

403 Forbidden

本电子书由CyberArticle制作。点击[这里](#)下载CyberArticle。注册版本不会显示该信息。[删除广告](#)

V7 WX系列无线控制器管理用户认证 典型配置案例（HWTACACS服务器）

目录

[V7 WX系列无线控制器管理用户认证典型配置案例（HWTACACS服务器）](#)

[1 配置需求或说明](#)

[适用场合](#)

[配置需求及实现的效果](#)

[2 组网图](#)

[3 配置步骤](#)

[配置HWTACACS服务器（IMC）](#)

[3.1.1 增加设备](#)

[3.1.2 增加启用认证的授权策略](#)

[3.1.3 增加设备用户](#)

[配置接入设备](#)

[登录设备](#)

1 配置需求或说明

1.1 适用场合

适用于设备管理员登录设备时需要进行身份验证的场合。

1.2 配置需求及实现的效果

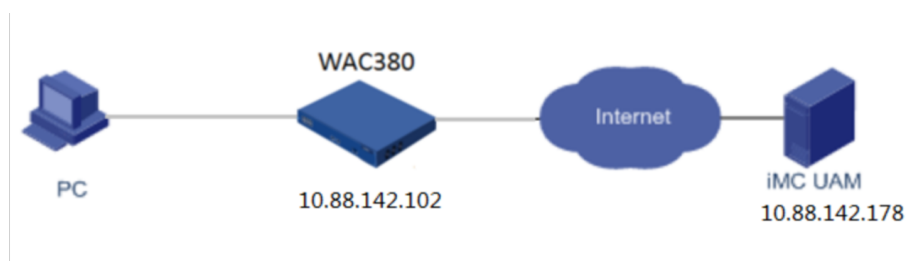
配置前需确保终端、设备、服务器相互连通。

设备管理员以Telnet 方式登录设备时，需要进行外置AAA服务器进行身份验证，输入账户密码：admin/admin，HWTACACS服务器进行验证，只有验证通过后才能登录到设备进行操作。

IMC作为HWTACACS服务器，该实验中以iMC为例（使用iMC版本为：iMC PLAT 7.3(E0605)、iMC EIA 7.3(E0504)）。

2 组网图

HWTACACS 服务器 IP 为 10.88.142.178，设备 IP 地址为 10.88.142.102。

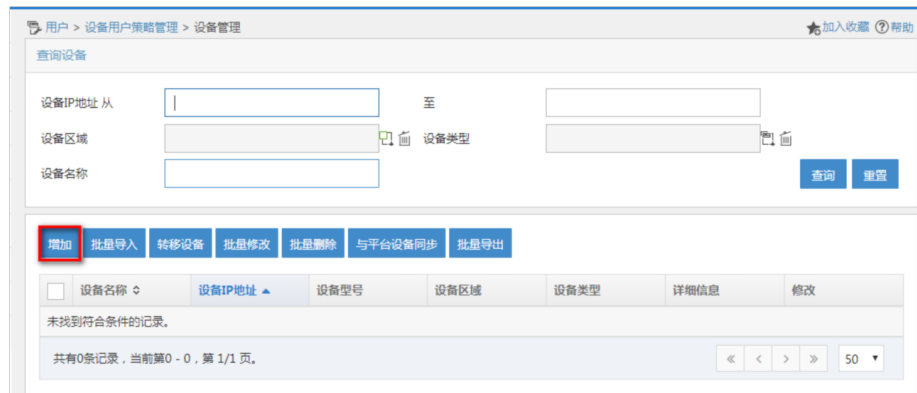


3 配置步骤

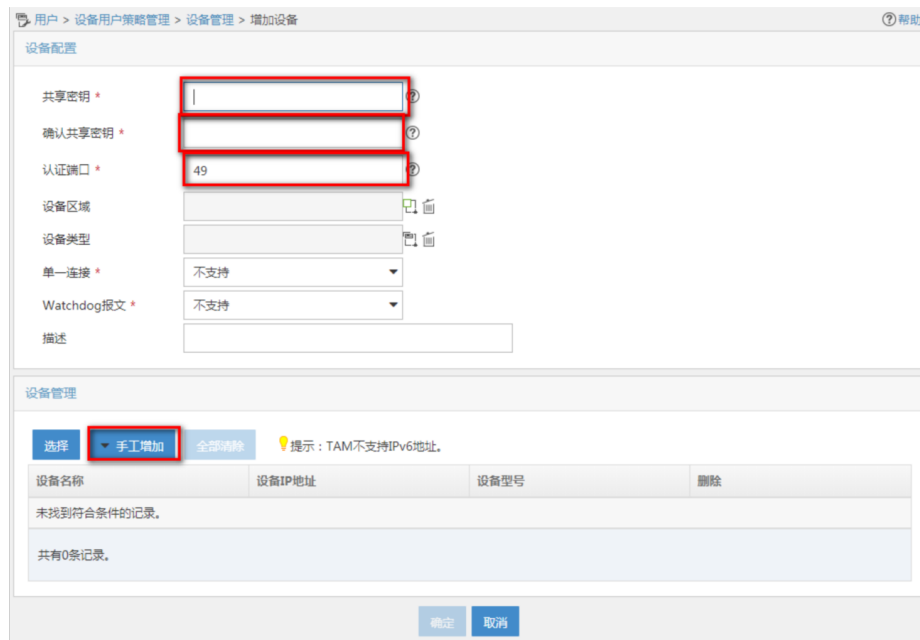
3.1 配置HWTACACS服务器（IMC）

3.1.1 增加设备

- (1) 选择“用户”页签。
- (2) 单击导航树中的“设备用户策略管理 > 设备管理”菜单项，进入“设备管理”页面。



(3) 单击<增加>按钮，进入“增加设备”页面。



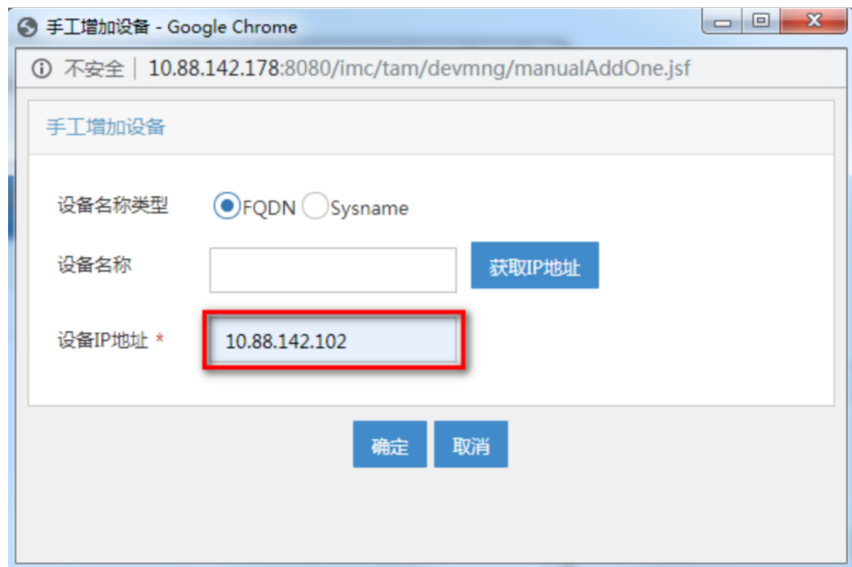
(4) 配置设备参数如下：

共享密钥/确认共享密钥：此处的配置必须与设备命令行配置的共享密钥保持一致。本例采用“fine”作为共享密钥。

认证端口：此处必须与设备命令行配置的端口保持一致。本例采

用缺省值 49。其他参数，保持缺省值。

- (5) 配置设备，手工增加：在设备管理区域，单击<手工增加>按钮，在弹出的下拉列表中选择“批量增加”项，弹出手工增加设备窗口。



- (6) 单击<确定>按钮，增加设备成功，返回增加设备页面。

用户 > 设备用户策略管理 > 设备管理 > 增加设备

设备配置

共享密钥 *

确认共享密钥 *

认证端口 *

设备区域

设备类型

单一连接 *

Watchdog报文 *

描述

设备管理

选择 手工增加 全部清除 提示：TAM不支持IPv6地址。

设备名称	设备IP地址	设备型号	删除
	10.88.142.102		

共有1条记录。

确定 取消

- (7) 单击<确定>按钮，增加设备完毕，进入“增加设备结果”页面。

3.1.2 增加启用认证的授权策略

- (1) 选择“用户”页签。
- (2) 单击导航树中的“设备用户策略管理 > 授权命令配置 > Shell Profile 配置 > 增加 Shell Profile”菜单项，进入“新增 Shell Profile”页面，输入名称：授权级别，授权级别选择最高级15。

用户 > 设备用户策略管理 > 授权命令配置 > Shell Profile配置 > 增加Shell Profile

增加Shell Profile

Shell Profile名称 *	授权级别
接入控制列表	?
授权级别	15
闲置时长	分钟
会话时长	分钟
自动执行命令	
自定义属性	增加属性 ?
描述	

确定 取消

(3) 单击导航树中的“设备用户策略管理 > 授权策略管理”菜单项，进入“授权策略管理”页面。

(4) 单击<增加>按钮，进入“增加授权策略”页面。

用户 > 设备用户策略管理 > 授权策略管理

★ 加入收藏 ? 帮助

增加 刷新

策略名称 ▲	描述	修改	删除
未找到符合条件的记录。			
共有0条记录。			

(5) 修改“接入授权信息”的缺省记录。点击“修改”图标，弹出“修改接入授权信息”窗口，

将“Shell Profile”修改为“授权级别”，将“授权命令集”设置为“不限”。

用户 > 设备用户策略管理 > 授权策略管理 > 增加授权策略

授权策略信息

基本信息

授权策略名 * test

描述

☐ 启用RSA

接入授权信息

增加

设备区域	设备类型	授权时段	Shell Profile	授权命令集	优先级	修改	删除
不限	不限	不限	拒绝	禁止使用			

确定 取消

10.88.142.178:8080/imc/tam/authpolicy/addAccessAuthorizeInfo.xhtml

接入授权信息

设备区域 不限

设备类型 不限

授权时段 不限

Shell Profile 授权级别

授权命令集 不限

确定 取消

- (6) 单击<确定>按钮，完成修改接入授权信息，返回“增加授权策略”页面。
- (7) 单击<确定>按钮，授权策略增加完毕，可在授权策略列表中查看新增的授权策略。

用户 > 设备用户策略管理 > 授权策略管理 > 修改授权策略

授权策略信息

基本信息

授权策略名 *

test

描述

☐ 启用RSA

接入授权信息

增加

设备区域	设备类型	授权时段	Shell Profile	授权命令集	优先级	修改
不限	不限	不限	授权级别	不限		

确定

取消

3.1.3 增加设备用户

设备用户是用户登录设备时使用的帐号，包含帐号名、密码和使用的授权策略等信息。

- (1) 选择“用户”页签。
- (2) 单击导航树中的“设备用户管理 > 所有设备用户”菜单项，进入“所有设备用户”页面。
- (3) 单击<增加>按钮，进入“增加设备用户”页面。
- (4) 输入“帐号名”、“登录密码”和“登录密码确认”，并且“用户的授权策略”选择“test”，其它参数保留缺省值，本例登录密码为admin。

3.2 配置接入设备

- (1) #首次登入会出现如下提示，要求输入国家码。需要配置国家码为CN，如选择其他区域可能会造成部分功能无法使用。以下标红色部分为设备自动打印部分。加粗的CN是需要手动输入的国家码。

Press ENTER to get started.

Please set your country/region code.

Input ? to get the country code list, or input q to log out.

CN

- (2) 配置用户Telnet 登录时通过账户密码认证。

```
[H3C]line vty 0 63
```

```
[H3C-line-vty0-63]authentication-mode scheme
```

```
[H3C-line-vty0-63]quit
```

- (3) 创建HWTACACS方案test。IP 地址指向iMC UAM 服务器，监

听端口、共享密钥fine需与iMC 中接入设备的配置保持一致。

```
[H3C]hwtacacs scheme test
[H3C-hwtacacs-test]primary authentication 10.88.142.178 49
[H3C-hwtacacs-test]primary authorization 10.88.142.178 49
[H3C-hwtacacs-test]primary accounting 10.88.142.178 49
[H3C-hwtacacs-test]key authorization simple fine
[H3C-hwtacacs-test]key authentication simple fine
[H3C-hwtacacs-test]key accounting simple fine
[H3C-hwtacacs-test]user-name-format without-domain
[H3C-hwtacacs-test]quit
```

- (4) 创建domain。配置域引用的 TACACS 方案。

```
[H3C] domain testdm
[H3C-isp-testdm] authentication login hwtacacs-scheme test
[H3C-isp-testdm] authorization login hwtacacs-scheme test
[H3C-isp-testdm] accounting login hwtacacs-scheme test
[H3C-isp-testdm]quit
```

- (5) 配置认证方式。开启 Telnet 开关

```
[H3C] telnet server enable
```

- (6) 配置默认域为testdm，登录设备时输入账户为admin，不需要带域名。为了不影响其他的认证，可以忽略该步骤，登录设备需要输入的用户是：admin@ testdm

```
[H3C]domain default enable testdm
```

3.3 登录设备

- (1) 以Telnet方式登录设备。

```

*****
* Copyright (c) 2004-2017 New H3C Technologies Co., Ltd. 个性设置, 点我看看
* Without the owner's prior written consent,
* no decompiling or reverse-engineering shall be allowed.
*****

```

授权

login: admin
Password:

- (2) 输入用户名和密码，其中用户名与iMC配置的设备管理用户的帐号名保持一致。

```

*****
* Copyright (c) 2004-2017 New H3C Technologies Co., Ltd. 个性设置, 点我看看
* Without the owner's prior written consent,
* no decompiling or reverse-engineering shall be allowed.
*****

```

授权

login: admin
Password:

sbus

<H3C>sys
System View: return to User View with Ctrl+Z.
[H3C]display users

Idx	Line	Idle	Time	Pid	Type
0	AUX 0	00:08:21	Jan 07 08:44:48	1846831	
10	VTY 0	00:00:22	Jan 03 06:18:08	392220	TEL
+ 11	VTY 1	00:00:01	Jan 07 09:05:23	1852355	TEL

Following are more details.

AUX 0 :
User name: admin

VTY 0 :
User name: admin
Location: 10.88.142.189

VTY 1 :
User name: admin
Location: 10.88.142.16

+ : Current operation user.
F : Current operation user works in async mode.

[H3C]