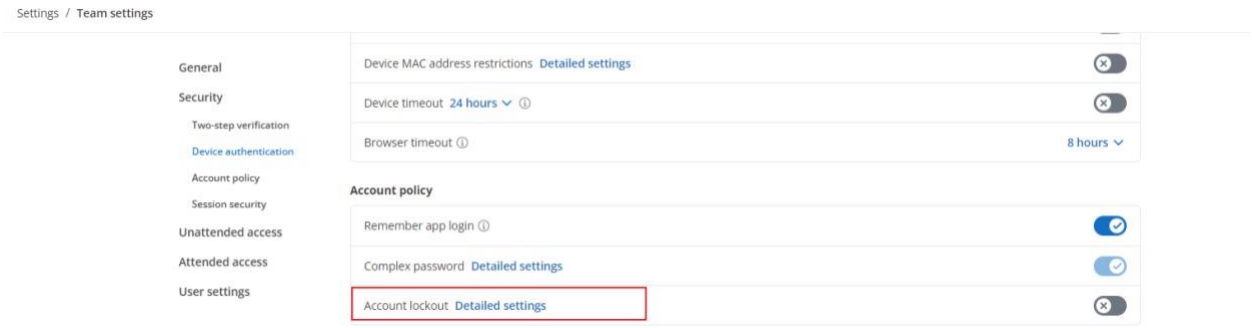
账户锁定阈值：该策略设置规定了登录尝试失败的次数，登录尝试失败会导致用户账户被锁定。

账户锁定持续时间：该策略设置规定了被锁定账户在自动解锁前保持锁定状态的分钟数。

手动解锁：管理员或所有者可以管理>用户页面中手动解锁被锁定账户。

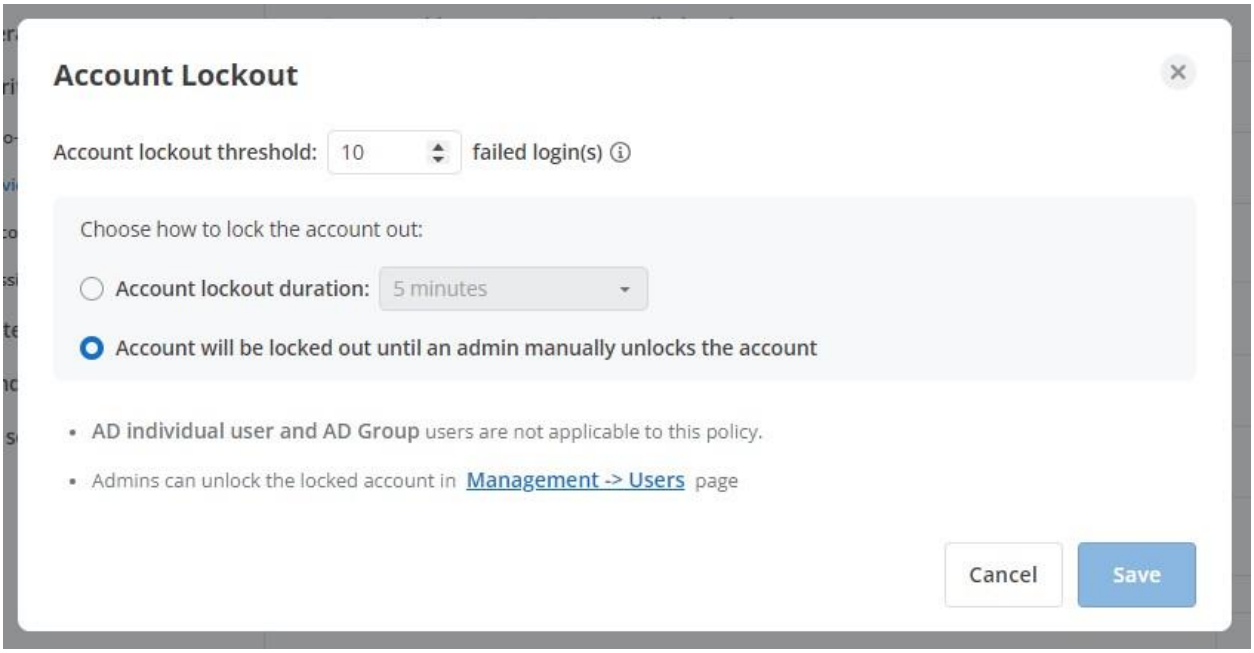
如何设置账户锁定策略？

1. 以团队所有者身份登录 Gateway 管理控制台，导航到设置 > 团队设置 > 账户策略 > 账户锁定。



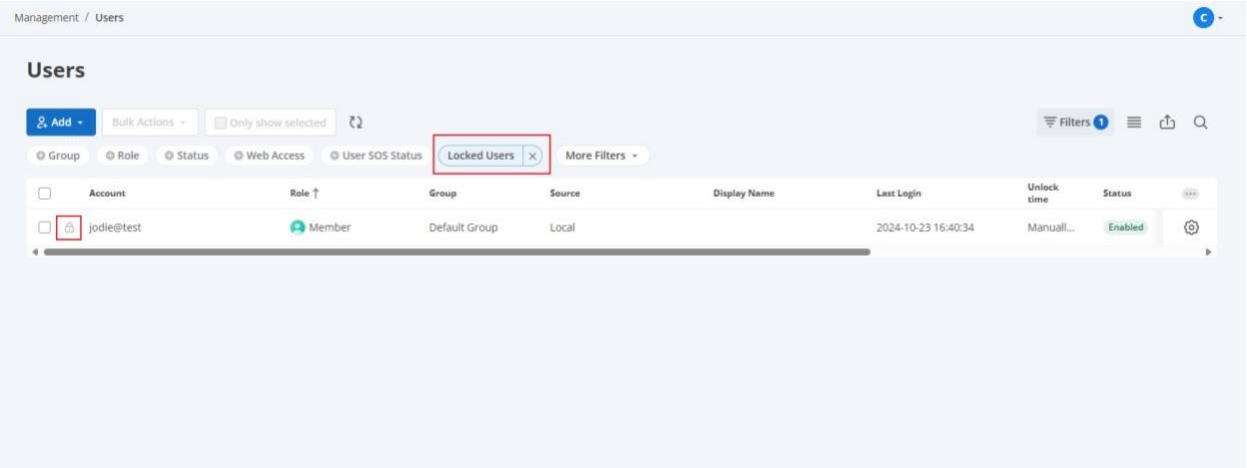
2. 然后，团队所有者可以在详细设置中配置账户锁定阈值和账户锁定持续时间。

点击保存按钮保存设置并打开该功能。

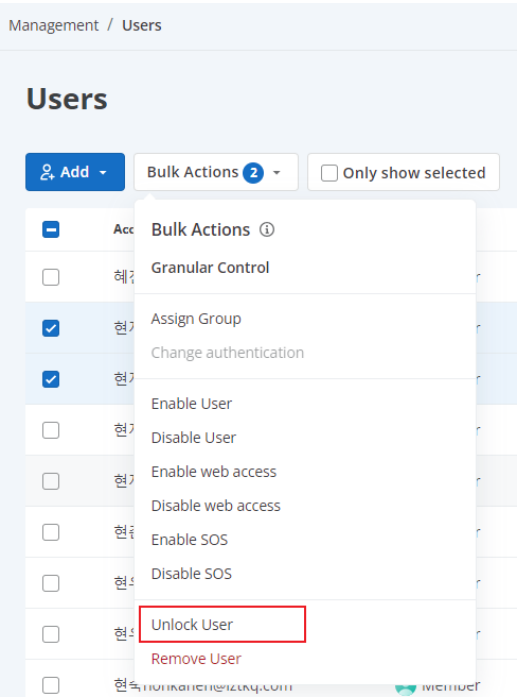


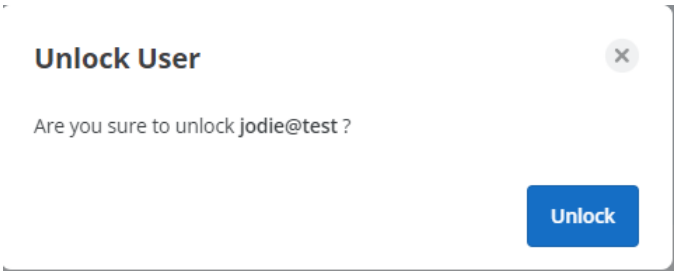
如何通过管理员解锁被锁定账户？

1. 以管理员或所有者身份登录 Gateway 管理控制台，导航到管理 > 用户页面。打开用户选项过滤器并选择 “锁定用户”。



2. 找到被锁定账户，单击齿轮图标并选择解锁用户。确认后，将解锁被锁定用户。





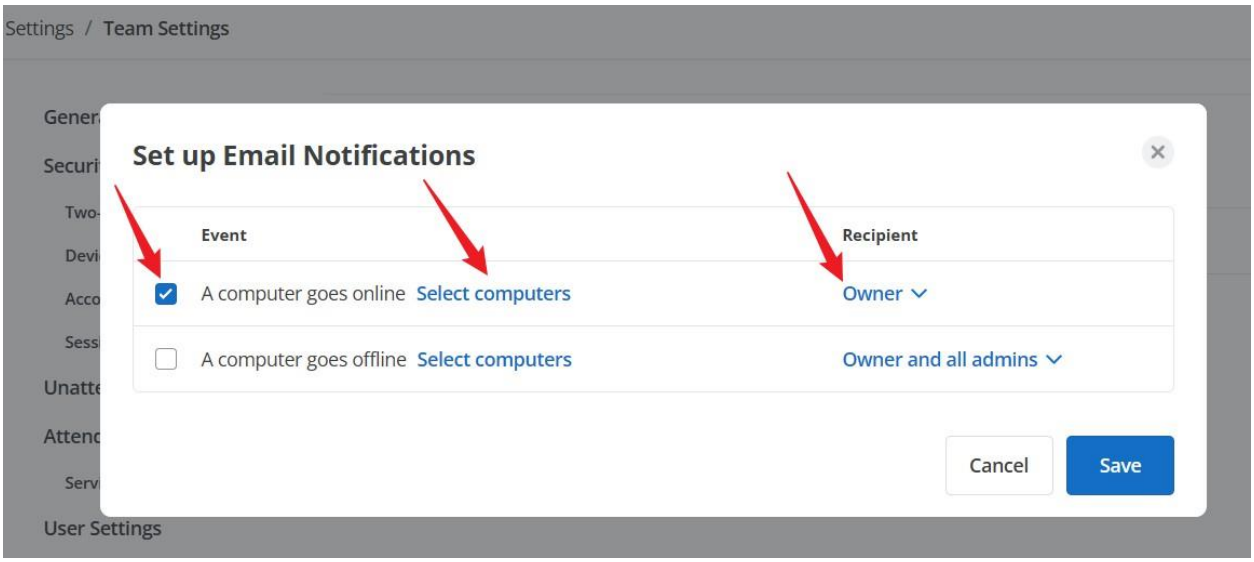
电脑在线或离线时通知

Splashtop On-Prem 支持电脑在线和离线状态通知功能。通知只能由所有者配置。

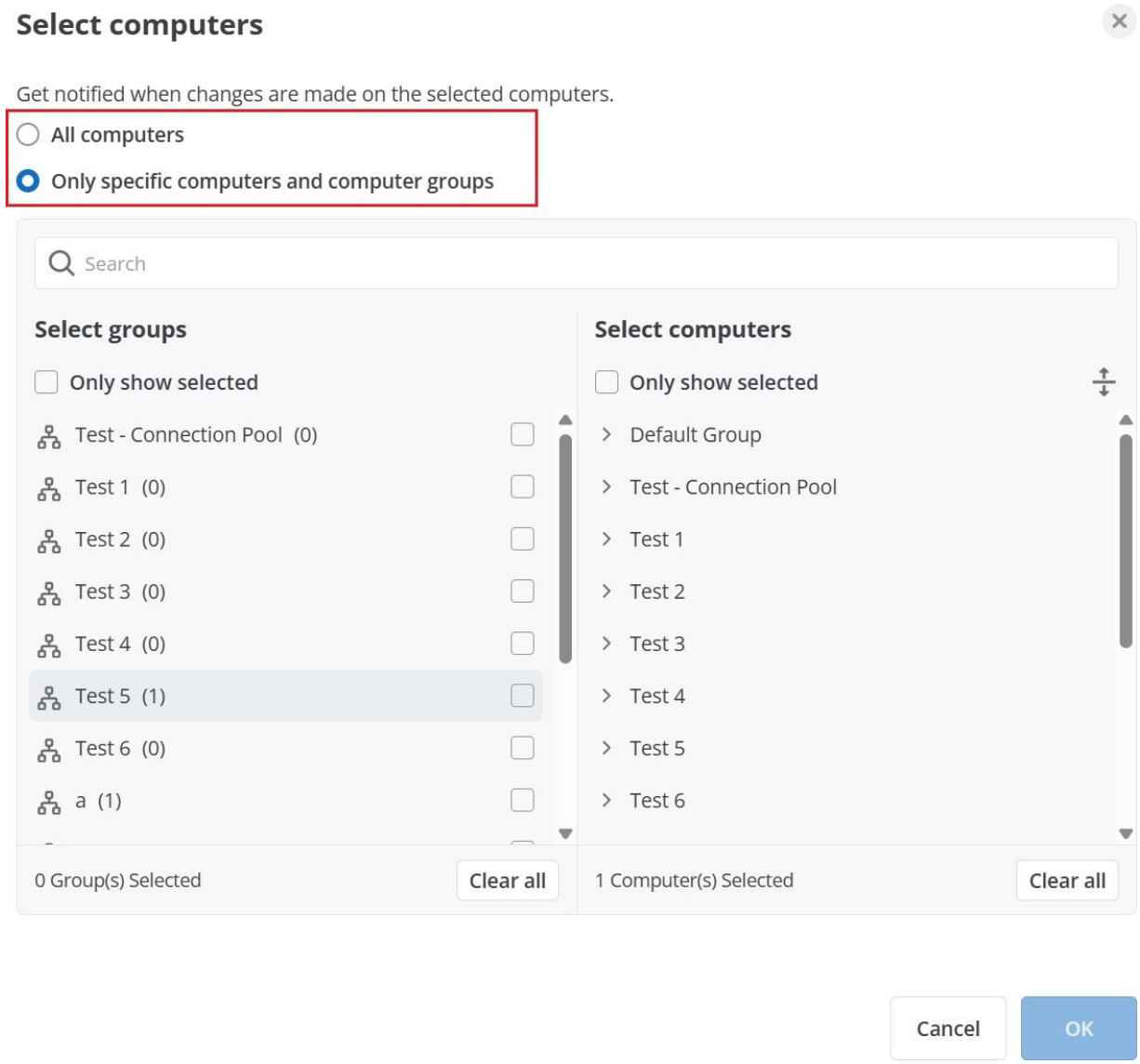
使用指南

登录 Gateway 网络控制台并导航到*设置->团队设置*。

然后点击“设置电子邮件通知”链接。可在此处启用/禁用通知并配置通知接收人。



选择要监控的电脑。电脑状态发生变化时，通知接收人将会收到通知。



注意

此功能在启用 SMTP 服务器时生效。

会话记录

Splashtop Gateway 从**3.36.0**版本开始支持会话记录功能，使管理员和审计员能够出于安全性和合规性目的审查用户会话的文本记录。包括以下内容：

聊天记录

记录远程支持会话期间技术员和远程用户之间的所有聊天对话。

远程命令记录

捕获通过远程命令功能执行的所有命令。

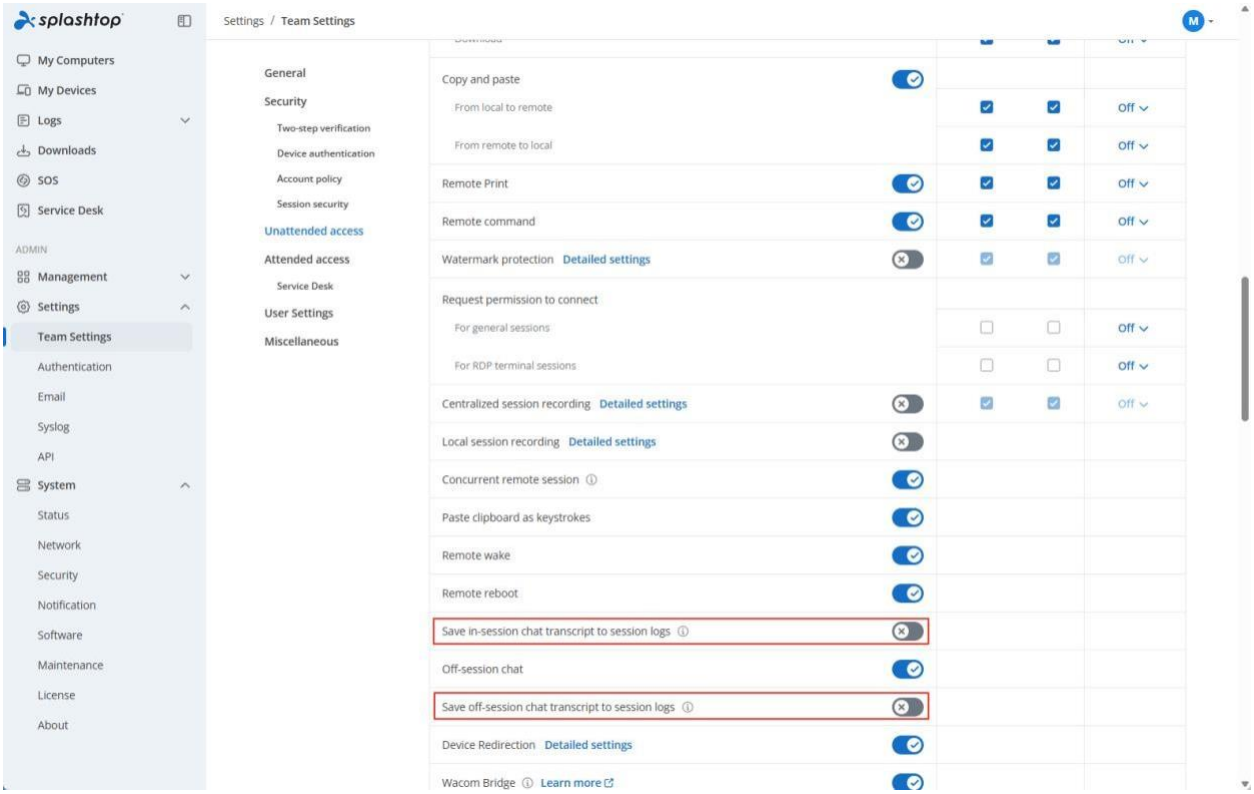
SSH 记录

记录通过 Splashtop 发起的 SSH 会话的终端输入/输出。

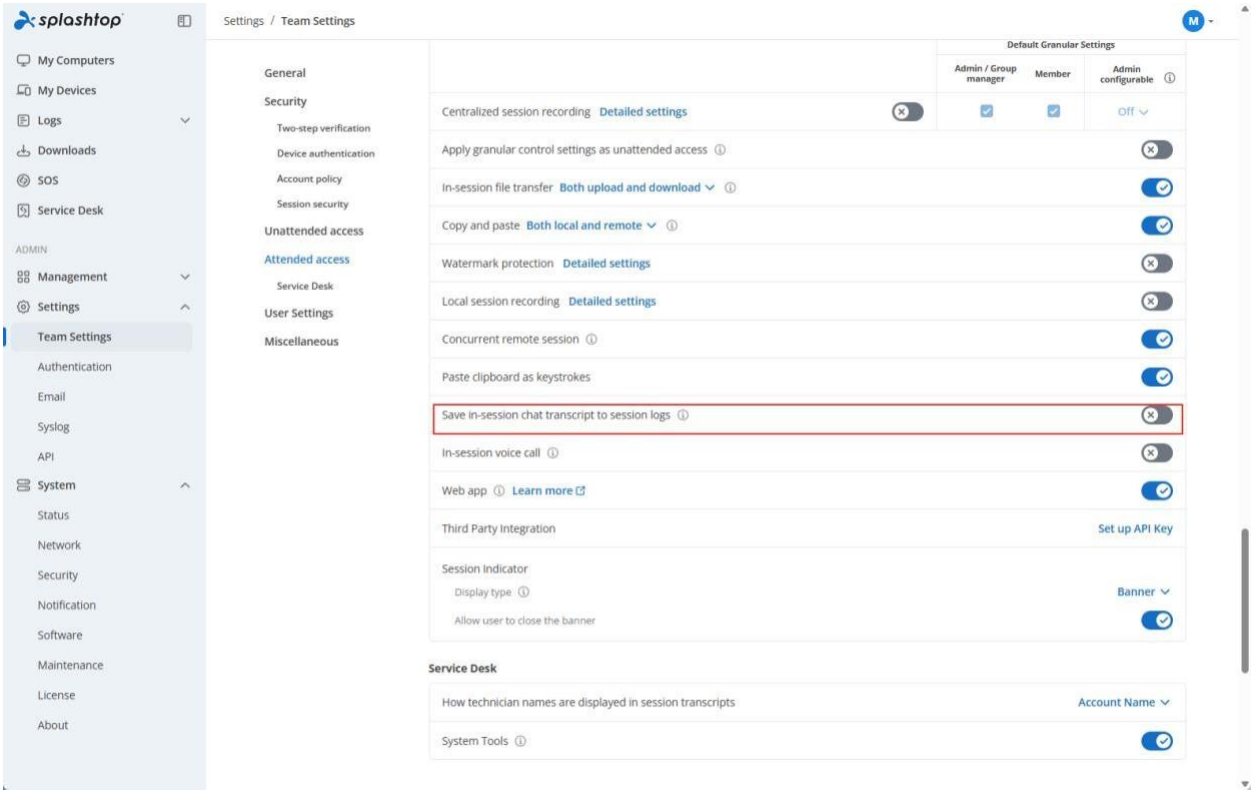
如何启用聊天记录？

团队所有者可以在团队设置中启用/禁用将会话中和会话外聊天记录保存到会话日志的选项。（要求 On-Prem Streamer v3.7.4.5或以上版本）。

对于**无人值守访问**，导航至 Gateway 的**【设置】>【团队设置】>【无人值守访问】**。



对于**有人值守访问**，导航到 Gateway 的**【设置】>【团队设置】>【有人值守访问】**。



如何查看会话记录

如果已启用聊天保存选项，则可以在网络控制台中查看会话记录。导航到【**日志**】>【**聊天**】以获取保存的聊天记录。

可以在网络控制台中查看会话记录。导航到【**日志**】>【**远程命令**】以获取保存的聊天记录。

可以在网络控制台中查看会话记录。导航到【**日志**】>【**SSH**】以获取保存的 SSH 记录。

身份验证

如何申请新的 SSO 方法？（SAML 2.0）

Splashtop 目前支持使用 SAML 2.0 身份提供商创建的凭据登录 Gateway 和 *Splashtop On-Prem 应用程序*。请按照以下说明为团队申请 SSO 方法。

要求

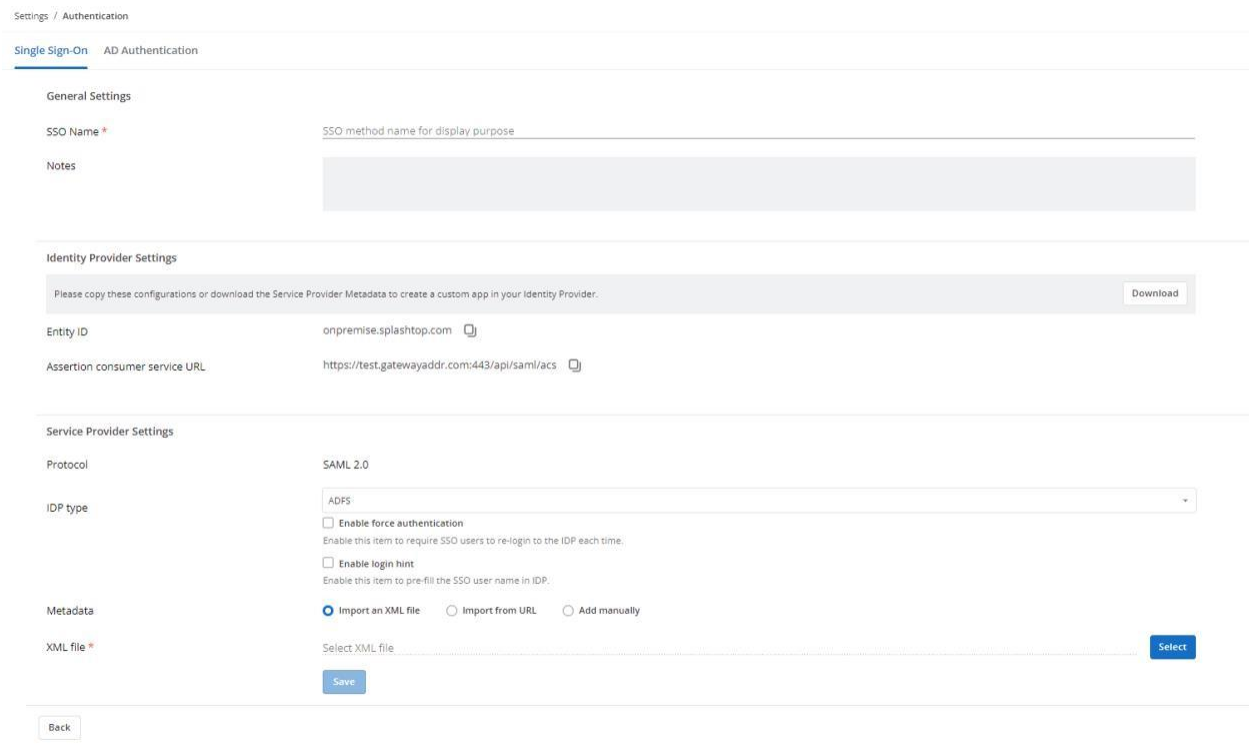
- **Splashtop Gateway v3.24.0** 或更高版本

输入 IDP/X.509 证书信息

1. 使用所有者账户登录 Gateway，然后转到管理/设置/身份验证/单点登录。

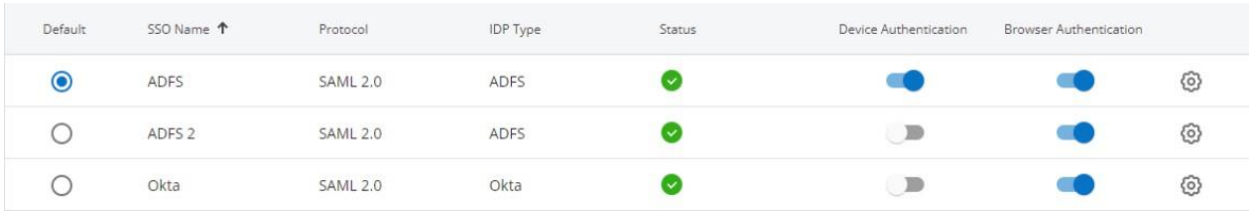
2. 单击“添加”以添加 Gateway URL。请填写正确的 Gateway URL，以确保 Gateway 和 IDP 之间的连接。

3. 点击“添加 SSO 方法”，然后输入所需信息并保存 SSO 方法的设置。



- **通用设置**
  - **SSO 名称**：输入 SSO 方法的名称。
  - **备注**：输入 SSO 方法的备注。
- **身份提供商设置**
  - **实体 ID**：请从 Gateway 复制实体 ID 和断言消费者服务 URL，然后将其粘贴到 IDP。
  - **断言消费者服务 URL**：请从 Gateway 复制实体 ID 和断言消费者服务 URL，然后将其粘贴到 IDP。
  - **下载服务提供商元数据**：此外，我们还提供元数据下载，以在 IDP 中导入 SP 的元数据。
- **服务提供商设置**
  - **协议**：已修复为 SAML 2.0。
  - **IDP 类型**：选择 IDP 类型。
- **元数据**（输入 **IDP SSO 登录 URL**、**IDP 颁发者**和 IDP 中的 **X.509 证书**信息：Okta、Azure AD、JumpCloud、OneLogin 或 ADFS 或其他 IdP）
  - 使用元数据导入自动填充设置
    - **上传 XML 或从 URL 导入**
  - 或**手动添加**
    - 对于 X.509，需要从 IdP 复制内容，并将其粘贴到以下字段。
    - 注意 **http** 地址与 **https** 地址

4. 点击“保存”将启用 SSO 方法。



- 可在齿轮按钮中启用/禁用/删除 SSO 方法。
- 可以根据不同 SSO 方法选择禁用设备身份验证，只需在“设备身份验证”列下取消选中相应的 SSO 方法即可。
- 可以根据不同 SSO 方法选择禁用浏览器身份验证，浏览器身份验证”列下取消选中相应的 SSO 方法即可。

- 还可以设置默认 SSO 方法。单击“默认”列下相应 SSO 方法的单选按钮。

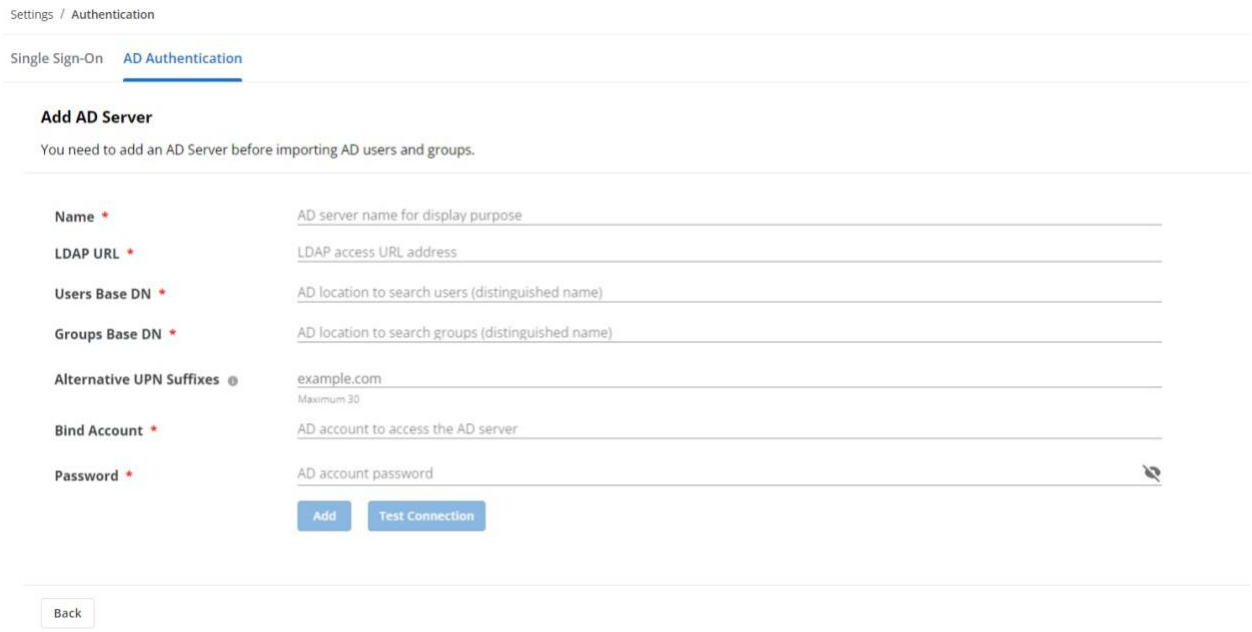
注意：

- **Gateway**（v3.24.0 或更高版本）和 **Splashtop On-Prem 应用程序**（v3.5.8.0 或更高版本）支持 SSO 登录。

活动目录

Splashtop On-Prem AD 集成与 Windows Server 2008 r2、2012、2016、2019 活动目录和 Microsoft Azure AD 兼容。团队所有者能够轻松验证和管理 AD 账户，并立即开始使用 Splashtop 远程服务。

要添加 AD 服务器，可使用团队管理员/所有者账户从**设置>身份验证>AD 身份验证**页面打开活动目录页面。



- **名称：**填写与组织的实际 AD 服务器连接的 AD 服务器名称。

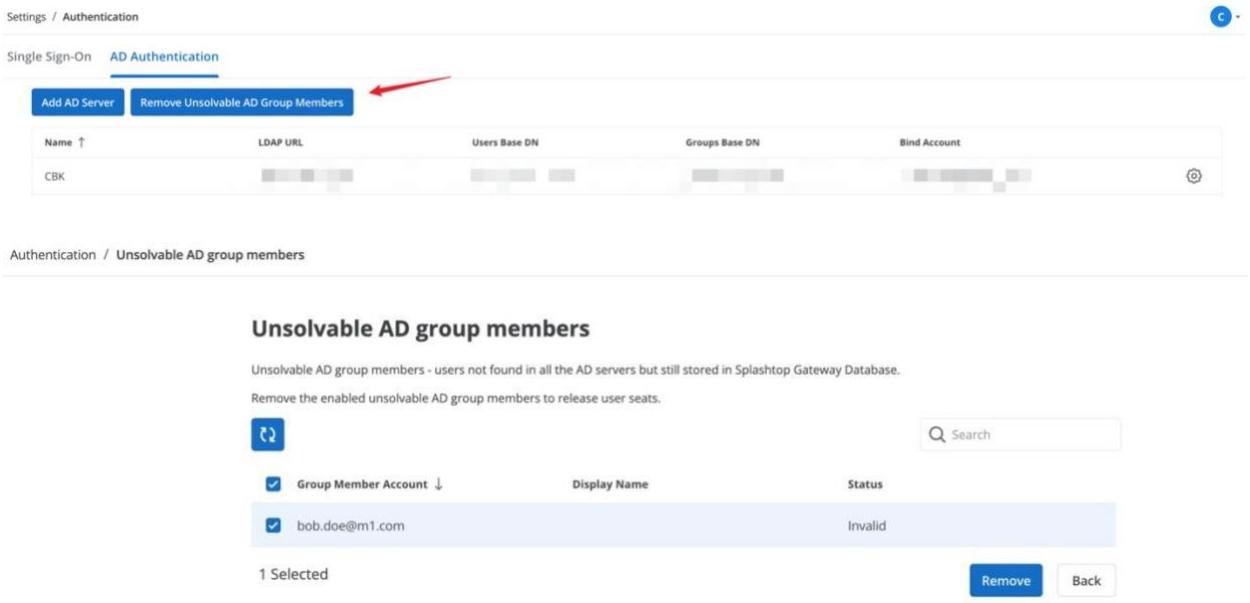
- **LDAP URL 语法**：该语法包括**ldap 地址 （ldap://） + 隐含地址（目标 AD 服务器） + 端口号（如果需要）。**支持 LDAPS。
- **用户 Base DN**：活动目录用户的 **Distinguished Name（DN）**。我们使用 Users Base DN 作为 AD 层次结构中的用户身份验证检查点。
- **组 Base DN**：活动目录组的 **Distinguished Name（DN）**。我们使用组 Base DN 作为 AD 层次结构中的组身份验证检查点。
- **备用 UPN 后缀**： 此字段允许添加 UPN 后缀，在用户管理页面添加 AD 用户时，可以选择用户可以使用哪个域后缀登录。
- **绑定账号**：目标 AD 服务器绑定的用户账号。用户账户语法：**sAMaccountName@ADLocalDomainName**
- **密码**：关联 AD 用户账户的 AD 密码。
- **测试连接**：单击此按钮可检查目标 AD 服务器的可用性以进行身份验证。
- **添加**：单击此按钮可将经过验证的 AD 服务器绑定到 Splashtop Gateway AD 服务器列表。

注意：避免添加多个范围重叠的 AD 服务器。请验证用户 Base DN 和组 Base DN 的唯一性，以确保每个用户和组只能来自一个 AD 服务器源。 范围重叠可能会导致**身份验证无效和组成员无法解析。**

AD 维护

AD 维护是一个内置工具，用于清理 Splashtop On-Prem 系统中无法解析的 AD 组成员。无法解析的 AD 组成员指外部 AD 服务器中缺失但仍存在于内部数据库中的用户。

建议清理无法解析的 AD 组成员，保持用户数据库整洁，并释放用户席位。要执行 AD 维护任务，请先检查要从 Splashtop On-Prem 系统中删除的用户，然后单击“删除”按钮。



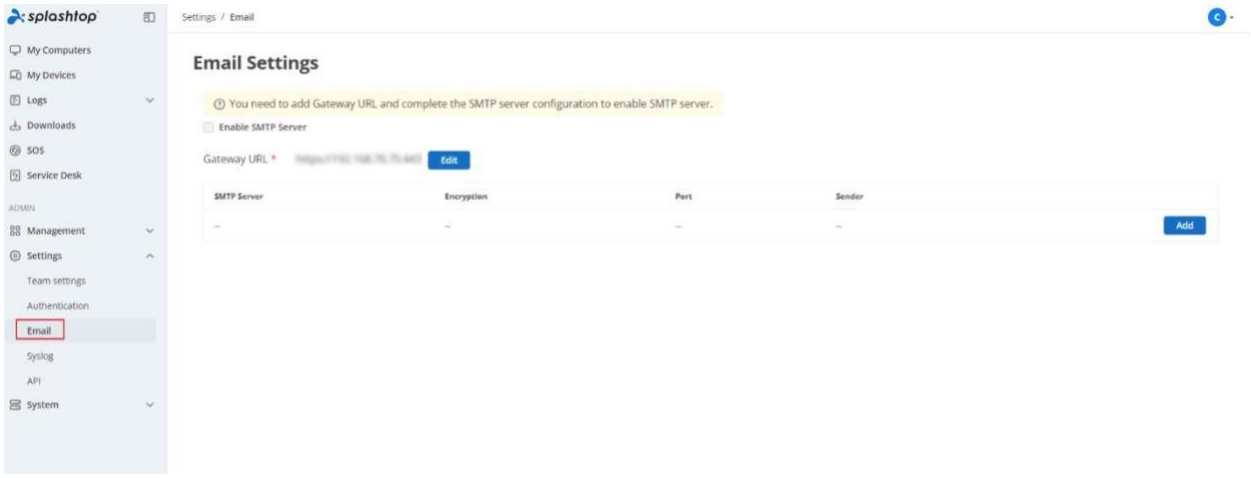
电子邮件设置（SMTP 服务器集成）

简介

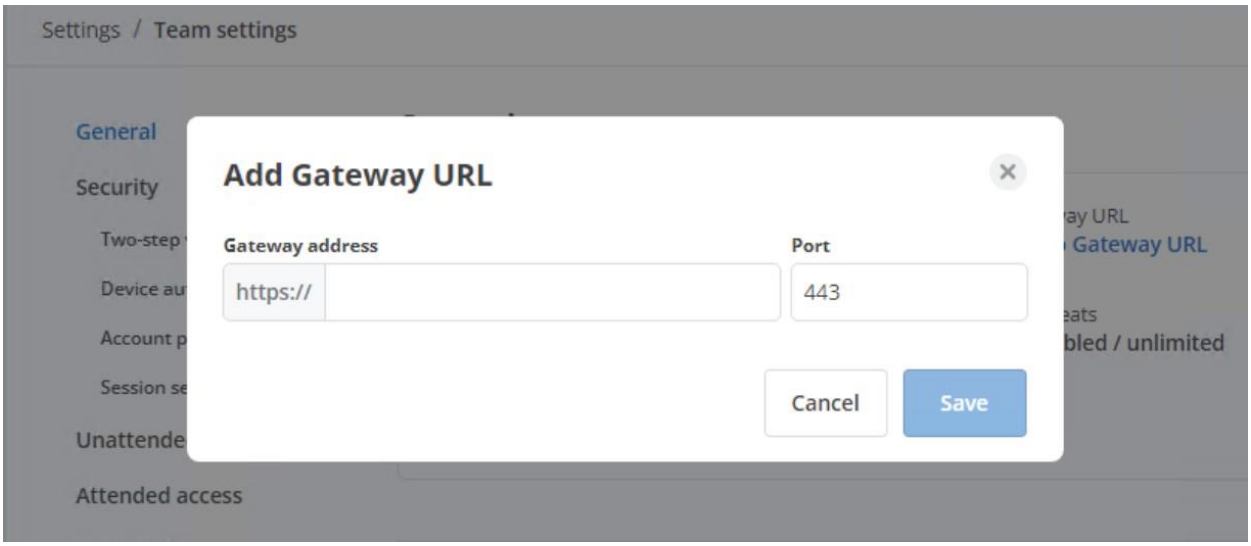
SMTP 服务器功能允许在团队设置中将 SMTP 服务器集成到 Splashtop On-Prem Gateway。成功配置 SMTP 服务器后，可以通过电子邮件对设备进行身份验证。

SMTP 服务器配置

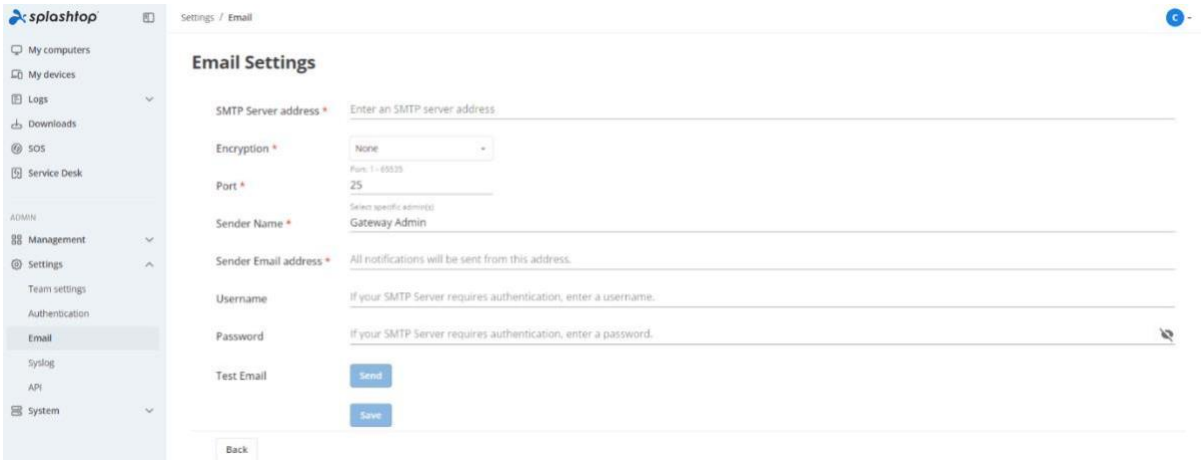
- 首先，打开网站 *https://{gatewayaddress}* -> *设置* -> *电子邮件*以配置 **SMTP 服务器**。只有在成功保存所有必要信息后，才能启用 SMTP 服务器。



- 单击“添加”将 Gateway URL 嵌入到电子邮件中。Gateway 服务器位于防火墙后面的情况下，Splashtop Gateway 自身获取其公共地址的能力受限，因此来自用户电子邮件客户端的请求将无法到达 Gateway，并导致某些事件失败。例如，设备身份验证是通过单击电子邮件中的身份验证链接来完成的，该链接将由 Gateway 系统处理。在这种情况下，需要插入正确的 Gateway URL，以确保每个身份验证请求都可以到达 Gateway 服务器。



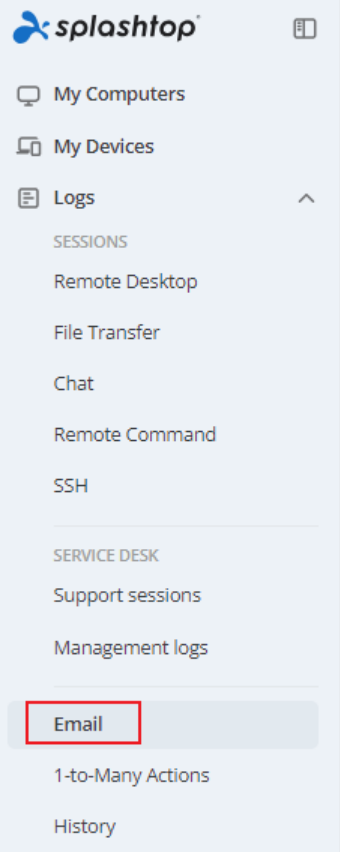
- 单击 SMTP 服务器的“添加”按钮并填写 SMTP 服务器的字段。要确保 SMTP服务器配置正确，保存前需要先验证 SMTP 服务器。



- 成功保存 Gateway URL 和 SMTP 服务器设置后，单击复选框以启用 SMTP 服务器。

电子邮件日志

- 打开网站 *https://{gatewayaddress}* -> *日志* -> *电子邮件*查看电子邮件日志。团队所有者/管理员可以在邮件日志中查看邮件发送状态，并及时发现问题。



- 在电子邮件日志中，已发送的每封邮件都将生成单独的日志。每个日志都包含时间、状态、来源、主题、发件人、收件人和类型。

注意

- 如果 SMTP 服务器有变更，请及时在 Gateway 中修改设置。否则，可能会导致邮件发送失败。
- 在电子邮件日志中，状态仅显示邮件是否已成功发送到 SMTP 服务器。请填写正确的电子邮件地址以收取邮件。

如何使用 Open API

Open API是一项新功能，允许访问数据并管理用户账户和电脑。还可以使用 Open API 开发应用程序，将 Splashtop On-Prem 功能集成到企业环境中。请按照以下说明为团队申请 Open API 应用程序。

更多详情请参阅此文API 参考 。

要求

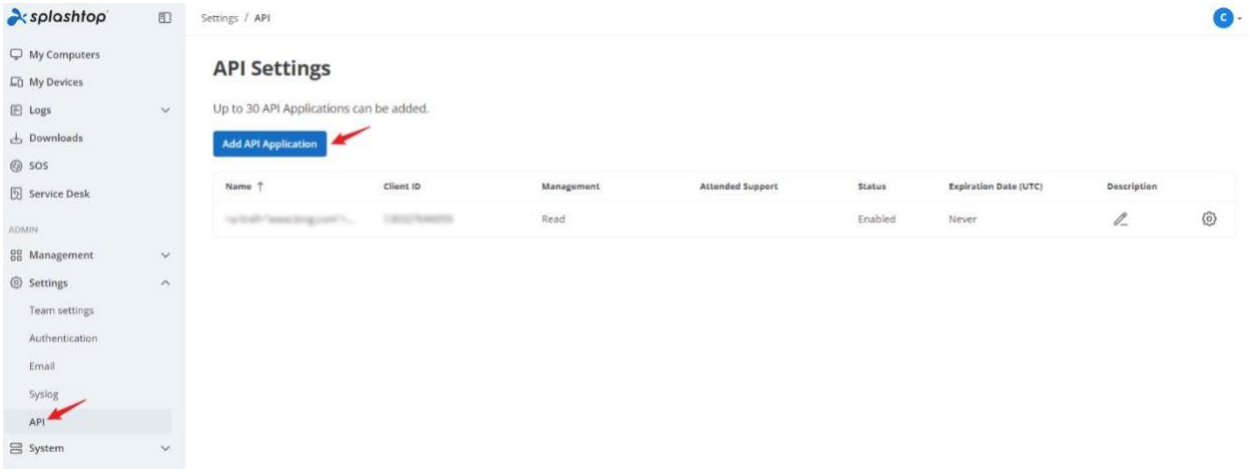
- **Splashtop Gateway v3.24.0**或更高版本。
- 已在许可证中启用 Open API。

配置方法

1. 确保已在许可证中启用 Open API。如果您有任何问题，请联系销售人员以了解更多。

2. 使用团队所有者凭证登录 Gateway。

3. 导航到**设置 > API**，然后单击 **API 设置**页面上的**添加 API 应用程序**按钮。



4. 输入 API 应用程序**名称**并配置 **API 权限** （读取或写入），然后单击**添加**按钮。

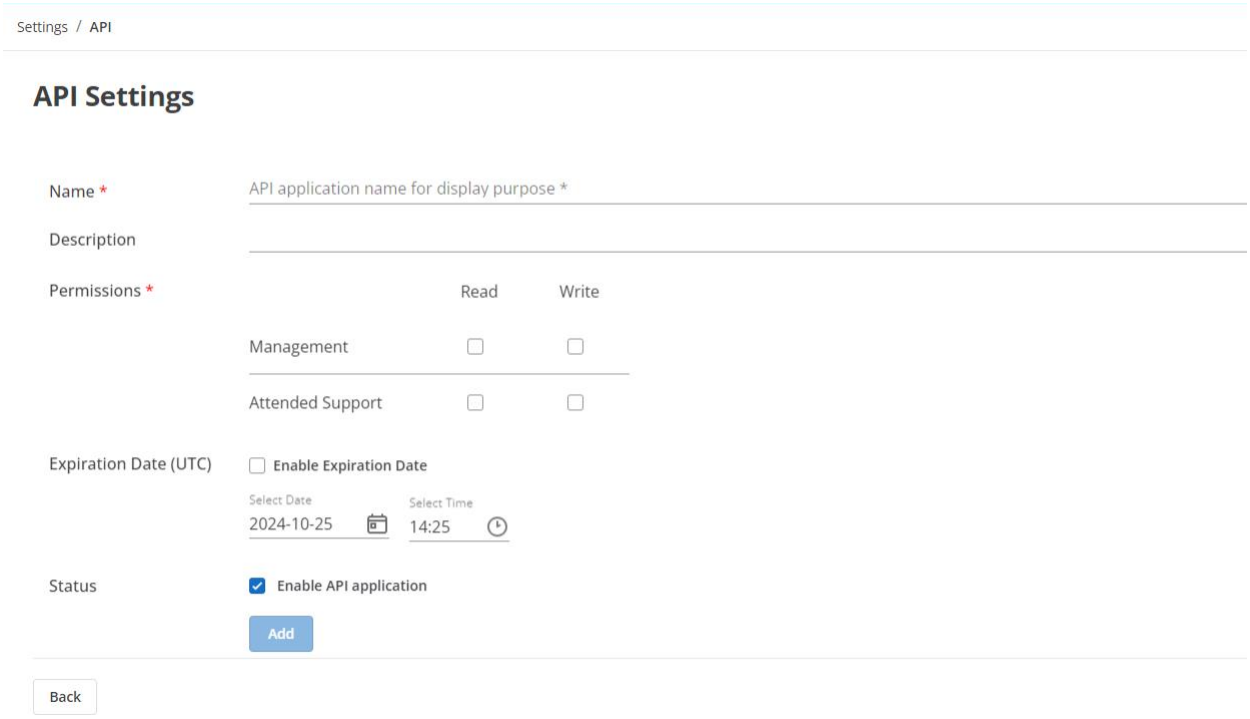
a. **名称**，用于显示 API 应用程序名称。

b. **权限**， 设置 API 应用程序的 API 权限。

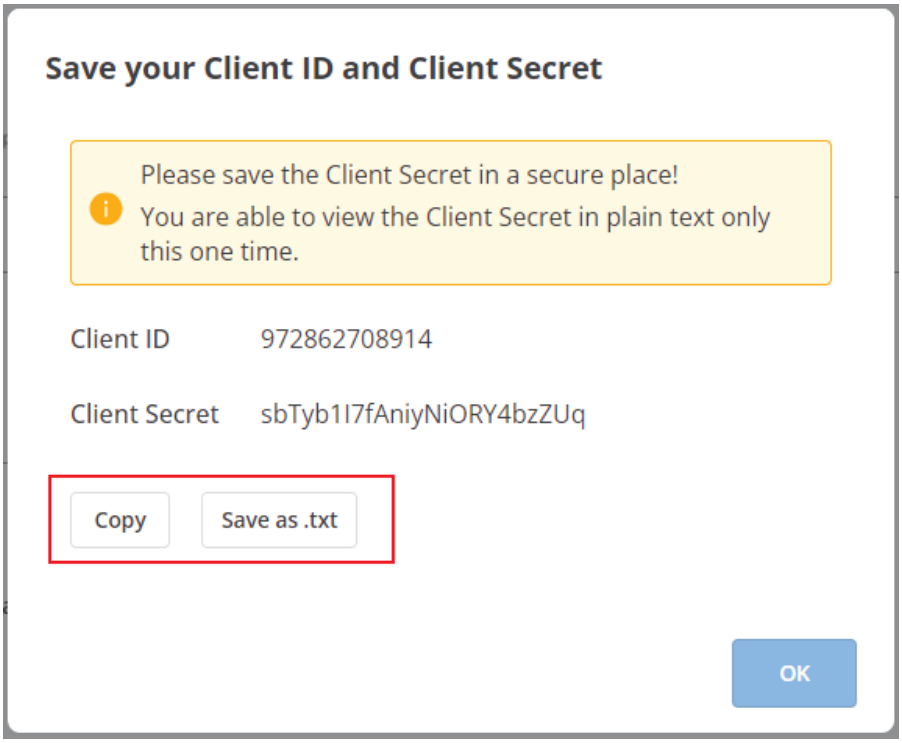
1) **管理**，启用此项以允许使用用户/访问权限/电脑/组/日程/安全相关 API
2) **有人值守支持**（要求 Gateway v3.28.0），启用此选项以允许使用 psa 相关 API。
3) **读取**，启用此选项以允许使用 **GET** API。
4) 写入，启用此选项以允许使用 **GET/PATCH/POST/PUT/DELETE** API。

c. **有效期限** （要求 Gateway v3.28.0），设置 API 应用程序的有效期限。当 API 应用程序过期时，从该 API 应用程序发起的 API 将被阻止。

d. **状态**，允许 API 应用程序使用 Open API。



5. 单击**复制**或**另存为.txt** 将**客户端 ID** 和**客户端密钥**妥善保存，然后单击**确定**。



API 函数

API 使用基于 **OAuth 2.0** 和 **REST** 的身份验证，使用 **JSON** 进行数据通信。

API 速率限制

每个 API 的调用限制为每分钟200次。

API 文档

API 参考

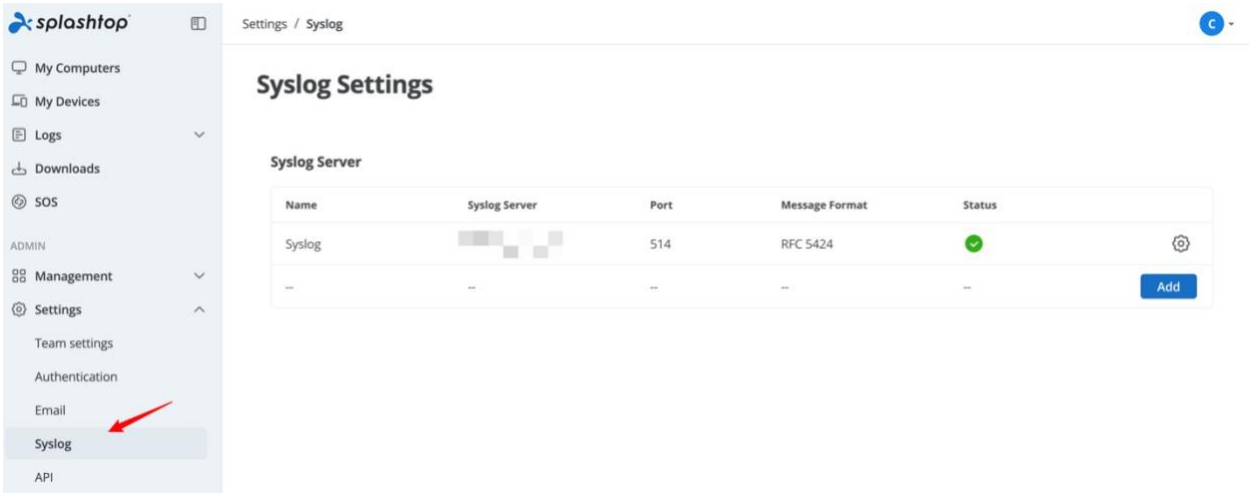
系统日志

除了从网络控制台访问日志外，Splashtop 日志事件还可以发送到本地环境中支持系统日志的 Syslog服务器或 SIEM 工具。Splashtop 事件日志的审计既可以从 Gateway 网络控制台访问，也可以同时下载为 CSV 或 Syslog 收集器。

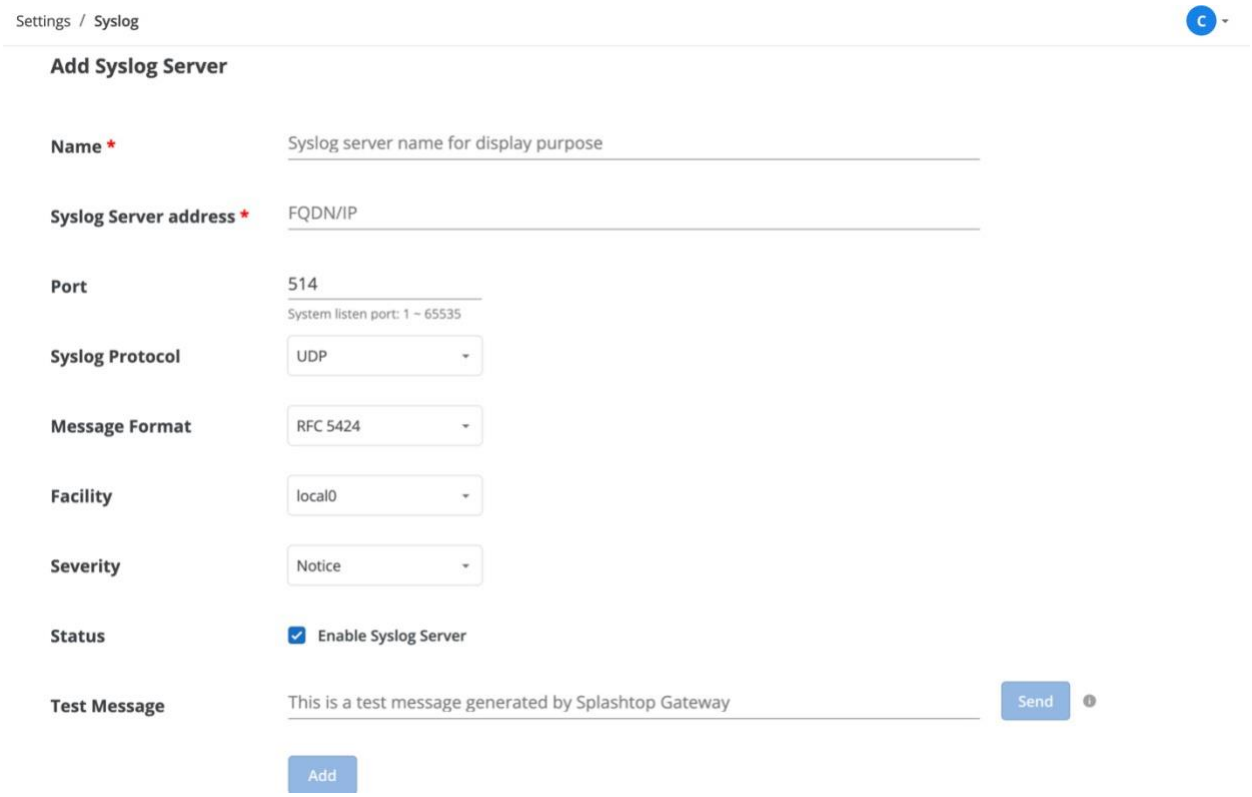
配置

1. 要将 Splashtop Gateway 配置为 Syslog 来源，可以团队所有者身份登录网络控制台，导航到设置 → Syslog。

2. 可以将 Gateway 配置为向最多两个 Syslog 服务器发送系统日志消息。



3. 单击添加以配置目标 Syslog 服务器。

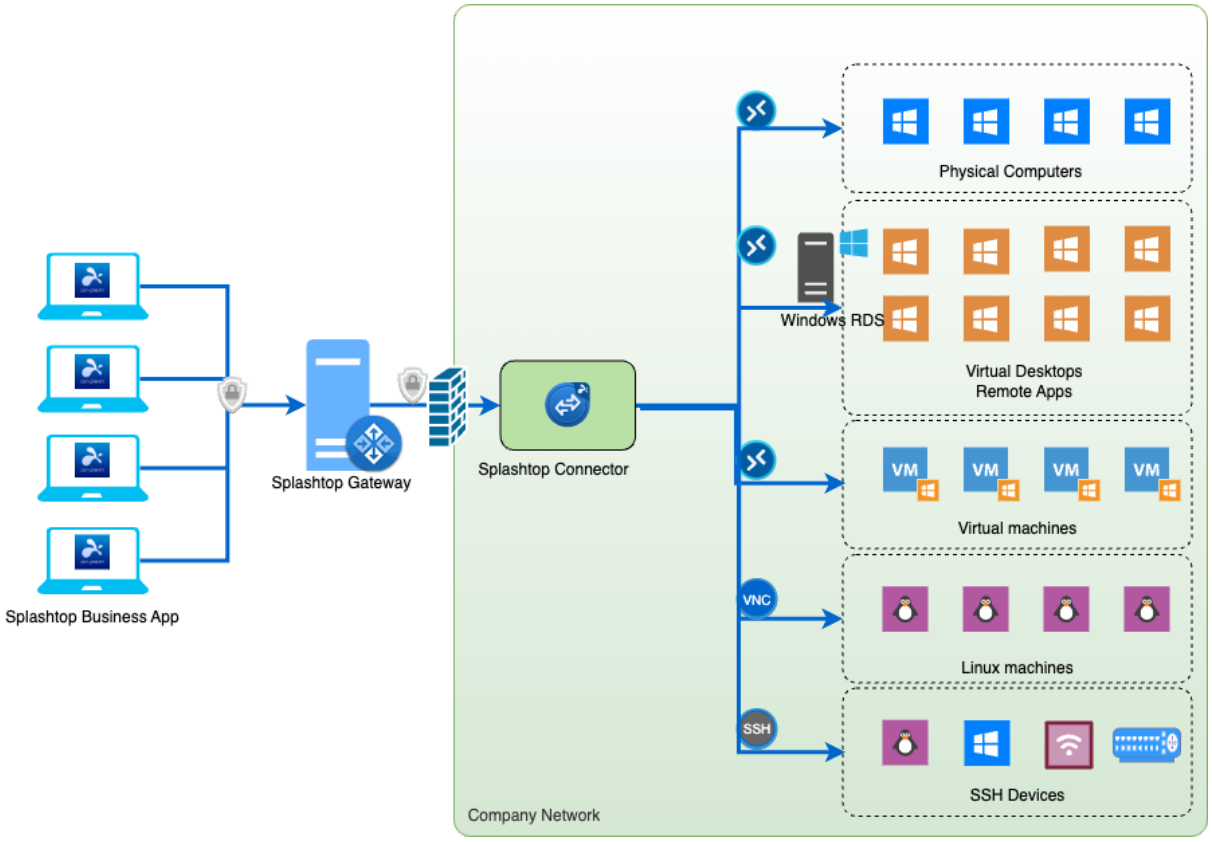


4. 系统日志设置

名称	Splashtop Gateway 中的系统日志主机名
Syslog 服务器地址	输入接收日志消息的 Syslog 服务器的主机名或 IP 地址。
端口	通过 UDP 传输系统日志消息默认使用端口514。默认端口可以更改。
Syslog 协议	支持 UDP 或 TCP。
消息格式	支持 RFC 5424 或 RFC 3164 （BSD）。
设备	从 local0 - local7中选择合适的设备。
严重性	选择适当的 Syslog 严重性。
状态	启用后，Splashtop Gateway 将开始向 Syslog 服务器持续发送系统日志消息。
测试消息	向 Syslog 服务器发送消息以测试上述设置。

Splashtop Connector

Splashtop Connector 允许用户连接电脑和其他设备，支持 RDP/RDS、VNC、SSH 等各种协议，用户可以直接连接到 Splashtop On-Prem 客户端应用程序中的电脑和其他设备，无需使用 VPN 或安装任何远程访问代理。



功能

- 访问 RDP 电脑
- 访问 RDS 服务器
- 访问 Remote 应用程序
- 允许从 Windows、Mac、iOS、Android 上的 Splashtop On-Prem 客户端访问
- 文件复制和粘贴（仅限 Windows）
- 文本复制和粘贴
- 会话录制

- 远程打印
- 多显示器
- IP 白名单/黑名单
- 访问 VNC 电脑
- 访问 SSH 电脑和其他设备

优势

- **简单易用**，IT 管理员可以在 Splashtop Connector 管理界面中预配置 RDP/VNC/SSH 配置文件，用户可以直接访问 RDP/VNC/SSH 资源，就像访问已安装 Splashtop Streamer 的普通 Windows 电脑一样简单。
- **安全性**，Splashtop Connector 将部署在本地网络中，经由本地网络路由到 RDP/VNC/SSH 设备，因此 IT 管理员无需通过网络打开 RDP/VNC/SSH 端口以允许用户访问。Splashtop Connector 模拟 RDP/VNC/SSH 资源并遵循 Splashtop 的访问权限系统，仅具有适当访问权限的用户才能连接到 RDP/VNC/SSH 资源。
- **审计**，使用 Splashtop Connector，所有 RDP/VNC/SSH 连接都会有会话日志记录。Splashtop Connector 还支持视频会话录制。

部署最佳实践

1. 可扩展性

单个 Splashtop 连接器有其同时进行 RDP/VNC/SSH 会话的限制，但您可以在网络中部署多个 Splashtop 连接器以扩展容量。

2. 网络访问

- 部署 Splashtop Connector 的电脑可以访问 Splashtop Gateway，以代理 RDP/VNC/SSH 协议。
- 部署 Splashtop Connector 的电脑应能通过 RDP/VNC/SSH 协议访问 RDP/VNC/SSH 电脑。为了提高安全性，只能通过本地 LAN 访问打开 RDP/VNC/SSH 协议。

3. 安全性

仅向需要访问这些 RDP/VNC/SSH 电脑的用户授予访问权限。

安装

下载 Splashtop Connector 软件

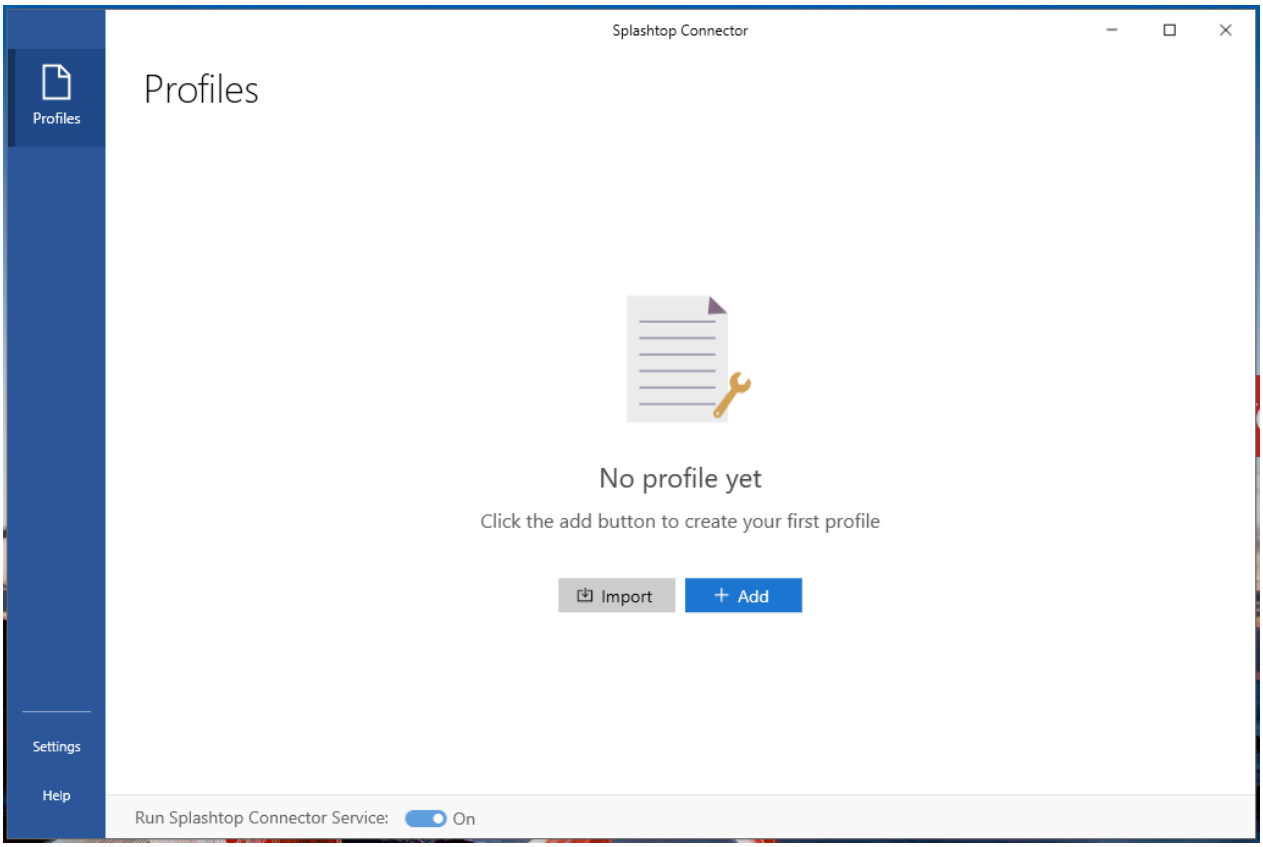
系统要求

- Windows 7、8、10、11，Windows Server 2012、2016、2019（.Net 4或更高版本）
- RAM：8G 或以上
- 存储：50G 或以上
- 网络
    - 可路由到 RDP/VNC/SSH 电脑

安装

运行 Splashtop Connector 安装程序。安装后，则可看到 Splashtop Connector 管理用户界面，如下图所示。请确保**运行 Splashtop Connector 服务器**已**打开**。

现在，可以创建配置文件以启用对 RDP/RDS 电脑的代理。

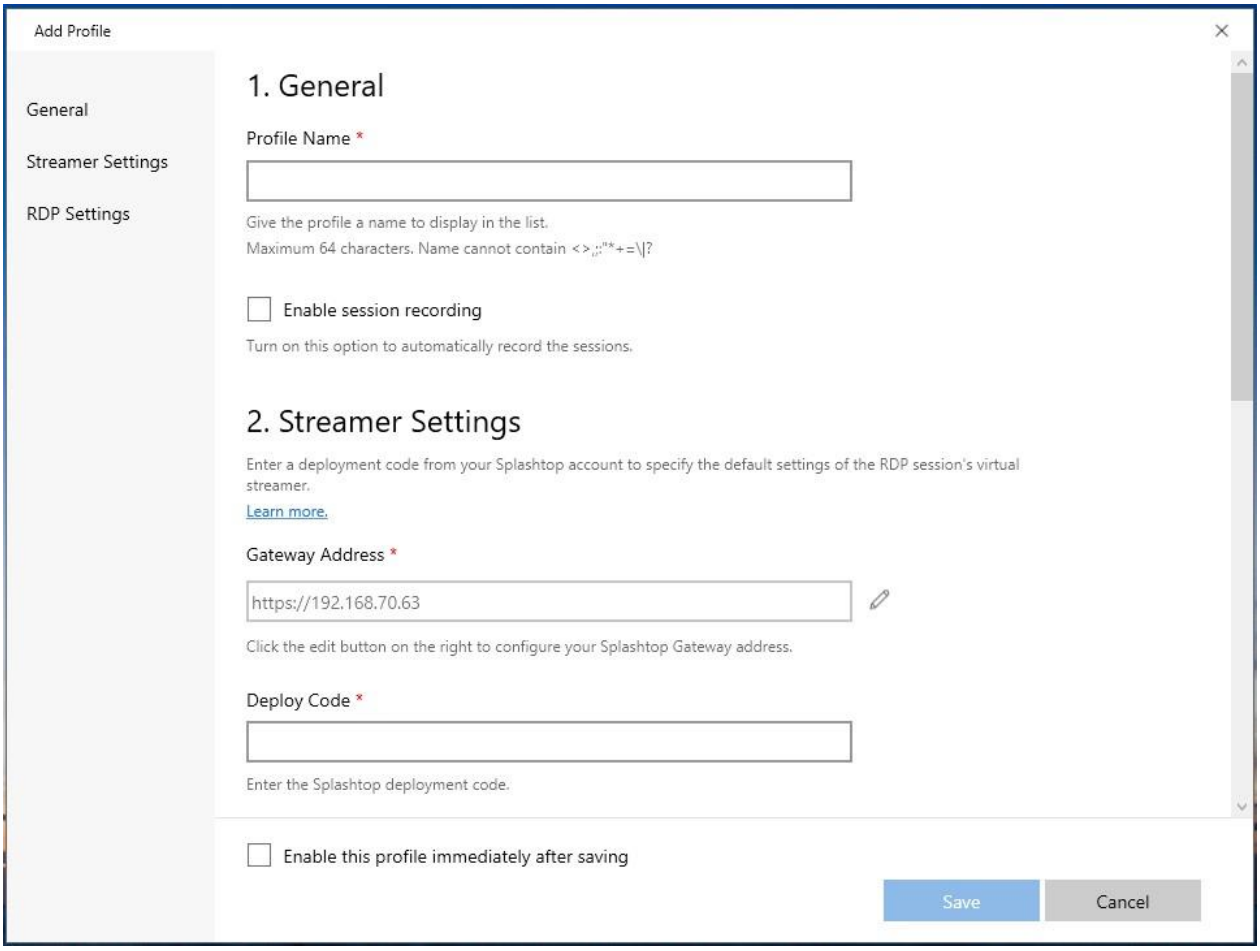


创建 RDP/RDS 配置文件

在 Splashtop Connector 中，RDP 资源可供 Splashtop On-Prem 应用程序通过设置配置文件来访问。配置文件设置由三个部分组成：**通用设置**、**Streamer 设置**和 **RDP 设置**。

可以在 Splashtop Connector 中创建多个配置文件。RDP 资源将计入 Splashtop 团队的电脑总数。

启用配置文件以使 RDP 资源可用于远程访问。



通用设置

- **配置文件名称**，将在 Splashtop On-Prem 客户端应用程序中显示。为配置文件指定名称，让用户清楚地了解 RDP 电脑的用途。
- **启用会话录制**，打开此选项可自动录制 RDP 会话，可以基于单个配置文件进行设置。录制内容将保存在 Splashtop Connector 电脑的指定路径。

Streamer 设置

- **Gateway 地址**，Splashtop Connector 将限制为一个Gateway。用户需要在设置页面配置 Gateway 地址。只能保存已验证的 Gateway 地址。

- **部署码**，Splashtop 使用部署套件确定 RDP 资源的默认电脑组和访问权限。请参阅此文以了解如何创建部署套件。创建后，在此字段中输入**部署码**。

RDP 设置

- **模式**，Splashtop Connector 支持用于单台电脑的 RDP，也支持作为虚拟桌面的 RDS。RDS 将需要 Windows Server 和 RDS 许可证。
- **池规模**，选择 RDS 则可设置资源池规模，即能够同时连接到 RDS 虚拟桌面的用户数量。池规模将影响 Splashtop 团队中的电脑总数。
- **远程电脑**，可以预先配置远程电脑的 IP/DNS，或在连接到电脑时要求用户输入此信息。
  - **要求用户指定要连接的远程电脑**，可用于提供临时支持
  - **具有指定信息的固定远程电脑**，用于连接特定电脑
  - 登录凭据
    - **要求用户使用 Windows 用户名和密码登录**，用户需要输入远程电脑的登录凭据才能连接
    - **固定用户名和密码**，用户可以使用预先配置的用户名和密码连接到远程电脑
- **在远程应用程序模式下运行**，如果已在 RDS 服务器上配置并发布远程应用程序，则可以让会话在远程应用程序模式下运行。打开此选项可为远程应用程序设置更多设置
  - Remote 应用程序别名或 Remote 应用程序完整路径，具体取决于您的选择。
  - 可选的远程应用程序参数，可在 RDS 服务器上启用远程应用程序参数支持。
- **色深**，选择颜色深度。
- **音频播放**，选择音频播放选项。
- **键盘布局**，选择键盘布局或在预设列表中添加不存在的键盘布局。

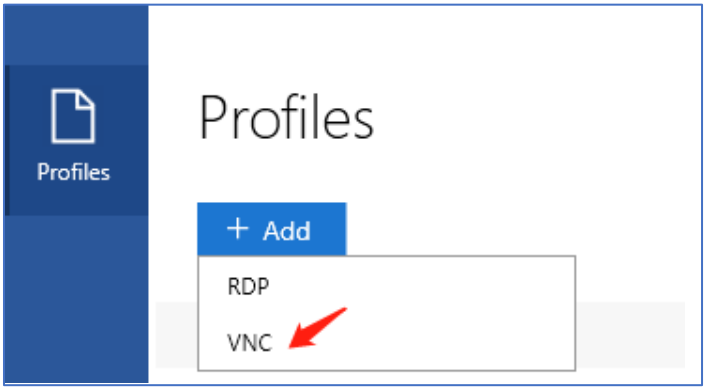
可以通过点击**保存后立即启用此配置文件**来立即启用此配置文件，或可在主窗口中启用。

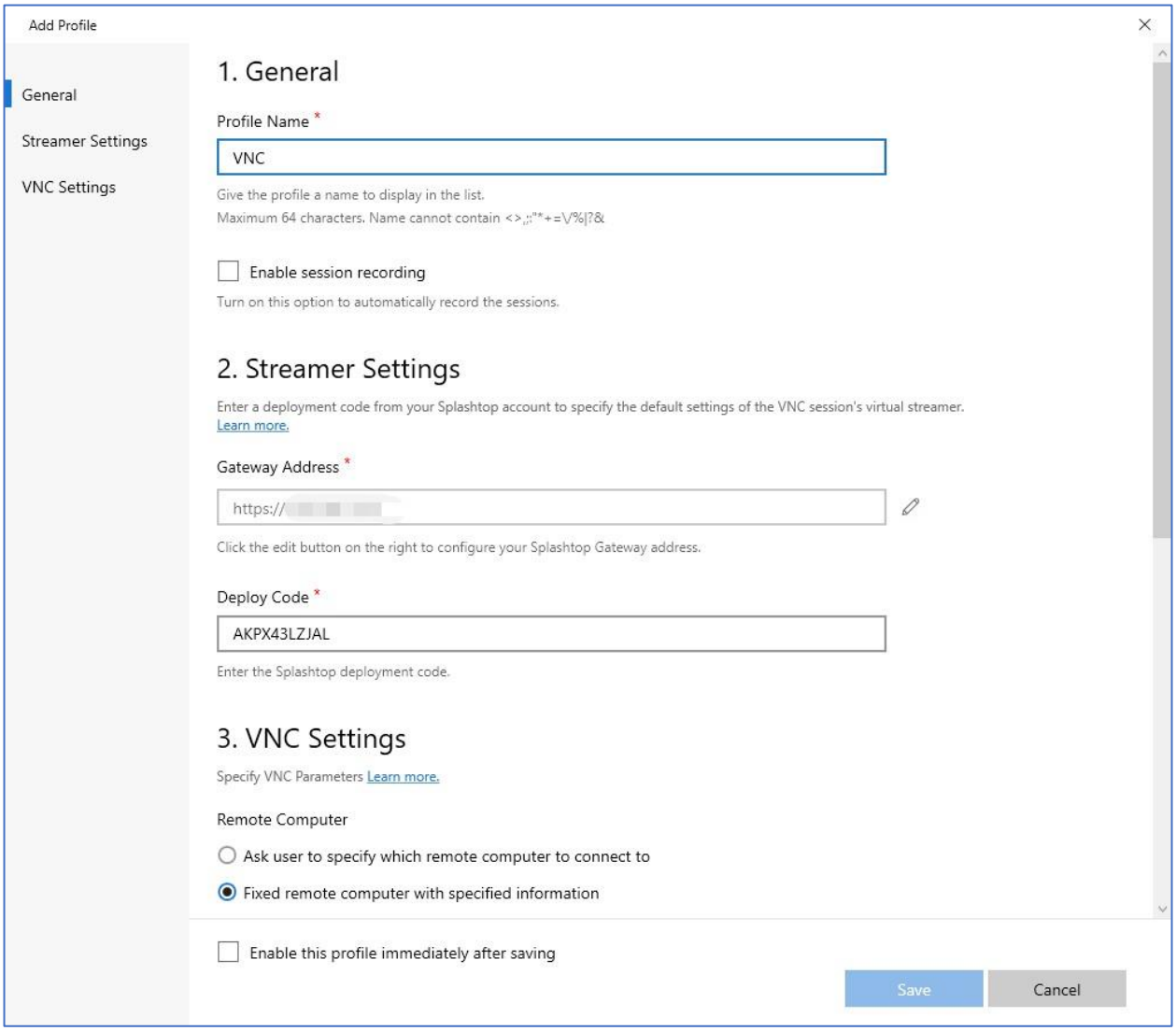
创建 VNC 配置文件

在 Splashtop Connector 中，可通过设置配置文件使 Splashtop On-Prem 应用程序能够访问 VNC 资源。配置文件设置由三个部分组成：**通用设置**、**Streamer 设置**和 **VNC 设置**。

可以在 Splashtop Connector 中创建多个配置文件。VNC 资源将计入 Splashtop 团队中的电脑总数。

启用配置文件以使 VNC 资源可用于远程访问。





通用设置

- **配置文件名称**，将在 Splashtop On-Prem 客户端应用程序中显示。为配置文件指定名称，让用户清楚地了解 VNC 电脑的用途。
- **启用会话录制**，启用此选项可自动录制此资源的会话。录制内容将保存在 Splashtop Connector 电脑的指定路径（详见 *设置 - >通用*）

Streamer 设置

- **部署码**，输入 Splashtop 部署码以确定 VNC 资源的默认电脑组和访问权限。请参阅此文以了解如何创建部署套件。创建后，在此字段中输入部署码。

VNC 设置

- **远程电脑**，可以预先配置远程电脑的 IP/DNS，或在连接到电脑时要求用户输入此信息。
  - **要求用户指定要连接的远程电脑**，要求用户在连接时输入 SSH 电脑的 IP/主机名。可用于临时支持。
    - **启用 IP 限制配置**，可以指定目标 VNC 电脑的白名单/黑名单
  - **具有指定信息的固定电脑**，允许 IT 管理员预配置 VNC 电脑的特定 IP/主机名和端口。
- 登录凭据
  - **连接会话时要求用户登录**，用户需要输入远程电脑的 VNC 密码才能连接
  - **固定密码**，用户可以使用预先配置的 VNC 密码连接到远程电脑

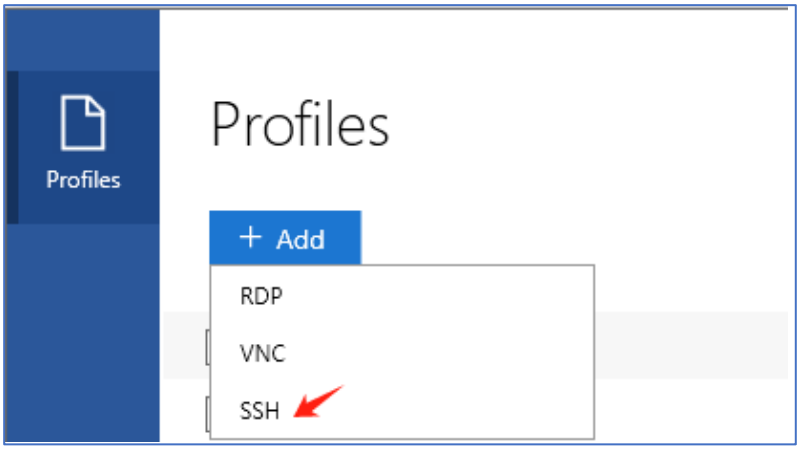
可以通过点击**保存后立即启用此配置文件**来立即启用此配置文件，或可在主窗口中启用。

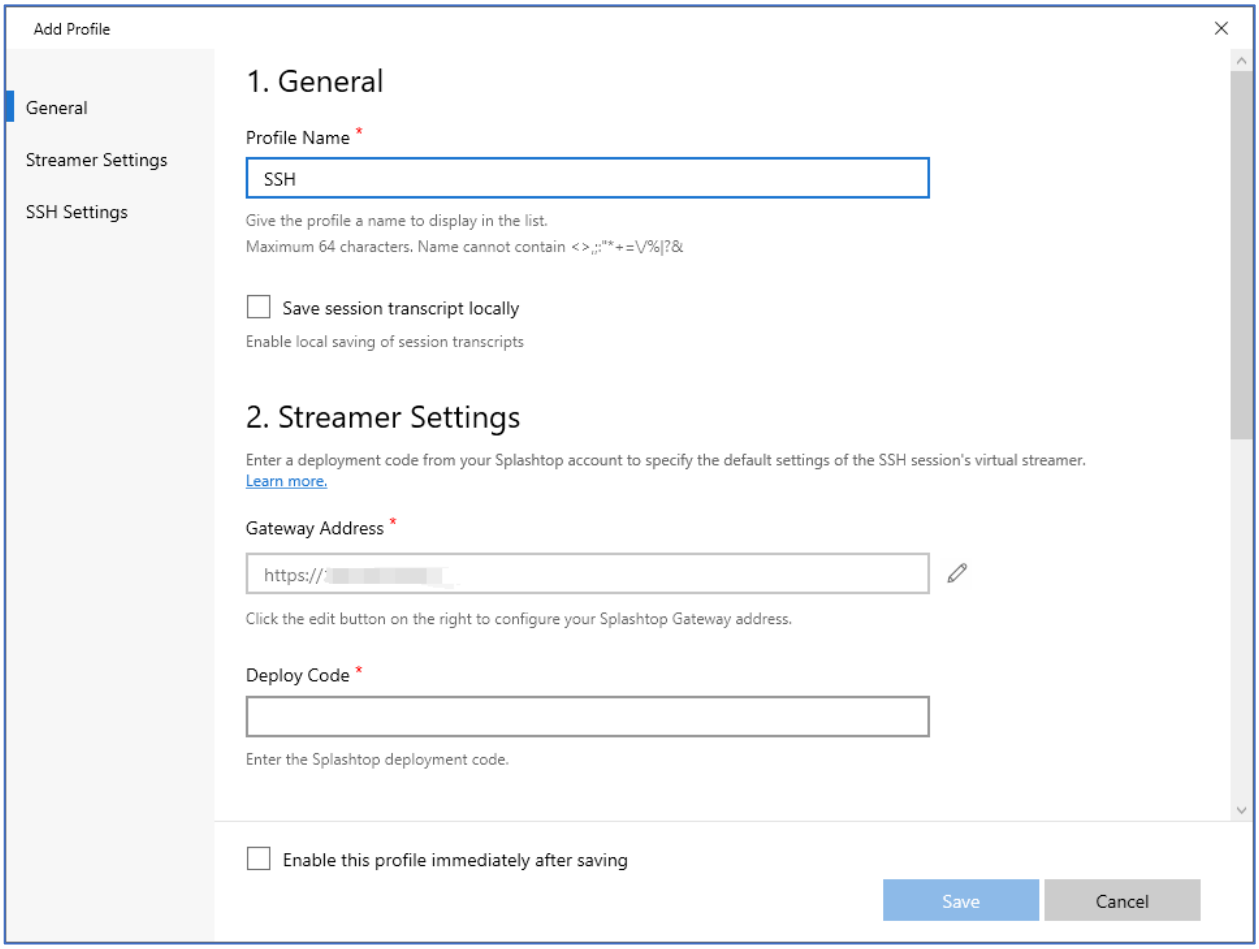
创建 SSH 配置文件

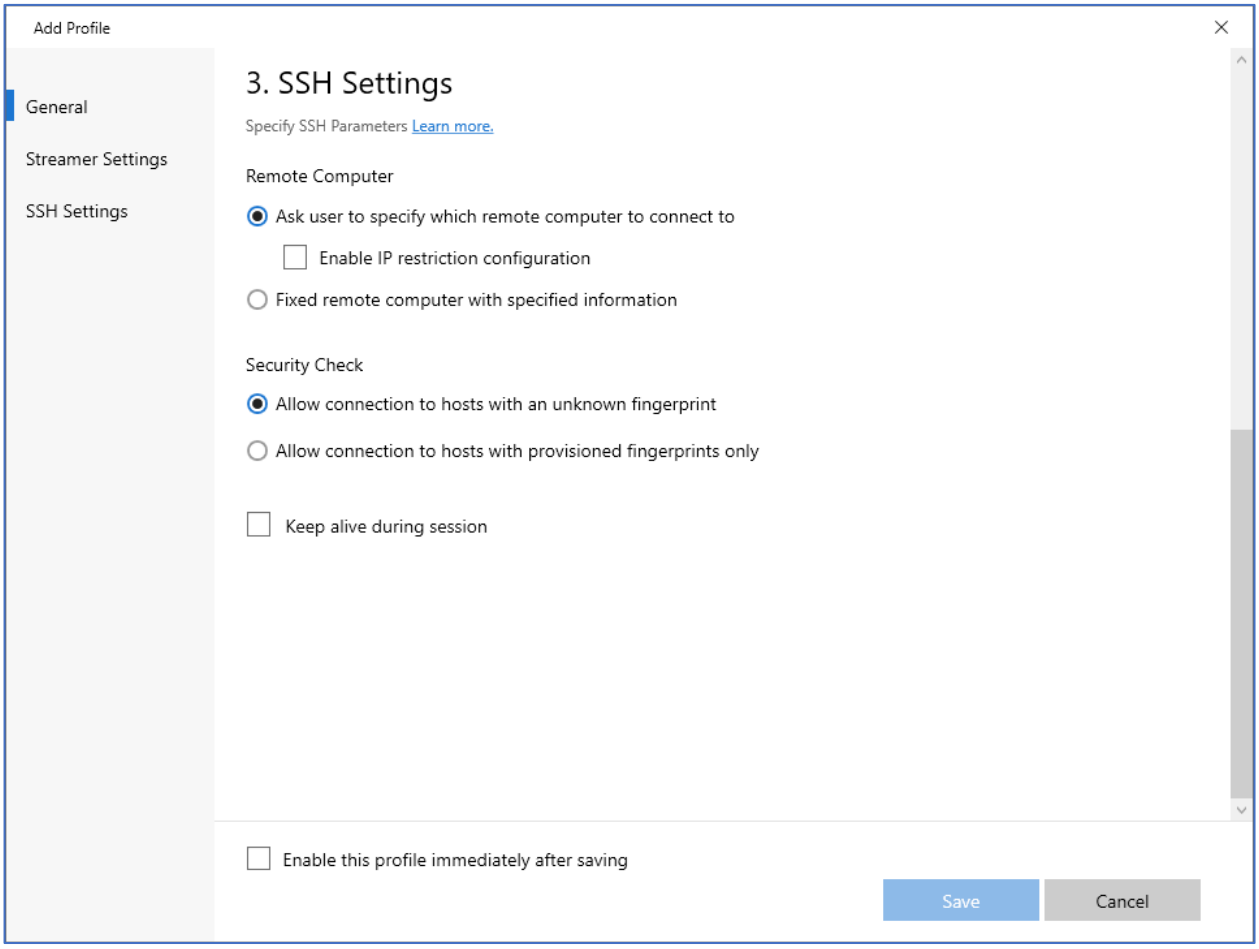
从 Splashtop Connector v1.1.8.4 开始，Splashtop On-Prem 应用程序可以通过设置配置文件来访问 SSH 资源。配置文件设置由三个部分组成：**通用设置**、**Streamer 设置**和 **SSH 设置**。

可以在 Splashtop Connector 中创建多个配置文件。这些 SSH 资源将计入 Splashtop 团队中的电脑总数。

启用配置文件以使 SSH 资源可用于 SSH 访问。







通用设置

- **配置文件名称**，将在 Splashtop On-Prem 客户端应用程序中显示。为配置文件指定名称，让用户清楚地了解 SSH 电脑的用途。
- **在本地保存会话记录，启用此选项可自动为此资源保存会话记录**，可以在个人配置文件的基础上设置。录制内容将保存在 Splashtop Connector 电脑的指定路径。

Streamer 设置

- **部署码**，输入 Splashtop 部署码以确定 SSH 资源的默认电脑组和访问权限。详见此文，以了解如何创建部署套件。创建后，在此字段中输入部署码。

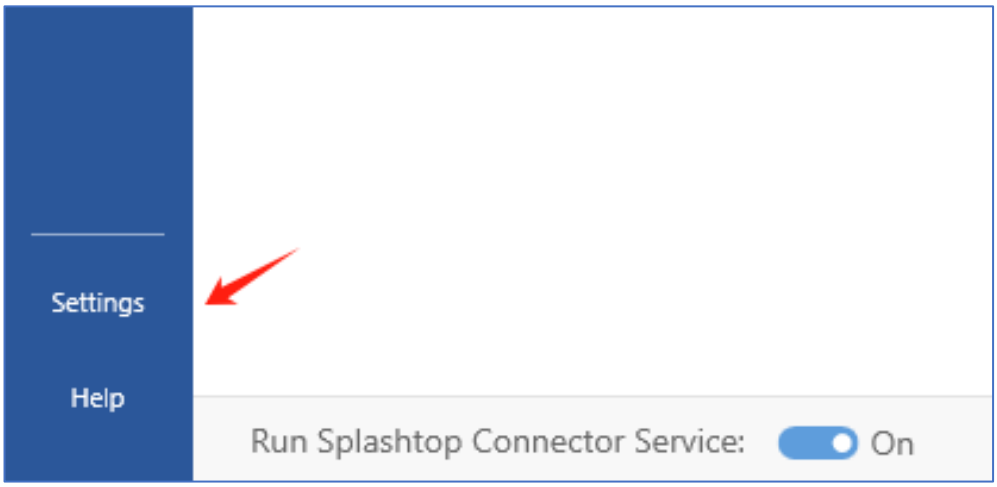
SSH 设置

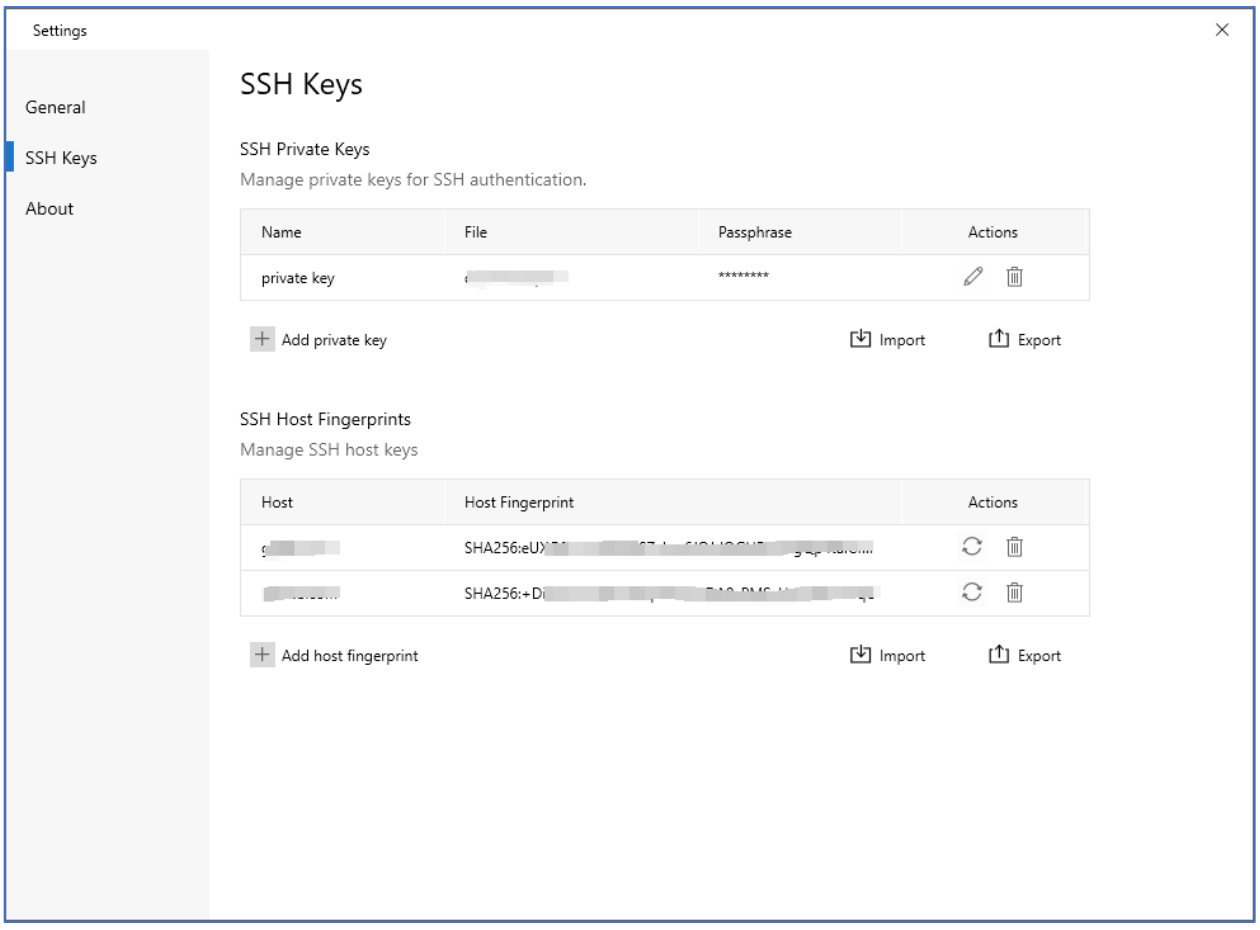
- **远程电脑**，可以预先配置远程电脑的 IP/DNS，或在连接到电脑时要求用户输入此信息。
  - **要求用户指定要连接的远程电脑**，要求用户在连接时输入 SSH 电脑的 IP/主机名。可用于临时支持。
    - **启用 IP 限制配置**，可以指定目标 SSH 电脑的白名单/黑名单。
  - **具有指定信息的固定电脑**，允许 IT 管理员预配置 SSH 电脑的特定 IP/主机名和端口。
    - **使用预设公钥身份验证**，可以打开公钥身份验证并选择预配置的私钥，以替代密码身份验证。
- 安全检查
  - **允许连接到指纹未知的主机**，用户可以连接到具有未知 SSH 主机指纹的 SSH 电脑。成功连接到 SSH 服务器后，该指纹将自动添加到 SSH 密钥中的 SSH 主机指纹中。
  - **允许使用预置指纹连接到主机**，用户只能使用 SSH 密钥中预配置的 SSH 主机指纹连接到 SSH 电脑。

可以启用**保存后立即启用此配置文件**选项或可在主窗口中立即启用此配置文件。

SSH 密钥

此外，可以导航到到*设置 - > SSH 密钥*来管理 Splashtop Connector 中的**私钥**和 **SSH 主机指纹**。





- **SSH 私钥**，允许 IT 管理员通过手动添加或导入来配置用于 SSH 身份验证的私钥。

- **SSH 主机指纹**，允许 IT 管理员通过手动添加或导入来配置 SSH 主机指纹。

可以访问在线支持门户网站获取更多有用资源。

支持资源

关于本文档

本文档仅供参考。Splashtop Inc 可能会更改本协议的内容，恕不另行通知。本文件不保证无任何错误，也不附带任何其他明示或默示的保证或条件，包括适销性或适用于特定目的的默示保证和条件。

关于 Splashtop On-Prem

Splashtop On-Prem 是一个本地化解决方案，可以在企业网络内自托管。借助集中式数据库和管理控制台，IT 管理员可以轻松解决系统安全问题，同时为用户提供流畅的远程控制体验。

产品网址： https://www.splashtop.com/on-prem

技术支持

Splashtop 致力于为客户提供卓越的技术支持。正在寻找更多支持资源？

帮助网站： https://support-splashtoponprem.splashtop.com/
联系我们： support-onprem@splashtop.com