天翼云
State Cloud

云密评专区

用户操作指南

天翼云科技有限公司

目录

版本记录

序号	说明	版本号	备注
1	初稿	V1.0	

1. 快速入门

1.1. 产品概述

本系统实现密码服务管理系统和 2 种典型密码服务，包括：

- 密码服务管理系统

为平台维护人员和机构用户提供密码资源和密码服务管理功能；

- 密码服务

实现 2 种典型的密码服务，包括：SSL 网关服务和 SSL VPN 服务。

1.2. 运行环境

- 操作系统：Windows7、10、11，Mac OS
- 浏览器版本： IE11 及以上，Chrome，Firefox，360 安全浏览器，safari

1.3. 角色与权限说明

不同角色的用户具有的权限不同，超级管理员可自定义角色。系统默认的角色及权限可参考下表，具体请以实际情况为准。本文的操作内容以超级管理员举例说明。

角色	权限
超级管理员	具有系统所有权限。
操作员	网关的业务操作管理。
系统管理员	用户管理。
审计员	查看用户的操作日志。

2. 系统登录

用户登录系统都支持采用口令登录和 Ukey 登录两种方式。

2.1. 口令登录

用户访问链接（以端口为 18090 为例）：http://127.0.0.1:18090/，进入登录页面，如图所示：

输入账号，密码，验证码后，点击【登录】按钮，登录成功，进入密码服务平台。

2.2. Ukey 登录

进入登录页面，选择 Ukey 登录，如图所示：

客户端先下载并安装 Ukey 控件，重新插入 Ukey 后系统会自动识别 Ukey 序列号，输入账号，Ukey 的 PIN 码，验证码，点击【登录】按钮，登录成功，进入平台。

【注意】

- ✧ 用户必须绑定 Ukey 后才能使用 Ukey 登录。
- ✧ 客户端必须安装 Ukey 控件，并启动 Ukey 控件，才能使用 Ukey 登录。

3. 菜单栏

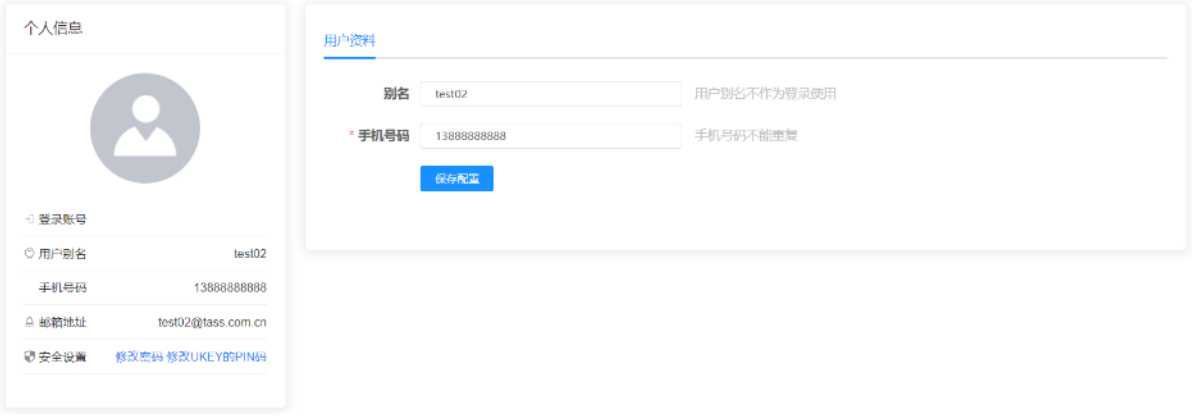
3.1. 菜单栏

序号	功能	二级功能	三级功能	功能描述
1	密码服务详情	SSL 网关服务	网关服务管理	用于管理网关服务，包括新增、删除、配置和查看详情等功能。
2			网关服务器组	用于管理网关服务器组，包括新增、删除、编辑、查看服务器列表、添加服务器等功能。
3			网关服务证书	用于管理网关服务证书，包括可信证书链、CSR 请求、证书应答、导入证书、下载证书、查看和停用等功能。
4			网关服务优化策略	用于优化外部应用访问。
5		SSL VPN 服务	VPN 服务管理	用于管理 VPN 服务，包括新增、删除、配置和查看详情等功能。
6			VPN 服务证书	用于管理 VPN 服务证书，包括可信证书链、CSR 请求、证书应答、导入证书、下载证书、查看和停用等功能。
7			VPN 用户	用于管理 VPN 用户，包括添加、删除等功能
8	管理日志审计			用于显示机构用户的操作日志，审计员可以对操作日志进行审核和验签
9	系统管理	用户管理		用户与角色设置、UKEY 绑定等
10		UKEY 管理		备份当前账号下所有数据信息

3.2. 个人中心

点击个人中心，即可跳转到个人中心页面，个人中心包含：

- ✧ 修改别名，手机号码
- ✧ 修改密码
- ✧ 修改 UKEY 的 PIN 码，必须绑定 UKEY 才有该功能显示



3.2.1. 修改密码

点击“修改密码”，会弹出“修改密码”对话框，如图所示：

填写旧密码、新密码和确认密码后点击【确定】按钮，即可完成修改。

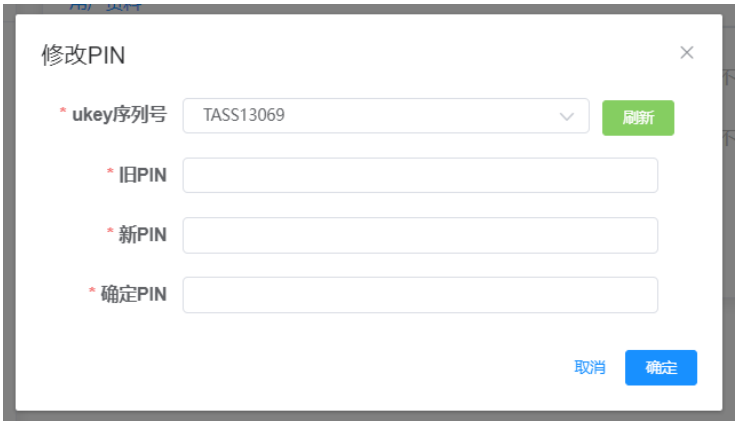
【字段说明】:

✧ 新密码：必填项，输入规则由平台配置里的用户相关安全配置里的密码复杂度决定；

✧ 确认密码：必填项；与新密码一致。

3.2.2. 修改 UKEY 的 PIN 码

点击“修改 UKEY 的 PIN 码”，会弹出“修改 PIN”对话框，如图所示：



选择 ukey 序列号，填写旧 PIN、新 PIN 和确认 PIN 后点击【确定】按钮，即可完成修改。

【字段说明】:

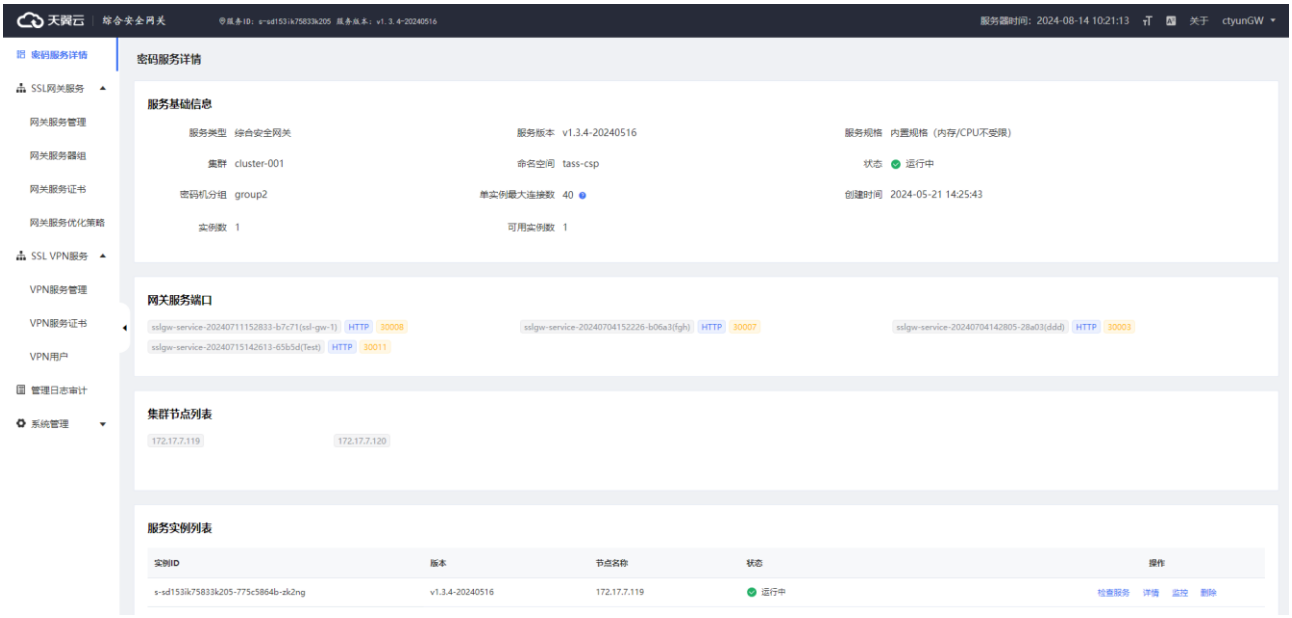
- ✧ Ukey 序列号：必填项，必须插入 ukey 后能修改 PIN 码；
- ✧ 新 PIN：必填项，只能是数字，长度为 4-16 位；
- ✧ 确认 PIN：必填项；与新 PIN 一致。

3.3. 退出登录

点击“退出登录”，然后再点击“确定”后系统会自动退出并跳转到登录页面。

4. 密码服务详情

密码服务详情页面显示密码服务基础信息、网关服务端口、集群节点列表和服务实例列表，密码服务包括：SSL 网关服务和 SSL VPN 服务。服务实例列表可以看到目前实例运行的信息。

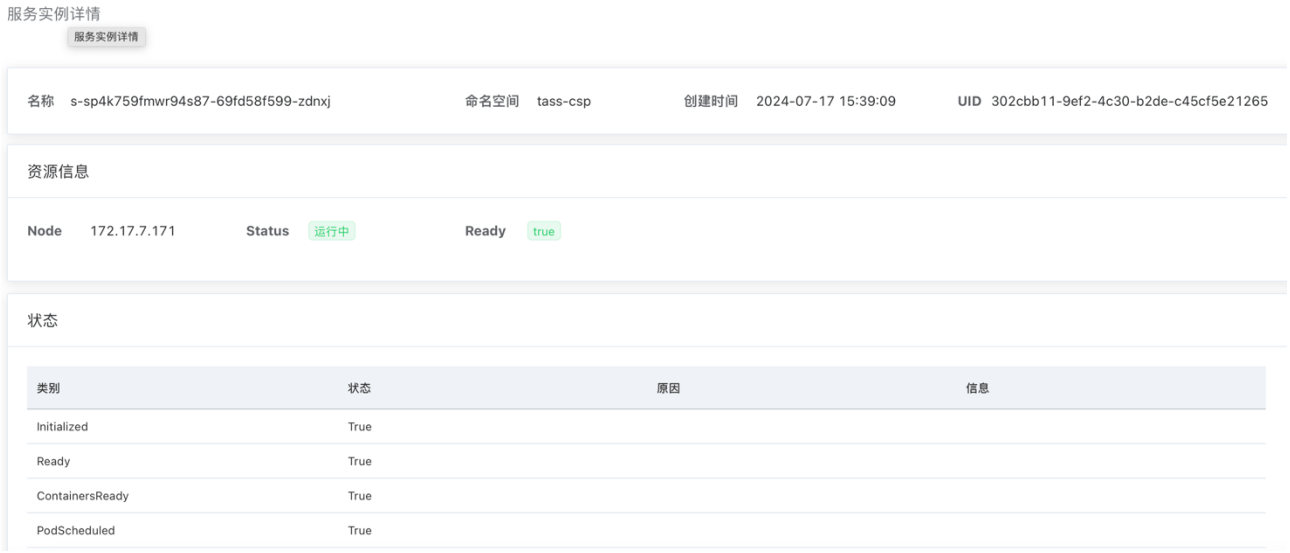


4.1. 检查服务

检查网关是否成功链接平台、完成配置。

4.2. 查看详情

查看服务实例的详情信息。



4.3. 监控

查看服务实例 CPU 使用率、内存以及网络流量。

5. SSL 网关服务

SSL 网关服务，主要分为网关服务管理，网关服务器组，网关服务证书、网关服务优化策略等 4 部分。

5.1. 功能介绍

网关服务管理：用于维护网关服务，提供开通网关服务，删除，配置，查询详情等功能。

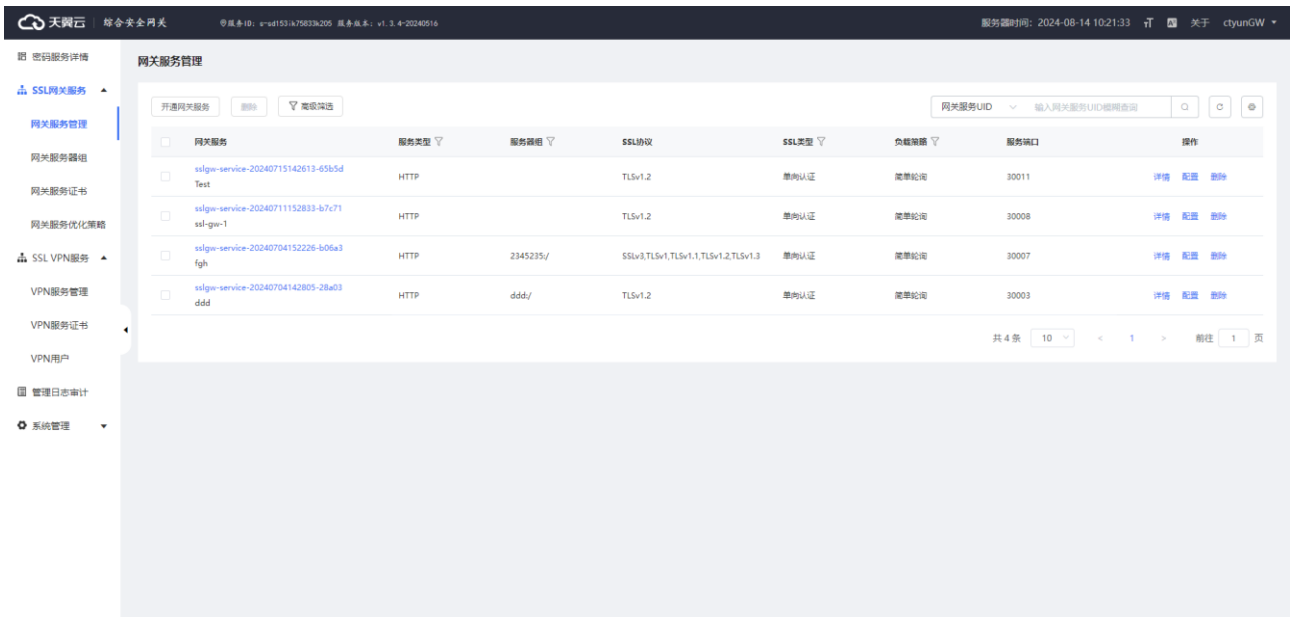
网关服务器组：SSL 网关服务功能的具体实现是由网关服务器实现的，而网关服务器则由网关服务器组统一管理，网关服务与网关服务器组是 1 对 1 的关系，提供服务器组的新增，编辑，删除，查看服务器列表，以及服务器的添加，修改，删除，启用/停用等功能。

网关服务证书：SSL 网关服务使用网关服务证书来进行安全认证工作，使用 SSL 网关服务的前提是必须安装相关网关服务证书，提供新增，查看详情，启用，停用，可信证书链管理，CSR 请求，证书应答，导入证书等功能。

网关服务优化策略：用于优化外部应用访问。

5.2. 网关服务管理

用于维护网关服务，提供新增，删除，配置，查询详情等功能，如图所示：



5.2.1. 新增

操作步骤：

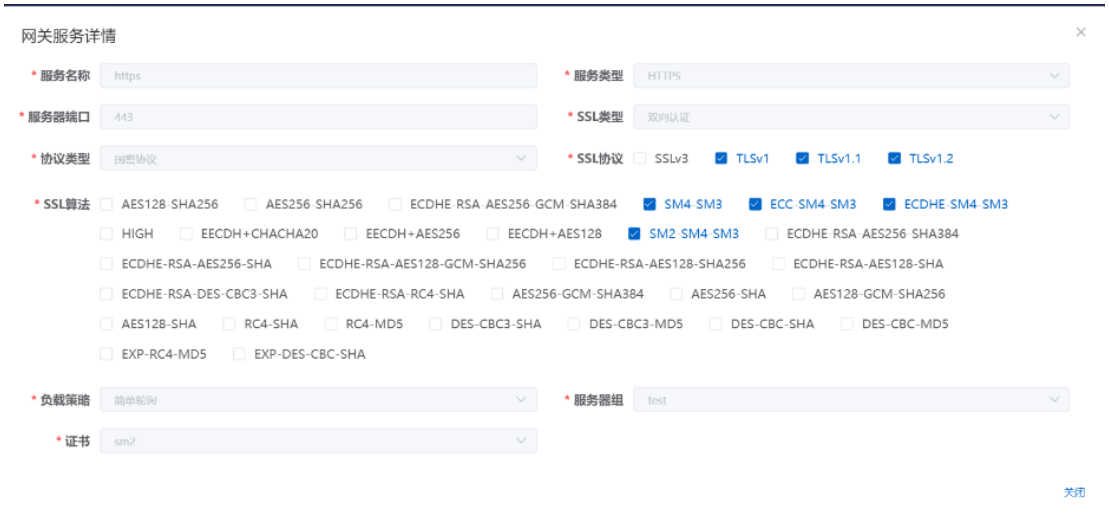
步骤1. 点击左上角的“开通网关服务”，弹出操作框，如图所示：

步骤2. 输入必输项(服务名称，选择服务类型，服务器端口)等。

步骤3. 确认无误后点击“确定”，即可新增成功。

5.2.2. 查看详情

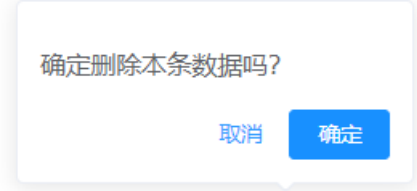
操作步骤：选择网关服务信息，点击右侧的“详情”，弹出操作框，如图所示：



5.2.3. 删除

单选删除，操作步骤：

步骤1. 选择网关服务信息，点击右侧的“删除”按钮，然后弹出操作框，如图所示：



步骤2. 确认后点击“确定”，即可删除成功。

多选删除，操作步骤：

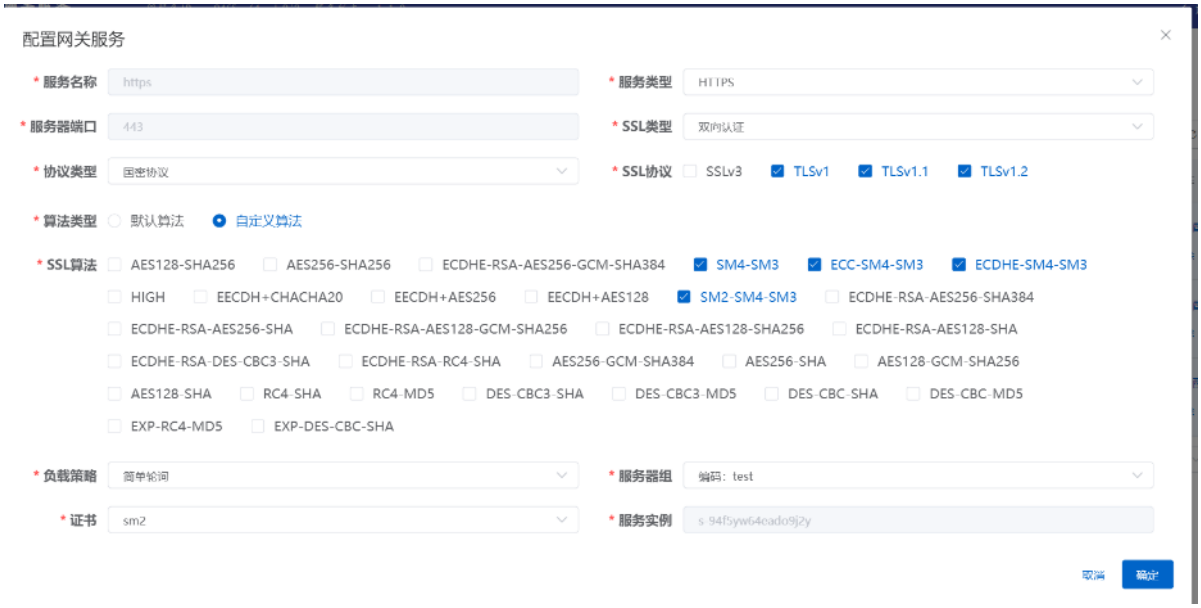
步骤1. 勾选多个网关服务信息，点击下方的“删除”按钮，然后弹出操作框，如图所示：

步骤2. 确认后点击“确定”，即可删除成功。

5.2.4. 配置

操作步骤：

步骤1. 选择网关服务信息，点击右侧的“配置”，弹出操作框，如图所示：

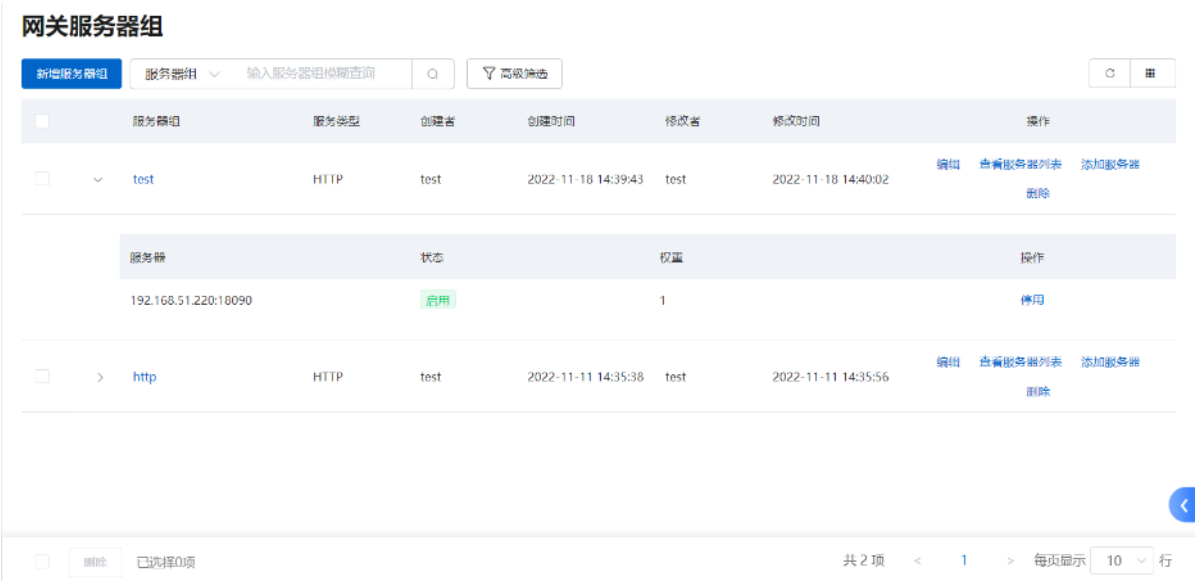


步骤2. 允许配置服务类型，SSL 类型，协议类型，SSL 协议，算法类型，SSL 算法，负载策略，服务器组，证书等，注意：证书是指网关服务证书。

步骤3. 确认无误后点击“确定”，即可配置成功。

5.3. 网关服务器组

SSL 网关服务功能的具体实现是由网关服务器实现的，而网关服务器则由网关服务器组统一管理，网关服务与网关服务器组是 1 对 1 的关系，提供新增，编辑，删除，查看服务器列表，添加服务器等功能，如图所示：



5.3.1. 新增

操作步骤：

步骤1. 点击左上角的“新增服务器组”，弹出操作框，如图所示：

步骤2. 输入必输项(分组名称，服务类型)等。

步骤3. 确认无误后点击“确定”，即可新增成功。

5.3.2. 编辑

操作步骤：

步骤1. 选择服务器组信息，点击右侧的“编辑”，弹出操作框，如图所示：

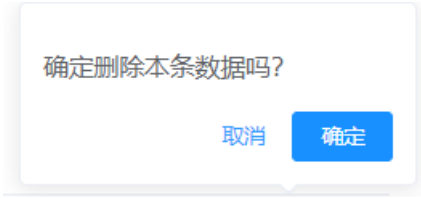
步骤2. 只允许修改分服务类型。

步骤3. 修改后点击“确定”，即可编辑成功。

5.3.3. 删除

单选删除，操作步骤：

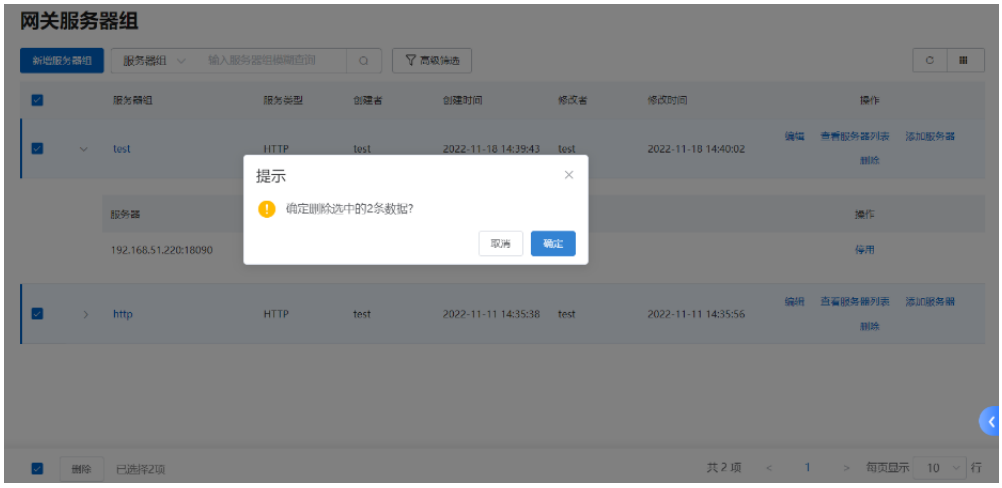
步骤1. 选择服务器组信息，点击右侧的“删除”按钮，然后弹出操作框，如图所示：



步骤2. 确认后点击“确定”，即可删除成功。

多选删除，操作步骤：

步骤1. 勾选多个服务器组信息，点击下方的“删除”按钮，然后弹出操作框，如图所示：



步骤2. 确认后点击“确定”，即可删除成功。

5.3.4. 查看服务器列表

操作步骤：

步骤1. 选择服务器组信息，点击右侧的“查看服务器列表”，即可跳转到网关服务器组详情页面，如图所示：

5.3.5. 添加服务器

操作步骤：

步骤1. 选择服务器组信息，点击右侧的“添加密码机”，弹出操作框，如图所示：

步骤2. 输入必输项(IP，端口，权重，启用)等。

步骤3. 确认无误后点击“确定”，即可添加成功。

5.3.6. 停用服务器

操作步骤：

步骤1. 点击服务器组名称左边的箭头，打开服务器组下方的服务器列表

步骤2. 选择服务器列表中的服务器信息，点击右侧的“停用”，弹出操作框，如图所示：

步骤3. 确认无误后点击“确定”，即可停用成功。

5.3.7. 启用服务器

操作步骤：

步骤1. 点击服务器组名称左边的箭头，打开服务器组下方的服务器列表

步骤2. 选择服务器列表中的服务器信息，点击右侧的“启用”，弹出操作框，如图所示：

步骤3. 确认无误后点击“确定”，即可启用成功。

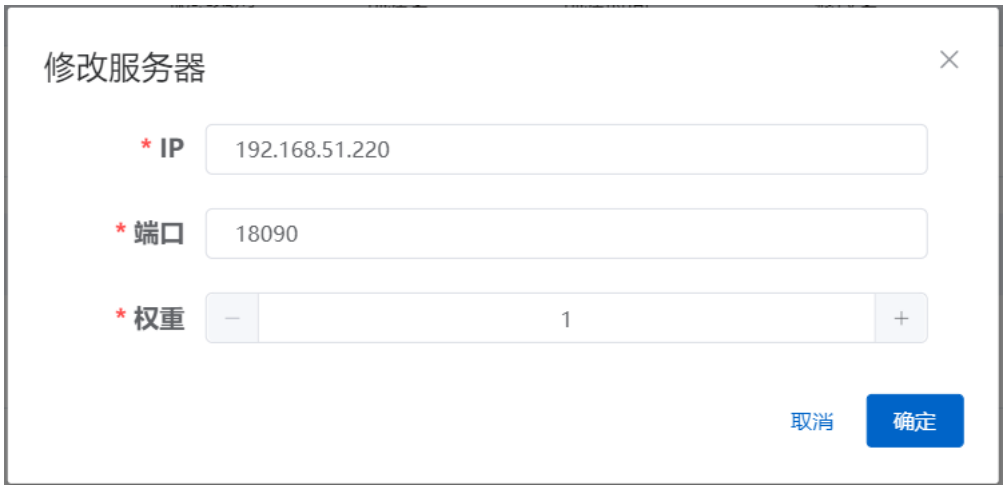
5.3.8. 修改服务器

注意：服务器必须停用后才能修改。

操作步骤：

步骤1. 点击服务器组名称左边的箭头，打开服务器组下方的服务器列表

步骤2. 选择服务器列表中的服务器信息，点击右侧的“修改”，弹出操作框，如图所示：



步骤3. 确认无误后点击“确定”，即可修改成功。

5.3.9. 删除服务器

注意：服务器必须停用后才能删除。

操作步骤：

步骤1. 点击服务器组名称左边的箭头，打开服务器组下方的服务器列表

步骤2. 选择服务器列表中的服务器信息，点击右侧的“删除”，弹出操作框，如图所示：

步骤3. 确认无误后点击“确定”，即可删除成功。

5.4. 网关服务证书

SSL 网关服务使用网关服务证书来进行安全认证工作，使用 SSL 网关服务的前提是必须安装相关网关服务证书，提供新增，查看详情，启用，停用，可信证书链管理，CSR 请求，证书应答，导入证书等功能，如图所示：

注意：当证书生成了 CSR 请求，然后又还没证书应答时，密钥信息会显示红色圆点。

5.4.1. 新增证书

操作步骤：

步骤1. 点击左上角的“新增证书”，弹出操作框，如图所示：

步骤2. 输入必输项(证书标识名，证书算法)等。

步骤3. 确认无误后点击“确定”，即可新增成功。

5.4.2. 查看证书

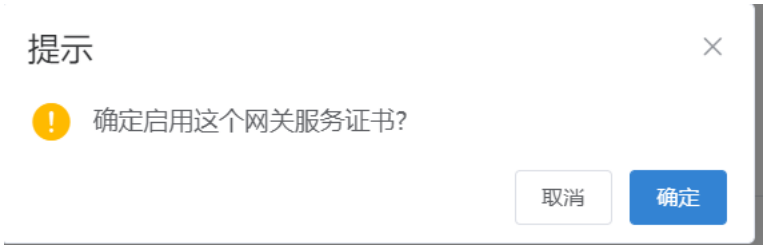
操作步骤：

步骤1. 选择证书信息，点击右侧的“查看”，即可跳转到证书详情页面，如图所示：

5.4.3. 启用

操作步骤：

步骤1. 选择网关服务证书信息，点击右侧的“启用”，弹出操作框，如图所示：

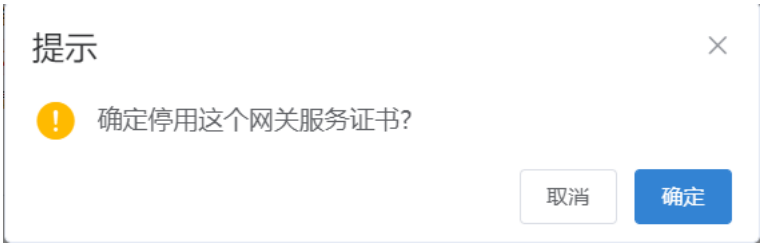


步骤2. 确认后点击“确定”，即可启用成功。

5.4.4. 停用

操作步骤：

步骤1. 选择网关服务证书信息，点击右侧的“停用”，弹出操作框，如图所示：



步骤2. 确认后点击“确定”，即可停用成功。

5.4.5. 可信证书链

网关服务证书的可信证书链，需要在选择网关服务证书信息后，点击右侧的“可信证书链”，然后再弹出的操作框里进行添加，删除，下载等操作。如图所示：

5.4.5.1. 添加可信证书

操作步骤：

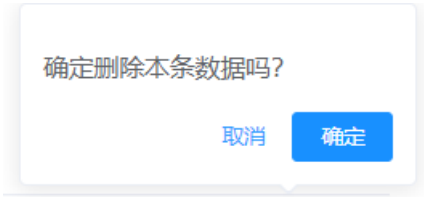
步骤1. 点击左上角的“添加可信证书”，弹出操作框，如图所示：

步骤2. 上传证书文件，确认后点击“确定”，即可添加成功。

5.4.5.2. 删除可信证书

单选删除，操作步骤：

步骤1. 选择可信证书信息，点击右侧的“删除”按钮，然后弹出操作框，如图所示：



步骤2. 确认后点击“确定”，即可删除成功。

5.4.5.3. 下载可信证书

操作步骤：

步骤1. 选择可信证书信息，点击右侧的“下载证书”，即可直接下载，结果如图所示：

5.4.6. CSR 请求

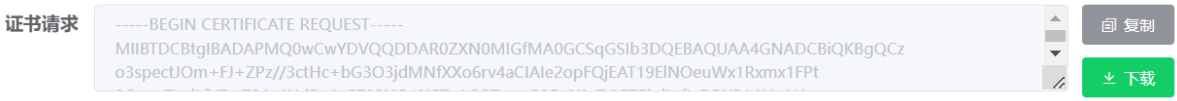
操作步骤：

步骤1. 选择证书信息，点击右侧的“CSR 请求”，弹出操作框，如图所示：

步骤2. 输入必输项(密钥长度，请求签名算法，公钥指数，主题格式，通用名 CN)等，

步骤3. 确认无误后点击“生成证书请求”，即可生成成功。

步骤4. 生成成功后，证书请求数据会回显在证书请求输入框里，如图所示：



5.4.7. 证书应答

操作步骤：

步骤1. 选择已经生成请求的证书信息，点击右侧的“证书应答”，弹出操作框，如图所示：

步骤2. 只能上传证书文件。

步骤3. 上传完后点击“导入证书”，即可应答成功。

5.4.8. 导入证书

操作步骤：

步骤1. 选择网关服务证书信息，点击右侧的“导入证书”，弹出操作框，如图所示：

步骤2. 注意：如果当前网关服务证书已有私钥数据(即已上传证书或生产 CSR 请求后)，会有覆盖已有私钥数据的提示，如上图顶部红色字体提示。

步骤3. 选择设置方法，上传证书文件和私钥文件。

步骤4. 确认后点击“保存”，即可导入成功。

5.5. 网关服务优化策略

显示网关服务优化策略，优化外部应用访问。

5.5.1. 新增优化策略

操作步骤：

步骤1. 点击左上角的“新增优化策略”，弹出操作框，如图所示：

步骤2. 输入必输项(策略名)等。

步骤3. 确认无误后点击“确定”，即可新增成功。

5.5.2. 查看详情

操作步骤：选择策略名信息，点击右侧的“详情”，弹出操作框，如图所示：

5.5.3. 编辑

操作步骤：选择策略名信息，点击右侧的“编辑”，弹出操作框，如图所示：

可以修改策略名以外的其他信息，修改完点击“确定”即修改完毕。

6. SSL VPN 服务

SSL VPN 服务，主要分为 VPN 服务管理，VPN 服务证书，VPN 用户等 3 部分。

6.1. 功能介绍

VPN 服务管理：用于维护 VPN 服务，提供配置 VPN 服务；对内网控制新增和删除；对静态路由表的新增，修改，删除等功能。

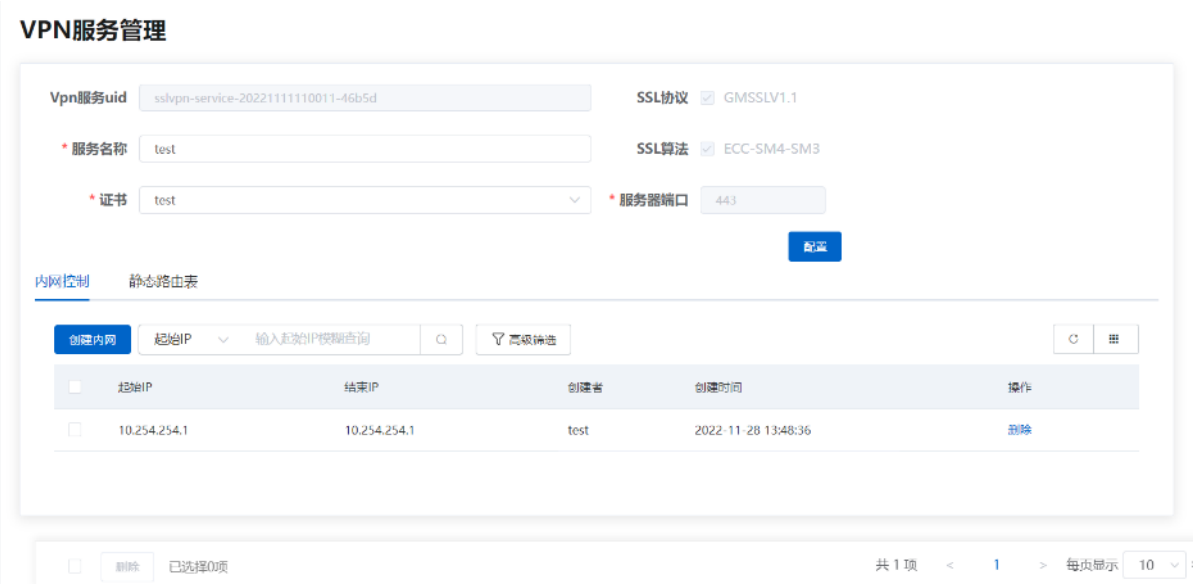
VPN 服务证书：SSL VPN 服务使用 VPN 服务证书来进行安全认证工作，使用 SSL VPN 服务的前提是必须安装相关 VPN 服务证书，提供新增，查看详情，启用，停用，可信证书链管理，CSR 请求，证书应答，导入证书等功能。

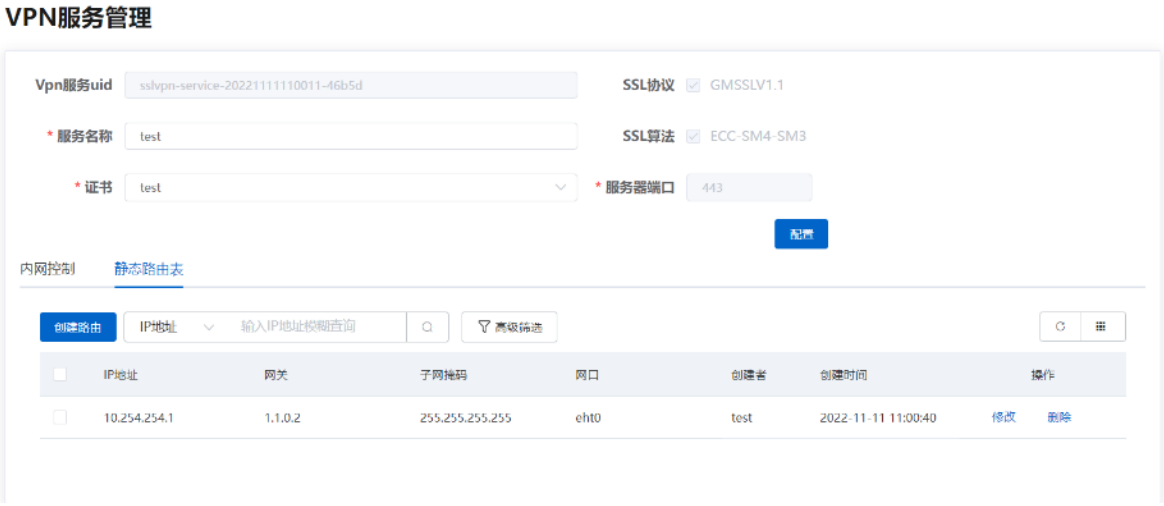
VPN 用户：提供对 VPN 网关的用户进行统一管理，支持新增，编辑，删除，启用/停用等功能。

6.2. VPN 服务管理

用于维护 VPN 服务，内网控制，静态路由表等数据；提供配置 VPN 服务；对内网控制新增和删除；对静态路由表的新增，修改，删除等功能，注意：在首次进入 VPN 服务管理时，会有提示，如图所示：

点击右上角的“配置”，即可进入配置页面，如图所示：

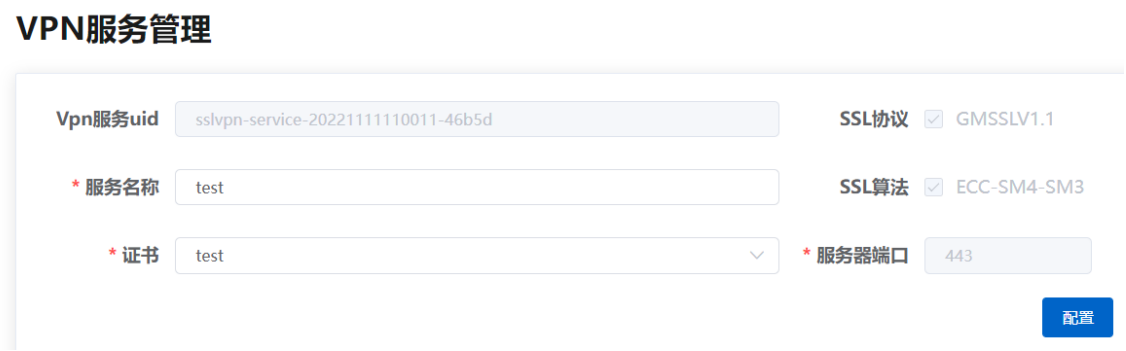




6.2.1. 配置 VPN 服务

操作步骤：

步骤1. 首先需要有证书，这里的证书指的是 VPN 服务证书，然后输入服务名称，最后点击“配置”即可完成 VPN 服务的配置，如图所示：



6.2.2. 新增内网控制

操作步骤：

步骤1. 点击内网控制列表的左上角“创建内网”按钮，弹出操作框，如图所示：

步骤2. 可以输入 IP 地址或 IP 网段。

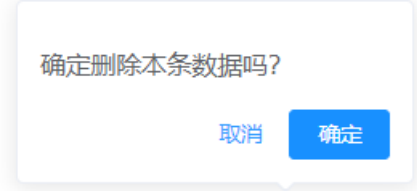
步骤3. 选择 IP 格式，然后输入 IP 地址或起始 IP，结束 IP 等。

步骤4. 确认无误后点击“确定”，即可新增成功。

6.2.3. 删除内网控制

单选删除，操作步骤：

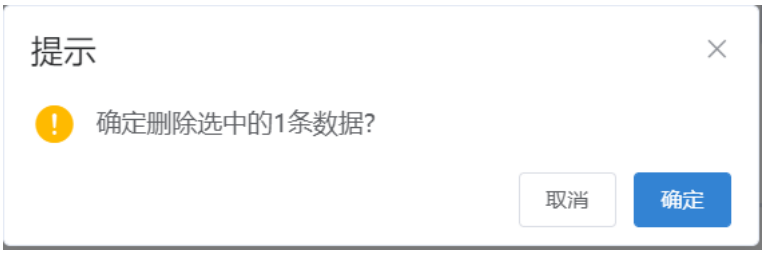
步骤1. 选择内网控制信息，点击右侧的“删除”按钮，然后弹出操作框，如图所示：



步骤2. 确认后点击“确定”，即可删除成功。

多选删除，操作步骤：

步骤1. 勾选多个内网控制信息，点击下方的“删除”按钮，然后弹出操作框，如图所示：



步骤2. 确认后点击“确定”，即可删除成功。

6.2.4. 新增静态路由

操作步骤：

步骤1. 点击中间的“静态路由表”tab 页，切换到静态路由表页面。

步骤2. 然后点击列表左上角的“创建路由”，弹出操作框，如图所示：

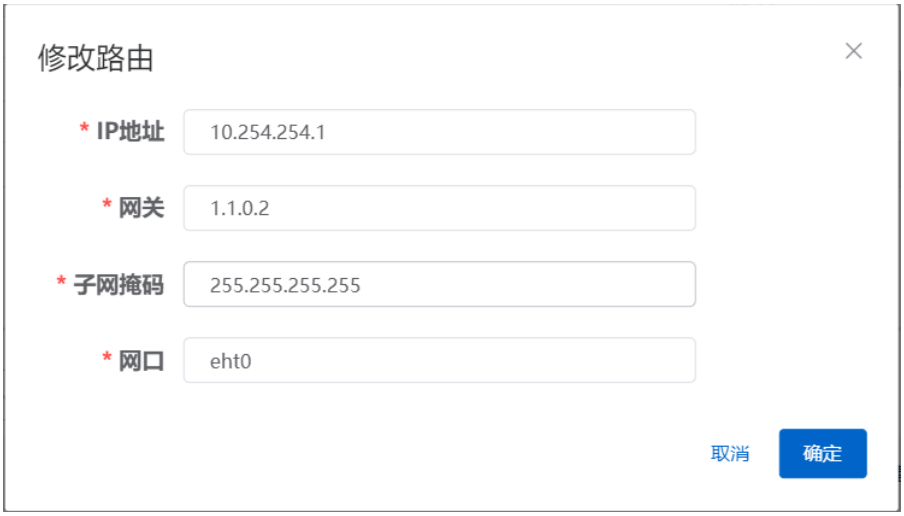
步骤3. 输入必输项(IP 地址，网关，子网掩码，网口，选择添加位置)等。

步骤4. 确认无误后点击“确定”，即可新增成功。

6.2.5. 修改静态路由

操作步骤：

步骤1. 选择静态路由信息，点击其右侧的“修改”，弹出操作框，如图所示：



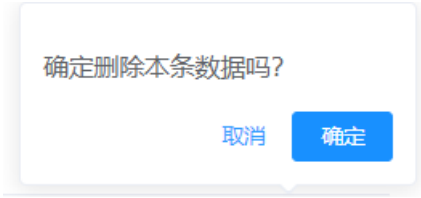
步骤2. 可修改项包括：IP 地址，网关，子网掩码，网口等。

步骤3. 确认无误后点击“确定”，即可修改成功。

6.2.6. 删除静态路由

单选删除，操作步骤：

步骤1. 选择静态路由信息，点击右侧的“删除”按钮，然后弹出操作框，如图所示：



步骤2. 确认后点击“确定”，即可删除成功。

6.3. VPN 服务证书

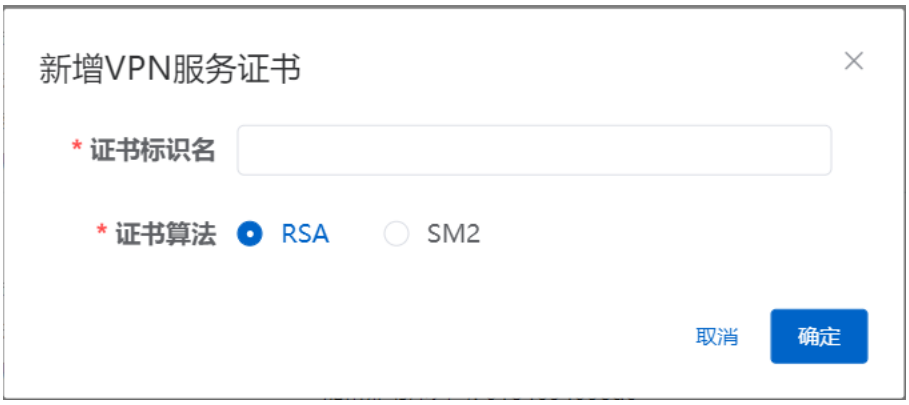
SSL VPN 服务使用 VPN 服务证书来进行安全认证工作，使用 SSL VPN 服务的前提是必须安装相关 VPN 服务证书，提供新增，查看详情，启用，停用，可信证书链管理，CSR 请求，证书应答，导入证书等功能，如图所示：

注意：当证书生成了 CSR 请求，然后又还没证书应答时，证书信息会显示红色圆点。

6.3.1. 新增证书

操作步骤：

步骤1. 点击左上角的“新增证书”，弹出操作框，如图所示：



步骤2. 输入必输项(证书标识名，证书算法)等。

步骤3. 确认无误后点击“确定”，即可新增成功。

6.3.2. 查看证书

操作步骤：

步骤1. 选择 VPN 服务证书信息，点击右侧的“查看”，即可跳转到网关服务证书详情页面，如图所示：

6.3.3. 启用

操作步骤：

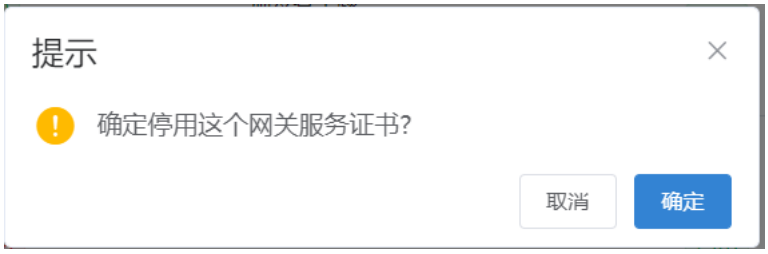
步骤1. 选择 VPN 服务证书信息，点击右侧的“启用”，弹出操作框，如图所示：

步骤2. 确认后点击“确定”，即可启用成功。

6.3.4. 停用

操作步骤：

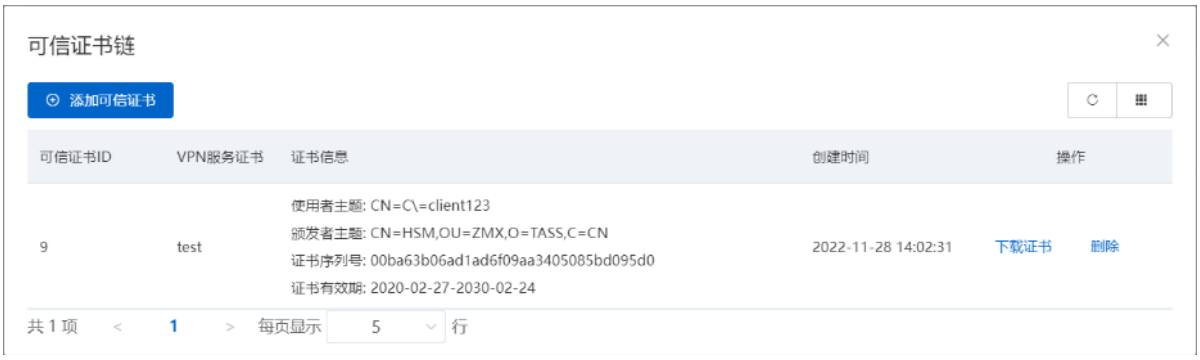
步骤1. 选择 VPN 服务证书信息，点击右侧的“停用”，弹出操作框，如图所示：



步骤2. 确认后点击“确定”，即可停用成功。

6.3.5. 可信证书链

VPN 服务证书的可信证书链，需要在选择 VPN 服务证书信息后，点击右侧的“可信证书链”，然后再弹出的操作框里进行添加，删除，下载等操作。如图所示：



6.3.5.1. 添加可信证书

操作步骤：

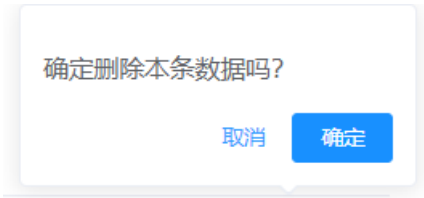
步骤1. 点击左上角的“添加可信证书”，弹出操作框，如图所示：

步骤2. 上传证书文件，确认后点击“确定”，即可添加成功。

6.3.5.2. 删除可信证书

单选删除，操作步骤：

步骤1. 选择可信证书信息，点击右侧的“删除”按钮，然后弹出操作框，如图所示：

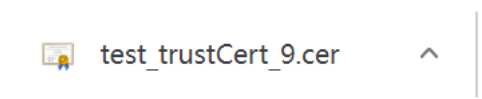


步骤2. 确认后点击“确定”，即可删除成功。

6.3.5.3. 下载可信证书

操作步骤：

步骤1. 选择可信证书信息，点击右侧的“下载证书”，即可直接下载，结果如图所示：



6.3.6. CSR 请求

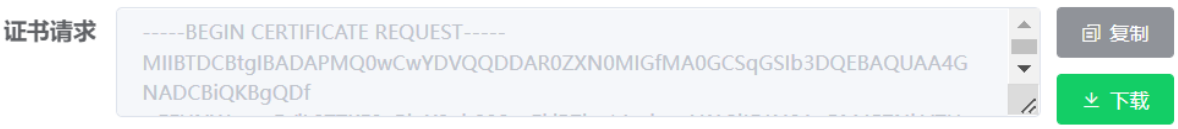
操作步骤：

步骤1. 选择 VPN 服务证书信息，点击右侧的“CSR 请求”，弹出操作框，如图所示：

步骤2. 输入必输项(密钥长度，请求签名算法，公钥指数，请求签名算法，主题格式，通用名 CN)等，

步骤3. 确认无误后点击“生成证书请求”，即可生成成功。

步骤4. 生成成功后，证书请求数据会回显在证书请求输入框里，如图所示：



6.3.7. 证书应答

操作步骤：

步骤1. 选择 VPN 服务证书信息，点击右侧的“证书应答”，弹出操作框，如图所示：

步骤2. 只能上传证书文件。

步骤3. 上传完后点击“导入证书”，即可应答成功。

6.3.8. 导入证书

操作步骤：

步骤1. 选择 VPN 服务证书信息，点击右侧的“导入证书”，弹出操作框，如图所示：

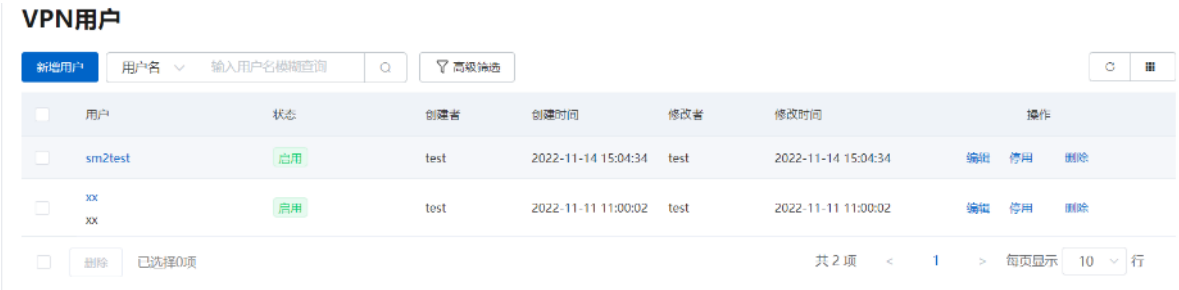
步骤2. 注意：如果当前 VPN 服务证书已有私钥数据(即已上传证书或生产 CSR 请求后)，会有覆盖已有私钥数据的提示，如上图顶部红色字体提示。

步骤3. 选择设置方法，上传证书文件和私钥文件。

步骤4. 确认后点击“保存”，即可导入成功。

6.4. VPN 用户

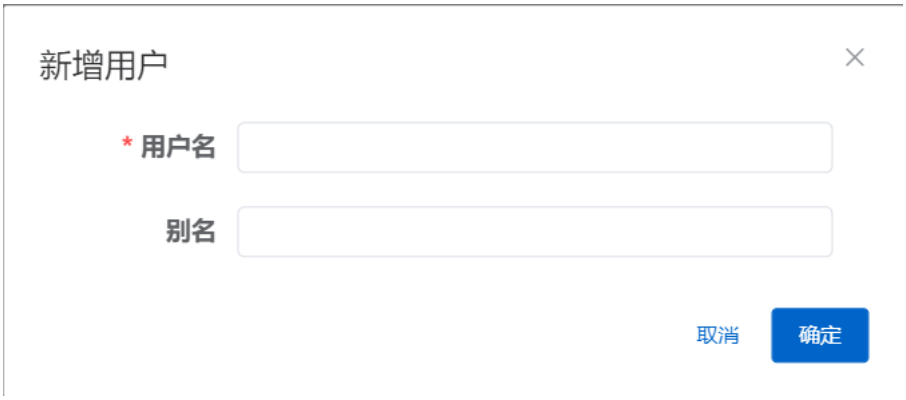
SSL VPN 提供了 VPN 用户管理的功能，只要在用户列表中的用户都可以使用 VPN 服务，提供新增，编辑，删除，启用，停用等功能，如图所示：



6.4.1. 新增

操作步骤：

步骤1. 点击左上角的“新增用户”，弹出操作框，如图所示：



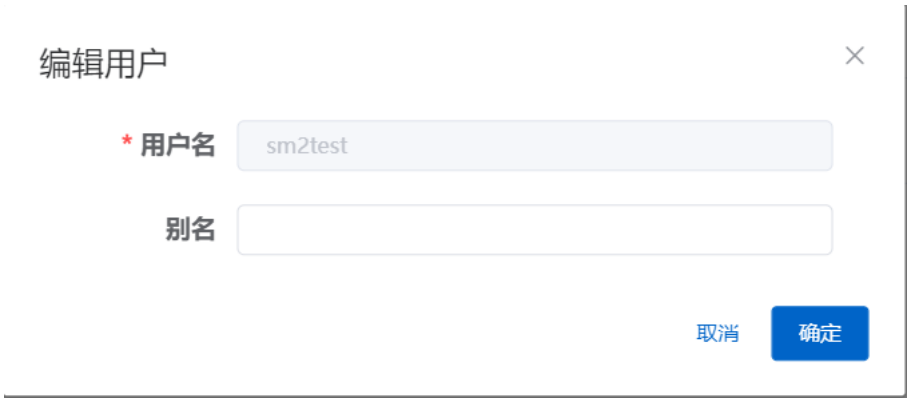
步骤2. 输入必输项用户名。

步骤3. 确认无误后点击“确定”，即可新增成功。

6.4.2. 编辑

操作步骤：

步骤1. 选择用户组信息，点击右侧的“编辑”，弹出操作框，如图所示：



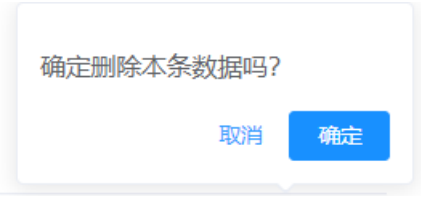
步骤2. 只允许修改别名。

步骤3. 修改后点击“确定”，即可编辑成功。

6.4.3. 删除

单选删除，操作步骤：

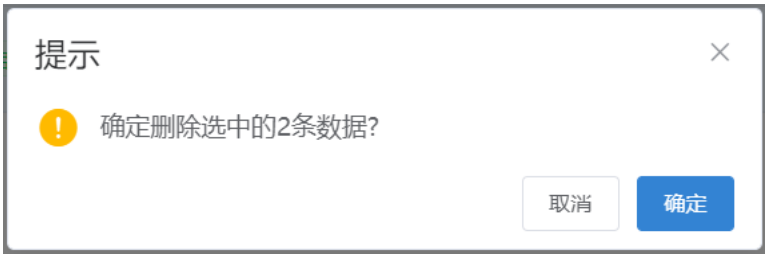
步骤1. 选择用户组信息，点击右侧的“删除”按钮，然后弹出操作框，如图所示：



步骤2. 确认后点击“确定”，即可删除成功。

多选删除，操作步骤：

步骤1. 勾选多个用户组信息，点击左下角的“删除”按钮，然后弹出操作框，如图所示：

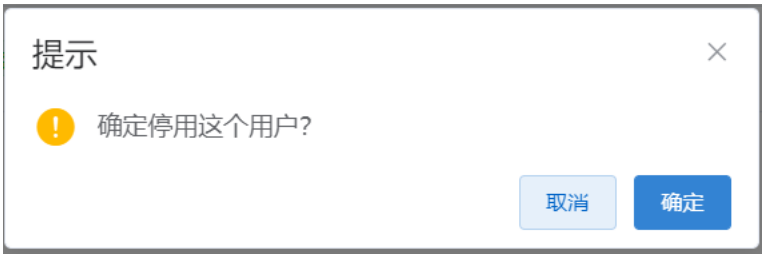


步骤2. 确认后点击“确定”，即可删除成功。

6.4.4. 停用

操作步骤：

步骤1. 选择用户信息，点击右侧的“停用”按钮，然后弹出操作框，如图所示：

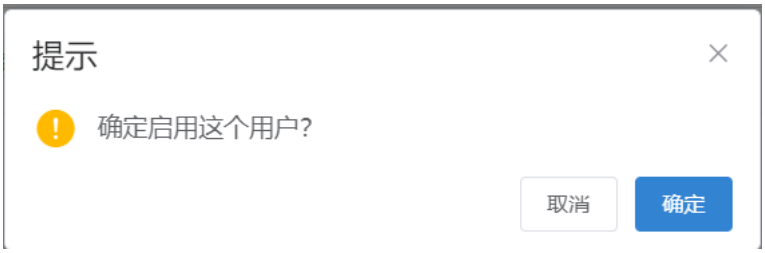


步骤2. 确认后点击“确定”，即可停用成功。

6.4.5. 启用

操作步骤：

步骤1. 选择用户信息，点击右侧的“启用”按钮，然后弹出操作框，如图所示：



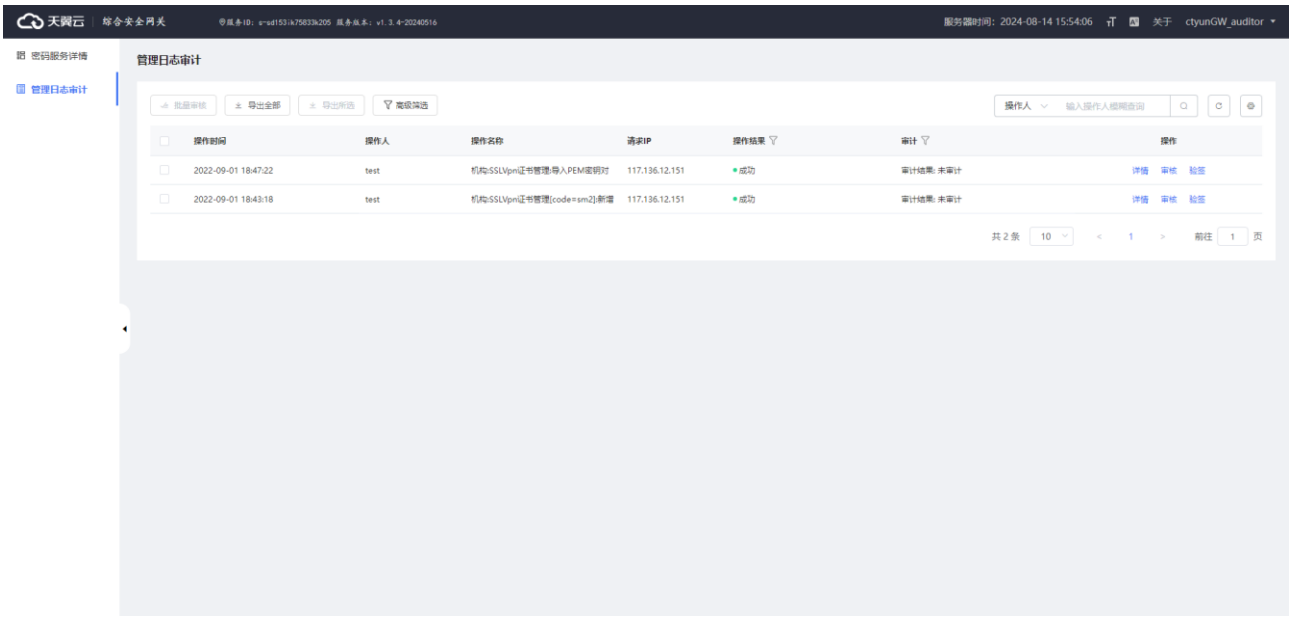
步骤2. 确认后点击“确定”，即可启用成功。

7. 管理日志审计

用户操作审计，记录了当前机构用户的管理操作日志。提供查看详情，审核，批量审核，验签等功能。

7.1. 机构用户操作审计

记录机构用户的操作日志，并提供查看详情，审核，批量审核，验签等功能，如图所示：



7.1.1. 查看详情

操作步骤：选择机构用户操作信息，点击右侧的“详情”，弹出操作框，如图所示：

7.1.2. 审核

操作步骤：

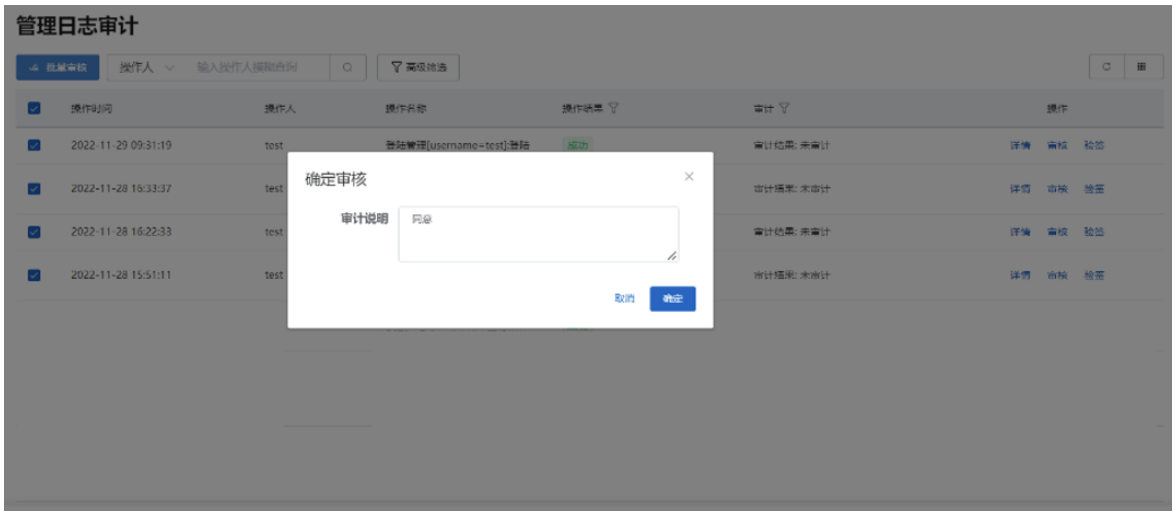
步骤1. 选择机构用户操作日志，点击右侧的“审核”，弹出操作框，如图所示：

步骤2. 输入审计说明后点击“确定”，即可审核成功。

7.1.3. 批量审核

操作步骤：

步骤1. 勾选机构用户多条操作信息，点击左上角的“批量审核”，弹出操作框，如图所示：



步骤2. 输入审计说明后点击“确定”，即可批量审核成功。

7.1.4. 验签

操作步骤：选择机构用户操作日志，点击右侧的“验签”，即可验签成，结果会在右上角显示，如图所示：


验证成功

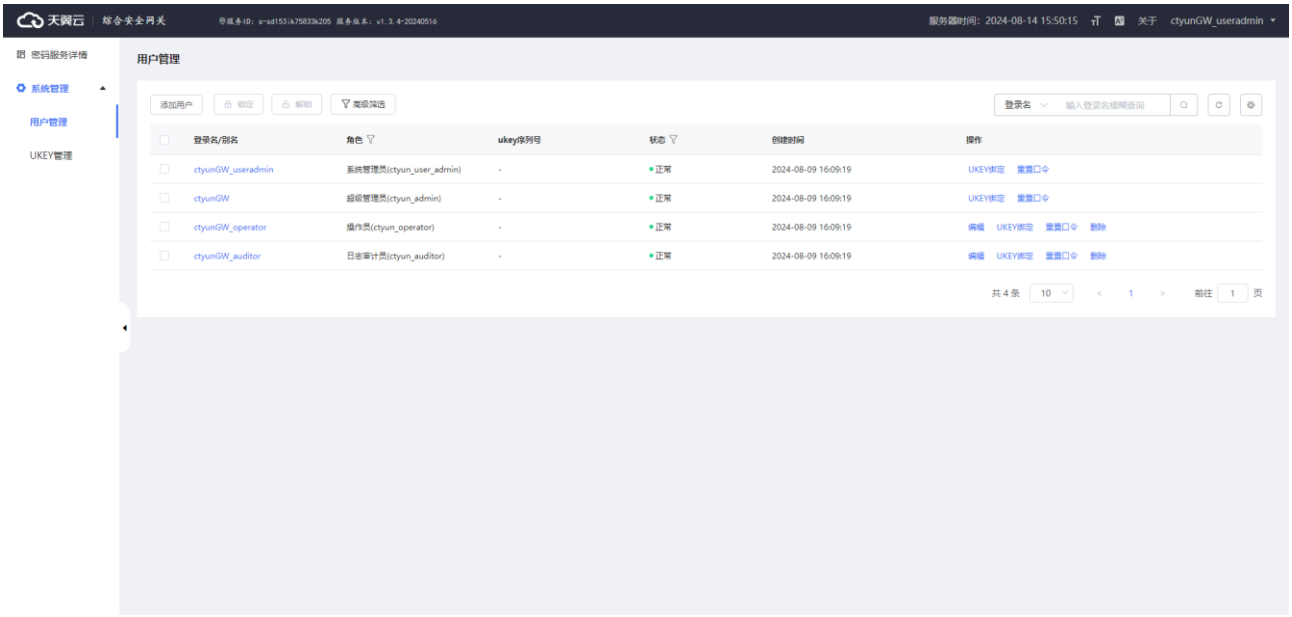
8. 系统管理

8.1. 功能介绍

机构用户操作系统管理，实现当前机构的用户身份设置,如：添加用户、绑定 Ukey、重置等功能，以及实现当前机构的 Ukey 管理，如：Ukey 初始化和 Ukey 信息的查询。

8.2. 用户管理

管理当前机构下所有用户信息，提供新增、编辑、Ukey 绑定、重置等功能，如图所示：



8.2.1. 添加用户

操作步骤：

步骤1. 点击左上角的“添加用户”按钮，弹出操作框，如图所示：

步骤2. 输入用户相关信息，其中登录名和角色是必填项

步骤3. 点击确定按钮，用户添加成功

步骤4. 注：角色列表来源于平台的角色配置和系统默认的角色

8.2.2. 编辑用户

操作步骤：

步骤1. 选择用户数据，点击右侧的“编辑”，弹出操作框，如图所示

步骤2. 输入此次编辑的相关信息(登录名置灰不可改，角色可更新必填)，点击确定按钮，编辑成功

8.2.3. UKEY 绑定

操作步骤：

步骤1. 选择用户数据，点击右侧的“UKEY 绑定”，弹出操作框，如图所示

步骤2. 选择绑定 UKEY 信息，输入 pin 码，点击绑定 UKEY，绑定成功

8.2.4. UKEY 解绑

操作步骤：

步骤1. 选择用户数据，点击右侧的“UEKY 解绑”，弹出操作框，如图所示

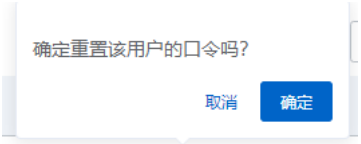
步骤2. 输入 pin 码，点击解绑 UKEY，解绑成功

注：UEKY 解绑的前提，需要当前用户已绑定 UKEY 信息

8.2.5. 重置口令

操作步骤：

步骤1. 选择用户数据，点击右侧的“重置口令”，弹出操作框，如图所示



步骤2. 点击确定按钮，重置口令成功

8.2.6. 删除

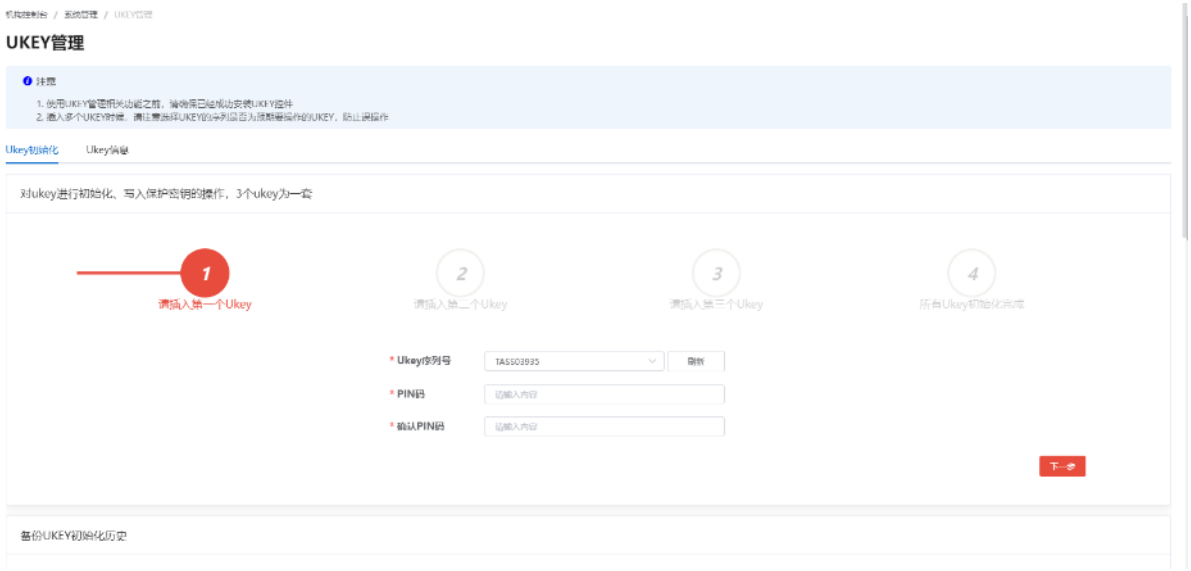
操作步骤：

步骤1. 选择用户数据，点击右侧的“删除”，弹出操作框，如图所示

步骤2. 点击确定按钮，删除成功

8.3. UKEY 管理

提供 UKEY 管理的相关功能，如：Ukey 初始化、ukey 信息查询和备份历史查询等，具体展示如图所示：



8.3.1. Ukey 初始化

8.3.1.1. 功能介绍

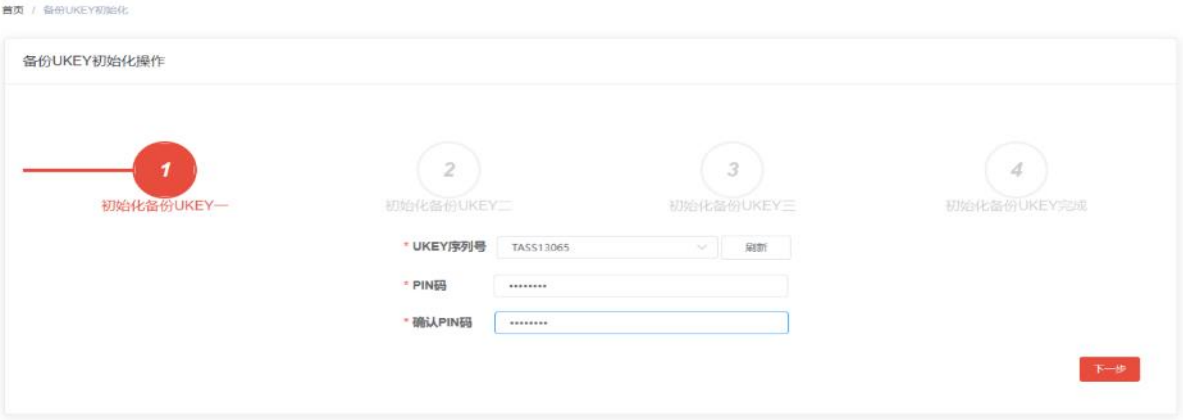
备份 UKEY 初始化，提供初始化备份 UKEY 的功能。备份 UKEY 用于密码服务的备份和恢复功能。

8.3.1.2. 备份 UKEY 初始化

如图所示：

操作步骤：

步骤3. 插入备份 UKEY 一，然后点击 UKEY 序列号右侧的“刷新”按钮(必须刷新，否则不会出现 UKEY 序列号选项)，如图所示：

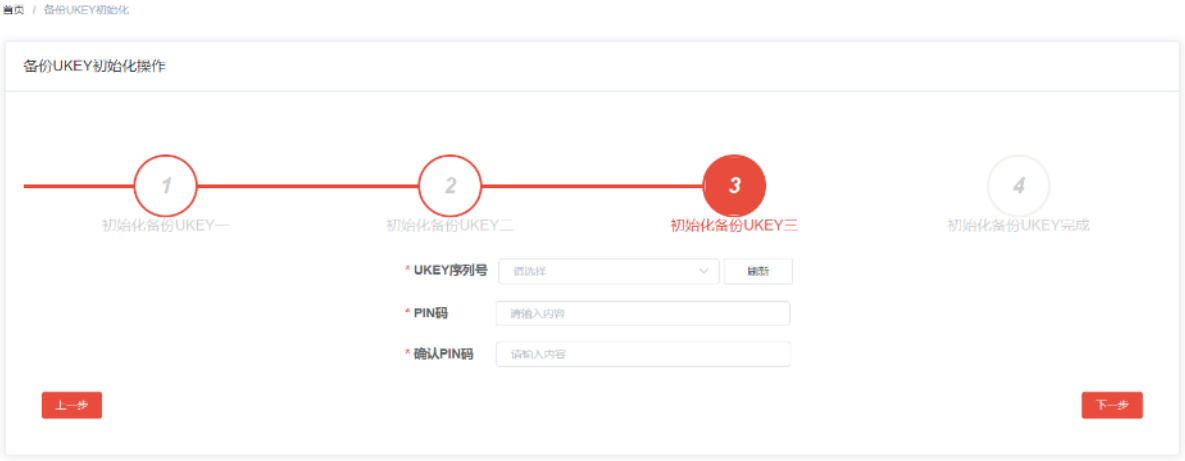


步骤4. 选择 UKEY 序列号，输入 PIN 码，确认 PIN 码。

步骤5. 确认无误后，点击“下一步”。

步骤6. 接着插入备份 UKEY 二，备份 UKEY 三。

步骤7. 重复步骤 1，2，3。

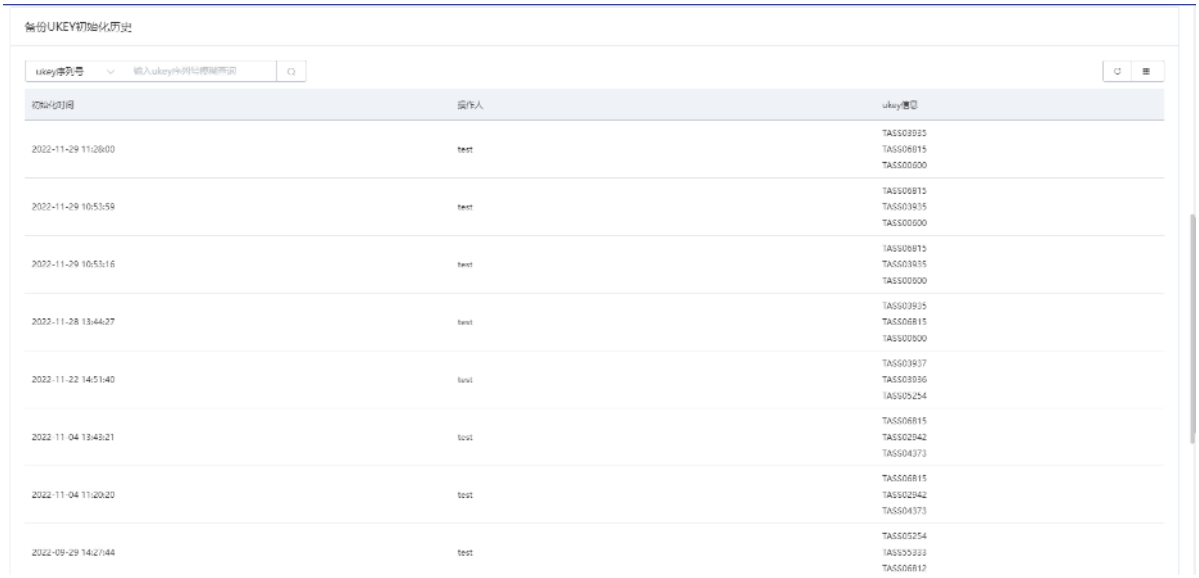


步骤8. 直到最后初始化完成，如图所示：

8.3.1.3. 备份 Ukey 初始化历史

操作步骤：

步骤1. 进入到 Ukey 初始化页面，滑动到页面底部，展示当前机构备份 Ukey 初始化历史列表，如图所示：



步骤2. 输入 ukey 序列号或操作人，点击搜索按钮，可以搜索到匹配的初始化记录。

8.3.2. Ukey 信息

8.3.2.1. 功能介绍

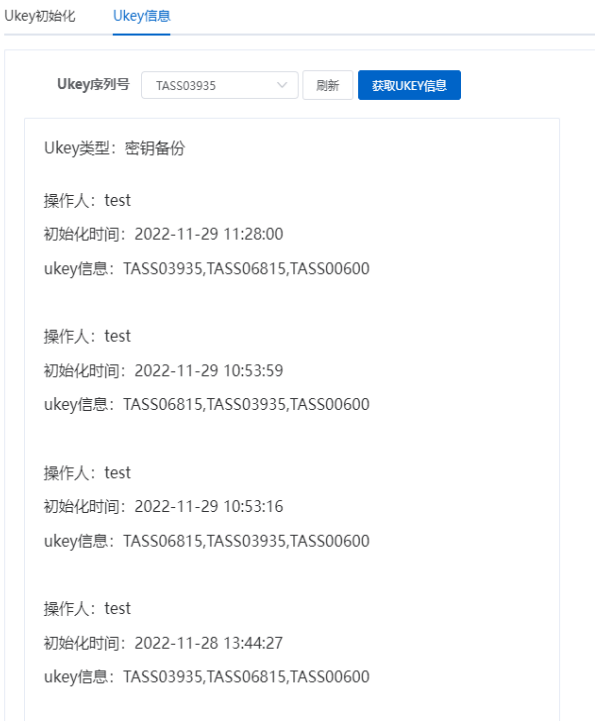
Ukey 信息，提供 UKEY 信息查询功能和 PIN 修改功能。

8.3.2.2. 获取 Ukey 信息

操作步骤：

步骤1. 进入到 Ukey 信息页面，插入后选择所要获取的 Ukey 序列号，点击获取 UKEY 信息，弹出弹窗如图所示：

步骤2. 输入 PIN 码，点击查询，展示 UKEY 相关信息，如图所示：



8.3.2.3. 修改 PIN 码

操作步骤：

步骤1. 进入到 Ukey 信息页面，插入 Ukey 后选择所要修改 PIN 码的序列号，输入旧 PIN 码、新 PIN 码和确认新 PIN 码，如图所示：

步骤2.　点击提交按钮，更新成功，旧 PIN 码失效，新 PIN 码生效