Amia Networks 简和网络

Secure WAN 管理员

用户使用手册

版本号：V25.8.0

简和网络科技（南京）有限公司

2025 年 8 月

目　录

1. 前言

1.1 产品简介

Secure WAN （以下简称 SWAN）是致力于探索全密化趋势下一站式安全广域网系统性解决方案，它集成了云原生+微服务、网络智能态安全保障、自适应微隔离零信任体系以及安全网络一体化等五大特色技术，旨在为用户提供全面、高效、安全的网络连接服务。可定制适用于个人用户安全升级、企业组网与云网融合、面向运营商与骨干网的一体化下一代 SD-WAN&SASE 方案，确保用户的数据安全和网络性能。

1.2 产品架构

SWAN 产品包含三大核心功能模块组件，分别承担不同的功能和角色：

- **Manager/安全广域网络一体化管控平台**：作为一体化统一管控中心，Manager 提供便捷的管理界面，使管理员能够高效地进行虚拟网络管理、用户管理、服务节点管理以及安全策略配置等操作。这一模块是 SWAN 系统的中枢，确保所有网络组件的协同工作和统一管理。
- **Servicenode/安全广域网络接入服务节点:** Servicenode 模块负责提供网络接入服务，确保用户能够稳定、安全地接入网络。
- **Client/安全广域网络接入客户端:** Client 客户端是用户接入 SWAN 网络的入口，用户通过 Client 客户端可以方便地接入服务节点，获取相应的服务资源。Client 客户端支持多种操作系统，提供友好的用户界面和便捷的操作方式，使用户能够轻松实现网络连接和资源共享。

1.3 使用说明

该用户使用手册专为 SWAN 产品的 V25.8.0 版本编制，请确保您已从官方指定网站下载并安装了对应版本的软件，以确保所有功能和指南的准确适用性。

SWAN 作为一款高性能、安全、易用的广域网解决方案，其设计初衷是为了满足各类用户群体的需求，从专业的 IT 运维人员到普通的网络使用者，都能从

中找到适合自己的使用方式：

- **IT 运维管理人员**：通过 Manager 安全广域网络一体化管控平台，轻松实现虚拟网络、用户、服务节点以及安全策略的一体化管理。管理员可以利用平台提供的日志审计监控功能，对网络状态进行全天候监控，及时发现并处理潜在的网络问题。
- **普通用户**：用户只需通过 Client 客户端，即可轻松接入 SWAN 网络，享受安全、稳定的网络连接服务。用户无需具备专业的网络知识，只需按照客户端的提示进行简单设置，即可实现网络的快速接入。

2. 系统安装与配置

2.1 准备网络环境

Manager 作为整个 SWAN 分布式系统的管理中心，需要确保所有的 Servicenode 节点与 Client 节点均能正常访问与连接，同时需要对状态信息以及用户等信息进行存储与管理，因此在安装部署前需根据您的实际网络环境进行配置，确保 SWAN 系统能够与其他网络设备进行通信：

若您在内网环境内中部署使用 Manager，那么请确认目标的 Servicenode 与 Client 能够通过局域网正常访问到这台机器的指定 Port 即可。

如您想要建立通过公网地址访问的服务，请确保公网地址正确、端口映射关系正确以及网络防火墙对指定端口的放行。

Manager 需要开放的端口如下：7926 默认监听端口（用于和客户端通信）、12762 默认监听端口（用于和 Servicenode 通信）和 12760 默认网页服务端口（用于提供可视化管理服务）。

Servicenode 需要开放自定义的服务端口，确保客户端能顺利通过这些端口与服务节点建立连接。

2.2 首次使用引导配置

Manager 设备部署完成后，由工程师根据网络情况进行设备 IP 配置，通过 http://<ip>:12760/service/swan/login，即可进入 Manager 端进行配置管理。当您首

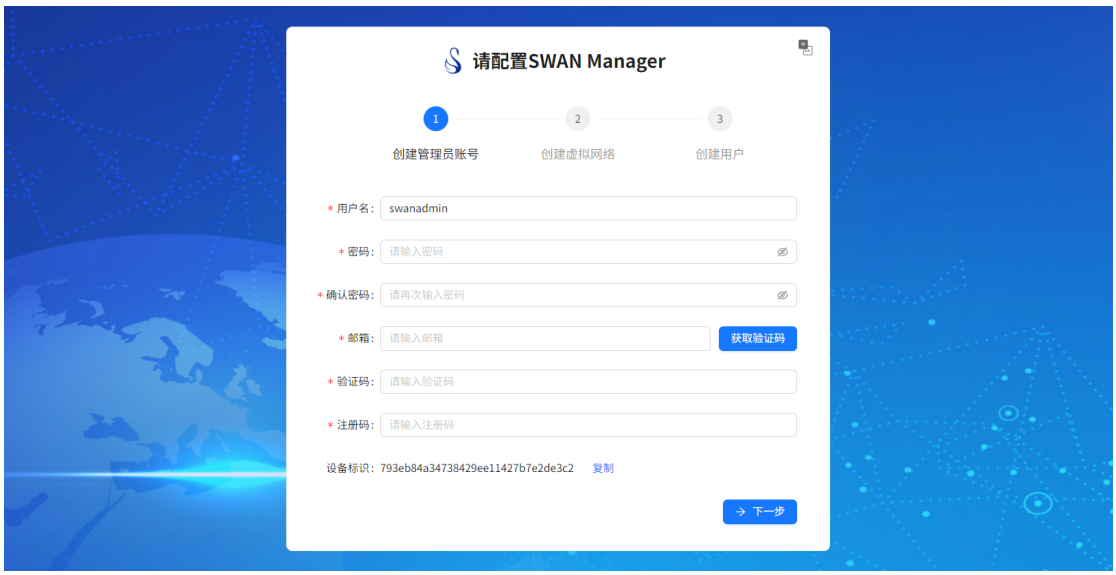
次访问 Manager（安全广域网络一体化管控平台）时，系统将自动跳转至安装引导页，引导页将一步步指导您完成 Manager 的相关配置。

2.2.1 创建管理员账号

在安装引导页上，您将看到一个用于创建管理员账号的表单。请按照页面提示，输入管理员的用户名、密码以及确认密码。同时确保密码强度足够，包含字母、数字和特殊字符的组合，以提高账户安全性。同时需绑定管理员的邮箱信息，以方便找回管理员账号密码。

SWAN 管理员按照权限等级分为两种：Network Admin 和 Servicenode Admin：Network Admin 具备网络、用户、服务节点、日志、系统配置等全部管理权限，能够全面管理 SWAN 网络；Servicenode Admin 则只能进行服务节点的管理，权限相对有限。在此处创建的管理员账号默认为 Network Admin，拥有最高级别的管理权限。

关于注册码，工程师将依据设备标识码为您生成专属的产品注册码，进行产品激活验证操作。在激活过程中，必须确保 Manager 机器处于联网状态，系统会对所输入注册码的有效性进行严格验证，若验证通过，Manager 的全部功能将正式启用。



2.2.2 创建虚拟网络

虚拟网络是一种基于软件定义的网络技术架构，是 SWAN 构建的一张互联互通的子网，允许处于不同地域不同子网的 SWAN Servicenode 加入其中，实现

对不同访问资源的灵活调度与管控。

对于 Client 客户端而言，用户无需直接感知底层服务节点的物理部署细节，只需加入该虚拟网络中的任意一个 Servicenode，即可触发代理机制自动完成路由决策，就能便捷地访问到该 Servicenode 所代理的网络资源。这种设计不仅简化了客户端 Client 的接入流程，还极大地提升了资源访问的灵活性和效率。

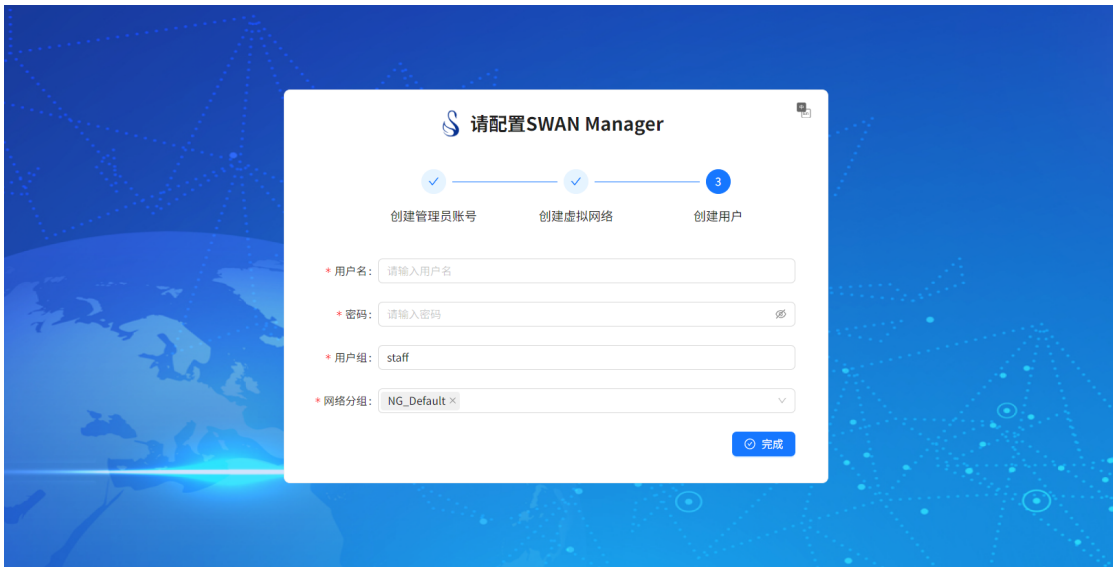
为了更好地管理和组织虚拟网络，SWAN 引入了虚拟网络分组的概念。用户可以创建一个或多个分组，并将虚拟网络划分到相应的分组中。

一个网络分组具备容纳多个虚拟网络的能力，即允许将多个虚拟网络纳入同一个网络分组进行统一管理；但是每个虚拟网络仅能被加入到一个特定的网络分组中，无法同时隶属于多个网络分组，避免因多分组策略叠加导致网络冲突的同时，还可以使权限映射关系更清晰，管理员可精准定义"用户组→网络分组→虚拟网络"的三级授权链路。

这种分组管理方式不仅使虚拟网络的管理更加有序和高效，还为后续的权限管理提供了极大的便利，虚拟网络分组可以与用户分组进行关联，从而实现精细化的权限控制。

2.2.3 创建普通用户

区别于管理员，普通用户是用于登录客户端 SWAN Client 的账号类型，客户端安装完毕后，使用普通用户的账户即可登录客户端系统，并选择加入所需的虚拟网络，轻松访问网络资源。



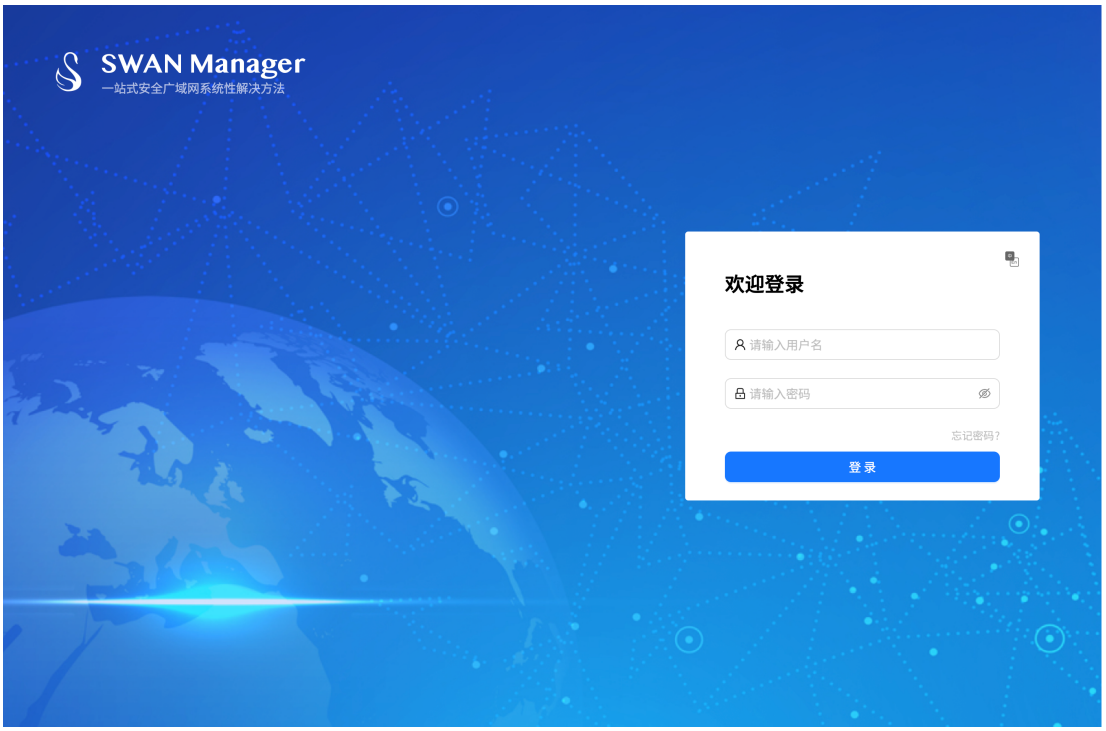
完成上述引导流程会即可进入正常 Manager 管理页面。

3. SWAN Manager 配置与使用

3.1 账户与密码

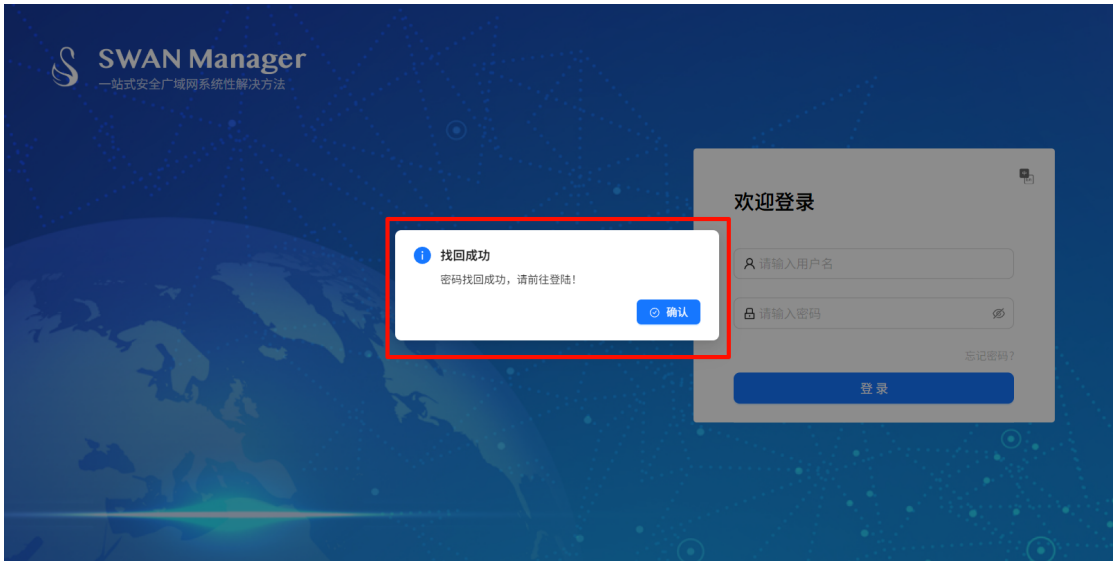
3.1.1 管理员登录

完成 SWAN Manager 引导配置后，点击“完成”按钮或浏览器输入打开页面：http://<ip>:12760/service/swan/login，即可进入 Manager 管控平台登录页面，使用您在引导流程中创建的管理员账号即可成功登录管控平台。



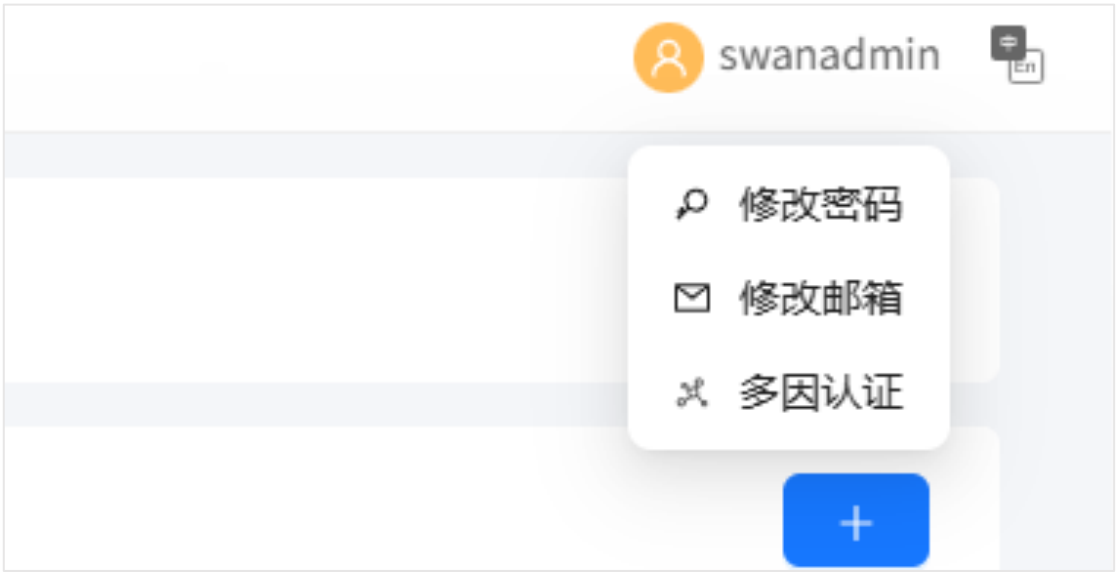
3.1.2 忘记密码

若您遗忘管理员配置的密码，可点击“忘记密码”，通过安全邮箱接收验证码后重新设置密码。如未设置安全邮箱或操作过程中遇到问题，请联系我们，我们将协助您完成密码重置。



3.1.3 用户信息修改

将鼠标悬停于右上角用户栏，即可显示“修改密码”与“修改邮箱”按钮。点击对应按钮后，按照页面提示步骤操作，即可完成用户信息修改。



修改密码：

修改邮箱：

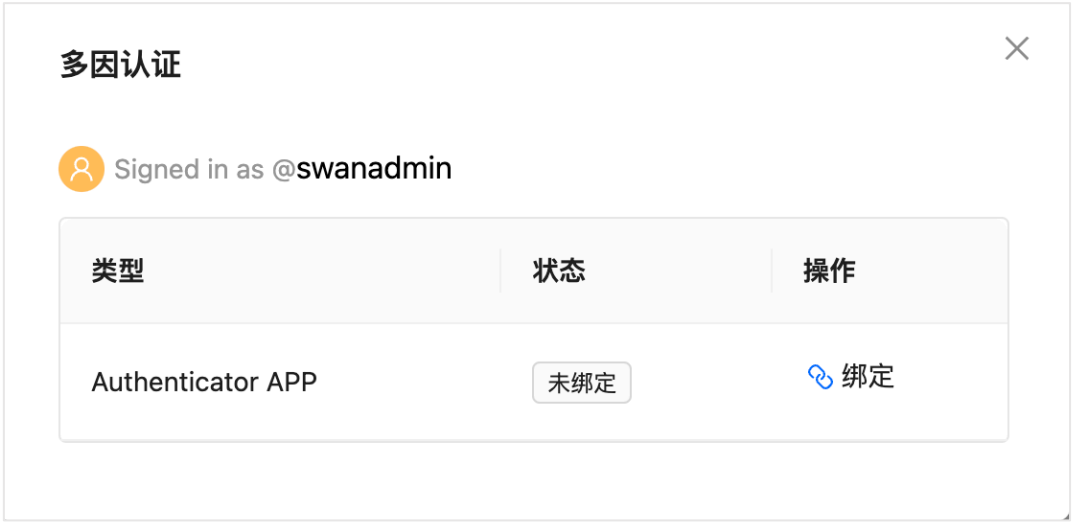
3.1.4 多因认证

SWAN 系统提供高度灵活的多因子认证（MFA）配置功能，通过增设额外的身份验证环节，可显著提升用户账户的安全性。您可按照以下步骤进行设置：

将鼠标悬停于右上角用户栏，点击弹出的“多因认证”按钮即可进入设置界

面。

目前，系统支持基于 TOTP Authenticator 的多因子认证方式。具体操作为：在手机端安装兼容的 Authenticator 应用（如谷歌验证器、微软验证器或其他 TOTP 标准验证工具），扫描系统生成的二维码完成绑定。绑定后，每次登录 SWAN 系统时，系统将触发二次验证流程，进一步保障账户安全。



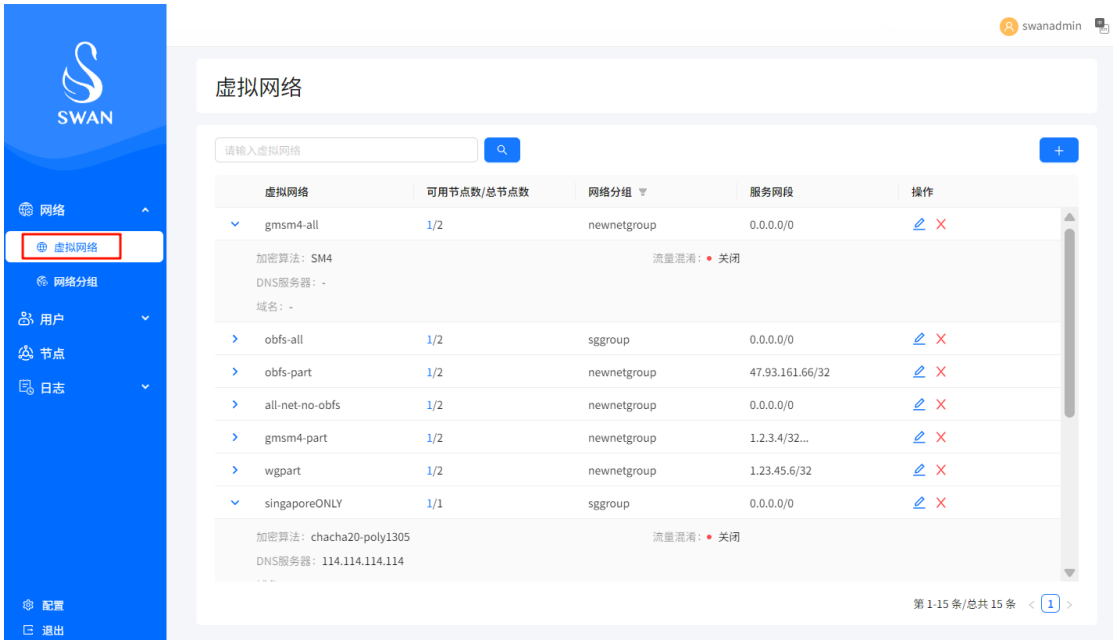
3.2 网络

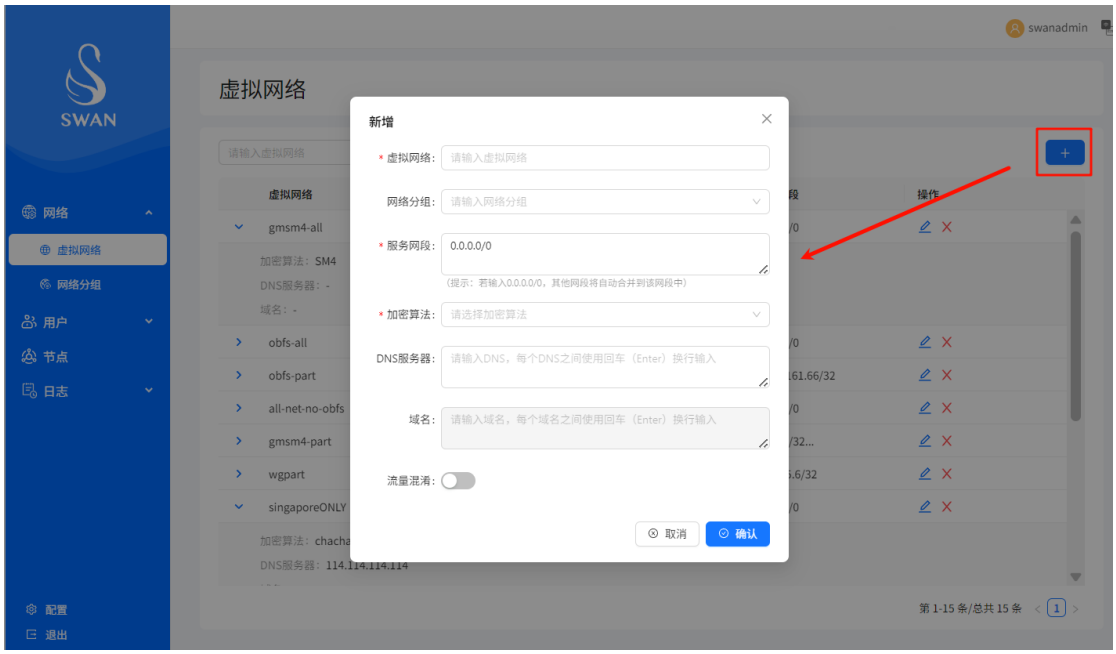
3.2.1 虚拟网络管理

在 SWAN 系统的操作界面中，用户可通过左侧导航栏快速访问虚拟网络管理功能。具体路径为：依次点击【网络】-【虚拟网络】，系统将跳转至虚拟网络管理页面。

在该管理页面中，用户可直观查看当前已配置的所有虚拟网络信息列表。列表呈现的关键字段包括：虚拟网络的自定义名称标识、关联服务节点的资源使用情况（以"可用节点数/总结点数"的占比形式展示）、所属网络分组名称，以及该虚拟网络预先定义的服务网段范围。

用户可通过点击列表中的任意虚拟网络项，展开查看其详细配置信息，包括：当前配置的加密算法类型、流量混淆功能的启用状态、已配置的 DNS 服务器地址及其关联的域名。此外，该页面还提供便捷的虚拟网络创建与删除操作入口，用户可根据实际需求灵活调整虚拟网络配置。





1）虚拟网络

- 配置说明：为了方便管理和识别虚拟网络，系统允许管理员为虚拟网络进行自定义命名。
- 注意事项：支持输入 2-16 位字符（中文、字母、数字、!、@、$、_、-、.），确保命名的简洁性和易读性。

2）网络分组

- 配置说明：支持用户将当前选中的虚拟网络快速绑定至指定网络分组，实现虚拟网络与网络分组的快速映射关系建立。
- 注意事项：一个网络分组可容纳多个虚拟网络，即支持将多个虚拟网络纳入同一网络分组进行统一管理；但每个虚拟网络仅能归属于一个特定的网络分组，不可同时隶属于多个网络分组。

3）服务网段

- 配置说明：虚拟网络创建时需明确配置该虚拟网络需要代理的全部服务网段，服务网段代表了当前虚拟网络所代理的网络服务资源（例如同时指定 172.171.0.0/16 和 192.168.0.0/16）。此步骤将一次性确定该虚拟网络可访问的完整网络范围。
- 注意事项：若您当前虚拟网络包含多个服务网段，请以换行进行配

置；若在服务网段配置项中输入 0.0.0.0/0（即全零子网掩码的默认路由表示形式），系统将自动判定为启用全代理模式，在此模式下，用户配置的其他所有服务网段参数均会被系统自动合并至 0.0.0.0/0 网段范围内。

4）加密算法

- 配置说明：加密算法用于保障数据传输的安全性。系统当前提供了两种加密算法供用户选择：

  -标准加密算法 chacha20-poly1305：属于国际标准加密算法，具备出色的性能优势，是兼顾安全性与传输效率的首选。

  -国密加密算法 SM4：使用国密算法体系，安全可靠，更适用于政务、金融等对安全性有更高要求的场景。

- 注意事项：当前国密加密算法的兼容性存在平台限制，仅适用于 Linux 系统下的 APP/CLI 客户端版本。对于 Windows、MacOS、iOS 及 Android 等操作系统的客户端，系统暂未提供国密算法支持。若用户已在虚拟网络配置中启用国密加密功能，则上述非 Linux 平台客户端将无法正常连接此虚拟网络。

5）DNS 服务器与域名

- 配置说明：允许用户在虚拟网络中配置内网 DNS 服务器地址和特定的内网域名。客户端接入虚拟网络后，访问这些内网域名时能够自动在配置的内网 DNS 服务器中进行轮询匹配，从而实现对私有网络资源的灵活访问。
- 注意事项：确保配置的 DNS 服务器地址是可达且可靠的，以避免域名解析失败导致网络异常。

6）流量混淆

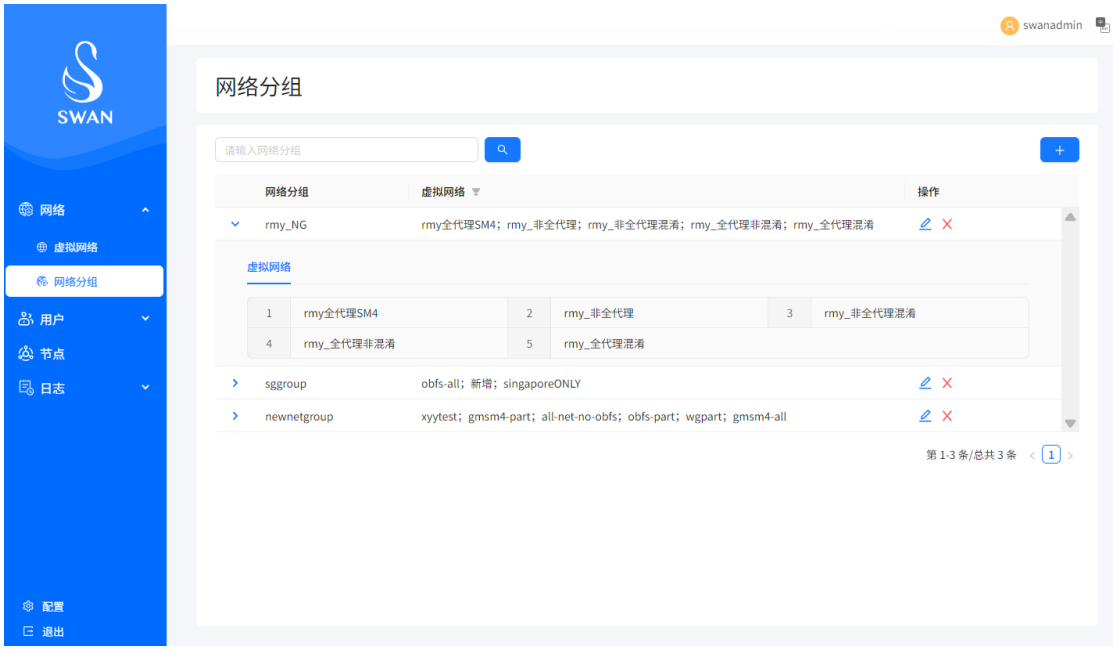
- 配置说明：流量混淆功能采用先进的协议伪装技术，能够将 UDP 流量巧妙地混淆并伪装成 TCP 流量，从而有效防止被恶意拦截和识别，增强隐私保护。
- 注意事项：当前仅 Linux（CLI/GUI）、MacOS（dmg 文件安装）、Windows 客户端支持流量混淆功能；MacOS（APP Store 下载）、iOS、Android 客户端暂不支持该功能，若虚拟网络配置中已启用流量混淆功能，上述暂不

支持该功能的客户端将无法正常连接此虚拟网络。

3.2.2 虚拟网络分组管理

在 SWAN 系统的左侧导航栏，点击【网络-虚拟网络分组】即可进入虚拟网络分组管理页面。在此页面，您可以方便地创建、删除及管理虚拟网络分组。

虚拟网络分组的设计旨在简化权限管控流程。通过用户组与虚拟网络组的映射关系，您可以精确地管理用户可访问的网络资源权限，确保网络资源的安全与合规使用。

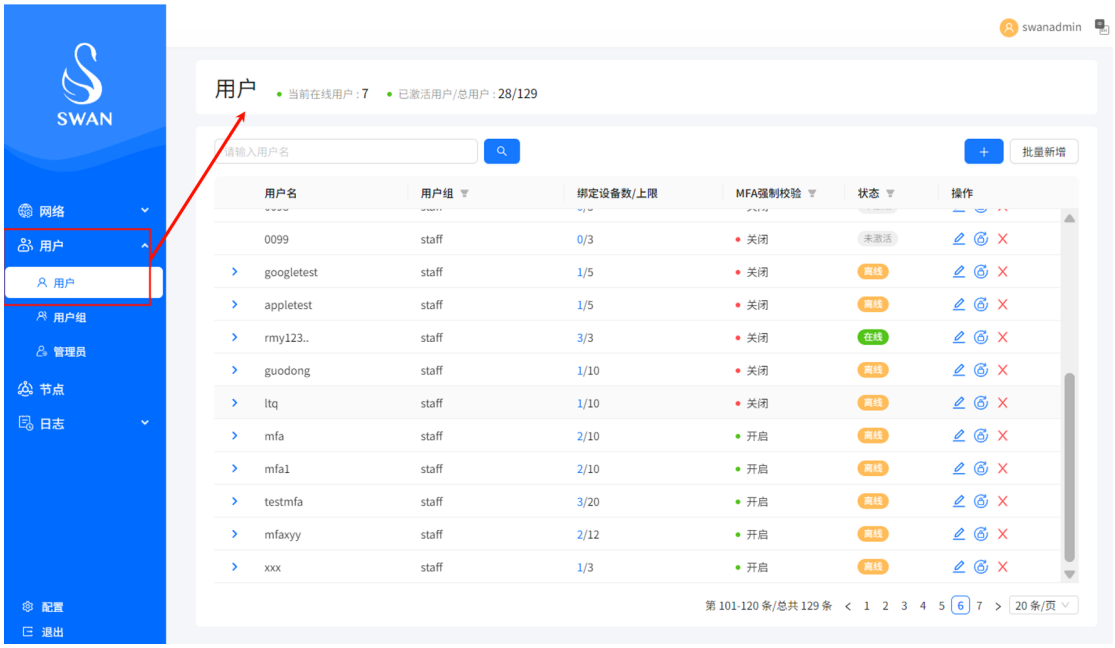


3.3 用户

3.3.1 普通用户管理

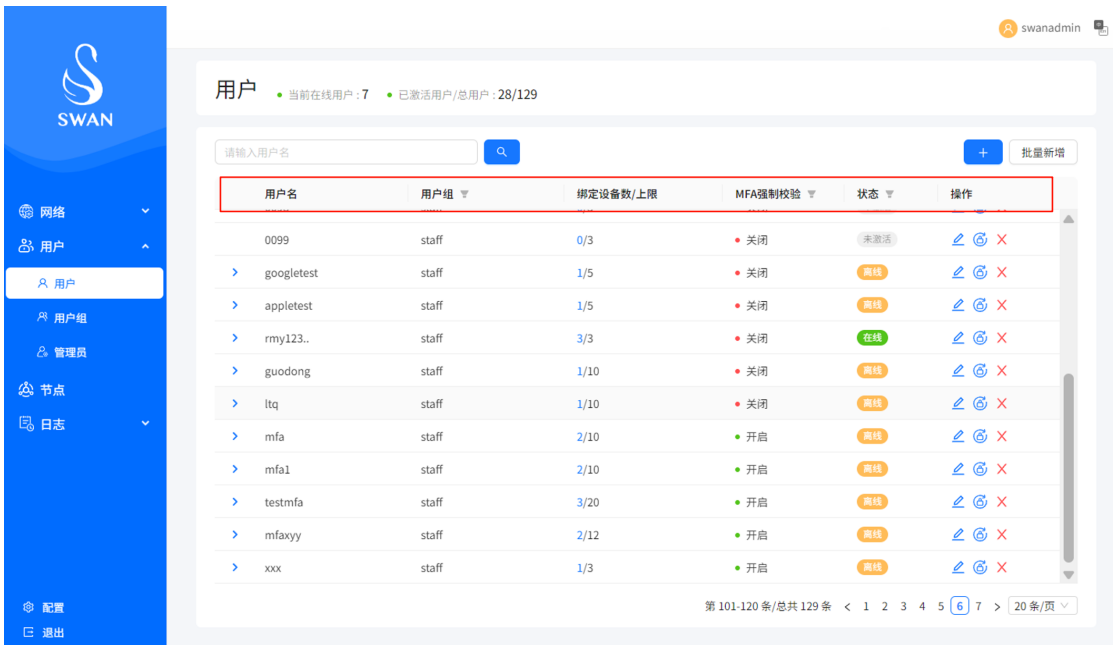
SWAN 系统中，普通用户是用于客户端登录验证的重要角色。要管理这些用户，只需点击左侧导航栏的【用户-用户】选项。

在此页面，您可执行普通用户的创建、批量创建、密码重置、绑定设备管理及删除等操作。页面顶端还会显示 SWAN 系统当前的关键用户数据，包括在线用户数、已激活用户数及总用户数。



a) 用户信息

页面将清晰呈现当前系统中所有已配置的普通用户及其详细状态信息，具体涵盖用户名以明确标识用户身份、用户所属用户组、该用户当前绑定设备的具体数量、系统为该用户设定的可绑定终端设备的最大数量限制即配置的绑定终端上限、该账户是否已启用多因素身份验证（MFA）强制校验功能以增强账户安全性，以及该用户当前处于在线、离线还是未激活的状态信息，方便您实时掌握用户动态。

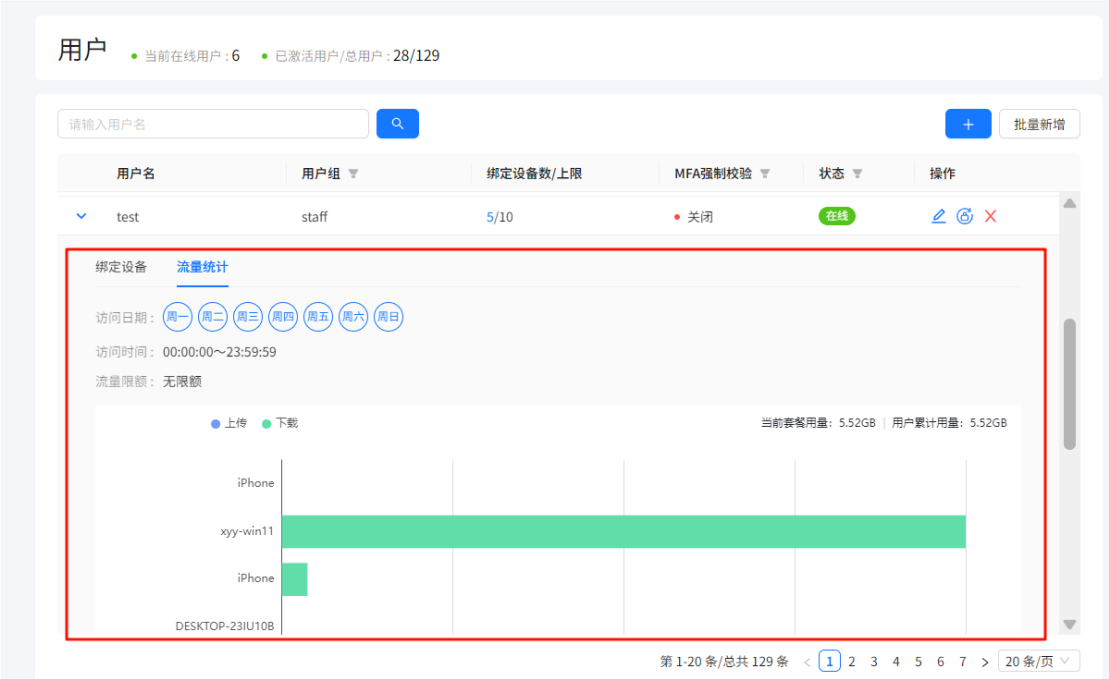


在 SWAN 系统中，点击用户列表中的任意用户，即可弹出便捷的下拉菜单。此菜单集成了多项实用功能，让您能够轻松查看和管理用户信息。

通过下拉菜单，您可以迅速浏览当前用户的登录设备列表，了解用户的设备使用情况。同时，系统还提供了流量使用情况统计，让您能够直观掌握用户的网络流量消耗。

在 SWAN 系统里，当您点击用户列表中的任意一位用户时，会弹出一个下拉菜单，便于您查看和管理用户信息，您能够快速浏览当前所选用户的登录设备列表，清晰掌握其设备使用状况。您可以对用户设备进行解绑及设备重命名标识操作。

此外，下拉菜单还集成了流量统计功能，可展示该用户当前配置的流量策略，以及各设备的实时上传/下载流量详情。通过这些信息，有助于实现网络资源的合理分配与安全使用。



b) 用户新增

在 SWAN 系统的用户管理界面中，新增用户按钮一次仅支持新增一个普通用户，您可以自由设定用户名和密码，并为用户分配特定的用户组。

1）用户名

- 配置说明：为了方便管理和识别普通用户，系统允许管理员为普通用户的用户名进行自定义命名。
- 注意事项：支持输入 2-16 位字符（字母、数字、!、@、$、_、-、.），确保命名的简洁性和易读性。

2）密码

- 配置说明：针对普通用户的密码设置了严格的复杂度配置要求，增加了密码被破解的难度，以此有效抵御暴力破解等常见攻击手段。
- 注意事项：支持输入 8-128 位密码，密码必须同时包含以下三种字符类型：字母、数字、支持的特殊字符（!, [,], @, #, *, &, $, _, ., -）。

3）用户组

- 配置说明：用户组在 SWAN 系统中扮演着关键角色。一旦用户被加入某个用户组，他们将自动获得该用户组所对应的虚拟网络分组的访问权限。这一设计不仅简化了权限管理流程，还确保了用户能够高效、安全地访问所需网络资源。
- 注意事项：每一个普通用户在系统中仅能被归属并加入到唯一的一个用户组内，避免了用户因同时处于多个用户组而可能引发的网络权限冲突或混乱。

4）用户类型

- 配置说明：用户可根据实际需求，将用户账户设置为“普通用户”或“临时用户”两种类型。若选择配置为“临时用户”，系统支持进一步为其设定账户到期时间。这一功能旨在满足短期、临时性的业务场景需求，例如临时项目参与人员、短期访问网络的外部合作方等。
- 注意事项：当临时用户的账户到达预设的到期时间后，系统将自动触发清除机制，该用户的账户信息会被从系统中彻底移除，同时其登录权限也将被即时撤销，此后该用户将无法再登录 SWAN 系统。

5）设备绑定上限

- 配置说明：管理员具备高度灵活的用户终端绑定数配置权限。针对任

意单个用户，管理员可依据实际业务场景与用户需求，自由设定该用户可绑定的终端设备的最大值数量，实现弹性调整。

- 注意事项：在配置过程中，系统设定了明确的边界条件，即所配置的终端绑定数不得超出产品授权所规定的客户端限制最大值；SWAN 支持通过 Manager 所在设备的配置文件（../swan/manager/config/swan.conf），修改参数 device_limit_min 值来设置全局默认的终端绑定数量，参数修改后请重启 Manager 服务：

```
# Application Configurations
application:
  device_limit_min: 1               # The minimum number of endpoints that the system allows a user to log in
  admin_access_token_expire: 60     # Admin access token expiration time in minutes (e.g., 60 = 1 hour)
  admin_refresh_token_expire: 1440  # Admin refresh token expiration time in minutes (e.g., 1440 = 1 day)
  client_access_token_expire: 1440  # Client access token expiration time in minutes (e.g., 1440 = 1 day)
  client_refresh_token_expire: 43200 # Client refresh token expiration time in minutes (e.g., 43200 = 30 day)
  snode_port_change_time: 120       # Service node port change time in minutes (e.g., 120 = 2 hour)
```

6）MFA 强制校验

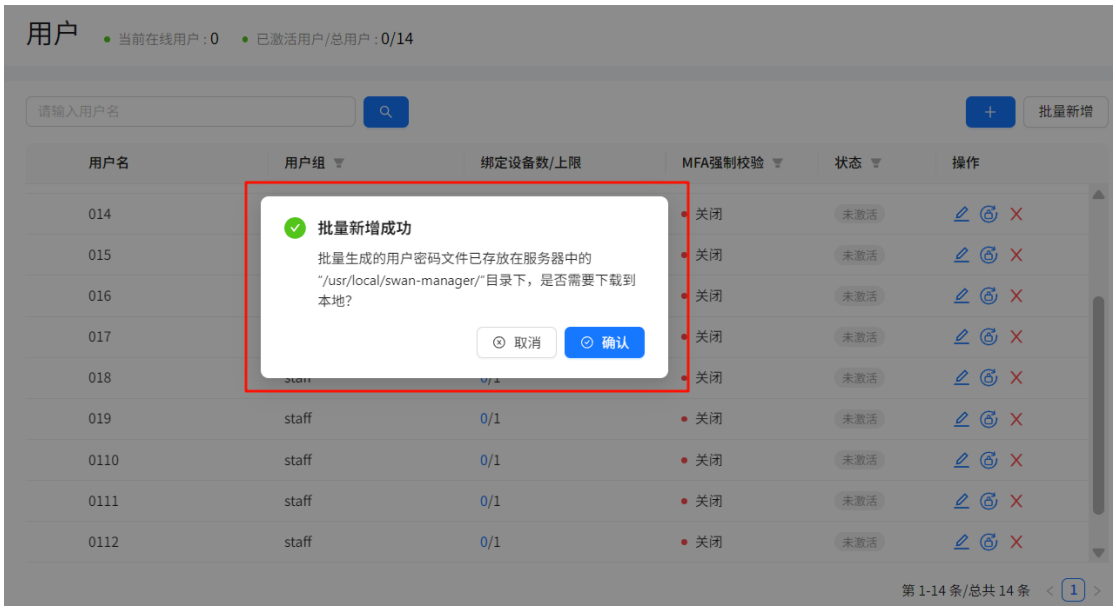
- 配置说明：启用该配置后，系统将强制普通用户启用多因素认证（MFA）功能。对于未绑定 MFA 的用户，其下次登录时，系统会强制引导完成 MFA 绑定流程，仅在绑定成功后，用户方可正常使用 SWAN 客户端，以此强化系统登录安全防护。

- 注意事项：管理端关闭普通用户的 MFA 强制校验功能后，不会对该用户客户端已启用的 MFA 校验功能产生影响；仅当用户主动关闭此功能后，其再次登录时，系统将不再强制引导进行 MFA 校验。

c) 批量新增

批量新增普通用户功能支持一次性添加多个用户，可有效提升管理效率。操作时，只需设置用户名前缀及用户总数，系统便会自动批量创建用户，并为每个用户随机生成密码。

为兼顾密码安全性与使用便捷性，这些随机生成的密码将统一存储于 Manager 机器的/usr/local/swan-manager 目录下的文件中。您也可以选择将包含用户名及对应密码的信息文件下载至本地，通过该文件即可查看用户名与密码的对应关系。

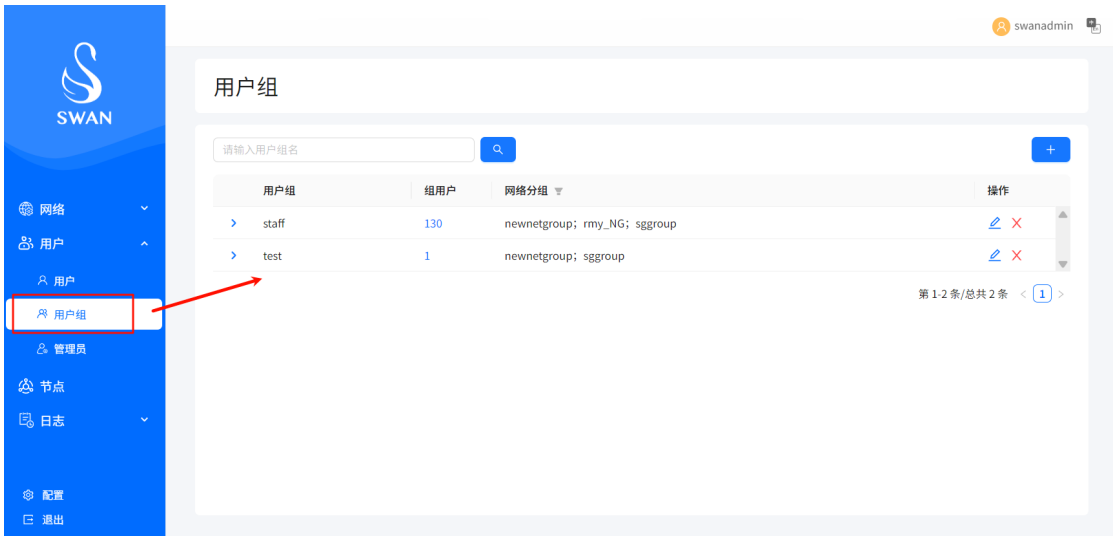


3.3.1 用户组管理

在 SWAN 系统中，普通用户的权限管控通过用户组实现映射，形成“用户组→网络分组→虚拟网络”的三级授权链路。这意味着，当用户被分配至不同用

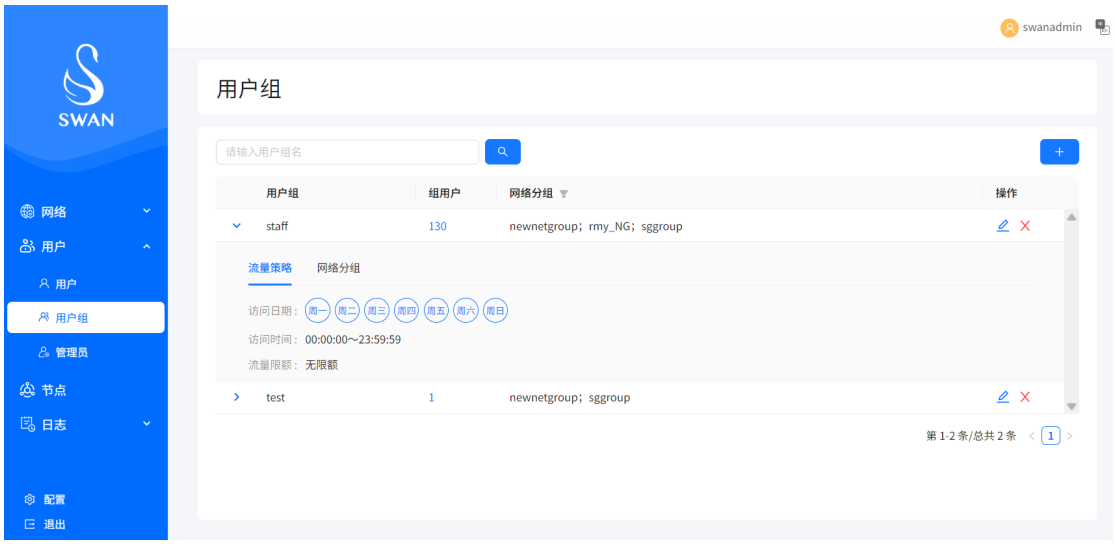
户组后，将自动获得该用户组对应的访问权限范围。

如需管理用户组，点击左侧导航栏的【用户-用户组】选项即可进入管理页面。在此页面，可执行用户组的创建、查询、管理及删除等操作。



a) 用户组信息

该页面会清晰展示系统中所有已配置的用户组及其详细状态信息，具体涵盖用户组名称、组内用户数量（点击可跳转至该组的详细用户列表）、该用户组关联的网络分组等信息。点击列表中的任意用户组，将弹出便捷的下拉菜单，通过菜单可查看该组的流量策略及关联网络分组的详细信息。



b) 用户组配置

点击“新增”或“修改”按钮，即可对用户组配置内容进行编辑操作：

1）用户组

- 配置说明：为了方便管理和识别用户组，系统允许管理员为用户组进行自定义命名。
- 注意事项：支持输入 2～16 位字符（中文、字母、数字、!、@、$、_、-、.），确保命名的简洁性和易读性。

2）组用户

- 配置说明：可将未分配用户组的用户加入当前用户组，用户加入后将自动获得该用户组对应的虚拟网络分组访问权限。
- 注意事项：每一个普通用户在系统中仅能被归属并加入到唯一的一个用户组内，避免了用户因同时处于多个用户组而可能引发的网络权限冲突或混乱。

3）网络分组

- 配置说明：将用户组与特定的网络分组进行关联，该用户组将获得所选网络分组的资源访问权限，由此形成“用户组→网络分组→虚拟网络”的三级授权链路。此时，用户组内的所有成员将自动继承网络权限，无需对每个用户单独进行配置。

- 注意事项：网络分组作为虚拟网络资源的逻辑集合，支持被多个用户组重复关联，通过这种方式可控制各用户组内用户的网络资源访问权限。当网络资源发生变化时，如新增或删除某些网络服务、调整 IP 地址段等，管理员只需在网络分组层面进行修改，所有关联该网络分组的用户组将自动继承这些变更，无需对每个用户组单独进行更新。

4）流量访问控制策略

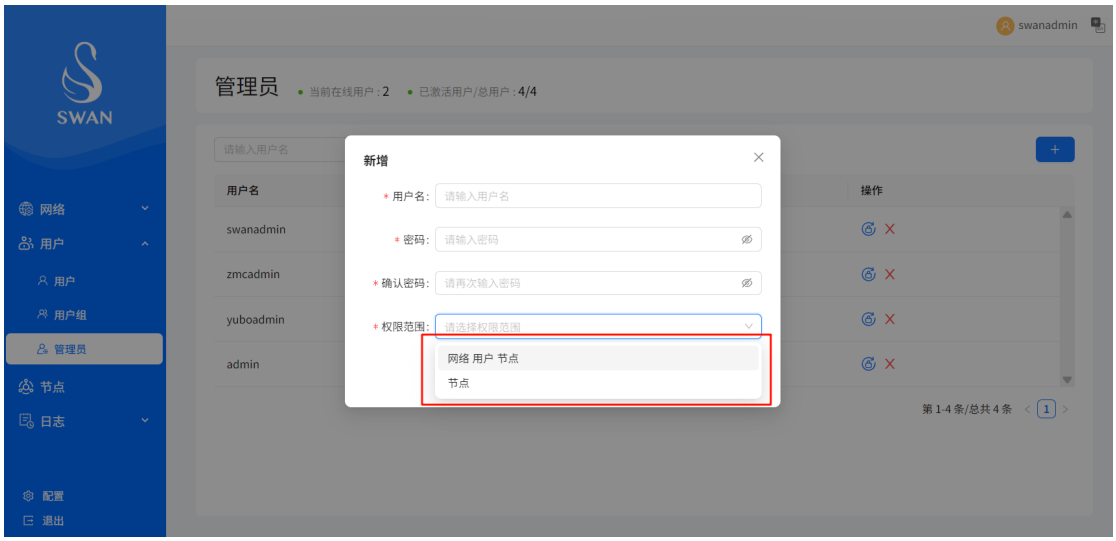
- 配置说明：SWAN 提供流量访问控制策略，系统管理员可以精准地对该用户组内所有用户的网络流量使用情况进行管控限制。
- 注意事项：流量控制能够对访问日期（周一至周日）、访问时间点（精确到秒）以及流量限额（包括无限制、总限额、周期限额三种类型）进行限制。该功能启用后，用户组内所有用户将统一应用此流量策略。

3.3.2 管理员

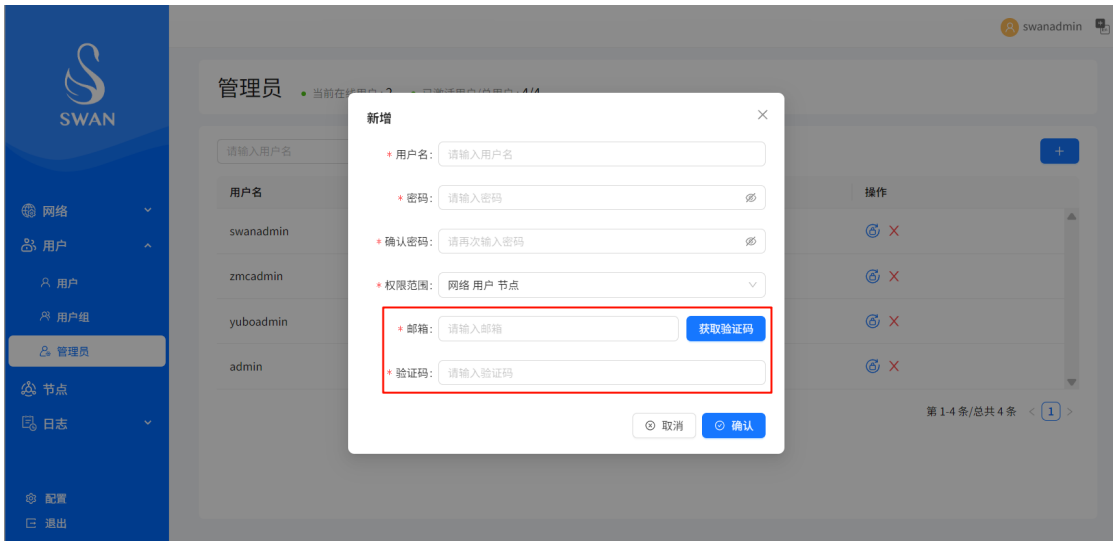
在 SWAN 系统中，管理员角色按照权限等级被明确划分为两种：Network Admin 和 Servicenode Admin。

Network Admin 作为超级管理员，拥有对网络、用户、服务节点以及系统配置的全面管理权限。这种广泛的权限使得 Network Admin 能够执行包括用户管理、网络配置、服务节点部署与监控等在内的所有关键任务。

相比之下，Servicenode Admin 的权限范围则更为局限，仅限于对服务节点的管理。Servicenode Admin 无法触及网络、用户或系统级别的配置和管理。



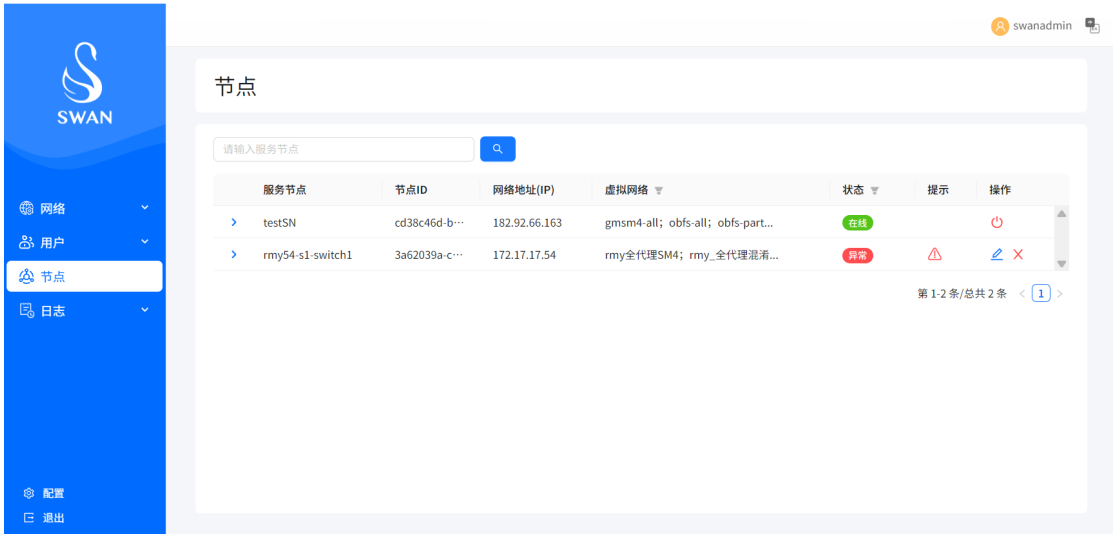
鉴于 Network Admin 权限的高度敏感性，为了确保系统的安全性和管理员账户的安全性，SWAN 要求 Network Admin 在注册或设置账户时绑定安全邮箱。这一措施为 Network Admin 提供了一个额外的安全保障层，使得在密码遗忘或账户被盗等紧急情况下，管理员能够通过安全邮箱快速找回账户控制权。



3.4 节点

在 SWAN 系统中，服务节点用于为客户端用户提供网络接入服务。如需管理服务节点，点击左侧导航栏的【节点】选项即可进入服务节点管理页面。

该页面以列表形式展示当前所有已存在的服务节点及其状态信息，具体包括节点信息、节点网络地址、节点代理的虚拟网络信息、节点状态及节点异常提示信息等内容，便于您快速了解各节点的详细情况。



3.4.1 节点配置

选择某一节点执行下线操作后，点击该节点最右侧的“编辑”按钮，即可对节点内容配置进行编辑。

1）服务节点

- 配置说明：为了方便管理和识别服务节点，系统允许管理员为服务节点进行自定义命名。
- 注意事项：支持 2-16 位字符（中文、字母、数字、!、@、$、_、-、.），确保命名的简洁性和易读性。

2）网络地址

- 配置说明：服务节点所配置的网络地址通常采用公网 IP，或者是在

特定网络环境下 Client 能够直接访问到的其他 IP 地址。该地址用于与客户端建立安全隧道，以保障客户端能够顺利实现访问。

- 注意事项：服务节点的网络地址与 Manager 并无直接关联，服务节点与 Manager 之间的通信连接地址，需在服务节点机器的 /etc/asn/servicenode/config/asn.conf 文件中进行配置。因此，请确保所配置的网络地址为客户端可访问的地址，且客户端能够顺利连接至该地址。

3）端口范围

- 配置说明：服务端口用于动态安全隧道的建立，每个关联的虚拟网络需要独立的安全网络来实现与 Client 的通信，所以服务端口范围与该节点关联的虚拟网络个数密切相关。具体而言，服务节点所需配置的端口数量必须大于或等于关联的虚拟网络个数。
- 注意事项：请确保所配置的端口处于通畅且可访问状态，建议选用非业务常用的端口范围，同时需注意开放防火墙对应端口。只有满足上述条件，客户端才能顺利通过这些端口与服务节点建立连接。

4）端口定时更新（当前版本暂不支持）

- 配置说明：启用端口定时更新功能后，系统默认每两小时自动更换服务端口，通过动态调整以规避固定端口被封禁的风险。
- 注意事项：启用此功能时，建议在配置服务端口范围时预留至少 2 倍的可用端口，若未满足此条件，可能因可用端口不足导致更新失败。

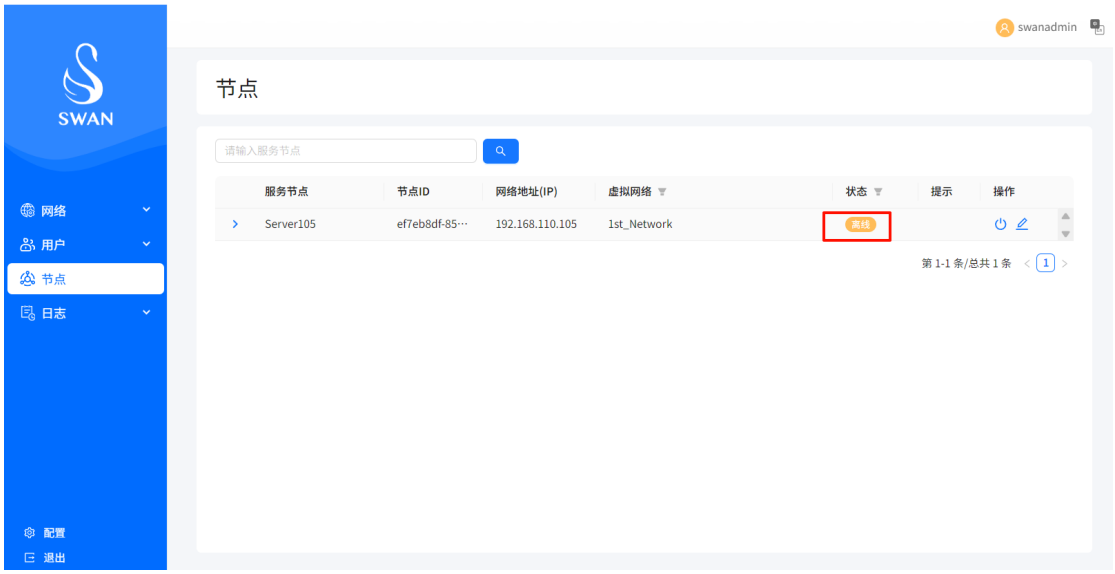
5）虚拟网络

- 配置说明：服务节点需关联至已有的虚拟网络，关联后，该服务节点将自动继承虚拟网络中预定义的服务网段及加密算法配置。
- 注意事项：目前，单个服务节点具备同时加入多个虚拟网络的能力，建议您根据实际需求选择合适的虚拟网络进行关联，同时需确保服务节点所在的物理机器能够支持对所选虚拟网络资源的访问。

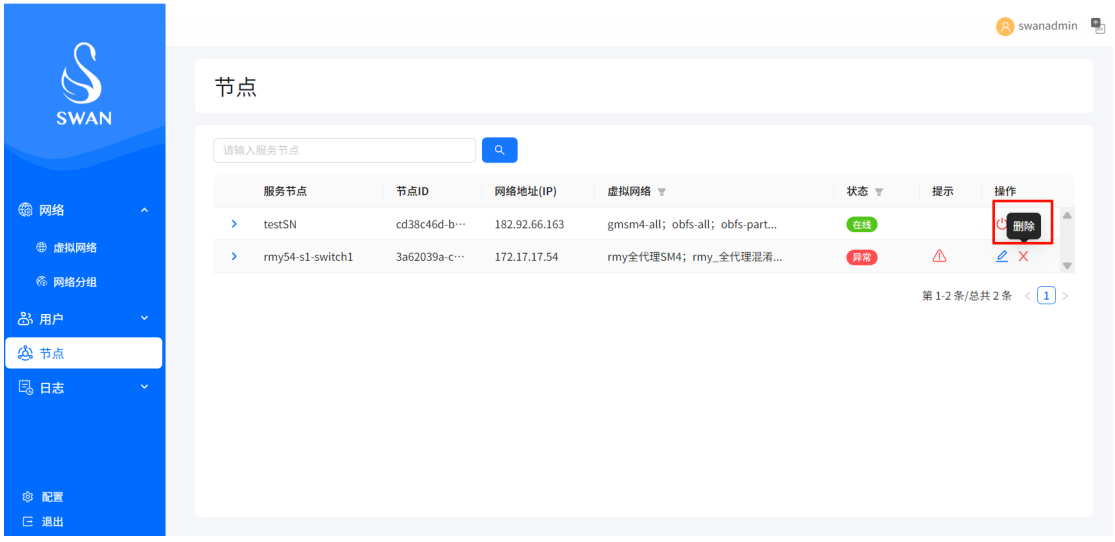
3.4.2 管理与删除

当服务节点处于上线运行状态时，系统不支持对该节点执行配置管理相关操

作。若需对服务节点的配置进行更新，必须先将服务节点执行下线操作，使其处于离线状态后，方可开展后续的配置管理工作。



系统对服务节点的删除操作设有严格限制条件。仅当服务节点出现异常告警情况时，例如系统检测到服务节点不可达、服务响应超时等严重影响节点正常运行的异常状况，管理员才具备对该节点执行删除操作的权限。通过此规则，防止因误删除正常运行的节点而导致服务能力下降或业务中断，保障系统的稳定性和可靠性。



3.4.3 监控与告警

在 SWAN 系统中，服务节点的详情与监控功能支持一键展开。只需点击对应的服务节点，即可下拉展示该节点的详尽配置信息与直观的状态监控仪表。

在配置信息方面，涵盖当前配置的网络地址、开放的端口范围，了解服务节

点对外提供服务的通道；关联的服务网段，掌握服务节点所代理的网络资源；配置的主机名，便于识别和管理；服务节点机器的 CPU 核心数、总磁盘容量、总内存大小，这些基础硬件信息有助于评估服务节点的性能承载能力；关联的虚拟网络启用的加密算法，以及端口定时更新功能的状态。

在状态监控方面，您能实时获取当前服务节点承载的加密吞吐速率，直观了解其数据处理能力；基础资源使用情况一目了然，包括 CPU 实时占用率，反映处理器的工作负载；内存占用率，显示内存资源的使用程度；磁盘占用率，了解磁盘存储空间的剩余情况；LOAD 负载情况，综合评估服务节点的整体运行压力。这些信息将助力您全面、精准地把握服务节点的运行状态，及时发现潜在问题并进行有效处理。

3.5 日志

SWAN 日志模块提供系统事件、风险告警和用户活动的概览，帮助管理员有效监控和管理网络安全。模块包括数据可视化图表、事件概览和详细日志，便于快速访问和分析。

3.5.1 总览

日志总览提供详细的仪表盘概览，默认展示最近三天的数据，支持对时间范围进行自定义查询。

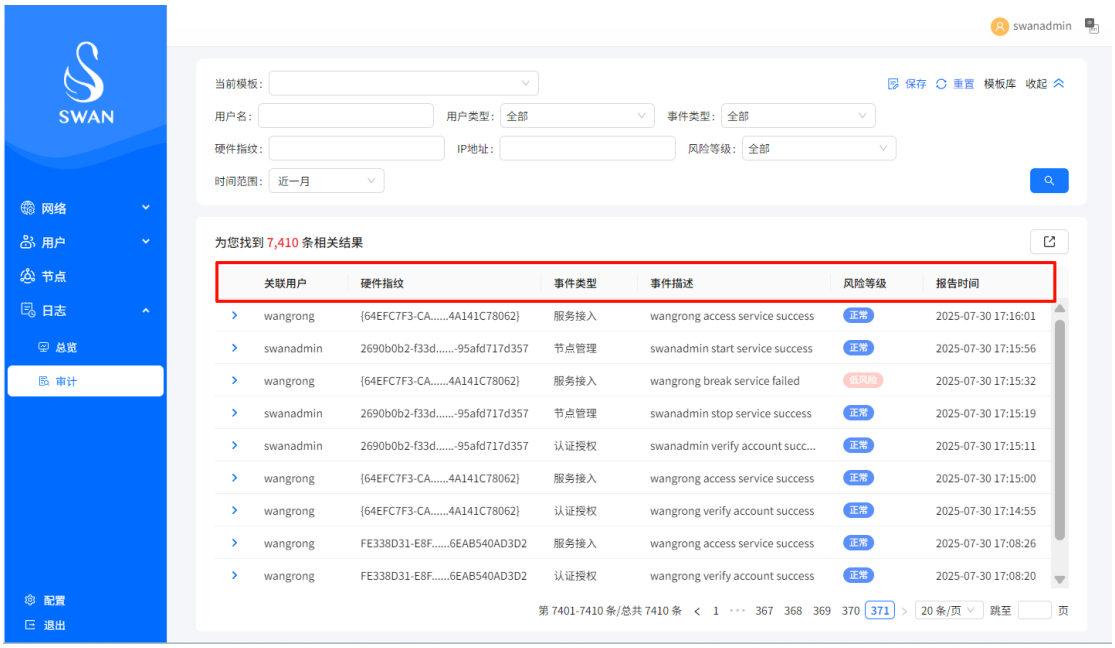
仪表盘概览包括以下内容：

- 事件数量：显示选定时间范围内检测到的事件总数。
- 告警数量：显示已触发的告警总数，提示可能需要注意的问题。
- 事件趋势：折线图展示事件的发生日期趋势，分为正常事件和告警事件。
- 风险等级分布：饼图显示按风险等级分类的事件概览。
- 事件类型分布：展示按类别划分的事件分布，便于用户识别最常见的事件类型。
- 事件用户源分布：展示不同用户类型的活动趋势。
- 事件上报时间趋势：显示选定时间范围内不同时间点位的事件趋势，分为正常事件和告警事件。
- 告警用户源 Top10：按告警数量列出用户排名，便于有针对性地进行审查。

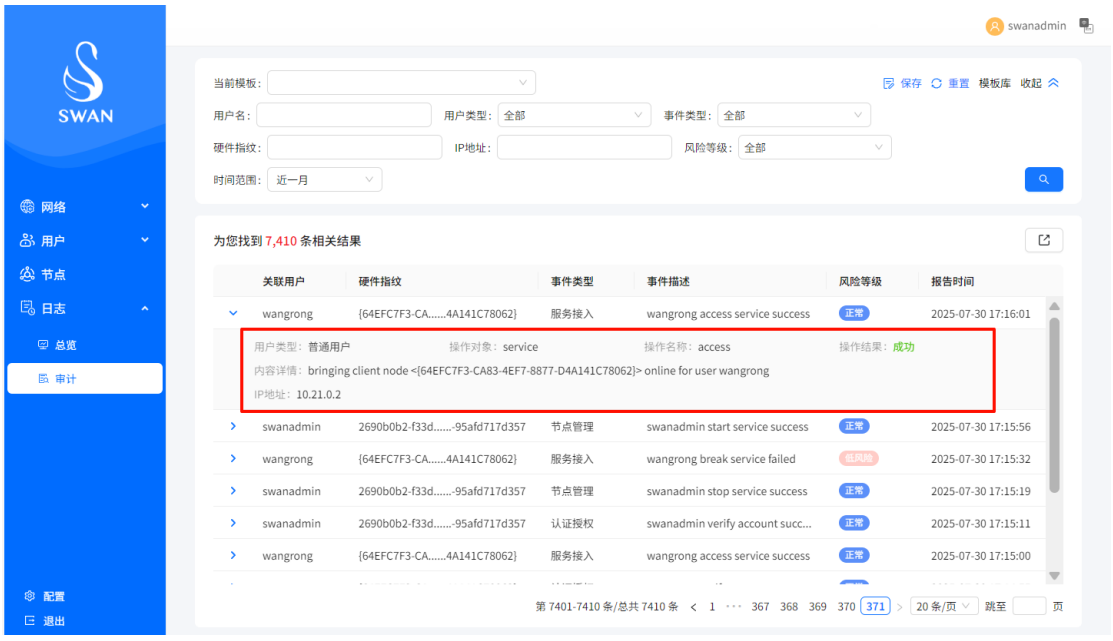
3.5.2 审计

审计界面提供详细的日志数据，用户可按用户名、用户类型、事件类型、硬件指纹、IP 地址、风险等级及时间范围自定义查询目标日志内容。同时，支持通过分页浏览事件记录，也可直接跳转到指定页面。

详细日志数据包含关联用户、硬件指纹、事件类型、事件描述、风险等级、报告时间等信息：



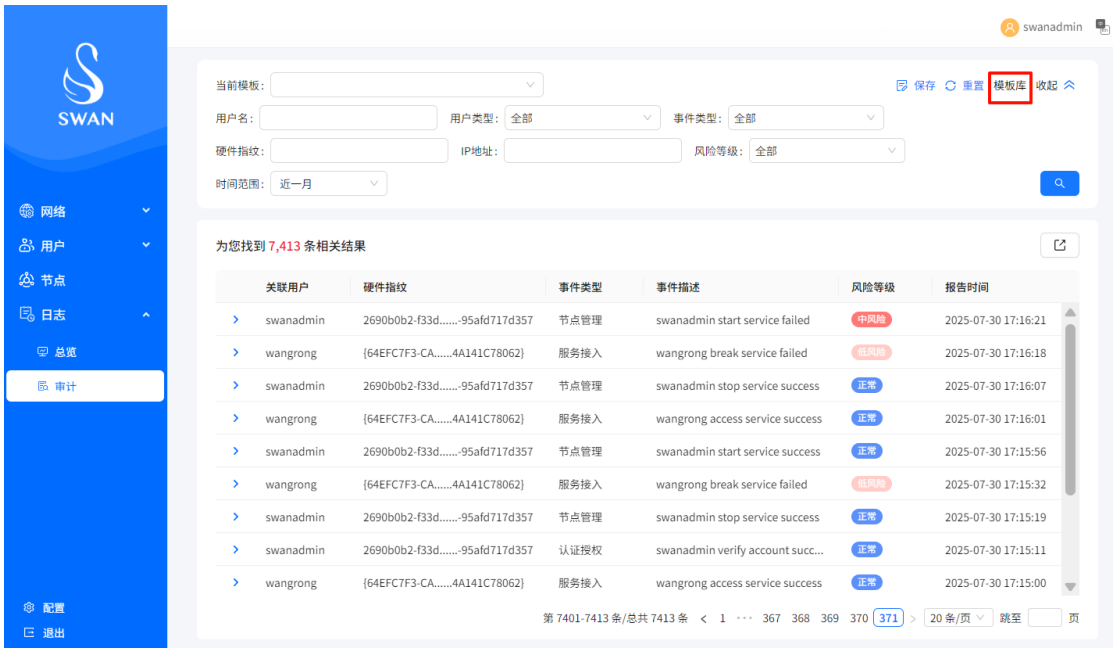
用户点击具体日志后，可以展开更为详细的日志信息，包括用户类型、操作对象、操作名称、操作结果、内容详情和 IP 地址等信息：



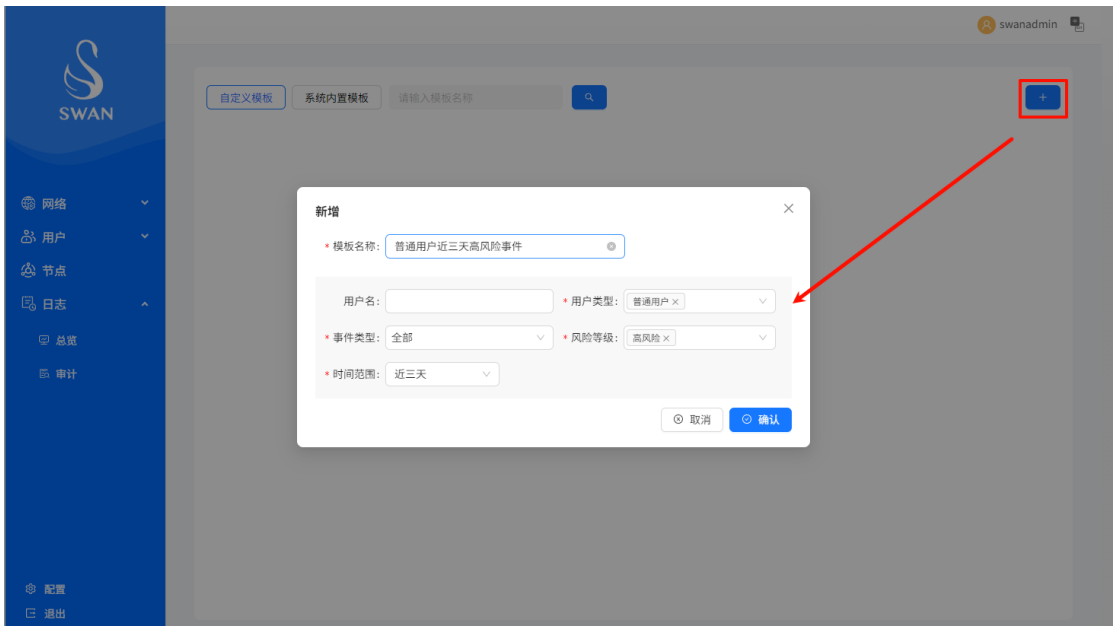
总览界面的每个仪表盘数据均与日志审计的过滤条件相关联，用户点击任意仪表盘，即可直接跳转至审计界面，系统会自动过滤出该条件下的所有日志数据，从而快速锁定并查询目标信息。

在事件日志表的过滤条件设置中，系统提供“模板”功能，用于帮助用户保

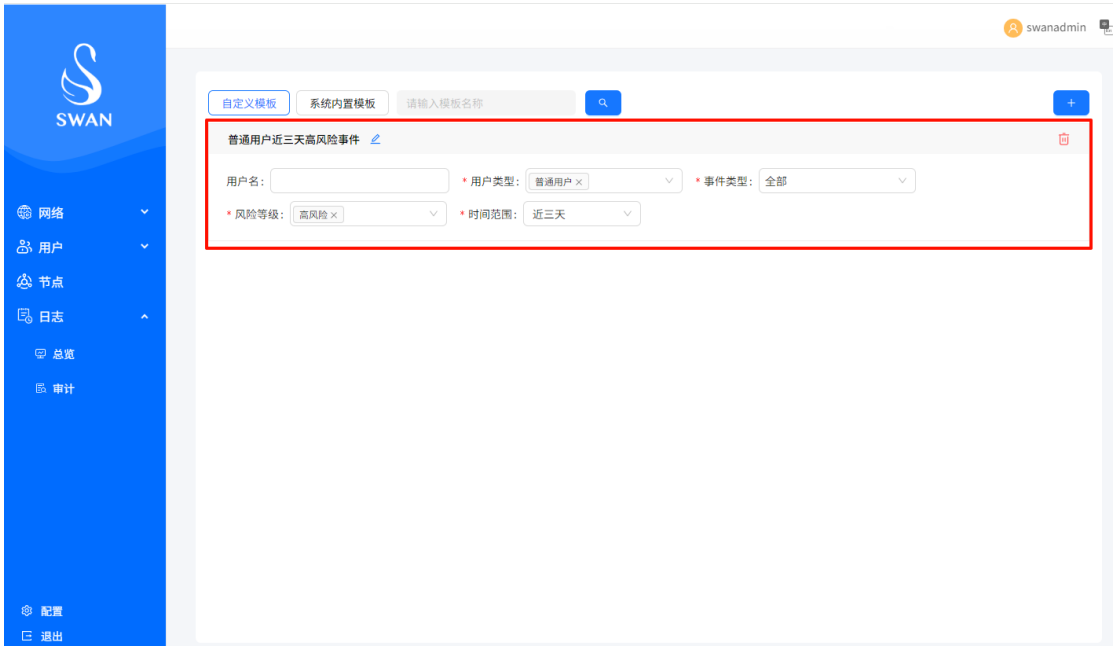
存和快速应用常用的过滤配置。用户点击审计页面右上角的“模板库”选项，即可进行“自定义模板”的管理维护。



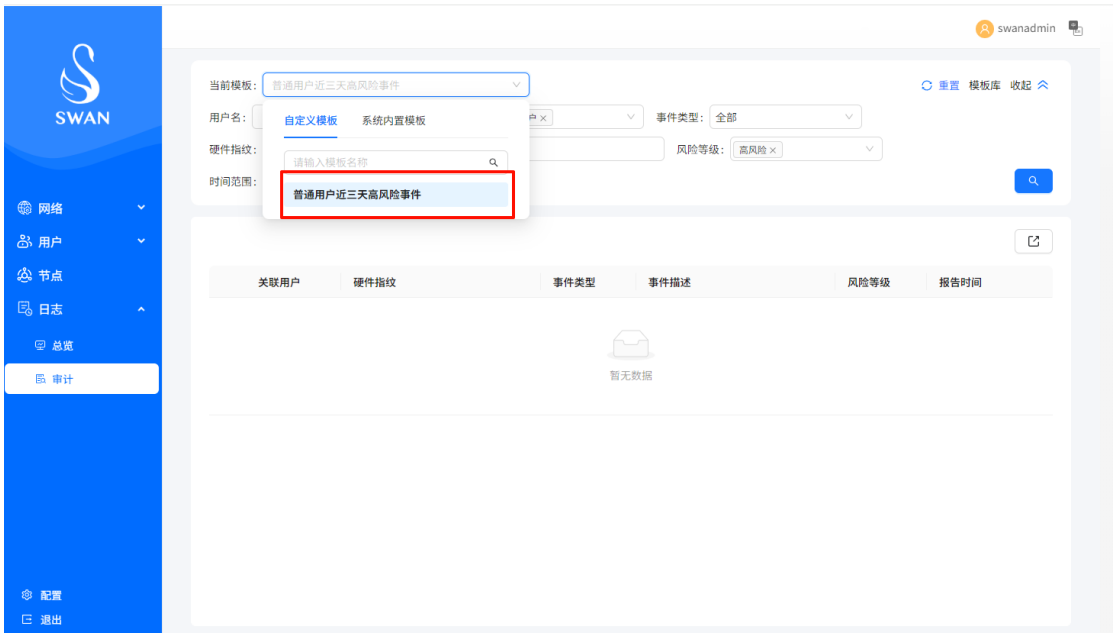
点击右上角“新增”按钮即可自定义日志过滤模板，当用户设置好过滤条件（如用户名称、用户类型、事件类型、风险等级和时间范围）后，可以点击“确认”按钮，将当前筛选条件保存为模板。在保存时，用户可以为模板命名，以便于识别和管理：



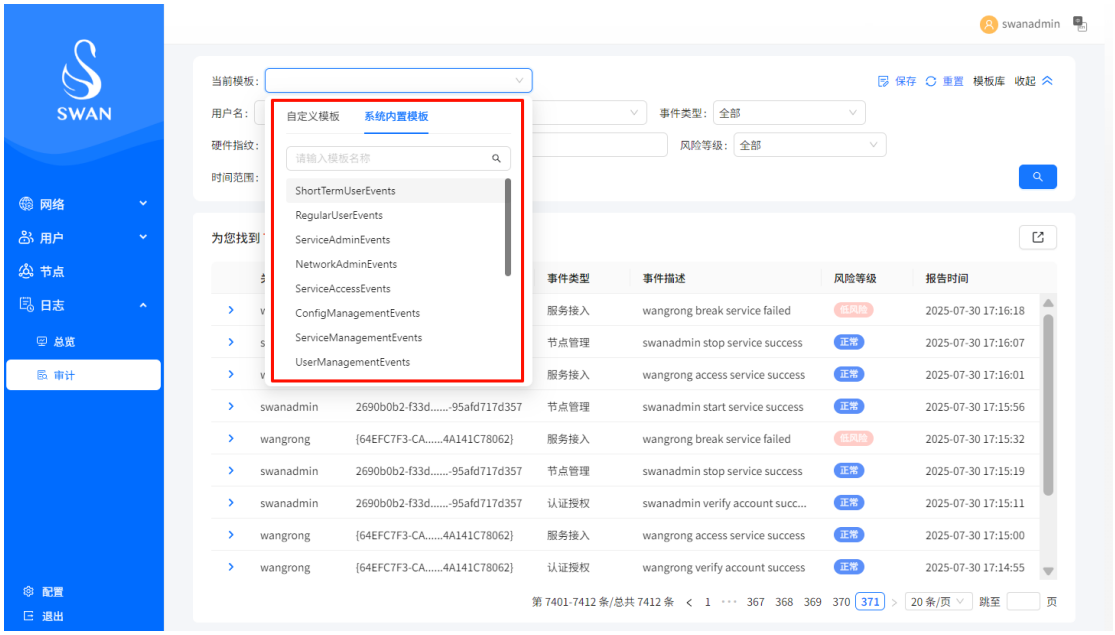
用户可以在“模板库”中查看所有已保存的模板，并对其进行管理，例如编辑或删除不再需要的模板：



借助该功能，用户可一键调用预设的筛选条件，有效提升工作效率，尤其适用于需要定期查看特定数据的场景。

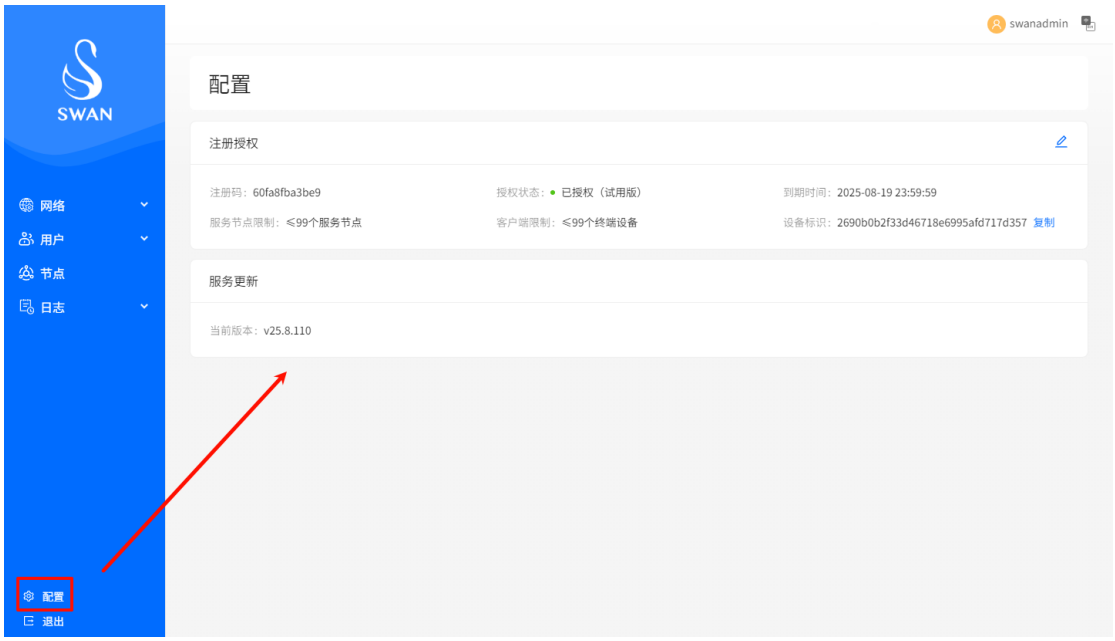


同时，审计模块内置了常用的审计模板，依据不同审计场景和常见需求定制，用户可直接调用这些模板来过滤日志内容：



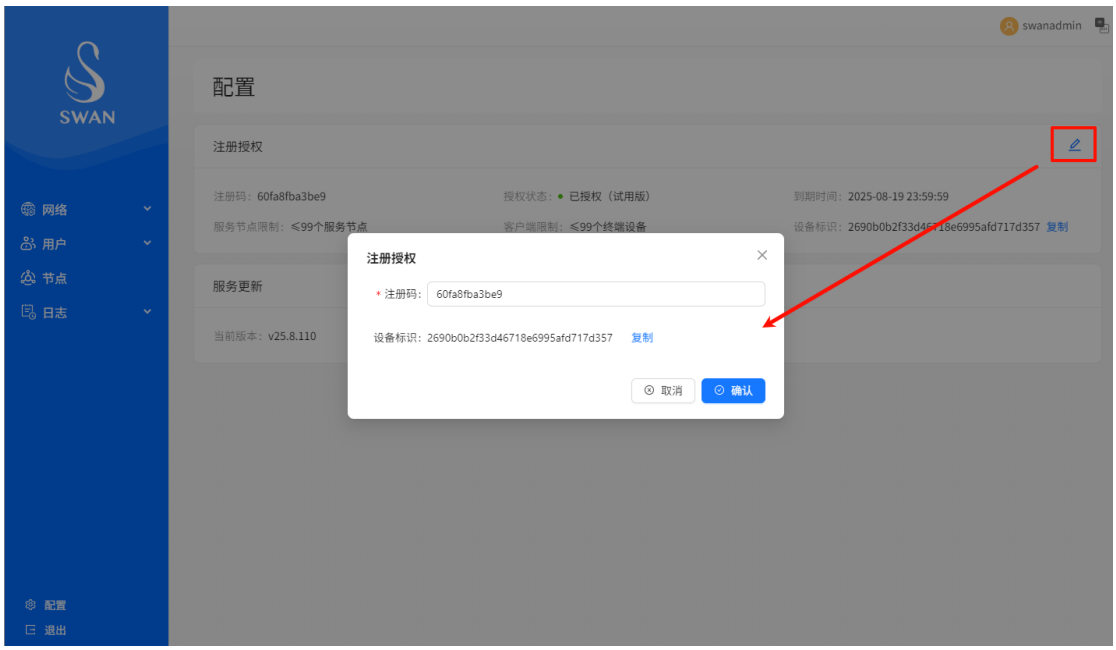
4. 配置

用户点击左侧导航栏中的【配置】选项，系统将展示当前 SWAN 系统的注册授权信息以及版本信息。这些信息以清晰、直观的方式呈现，方便用户快速了解系统的授权状态和版本情况。注册授权信息包含但不限于当前授权状态、有效期、服务节点限制、客户端限制等信息，版本信息则明确显示系统当前运行的版本号：



SWAN 系统采用严格的注册码与设备绑定策略。每个设备都拥有唯一的设备标识，系统依据该设备标识为设备生成专属的激活码此激活码是激活 SWAN 服务的关键凭证。

当用户需要更新系统的授权或获取新的激活码时，需根据设备标识码去申请新的激活码。获取新的激活码后，点击“编辑”按钮，填入新的注册码，即可获取新的授权并更新系统的到期时间。



5. 注意事项

5.1 客户端功能支持情况

客户端平台	安装方式	流量分流	流量混淆	国密隧道
MacOS	AppStore（需美区账户）	路由规则自定义	❌不支持	❌不支持
	dmg 文件安装	路由规则自定义	✅支持	❌不支持
Linux CLI	wget 文件下载	国际地址智能分流	✅支持	✅支持
Linux GUI	dpkg 文件安装	国际地址智能分流	✅支持	✅支持
Windows	exe 文件安装	路由规则自定义	✅支持	❌不支持
iOS	AppStore（需美区账户）	路由规则自定义	❌不支持	❌不支持
Android	APK 文件安装	路由规则自定义	❌不支持	❌不支持

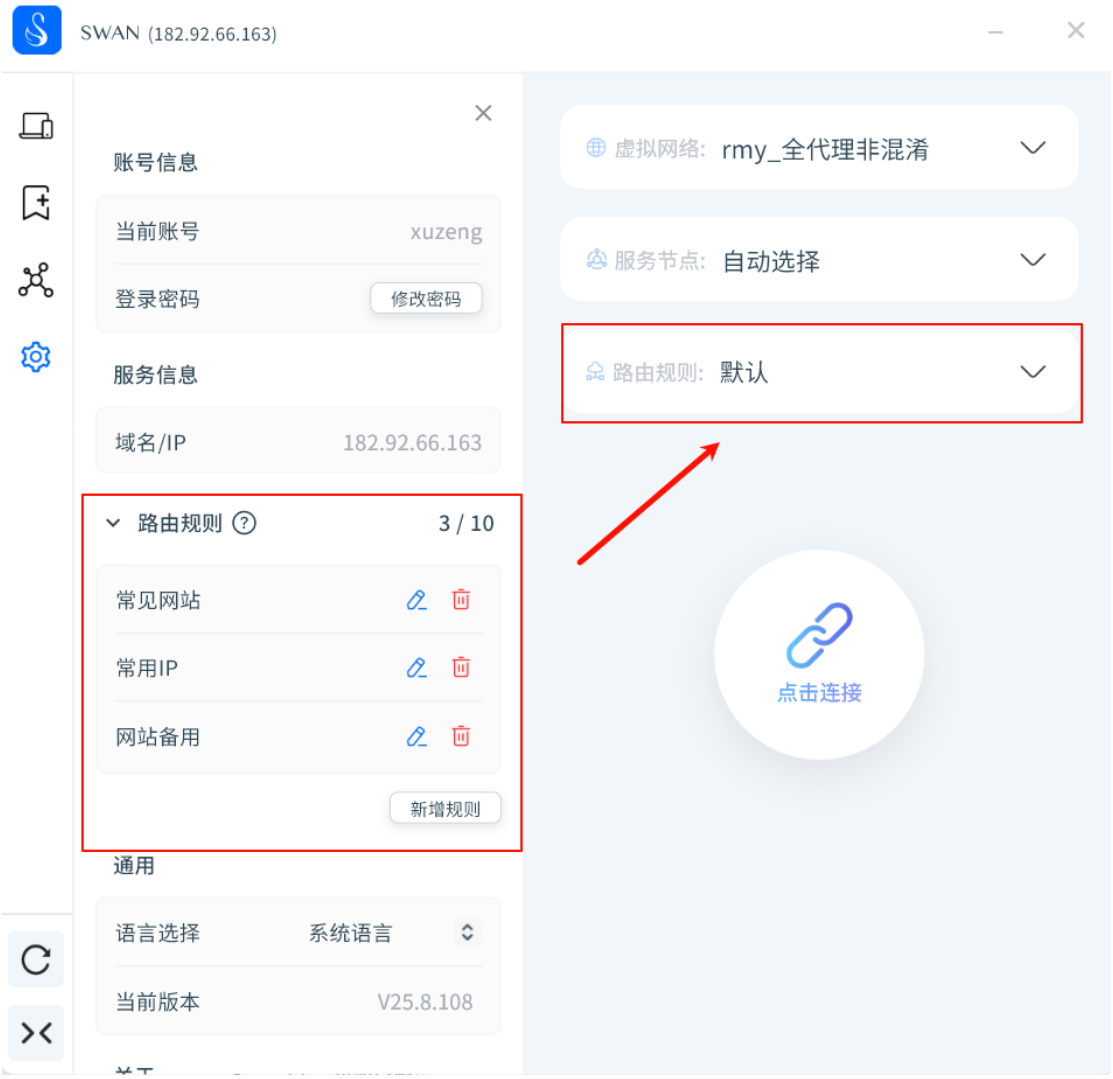
*注意：若虚拟网络已启用流量混淆或者国密隧道功能，则使用上述不支持该功能的客户端将无法连接至该虚拟网络。

5.1.1 流量分流

a) 路由规则自定义

针对 MacOS、Windows、iOS、Android 客户端，可以通过路由规则自定义功能，允许用户灵活控制流量转发路径，实现按需代理。当虚拟网络处于全代理模式（0.0.0.0/0）时，通过配置路由规则可指定特定域名/CIDR 通过服务节点代理，其余流量走本地网络，避免全量代理的性能开销和潜在隐私问题。

- 代理流量：匹配路由规则中配置的域名/CIDR 的流量 → 转发至服务节点进行流量代理
- 直连流量：未匹配任何路由规则的流量 → 直接通过本地网络访问



b) 智能分流

针对 Linux CLI/GUI 客户端，它们不支持路由规则自定义功能，而是通过“智能分流”功能实现国际流量与本地流量的自动识别与路由，无需用户干预。

5.1.2 流量混淆

为应对网络流量监控和深度包检测（DPI）对 UDP 流量的识别与拦截，采用协议伪装技术将 UDP 流量动态转换为 TCP 流量，从而隐藏真实通信特征，增强隐私保护。

5.1.3 国密隧道

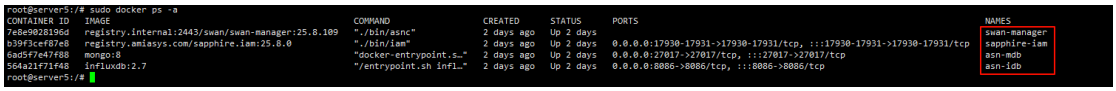
国密隧道能力是指 SWAN 隧道加密算法支持国密 SM4 分组密码算法，实现对数据传输的国产化加密保护。相较于国际主流的 ChaCha20-Poly1305 算法，SM4 在传输速率上虽有一定差距，但其基于国密算法体系更合适于政务、金融等对安全性有更高要求的场景。

5.2 日常维护操作

5.3.1 查看服务状态

1）SWAN Manager

在 Manager 所在机器上执行 sudo docker ps -a 命令，查看 asn-mdb、asn-idb、sapphire-iam、swan-manager 容器的运行状态。若这些容器未处于正常运行（up）状态，请及时联系我们进行问题定位。

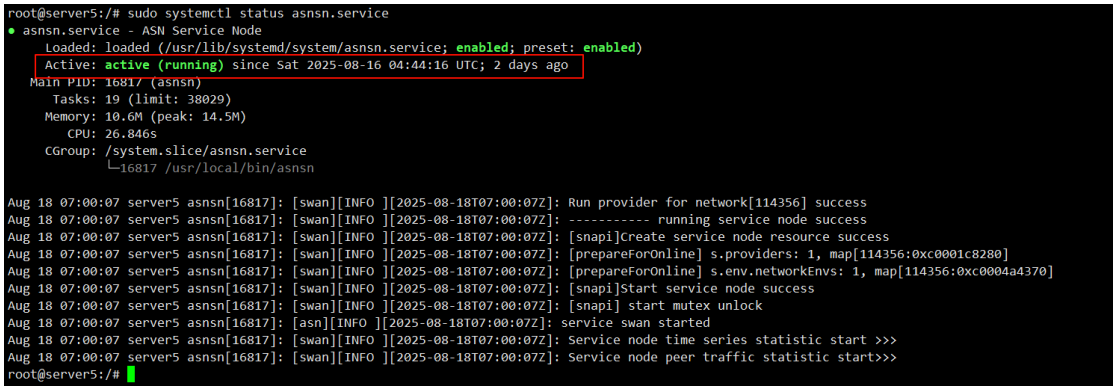


2）SWAN Servicenode

在 Servicenode 所在机器上执行 sudo systemctl status asnsn.service 命令，查看 asnsn.service 服务的运行状态是否正常。

服务状态：确认输出中 Active: 字段是否为 active (running)。

若服务状态存在异常，请及时联系我们进行问题定位。



5.3.2 服务端口说明

端口	作用	说明
12760	web 端访问服务端口。	如果 SWAN 管理端页面仅在内部网络访问，则无需将相关端口进行公网映射。
12762	用于 Manager 和 Servicenode 通信	如果 Manager 和 Servicenode 部署在公网，需开放对应端口，确保正常通信。

端口	作用	说明
7926	用于 Manager 和 Client 通信	如果 Manager 部署在公网，需开放对应端口，确保正常通信。
自定义服务端口，如 21000-21005	Servicenode 服务端口用于动态安全隧道的建立。	需开放防火墙对应服务端口，确保客户端能顺利通过这些端口与服务节点建立连接。

5.3.3 查看系统日志

a) 管理端

1）SWAN Manager

在部署的项目路径下（通常是../swan/manager/log/asn/），进入后找到 log/asn_runtime.log 和 log/swan_runtime.log 文件。

查看 ASN 框架日志：

```
cat  ../swan/manager/log/asn/asn_runtime.log
```

查看 SWAN 日志：

```
cat ../swan/manager/log/asn/swan_runtime.log
```

2）SWAN Servicenode

查看 ASN 框架日志：

```
cat /var/log/asn/servicenode/asn_runtime.log
```

查看 SWAN 日志：

```
cat /var/log/asn/servicenode/swan_runtime.log
```

b) 客户端

1）Windows 日志路径：

```
C:\Users\用户名\AppData\Roaming\Amianetworks\swan\logs\
```

2）Linux GUI 日志路径：

/var/log/swanAppClient/

3）Linux CLI 日志路径：

/var/log/swan/

4）Mac OS (AppStore) 日志路径：

/Users/<用户名>/Library/Application Support/com.amianetworks.swan/logs/

5）Mac OS (dmg 安装方式) 日志路径：

/Users/<用户名>/Library/Application Support/com.amianetworks.swan/logs/

6）Android 日志路径：

根目录/Android/data/com.amianetworks.swan/files/logs/

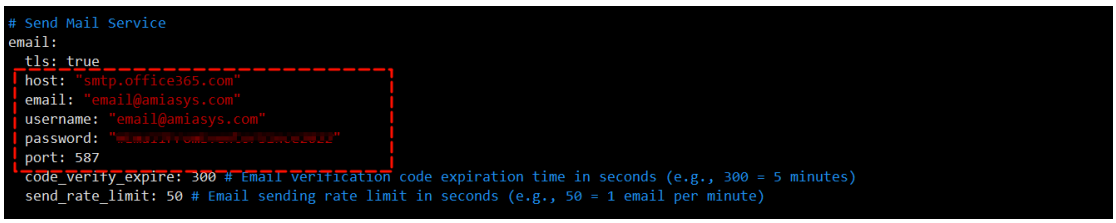
7）iOS 日志路径：

/var/mobile/Containers/Data/Application/<UUID>/Library/Application Support/logs/

5.3.4 邮箱地址配置

在部署 SWAN 系统之前，需预先准备一个邮箱账户。SWAN 系统将使用该邮箱账户来执行发送邮件的操作，具体用于管理员账户的绑定、密码修改以及密码找回等流程。

邮箱账户的配置信息存储于部署项目路径下的配置文件中，该文件通常位于../swan/manager/config/路径。您需要打开 swan.conf 配置文件，并修改其中 #email 配置部分的相关参数。



*注意：若您已使用当前配置的邮箱账户绑定了 SWAN 相关账户，在后续更

换该邮箱账户的配置信息后，将无法再通过新邮箱关联并找回之前绑定的 SWAN 账户。请谨慎操作！

5.3 常见问题处理

5.3.1 无法通过 Servicenode 进行网络代理

问题现象：

Client 客户端可正常访问 Servicenode 设备自身的所有地址，但无法通过 Servicenode 访问其代理的服务网段地址，此情况可能是由于 Servicenode 机器未启用数据包转发功能所致。

解决方案：

SWAN Servicenode 需开启所在设备的数据包转发功能（net.ipv4.ip_forward），其中 0 表示关闭，1 表示开启，具体配置方法如下：

（1）临时生效配置（系统或网络服务重启后失效）：

- 开启命令：sudo sysctl -w net.ipv4.ip_forward=1
- 查看配置：sudo sysctl -a | grep net.ipv4.ip_forward

（2）永久生效配置（系统或网络服务重启后仍保持生效）：

- 修改 vim /etc/sysctl.conf 文件，将 net.ipv4.ip_forward 取消注释并设置为 1
- 执行命令使配置生效：sudo sysctl -p

5.3.2 虚拟网络采用国密算法后，导致代理网络不通

问题现象：

若 Servicenode 代理的虚拟网络采用国密算法，而 Client 客户端无法通过 Servicenode 访问其代理的服务网段地址，此情况可能是由 Servicenode 机器的防火墙策略导致。

解决方案：

需检查并调整 Servicenode 的 iptables 中 FORWARD 链默认策略，确保允许

数据包转发。查看方式：

- $ sudo iptables -L FORWARD -v -n --line-numbers

Chain FORWARD (policy DROP 9145 packets, 768K bytes)　#默认拒绝所有转发

若显示 policy DROP，则需修改为 ACCEPT，可通过以下命令修改（通常需要 sudo 权限）：

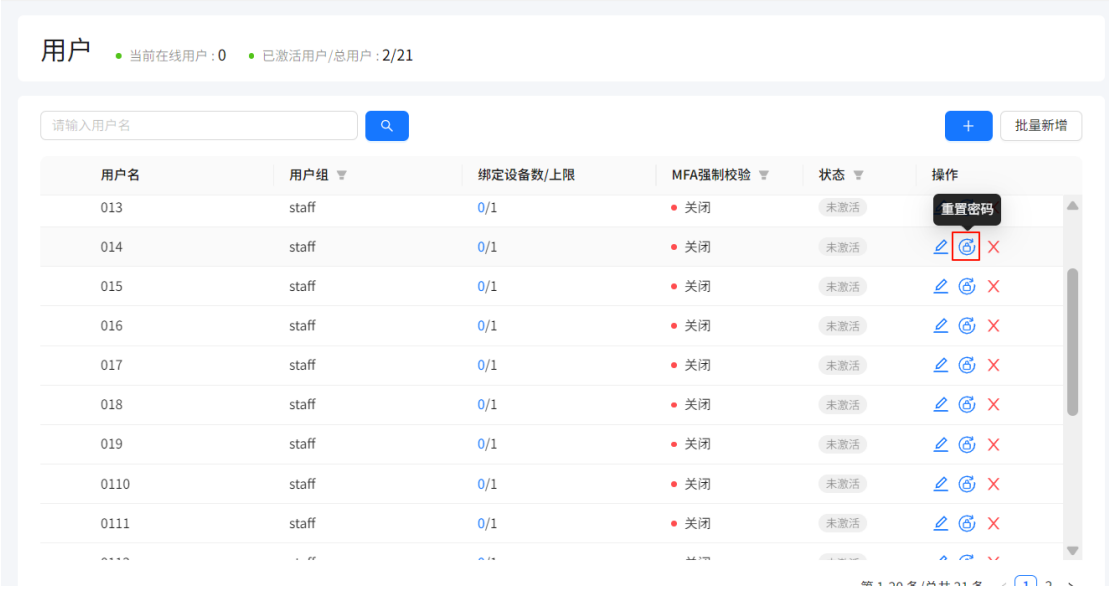
- sudo iptables -P FORWARD ACCEPT　# 将 FORWARD 链默认策略改为允许

最后重新运行 iptables -L FORWARD 进行验证，确认输出中 policy 变为 ACCEPT。

5.3.3　账户找回密码

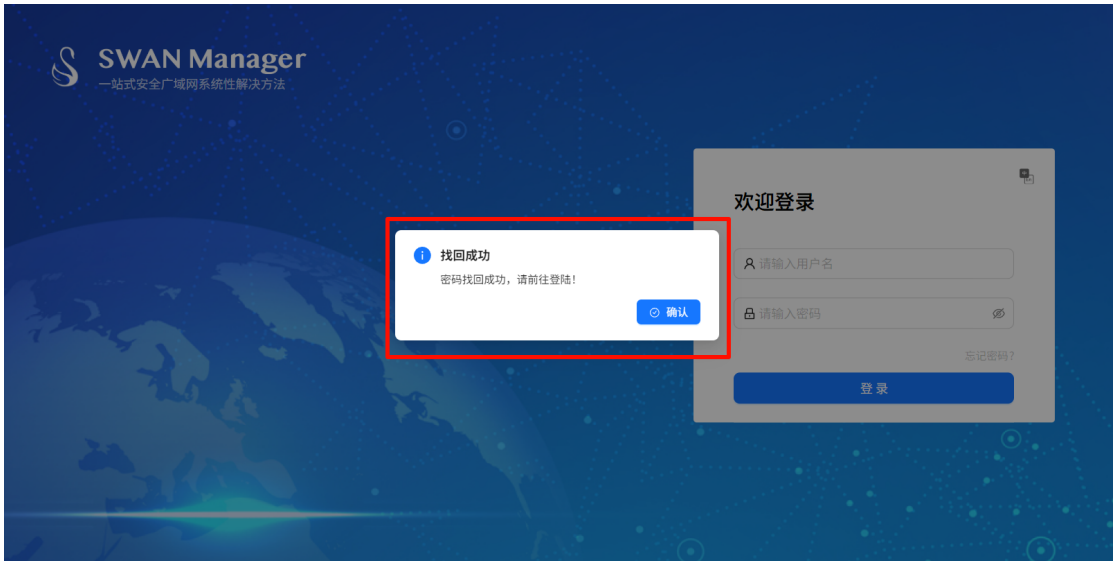
a)　普通用户

普通用户若忘记密码，可联系 SWAN Manager 管理员。管理员登录 Web 管理端后，进入【用户 - 用户】页面，在用户管理功能中为其重置密码。



b) 管理员

若您遗忘管理员配置的密码，可在登录页面点击“忘记密码”，通过安全邮箱接收验证码后重新设置密码。如未设置安全邮箱或操作过程中遇到问题，请联系我们，我们将协助您完成密码重置。


SWAN Manager
一站式安全广域网系统性解决方法
找回成功
密码找回成功，请前往登陆！
确认
欢迎登录
请输入用户名
请输入密码
忘记密码？
登录