

签名验签服务器

用户手册

格尔软件股份有限公司

2022年1月

目录

第一章 手册指南	11
1.1. 概述.....	11
1.2. 目的.....	11
1.3. 适用范围.....	11
1.4. 适用对象.....	11
1.5. 名词解释.....	11
1.6. 必读声明.....	12
第二章 产品简介	13
2.1. 主要功能.....	13
第三章 登录服务器.....	13
3.1. 登录系统.....	13
3.2. 更改密码.....	18
3.3. 退出登录.....	19
第四章 快速部署	19
4.1. 单机模式.....	19
4.1.1. 修改 IP	19
4.1.2. 启动加密设备	20
4.1.2.1. 启动加密卡.....	20
4.1.2.2. 启动加密机.....	21
4.1.3. 配置证书链黑名单及服务证书链	21
4.1.4. 配置证书信息（申请证书、导入证书、导入证书白名单）	24
4.2. 统一管理模式.....	27
4.2.1. 修改 IP	27
4.2.2. 启动加密设备	28
4.2.3. 修改运行模式	28
4.2.4. 添加本机	29
4.2.5. 从机修改运行模式	29
4.2.6. 管理节点添加工作节点	29
4.2.7. 配置证书链黑名单及服务证书链	30
4.2.8. 配置证书信息（申请证书、导入证书、导入证书白名单）	30
4.2.9. 数据发布及同步	30

第五章 CA 信息管理	31
5.1. 添加 CA 信息	33
5.2. 查看导出 CA 证书	34
5.3. 删除 CA 信息	34
5.4. 配置黑名单	36
5.4.1. LDAP 配置	37
5.4.2. HTTP 配置	38
5.4.3. OCSP 配置	38
第六章 服务管理	39
6.1. 添加	39
6.2. 删除	40
6.3. 配置服务	40
6.4. 退出服务配置	41
第七章 证书管理	41
7.1. 我的证书申请管理	42
7.1.1. 生成证书请求	42
7.1.2. 导出证书请求	45
7.1.3. 申请证书	46
7.1.4. 导入证书	46
7.1.5. 删除证书请求	47
7.1.6. 查询证书请求	47
7.2. 我的证书列表	48
7.2.1. 查看我的证书	48
7.2.2. 编辑我的证书	48
7.2.3. 查询我的证书	49
7.2.4. 删除我的证书	49
7.2.5. 重置操作码	49
7.2.6. 导入 pfx 证书	50
7.3. 我的白名单	50
7.3.1. 导入证书	51
7.3.2. 编辑别名	52
7.3.3. 删除	52
7.3.4. 导出	53

7.3.5. 详细信息	53
第八章 服务 CA 信息管理	54
8.1. 选择 CA	54
8.2. 添加 CA	55
8.3. 删除 CA	56
8.4. 查看 CA/配置黑名单	56
第九章 服务日志	57
9.1. 服务日志	57
第十章 服务策略管理	58
10.1. 证书白名单策略	58
10.2. 签名策略	60
第十一章 时间服务器	60
11.1. 时间服务管理	60
第十二章 日志查看	61
12.1. 操作日志	61
12.2. 登录日志	62
第十三章 系统管理	62
13.1. 网络管理	63
13.2. 加密设备管理	64
13.2.1. 硬件设备加密卡管理	64
13.2.1.1. 启用加密设备	64
13.2.1.2. 停用加密设备	64
13.2.1.3. 快照	65
13.2.2. 云平台加密设备管理	66
13.2.2.1. 启用加密设备	66
13.2.2.2. 停用加密设备	66
13.3. 电源管理	67
13.4. 许可证管理	67
13.5. 版本管理	68
13.5.1. 版本信息	69
13.5.2. 版本升级	69
13.6. 备份恢复管理	70
	4

13.6.1. 备份	71
13.6.1.1. 手动备份	71
13.6.1.2. 自动备份	72
13.6.1.3. 导出备份	72
13.6.1.4. 删除备份	73
13.6.2. 恢复	73
13.6.2.1. 上传备份包恢复	73
13.6.2.2. 本地恢复	74
13.7. 策略管理	75
13.7.1. SSH 管理	75
13.7.2. 可视化监控	76
13.7.3. 密管审计管理	76
13.7.4. 系统重置	77
13.7.5. 站点根证书下载	78
13.7.5.1. 下载站点根证书	78
13.7.5.2. 浏览器导入站点根证书	79
13.7.6. SATELLITE 管理	81
13.8. 系统时间	82
13.9. 运行模式管理	82
13.9.1. 单机模式	83
13.9.2. 统一管理模式	83
13.9.2.1. 添加本机	85
13.9.2.2. 添加工作节点	85
13.9.2.3. 数据同步	86
13.9.2.4. 加密快照恢复	88
13.9.2.5. 数据发布管理	88
13.9.2.6. 删除节点变为单机	89
13.9.2.7. 服务日志查看	90
第十四章 负载均衡模式	90
第十五章 常见错误码表	90
第十六章 FAQ	99

图表目录

图表 9 : 登录系统	14
图表 10 云版本登录	14
图表 11 证书登录	15
图表 12 选择登录证书	15
图表 13 登录系统	16
图表 14 : 业务管理员登录首页	16
图表 15 : 安全管理员登录首页	17
图表 16 : 审计管理登录首页	17
图表 17 : 超级管理员登录首页	17
图表 18 : 修改密码对话框	18
图表 19 : 退出登录	19
图表 20 : 部署时配置网络	20
图表 21 : 部署后配置网络	20
图表 22 : 启用加密卡	21
图表 23 启动加密机	21
图表 24 : 添加证书链	22
图表 25 : 配置黑名单-HTTP 下载	22
图表 26 : 配置黑名单-LDAP 下载	23
图表 27 : 配置 OCSP 方式	23
图表 28 : 选择服务匹配证书链	24
图表 29 : 开启服务证书白名单策略	25
图表 30 : 生成证书请求-不用加密设备	25
图表 31 : 生成证书请求-使用加密设备	26
图表 32 : 导出证书请求	26
图表 33 : 导入签发证书	26
图表 34 : 导入证书白名单	27
图表 35 : 修改网络	27
图表 36 : 设置管理节点	28
图表 37 : 添加主机	28
图表 38 : 添加本机	29
图表 39 切换运行模式	29
图表 40 : 添加其他节点	30

图表 41 : 数据发布及数据同步	31
图表 47 : 证书链结构	32
图表 48 : CA 信息管理	32
图表 49 : 添加 CA	33
图表 50 : 传入错误证书链	33
图表 51 : 查看-/导出 CA 证书	34
图表 52 : 业务管理员删除 CA	35
图表 53 系统管理员删除 CA	35
图表 54 : 删除 CA	36
图表 55 : HTTP 下载更新	36
图表 56 : 黑名单下载更新	37
图表 57 : LDAP 下载更新	37
图表 58 : 禁用黑名单	38
图表 59 配置 OCSP	39
图表 60 : 服务列表	39
图表 61 : 添加服务	40
图表 62 删除服务	40
图表 63 退出服务配置页面	41
图表 64 证书管理页面	42
图表 65 添加证书请求	43
图表 66 使用加密设备申请-自动分配索引	44
图表 67 使用加密设备申请-手动输入索引	45
图表 68 导出证书请求	45
图表 69 导入签发后的证书	46
图表 70 导入与请求不匹配的证书	47
图表 71 删除证书请求	47
图表 72 我的证书管理	48
图表 73 编辑我的证书	48
图表 74 删除我的证书	49
图表 75 重置操作码	50
图表 76 导入 PFX 格式证书	50
图表 77 证书白名单列表	51
图表 78 上传证书	52
图表 79 编辑别名	52
图表 80 删除证书	53

图表 81 导出证书	53
图表 82 证书详细信息	54
图表 83 添加 CA	54
图表 84 进入服务配置页面	55
图表 85 服务选择 CA	55
图表 86 服务直接添加证书链	56
图表 87 删除证书链	56
图表 88 服务日志	57
图表 89 证书白名单策略	58
图表 90 签名策略	58
图表 91 证书白名单	59
图表 92 证书签名策略	60
图表 93 启用时间同步	60
图表 94 审计管理员-操作日志	61
图表 95 查看详细日志	62
图表 96 审计管理员-登录日志	62
图表 97 系统管理页面	63
图表 98 修改网络配置	64
图表 99 启用加密设备	64
图表 100 停用加密设备	64
图表 101 创建快照	65
图表 102 恢复加密快照	65
图表 103 启动加密卡	66
图表 104 停止加密卡	67
图表 105 系统关机与重启	67
图表 106 设备状态	68
图表 107 许可证管理	68
图表 108 版本信息	69



图表 109 版本升级	70
图表 110 查看详细升级日志	70
图表 111 手动备份	71
图表 112 自动备份	72
图表 113 导出备份	73
图表 114 删除备份	73
图表 115 上传备份包恢复	74
图表 116 本地恢复	74
图表 117 恢复历史记录	75
图表 118 策略管理	75
图表 119 SSH 管理页面	76
图表 120 可视化监控配置	76
图表 121 密管审计管理	77
图表 122 系统重置部署	78
图表 123 不安全登录	78
图表 124 下载站点根证书	79
图表 125 将站点根证书导入浏览器	81
图表 126 导入根证书后登录系统显示	81
图表 127 查看系统时间	82
图表 128 系统运行单机模式	83
图表 129 系统运行统一管理模式	84
图表 130 主机管理-安全管理员	84
图表 131 主机管理-业务管理员	84
图表 132 添加本机	85

图表 133 添加其他主机 86

图表 134 添加主机网络不通 86

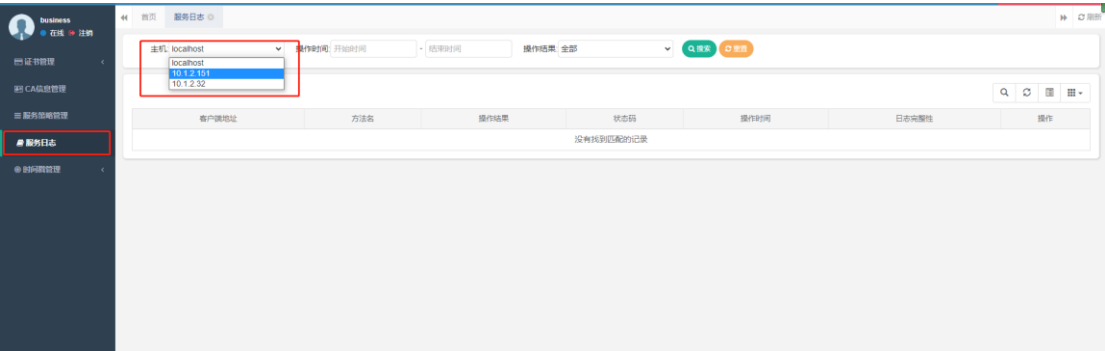
图表 135 数据同步 87

图表 136 未数据发布直接同步 87

图表 137 统一管理模式加密快照恢复..... 88

图表 138 数据发布 88

图表 139 删除节点和主机切换为单机..... 89



图表 140 各节点服务日志 90

第一章 手册指南

1.1. 概述

本手册主要介绍格尔签名验签服务的使用及维护。其中涵盖了签名验签服务所涉及的使用配置方法及其相关说明。

我们将以提供具体实例的方法来引导使用者安装配置符合自己应用环境的签名验签服务。

1.2. 目的

本手册详细描述了如何部署、配置、管理和使用签名验签服务器，目的是指导用户能正确的管理和使用签名验签服务器。

1.3. 适用范围

本手册适用于 SVS 2.4 版本。

1.4. 适用对象

本手册适用对象为网络管理员、签名验签服务器实施人员、售前支持人员和技术支持人员，假定具备以下概念知识：

- 数字证书
- Web 服务器

1.5. 名词解释

证书认证机构（Certificate Authority）：一个产生和确定公开密钥证书的可靠和可信的第三方机构。它发行数字证书并确保证书的可信性，或证明一个用户和它们的公共密钥的身份。认证机构也可以为实体产生和确定密钥。习惯上又称作认证中心（CA）。

数字证书（Certificate）：数字证书中心签发的用于代表实体身份的一段电文。本手册中涉及代表用户身份的用户证书和代表服务端身份的站点证书（服务器证

书）。

黑名单：通常所说的 CRL（Certificate Revoke List），因时间或者安全原因被废除的证书列表，一般发布在 LDAP 上。

✧ 数字签名（digital signature）：具有手写签名功能一如身份证明的一组电子数据。这些附加在数据单元上的一些数据，或是对数据单元所作的密码变换，允许数据单元的接收者用以确认数据单元的来源和完整性，并保护数据，防止被人（例如接收者）伪造。

1.6. 必读声明

本文档中有以下约定，特此声明：

- 配置界面中信息输入框后面带“*”，表示此信息为必填项。
- 文档中关于配置的一些注意事项和建议都在各个配置项描述后面的“提示”中，配置前务必查看清楚。

第二章 产品简介

2.1. 主要功能

格尔签名验签服务能够对应用系统提供证书签名以及签名的验证功能，主要包括：

- ◇ 数据、文件签名及验证
- ◇ 数据、文件 PKCS7 格式签名及验证
- ◇ 支持 sha1、sha256、sha384、sha512、md5 算法签名和验签
- ◇ 支持 SM2 签名格式 GM, OPL, CIPS
- ◇ 支持 RSA 1024、2048 加密（签名）算法
- ◇ 支持国密局 SM2 签名算法及 SM3 摘要算法

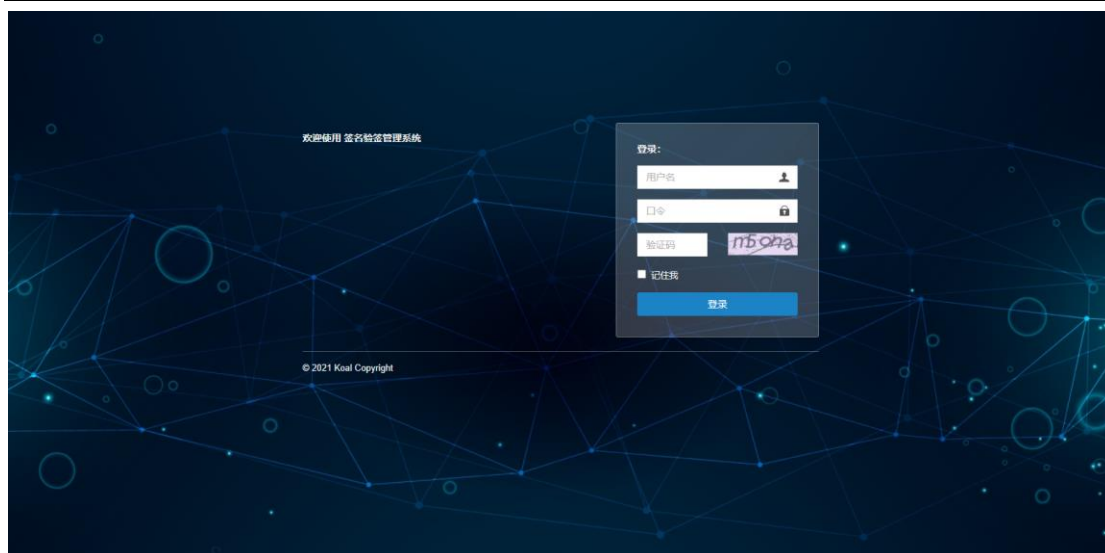
第三章 登录服务器

对服务器的所有配置和管理，管理员都可以通过 web 配置界面方式进行。为了保证系统的安全，本章节描述了如何使管理客户端通过管理口登录格尔签名验签服务器及快速使用服务器。

3.1. 登录系统

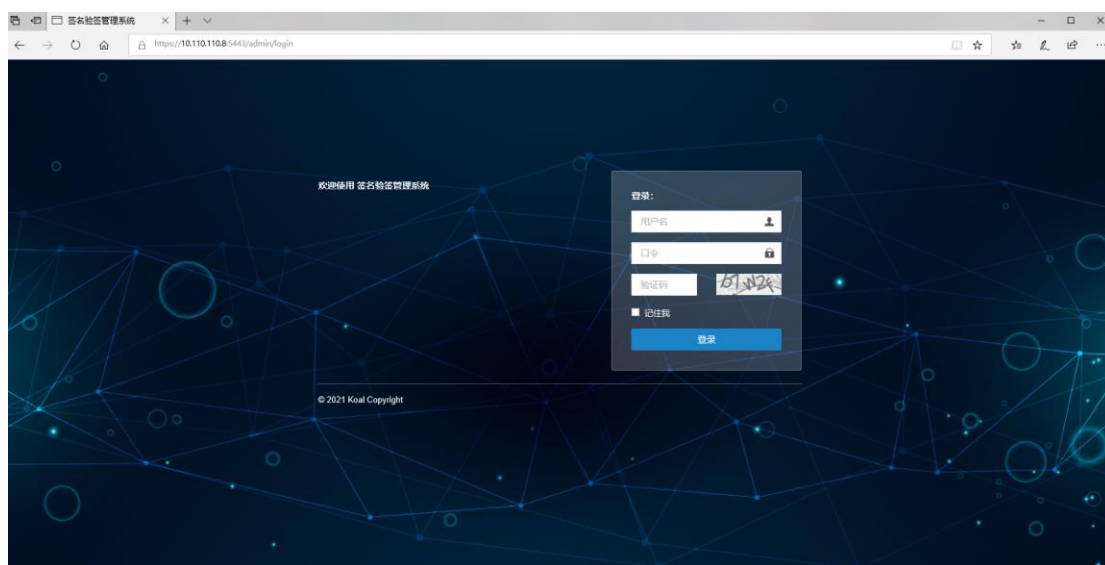
由于部署时【配置服务】-【管理服务】选择的模式不同，登录系统的方式也不同，若选用 https，则在客户端机器上打开谷歌浏览器或火狐浏览器（建议用较新版本的谷歌和火狐浏览器），在地址栏中键入 https://192.168.190.8:5443/admin 进行登录；若为 http 方式，则键入 http://192.168.190.8:5443/admin 然后回车，出现如下所示登录页面：

登录页面如下图所示：



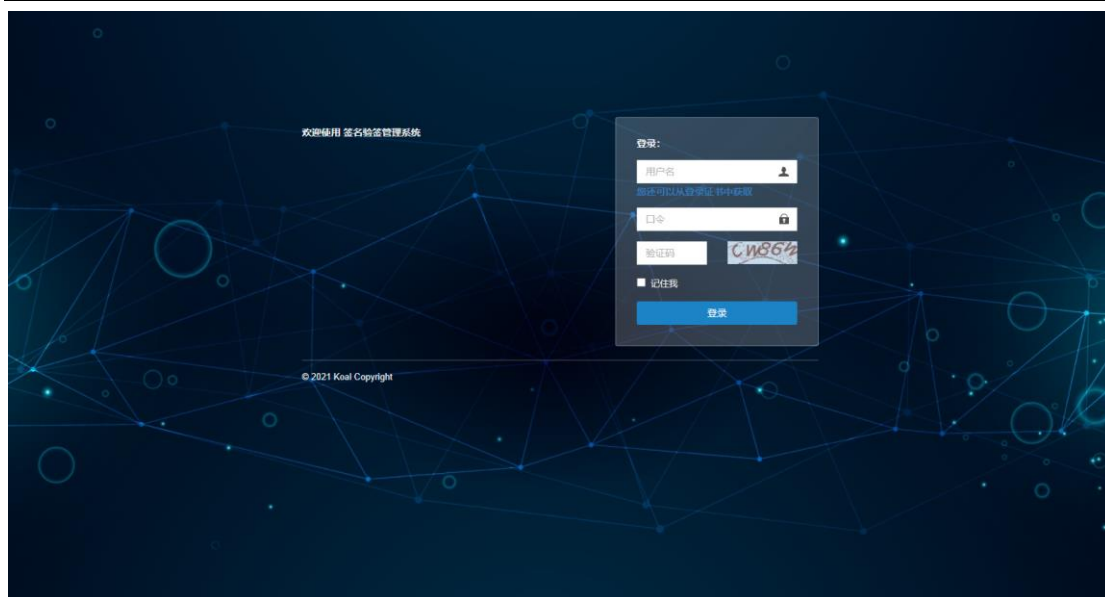
图表 1：登录系统

云版本使用 <https://IP:5443/admin> 或 <http://IP:5443/admin> 登录页面，如图：

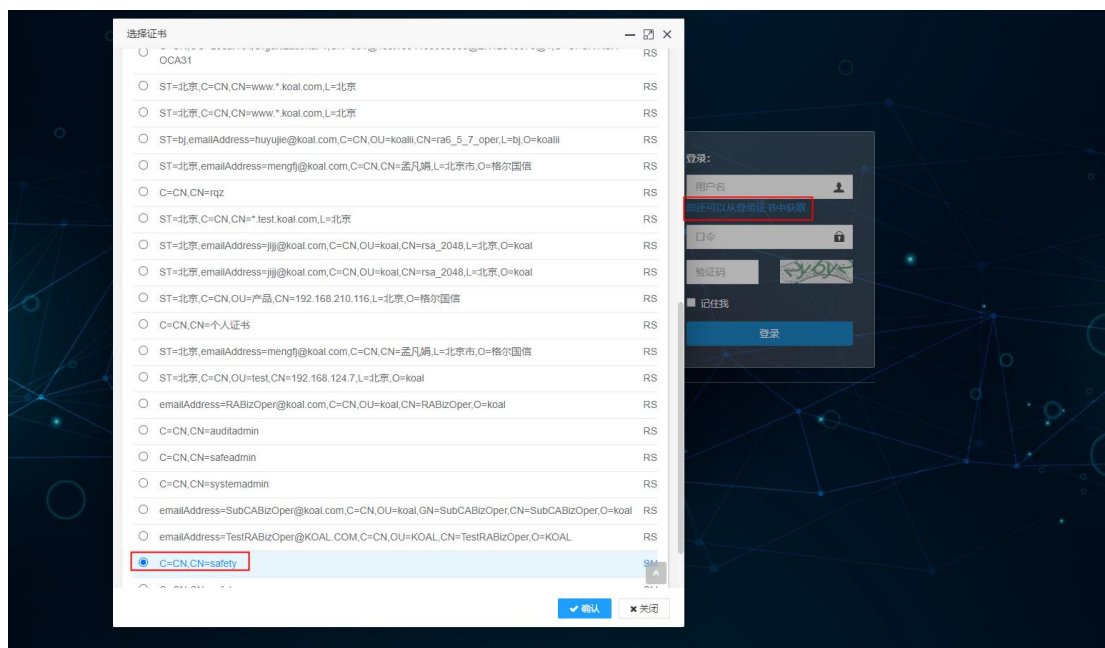


图表 2 云版本登录

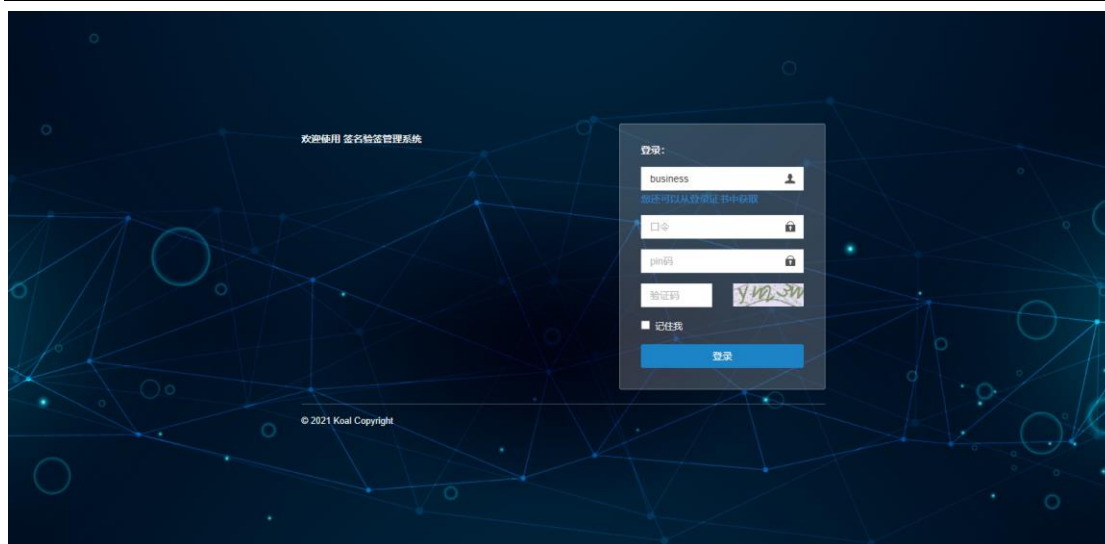
也可以证书登录，后台进入 `/koalii/e-fn` 目录，执行 `./certLogin.sh true` 为开启证书登录，`./certLogin.sh false` 为关闭证书登录，目前适配 key 为龙脉 key，同时还需要中间件 `kunionseccservice_1.17.1.0d6e0851_x64-20210929.exe`，证书登录页面如下：



图表 3 证书登录



图表 4 选择登录证书



图表 5 登录系统

若部署时配置管理模式为三员模式，则用配置的不同管理员分别进行登录。

若部署时配置管理模式选用简单模式，则用超级管理员进行登录。

登录用户名为配置的管理员名称，密码为相应初始化密码。登录后可以看到系统主页及系统版本信息和登录的系统管理员信息。如图

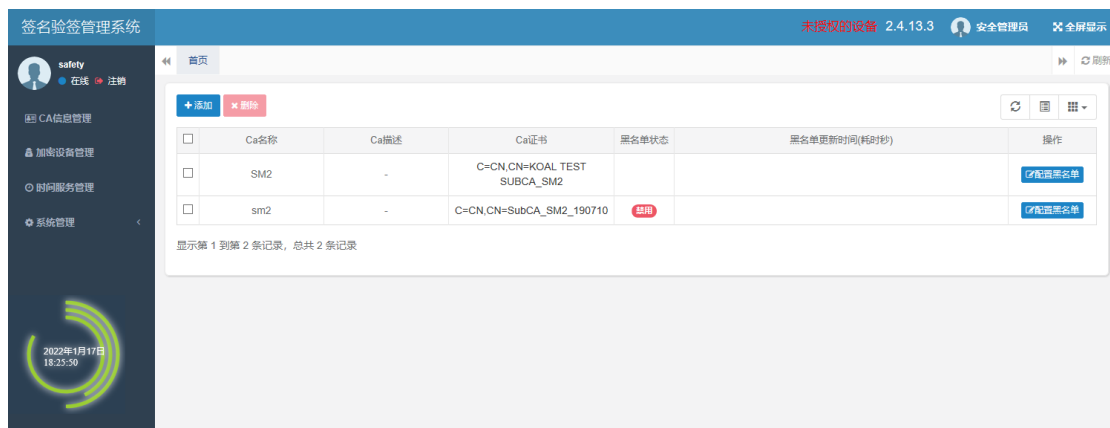
三员模式中由于每个用户所分配的权限不同，故在登录系统之后只能访问被授权的功能模块。

业务管理员：主要负责签名验签服务的维护。如服务管理、加密设备管理等。右上角显示业务管理员。



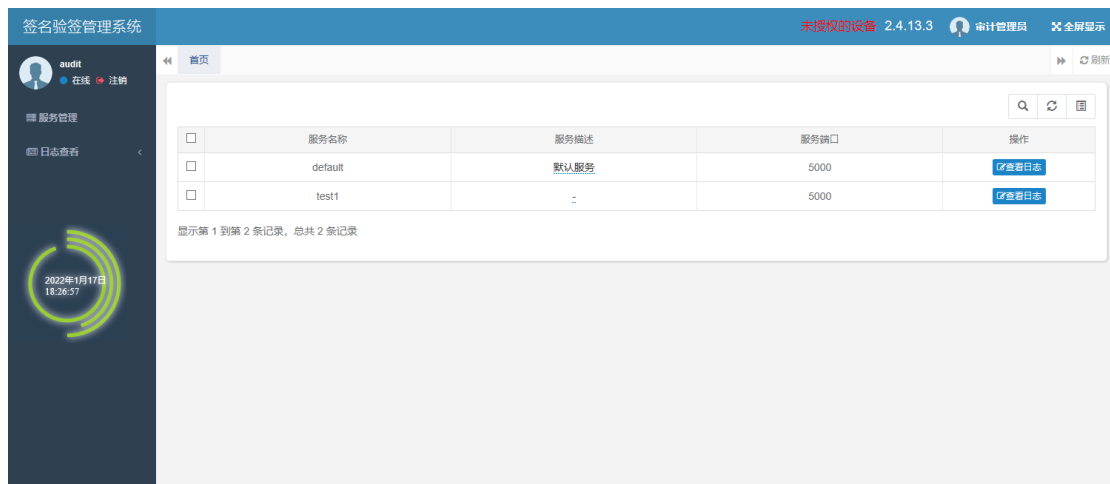
图表 6：业务管理员登录首页

安全管理员：主要负责 CA 信息管理、加密设备管理、时间服务器管理、系统管理。



图表 7：安全管理员登录首页

审计管理员：主要负责服务日志、登录和操作日志的审计工作。



图表 8：审计管理登录首页

简单模式中超级管理员拥有系统所有操作权限。如图



图表 9：超级管理员登录首页

- 为了保证安全，管理员第一次登录系统后会提示立即更改默认密码。
- 自该版本右上角显示版本信息及不同模式管理员信息

考虑系统安全性和典型性，我们以部署三员模式为例进行功能介绍。根据不同管理员登录来分模块进行功能介绍。简单管理模式超级管理员具有所有功能菜单。

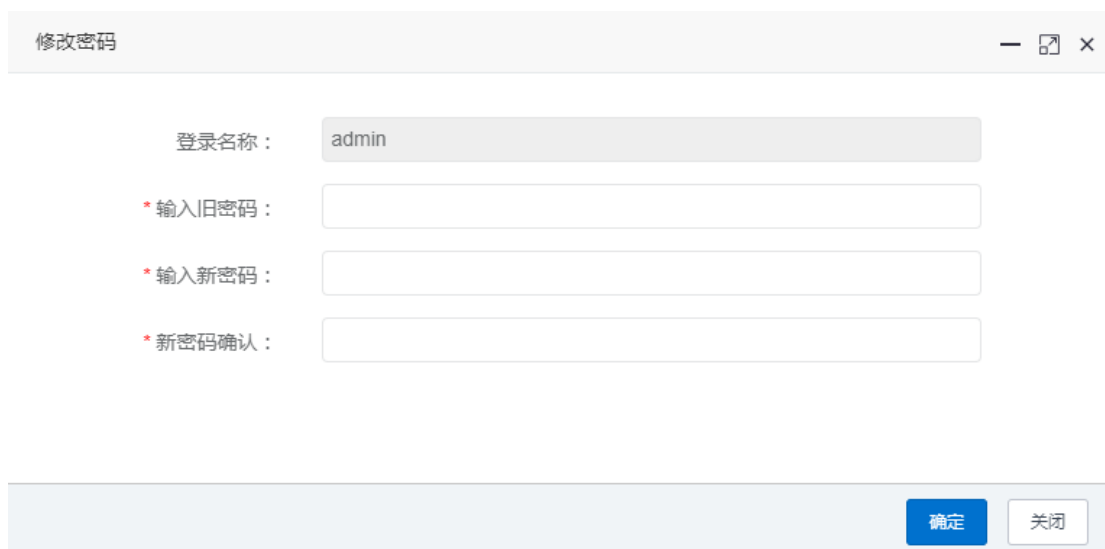
3.2. 更改密码

为了保证安全，管理员应该定期改变密码。该版本支持 30 天后自动提示修改密码功能。

更改密码的前提是管理员已经成功登录系统，更改后的密码将从下次登录起生效。

更改密码步骤：

- 管理员点击管理面右上角“修改密码”按钮，出现以下对话框：



修改密码对话框的截图。对话框标题为“修改密码”，右上角有最小化、最大化和关闭按钮。对话框内有四个输入项：1. “登录名称”：已输入“admin”。2. “* 输入旧密码”：空输入框。3. “* 输入新密码”：空输入框。4. “* 新密码确认”：空输入框。对话框底部右侧有两个按钮：“确定”（蓝色）和“关闭”（白色）。

图表 10： 修改密码对话框

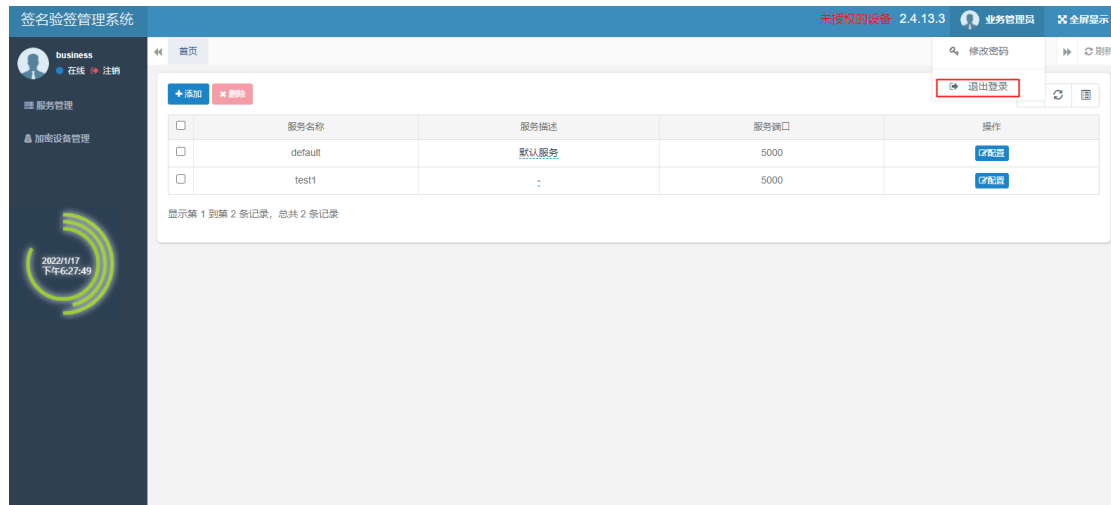
- 在修改密码对话框中输入旧密码，输入新密码以及确认新密码（必须与新密码相同），密码为 8~64 位，必须包含数字、字母、特殊字符，点击“确定”修改密码。

提示：

- 请妥善保管好管理员密码，管理员密码丢失将无法登录管理系统，需安全管理员或超级管理员进行系统重置后才能登录。重置步骤请参考【系统管理】-【策略管理】-【系统重置】部分

3.3. 退出登录

在右上角点击【退出登录】即可退出本系统



图表 11: 退出登录

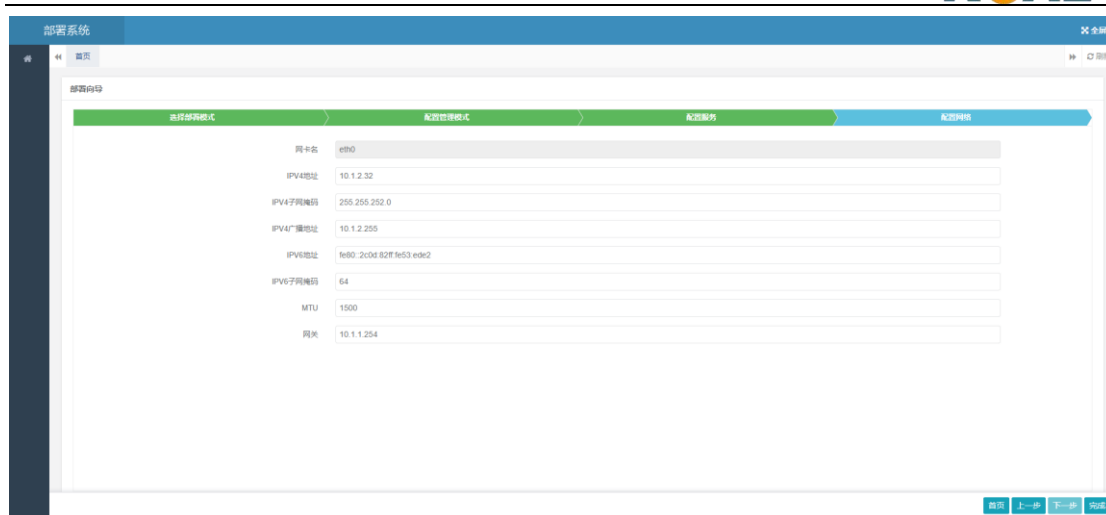
第四章 快速部署

4.1. 单机模式

出厂机器默认为单机模式，单机模式不需要进行数据同步，只要配置证书及相关配置即可。

4.1.1. 修改 IP

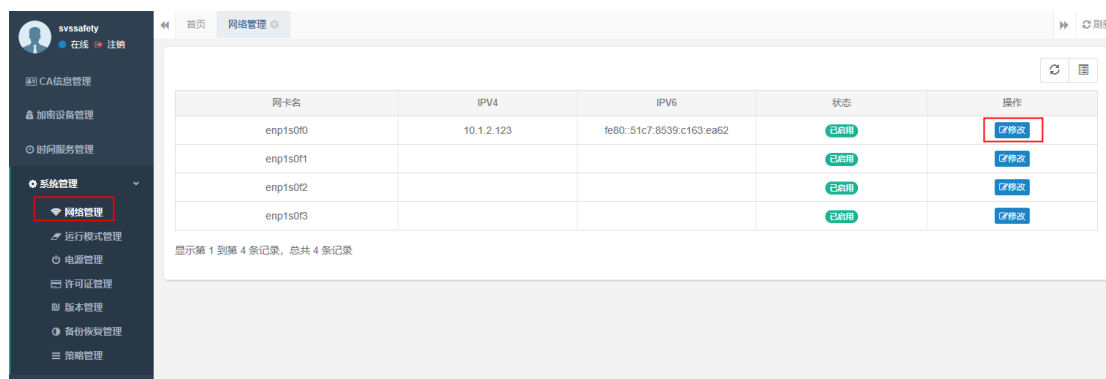
在系统部署时【配置网络】标签下修改网络 IP 或部署完成后安全管理员或超级管理员登录【系统管理】->【网络管理】页面先修改 IP 并保存。



The screenshot shows a web-based configuration interface for network settings. It features a sidebar with navigation options and a main content area with a progress bar indicating the current step in the deployment process. The configuration fields include:

网卡名	配置管理模式	配置服务	配置网络
enb0			
IPv4地址	10.1.2.32		
IPv4子网掩码	255.255.252.0		
IPv4广播地址	10.1.2.255		
IPv6地址	fe80::2c0d:82ff:fe53:ed92		
IPv6子网掩码	64		
MTU	1500		
网关	10.1.1.254		

图表 12：部署时配置网络



The screenshot shows a web-based network management interface. It includes a sidebar with navigation options and a main content area displaying a table of network interfaces. The table has columns for interface name, IPv4 address, IPv6 address, status, and actions. The '网络管理' (Network Management) option is highlighted in the sidebar.

网卡名	IPv4	IPv6	状态	操作
enp1s0f0	10.1.2.123	fe80::51c7:8539:c163:ea62	已启用	已修改
enp1s0f1			已启用	已修改
enp1s0f2			已启用	已修改
enp1s0f3			已启用	已修改

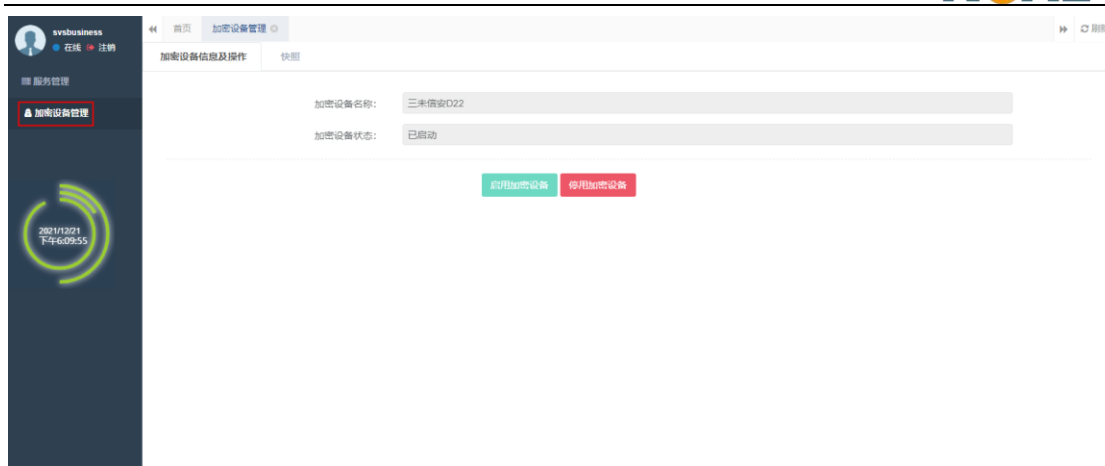
显示第 1 到第 4 条记录，总共 4 条记录

图表 13：部署后配置网络

4.1.2. 启动加密设备

4.1.2.1. 启动加密卡

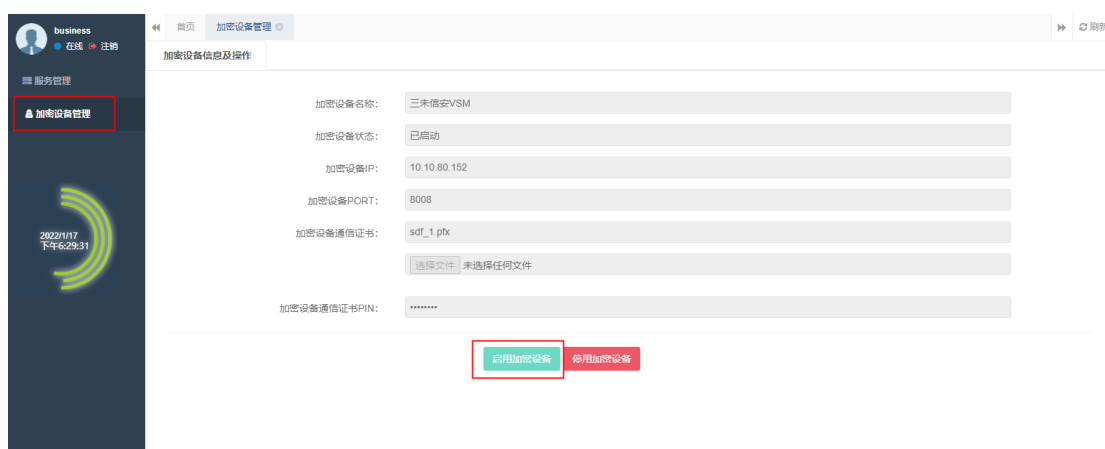
业务管理员登录，点击【加密设备管理】，进入加密卡管理页面，默认适配的为三未 D22 加密卡，点击“启用加密设备”按钮可启用加密卡。



图表 14: 启用加密卡

4.1.2.2. 启动加密机

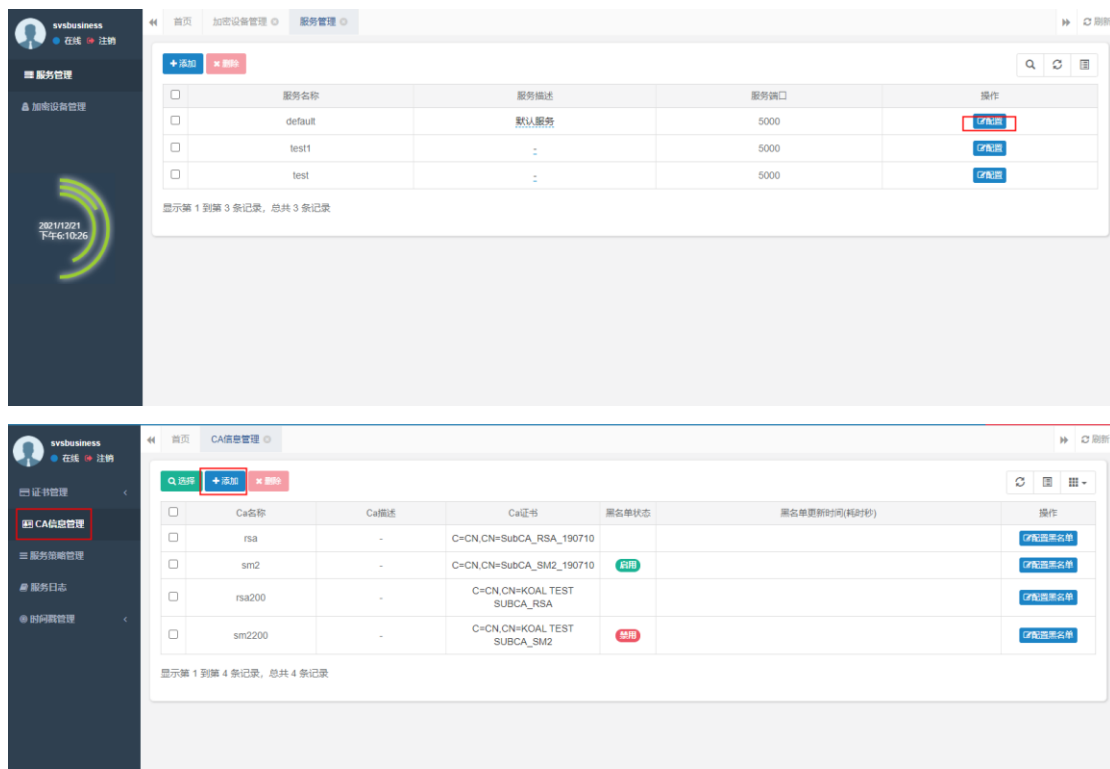
云版本适配的是加密机，使用业务管理员或系统管理员登录系统，点击【加密设备】管理页面，添写加密设备 IP、PORT，上传通讯证书，输入通讯证书 PIN，最后点击“启用加密设备”按钮启动加密机，如下图：



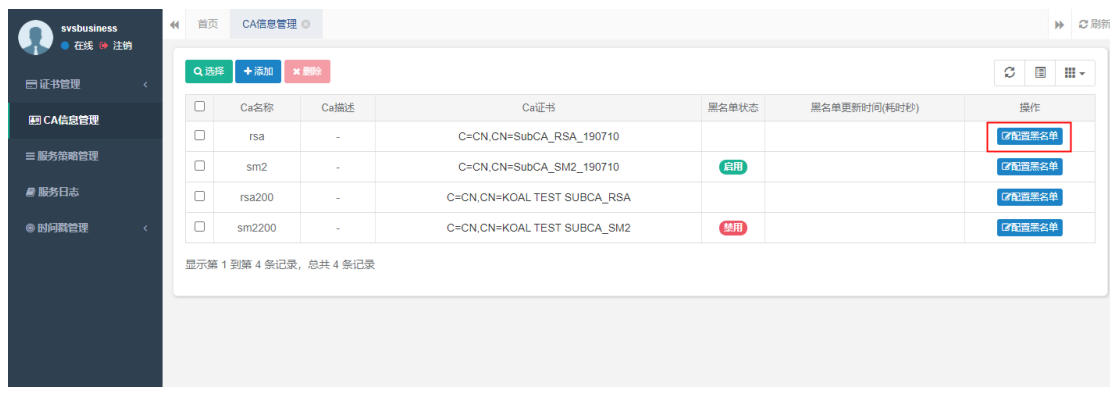
图表 15 启动加密机

4.1.3. 配置证书链黑名单及服务证书链

业务管理员登录，先进入服务配置，然后配置 CA 信息，包括添加 CA 信息管理，配置黑名单，配置服务 CA 证书链



图表 16: 添加证书链



黑名单下载更新: 5分钟

黑名单日志级别: 错误

黑名单下载方式: ☐ LDAP配置 ☒ HTTP配置 ☐ OCSP配置

HTTP服务器地址: http://192.168.8.200:8880/download/KOAL TEST SUBCA_SM2.crl

启用 禁用

图表 17: 配置黑名单-http 下载

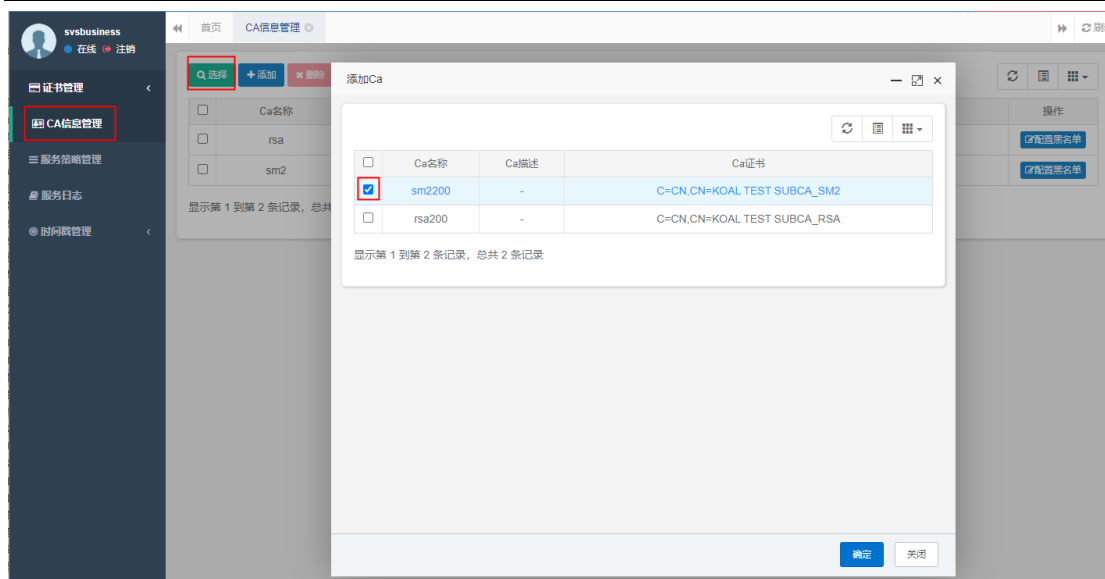
黑名单下载更新:	5分钟
黑名单日志级别:	错误
黑名单下载方式:	☒ LDAP配置 ☐ HTTP配置 ☐ OCSP配置
LDAP服务器地址:	10.1.1.251
LDAP服务器端口号:	389
LDAP服务器用户名:	cn=admin,dc=example,dc=com
LDAP服务器密码:	*****
LDAP链接超时限制(秒):	30
搜索路径:	ou=CRLDistributePoints,dc=example,dc=com
过滤字符串:	cn=SubCA_SM2_190710
LDAP节点属性名:	certificateRevocationList;binary

图表 18: 配置黑名单-LDAP 下载

The screenshot shows the 'Configure Blacklist' (配置黑名单) page in the svssafety system. The left sidebar contains navigation links: CA信息管理, 加密设备管理, 访问服务管理, and 系统管理. The main content area shows the configuration for the blacklist download method. The '黑名单下载方式' (Blacklist download method) is set to 'OCSP配置' (OCSP configuration), which is highlighted with a red box. Other settings include '黑名单下载更新' (5 minutes), '黑名单日志级别' (Error), and 'OCSP服务器地址' (http://10.1.1.252:3018/). The '启用' (Enable) button is visible at the bottom.

图表 19: 配置 OCSP 方式

黑名单下载更新:	5分钟
黑名单日志级别:	错误
黑名单下载方式:	☐ LDAP配置 ☐ HTTP配置 ☒ OCSP配置
OCSP服务器地址:	http://10.1.1.252:3018/

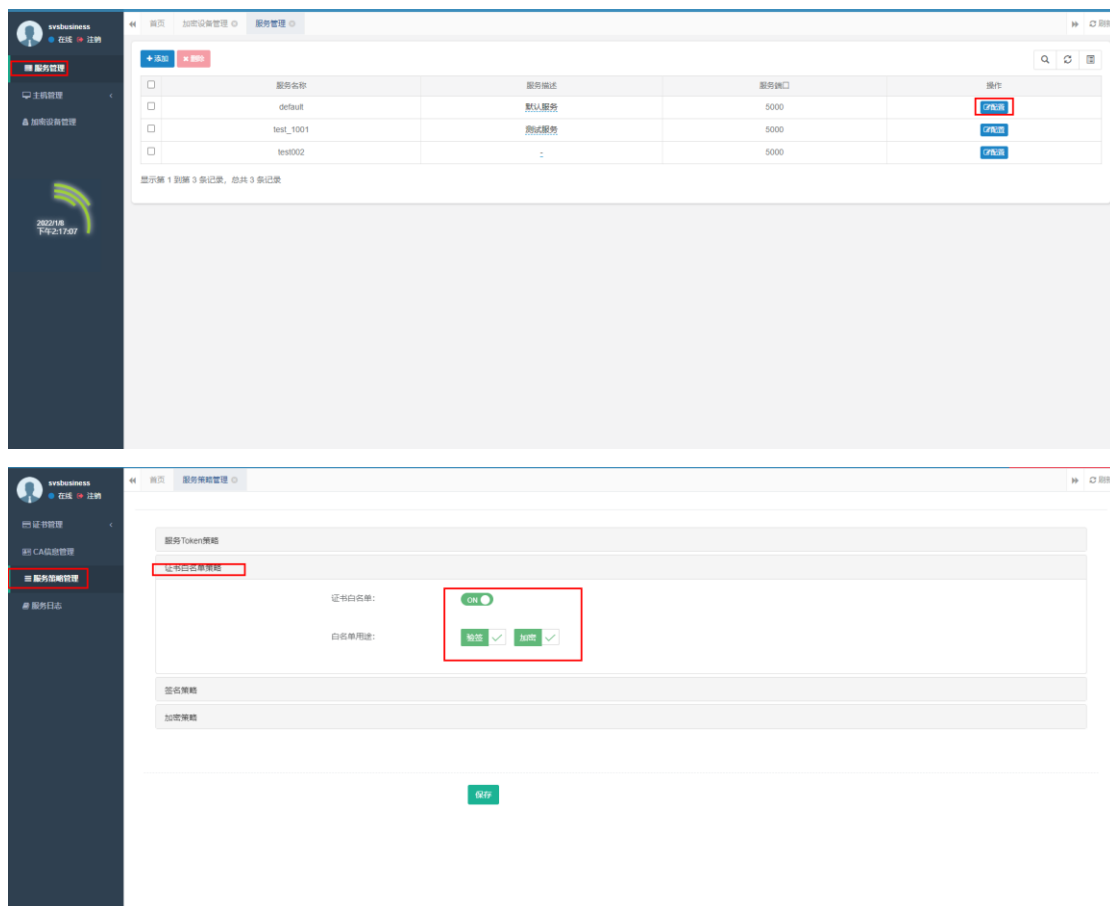


图表 20：选择服务匹配证书链

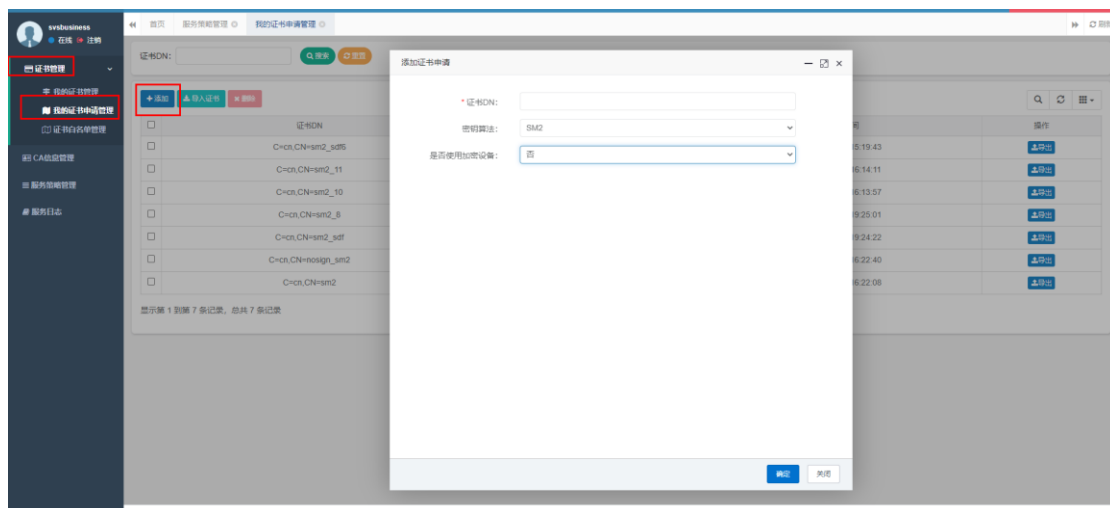
添加 CA 信息管理详细步骤请参考 [5.1 添加 CA 信息](#)，添加黑名单详细步骤请参考 [5.4 配置黑名单](#)，添加服务 CA 证书链请参考 [8.1 选择 CA](#)

4.1.4. 配置证书信息（申请证书、导入证书、导入证书白名单）

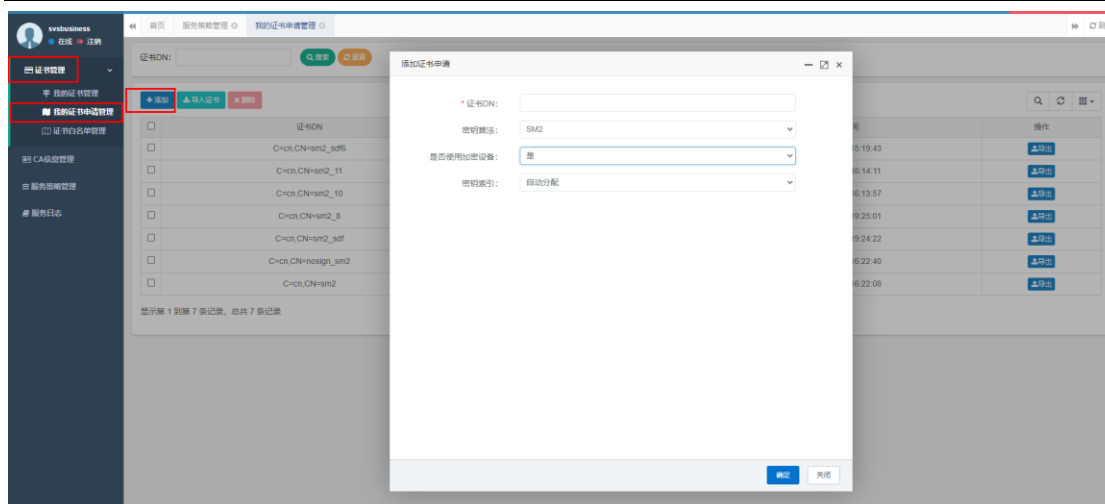
业务管理员登录【服务管理】菜单点击 default 服务【配置】按钮，进入默认服务配置页面，【服务策略管理】服务开启证书白名单（业务验签或者加密时直接传证书内容而不是使用服务器证书时可以不开启此项）。在【我的证书申请管理】菜单生成证书请求，如用加密设备生成，需在“是否使用加密设备”选择“是”，在 CA 中心签发证书，导入证书，【我的证书管理】显示已签发的证书。



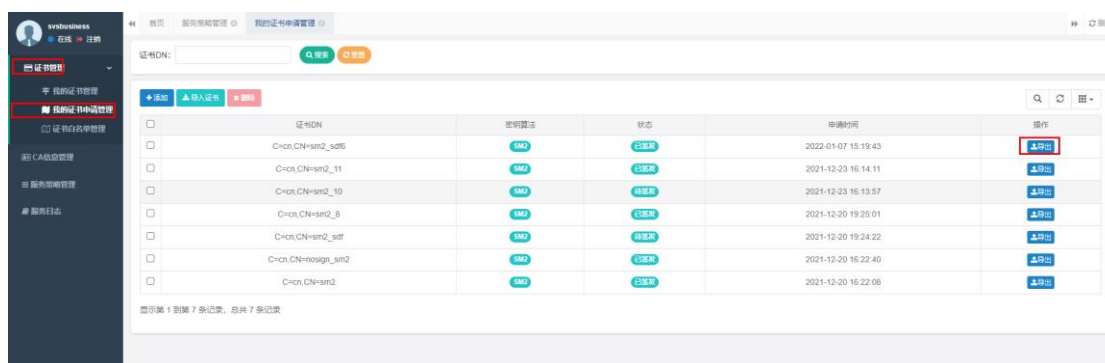
图表 21：开启服务证书白名单策略



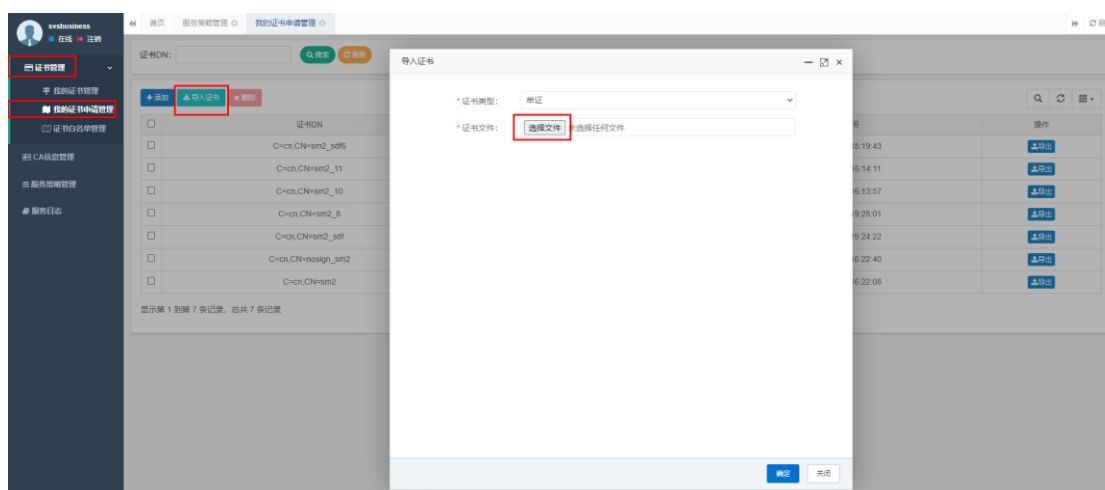
图表 22：生成证书请求-不用加密设备



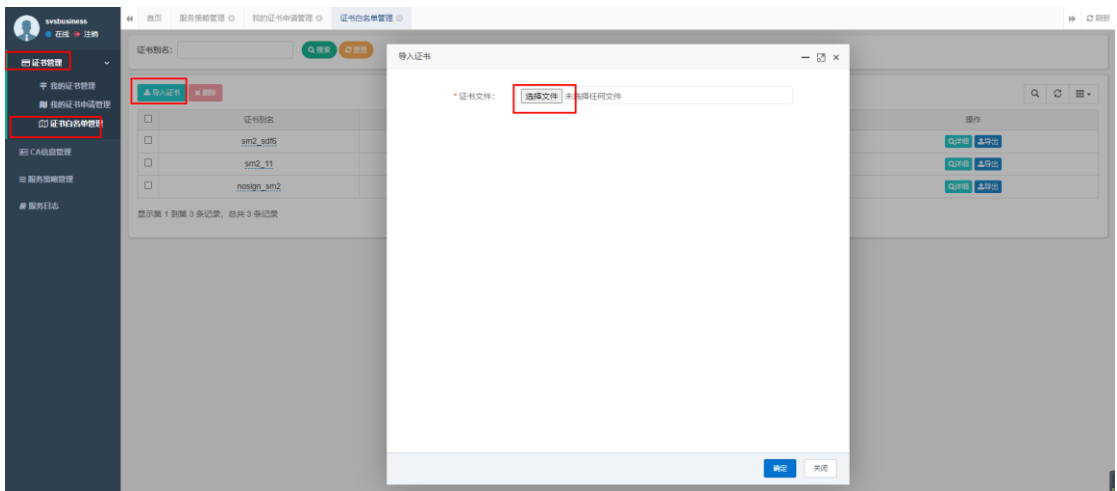
图表 23：生成证书请求-使用加密设备



图表 24：导出证书请求



图表 25：导入签发证书



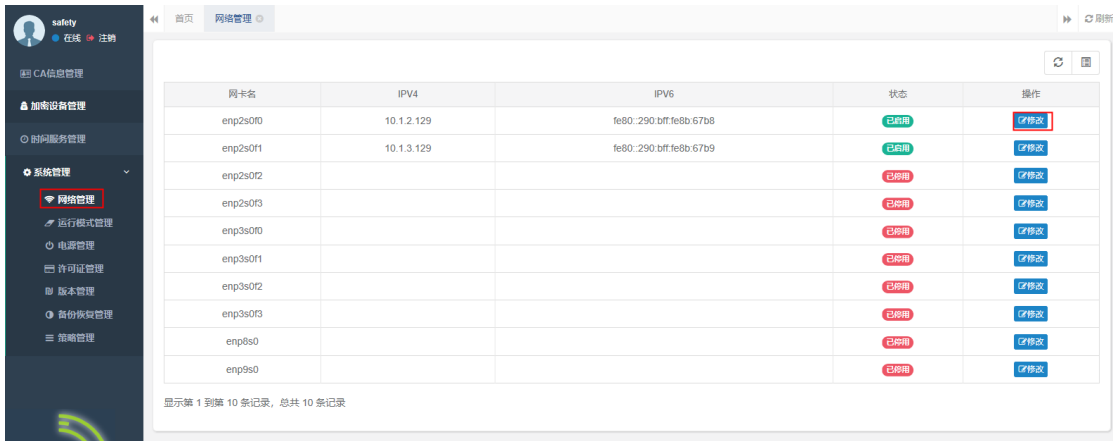
图表 26：导入证书白名单

申请证书详细步骤请参考 [7.1.1](#) 生成证书请求, [7.1.2](#) 导出证书请求, [7.1.4](#) 导入证书, [7.3.1](#) 导入证书

4.2. 统一管理模式

4.2.1. 修改 IP

安全管理员在【系统管理】->【网络管理】页面先修改 IP 并保存。



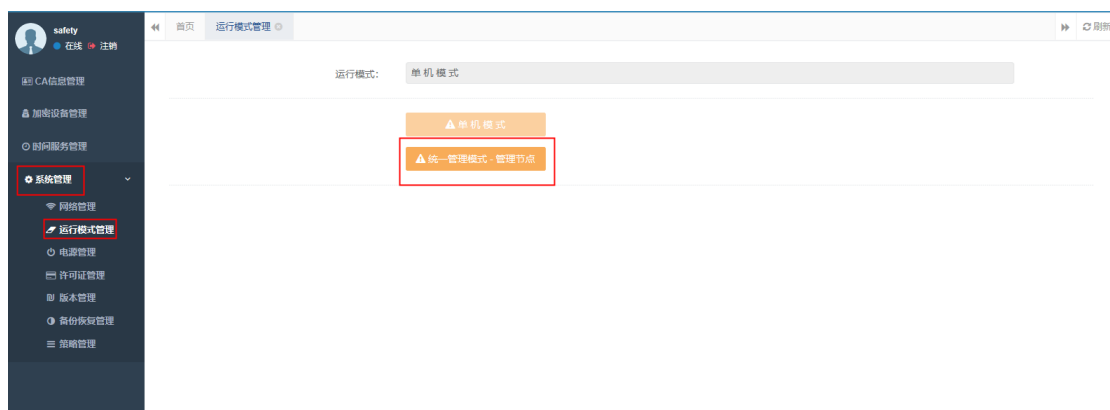
图表 27：修改网络

4.2.2. 启动加密设备

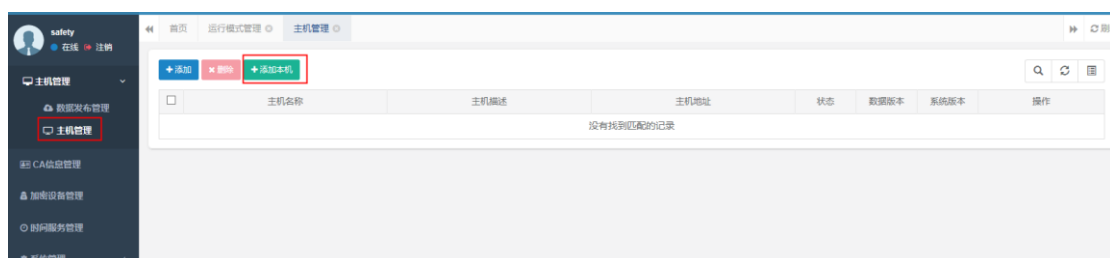
统一管理模式下配置前，先在单机模式下把每台机器的加密设备都启用，然后重启，注意是每一台都要在转换模式前先把加密设备启用，[具体步骤 4.1.1 启动加密设备](#)

4.2.3. 修改运行模式

确保每台主机的加密设备都启用后，就可以配置统一管理模式了，先确定哪台做管理节点，确定后管理节点后将该主机的运行模式修改为管理节点，点击【系统管理】-【运行模式管理】将运行模式设为“统一管理模式 - 管理节点”如图：



图表 28：设置管理节点



图表 29：添加主机

[添加主机及其他主机详细信息请参考第十一章 11.9.1、11.9.2](#)

4.2.4. 添加本机

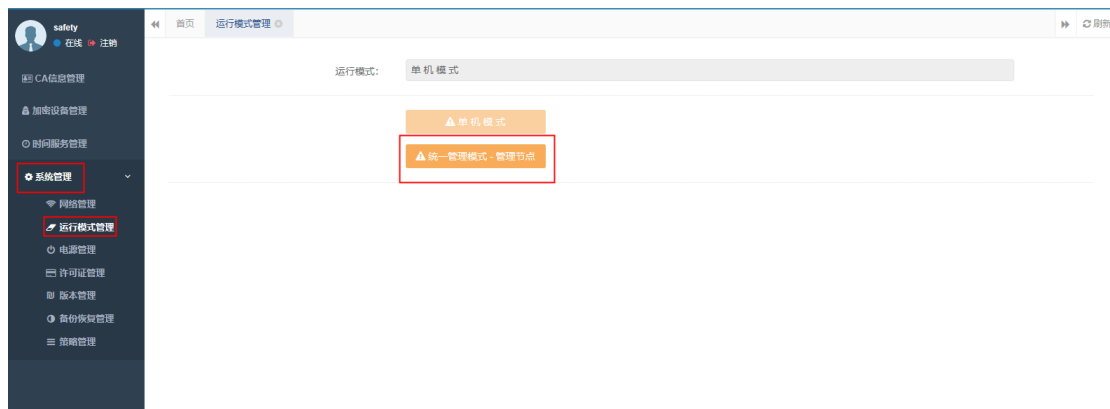
管理节点主机，点击【主机管理】->【主机管理】下的“添加本机”按钮，如图



图表 30：添加本机

4.2.5. 从机修改运行模式

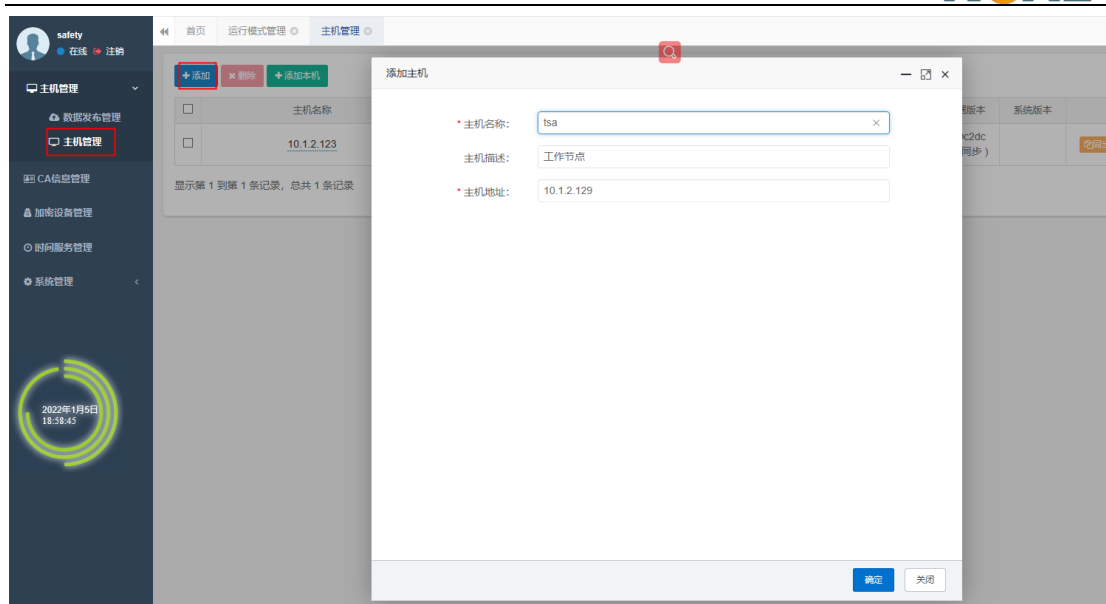
从机也需要将运行模式修改为统一管理模式，点击【系统管理】-【运行模式管理】将运行模式设为“统一管理模式 - 管理节点”



图表 31 切换运行模式

4.2.6. 管理节点添加工作节点

然后添加工作节点，管理节点主机，点击【主机管理】->【主机管理】下的“添加”按钮，添加主机，如图



图表 32：添加其他节点

4.2.7. 配置证书链黑名单及服务证书链

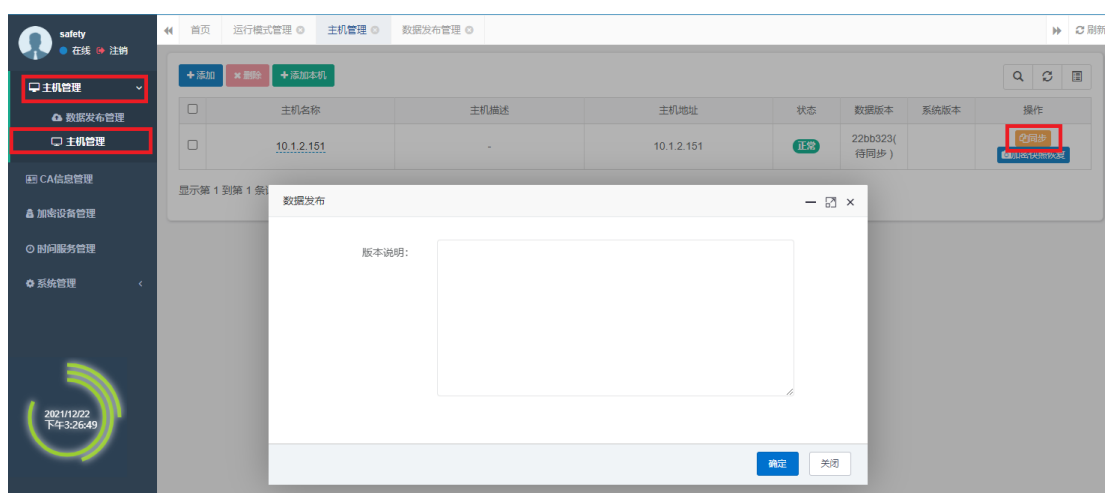
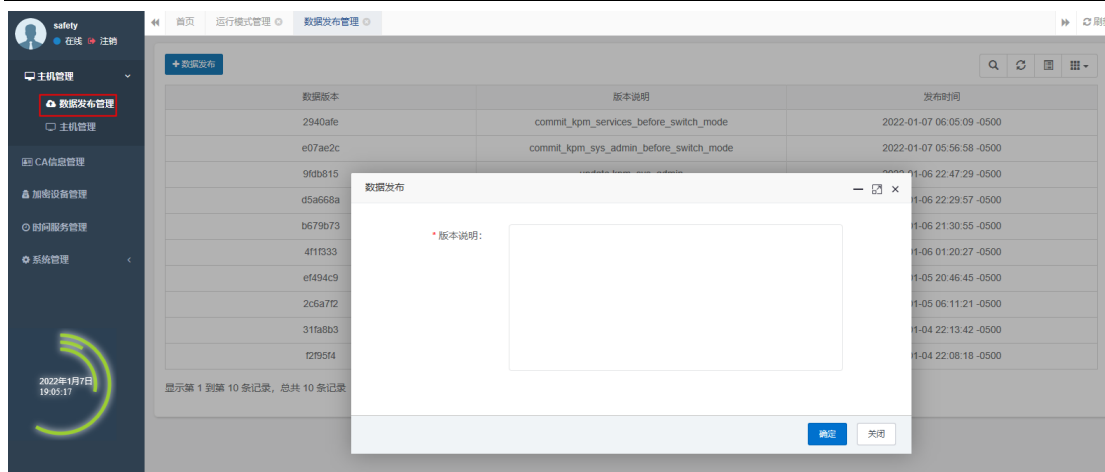
[参考 4.1.3 配置证书链黑名单及服务证书链](#)

4.2.8. 配置证书信息（申请证书、导入证书、导入证书白名单）

[参考 4.1.4 配置证书信息（申请证书、导入证书、导入证书白名单）](#)

4.2.9. 数据发布及同步

所有配置都添加完成后，可以在【数据发布管理】页面进行发布，如下图，也可以在【主机管理】菜单点击【同步】按钮，未进行数据发布的直接弹出发布提示，发布完成再点击【同步】才能将本地配置同步到本地服务及其他主机服务中。



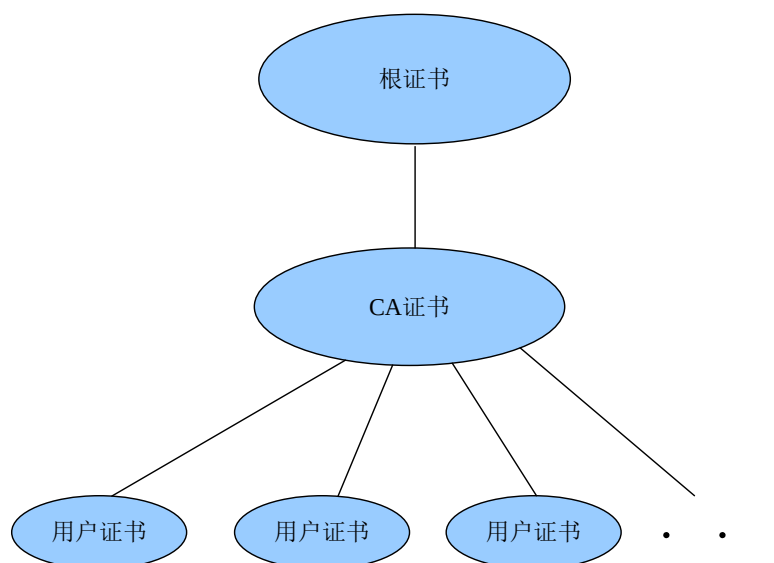
图表 33：数据发布及数据同步

第五章 CA 信息管理

这里提到的 CA 就是所谓的信任证书链，服务器在对用户证书进行验证的时候重要的一条就是验证证书链，即用户证书是否是服务器信任的 CA 中心签发，因此，服务器为了验证用户，必须首先将信任 CA 中心的证书配置到信任列表中。

之所以称之为证书链是因为 CA 证书是分层次的，通常由根证书、一级 CA

证书、二级 CA 证书等组成一条信任链，如图：



图表 34：证书链结构

签名验签服务必须配置了 CA 作为信任链，才能验证此链下面的用户证书。

【CA 信息管理】是对本系统的 CA 信息进行统一管理，包括 CA 证书链的添加、删除及配置黑名单作业。如图，列表显示的是本系统所有服务的 CA 信息、包含 CA 名称、CA 描述、CA 证书、黑名单状态、黑名单更新时间、配置黑名单等数据项。每个服务可以根据需要选择匹配证书链作为签名验签服务 CA 证书链。

☐	Ca名称	Ca描述	Ca证书	黑名单状态	黑名单更新时间(毫秒)	操作
☐	SM2	-	C=CN,CN=SubCA_SM2_190710	启用		配置黑名单
☐	RSA	-	C=CN,CN=SubCA_RSA_190710	启用	2022-01-08 09:47:05(0)	配置黑名单
☐	KoalSM2	-	C=CN,CN=KOAL TEST SUBCA_SM2	启用		配置黑名单
☐	KoalRSA	Koal链1	C=CN,CN=KOAL TEST SUBCA_RSA	启用		配置黑名单

显示第 1 到第 4 条记录，总共 4 条记录

图表 35：CA 信息管理

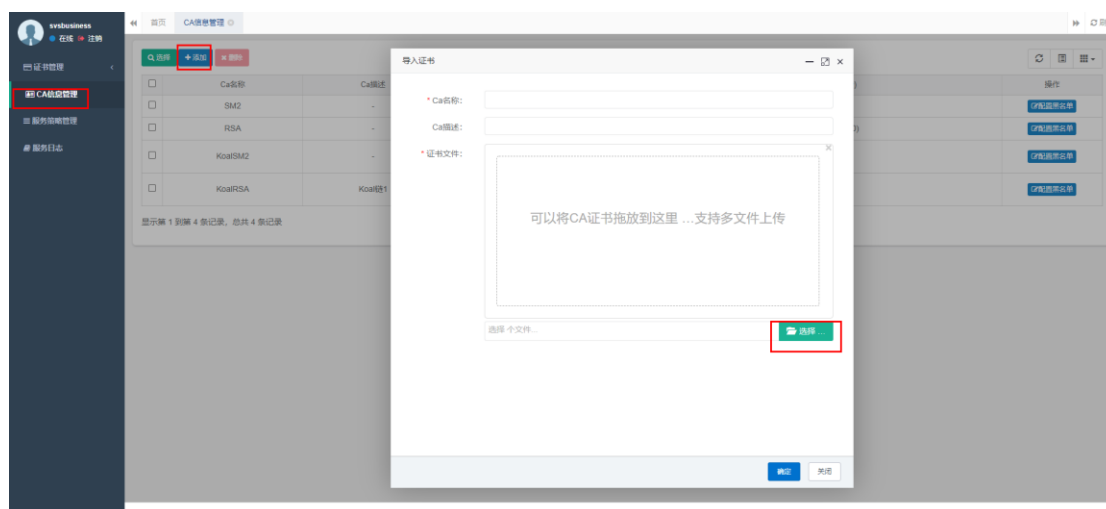
提示：

- 证书链显示的名称是 **Ca** 证书名称、**Ca** 描述、**DN** 项值、相应证书链证书黑名单状态、黑名单更新时间、配置黑名单等操作信息。

5.1. 添加 CA 信息

注意：在业务管理员中对 CA 信息管理中的任何操作都会同步至安全操作员 CA 信息管理中。

业务管理员登录，在 CA 列表页面中点击“添加”按钮，填写“Ca 名称”、“Ca 描述”、选择需要导入的证书链文件（也可以直接将 Ca 多级证书链拖到证书文件框内），点击“确定”按钮，就可以将多级 CA 证书直接传到系统中，如下图所示：



图表 36：添加 CA

上传 ca 证书时会对证书链进行上级匹配，若已经存在上级证书则显示证书名，若没有相应的上级证书，则系统将进行提示，显示如下信息：



图表 37：传入错误证书链

提示：

- 支持一次传入多张证书链
- 上传的证书文件必须为 **cer** 为后缀的证书,且证书为 **Base64** 编码格式,如果证书文件是 **DER** 格式的,则可以将其导入 **IE**,然后选择 **Base64** 格式导出。
- 请勿将多个证书合并到一个文件中上传。
- 系统仅检测证书的上级证书是否存在,因此根 **CA** 可以单独上传,二级 **CA** 不能单独上传。

5.2. 查看导出 CA 证书

1. 查看导出 ca

在 CA 列表页面中,选择一个 CA,点击“Ca 证书”项后,可以看到该条 CA 的证书

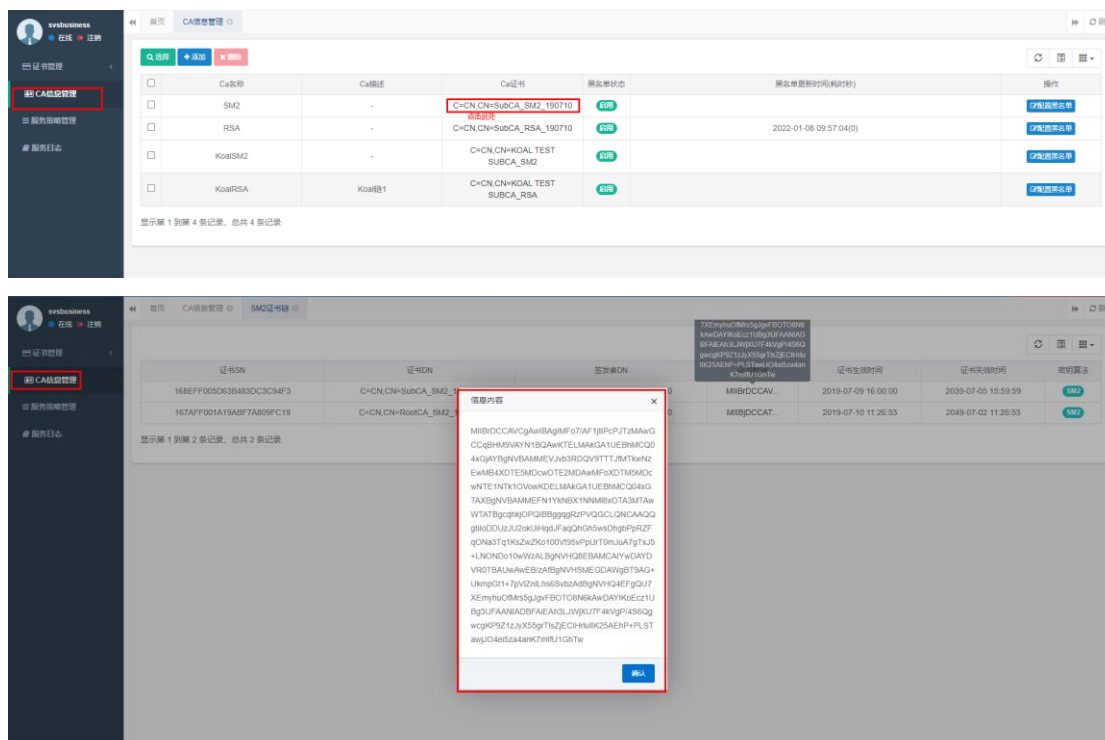
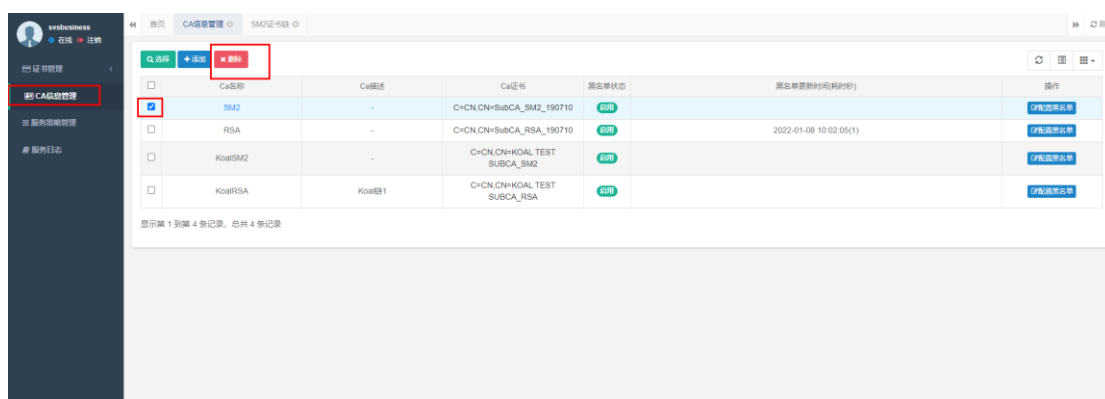


图 38: 查看-/导出 CA 证书

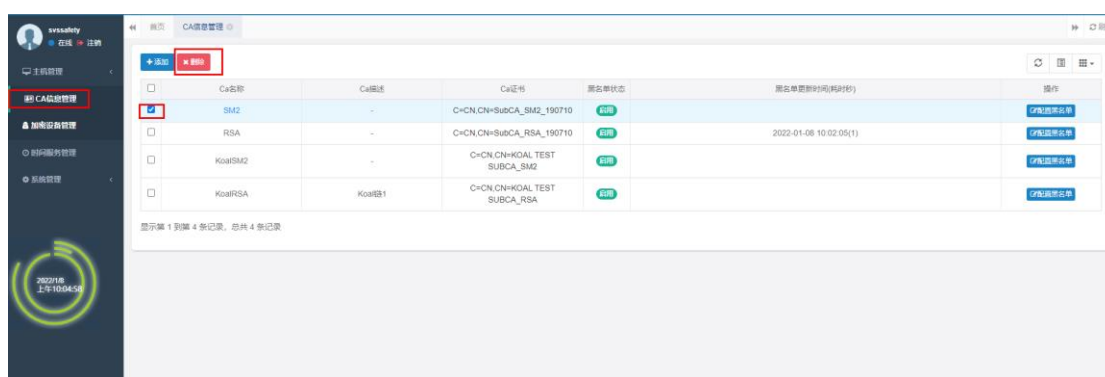
5.3. 删除 CA 信息

在 CA 列表页面中选择一条或多条 CA 证书链, 点击【删除】按钮, 所选中的证书链将被删除, 这里的删除 CA 只是删除的引用关系, 要彻底删除 CA 需在

系统管理员



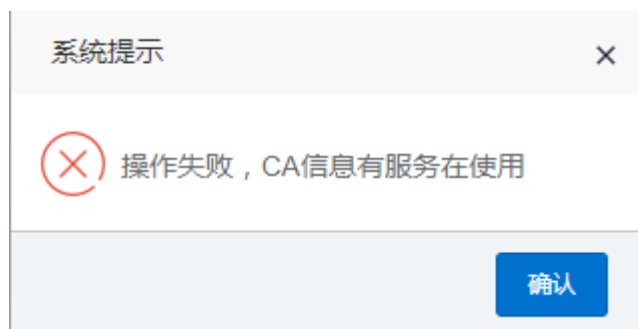
图表 39：业务管理员删除 CA



图表 40 系统管理员删除 CA

提示：

- 删除证书链会导致使用此证书链的签名验签服务无法验证此证书链中的用户证书。
- 如果现有的服务配置中引用了此 **CA**，**CA** 不能删除，需要先在服务配置中删除引用的 **CA**，然后退出服务配置页面，再去 **CA** 列表中删除该条 **CA**，如下图：



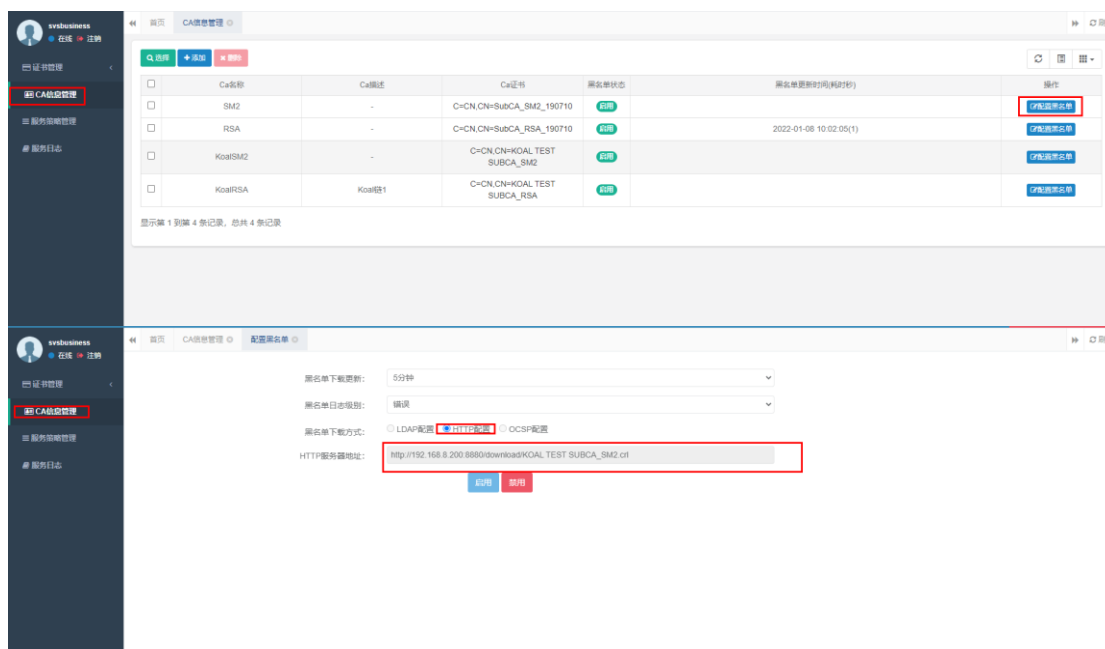
图表 41: 删除 CA

5.4. 配置黑名单

黑名单即证书吊销列表，英文简称 CRL，由 CA 中心定期发布到公开的发布点（通常为 LDAP 服务器），列在黑名单内的证书都是有潜在安全隐患的证书，是系统不再信任的证书。因此对用户证书进行验证时必须对黑名单进行检查，不能使不受信任的证书通过，以免造成安全隐患。

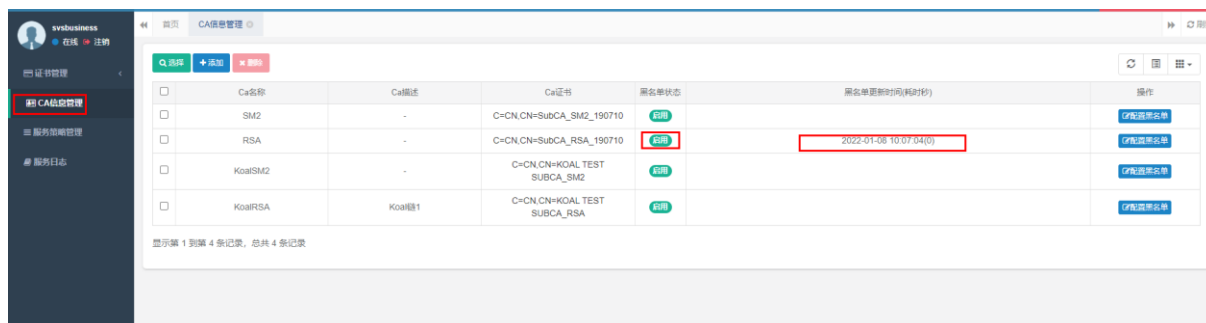
黑名单对于基于证书的应用来说至关重要，黑名单是不断更新的，体现了一个动态的信任关系，应用也必须及时动态的检查黑名单，保持信任关系的正确性，服务器专门提供一个黑名单下载服务，定期下载黑名单，然后通知相关服务进行动态更新，不需要用户手动更新服务。

进入黑名单配置页面，配置黑名单下载更新时间及下载方式，输入下载地址及参数，点击【启用】按钮，即可按照设定时间定时更新黑名单，如图



图表 42: HTTP 下载更新

返回证书链页面，显示“黑名单状态”为“启用”，如图，则黑名单按照定时任务定时下载更新，如列表中更新时间为“2022-01-08 10:07:04 (0)”，更新时长为 0 秒。

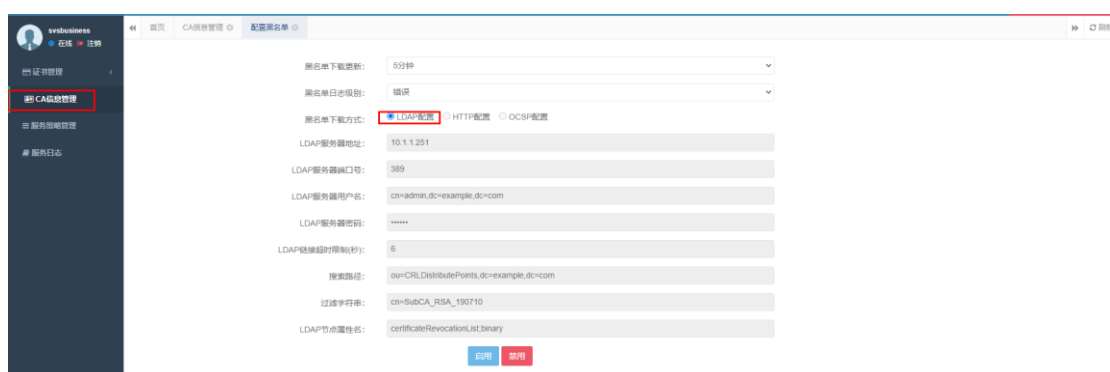


Ca名称	Ca描述	Ca证书	黑名单状态	黑名单更新时间(相对时)	操作
SM2	-	C=CN,CN=SubCA_SM2_190710	在线		配置黑名单
RSA	-	C=CN,CN=SubCA_RSA_190710	在线	2022-01-28 10:07:04(0)	配置黑名单
KoaSM2	-	C=CN,CN=KOAL TEST SUBCA_SM2	在线		配置黑名单
KoaRSA	KoaRSA1	C=CN,CN=KOAL TEST SUBCA_RSA	在线		配置黑名单

显示第 1 到第 4 条记录, 总共 4 条记录

图表 43: 黑名单下载更新

黑名单有两种下载方式: LDAP 和 HTTP, 一种在线查询黑名单功能即 OSCP 功能如图。



黑名单下载更新: 5分钟

黑名单日志级别: 错误

黑名单下载方式: ☒ LDAP配置 ☐ HTTP配置 ☐ OSCP配置

LDAP服务器地址: 10.1.1.251

LDAP服务器端口号: 389

LDAP服务器用户名: cn=admin,dc=example,dc=com

LDAP服务器密码: *****

LDAP连接超时限制(秒): 5

搜索路径: ou=CN,DistributePoints,dc=example,dc=com

过滤字符串: cn=SubCA_RSA_190710

LDAP节点属性名: certificateRevocationList.binary

[应用](#) [取消](#)

图表 44: LDAP 下载更新

- 黑名单下载更新: 定时下载更新, 包括 **5、10、30** 分钟, 默认为 **5** 分钟
- 黑名单日志级别: 默认为错误。
- 黑名单下载方式: 支持 **ldap** 和 **HTTP** 两种方式。默认为 **HTTP** 方式

5.4.1. LDAP 配置

LDAP 服务器地址: 填写黑名单发布服务器的 IP 地址

LDAP 服务器端口号: 发布服务器对外服务的端口号

LDAP 服务器用户名: 填写连接 LDAP 服务器需要认证的用户名 (若服务器需要认证)

LDAP 服务器密码: 填写用户名对应的密码

LDAP 连接超时限制: 填写一个整数值, 代表与 LDAP 初始连接时需要等待的时间, 若连接时超过此值还未得到服务器响应, 则放弃连接

搜索路径：下载服务开始从 LDAP 上搜索的根节点，此路径填写的越详细，搜索效率越高

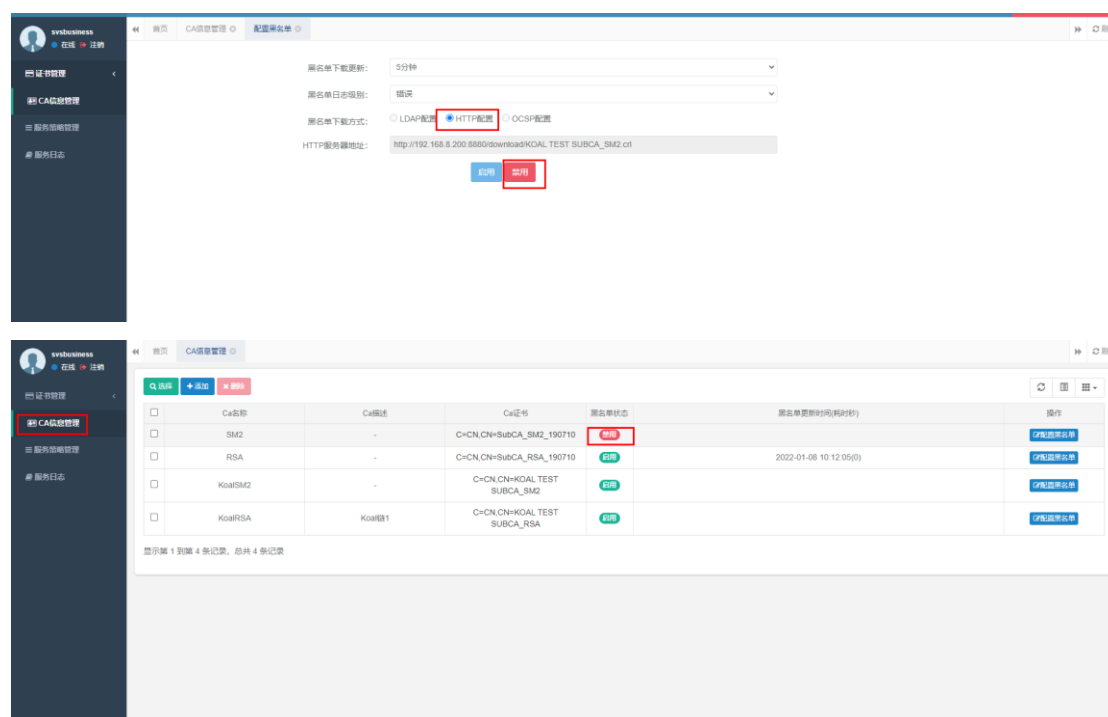
过滤字符串：所需查找对象应该具备的特征或者条件，条件可组合使用，详细语法可参考 <http://www.ietf.org/rfc/rfc2254.txt>。

LDAP 节点属性名：查找对象中需要获取内容的属性名称，

5.4.2. HTTP 配置

HTTP 服务器地址：填写黑名单发布服务器的 HTTP 下载地址。

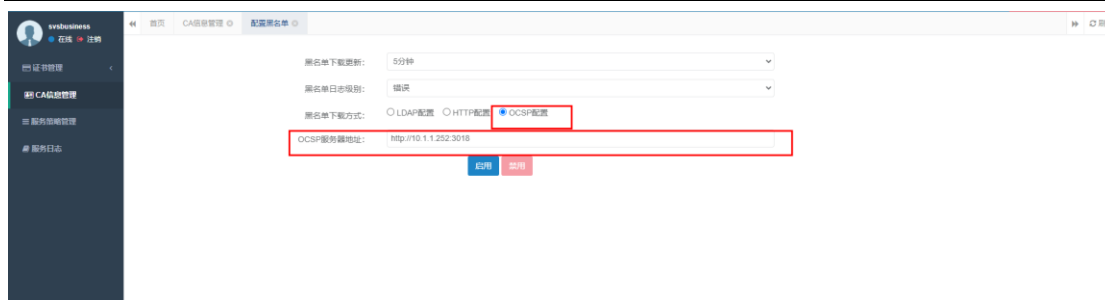
在配置黑名单页面，点击【禁用】按钮，则证书链黑名单不会再定时下载更新，如图



图表 45：禁用黑名单

5.4.3. OCSP 配置

【CA 信息管理页面】，选择一条 CA 信息，点击“配置黑名单”按钮，选择“OCSP 配置”，然后配置正确的 OCSP 服务器地址，最后点击“启用”按钮。



图表 46 配置 OSCP

第六章 服务管理

每个签名验签服务都可以同时提供以下一个或多个功能

- RSA 签名与验签
- SM2 签名与验签

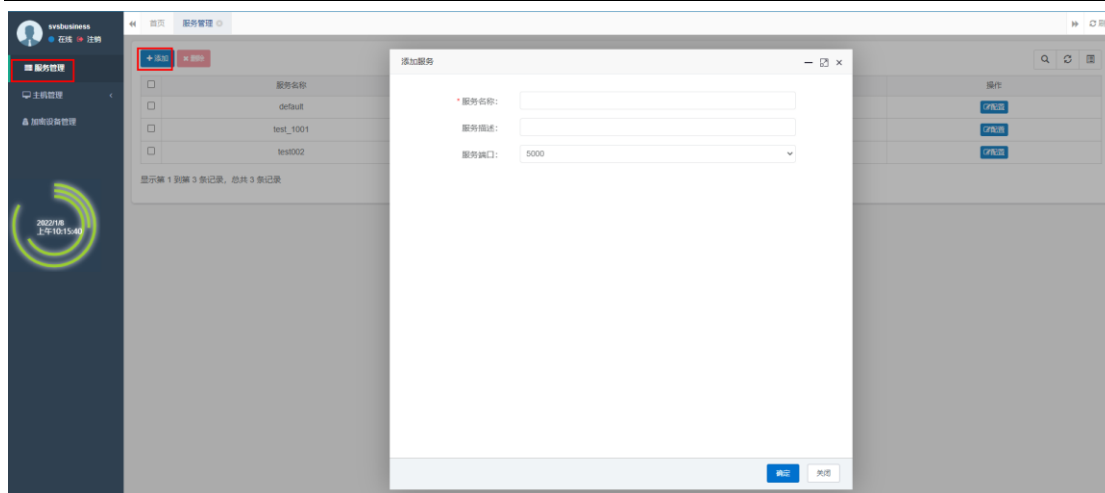
服务列表下有一个默认服务，也可以配置多个服务，服务列表中显示服务名称、服务描述、服务端口、服务类型、服务版本等，不同服务以服务名称进行区分，服务端口都为 5000。



图表 47：服务列表

6.1. 添加

系统可以添加多个服务，点击【添加】按钮，弹出添加服务页面，如图、



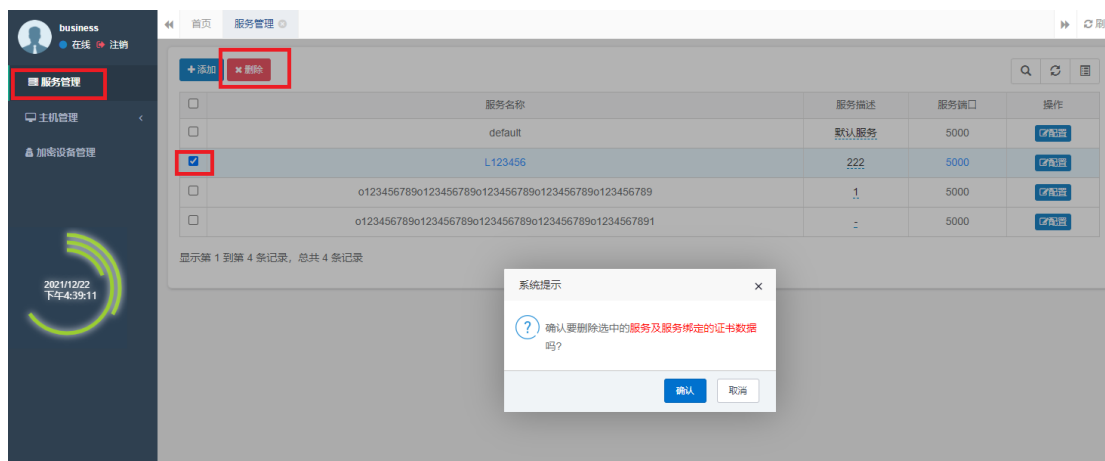
图表 48：添加服务

添加服务名称时，服务名称只能是数字或字母，并且以字母开头。不同服务以服务名称进行区分，服务端口都为 5000。

- 签名验签服务以服务名称进行区分，服务端口都为 5000。

6.2. 删除

选择一个或多个服务进行删除，删除服务成功。



图表 49 删除服务

- 服务删除后，服务中证书对应关系也会清空，服务删除时需谨慎。

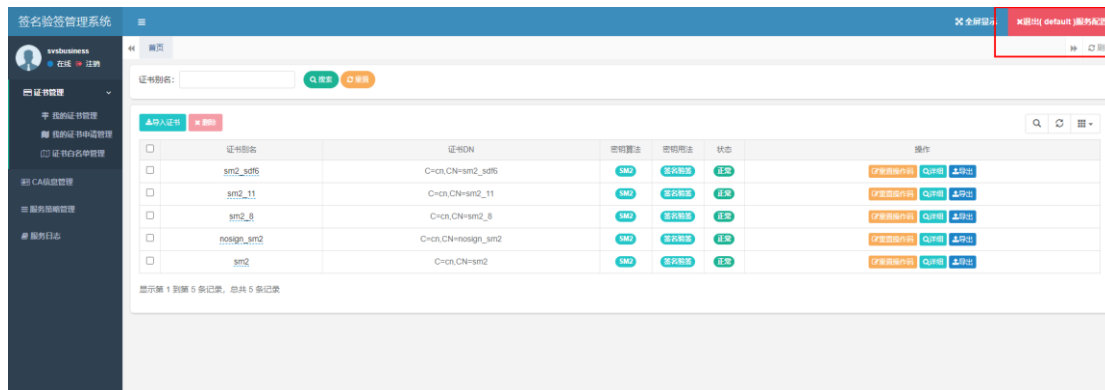
6.3. 配置服务

点击【配置】按钮，直接进入服务配置页面，可以配置服务各项信息，包括

【证书信息】，【CA 信息管理】，【服务日志】，【服务策略管理】等，[详情请参考第七章、第八章、第九章、第十章。](#)

6.4. 退出服务配置

进入服务配置页面后，如果想退出当前服务可以点击右上角的“退出服务配置”按钮，如下图所示：



图表 50 退出服务配置页面

第七章 证书管理

证书管理中包含了对服务涉及到的证书进行管理，包括证书和 CA 信息管理。

根据服务器的用途进行配置，TSA 服务器可用于：

- RSA 签名与验签
- SM2 签名与验签

请用户提前准备好需要使用的证书及证书链

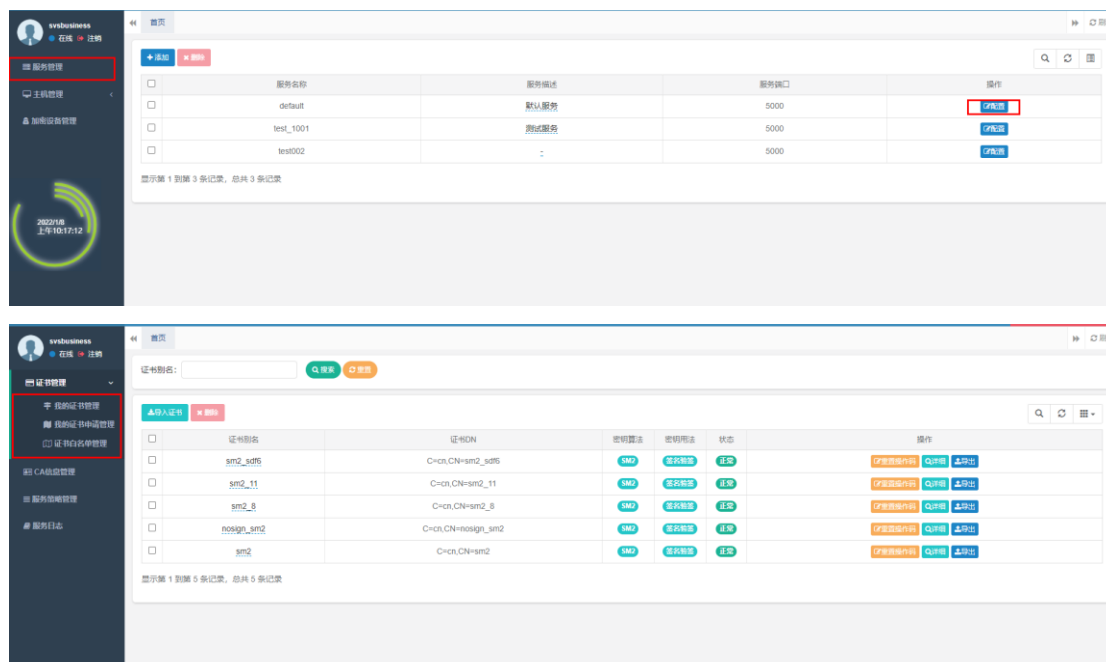
目前服务器的证书都是 CA 签发给签名验签服务的，签名验签服务使用证书进行签名表明自己的数字身份。

为了保障站点证书的唯一性，证书生成的流程是：

- 服务器生成证书请求。私钥本地产生和保存，将公钥及描述信息作为证书请求。
- 将证书请求发送到 CA 中心签发证书。
- 将签发的站点证书导入服务器与私钥匹配成功后完成证书生成。

目前，该版本的 TSA 服务器支持 RSA 签名证书和 SM2 签名证书。

点击服务后面的【配置按钮】可进入证书管理页面，如下图



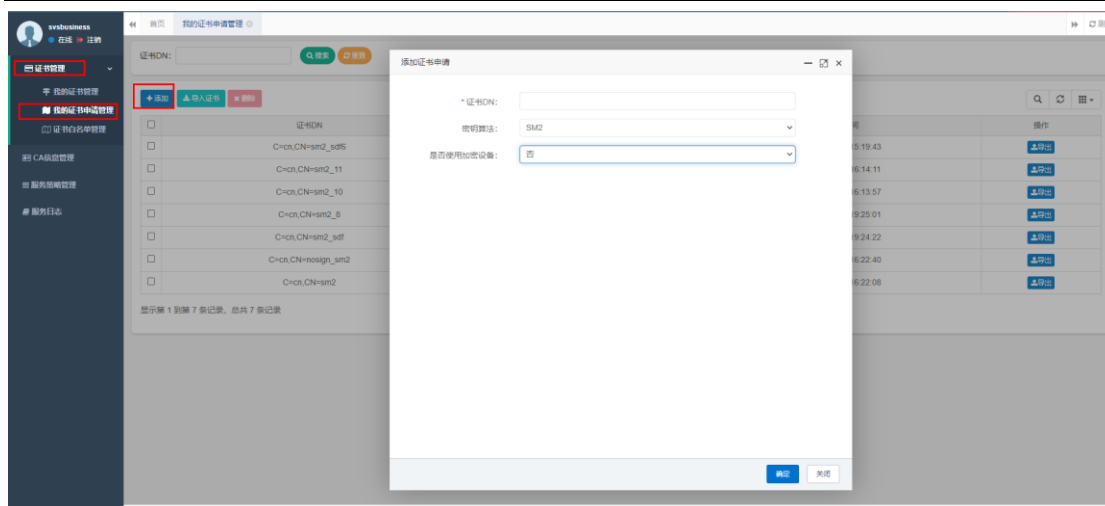
图表 51 证书管理页面

证书管理分为【我的证书管理】、【我的证书申请管理】和【证书白名单管理】三部分，【我的证书管理】中展示的是系统中已签发含私钥的证书；【我的证书申请管理】展示的是所有我们申请的证书请求，包含未签发和已签发的证书请求，【证书白名单管理】中展示的是需要白名单验证的证书信息。

7.1. 我的证书申请管理

7.1.1. 生成证书请求

在【我的证书申请管理】中，点击【添加】按钮，进入证书请求页面：



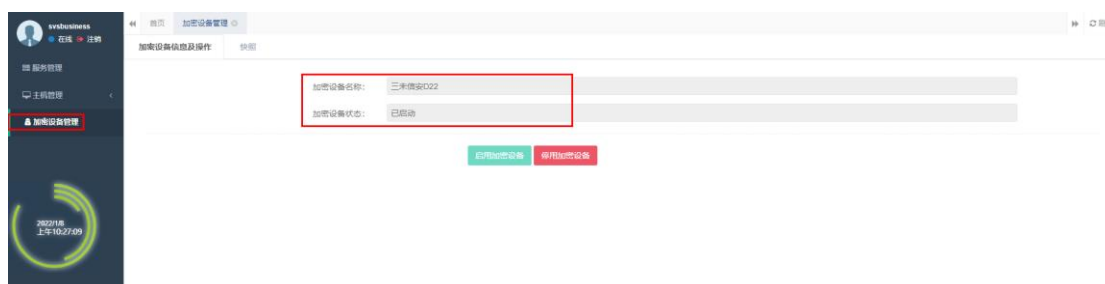
图表 52 添加证书请求

以上各个输入框的说明如下：

证书 DN：需填写正确且完整的 DN 信息。

密钥算法：展示证书请求的密钥算法，包含 RSA1024、RSA2048 和 SM2(默认)。

是否使用加密设备：默认为否。若使用加密设备申请证书，则需在安全管理员用户下【加密设备管理】菜单中加密设备已经启用前提下。



添加证书申请

* 证书DN:

C=CN,CN=格尔国信,O=北京,OU=项目管理部,ST=北京市,L=北京市

密钥算法:

SM2

是否使用加密设备:

是

密钥索引:

自动分配

确定

关闭

图表 53 使用加密设备申请-自动分配索引

添加证书申请

* 证书DN:

C=CN,CN=格尔国信,L=北京市,O=北京,OU=项目管理部,ST=北京市

密钥算法:

SM2

是否使用加密设备:

是

密钥索引:

手动输入

* 索引值:

7

确定

关闭

图表 54 使用加密设备申请-手动输入索引

当证书 DN 格式不正确会提示图所示信息，然后点击“确定”即可，完整的 DN 格式示例如下：

C=CN,O=OCA11,OU=ZHHRBC,CN=440500H100000127



图表 55：错误的 DN 格式请求

当加密设备索引被占用或加密设备未启用直接选用加密设备申请证书时会弹出如下提示信息



证书申请添加成功后可以在【我的证书申请管理】中看到该条状态为“待签发”申请信息。包含证书 DN、算法、状态、申请时间及操作功能如导出证书申请等。

7.1.2. 导出证书请求

选择一个证书请求，点击后面的“导出”按钮，可将请求导出，如下图：

图表 55 导出证书请求

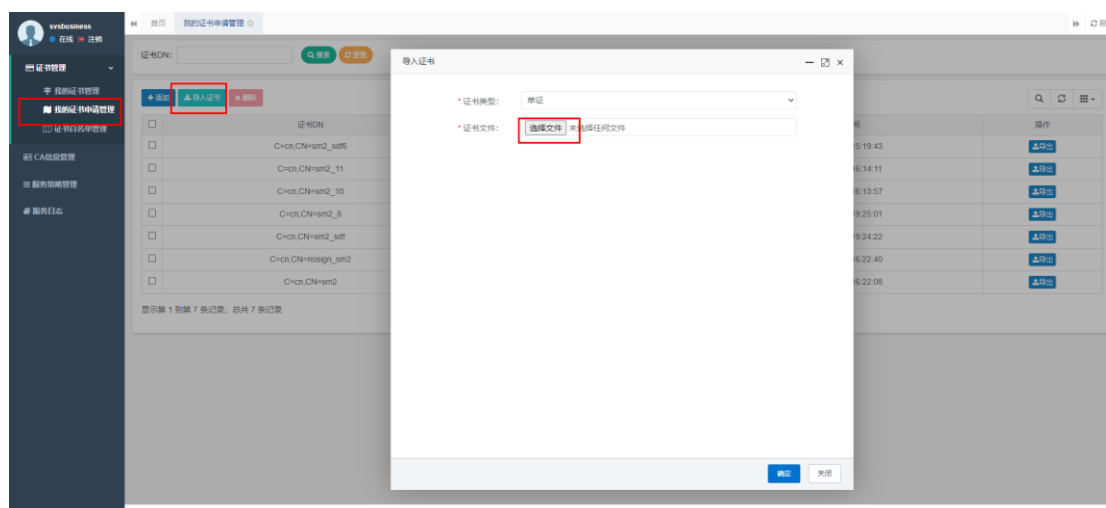
7.1.3. 申请证书

申请证书的过程是将生成的证书请求发送到 CA 中心，CA 中心根据请求签发证书，然后将证书文件返回给用户，用户得到证书文件后就可以进行最后一步操作：导入证书。

7.1.4. 导入证书

导入证书就是将 CA 中心签发的证书导入服务器中与相应的私钥匹配，形成完整的证书。导入正确证书后，服务才可以选择该证书。

点击“导入证书”按钮，弹出导入证书页面，选择从 CA 签发回来的证书，再点击“确定”按钮，系统将上传的证书文件与系统内的私钥进行匹配，如下图：



图表 56 导入签发后的证书

如果匹配成功就可以将证书导入服务器中，且该证书请求后面的状态会变为“已签发”，在【我的证书管理】中也会看到该证书。

如果匹配失败，则会报错，如下图：



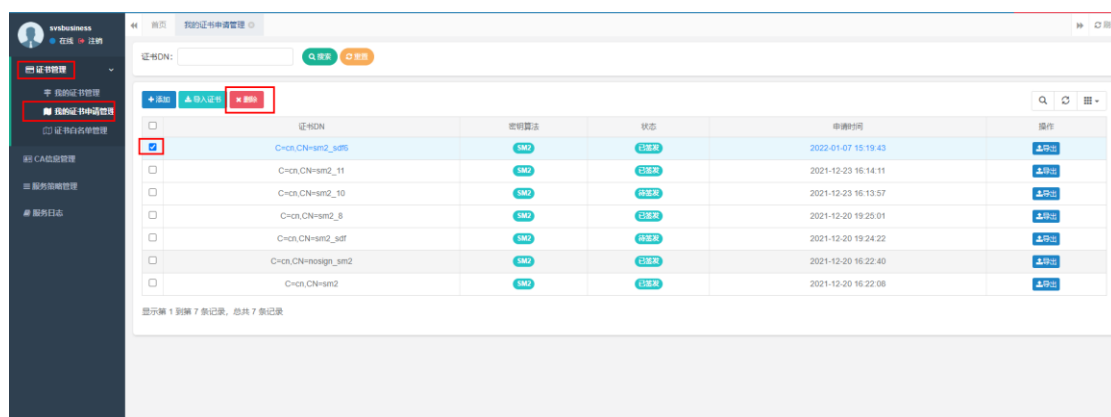
图表 57 导入与请求不匹配的证书

提示：

- 上传的站点证书文件必须为 **Base64** 编码。

7.1.5. 删除证书请求

证书请求也可以删除，点击某条证书请求后面的“删除”按钮就可以把该条请求删除；也可以选择勾选一个证书请求，点击左上角的“删除”按钮进行删除，如下图所示：



图表 58 删除证书请求

7.1.6. 查询证书请求

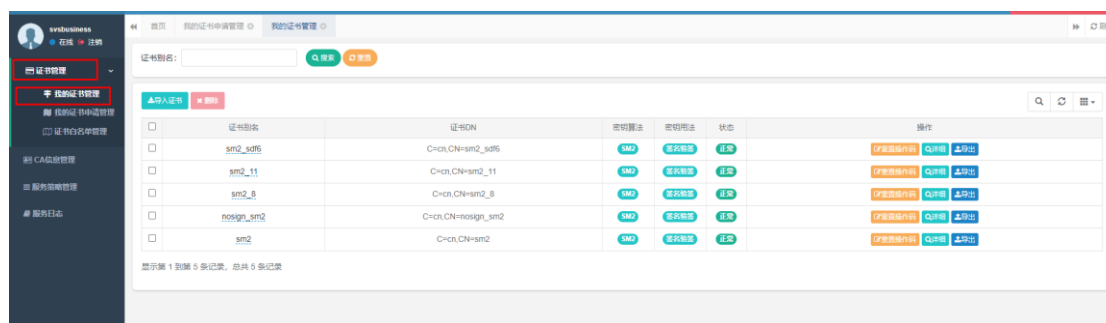
如果想查看某条证书请求的详细信息，但证书申请列表中请求很多时，也可以使用查询功能，在【我的证书申请管理】页面左上角“证书 DN 位置”输入需要查询的证书 DN，再点击“搜索”按钮，“重置”按钮可清除搜索框里的内容。

7.2. 我的证书列表

我的证书列表展示的是系统服务中带私钥的证书列表。

7.2.1. 查看我的证书

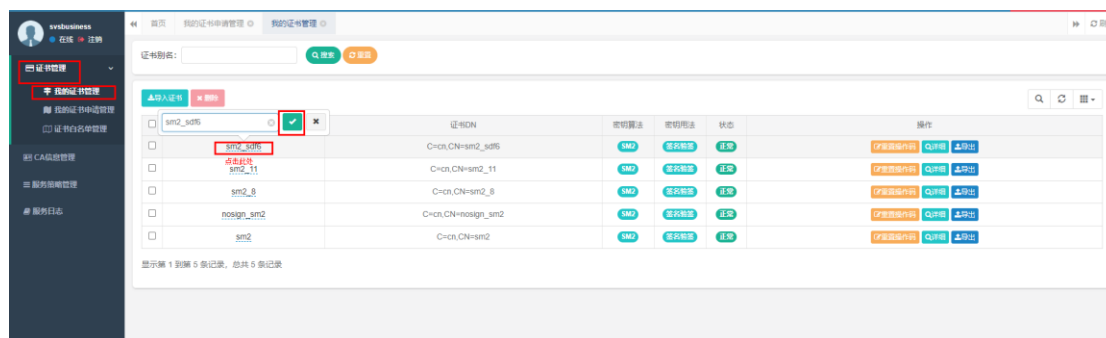
在证书管理页面中，点击【我的证书管理】按钮，进入我的证书管理页面，如图所示，可以查看系统服务所有带私钥证书。



图表 59 我的证书管理

7.2.2. 编辑我的证书

在“证书别名”列点击某个证书别名，即可修改证书别名，如下图所示：



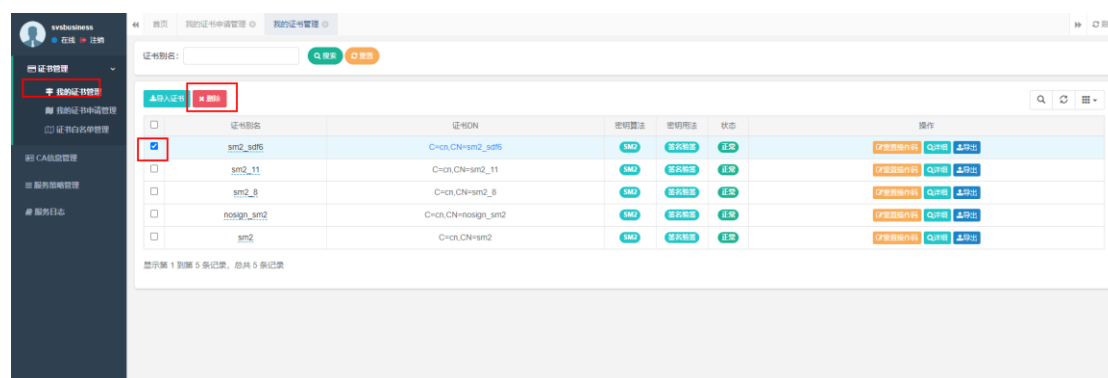
图表 60 编辑我的证书

7.2.3. 查询我的证书

当【我的证书管理】中列出的证书较多时，可以通过证书别名快速搜索需要的证书。

7.2.4. 删除我的证书

在我的证书管理页面中选中一条或多条需要删除的站点证书，点击“删除”按钮，所选中的站点证书将被删除。

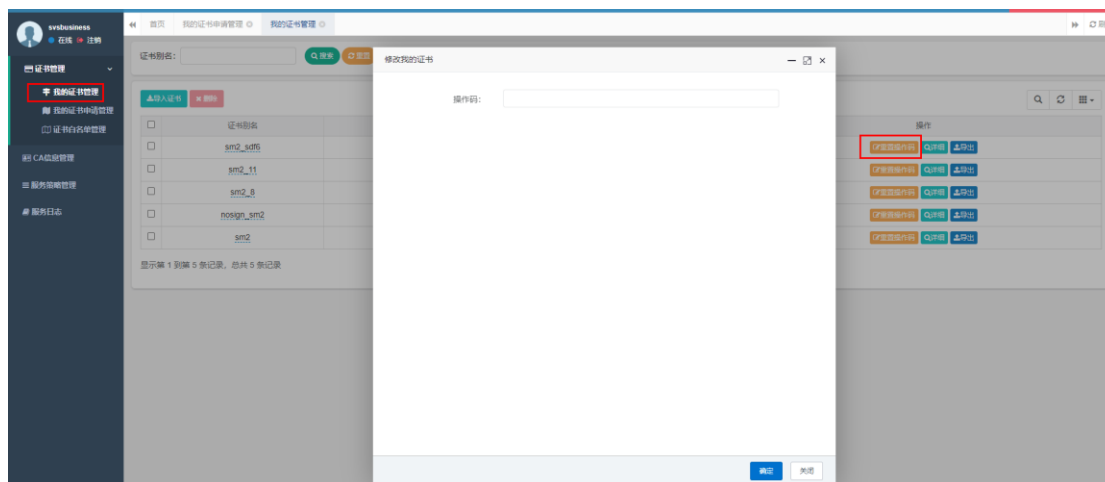


图表 61 删除我的证书

7.2.5. 重置操作码

证书支持设置操作码功能，已经设置操作码证书必须使用正确操作才能进行签名，否则不能使用该证书，点击我的证书后面的“重置操作码”按钮，在弹出的页面中输入操作码，然后点击“确定”按钮，证书的操作码就设置成功了，如下图：

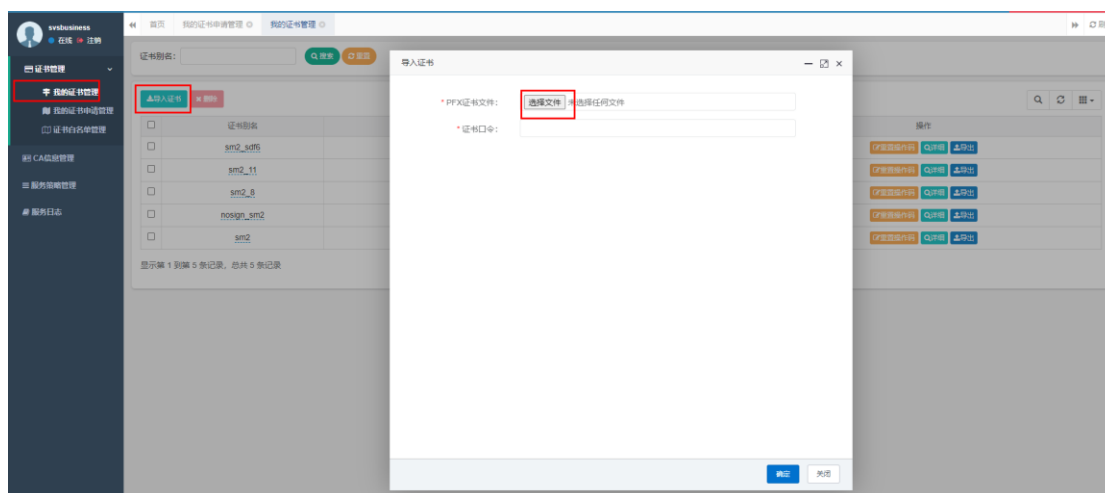
- 操作码为 8-16 个字符
- 操作码可以为空



图表 62 重置操作码

7.2.6. 导入 pfx 证书

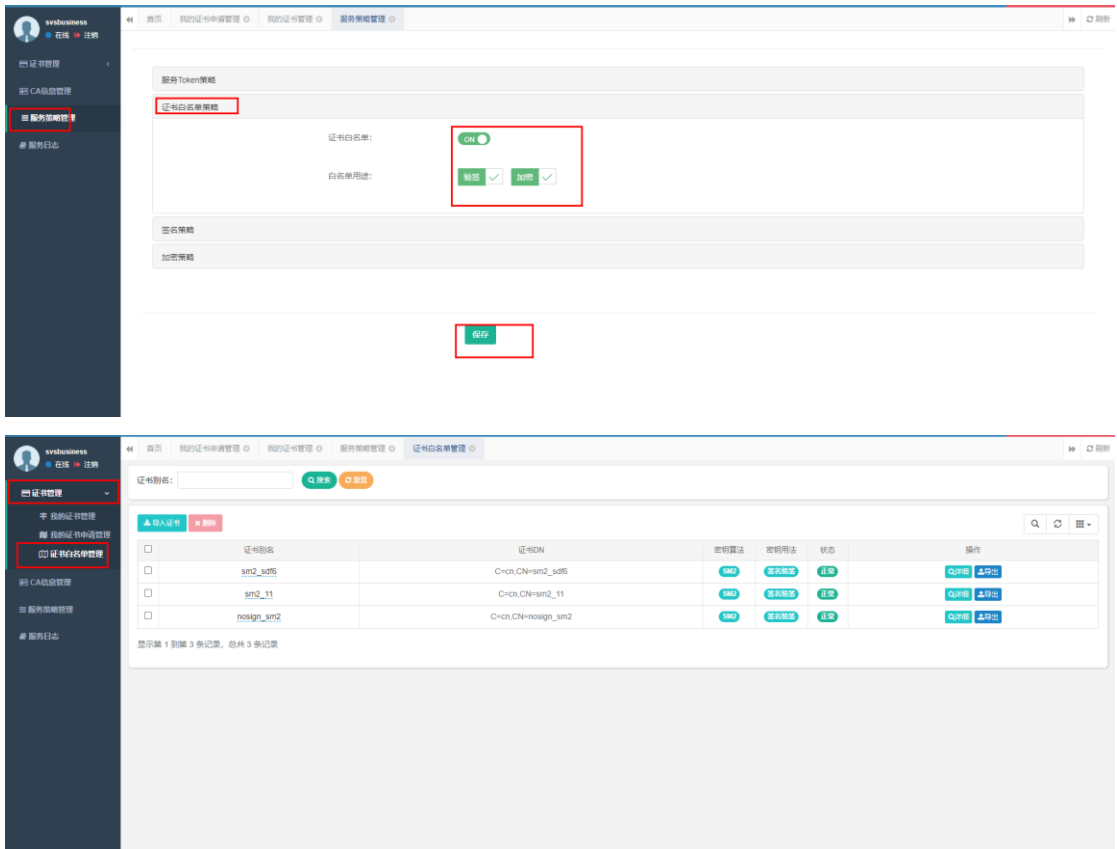
【我的证书列表】可以导入带私钥的.pfx 格式证书，点击【导入证书】按钮，弹出导入证书页面，如图，导入后新上传证书显示在列表中。



图表 63 导入 pfx 格式证书

7.3. 我的白名单

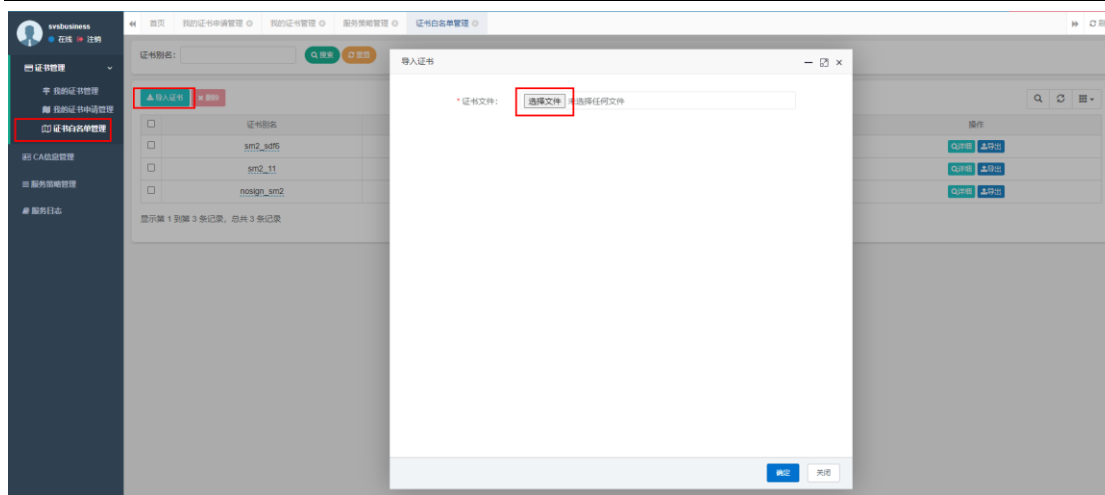
服务默认白名单状态为关闭，当业务验签或者加密时使用服务器证书时需开启白名单，配置方式在【服务策略管理】中，证书白名单策略为 on，白名单用途验签加密开启时，【证书白名单管理】菜单才可以正常显示，如图。



图表 64 证书白名单列表

7.3.1. 导入证书

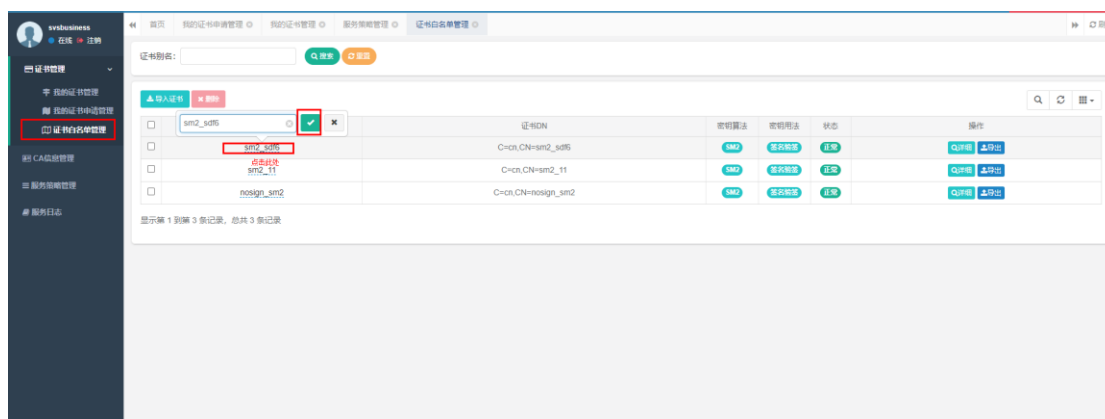
点击【导入证书】按钮，弹出【导入证书】页面，如图，浏览上传.cer 格式的证书，点击【确定】按钮，上传成功，证书显示在白名单列表中。



图表 65 上传证书

7.3.2. 编辑别名

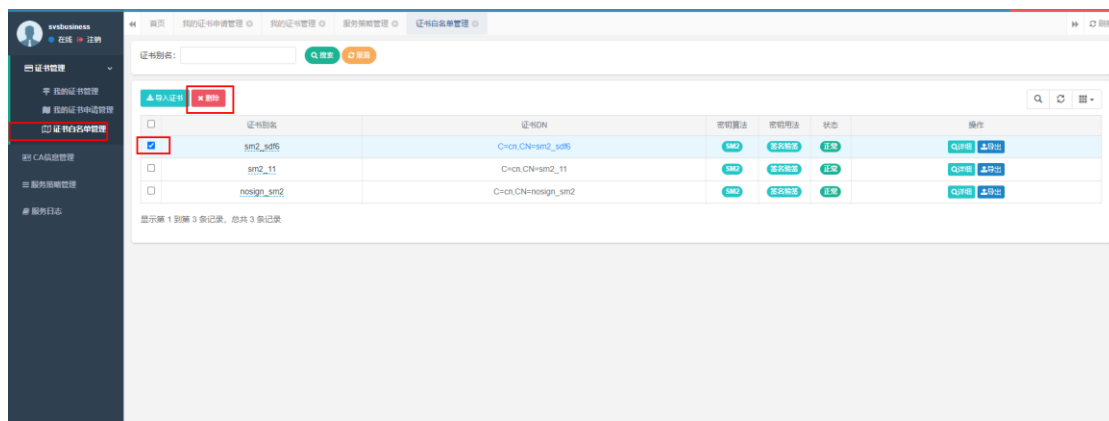
点击某个证书的别名，弹出修改别名提示框，修改别名后，直接点击“√”，证书别名修改成功。



图表 66 编辑别名

7.3.3. 删除

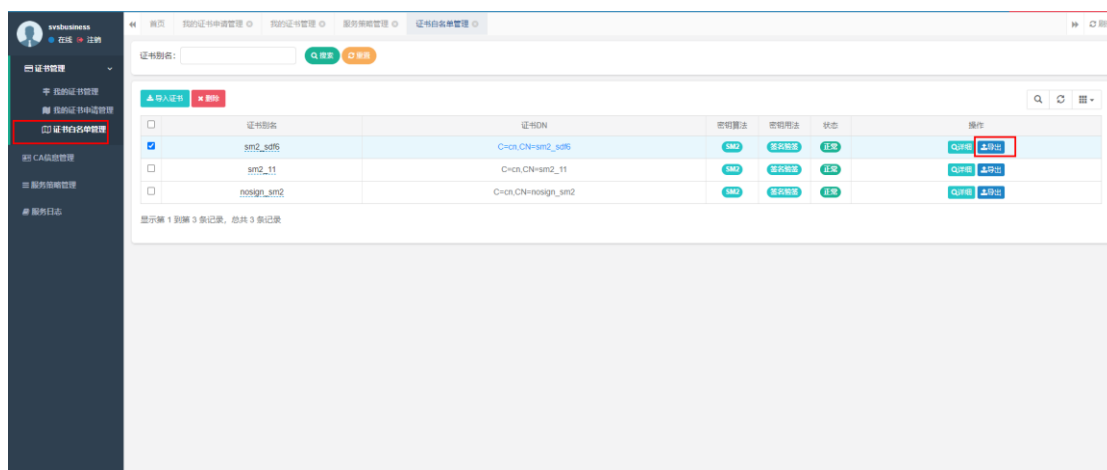
选择一个或多个证书，点击【删除】按钮，弹出确定要删除的数据条数，点击【确定】按钮，证书删除成功。



图表 67 删除证书

7.3.4. 导出

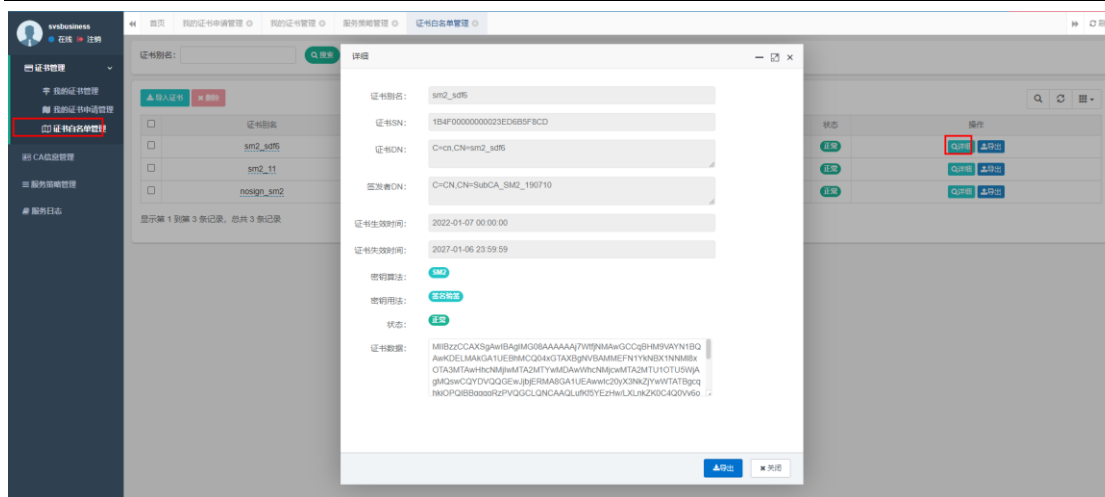
在相应证书后面点击【导出】按钮，可以导出证书到本地默认路径。



图表 68 导出证书

7.3.5. 详细信息

点击某个证书的【详细】按钮，弹出详细信息页面，如图，包括证书别名，证书 SN, 证书 DN, 签发者 DN, 证书生效时间、失效时间、证书算法、证书用法、状态、证书 base64 数据信息。



图表 69 证书详细信息

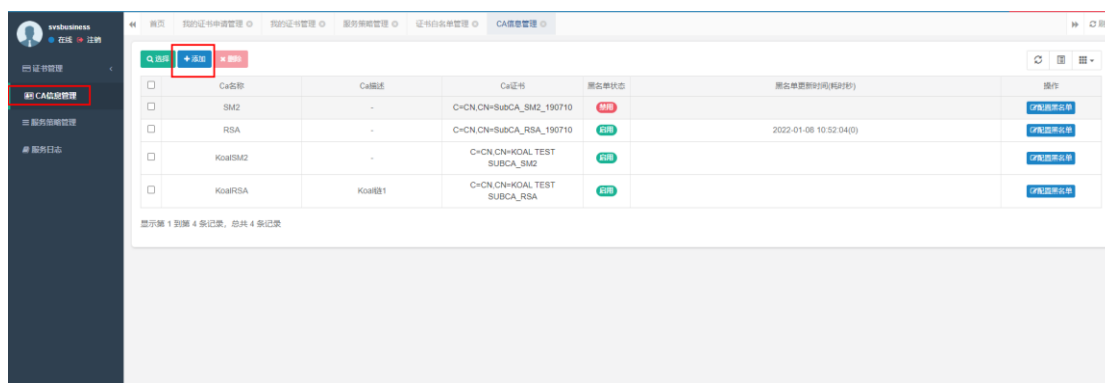
第八章 服务 CA 信息管理

8.1. 选择 CA

添加系统 Ca 文件后，在服务配置页面需选择该条 CA 后，服务才能验证此链下面的用户证书。

选择 CA 证书流程是：

- 在 CA 列表页面添加 CA 证书



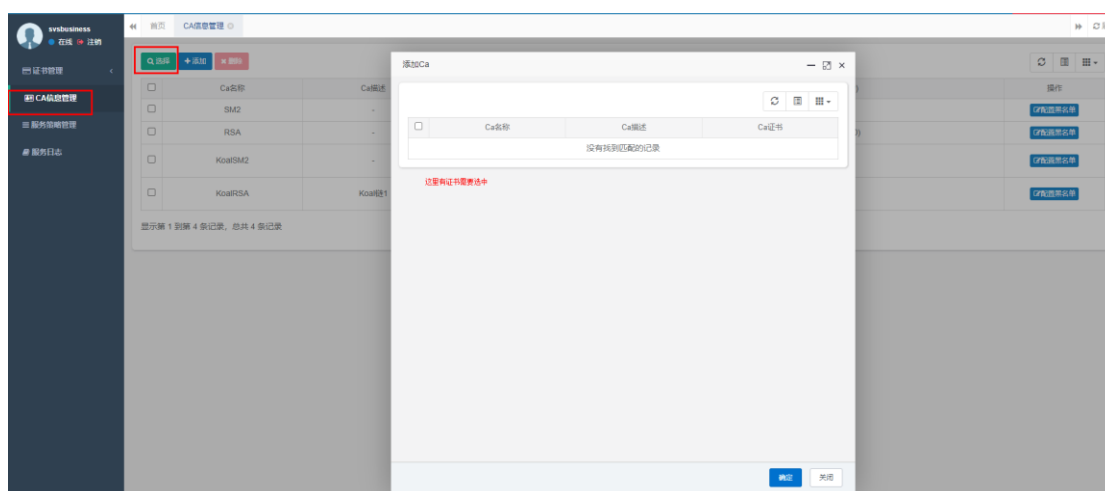
图表 70 添加 CA

- 进入服务配置页面



图表 71 进入服务配置页面

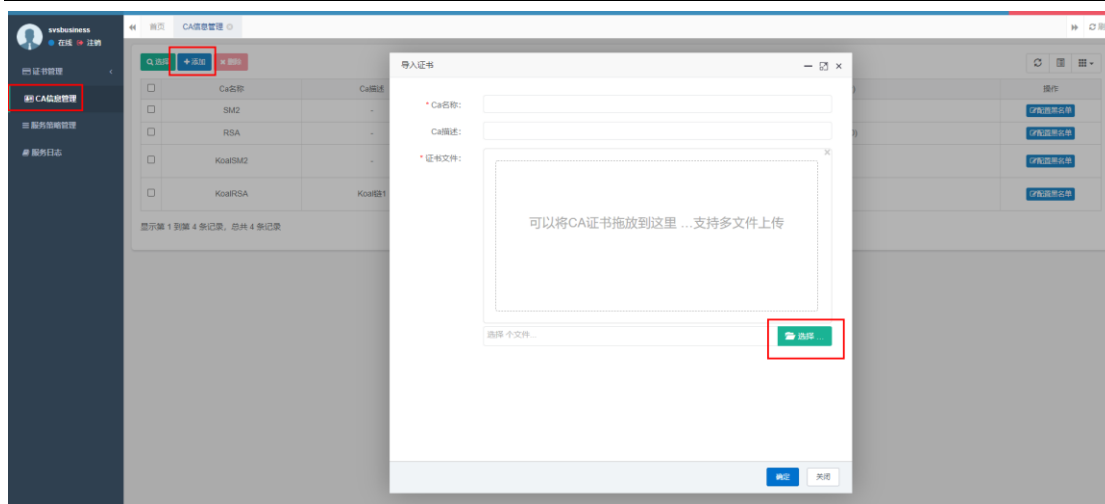
- 在服务配置页面中的【CA 列表】中点击“选择”按钮，勾选需要添加到服务的 CA，点击“确定”。



图表 72 服务选择 CA

8.2. 添加 CA

系统也支持在服务 CA 证书链菜单直接添加证书链，如图

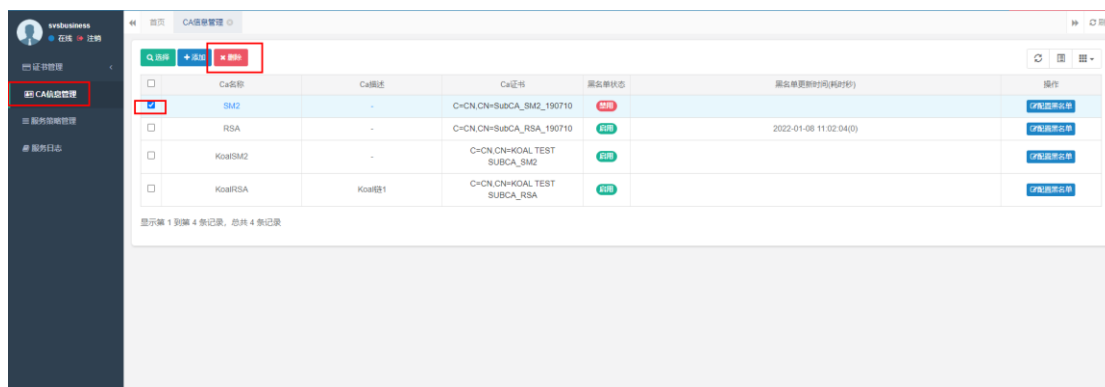


图表 73 服务直接添加证书链

- 提示：服务 **CA** 信息管理支持从系统 **CA** 信息中选择证书链，也支持直接添加证书链，添加完成的证书链会自动显示在系统 **CA** 中。

8.3. 删除 CA

选择一个或多个证书链，点击删除，则服务选用的证书链引用关系被删除。



图表 74 删除证书链

8.4. 查看 CA/配置黑名单

点击 CA 证书即可查看 CA 证书详情信息，[配置黑名单功能请参考 5.4 章节，配置黑名单。](#)

9.1. 服务日志

esbusiness 在线 注册

服务管理

主数据管理

新增设备管理

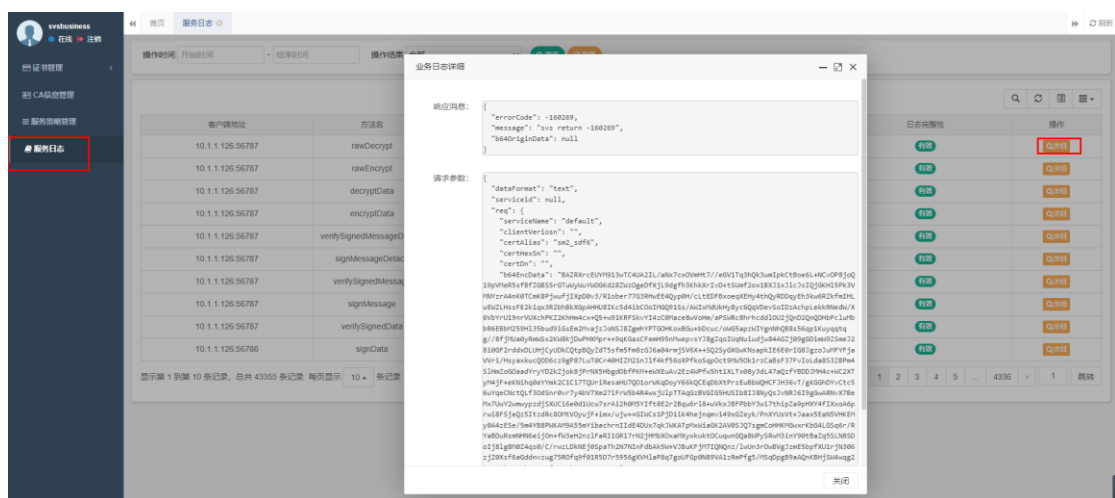
2023年11月11日 上午11:11:02

服务管理

新增 删除

☐	服务名称	服务描述	服务端口	操作
☐	default	默认服务	5000	编辑
☐	test_1001	测试服务	5000	编辑
☐	test002	测试服务	5000	编辑

显示第 1 到第 3 条记录, 总共 3 条记录

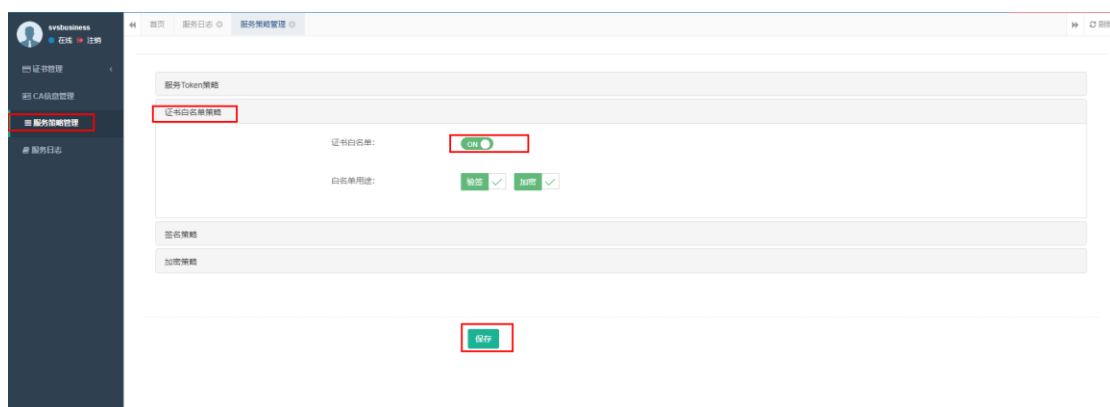


图表 75 服务日志

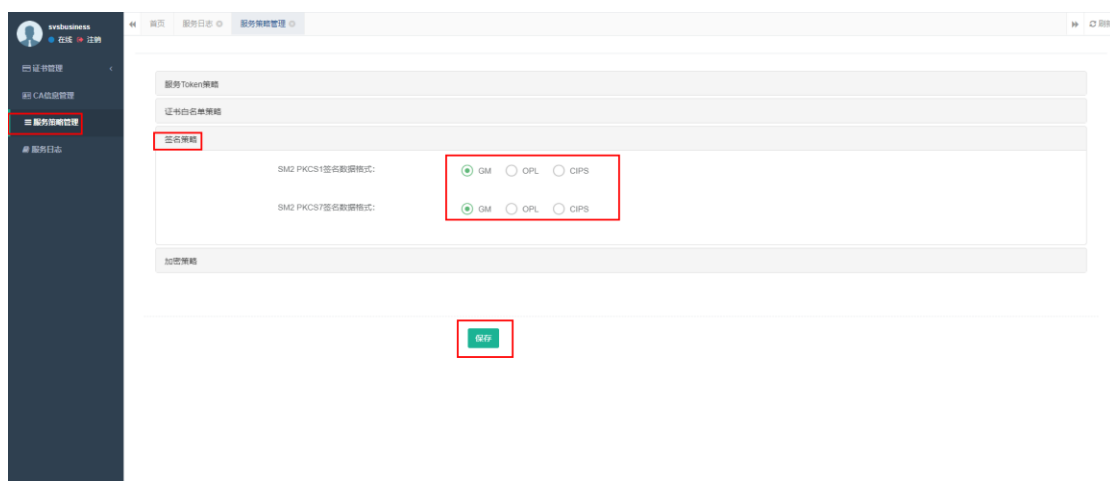
- 服务日志可显示日志的“方法名”、“操作结果”、“错误码”、“操作时间”、“日志完整性”和“操作”
- 点击“详细”按钮可以查看某一条日志的详细信息
- 可通过“操作时间”和“操作结果”查询操作日志。

第十章 服务策略管理

服务策略管理包括证书白名单策略、签名策略。



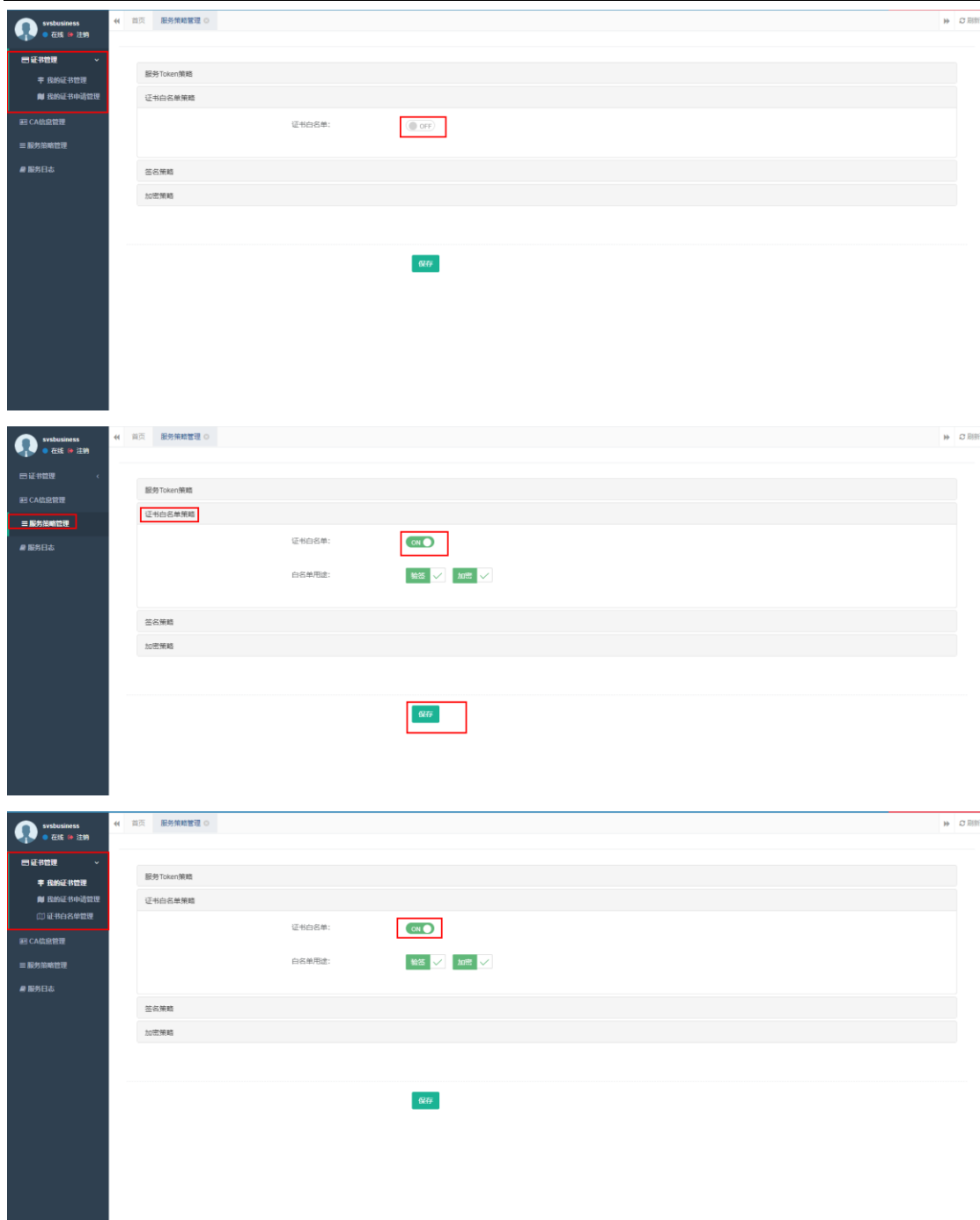
图表 76 证书白名单策略



图表 77 签名策略

10.1. 证书白名单策略

初次进入服务配置页面时，证书白名单默认为 OFF，没有【证书管理】-【证书白名单】菜单，当证书白名单设置为 ON 时，相应的【证书白名单】才显示出来，如图

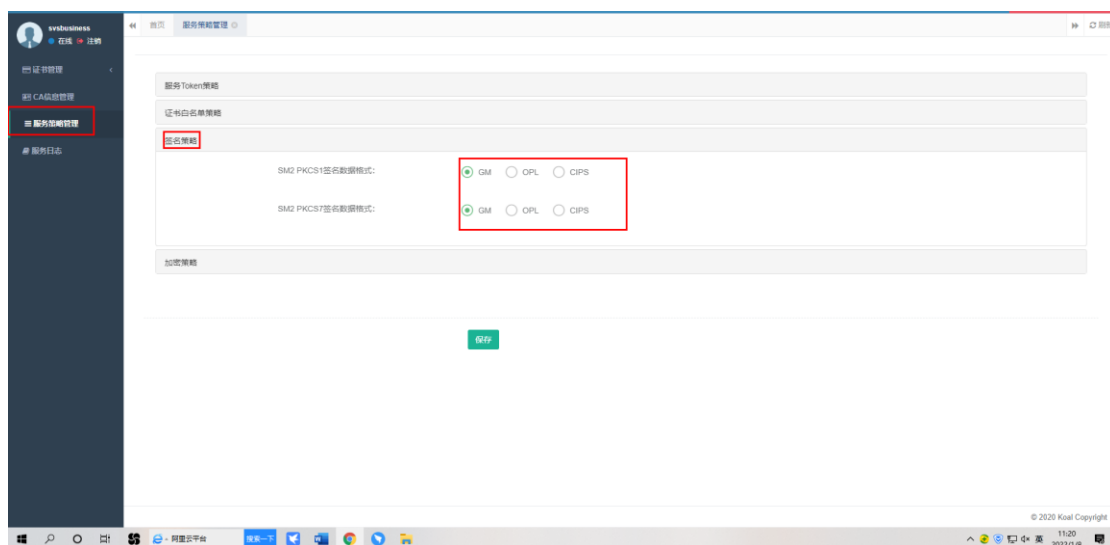


图表 78 证书白名单

证书白名单与黑名单相对应，如果开启了证书白名单，则系统验签加密时会验证白名单中的证书，未在白名单中的证书会验证不通过。

10.2. 签名策略

证书签名策略 SM2 PKCS1 和 PKCS7 默认都为 GM 格式。



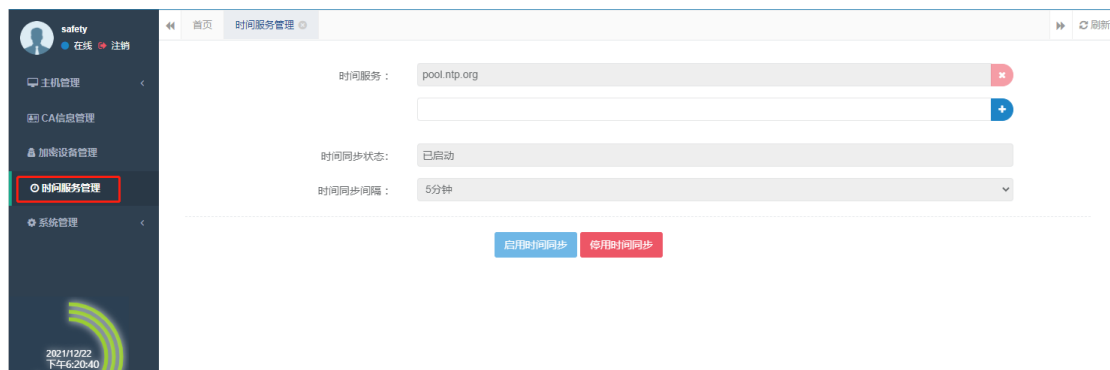
图表 79 证书签名策略

第十一章 时间服务器

11.1. 时间服务管理

系统时间支持远端及网络时间定时同步。

安全管理员进入【时间服务管理】菜单，在保证网络通畅的情况下，输入远端 IP 地址，可以点击“+”号输入多个远端 IP，选择同步时间间隔，点击【启用时间同步】按钮，系统会等待几秒，页面时间同步状态会由【已停止】变为【已启用】，系统会定时按同步时间间隔进行时间同步。



图表 80 启用时间同步

查看左下角可以看到系统时间。点击【停止时间同步】按钮则取消定时同步远端时间功能。

注意：系统支持设置多个时间服务器，优先使用第一个，若第一个时间服务器异常，系统会自动同步第二个时间服务器时间。

第十二章 日志查看

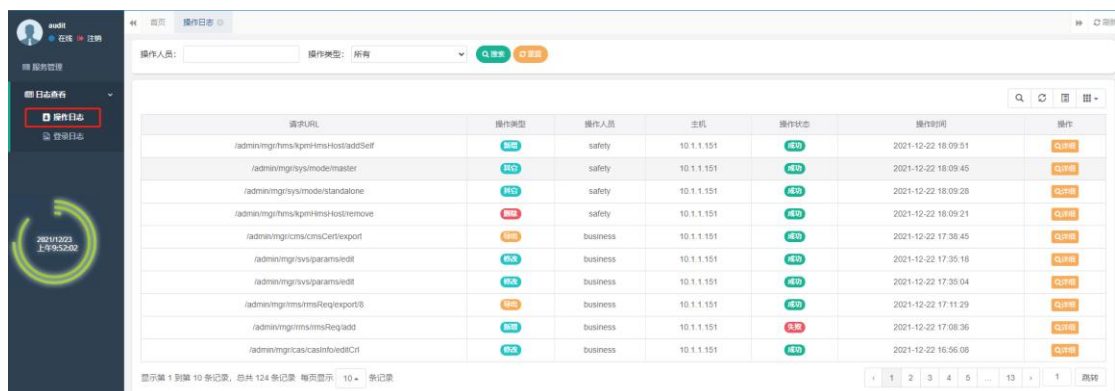
系统提供日志查看功能，包括登录日志和操作日志。通过日志便于排查系统层面出现的问题。方便日后审计工作。不同管理员查看的日志权限有所不同。

业务管理员具有查看所有管理员的登录日志和操作日志、

审计管理员具有查看业务管理员和安全管理员的登录日志和操作日志。

12.1. 操作日志

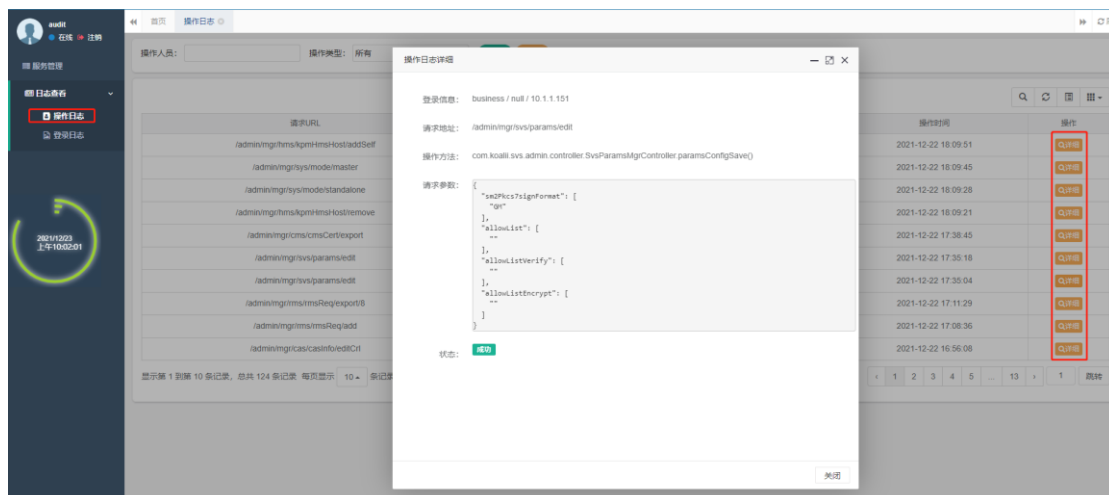
业务管理员登录，只可查看服务日志。审计管理员可查看操作日志、登录日志。



请求URL	操作类型	操作人员	主机	操作状态	操作时间	操作
/admin/mgr/cms/appr/cmsHost/addSelf	新增	safety	10.1.1.151	成功	2021-12-22 18:09:51	查看详情
/admin/mgr/sys/modemaster	修改	safety	10.1.1.151	成功	2021-12-22 18:09:45	查看详情
/admin/mgr/sys/modestandalone	修改	safety	10.1.1.151	成功	2021-12-22 18:09:28	查看详情
/admin/mgr/cms/appr/cmsHost/remove	删除	safety	10.1.1.151	成功	2021-12-22 18:09:21	查看详情
/admin/mgr/cms/cms/CmsExport	导出	business	10.1.1.151	成功	2021-12-22 17:38:45	查看详情
/admin/mgr/sys/params/edit	修改	business	10.1.1.151	成功	2021-12-22 17:35:18	查看详情
/admin/mgr/sys/params/edit	修改	business	10.1.1.151	成功	2021-12-22 17:35:04	查看详情
/admin/mgr/cms/cms/ReqReport@	导出	business	10.1.1.151	成功	2021-12-22 17:11:29	查看详情
/admin/mgr/cms/cms/Req/add	新增	business	10.1.1.151	失败	2021-12-22 17:08:36	查看详情
/admin/mgr/cms/cms/Info/editCtrl	修改	business	10.1.1.151	成功	2021-12-22 16:56:08	查看详情

图表 81 审计管理员-操作日志

- 操作日志分条展示，每条展示日志的“请求 URL”、“操作类型”、“操作人员”、“主机”、“操作时间”、“操作状态”、“操作”等。
- 每页默认显示 10 条，也可选择 25 或者 50 条
- 点击某条日志后面的“详细”按钮，可查看该条日志的详细信息

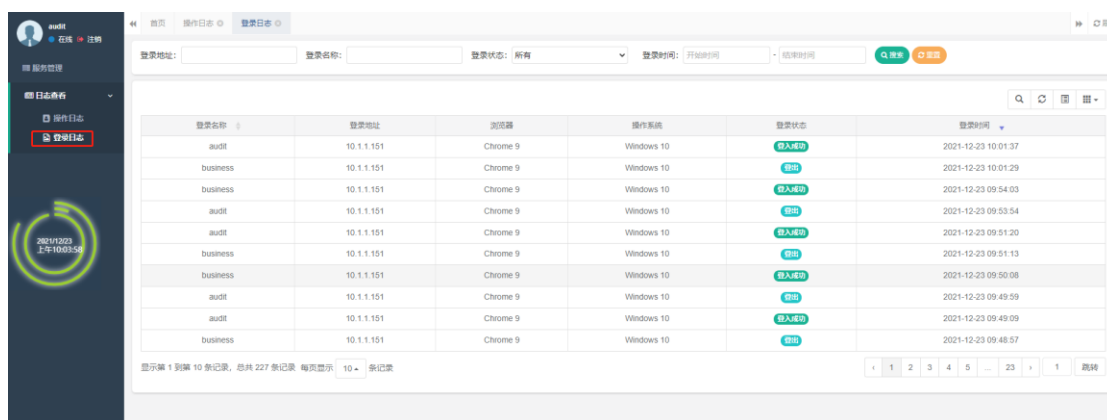


图表 82 查看详细日志

可按照“操作人员”、“操作类型”来查询操作日志。

12.2. 登录日志

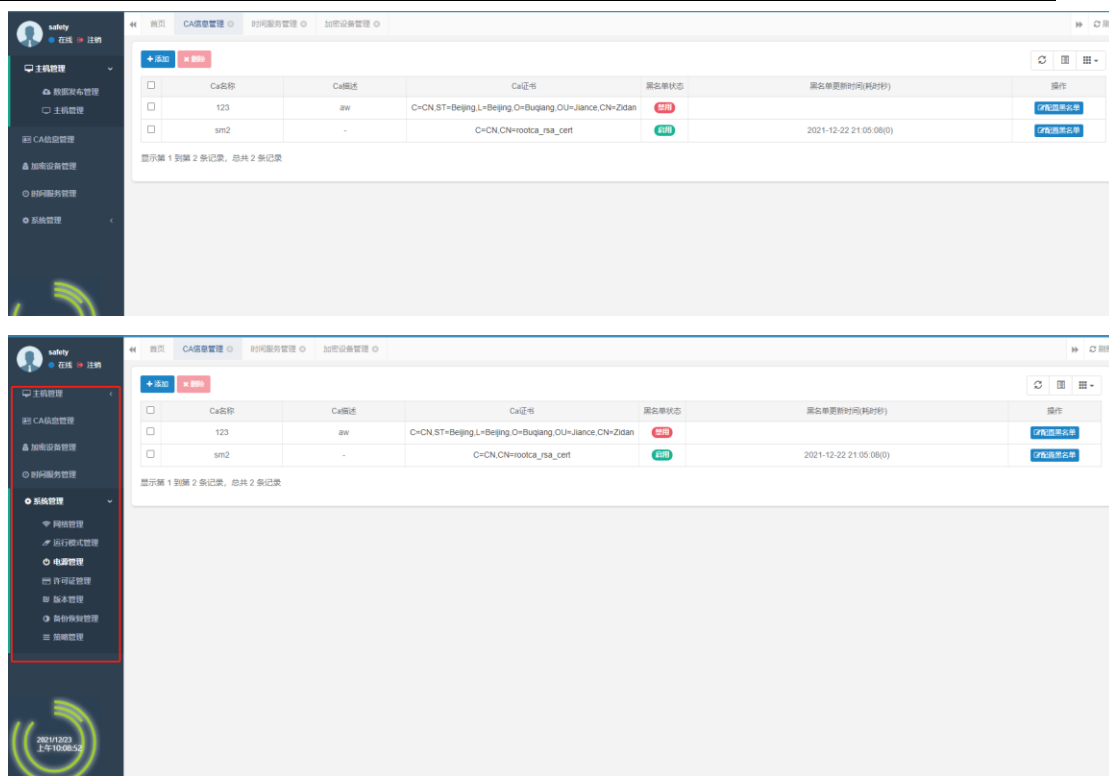
审计管理员登录可以查看登入系统的管理员名称，所用浏览器、登录地址，登录状态及操作系统、及登入时间。便于系统审计工作。



图表 83 审计管理员-登录日志

第十三章 系统管理

系统管理由安全管理员进行维护，包括网络管理、运行模式管理、电源管理、许可证管理、版本管理、备份恢复管理、策略管理。主机管理（数据发布管理、主机管理）、CA 信息管理、加密设备管理、时间服务器管理

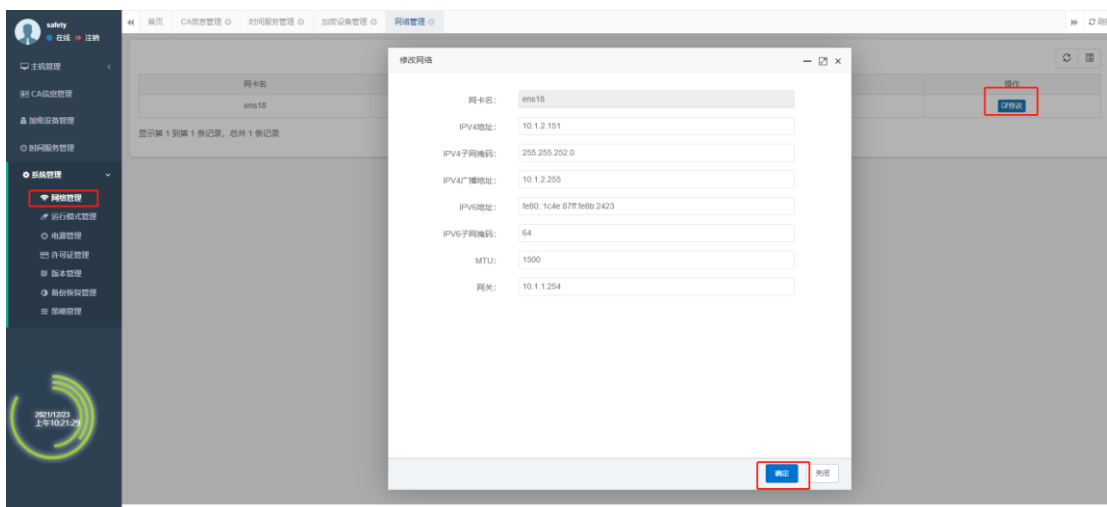


图表 84 系统管理页面

13.1. 网络管理

网络接口配置即网卡地址配置，网络地址代表了服务器在网络中所处的位置。配置了网络地址后，服务器的各项服务才能够正常启动，用户才能通过地址访问服务器，获取服务。

【网络管理】菜单用来配置系统网络，系统自动获取网卡名称，可以手动配置网卡的网络 IP 及子网掩码、网关信息，如图，保存后配置立即生效。



图表 85 修改网络配置

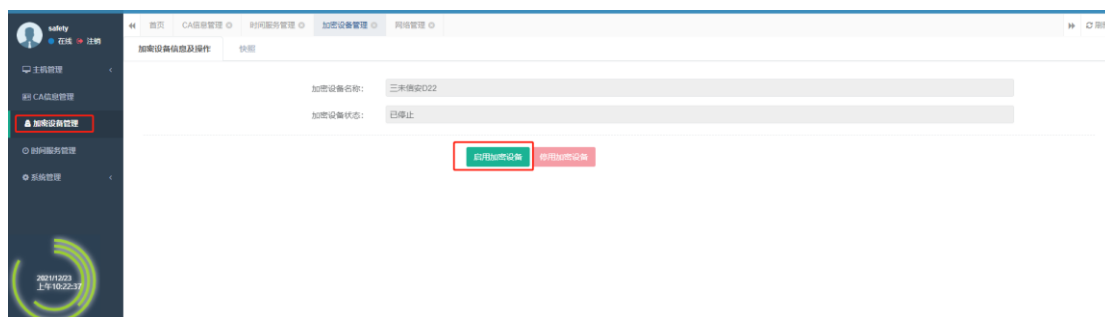
13.2. 加密设备管理

目前产品支持硬件三未信安 D22 加密卡和云平台密码机两款加密设备。

13.2.1. 硬件设备加密卡管理

13.2.1.1. 启用加密设备

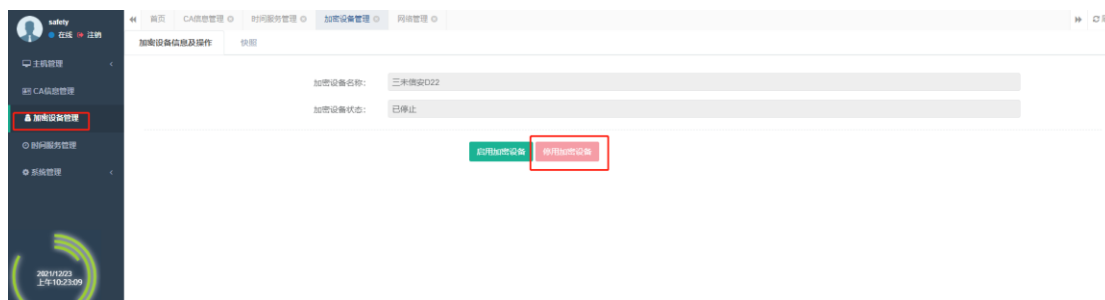
点击【加密设备管理】，进入加密卡管理页面，默认适配的为三未信安 D22 加密卡，点击“启用加密设备”按钮可启用加密卡，如下图，弹出提示，需重启系统加密卡配置才能生效。在安全管理员中对加密设备的操作会同步在业务管理员中。



图表 86 启用加密设备

13.2.1.2. 停用加密设备

在加密卡启动的状态下，点击“停用加密设备”，弹出停用成功提示，需重启系统加密卡配置才能生效。



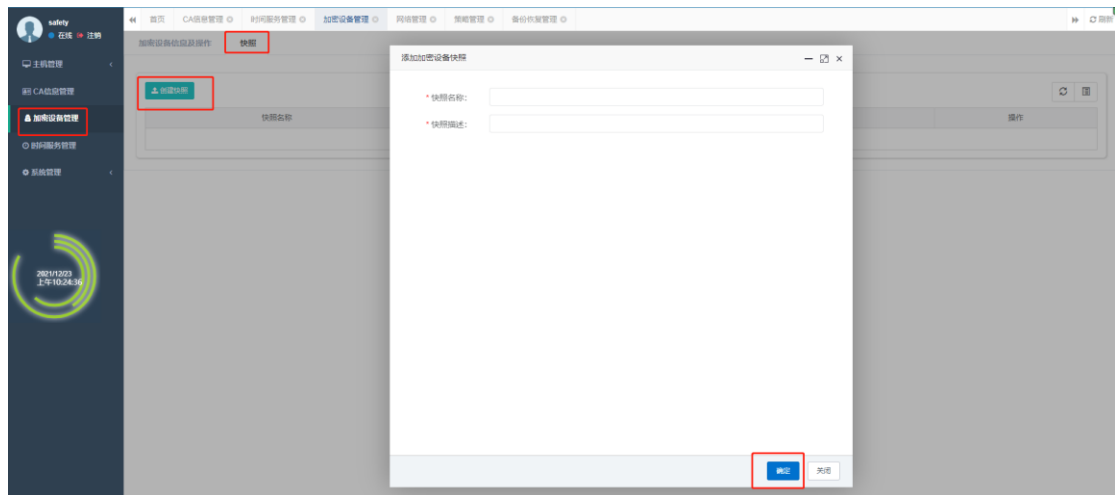
图表 87 停用加密设备

提示：加密卡配置启用或停用后需要重启系统配置才能生效。

13.2.1.3. 快照

■ 创建快照

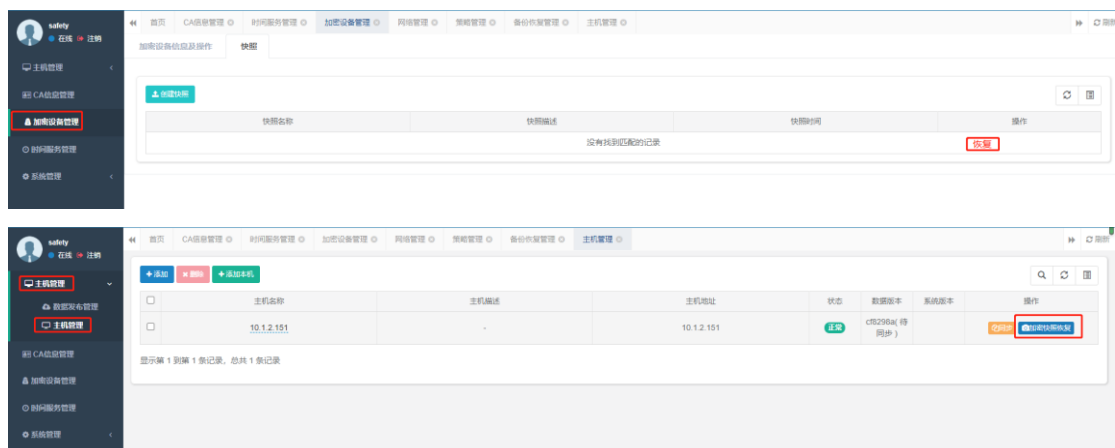
加密卡可以制作快照，点击“快照”按钮可以创建快照。



图表 88 创建快照

■ 恢复快照

快照是可以恢复的，点击“恢复快照”按钮可恢复制作快照时的加密卡状态，在【主机管理】页面也可以恢复快照。

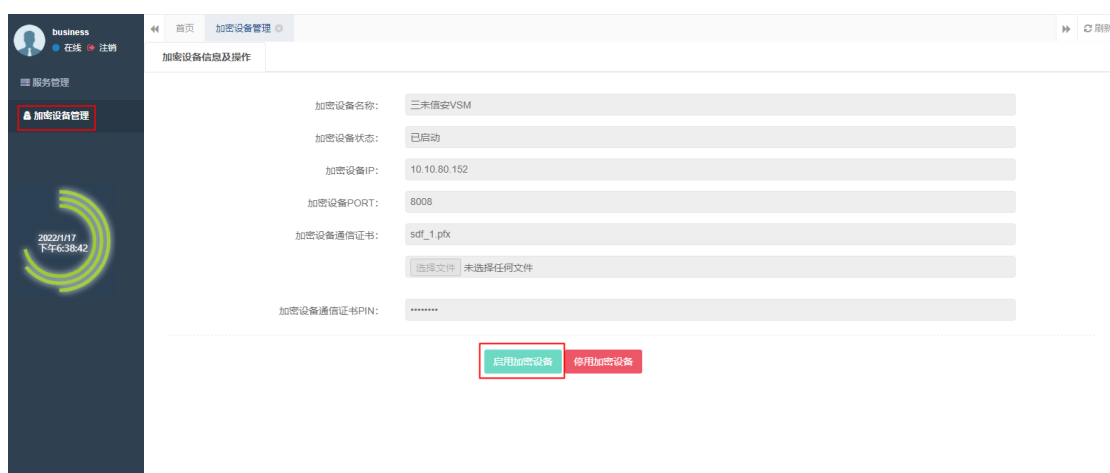


图表 89 恢复加密快照

13.2.2. 云平台加密设备管理

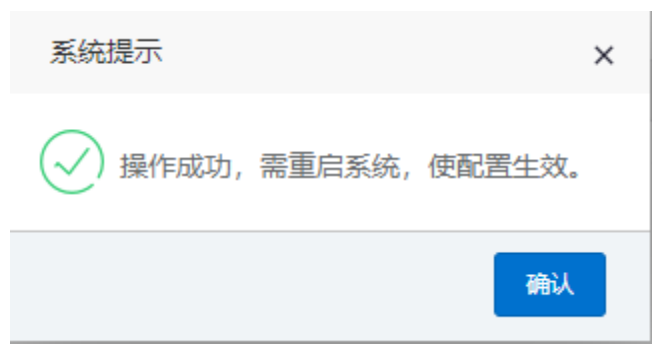
13.2.2.1. 启用加密设备

业务管理员或系统管理员登录系统，点击【系统管理】->【加密设备管理】，填写“加密卡名称”“加密设备 IP”“加密设备 PORT”、“加密设备通讯证书”、“加密设备通讯证书 PIN”，然后点击“启用加密设备”按钮，如下图：



图表 90 启动加密卡

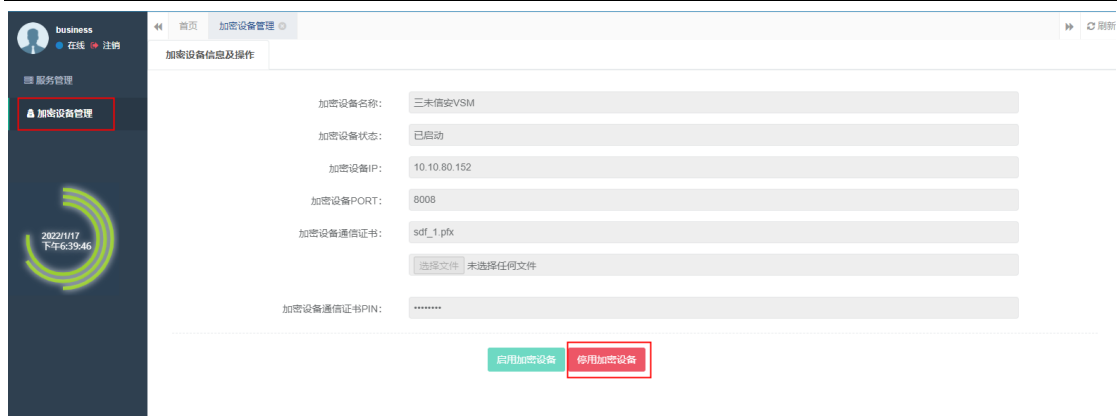
然后弹出提示“操作成功，需重启系统，使配置生效”，点击确定，然后重启系统。



注：如果需要点击【启用加密设备】按钮，必须先上传通讯证书。

13.2.2.2. 停用加密设备

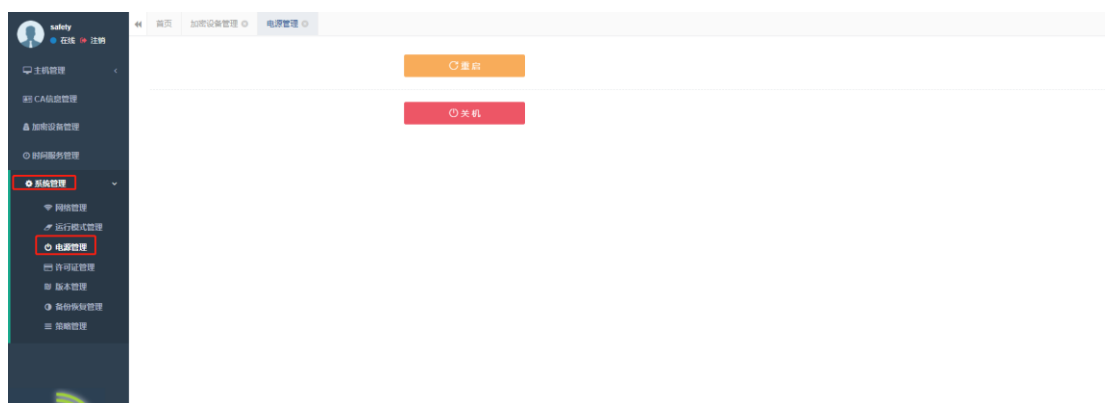
在加密卡启动的状态下，点击“停止加密卡”，即可停止加密卡的使用。



图表 91 停止加密卡

13.3. 电源管理

可以通过系统管理中的电源管理可关闭和重启系统。



图表 92 系统关机与重启

13.4. 许可证管理

自 2.4.7 版本开始增加了许可证管理，未签发许可证的设备会在页面右上角显示“未授权的设备”，如下图：

签名验签管理系统

未授权的设备 2.4.13.3 安全管理员 全屏显示

安全管理员 在线 注册

CA信息管理 加密设备管理 时间服务管理

系统管理

运行模式管理 电源管理 许可证管理 版本管理 备份恢复管理 策略管理

2022年1月17日 18:40:38

签发 详情

设备序列号: 0dad40ccaf77e847840327273bf351b247498aa2fd9d1b5b00b484fa163e066d02

签发方式: ☒ 在线方式 ☐ 离线方式

许可证服务地址:

许可证服务端口:

服务端证书: 选择文件

客户端证书: 选择文件

客户端私钥: 选择文件

私钥密码:

扩展项:

验证

图表 93 设备状态

目前使用的是离线方式授权，将签发好的 license 导入系统后系统授权成功。

签名验签管理系统

未授权的设备 2.4.13.3 安全管理员 全屏显示

安全管理员 在线 注册

CA信息管理 加密设备管理 时间服务管理

系统管理

运行模式管理 电源管理 许可证管理 版本管理 备份恢复管理 策略管理

2022年1月17日 18:41:36

签发 详情

设备序列号: 0dad40ccaf77e847840327273bf351b247498aa2fd9d1b5b00b484fa163e066d02

签发方式: ☐ 在线方式 ☒ 离线方式

上传许可证: 选择文件

验证

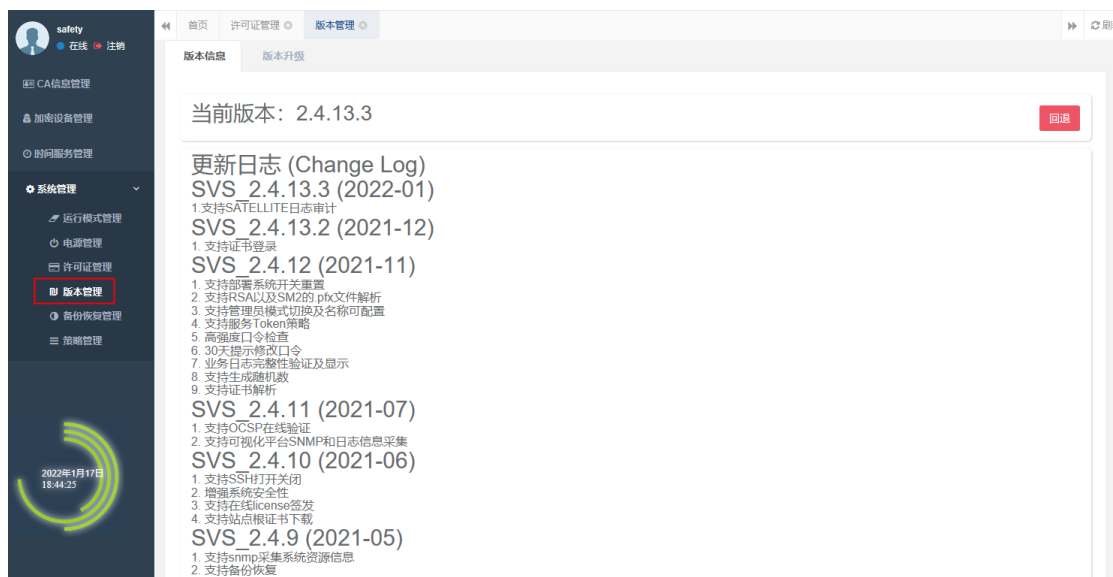
图表 94 许可证管理

13.5. 版本管理

点击【系统管理】->【版本管理】，进入版本管理页面，该页面分为版本信息和版本升级两个页面。

13.5.1. 版本信息

进入版本管理页面，可以看到该版本更新的功能，如下图：



图表 95 版本信息

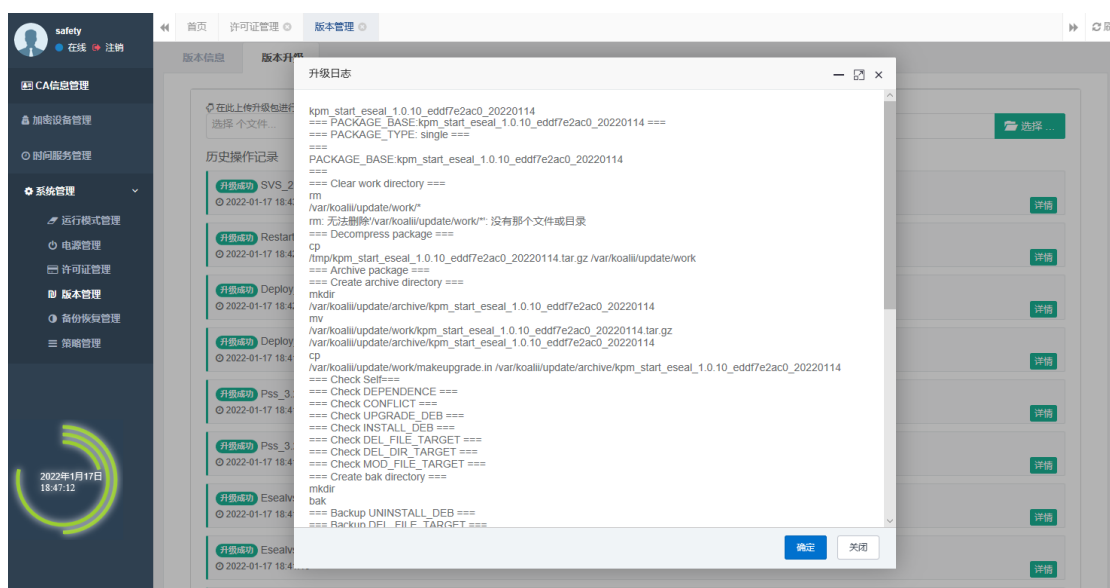
13.5.2. 版本升级

版本升级页面可以进行升级版本和查看升级历史，点击“选择”按钮可以上传安装包进行升级，升级包名称形如 TSA_2.4_UpdateXXX_ABS_2.4.X_ALL.zip。



图表 96 版本升级

升级完成后，列表展示已经升级的安装包信息，点击详情可以查看内部详细升级日志信息。



图表 97 查看详细升级日志

13.6. 备份恢复管理

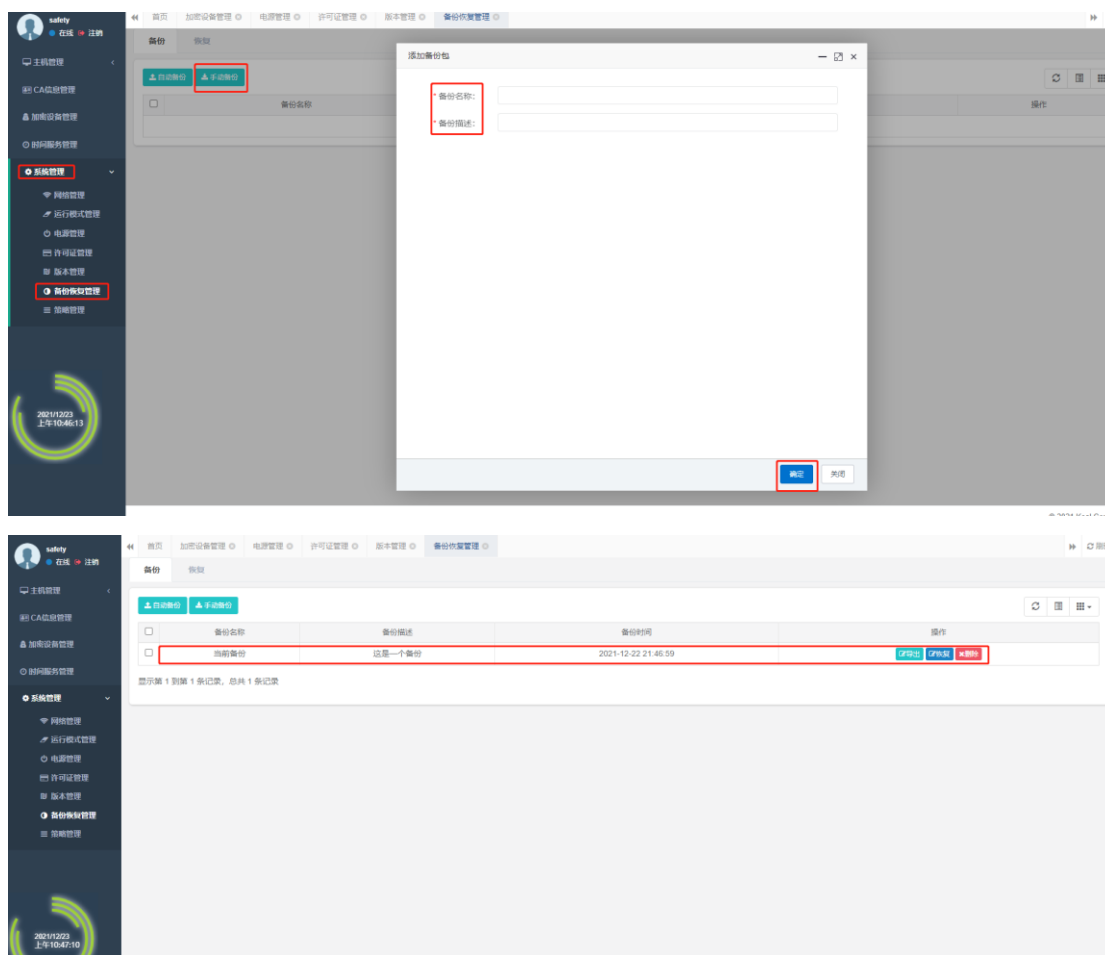
自 2.4.9 版本开始支持备份恢复功能，备份内容包含服务及服务相关配置。

13.6.1. 备份

备份分为自动备份和手动备份两种方式。主机的运行模式为单机或统一管理模式都支持备份作业。

13.6.1.1. 手动备份

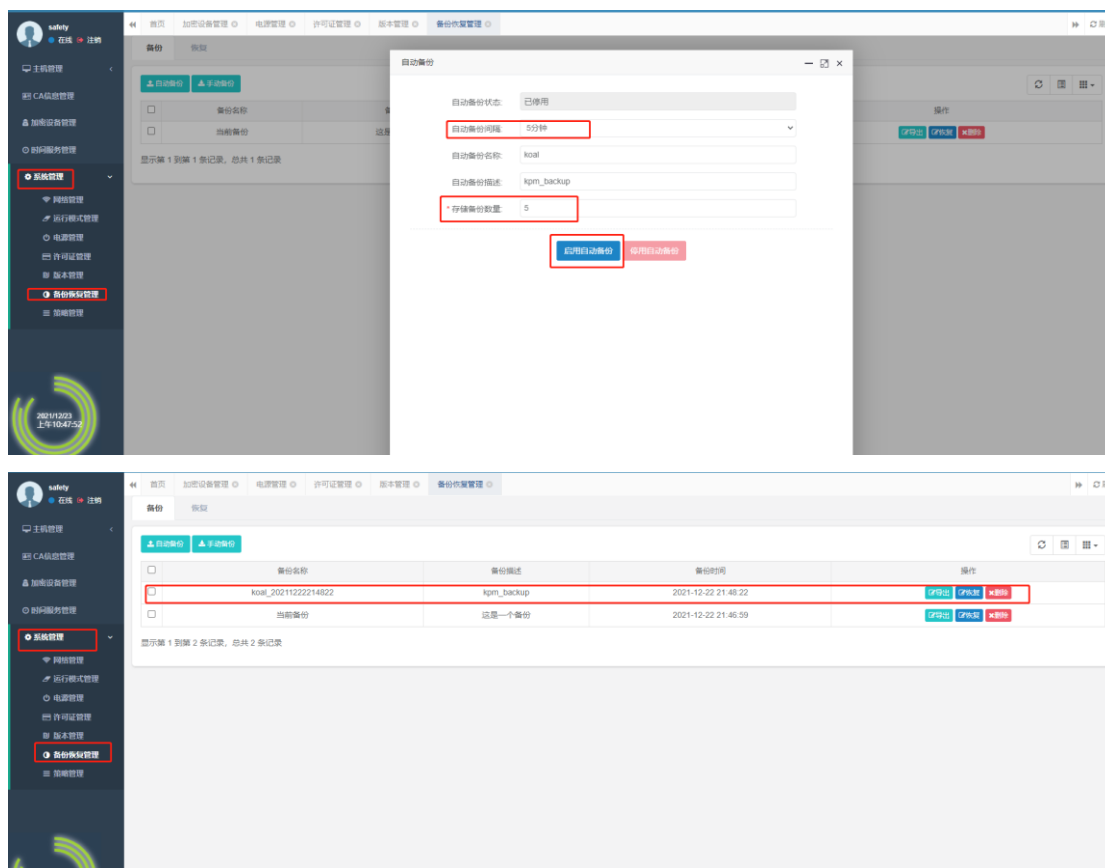
点击【系统管理】->【备份恢复管理】，点击手动备份，在弹出框中输入“备份名称”和“备份描述”，然后点击确定按钮即可，备份列表中会增加一条备份记录，如下图：



图表 98 手动备份

13.6.1.2. 自动备份

在【系统管理】->【备份恢复管理】，点击“自动备份”按钮，选择时间间隔和备份数量，点击“启用自动备份”按钮即可自动备份，如下图：



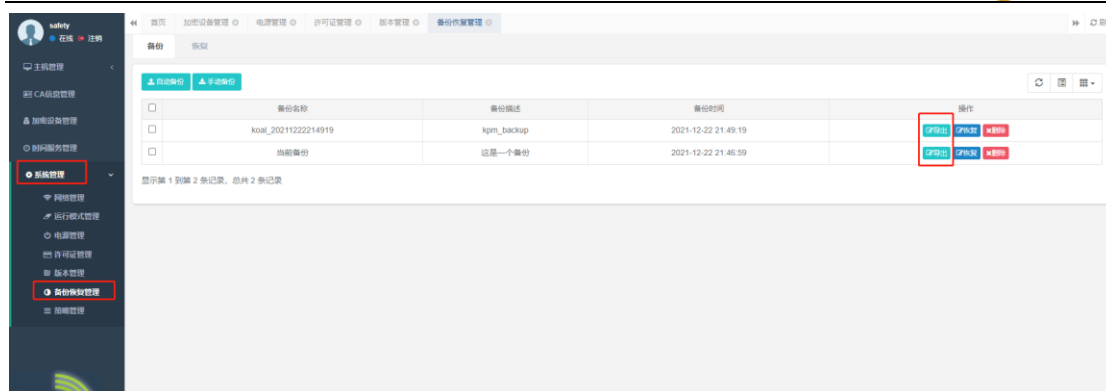
图表 99 自动备份

点击“停用自动备份”按钮即可停用自动备份。

当自动备份数量超过存储备份上限后，旧的备份包会自动回滚。

13.6.1.3. 导出备份

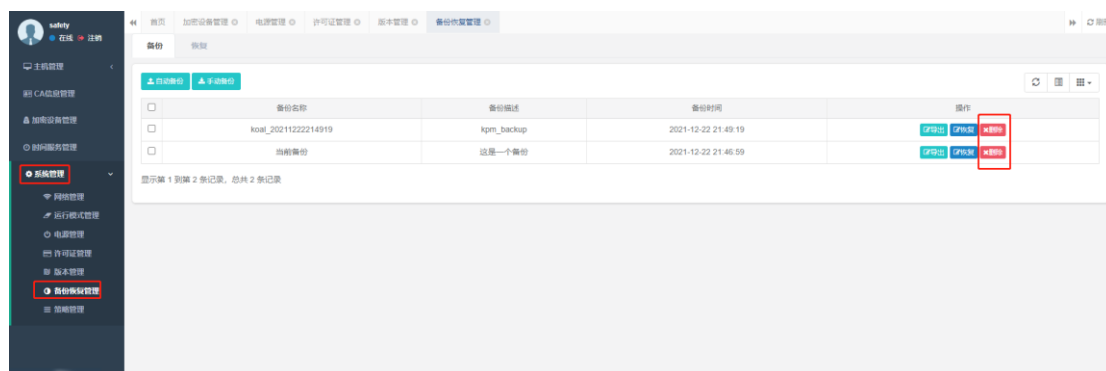
在【系统管理】->【备份恢复】管理页面，点击备份列表每条备份记录后面的“导出”按钮即可导出备份，如下图：



图表 100 导出备份

13.6.1.4. 删除备份

在【系统管理】->【备份恢复】管理页面，点击备份列表每条备份记录后面的“删除”按钮即可删除备份，如下图：



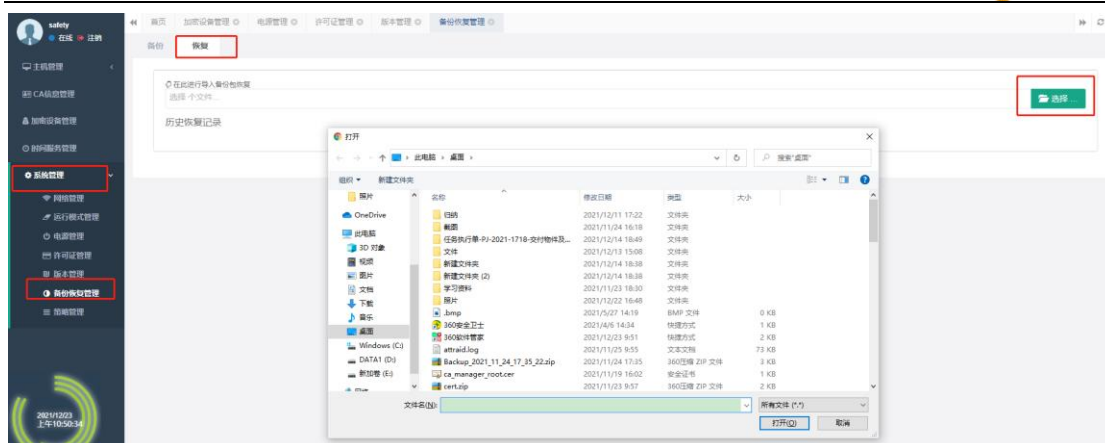
图表 101 删除备份

13.6.2. 恢复

恢复分两种模式，本地恢复和上传备份包恢复。主机的运行模式为单机或统一管理模式都支持恢复作业。

13.6.2.1. 上传备份包恢复

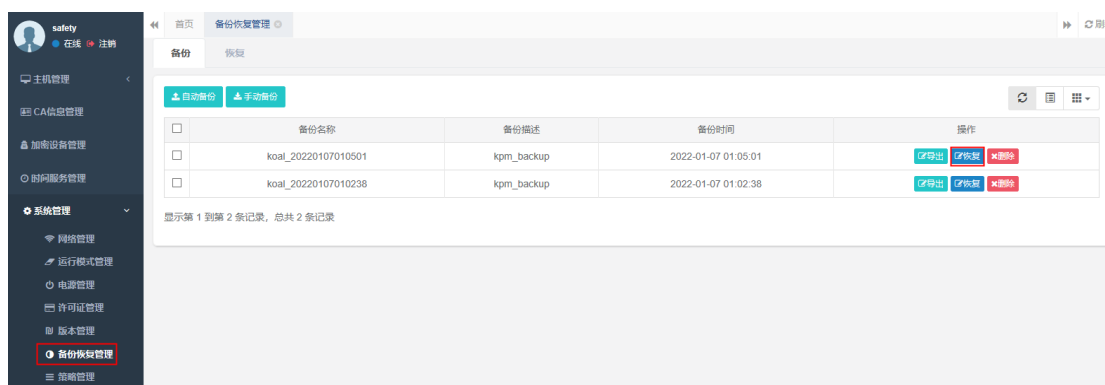
在【系统管理】->【备份恢复】-【恢复】页面，点击“选择按钮”，选择备份包上传到系统中，再点击“上传”按钮即可，如下图：



图表 102 上传备份包恢复

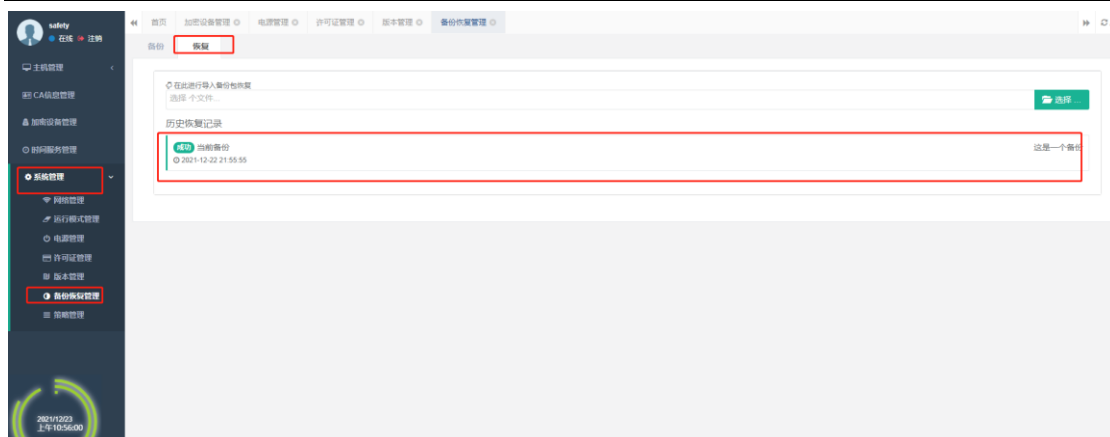
13.6.2.2. 本地恢复

在【系统管理】->【备份恢复】管理页面，点击备份列表每条备份记录后面的“恢复”按钮即可恢复备份，如下图：



图表 103 本地恢复

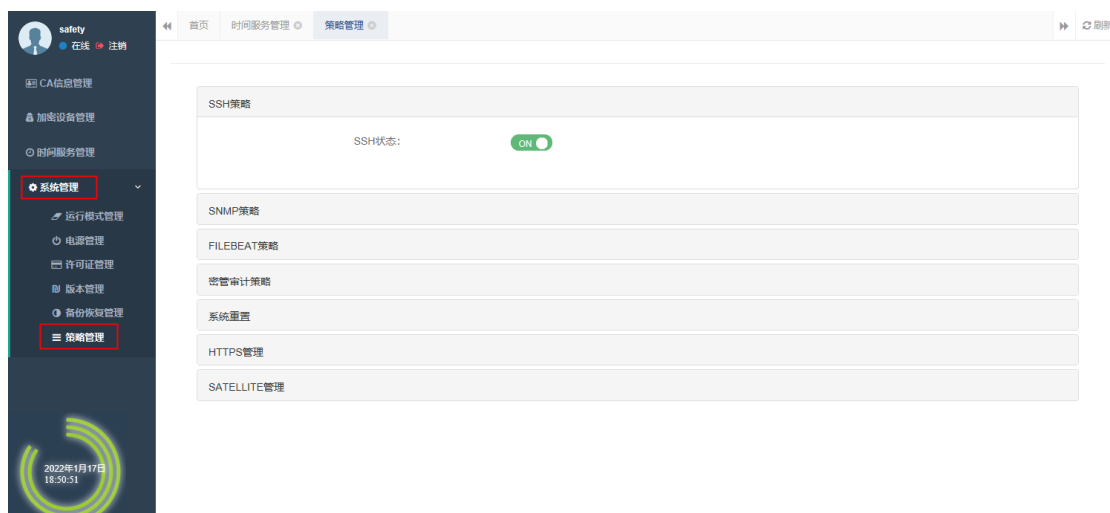
两种方式恢复完成后，在【系统管理】-【恢复】菜单可以看到所有的历史恢复记录。如图。



图表 104 恢复历史记录

13.7. 策略管理

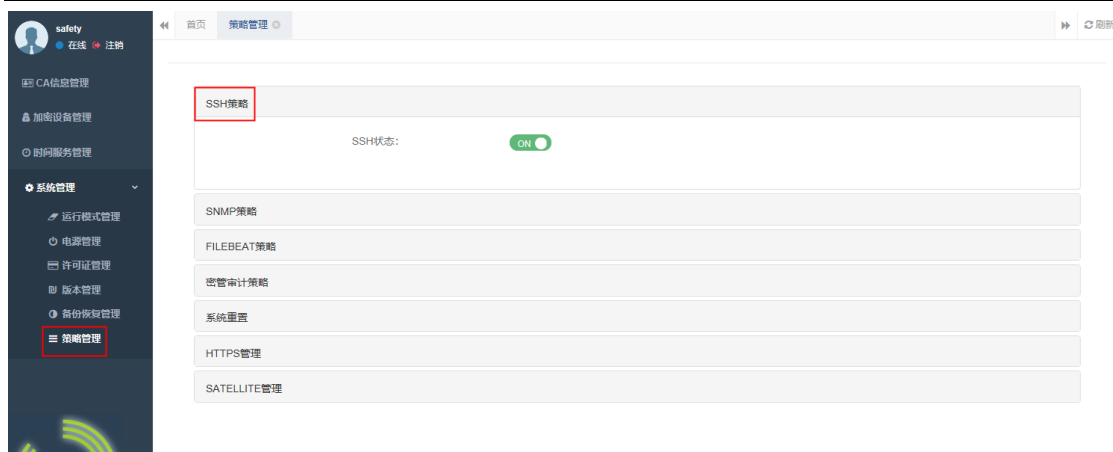
系统策略包括对系统的 SSH、SNMP、密管审计、系统重置、HTTPS 策略配置。



图表 105 策略管理

13.7.1. SSH 管理

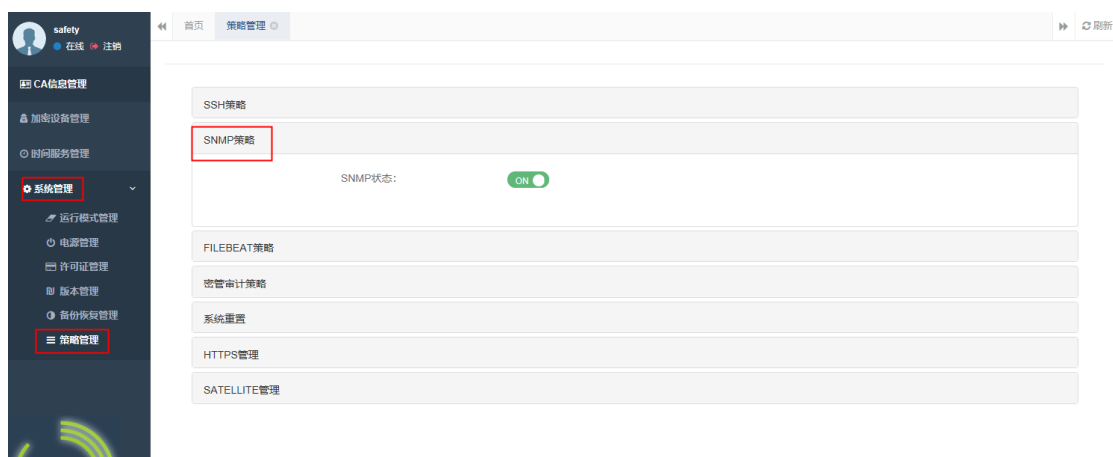
2.4.10 版本开始增加 SSH 管理，页面可开启与关闭 SSH。



图表 106 SSH 管理页面

13.7.2. 可视化监控

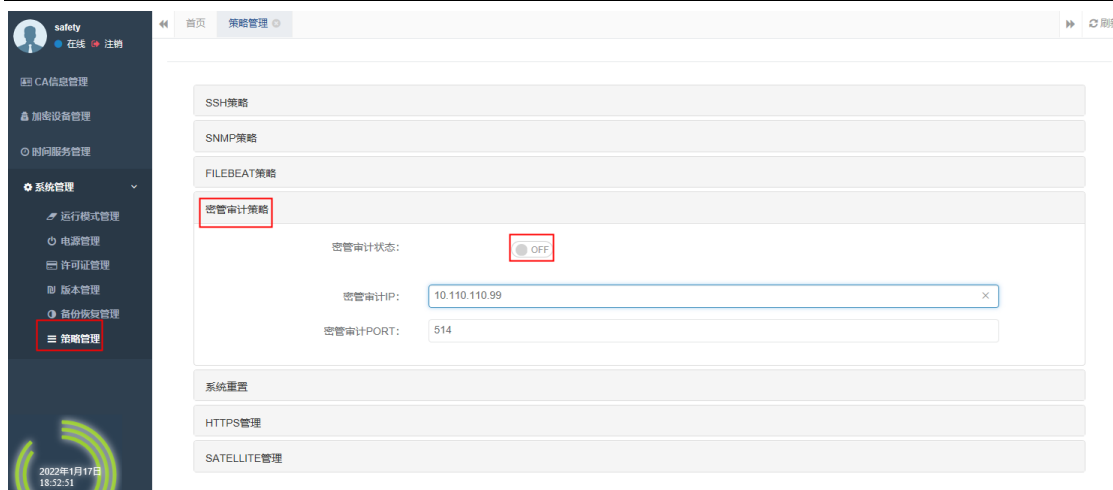
自 2.4.9 版本系统支持可视化监控，在【策略管理】SNMP 标签页面可以启用/停用可视化监控。



图表 107 可视化监控配置

13.7.3. 密管审计管理

点击【策略管理】-【密管审计管理】标签，进入密管审计页面，添加密管审计 IP、密管审计 PORT，再点击 ON 启用按钮，弹出启用成功提示，即可启用密管审计，如下图：

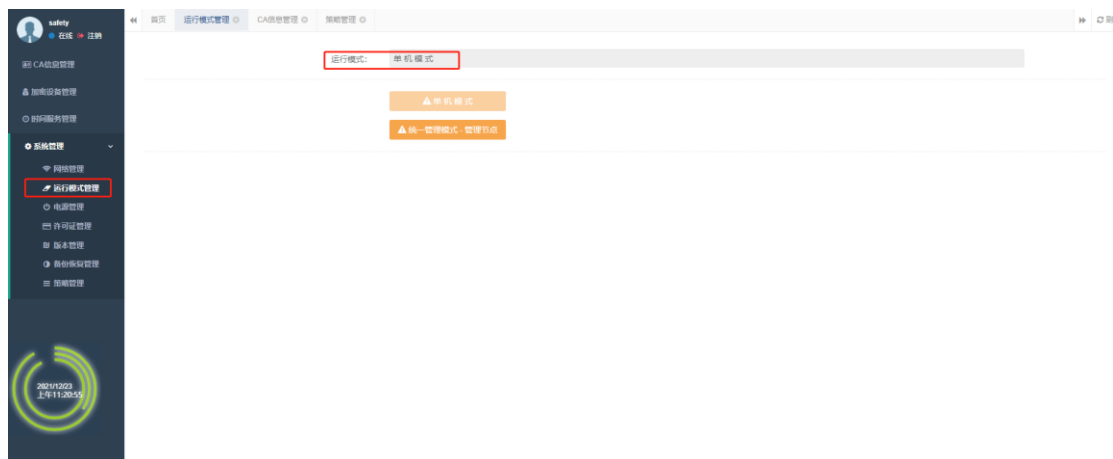


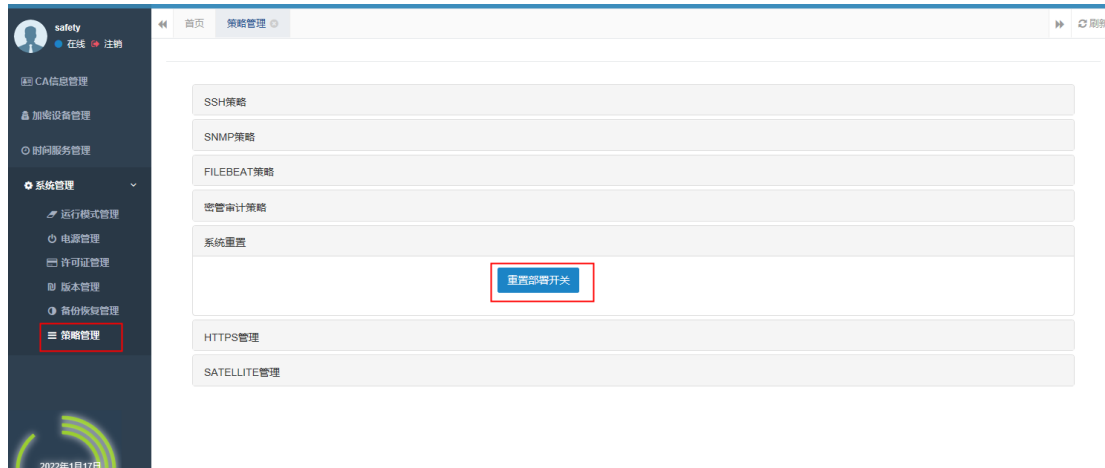
图表 108 密管审计管理

点击“停用密管审计”按钮即可停用密管审计。

13.7.4. 系统重置

当管理员忘记密码或需要重新部署时，系统支持重置功能进行重新部署，仅在单机模式下



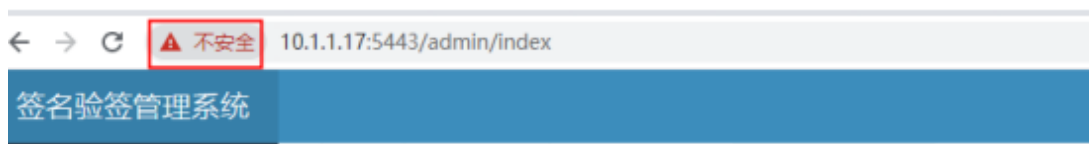


图表 109 系统重置部署

点击重置按钮后，系统可登录 <https://ip:9091> 或 <http://ip:9091> 进行重新部署。

13.7.5. 站点根证书下载

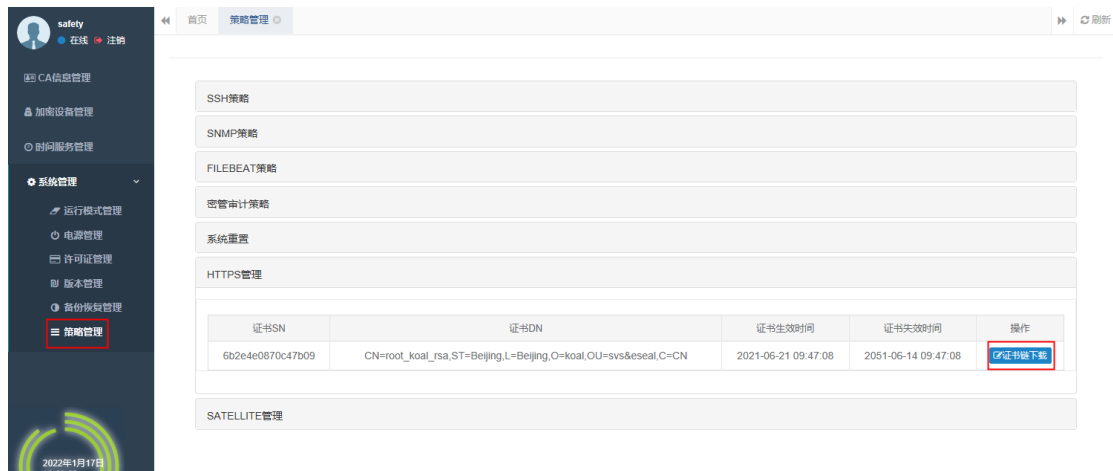
从 2.4.10 版本开始使用 <https> 方式登录，如果登录时客户端不导入站点证书的根证书，登录时页面会显示不安全的登录，如下图：这就需要将站点证书的根证书导入浏览器中。



图表 110 不安全登录

13.7.5.1. 下载站点根证书

点击【系统管理】->【站点根证书下载】页面的“下载”按钮，可将根证书下载到本地



图表 111 下载站点根证书

13.7.5.2. 浏览器导入站点根证书

导出后将根证书安装到 windows 系统中，存储位置选择“受信任的根证书颁发机构”和“受信任的颁发者”



← 证书导入向导

证书存储

证书存储是保存证书的系统区域。

Windows 可以自动选择证书存储，你也可以为证书指定一个位置。

☐ 根据证书类型，自动选择证书存储(U)

☒ 将所有的证书都放入下列存储(P)

证书存储:

受信任的根证书颁发机构

浏览(R)...

下一步(N)

取消

← 证书导入向导

证书存储

证书存储是保存证书的系统区域。

Windows 可以自动选择证书存储，你也可以为证书指定一个位置。

☐ 根据证书类型，自动选择证书存储(U)

☒ 将所有的证书都放入下列存储(P)

证书存储:

受信任的发布者

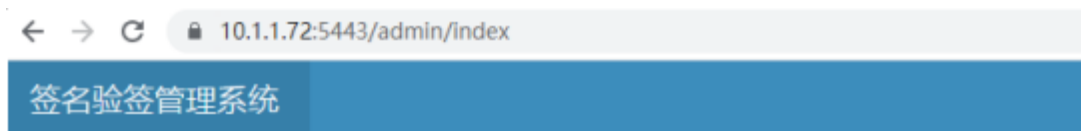
浏览(R)...

下一步(N)

取消

图表 112 将站点根证书导入浏览器

完成后再登陆系统时左上角不会在显示不安全。

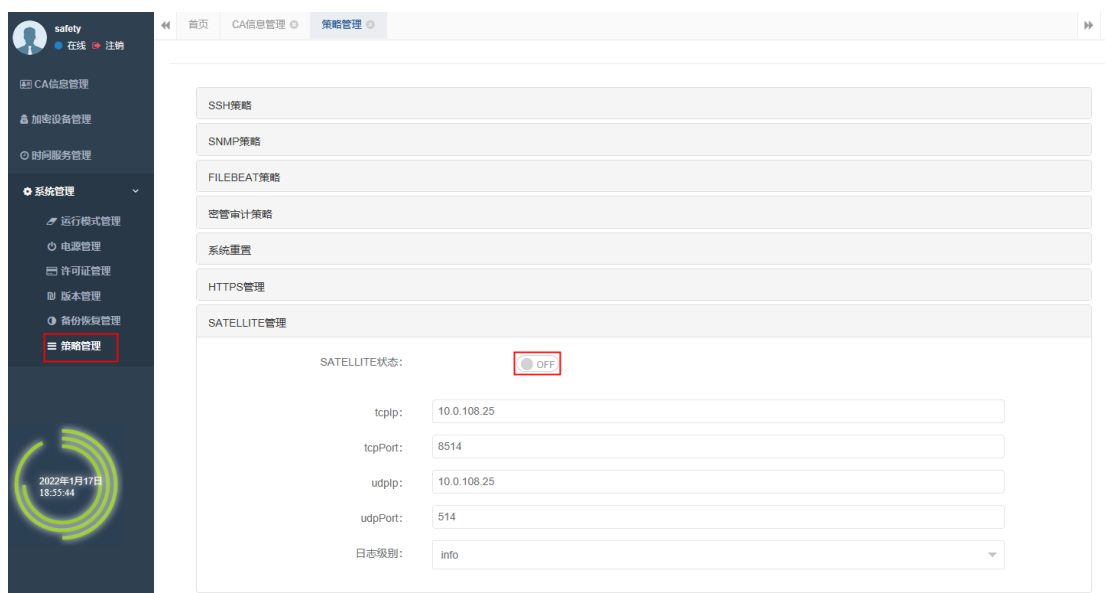


图表 113 导入根证书后登录系统显示

13.7.6. SATELLITE 管理

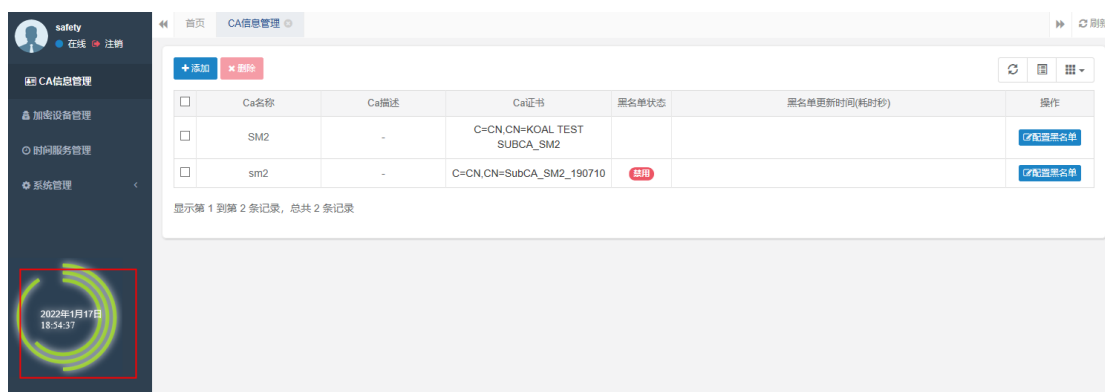
点击【策略管理】-【SATELLITE 管理】标签，进入 SATELLITE 页面，添加

tcpip、tcpport、udpip、udpport,选择日志级别,再点击 ON 启用按钮即可启用 SATELLITE, 如下图:



13.8. 系统时间

可以查看系统当前时间。



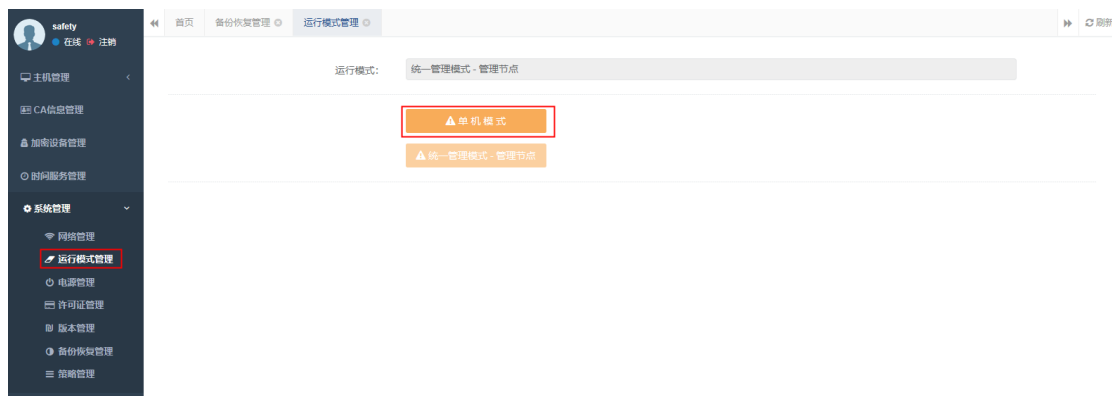
图表 114 查看系统时间

13.9. 运行模式管理

运行模式分为单机模式、统一管理模式-管理节点和统一管理模式-工作节点,默认出厂都为单机模式。

13.9.1. 单机模式

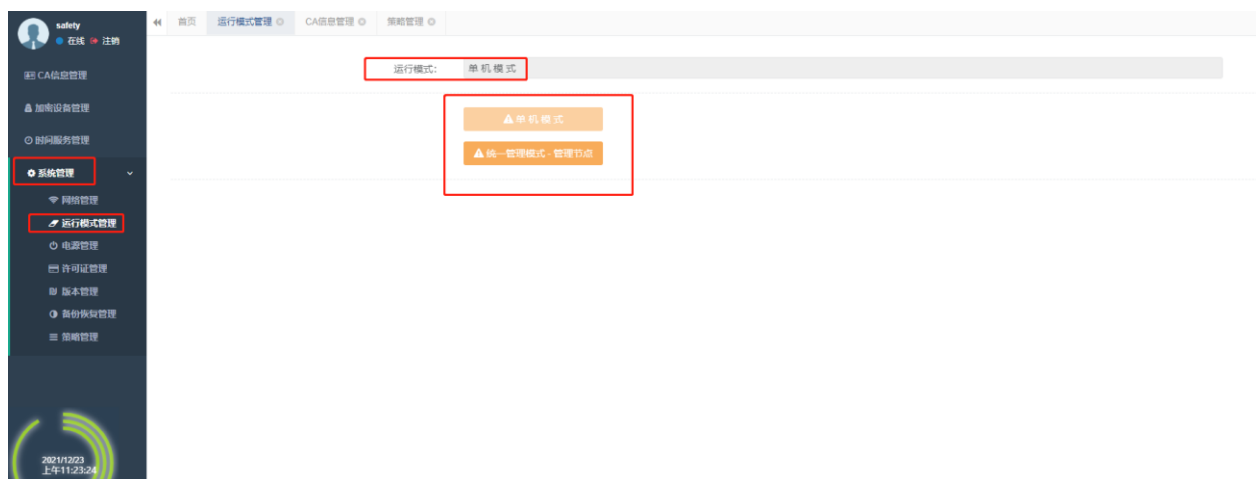
系统出厂时默认为单机模式。只有一台主机工作时可将主机调至单机模式，单机模式不需要进行数据同步，点击【系统管理】下的【运行模式管理】进入运行管理页面，点击“单机模式”即可切换为单机模式。

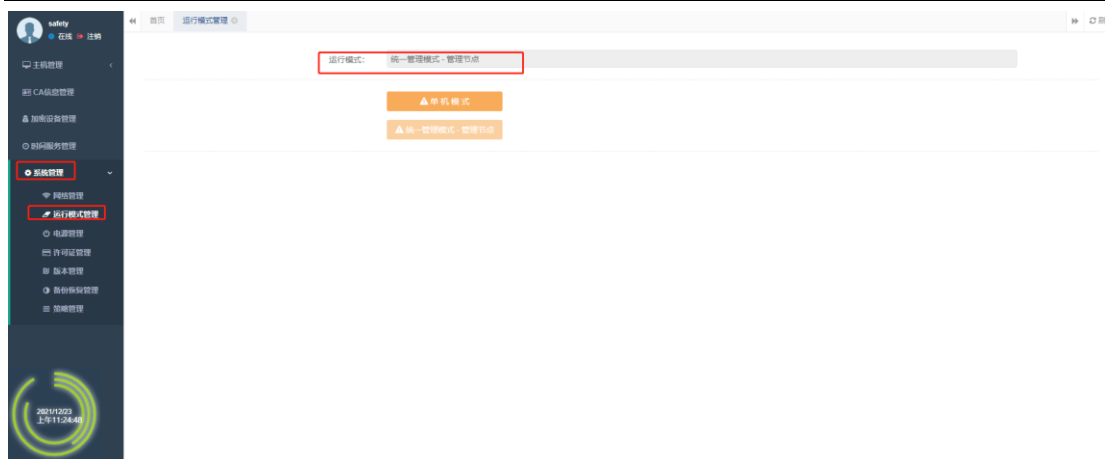


图表 115 系统运行单机模式

13.9.2. 统一管理模式

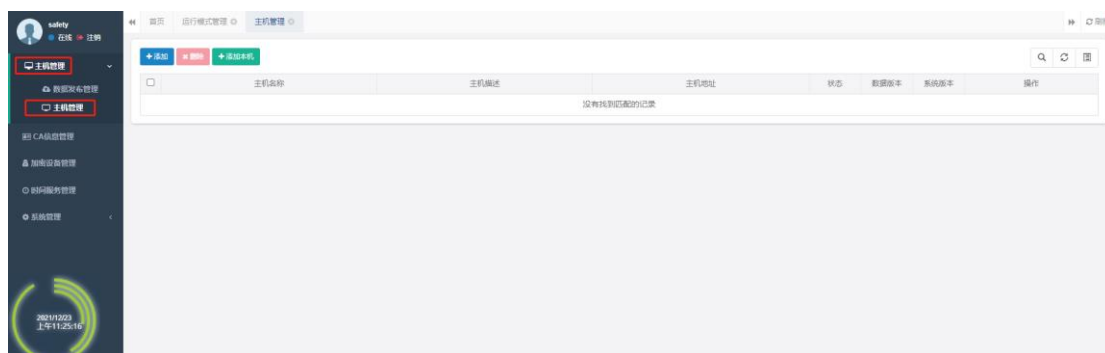
统一管理模式适用于多台主机之间，一台主机作为管理节点，其他主机作为工作节点。



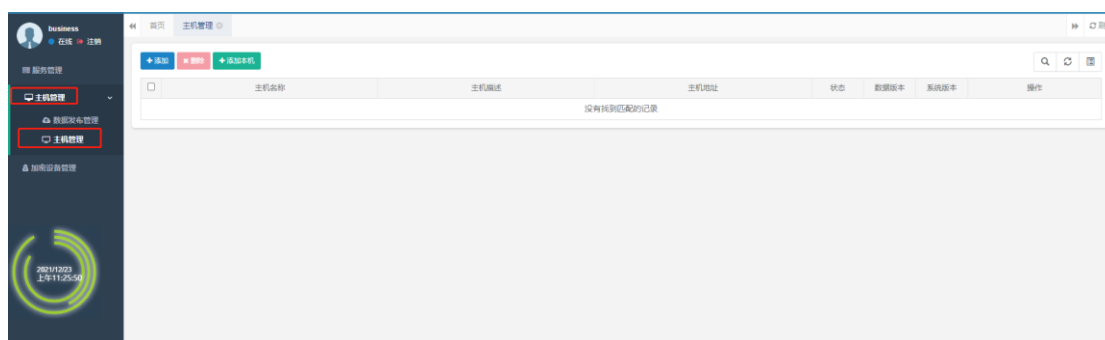


图表 116 系统运行统一管理模式

当运行模式切换到统一管理模式后,安全管理员和业务管理员登录后都会增加【主机管理】菜单,如图,两个管理员都数据配置更新后均支持数据同步功能。



图表 117 主机管理-安全管理员



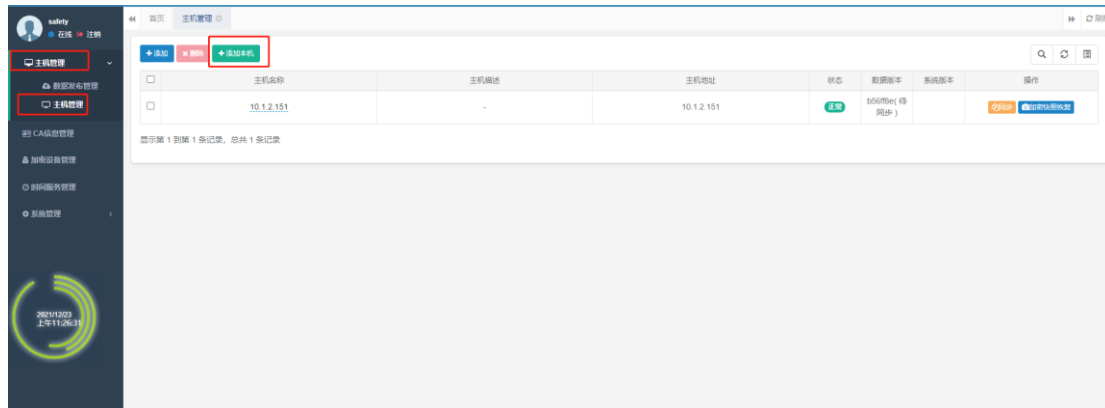
图表 118 主机管理-业务管理员

主机管理是用来管理主机及多个从机的服务配置的,只有运行模式变为统一管理模式才会有这个菜单,通过添加本机及从机,数据同步后,来进一步实现数据由本地仓库同步到相应主从机的服务配置中,如图,以下以安全管理员配置数据同步为例进行示例介绍。

13.9.2.1. 添加本机

添加主机时首先需要添加本机，再进行其他主机的添加。

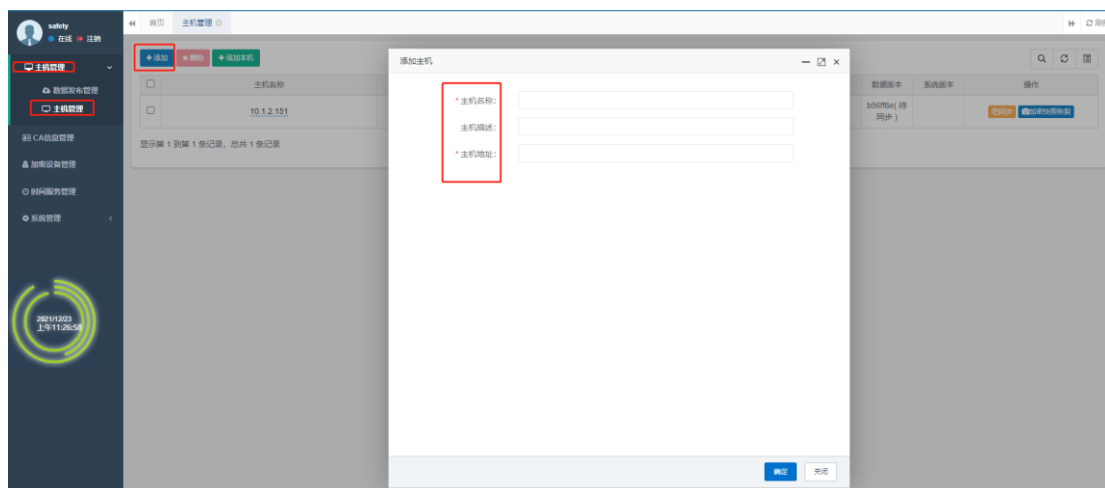
点击【添加主机】按钮，直接弹出添加主机成功提示，列表中增加主机信息，如图

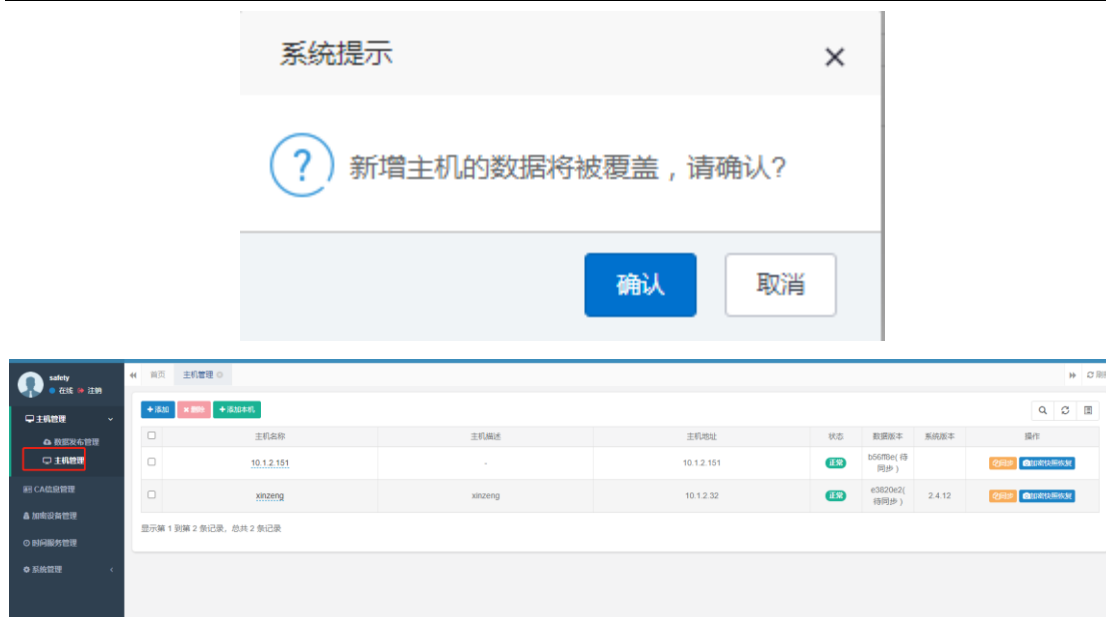


图表 119 添加本机

13.9.2.2. 添加工作节点

点击【添加】按钮，弹出添加主机页面，进行其他主机的添加，填写主机名称，主机地址后，点击【确定】按钮，弹出“新增主机将被覆盖”提示信息，点击【确定】后添加成功，页面显示本机和其他主机（简称从机）信息。





图表 120 添加其他主机

当添加的主机网络不通时会弹出添加失败提示信息，如图



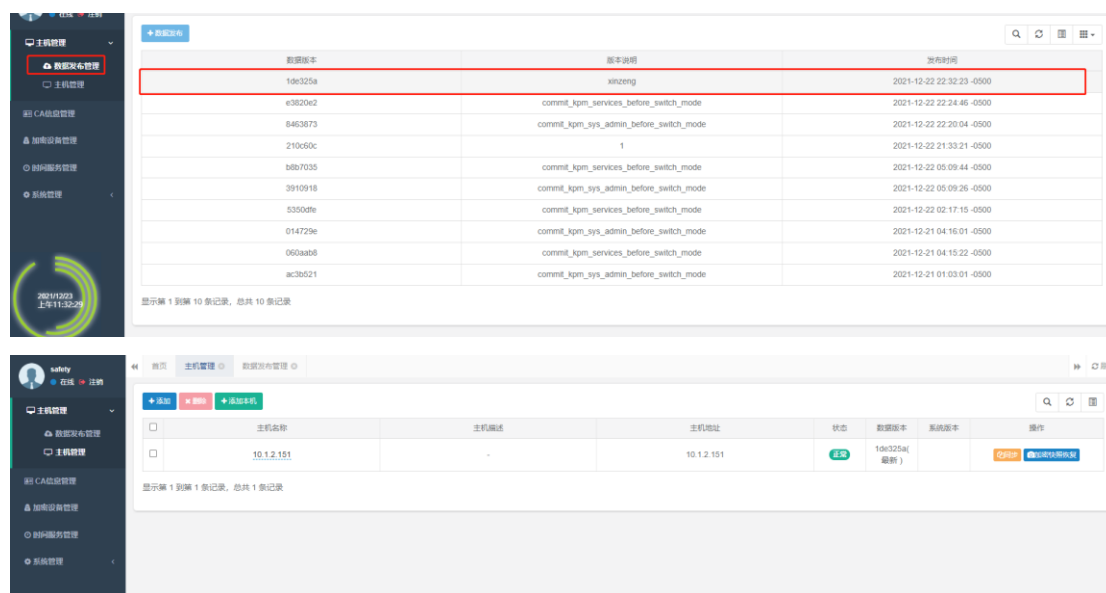
图表 121 添加主机网络不通

主机添加完成后，主机列表显示“主机名”、“主机描述”、“主机地址”、“主机状态”、“数据版本”、“操作”项。本机系统主机名为 local，各个主从机数据版本直接获取各个主机服务的最新数据版本。

13.9.2.3. 数据同步

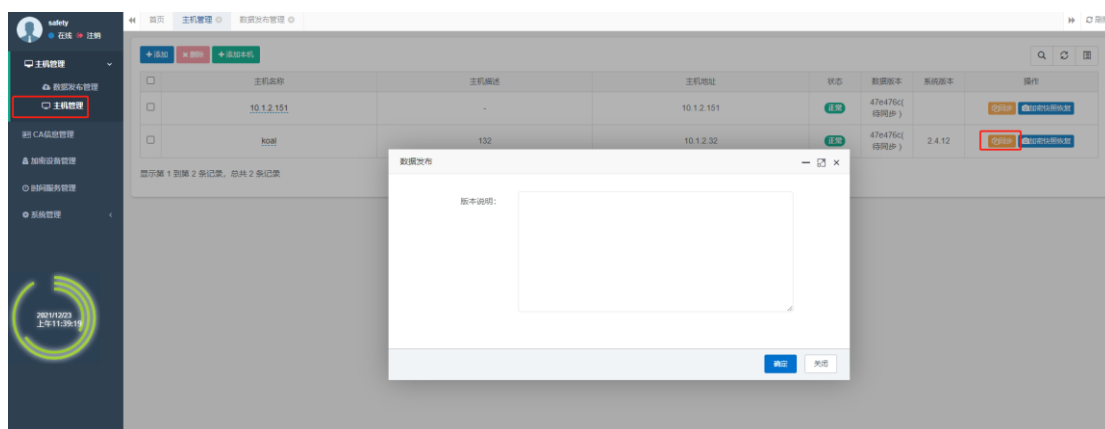
主机列表中数据版本显示不同主机服务的最新数据版本，每次数据版本有更新时，需要先进行数据发布，然后在进行各个主机数据同步，可以直接点击【主机管理】->【数据发布管理】页面的“数据发布”按钮进行数据发布，也可以直接在【主机管理】->【主机管理】页面直接点击主机后的“同步”按钮进行发布，

同步完成后从机服务的数据版本更新为最新的数据版本。



图表 122 数据同步

当系统有数据更新后，没有数据发布直接进行数据同步，在同步时会弹出数据发布信息，发布完成后再次点击【同步】按钮，则完成数据同步。



图表 123 未数据发布直接同步

提示：

- 只有数据发布后才能进行数据同步
- 若没有数据发布直接数据同步，会弹出数据发布操作，直接发布完成再进行数据同步
- 所有主从机数据同步完成，检查显示的服务数据版本应保持一致，且都为系统数据发布的最新版本

向工作节点进行同步时，工作节点主机管理系统会自动关闭，将工作节点从主机管理中删除后，工作节点主机的管理页面会自动启动。

13.9.2.4. 加密快照恢复

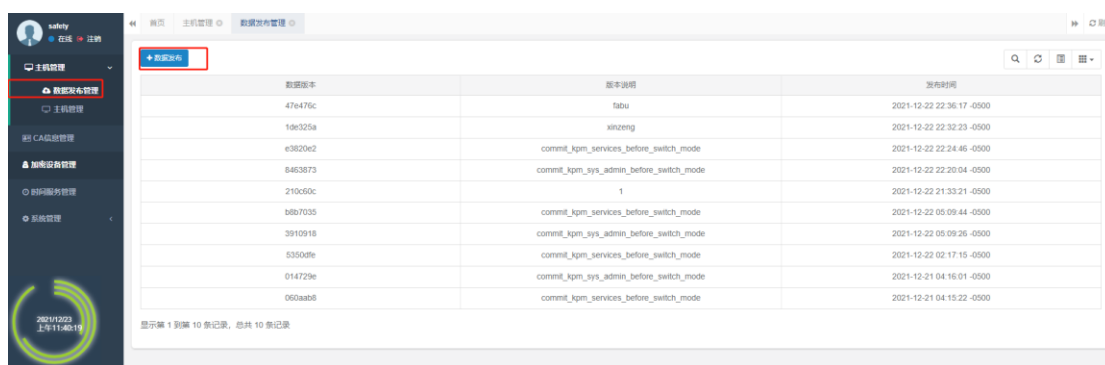
目前支持三未信安 D22 加密卡快照的恢复，可以将管理节点的加密快照恢复到工作节点，点击主机后面的“加密快照恢复”按钮，选择想要恢复的快照即可，如下图：



图表 124 统一管理模式加密快照恢复

13.9.2.5. 数据发布管理

当系统主机作业完成后，需要进行数据同步才能发布到本地仓库中，如图



图表 125 数据发布

数据发布完成后，数据发布按钮为置灰状态，不能再次操作，进一步在【主机管理】点击【同步】才能将配置数据同步到各个主从机服务中。

提示：

- 管理系统配置每次更新完都需要进行数据发布操作、建议一次配置完成后统

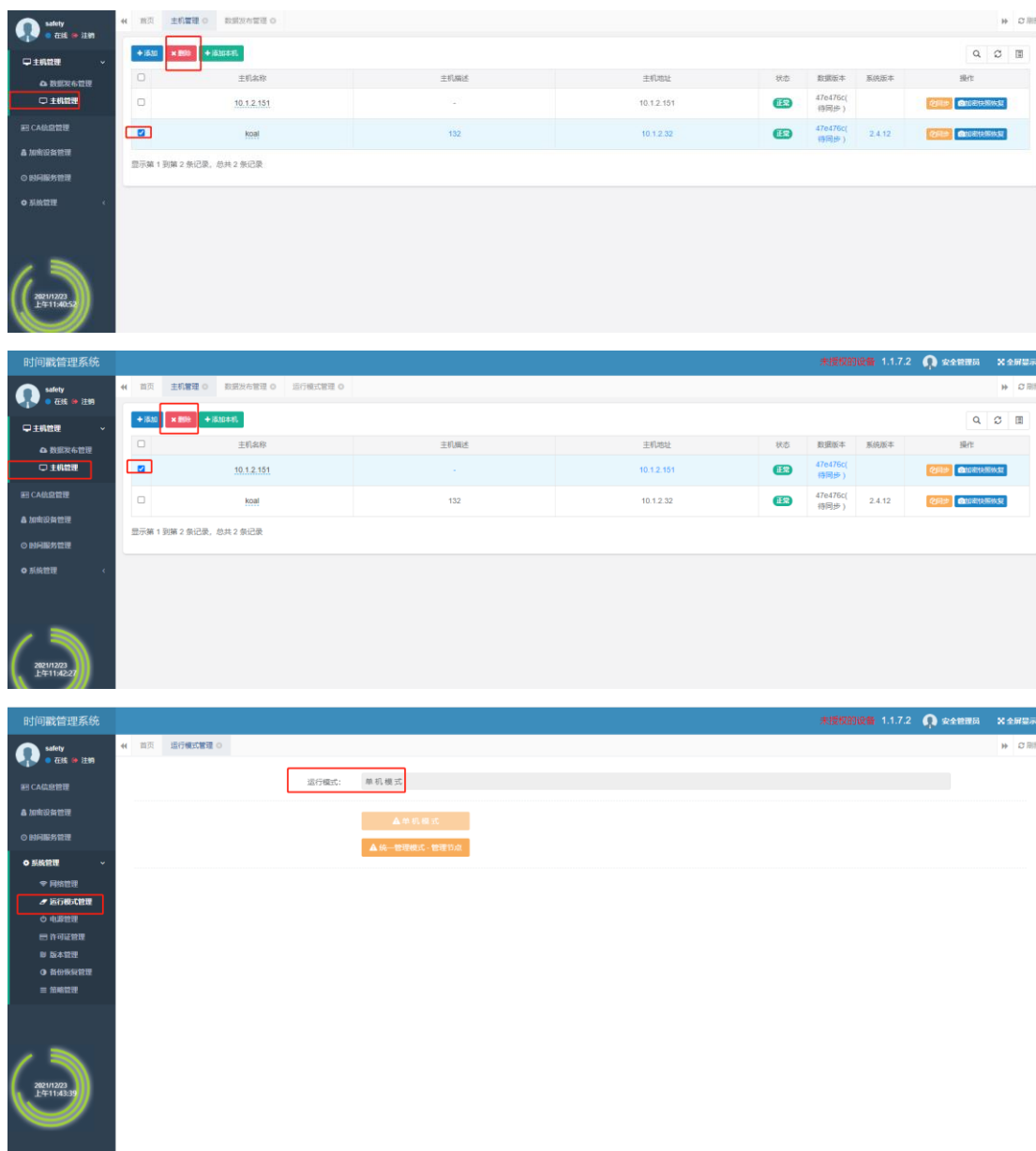
一进行发布。

- 数据发布完成后系统为最新版本，发布按钮置灰，不能再次操作。
- 只有发布完成的数据才能进行数据同步。

13.9.2.6. 删除节点变为单机

选择一个或多个主机，点击【删除】按钮，则相应主机即被删除。

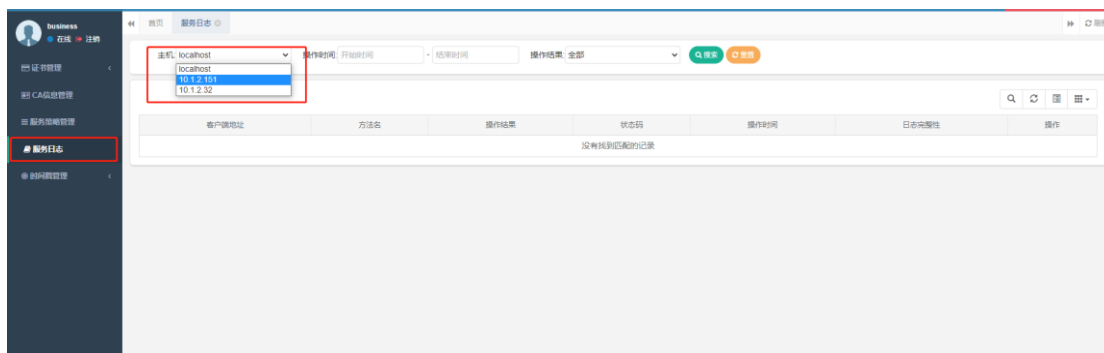
当运行模式切换到单机时，需先将主机管理中节点和主机都删除，在切换为单机。



图表 126 删除节点和主机切换为单机

13.9.2.7. 服务日志查看

统一管理模式下,通过主节点对应服务日志可以查看各个工作节点的服务日志,如图,从而可以观察各个节点服务日志。



图表 127 各节点服务日志

第十四章 负载均衡模式

主从机连同客户端 API 支持负载均衡功能,当主控服务器出现故障时,其他服务器可以自动接替主控服务器的业务,完成系统切换,使用户业务不会因为设备故障而受到影响。

这样,主从机数据保持一致,当客户端 API 同时连接多个主从机进行负载作业,当主机或从机一台或多台出现故障后,客户端 API 会直接向可以连通的服务器进行业务作业,保证服务能签名验签服务能正常进行。

统一管理模式就可以满足负载的需求,具体操作步骤参考 [13.9.2 统一管理模式](#)。

第十五章 常见错误码表

-3002	证书不在有效期
-3004	没有匹配的证书链
-3015	服务没有配置证书链

-3017	加载证书失败
-3018	证书用途错误
-3020	黑名单对应的 list 文件不存在
-3021	证书在黑名单中
-3035	初始化加密卡时未找到加密卡名字配置
-3036	初始化加密卡时未找到加密卡 so 配置
-3037	Load 加密卡失败
-3051	初始化日志水平不在范围内
-3052	日志文件大小不可设置为负值
-3053	日志输出配置只可设为 console
-3054	日志回滚大小不可为负值
-3055	系统日志最大值只能为正数
-3056	生成 Verify.log 的日志上下文失败
-3057	生成 error.log 的日志上下文失败
-3058	生成 system.log 的日志上下文失败
-3059	生成 debug.log 的日志上下文失败
-3101	服务端口号应大于 0 ，小于等于 65535
-3102	没有配服务端口
-3103	服务启动进程数设置应大于等于 0
-3104	服务启动加密卡进程数应大于等于 0
-3105	服务连接数应大于 1 ，小于等于 65535
-3106	设置服务接收报文最大值超过允许范围
-3107	证书有效期误差单位 y, m, d, h, s 不区分大小写
-3111	获取子进程的 pid 失败
-3112	主进程没有生成子进程
-3114	监听 ip, port 失败
-3221	不存在服务主配置目录
-3222	/koalii/TSA 默认主目录下不存在服务主配置

-3223	加载 verify.xml 失败
-3224	加载 sdf.xml 失败
-3231	裸验时签名数据解 b64 失败
-3241	Hash 数据和 hash 算法不匹配
-3701	检查 xml 报文开头失败
-3702	检查 xml 报文结尾失败
-3703	数据过大
-3705	不存在原文
-3706	没有签名数据
-3707	需要证书数据
-3714	没有加密数据
-3715	没有证书序列号
-3716	公钥内部格式转 der 格式失败
-3717	数字信封解析颁发者信息失败
-3718	数字信封的颁发者序列号转换失败
-3719	生成加密卡上下文失败
-3720	导出加密卡公钥失败
-3722	没有私钥信息
-3723	没有公钥信息
-3735	没有对应消息的处理过程
-3736	解析器没有响应处理
-3737	没有 xml 解析器
-3741	Xml 解析失败
-3742	检查 xml 报文开头失败
-3743	证书重复设置
-3744	数字信封数据重复设置
-3745	摘要值不能小于零
-3746	原文重复设置

-3748	原文摘要重复设置
-3749	签名数据重复设置
-3750	私钥信息重复设置
-3751	私钥格式重复设置
-3752	私钥密码重复设置
-3760	没有响应处理
-3761	没有请求处理
-3801	签名解密库没有证书
-3802	签名解密库没有私钥
-3804	私钥支持 opl 和 sdf 两种类型
-3806	签名解密库初始化失败
-3807	加密卡私钥格式转上下文失败
-3808	证书加载失败
-3809	证书算法错误
-3810	外部签名，外传证书和 pfx 证书同时存在，但俩张证书不同时报此错误码
-3811	验签加密库没有证书
-3812	验签加密库证书算法错误
-3813	加载验签加密库证书失败
-3814	加载颁发者证书失败
-3820	Sm2 格式设置有误
-3821	P7 数据中不包含证书
-3822	生成密钥对只支持 sdf 格式私钥
-3825	对称加密 padding 设置错误
-3826	非对称加密 padding 设置错误
-3827	不支持该对称加密算法
-3829	Key 算法只支持 rsa1024 , rsa2048 , sm2
-3830	Key 用途支持 sign , encrypt

-10002	参数为 NULL
-10003	参数长度错误
-10004	参数非法
-150001	ASN.1 转换 UTF-8 字符串
-150004	ASN.1TIME 转换为 TM 结构
-150007	证书非对称算法类型不匹配
-150009	大整数转换
-150010	生成随机数失败
-150041	XML 签名错误签名算法
-150044	签名数据长度错误
-150045	签发证书请求失败
-150050	算法名称错误
-150051	证书非对称算法类型错误
-150052	签名算法错误
-150061	摘要 SHA1 错误
-150062	摘要 SHA256 错误
-150063	摘要 MD5 错误
-150064	摘要算法长度不对
-150065	摘要算法错误
-150066	PKCS7 解析未知 OID
-150067	解析签名数据失败
-150068	摘要 SHA384 错误
-150069	摘要 SHA512 错误
-150101	证书解析失败
-150102	证书扩展项解析失败
-150121	证书 DN 项解析失败
-150122	证书扩展项设置失败
-150123	证书扩展项创建失败

-150131	ASN.1 解码失败
-150132	ASN.1 解码数据长度错误
-150151	证书链解析未找到发布者
-150201	KEYSTORE 校验失败
-150202	KEYSTORE 创建失败
-150203	密钥解析失败
-150204	KEYSTORE 为 NULL
-150301	RSA 签名失败
-150302	RSA 验签失败
-150303	RSA 公钥解密失败
-150304	RSA 公钥解密数据长度错误
-150305	RSA 公钥加密失败
-150306	RSA 私钥解密失败
-150309	RSA 私钥加密失败
-150310	RSA PADDING 失败
-150401	SM2 加载大整数失败
-150402	SM2 获取参数失败
-150403	SM2 获取 ECC 参数失败
-150405	SM2 密钥检查失败
-150406	SM2 获取公钥失败
-150407	SM2 获取私钥失败
-150408	SM2 签名失败
-150409	SM2 签名数据 DER 转化失败
-150410	SM2 签名数据非法
-150412	SM2 验签失败
-150413	SM2 加载证书失败
-150414	SM2 签名数据长度错误
-150415	SM2 生成随机数失败

-150416	SM2 ECC 参数非法
-150417	SM2 解密失败
-151101	PKCS7 解析失败
-151102	PKCS7 创建失败
-151103	PKCS7 创建失败
-151106	PKCS7 设置类型失败
-151107	PKCS7 设置 RECIPIINFO 失败
-151108	PKCS7 设置证书失败
-151109	PKCS7 设置 SIGNER 失败
-151110	PKCS7 FINAL 失败
-151111	PKCS7 转化为 DER 编码失败
-151201	PKCS7 签名失败
-151202	PKCS7 验签失败
-151203	PKCS7 获取原文失败
-151204	PKCS7 获取签名原文失败
-151205	PKCS7 获取签名证书失败
-151206	PKCS7 获取签名摘要失败
-151301	PKCS7 加密失败
-151302	PKCS7 解密失败
-151303	PKCS7 获取证书失败
-151304	PKCS7 加密获取对称加密算法失败
-151305	PKCS7 设置版本号失败
-151306	PKCS7 设置 RECIPIINFO 失败
-151307	PKCS7 设置 RECIPIINFOS 失败
-151308	PKCS7 设置算法分配失败
-151309	PKCS7 设置算法创建失败
-151309	PKCS7 设置算法 ID 失败
-151310	PKCS7 设置 ENCCONTENT 失败

-151311	PKCS7 设置证书转码失败
-151312	PKCS7 设置 EXTENDCERT 失败
-151313	PKCS7 设置 SIGNINFO 失败
-152201	CRL 解析失败
-152301	对称解密输出缓冲区过小
-152302	对称加解密未知算法
-152303	对称加解密未知 PADDING
-152304	对称加密机 PADDING 长度不对
-152305	算法名称未知
-152306	对称加密算法需要 IV 向量
-152307	对称加密算法不需要 IV 向量
-152308	对称加解密未知 OID
-152310	对称加解密 INIT 失败
-152311	对称加解密 UPDATE 失败
-152312	对称解密 FINAL 失败
-152313	对称加解密创建上下文失败
-152320	对称加解密 BLOCK 长度错误
-152401	摘要未知算法 KID
-152402	摘要未知算法 NID
-152403	摘要未知算法名称
-152404	摘要 INIT 失败
-152405	摘要 UPDATE 失败
-152406	摘要 FINAL 失败
-152407	摘要输出缓冲区过小
-110004	BASE64 解码失败
11400001	证书存在不唯一
11400002	私钥密码错误
11400003	私钥算法不支持

11400004	对私钥加密失败
11400005	对私钥解密失败
11400006	获得公钥 key 指纹失败
11400007	请求类型不支持
11400008	生成 P10 请求失败
11400009	保存 P10 请求失败
11400010	导入证书解析失败
11400011	请求未发现
11400012	证书已存在
11400013	导入证书失败
11400014	证书未发现
11400015	未配置证书链
11400016	解析 P7 失败
11400017	原文为空
11400018	签名结果为空
11400019	签名消息为空
11400020	签名证书为空
11400021	加密证书为空
11400022	数字信封为空
11400023	解析数字信封失败
11400024	数字信封未包含证书信息
11400025	证书已损坏
11400026	白名单未支持该用途
11400027	白名单验签功能未启用
11400028	白名单加密功能未启用
11400029	证书不在白名单
11400030	证书别名/ SN / DN 为空

第十六章 FAQ

1. 统一管理模式每次更新数据后必须进行数据发布和同步
2. 点击【启用加密设备】按钮前必须上传加密通讯证书（云版本）
3. 如果加密机第一次启动失败，点击【启用加密设备】前重新上传一次证书及密码，然后再重启系统
4. 当主机中黑名单启用定时任务下载更新失败时，进行数据同步会弹出提示信息：“XXX 黑名单定时任务下载失败”，需将相应下载黑名单禁用或保持下载更新成功在进行数据同步
5. 二代支付、跨境支付业务签名数据格式为 CIPS
6. 网联业务签名数据格式为 CIPS
7. 银联业务签名数据格式为 GM
8. 组织部签名数据格式为 OPL
9. 网口说明：enp5s0 为 eth0,enp6s0 为 eth1
10. 负载模式时从机需关闭管理服务
11. 如果在【主机管理】页面点击“添加主机”时显示“无法通信”时，可以查看防火墙状态，执行 `systemctl status firewalld`，如果显示为 `enable` 状态，需要关闭防火墙，执行 `systemctl disable firewall`，然后 `reboot`
12. 出厂网络 IP 在管理系统修改后拔掉网线重新插上后系统 IP 变为出厂网络 IP 解决办法？
 - （1）在管理系统【网络管理】菜单修改网络 IP 为可用 IP。（这一条非常重要）
 - （2）进入后台执行 `systemctl disable NetworkManager.service` 命令。
 - （3）然后 `reboot`
13. 加密卡断电不能正常加载如何解决？

有时加密卡断电后不能正常加载，需再次断电才能正常加载。