Aten 宏正信息集中管理系统

启用安盟多因素动态口令身份认证系统

操作手册

四川安盟电子信息安全有限责任公司

2020 年 06 月

版本管理

版本	摘要	编者	日期
1.00	基本配置	陈俊	2020/06/29
1.01	增加安盟认证服务器基本配置	陈俊	2020/07/30
1.02	增加认证逻辑图	陈俊	2020/07/30

1 目录

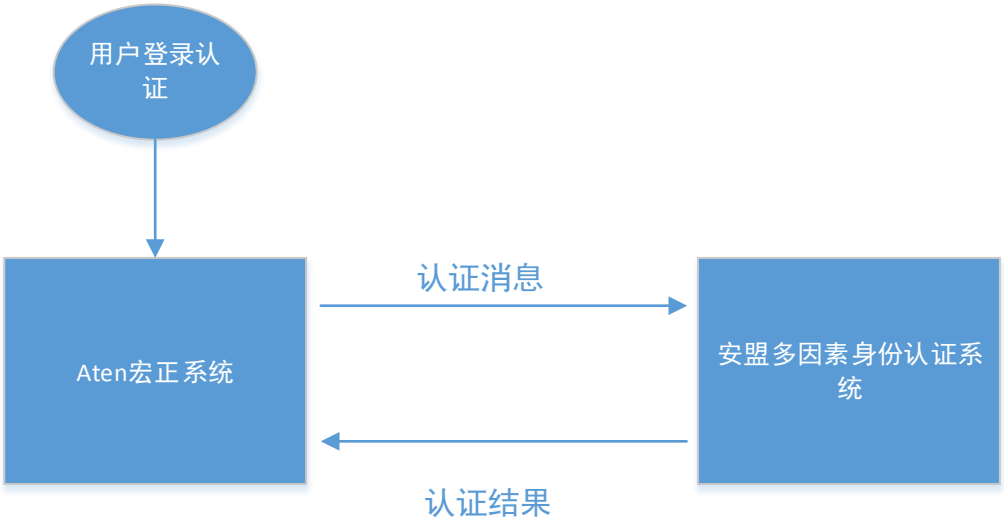
2 概述

Aten 宏正信息管理系统，是一种将账户信息进行统一管理的集成系统。该系统账户管理支持第三方认证，使用标准 Radius 认证协议。

启用安盟动态口令多因素身份认证系统，可以接管原有系统的密码验证。密码由原先的静态口令变换为动态口令模式。

3 认证逻辑

信息管理系统自身有一套密码登录管理系统，该身份认证方式为静态密码系统。启用安盟身份认证系统，可以完成动态口令强身份认证。



Aten 宏正信息管理系统密码验证由安盟身份认证服务器接管。原本的登录画面不会改变，在输入密码的内容里边，更换为安盟的动态密码。

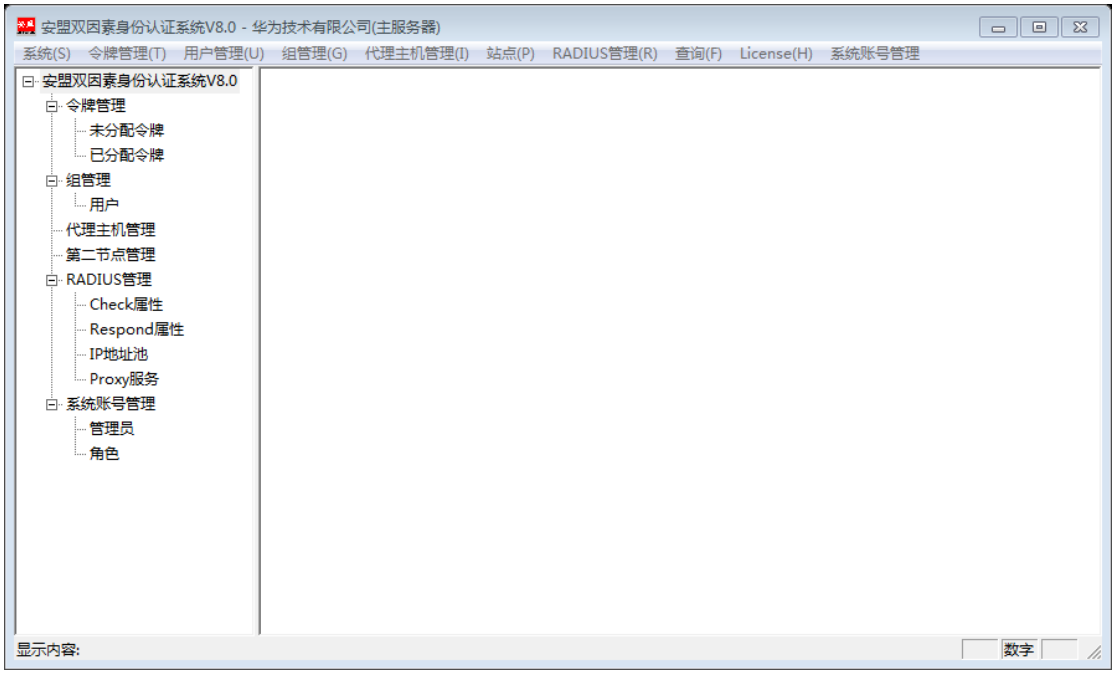
4 安盟身份认证系统配置

安盟身份认证系统需要将宏正信息管理系统添加到代理主机中。添加用户，需要注意该用户名称需要和宏正信息管理系统中的用户一致。因为管理系统只有分配了资源，才能赋权给其它设备联动。

假设应用场景，是一个叫张三的用户是一个维护管理员，信息管理系统创建维护账号 zhangsan，同样需要在安盟认证服务器上创建一个 zhangsan 的用户。

4.1 登录安盟服务器管理器

以管理员身份登录安盟服务器管理器



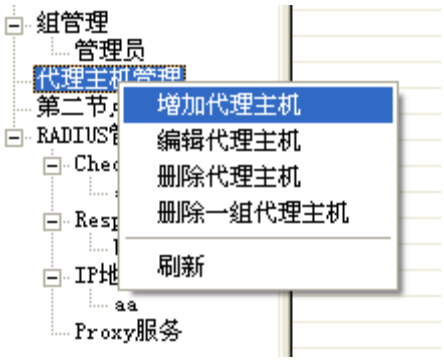
4.2 添加认证用户

添加用户

注意，为了测试方便，勾选 [在所有代理主机上激活]

4.3 添加代理主机

第一步：在左侧窗口，要增加代理主机的站点>代理主机管理，在右侧窗口右键>增加代理主机。



弹出编辑代理主机对话框，输入代理主机的机器名和 IP 地址。

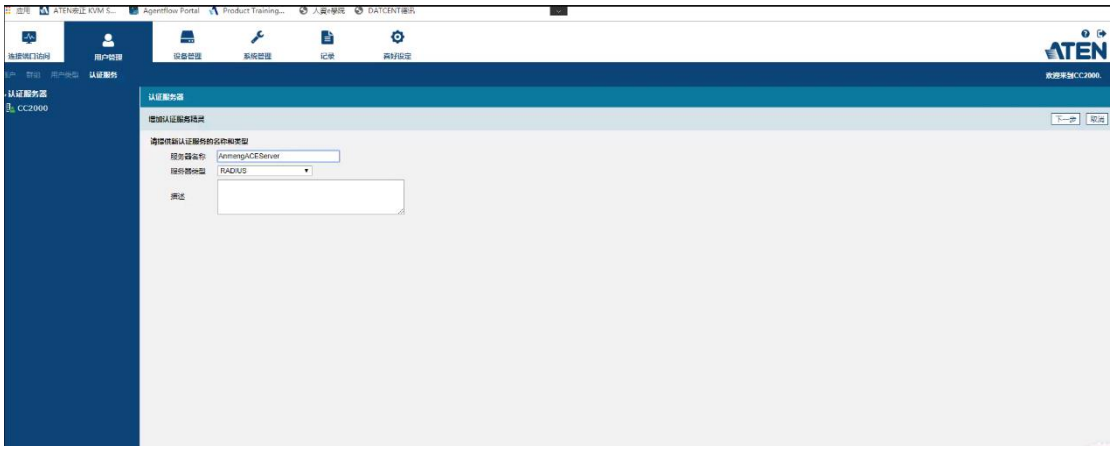
点击保存。

注意：Radius 密钥，为共享密钥，此处设置要与安恒堡垒机一致，勾选向所有代理主机激活。

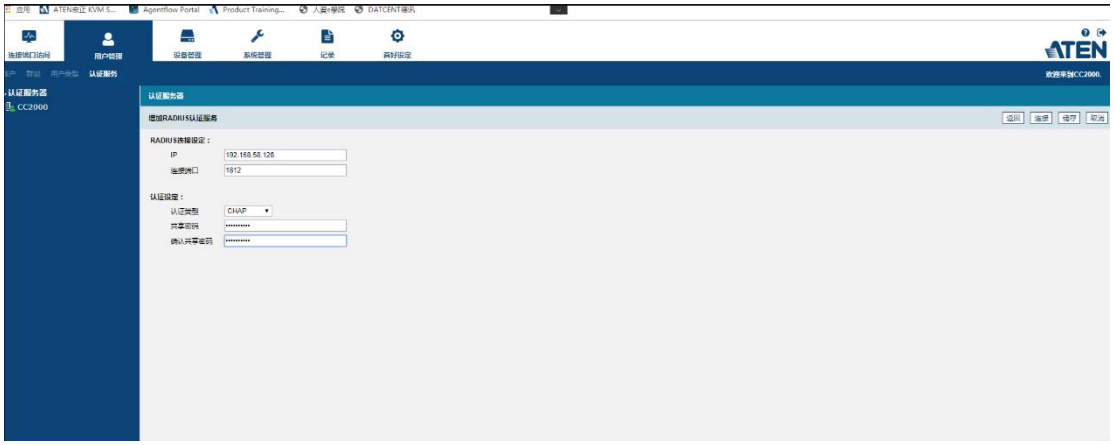
5 宏正系统配置方式

使用超级账户进入管理界面

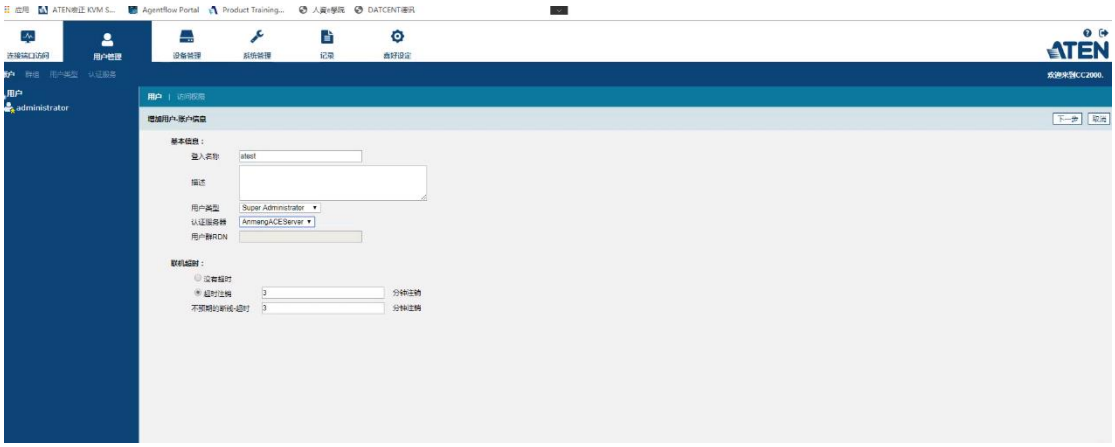
用户管理



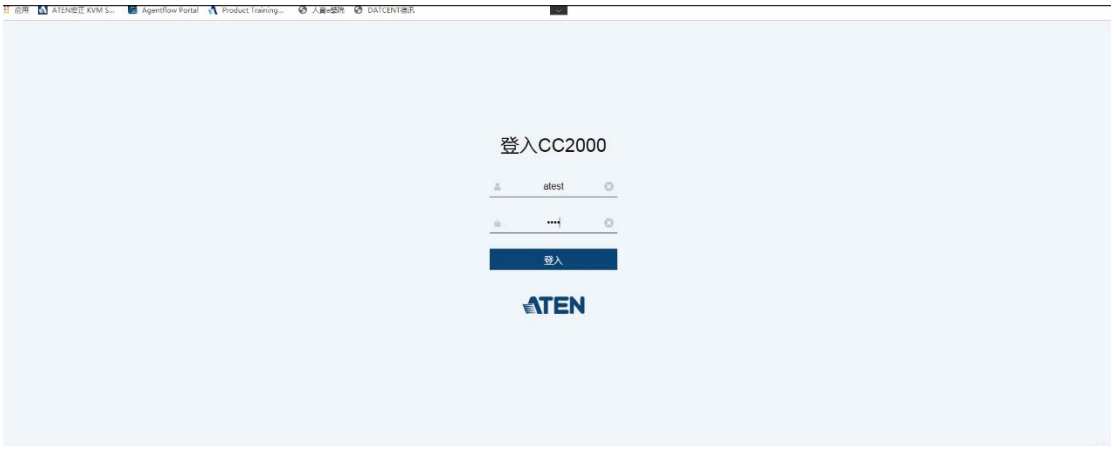
添加安盟认证服务器地址和 Radius 公钥



创建一个测试用户



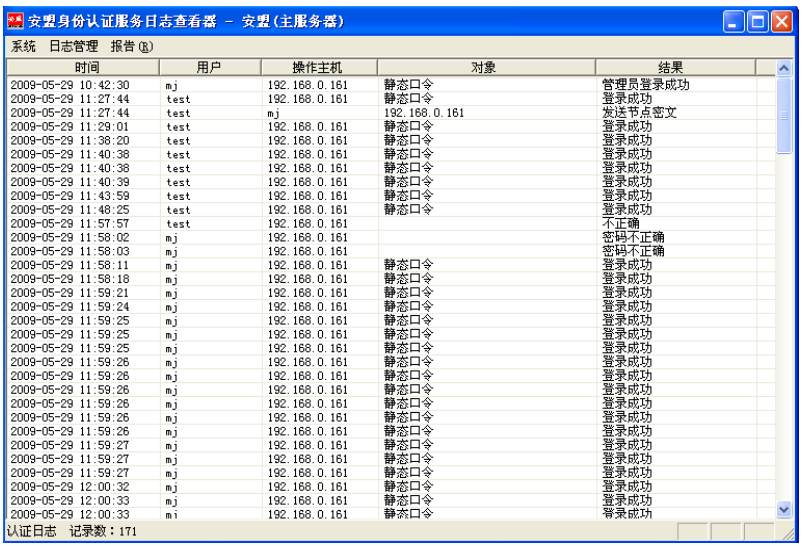
登录测试



6 常见问题排除方法

6.1 查看认证日志

以日志管理员身份，登录安盟身份**认证日志查看器**



各列的具体含义见下表：

列名	含义
时间	用户进行操作的时间
用户	进行操作的用户的帐号
操作主机	用户进行操作时所在主机的标识
对象	被操作的用户帐号

结果	用户进行的具体的操作

6.2 用户登录没有认证日志

检查网络是否畅通，从客户端 PING 认证服务器是否能连通。

6.3 认证日志提示”未注册用户”

检查用户名称是否正确，如果用户名正确，检查认证服务器上边是否有这个用户。

6.4 认证日志提示”用户不在代理主机上”

检查用户是否在该代理主机上激活，若没有执行激活代理主机。用户在安盟服务器上有访问规则限制，根据需要设计是否在代理主机上访问，由于认证信息是瞬间完成，因此，需要用户在目标机器上激活。

6.5 认证日志提示”用户密码错”源地址与目的地址不一致

检查代理主机客户端，添加 IP 地址映射，标明本地主网卡地址。这种情况是由于机器有多个网卡造成，需要指定一个主要网卡。

6.6 认证日志提示”用户密码错”，未生成节点密文

检查保护主机是否有多个网卡，需要在 host 文件中指明主网卡

6.7 清理节点密文

此种情况是，原先可以正常认证，后期变动路由或交换机等网络设备，致使消息包传送路径发生变化，需要执行请节点密文操作。