SUNDRAY 信锐技术

单点登录原理与测试指导手册

2019 年 6 月

Sundray TAC

信锐技术

文档密级：渠道合作伙伴

前　言

概述

单点登录 SSO（Single Sign On）说得简单点就是在一个多系统共存的环境下，用户在一处登录后，就不用在其他系统中登录，也就是用户的一次登录能得到其他所有系统的信任。即无线控制器和深信服上网行为管理做单点登录，不需要重复认证两次，只需要在无线控制器认证一次就可以实现双方认证信息共享。

修订记录

日期	版本	修订说明	作者
2019-6	v1.0	第一次发布	sundray_tac

图示

符号	说明
注意	有潜在风险，请谨慎操作。
窍门	能帮助您解决某个问题或节省您的时间。
说明	是正文的附加信息，是对正文的强调和补充。

目录

1 单点登录介绍

1.1 适用场景

单点登录是将用户的认证信息发送到深信服上网行为管理设备（或深信服防火墙等其他深信服设备），避免用户再次认证。即适用于无线控制器和深信服设备都做认证，但为了避免出现重复认证的现象，通过配置单点只需在无线控制器做认证后把认证用户信息传递到深信服上网行为管理，达到避免重复认证的问题发生。

1.2 用户类型

a) 无线用户：无线用户，包括本地转发和集中转发的用户
b) 控制器有线用户：在控制器上完成有线认证的用户
c) 接入点有线用户：完成接入有线认证的用户
d) 所有用户：包括无线用户、控制器有线用户、接入点有线用户。

1.3 协议类型区别

深信服单点登录协议 0.1

深信服上网行为管理设备使用的单点登录协议（AC11.0 之前版本支持），协议默认使用 1773 端口。

深信服单点登录协议 1.0

深信服上网行为管理设备使用的单点登录协议（AC11.0 及后续版本支持），协议同时兼容 0.1 版本。协议默认使用 1775 端口。

2 典型场景配置

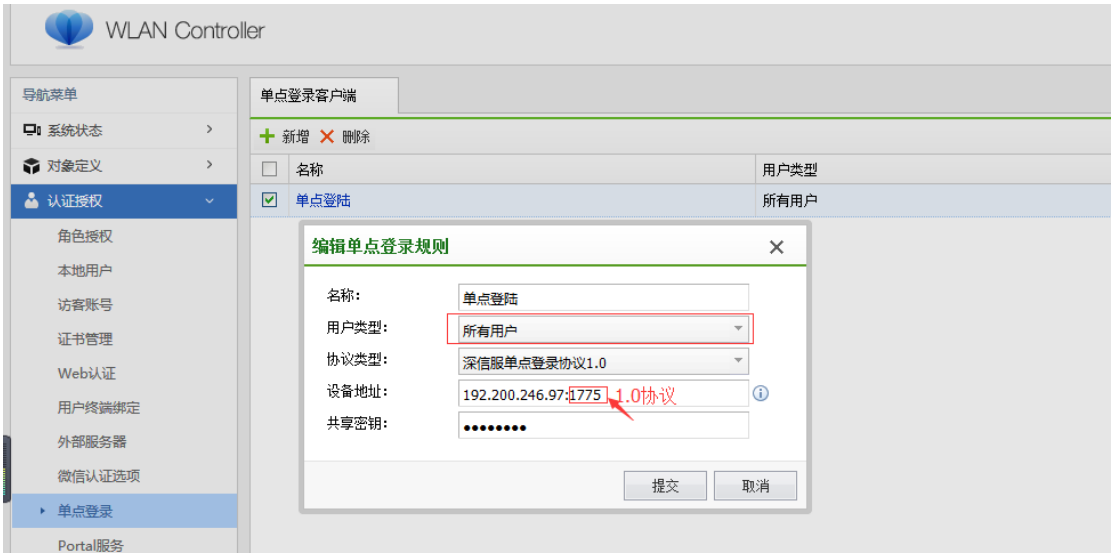
2.1 AC 和 NAC 同一局域网

无线控制器（NAC）和上网行为管理(AC)在一个局域网内，即终端用户认证流量经过双方设备后导致终端进行两次认证；在此环境下一般上网行为管理作为上层设备，因此无线控制器（NAC）需要配置单点登录防止终端出现重复认证。

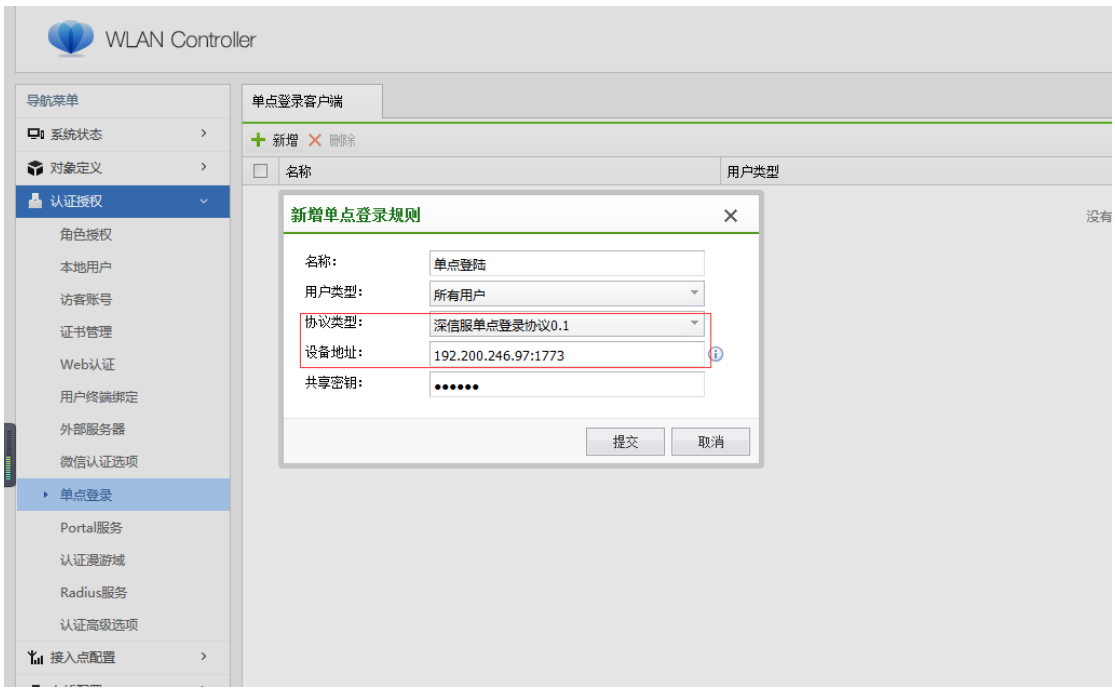
2.1.1 NAC 配置

在控制器 WEB 界面【认证授权】-【单点登录】-【新增单点登录客户端】-用户类型自选择，有“所有用户”、“无线用户”、“控制器有线用户”和“接入点有线用户”，协议类型根据深信服上网行为管理（AC）来决定，设备地址填写深信服上网行为管理（AC）的“IP+端口”，共享密钥需双方一致。

深信服 AC11.0 及以上版本配置：协议选择 1.0，端口 1775

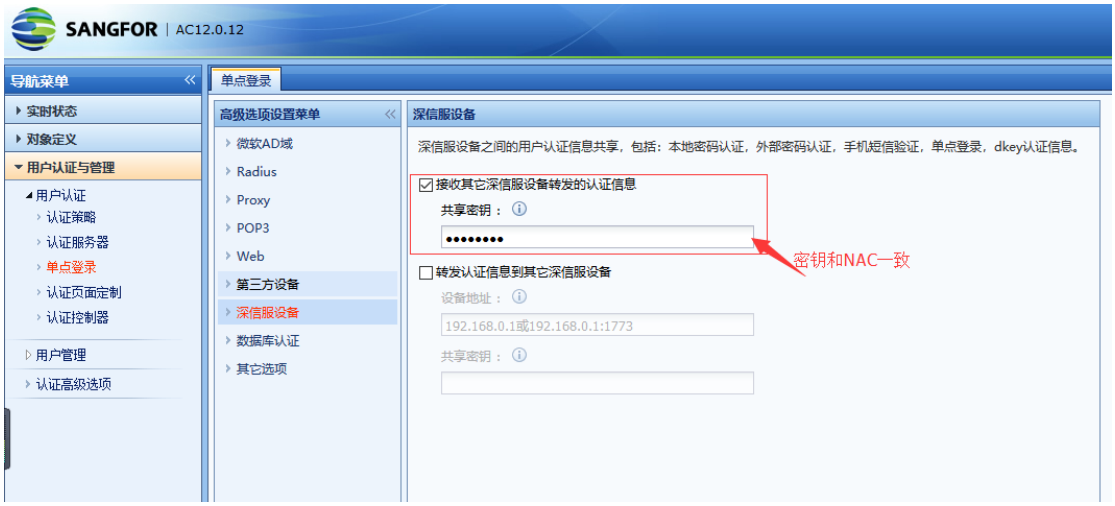


深信服 AC11.0 版本配置：协议选择 0.1，端口 1773

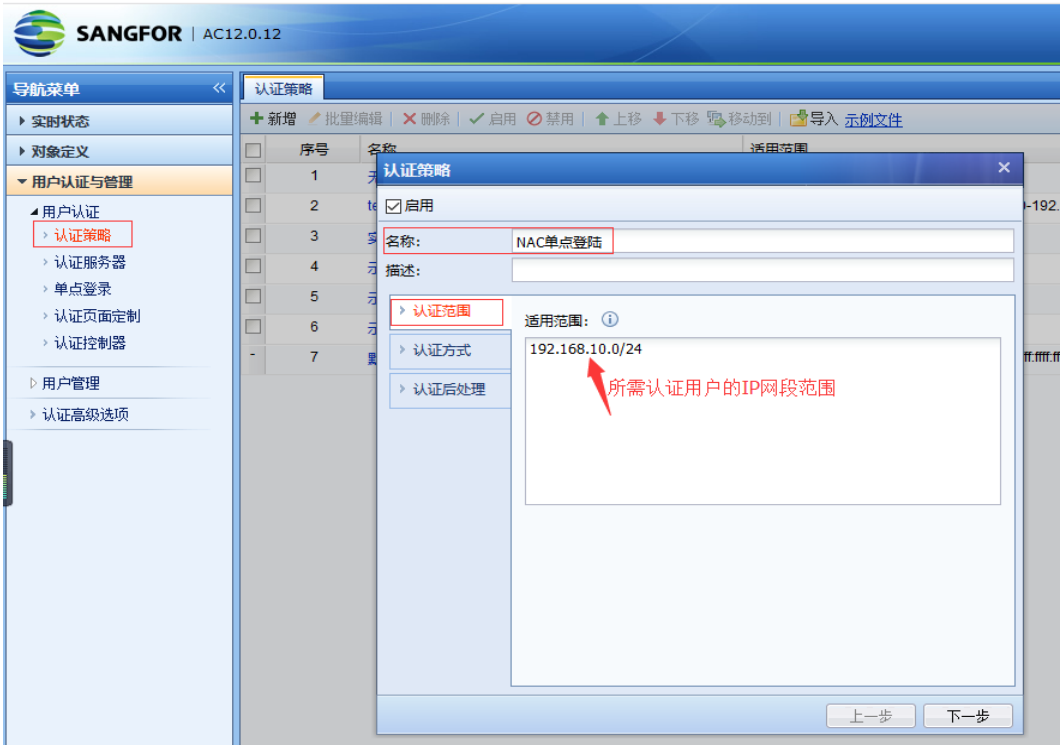


2.1.2 深信服设备配置

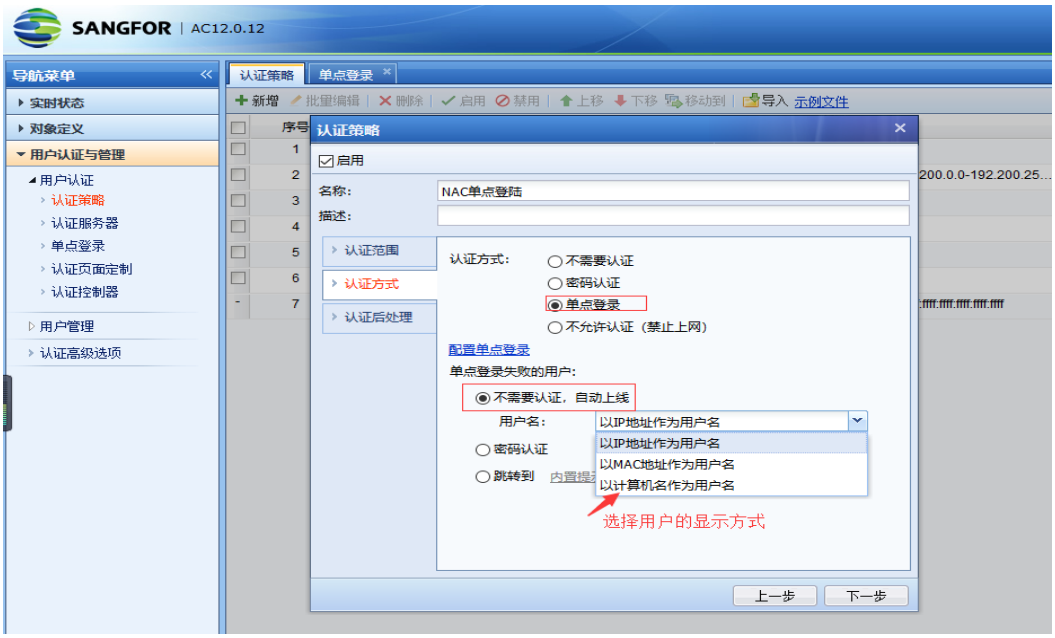
这里以深信服上网行为管理 AC（v12.0.12）为例，在【用户认证与管理】-【用户认证】-【单点登录】-【深信服设备】勾选“接收其他深信服设备转发的认证信息”，填入和无线控制器（NAC）一致的共享密钥然后提交。



【用户认证与管理】-【用户认证】-【认证策略】-【认证范围】 填入“无线控制器”的网段范围。

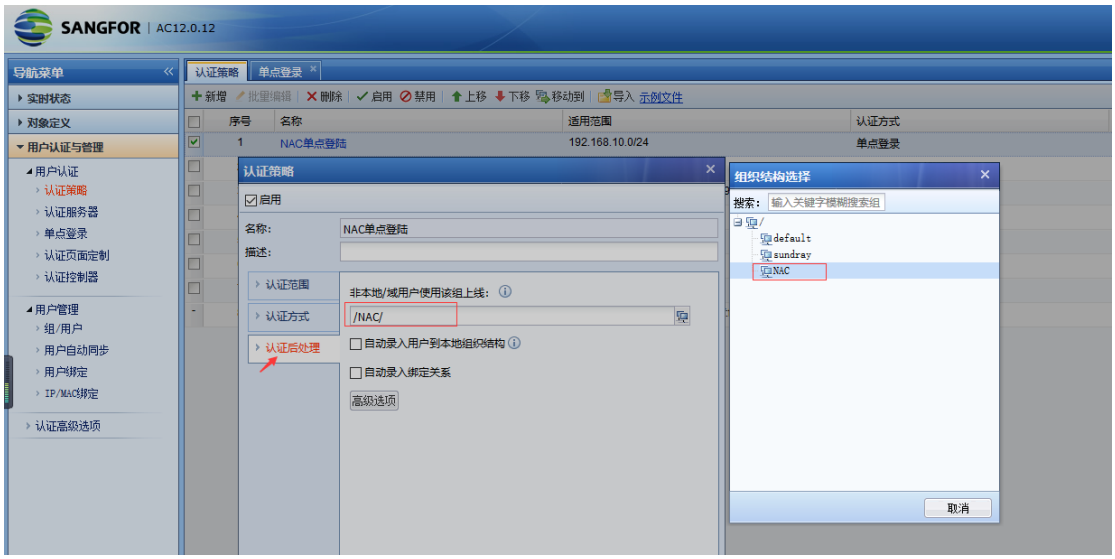


认证方式选择“单点登录”，选择“不需要认证，自动上线”，用户名根据实际情况选择以下“以 IP 地址为用户名”、“ 以 MAC 地址为用户名”、“ 以计算机名为用户名”这三种方式。



在【用户认证与管理】-【用户管理】-【组/用户】新增用户组名为“NAC”

在刚才认证策略中最后一步，认证后处理选择用户组为新增的“NAC”组，这样只要是经过无线控制器的用户认证成功后，都会被分配到这个组方便后期的维护和管理。



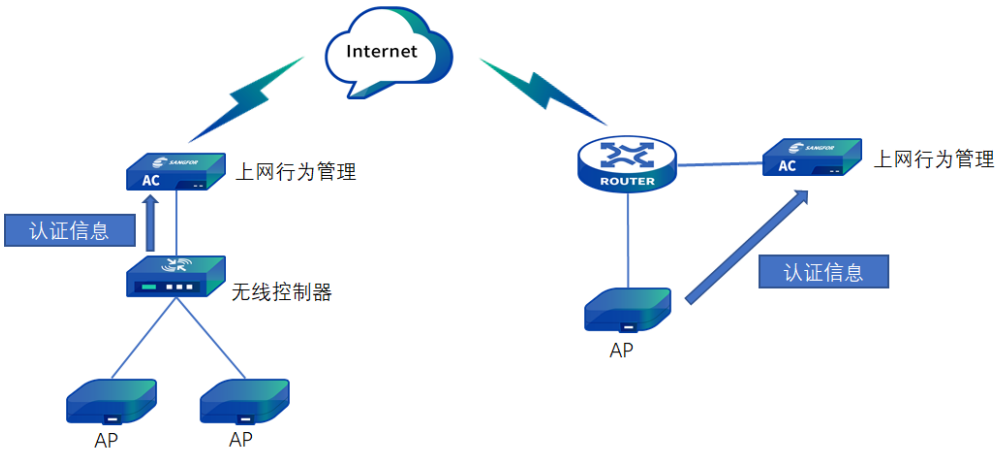
2.1.3 认证效果展示

认证后在新增的指定“NAC”组里查看到认证方式为“深信服转发”，网段也是192.168.10.0/24 段的终端用户认证信息，说明此单点登录的配置生效了。

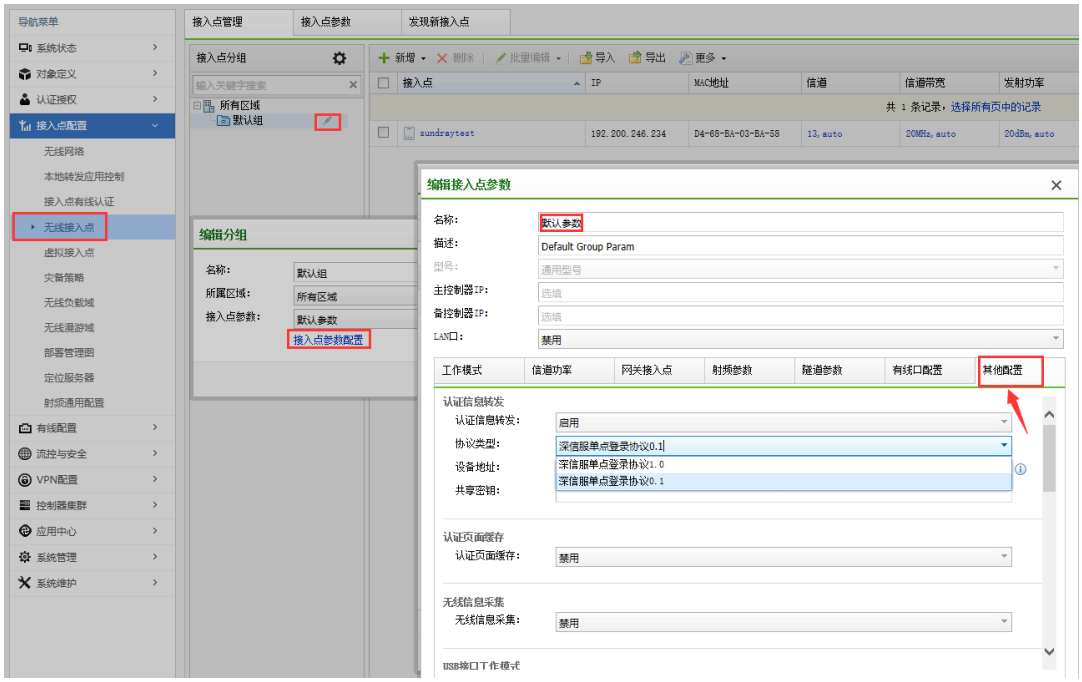
2.2 AC 和 NAC 跨公网部署

无线控制器（NAC）和上网行为管理(AC)跨公网部署，分支端有上网行为管理（AC）和远程部署 AP，AP 通过本地转发出去上网，同时上网行为管理（AC）也开启了认证功能，这样导致分支端用户无线认证完后还需要在上网行为管理上做认证；因此这边需要配置单点登录防止终端出现重复认证。

个别 AP 通过 AP 自身将无线用户的认证信息转发至深信服设备，多适用于远程部署本地转发情况下。

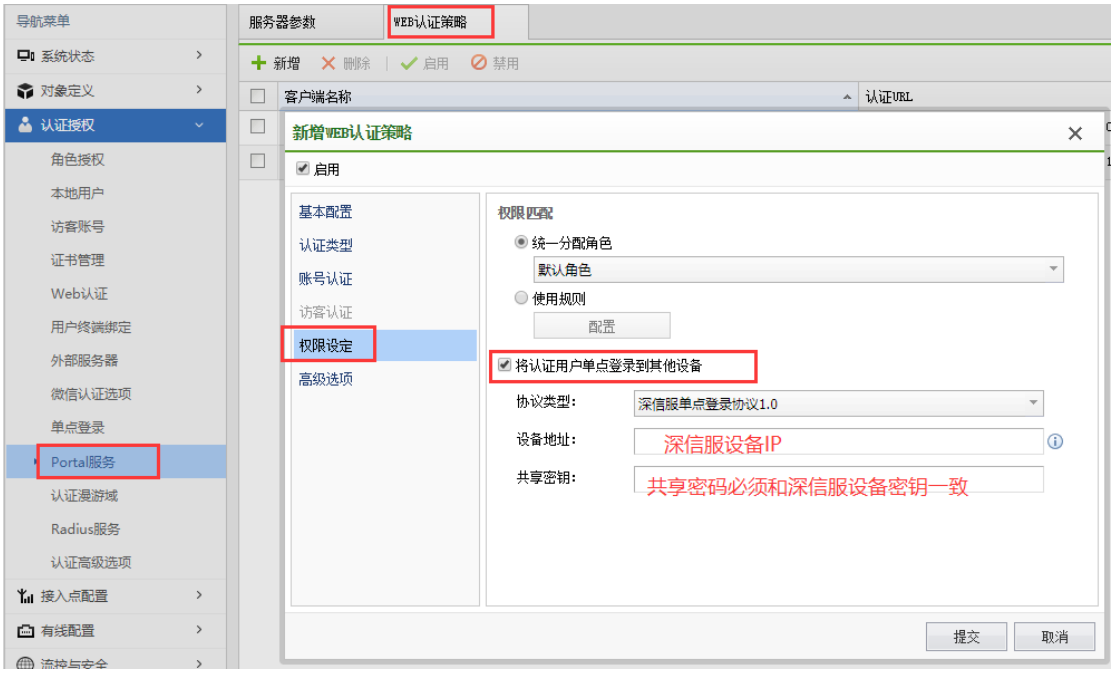


在接入点（编辑->参数配置->其他配置）或接入点分组（编辑->接入点参数配置->其他配置）中 ，配置认证信息转发。



2.3 NAC 作为 Portal 服务器环境

适用于无线控制器做 Portal 服务器时，由控制器将 Portal 用户认证信息转发至深信服设备，在【认证授权】-【Portal 服务】-【WEB 认证策略】中，编辑认证策略->权限设定中配置。



3 注意事项

1、对于远程部署的 AP，需要单独在 AP 上配置单点登录。

2、对于 Portal 对接，单点登录是在 Portal 服务的 WEB 策略里面进行配置

3、无线控制器配置单点登录需根据深信服上网行为管理（AC）的软件版本进行配置，AC11.0 及以后版本支持 1.0（端口 1775）或 AC11.0 之前版本支持 0.1（端口 1773）协议类型。