

5760基于Web界面权限级别的访问控制配置示例，使用思科访问控制服务器(ACS)

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[配置](#)

[在ACS中创建几个测试用户](#)

[设置策略元素和外壳配置文件](#)

[创建权限15级外壳访问配置文件](#)

[为管理员用户创建命令集](#)

[为只读用户创建外壳配置文件](#)

[创建服务选择规则以匹配tacacs协议](#)

[为完全管理访问创建授权策略。](#)

[为只读管理访问创建授权策略。](#)

[配置5760 for tacacs](#)

[使用两个不同的配置文件访问同一5760](#)

[相关的思科支持社区讨论](#)

简介

本文档将说明如何创建具有不同权限级别的Cisco ACS Tacacs+身份验证和授权配置文件，并将其与5760集成以访问WebUI。从3.6.3开始支持此功能（但在撰写本文时不支持3.7.x）。

先决条件

要求

假设读者熟悉Cisco ACS和融合接入控制器配置。本文档仅重点介绍tacacs+授权范围内这两个组件之间的交互。

使用的组件

本文档中的信息基于以下软件和硬件版本：

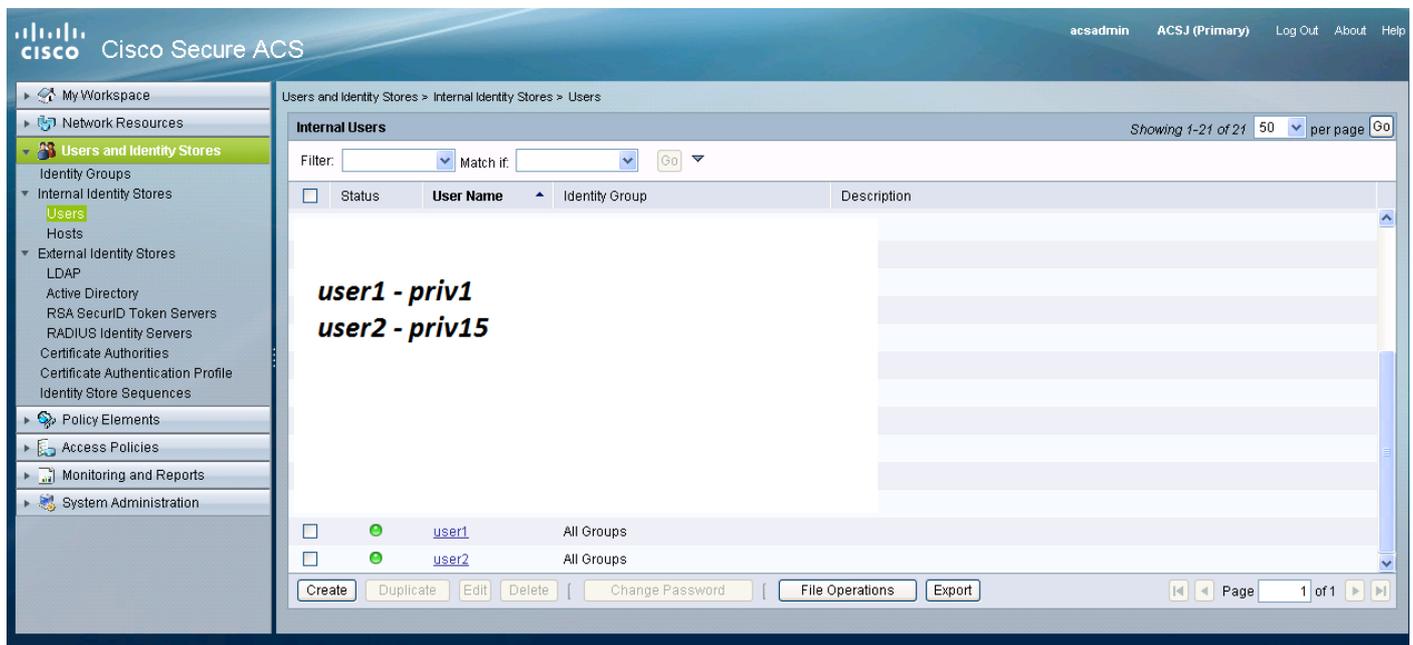
- 思科融合接入5760，版本3.6.3
- 思科访问控制服务器(ACS)5.2

配置

在ACS中创建几个测试用户

点击“用户和身份库”，然后选择“用户”。

单击“创建”并配置几个测试用户，如下图所示。



设置策略元素和外壳配置文件

您需要为两种不同类型的访问创建2个配置文件。在cisco tacacs世界中，权限15意味着提供对设备的完全访问，而不受任何限制。另一方面，权限1仅允许您登录并执行有限数量的命令。下面是对思科提供的访问级别的简短说明。

权限级别 1 = 无特权（提示符是 router>），这是登录的默认级别

权限级别 15 = 有特权（提示符是 router#），这是进入启用模式后的级别

权限级别 0 = 很少使用，但包括 5 个命令：**disable**、**enable**、**exit**、**help** 和 **logout**

在5760上，第2-14级被视为与第1级相同。它们被赋予与第1级相同的权限。**请勿在5760上为某些命令配置tacacs权限级别**。5760中不支持每个选项卡的UI访问。您可以拥有完全访问权限(priv15)，也可以只访问监控选项卡(priv1)。此外，权限级别为0的用户不允许登录。

创建权限15级外壳访问配置文件

使用下面的打印屏幕创建该配置文件：

点击“策略元素”。单击“Shell Profiles”。

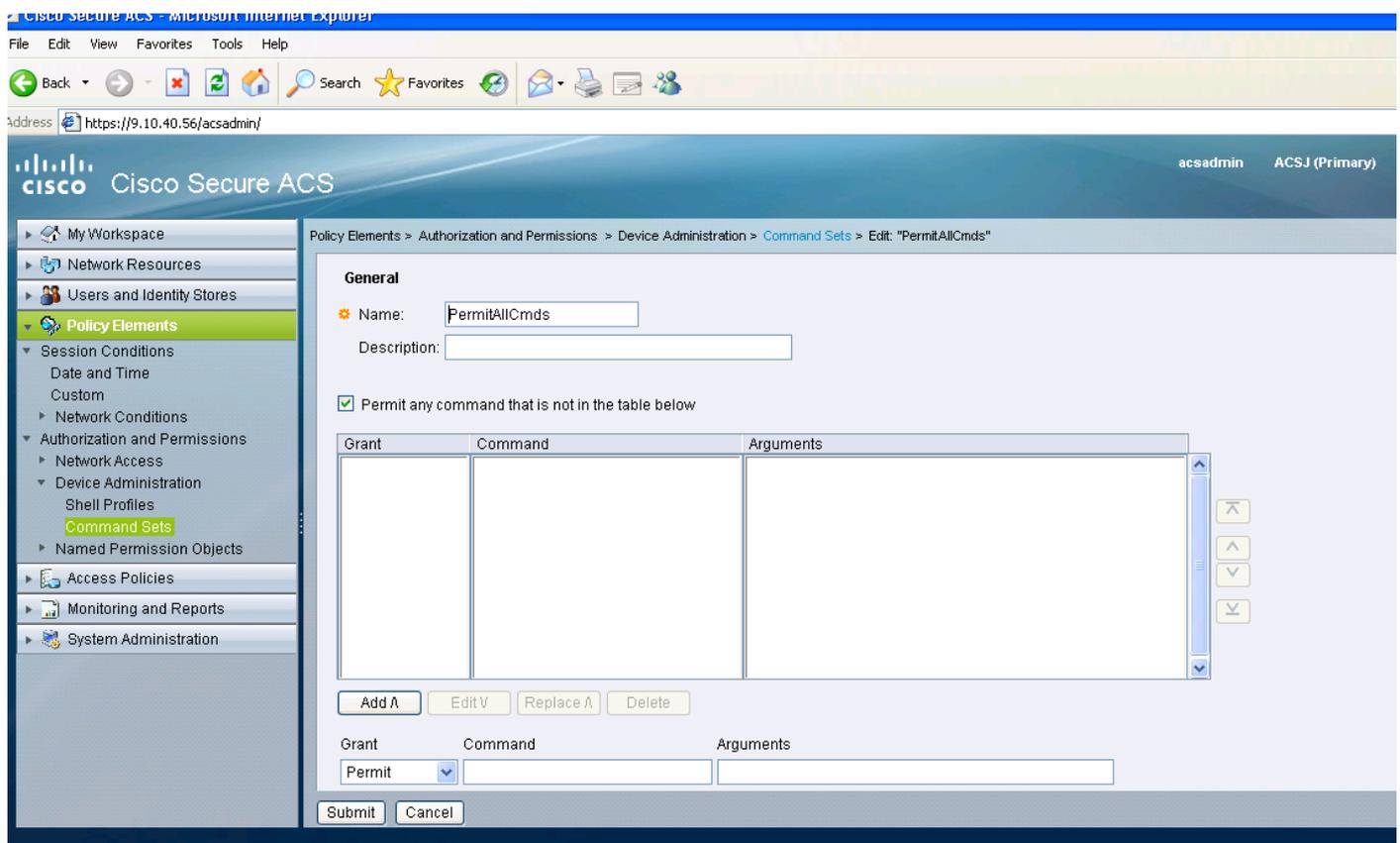
创建新的。

进入“常见任务”选项卡，将默认权限级别和最大权限级别设置为15。



为管理员用户创建命令集

命令集是所有tacacs设备使用的一组命令。它们可用于限制用户在分配特定配置文件时允许使用的命令。由于在5760上，根据所传递的权限级别对Webui代码进行限制，因此权限级别1和15的命令集相同。



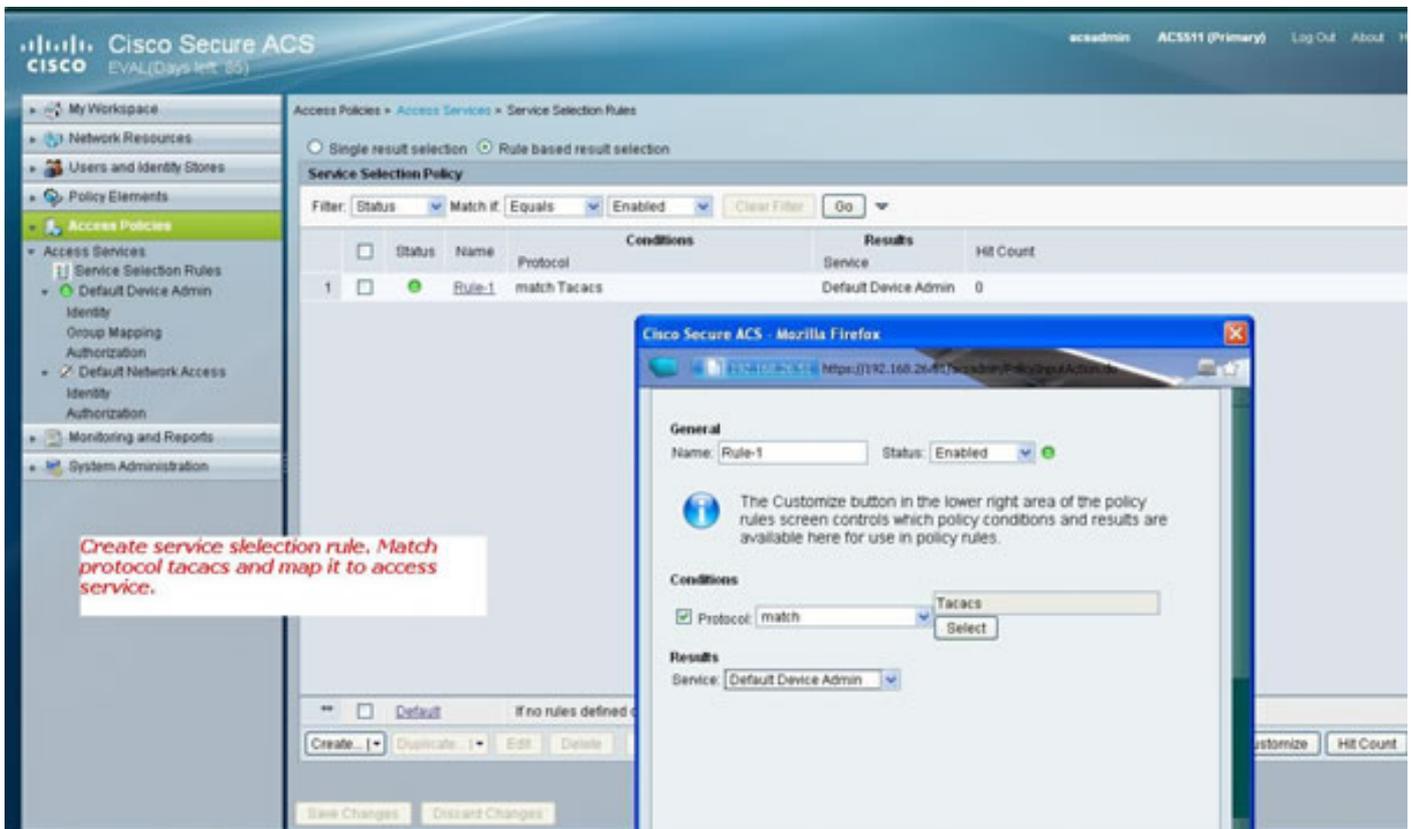
为只读用户创建外壳配置文件

为只读用户创建另一个外壳配置文件。此配置文件将因权限级别设置为1而异。

The screenshot displays the Cisco Secure ACS web interface. The left-hand navigation pane shows a tree structure with 'Policy Elements' selected and expanded to 'Shell Profiles'. The main content area is titled 'Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles > Edit: "joseph1"'. It features three tabs: 'General', 'Common Tasks', and 'Custom Attributes', with 'Common Tasks' currently active. Under the 'Common Tasks' tab, there are two sections: 'Privilege Level' and 'Shell Attributes'. The 'Privilege Level' section includes 'Default Privilege' and 'Maximum Privilege', both set to 'Static' with a 'Value' of '1'. The 'Shell Attributes' section includes 'Access Control List', 'Auto Command', 'No Callback Verify', 'No Escape', 'No Hang Up', 'Timeout', 'Idle Time', 'Callback Line', and 'Callback Rotary', all set to 'Not in Use'. A legend at the bottom indicates that a red asterisk icon represents 'Required fields'. At the bottom of the form are 'Submit' and 'Cancel' buttons.

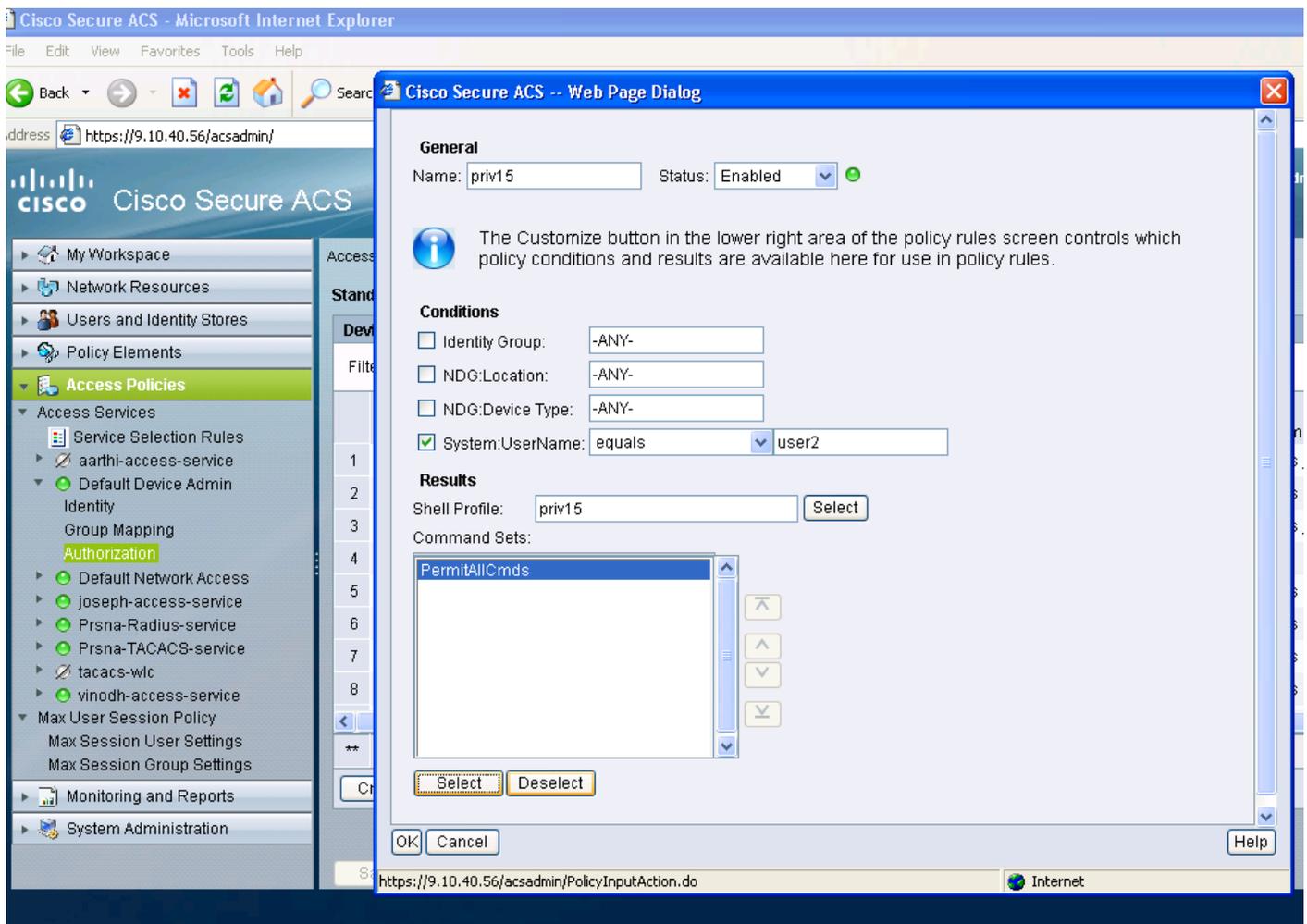
创建服务选择规则以匹配tacacs协议

根据您的策略和配置，确保您有与5760中的tacacs匹配的规则。



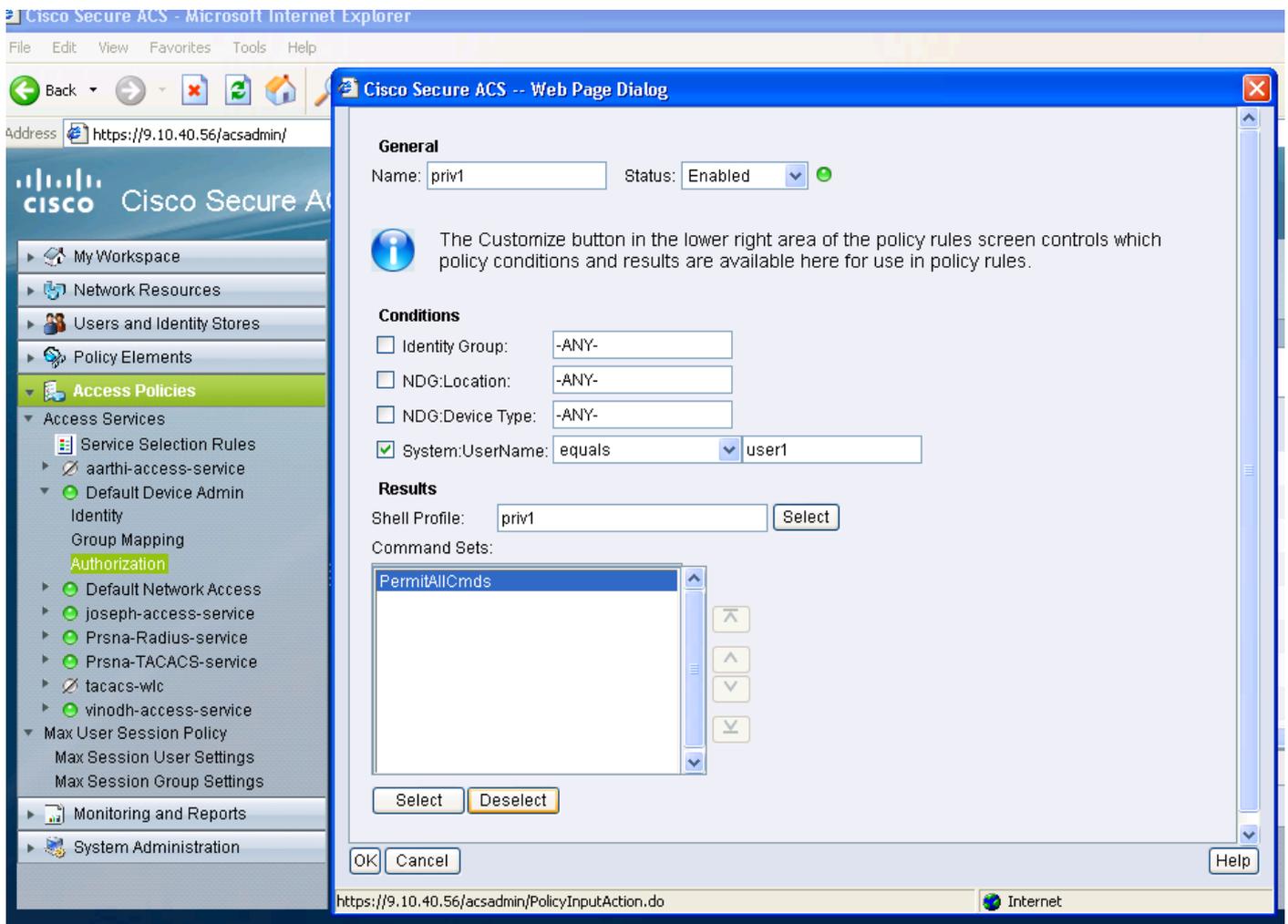
为完全管理访问创建授权策略。

在评估策略流程中，选择与tacacs协议选择一起使用的默认设备管理策略。使用tacacs协议进行身份验证时，选择的服务策略称为默认设备管理策略。该策略本身包括2个部分。身份表示用户是谁以及他属于哪个组（本地或外部），以及根据配置的授权配置文件允许他执行的操作。分配与您正在配置的用户相关的命令集。



为只读管理访问创建授权策略。

只读用户也是如此。本示例为用户1配置权限级别1外壳配置文件，为用户2配置权限级别15。



配置5760 for tacacs

1. 需要配置Radius/Tacacs服务器。

tacacs server tac_acct

地址ipv4 9.1.0.100

关键思科

2. 配置服务器组

aaa group server tacacs+ gtac

服务器名称tac_acct

在上述步骤之前，不存在前提条件。

3. 配置身份验证和授权方法列表

aaa authentication login <method-list> group <srv-grp>

aaa authorization exec <meth-list> group srv-grp

aaa authorization exec default group <srv-grp> —à解决方法，在http上获取tacacs。

上述3条命令以及所有其他身份验证和授权参数应使用相同的数据库，即radius/tacacs或local

例如，如果需要启用命令授权，则还需要指向同一数据库。

例如：

aaa authorization commands 15 <method-list> group <srv-grp> —>指向数据库 (tacacs/radius或本地) 的服务器组应相同。

4. 配置http以使用上述方法列表

ip http authentication aaa login-auth <method-list> —>方法列表需要在此处显式指定，即使方法列表是“default”

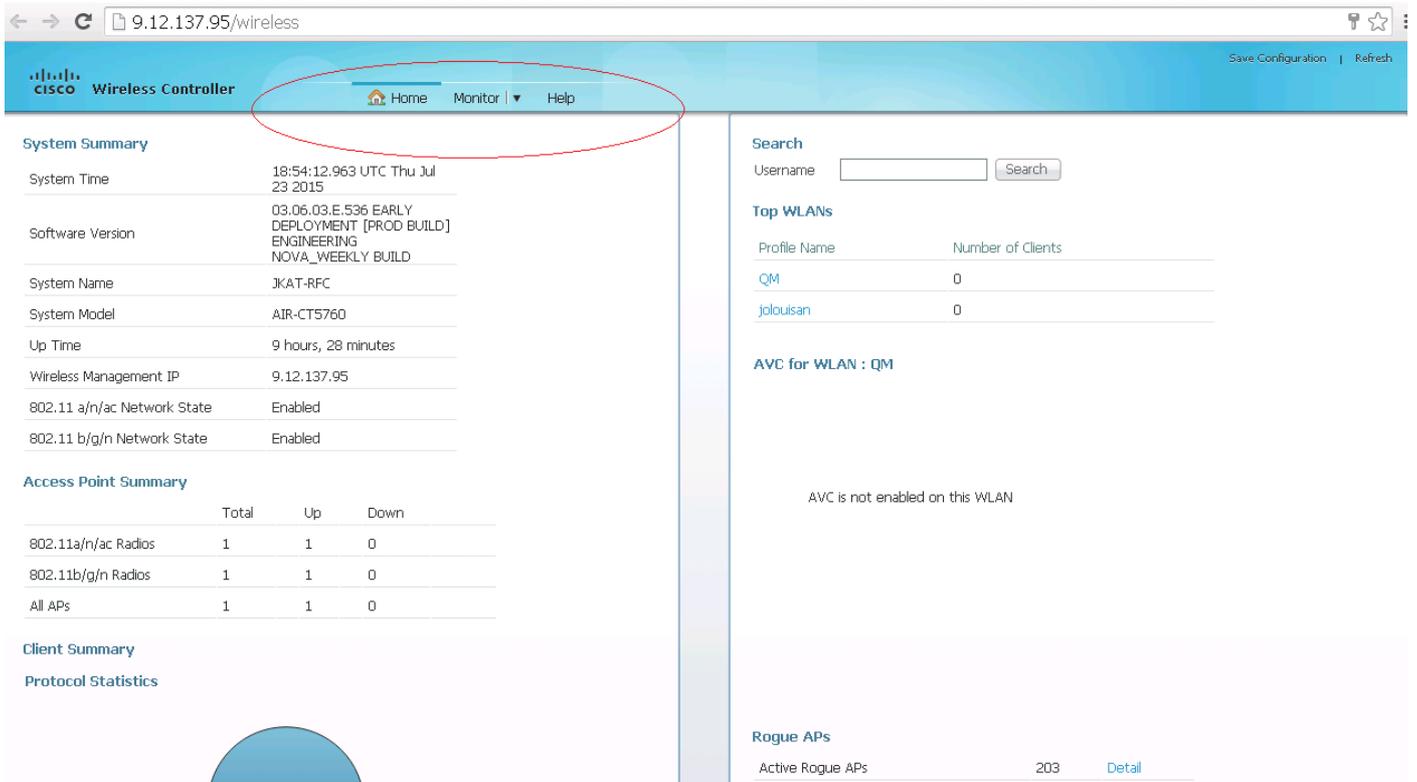
ip http authentication aaa exec-auth <method-list>

**注意事项

- 请勿在“line vty”配置参数上配置任何方法列表。如果上述步骤和线路vty具有不同的配置，则线路vty配置优先。
- 所有管理配置类型 (如ssh/telnet和webui) 的数据库应相同。
- Http身份验证应明确定义方法列表。

使用两个不同的配置文件访问同一5760

以下是权限级别为1的用户的访问权限，其中授予了有限访问权限



The screenshot shows the Cisco Wireless Controller web interface. The browser address bar displays '9.12.137.95/wireless'. The interface includes a navigation menu with 'Home', 'Monitor', and 'Help' options. The main content area is divided into several sections:

- System Summary:** A table listing system details such as System Time (18:54:12.963 UTC Thu Jul 23 2015), Software Version (03.06.03.E.536 EARLY DEPLOYMENT [PROD BUILD] ENGINEERING NOVA_WEEKLY BUILD), System Name (JKAT-RFC), System Model (AIR-CTS760), Up Time (9 hours, 28 minutes), and Wireless Management IP (9.12.137.95).
- Access Point Summary:** A table showing the status of access points:

	Total	Up	Down
802.11a/n/ac Radios	1	1	0
802.11b/g/n Radios	1	1	0
All APs	1	1	0

- Client Summary:** A section for client-related information.
- Protocol Statistics:** A section for protocol-related information.
- Search:** A search bar for finding specific information.
- Top WLANs:** A table listing the top WLANs and their client counts:

Profile Name	Number of Clients
QM	0
jalousian	0

- AVC for WLAN : QM:** A section indicating that AVC is not enabled on this WLAN.
- Rogue APs:** A section showing 203 Active Rogue APs with a 'Detail' link.

以下是权限级别为15的用户的访问权限，在该权限级别上，您可以获得完全访问权限

System Summary

System Time	18:51:40.772 UTC Thu Jul 23 2015
Software Version	03.06.03.E.536 EARLY DEPLOYMENT [PROD BUILD] ENGINEERING NOVA_WEEKLY BUILD
System Name	JKAT-RFC
System Model	AIR-CTS760
Up Time	9 hours, 26 minutes
Wireless Management IP	9.12.137.95
802.11 a/n/ac Network State	Enabled
802.11 b/g/n Network State	Enabled
Software Activation	Detail

Access Point Summary

	Total	Up	Down
802.11a/n/ac Radios	1	1	0
802.11b/g/n Radios	1	1	0
All APs	1	1	0

Client Summary

Protocol Statistics

Search

Username

Top WLANs

Profile Name	Number of Clients
QM	0
jalousian	0

AVC for WLAN : QM

AVC is not enabled on this WLAN

Rogue APs

Active Rogue APs 207 [Detail](#)