WAPI 鉴别服务器产品
TH-AS5001 用户手册

目录

1 前言

1.1 手册说明

本手册对应产品型号：WAPI 鉴别服务器产品——TH-AS5001 本手册对应产品软件版本：V1.00.23XX.xx.xxx

1.2 手册简介

本手册主要介绍了 WAPI 鉴别服务器 TH-AS5001 的使用方法，包括但不限于 WAPI 鉴别服务器的用户和网络配置、升级、Licence 授权使用方法，WAPI 证书的颁发、吊销、下载、查询、管理使用方法，WAPI 鉴别、漫游配置使用方法等。

1.3 读者对象

本手册适合下列人员阅读：

网络规划、管理人员

网管系统维护人员

2 产品简介

TH-AS5001 是一款 WAPI 鉴别服务器（AS）产品，采用我国自主知识产权的 WAPI 安全技术和国家密码管理局批准的密码算法，完全符合中国无线局域网国家标准 GB 15629.11 系列和 WAPI 产业联盟团体标准 T/WAPIA 010.2 的相关要求，在 WAPI 过程中提供安全接入认证用户身份识别，为构建安全可靠的无线局域网网络提供基础支撑。

TH-AS5001 在整个 WAPI 网络安全体系架构中做为可信第三方角色，是 WAPI 三元对等安全架构的重要组成部分。设备采用高性能硬件架构，提供用户证书的鉴别、申请、下载、吊销、查询等证书管理功能。并且有完备的日志管理和用户管理等辅助功能。

2.1 产品特点

TH-AS5001 具有以下特点：

1. 采用 WAPI 安全技术，提供更高安全级别的网络部署，满足各行业对无线网络安全的要求；
2. 完全符合中国无线局域网国家标准 GB 15629.11 系列和 WAPI 产业联盟团体标准 T/WAPIA 010.2 的相关要求；
3. 支持多用户 WAPI 证书并发鉴别；
4. 采用国家密码管理部门批准的椭圆曲线公钥密码算法进行核心签名运算；
5. 支持 WAPI 证书批量颁发、吊销和下载；
6. 支持 P10 文件导入方式申请 WAPI 证书；
7. 支持 WAPI 证书分组管理；
8. 支持重新颁发 WAPI 证书（证书更新）；
9. 支持 WAPI 漫游鉴别，用户在漫游地同样可以鉴别身份，漫游协议符合 T/WAPIA 010.2 标准要求；
10. 支持根证书导入功能，部署使用方式更加灵活；
11. 多种漫游方式（中心转发、直接转发），适用多种网络拓扑结构，满足用户多业务需求；
12. 运营级日志系统和多级用户管理系统，为系统后期的故障排除和责任定位等运维工作提供了技术支撑；

13. 支持日志审计；

14. 支持大型数据库，提高了系统信息处理和容错能力；

15. 友好且完善的设备操作管理 Web 界面；

2.2 产品组成

序号	名称	数量	备注
1	主机	1 台	
2	电源线	1 根	

2.3 产品外观

图 2-1 AS 外观

3 管理界面

AS 的管理和配置是通过 Web 页面的方式来操作的，友善的人机交互界面方便客户对设备进行配置和管理。可通过 LAN 口连接登录进行设备配置（请勿连接 AS 的最后一个网口），AS 的默认 IP 地址为 192.168.1.1。

3.1 页面登录

页面登录的方法：

1．在浏览器的地址栏输入 http://192.168.1.1（AS 的默认地址），回车，即可打开鉴别服务器 Web 登录界面。用户名为 **admin**，默认密码为 **12345678**。

图 3-1 登录页面

2．输入用户名、密码后，点击登录，即可进入 AS 管理页面。

图 3-2 管理界面

4 管理与配置

4.1 首页

当前页面显示 AS 证书信息、设备信息，其中证书信息包含可颁发证书数、已颁发证书数、证书组数和证书类别等，设备信息包含主机名、主机 IP 和当前 CPU 和内存占用情况等。

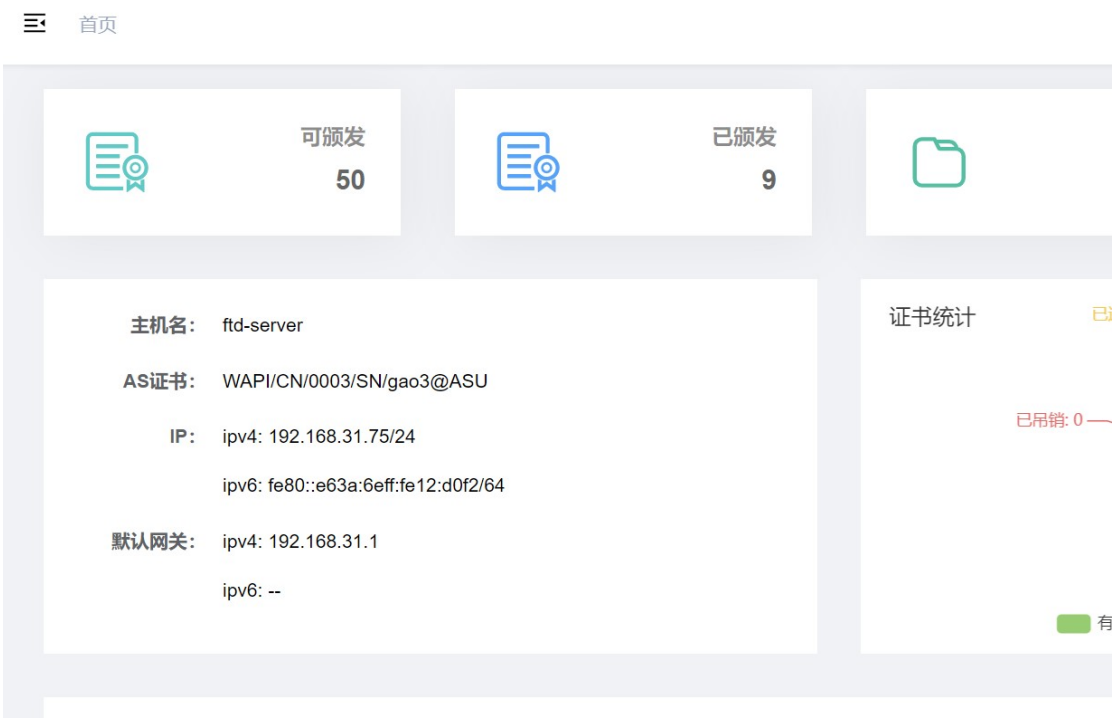

图 4-1 首页

4.2 基本配置

基本配置菜单包含**初始化**和**网络配置**两个功能。

图 4-2 基本配置菜单

4.2.1 初始化

初始化操作用于生成鉴别服务器的 ASU 证书，该服务器颁发的所有证书都是基于该 ASU 证书。初始化有两种方式：**手动配置**和**外部导入**。

4.2.1.1 手动配置

手动配置时，用户需配置 ASU 证书的五个域（强制域、国家域、管理域、网路域和设备域)。

图 4-3 初始化 – 手动配置

4.2.1.2 外部导入

外部导入是指用户以从其他 AS 或 CA 颁发的 ASU 证书（PKCS#12 格式）作为本 AS 的 ASU 证书。

图 4-4 初始化 – 外部导入

点击<确定>按钮，就可以初始化 ASU 证书，该操作需要输入管理员密码。

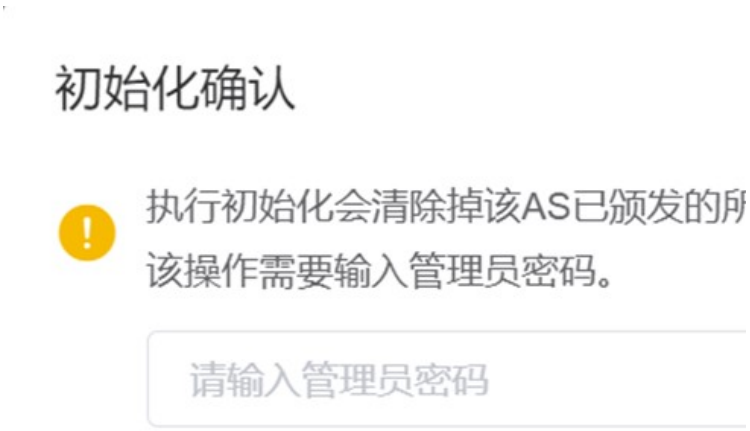

图 4-5 初始化确认

注意 **执行初始化会清除掉该 AS 已颁发的所有证书，请谨慎操作。**

4.2.2 网络配置

网络配置是用于配置 AS 的主机名和 IP 等网络信息。

图 4-6 网络配置

4.3 证书管理

证书管理菜单包含**证书组管理**和**证书管理**两大功能。

图 4-7 证书管理菜单

4.3.1 证书组管理

证书组是为了方便管理一组相关的证书，证书在颁发时必须选择相应的证书组，证书组管理功能包含证书组的**增加**和**删除**功能。

图 4-8 证书组管理

4.3.1.1 新建证书组

点击<新建>按钮会弹出一个对话框，输入证书组名字和证书组描述信息，然后点击<确定>按钮就可以新建一个证书组。

图 4-9 新建证书组

成功后，在证书列表里就可以看到新建的证书组。

图 4-10 新增的证书组

4.3.1.2 删除证书组

点击证书列表里某一条记录的右边的<删除>按钮，就可以删除对应的证书组。

组名	组描述	证书总数	有效证书
证书组1	单位1的证书组	0	0
aaa		2	1

图 4-11 删除证书组

4.3.2 证书管理

证书管理功能包含证书的**颁发**、**查询**、**吊销**、**下载**和**重新颁发**，此外还包含**根证书的下载**和**证书吊销列表（CRL）下载。**

图 4-12 证书列表

4.3.2.1 证书颁发

点击<证书颁发>按钮，就可以打开证书颁发界面。

图 4-13 证书颁发

证书颁发可以颁发两类证书: ASUE 证书和 AE 证书，有两种方式：**自主生成**和**导入申请文件。**

4. 3. 2. 2. 1 自主颁发

自主颁发需要选择证书组，输入持有者名称，选择证书有效期、选择绑定 MAC 地址方式。

图 4-14 自主生成证书

4. 3. 2. 2. 2 导入申请文件

导入申请文件方式颁发证书时只需要选择所属证书组和证书有效期，然后导入证书申请文件就可以颁发证书了。该功能可以导入**单个 PKCS#10 文件**颁发单个证书，也可以导入**包含多个 PKCS#10 文件的 zip 压缩包**颁发多个证书。

图 4-15 导入申请文件生成证书

4.3.2.2 颁发者证书下载

颁发者证书为 AS 自身的证书，是该设备颁发的所有证书的根证书。AS 初始化后，就生成了该证书。用户点击<颁发者证书下载>按钮就可以下载该证书。

图 4-16 根证书下载

4.3.2.3 CRL 下载

证书吊销列表（CRL）适用于记录已经吊销的证书信息的文件。用户点击<CRL 下载>按钮就可以下载该文件。

图 4-17 CRL 下载

4.3.2.4 证书查询

证书查询条件有证书组、持有者、序列号、证书状态、颁发时间和有效期范围。

图 4-18 证书查询

4.3.2.5 证书下载

证书在颁发的时候会提示用户保存本次颁发的证书。如果后续用户证书丢失，也可以在本页面下载相应的证书。 用户可以点击证书记录右侧的<下载>按钮下载单个证书，也可以勾选左侧的多选框下载多个证书。

图 4-19 证书下载

4.3.2.6 证书吊销

点击<吊销>按钮就可以吊销指定的证书。用户吊销单个证书，也可以吊销多个证书。

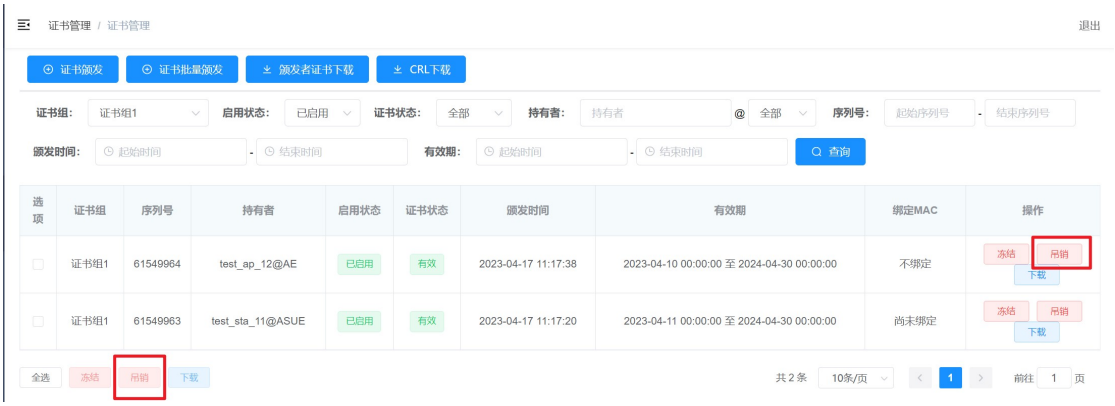

图 4-20 证书吊销

注意 证书吊销后，安装该证书的设备将无法正常连接 WAPI 网络，请谨慎操作。

4.3.2.7 证书重新颁发

当证书已吊销或者过期时，可以重新颁发该证书。重新颁发的证书保留了原证书的除有效期外的所有信息。

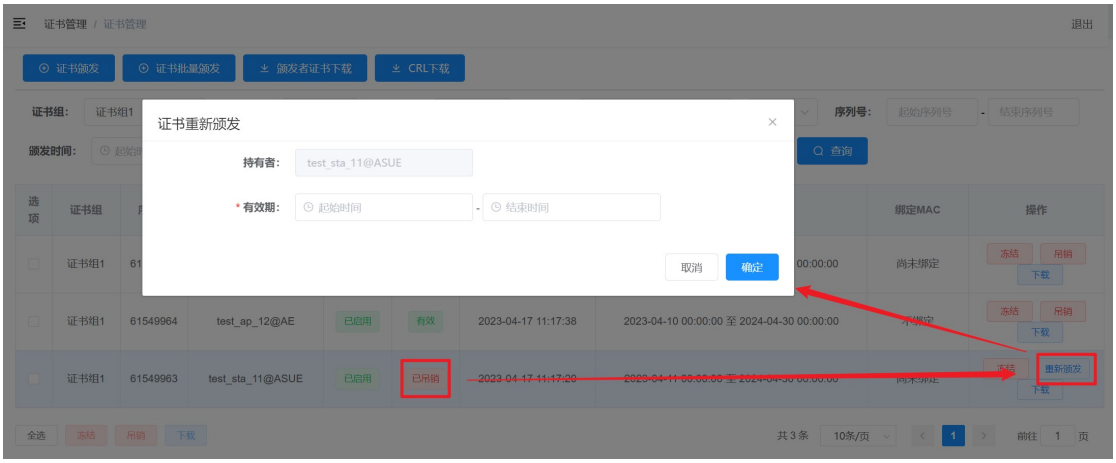

图 4-21 证书重新颁发

点击<重新颁发>会弹出对话框，用户选择新的证书有效期范围，点击<确定>，证书就重新颁发了。

4.4 日志查询

日志查询菜单包含**鉴别日志查询**和**管理日志查询**两个功能。

图 4-22 日志查询菜单

4.4.1 鉴别日志查询

鉴别日志记录的是 STA 和 AP 设备请求鉴别的结果。可以查询某个时间段内的鉴别日志，也可以通过 STA 或 AP 的 MAC 地址、证书名和证书鉴别结果来查询。

图 4-23 鉴别日志查询

4.4.2 管理日志查询

管理日志记录的是通过 web 界面进行的操作。可以通过**操作者**、**操作时间**、**行为类型**和**审计状态**等条件查询。

图 4-24 管理日志查询

4.4.3 管理日志审计

管理员需要每隔一定时间对管理日志进行审计，以确保用户操作的合规。

图 4-25 管理日志审计

4.5 设备管理

设备管理菜单包含**安装 License**、**备份与恢复**、**系统升级**和**设备重启**功能。

图 4-26 设备管理菜单

4.5.1 安装 License

AS 设备只有导入了 License 才能正常使用鉴别服务。License 还决定了鉴别服务器能容纳的有效证书数量。如果用户想扩容证书数量，需向厂家申请新的 License 文件并导入。

图 4-27 安装 License 文件

4.5.2 备份与恢复

备份与恢复功能用于**备份 AS 数据**、**恢复 AS 数据**。

图 4-28 备份与恢复

此外该页面还包含了**恢复出厂设置**功能。恢复出厂配置将系统重置为系统初始状态：重置 IP 地址、主机名称和网关，并恢复出厂的登录用户名和密码，清空根证书和所有用户证书。

图 4-29 恢复出厂配置

4.5.3 系统升级

系统升级用于修复系统缺陷和引进新功能或新特性。

图 4-30 系统升级

4.5.4 设备重启

设备重启用于重启鉴别服务器。

图 4-31 设备重启

4.6 用户管理

图 4-32 用户管理菜单

用户管理包含**添加用户**、**删除用户**、**修改密码**和**重置密码**等功能。

4.6.1 添加用户

超级管理员可以添加新用户。用户共分三个等级：超级管理员（只有 1 个）、普通管理员（最多 3 个）和普通用户（最多 3 个）。

其中，超级管理员拥有所有功能的权限。 普通管理员拥有大部分权限，除了初始化、网络配置、系统升级 和 恢复出厂等可能因操作不当而造成系统损坏的功能。 普通用户只拥有查询 和 下载权限。

图 4-33 添加用户

4.6.2 删除用户

超级管理员可以删除普通管理员和普通用户账号。

图 4-34 删除用户

4.6.3 修改用户密码

用户可以修改自己的账号密码。

图 4-35 修改用户密码

4.6.4 重置用户密码

超级管理员可以重置普通管理员和普通用户的账号密码。

图 4-36 重置用户密码

4.7 高级配置

高级配置菜单包含**漫游配置**功能和**双机热备**功能。

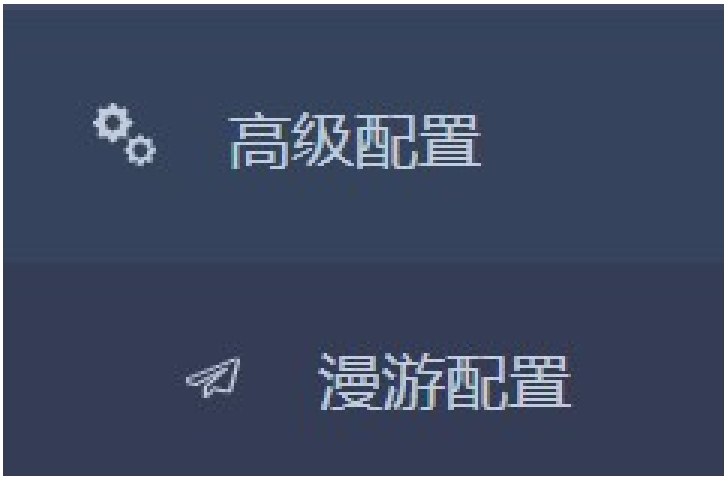

图 4-37 高级配置菜单

4.7.1 漫游配置

漫游配置功能包含**添加漫游**和**删除漫游**功能。

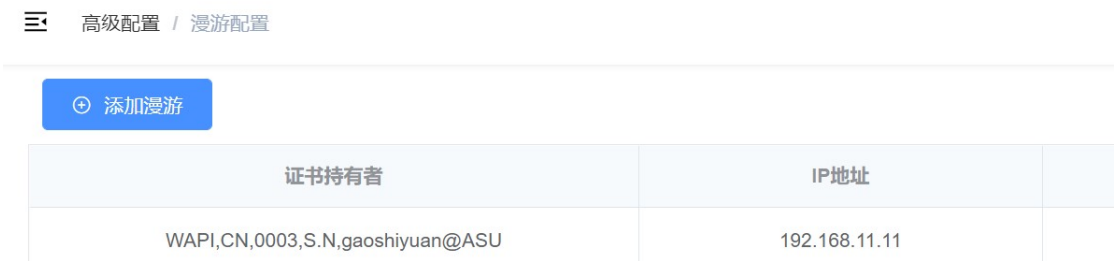

图 4-38 漫游配置

4.7.1.1 添加漫游

点击<添加漫游>按钮会弹出添加漫游的界面。用户需要输入信任 **AS 的 IP**，并导入信任 AS 的 **ASU 证书**并选择**是否中心 AS**。

图 4-39 添加漫游

配置成功后，就会在漫游列表里看到新添加的漫游记录。

图 4-40 新添加的漫游记录

4.7.1.2 删除漫游

点击想要删除的漫游记录右边的<删除>按钮就可以删除该条漫游记录。

图 4-41 删除漫游

4.7.2 双机热备

双机热备功能需要两台 AS 设备，两台 AS 需要使用网线将 ETH7 网口互相连接。一台配置为主设备，一台配置为从设备。配置项如下图，其中，热备共用 IPv4 地址为两台 AS 的对外工作 IP。

热备配置流程如下：

1） 从设备在配置热备前，需要先执行“初始化”功能，执行完成之后，不要颁发证书；
2） 将 AS1 配置为主设备；
3） 将 AS2 配置为从设备；
4） 等待 2-5 分钟，从设备会自动从主设备同步数据；
5） 从设备数据同步完成之后，需要手动重启一次；

热备配置完成之后，等待 2-5 分钟，可在 web 页面观察数据同步是否完成。例如可以查看从设备 AS 根证书基本信息是否与主设备一致，AS 证书管理页面查询到用户证书信息是否一致。当从设备数据同步完成之后，需要重启一次从设备。

图 4-42 热备配置

4.8 版本信息

版本信息界面显示了当前 AS 的版本信息。

图 4-43 版本信息

4.9 退出

为了系统的安全，完成管理操作后，应先注销登录后，再关闭浏览器的窗口。注销登录的方法为：点击 web 页面上右上角的<退出>按钮，返回到登录界面，即退出了系统的登录。

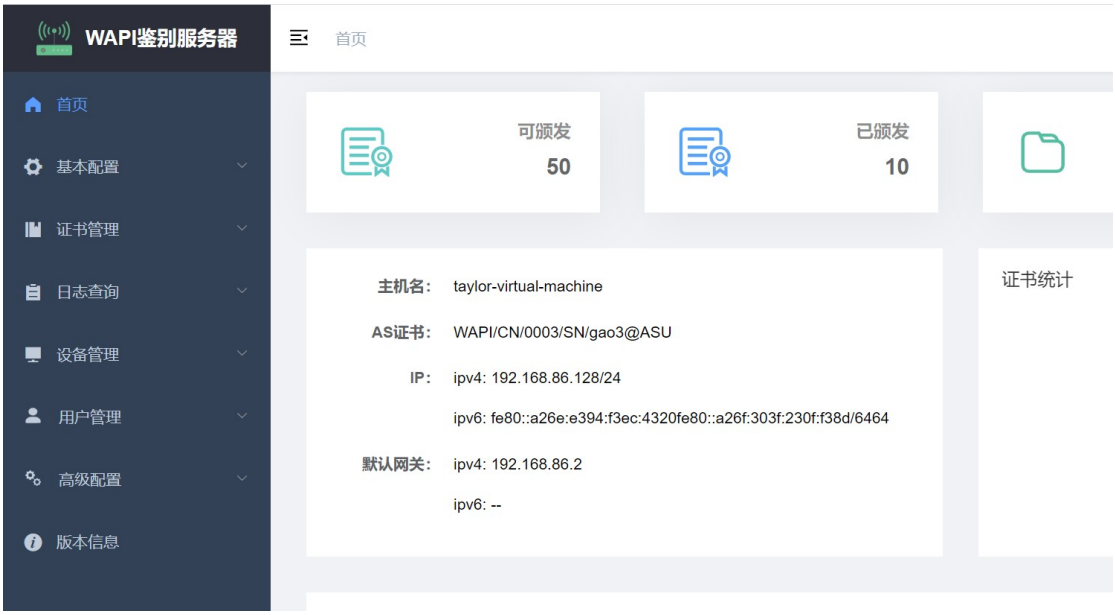

图 4-44 注销登录

5 术语

缩略语	意义
WAPI	无线局域网鉴别与保密基础结构
AS	鉴别服务器
AE	鉴别器实体
AP	WLAN 接入点
ASUE	鉴别请求者实体
STA	终端
CRL	证书吊销列表