Contents

Introduction

This document will explain how to create Cisco ACS Tacacs+ authentication and authorization profiles with different privilege levels and Integrate it with 5760 for access to WebUI. This feature is supported from 3.6.3 onwards (But not on 3.7.x at time of this writing).

Prerequisites

Requirements

It is assumed that the reader is familiar with Cisco ACS and Converged Access controller configuration. This document only focuses on the interaction between those 2 components in the scope of tacacs+ authorization.

Components Used

The information in this document is based on these software and hardware versions:

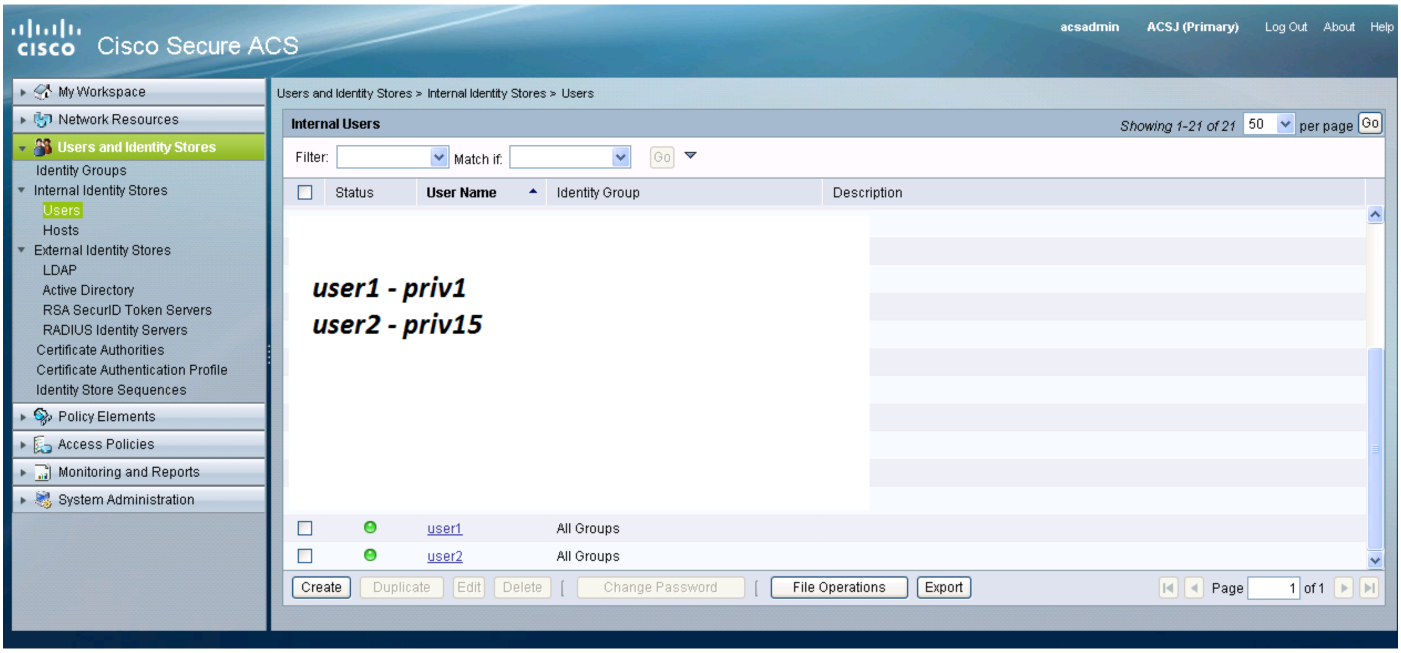
- Cisco Converged Access 5760, release 3.6.3
- Cisco Acess Control Server (ACS) 5.2

Configuration

Create a few test users in ACS

Click on "Users and Identity Stores", then select "Users".

Click "Create" and configure a few test users such as illustrated below.



user1 - priv1
user2 - priv15

☐	Status	User Name	Identity Group	Description
☐	●	user1	All Groups	
☐	●	user2	All Groups	

Setting up Policy elements and shell profiles

You need to create 2 profiles for the 2 different types of access .Privilege 15 in the cisco tacacs world means providing full access to the device without any restriction. Privilege 1 on the other hand will allow you to login and execute only a limited amount of commands .Below is a short description of the levels of access provided by cisco.

privilege level 1 = non-privileged (prompt is router>), the default level for logging in

privilege level 15 = privileged (prompt is router#), the level after going into enable mode

privilege level 0 = seldom used, but includes 5 commands: **disable**, **enable**, **exit**, **help**, and **logout**

On 5760, levels 2-14 are considered the same as level 1. They are given the same privilege as 1. **Do not configure tacacs privilege levels for certain commands on the 5760**. UI access per tabs is not supported in 5760. You can either have full access (priv15) or only access to the Monitor tab (priv1). Also, users with privilege level 0 are not alowed to login.

Creating privilege 15 level shell access profile

Using the below print screen create that profile :

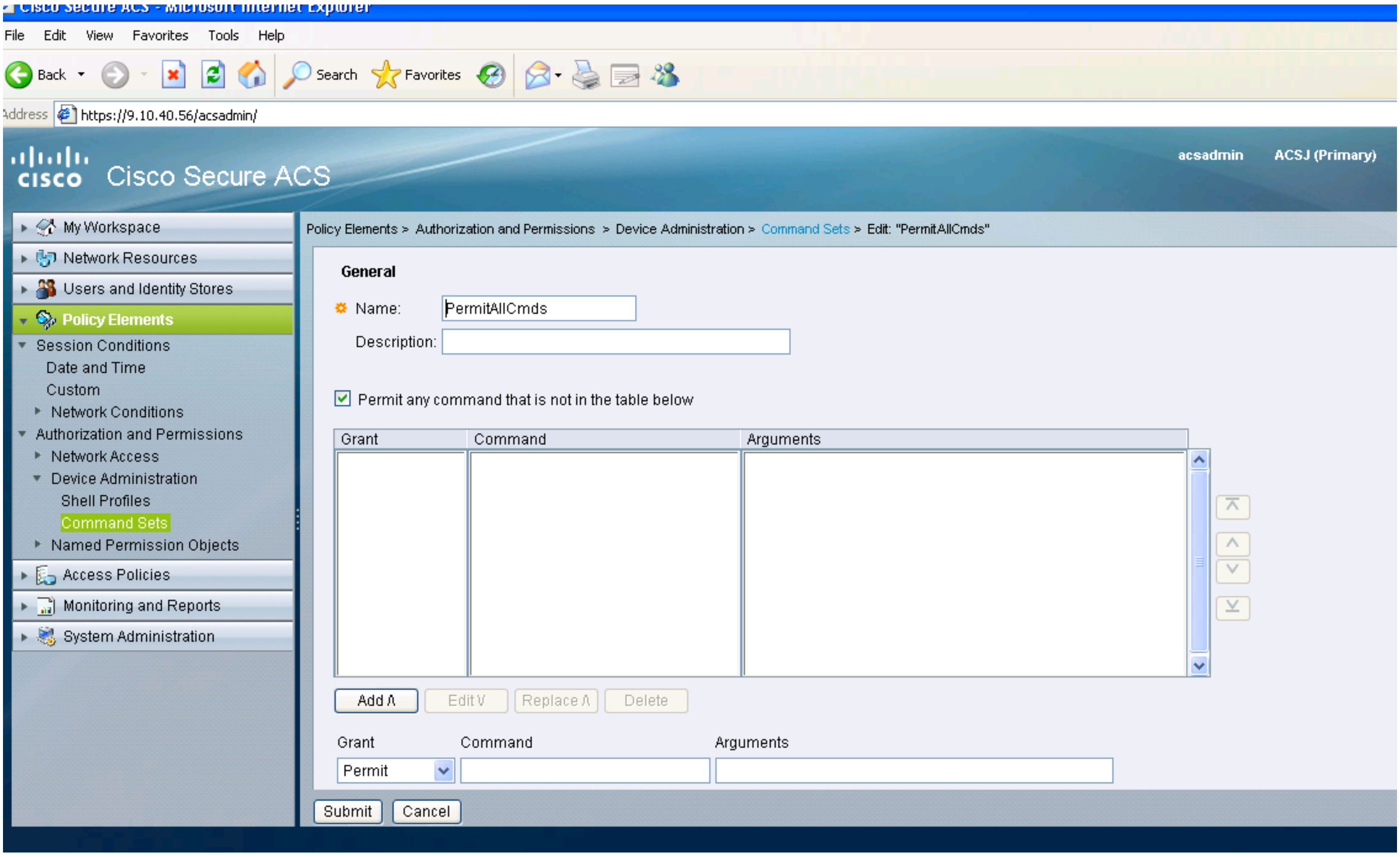
Click on "Policy Elements". Click on "Shell Profiles".

Create a new one.

Go in the "Common Tasks" tab and set the default and maximum privilege levels to 15.

Creating command sets for admin user

Command sets are sets of commands used by all the tacacs devices.They can be used to restrict the commands that a user is allowed to use if assigned that specific profile. Since on the 5760, restriction is done on the Webui code based on the privilege level passed, the command sets for both privilege level1 and 15 are the same.



Policy Elements > Authorization and Permissions > Device Administration > Command Sets > Edit: "PermitAllCmds"

General

Name: PermitAllCmds

Description:

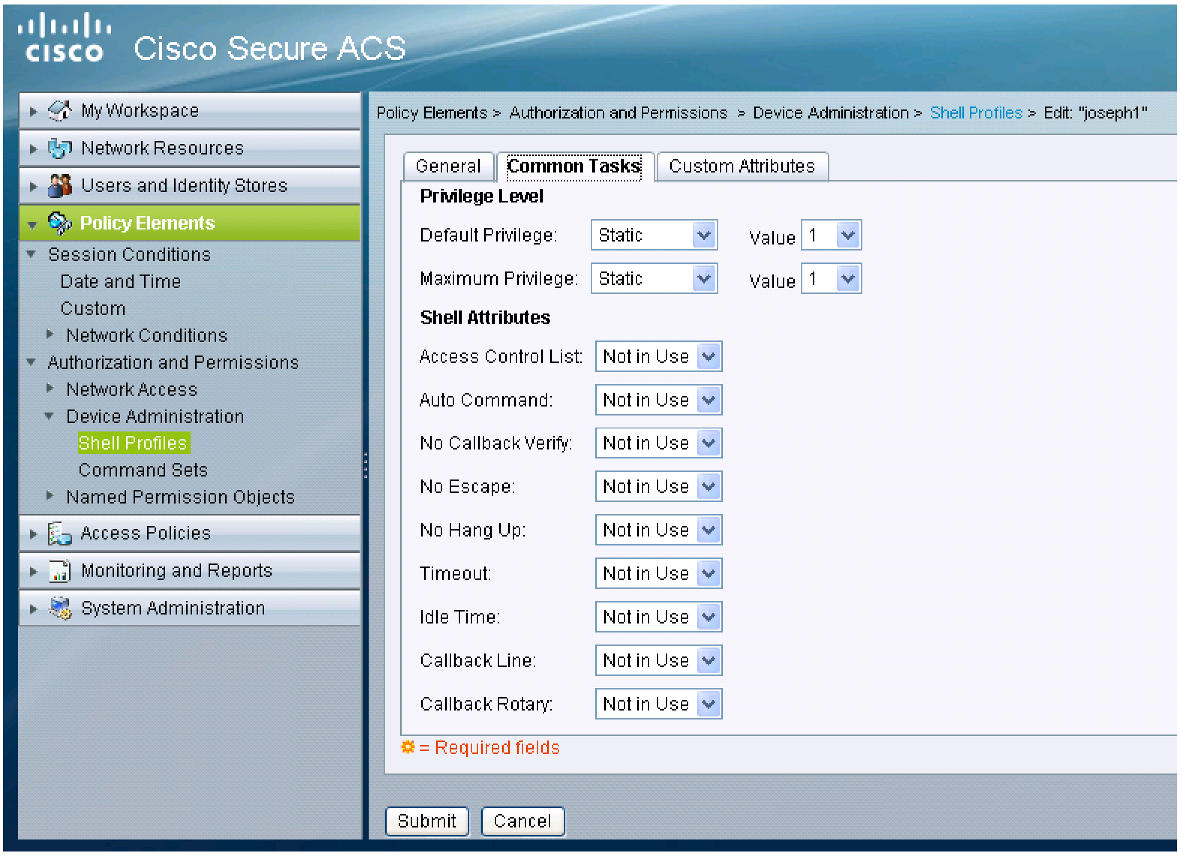
☑ Permit any command that is not in the table below

Grant	Command	Arguments

Grant: Permit
Command:
Arguments:

Creating shell profile for read only user

Create another shell profile for read-only users. This profile will differ by the fact the privilege levels are set to 1.



Policy Elements > Authorization and Permissions > Device Administration > Shell Profiles > Edit: "joseph1"

Privilege Level

Default Privilege: Static Value 1

Maximum Privilege: Static Value 1

Shell Attributes

Access Control List: Not in Use

Auto Command: Not in Use

No Callback Verify: Not in Use

No Escape: Not in Use

No Hang Up: Not in Use

Timeout: Not in Use

Idle Time: Not in Use

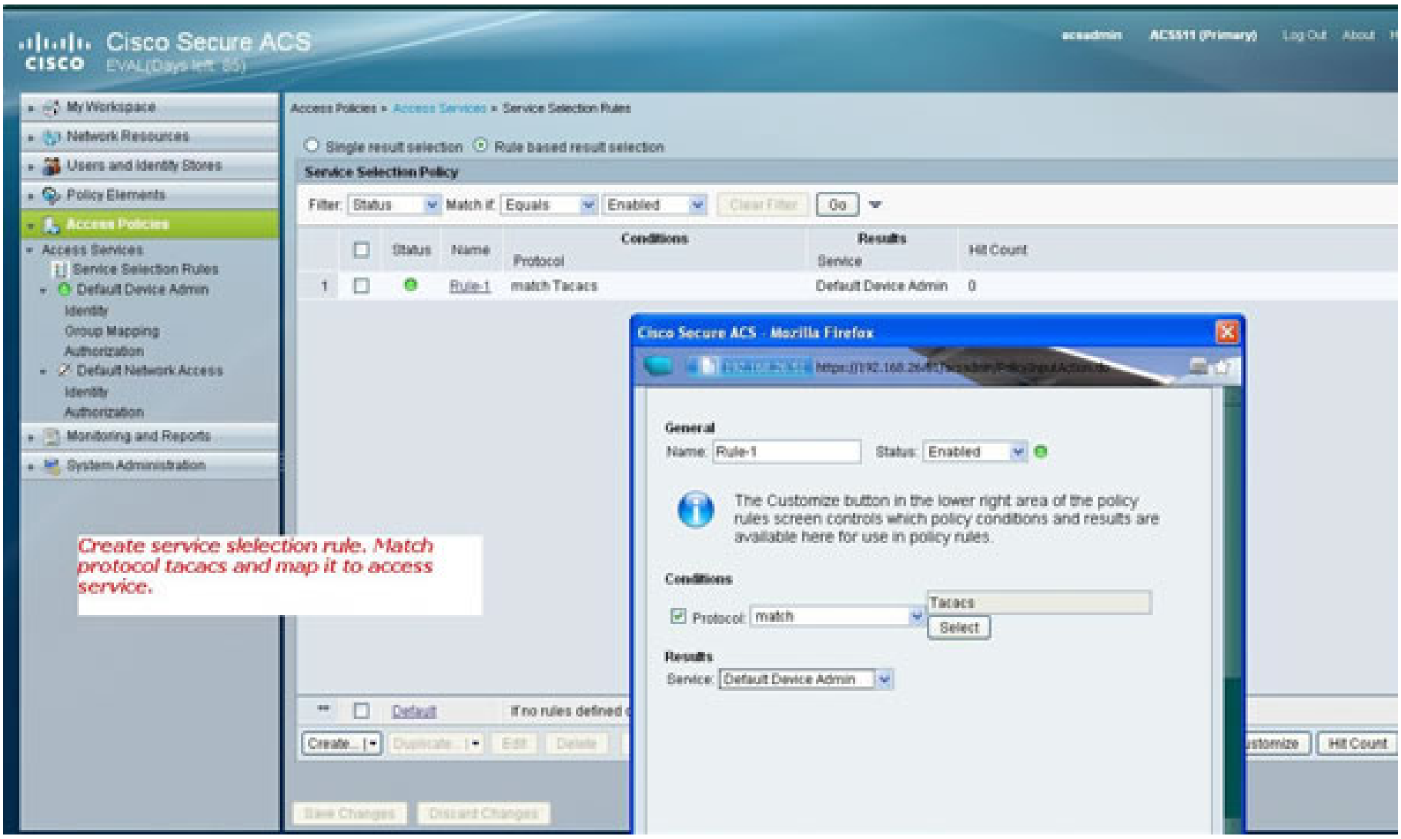
Callback Line: Not in Use

Callback Rotary: Not in Use

= Required fields

Create a service selection rule to match the tacacs protocol

Depending on your policies and configuration, make sure that you have a rule matching tacacs coming from the 5760.



○ Single result selection ● Rule based result selection

Service Selection Policy

Filter: Status Match if: Equals Enabled Clear Filter Go

	□	Status	Name	Conditions Protocol	Results Service	Hit Count
1	□	●	Rule-1	match Tacacs	Default Device Admin	0
**	□		Default	If no rules defined o		

General

Name: Rule-1 Status: Enabled ●

The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.

Conditions

☑ Protocol: match Tacacs

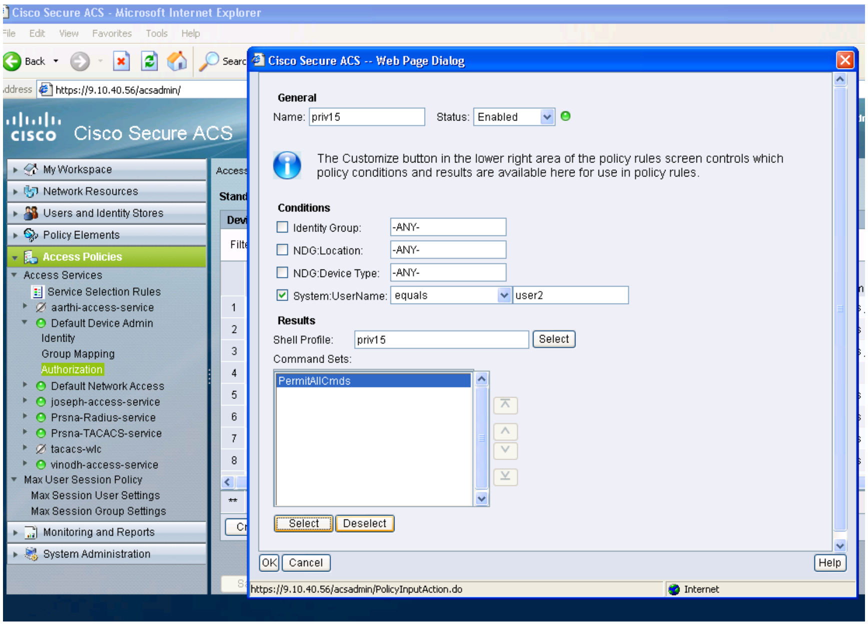
Results

Service: Default Device Admin

Create service slelection rule. Match protocol tacacs and map it to access service.

Create authorization policy for full administration access.

The Default Device Admin policy used with tacacs protocol selection is selected as part of the evaluation policy process. When using tacacs protocol to authenticate, the service policy selected is called Default Device Admin policy. That policy in itself comprises 2 sections . Identiy means who the user is and what group does he belong to (local or external) and what he is allowed to do according to the authorization profile configured. Assign the command set related to the user you are configuring.



Cisco Secure ACS -- Web Page Dialog

General

Name: priv15 Status: Enabled

The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.

Conditions

□ Identity Group: -ANY-

□ NDG:Location: -ANY-

□ NDG:Device Type: -ANY-

☑ System:UserName: equals user2

Results

Shell Profile: priv15 Select

Command Sets:

PermitAllCmds

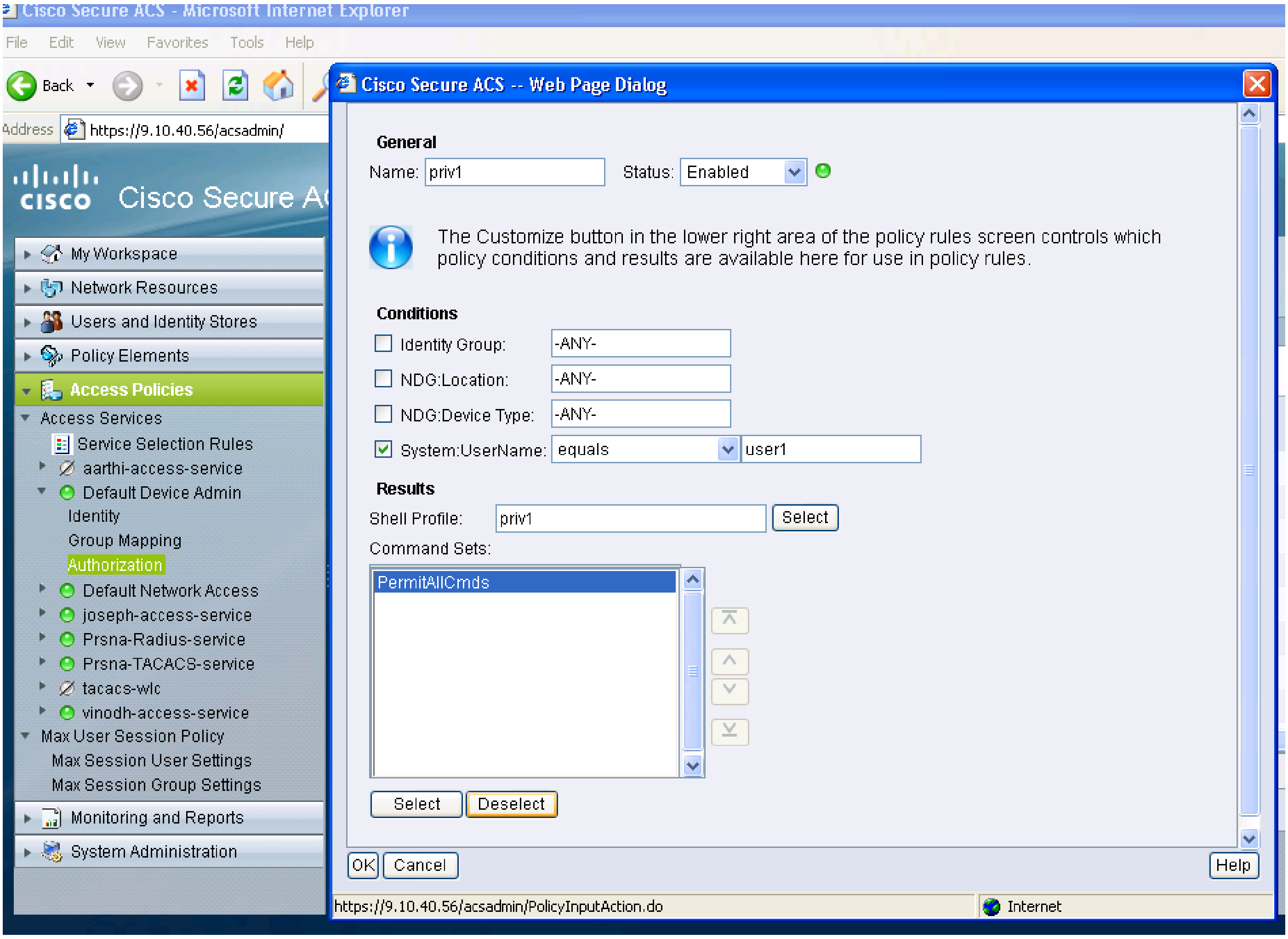
Select Deselect

OK Cancel Help

https://9.10.40.56/acsadmin/PolicyInputAction.do Internet

Create authorization policy for read only administration access.

The same is done for read-only users. This examples configure the privilege level 1 shell profile for user 1 and the privilege 15 to user 2.



Cisco Secure ACS -- Web Page Dialog

General

Name: priv1 Status: Enabled

The Customize button in the lower right area of the policy rules screen controls which policy conditions and results are available here for use in policy rules.

Conditions

□ Identity Group: -ANY-

□ NDG:Location: -ANY-

□ NDG:Device Type: -ANY-

☑ System:UserName: equals user1

Results

Shell Profile: priv1 Select

Command Sets:

PermitAllCmds

Select Deselect

OK Cancel Help

https://9.10.40.56/acsadmin/PolicyInputAction.do Internet

Configuring the 5760 for tacacs

1. Radius/Tacacs server needs to be configured.

```
tacacs server tac_acct

 address ipv4 9.1.0.100

 key cisco
```

1. Configure the server group

```
 aaa group server tacacs+ gtac

 server name tac_acct
```

There are no pre-requisite until the above step.

1. configure authentication and authorization method lists

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

aaa authorization exec <method-list> group srv-grp>
```

aaa authorization exec default group <srv-grp>   ----à workaround to get tacacs on http.

The above 3 commands and all other authentication and authorization parameters should be using the same database, either radius/tacacs or local

For example, if command authorization needs to enabled, it also needs to be pointing to the same database.

For Ex:

aaa authorisation commands 15 <method-list> group <srv-grp>   ——> the server group pointing to the database (tacacs/radius or local) should be the same.

1. configure http to use the above method lists

ip http authentication aaa login-auth <method-list>   ———> the method list needs to specified explicitly here, even if the method list is "default"

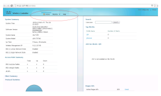
```
ip http authentication aaa exec-auth <method-list>
```

** Points to Note

- Do not configure any method-lists on the "line vty" config parameters. If the above steps and the line vty have different configs, then line vty configs would take precedence.
- The database should be the same across all management configuration types like ssh/telnet and webui.
- Http authentication should have the method list defined explicitly.

Accessing the same 5760 with the 2 different profiles

The below is a access from a privilege level 1 user where limited access is given



The below is a access from a privilege level 15 user where you are given full access

Wireless Controller
Home
Monitor
Configuration
Administration
Help
System Summary
System Time
Software Version
System Name
System Model
Up Time
Wireless Management IP
Access Point Summary
Total
Up
Down
Search
Top WLANs
Profile Name
Number of Clients
Rogue APs
Active Rogue APs
Detail