

# o nível de privilégio de 5760 interfaces da WEB baseou o exemplo de configuração do controle de acesso com Access Control Server de Cisco (o ACS)

## Índice

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configuração](#)

[Crie alguns usuários de teste no ACS](#)

[Estabelecendo elementos da política e perfis do shell](#)

[Criando o perfil nivelado do acesso do shell do privilégio 15](#)

[Criando conjuntos de comandos para o usuário admin](#)

[Criando o perfil do shell para o usuário do read only](#)

[Crie uma regra de seleção do serviço combinar o protocolo dos tacacs](#)

[Crie a política da autorização para o acesso completo da administração.](#)

[Crie a política da autorização para o acesso da administração do read only.](#)

[Configurando os 5760 para tacacs](#)

[Alcançando os mesmos 5760 com os 2 perfis diferentes](#)

[Cisco relacionado apoia discussões da comunidade](#)

## Introdução

Este documento explicará como criar perfis da autenticação TACACS+ e da autorização de Cisco ACS com os níveis de privilégio diferentes e integrá-los com os 5760 para o acesso ao WebUI. Esta característica é apoiada de 3.6.3 avante (mas não em 3.7.x na época desta escrita).

## Pré-requisitos

### Requisitos

Supõe-se que o leitor é familiar com Cisco ACS e configuração de controle convergida do acesso. Este documento centra-se somente sobre a interação entre aqueles 2 componentes no âmbito da autorização TACACS+.

### [Componentes Utilizados](#)

As informações neste documento são baseadas nestas versões de software e hardware:

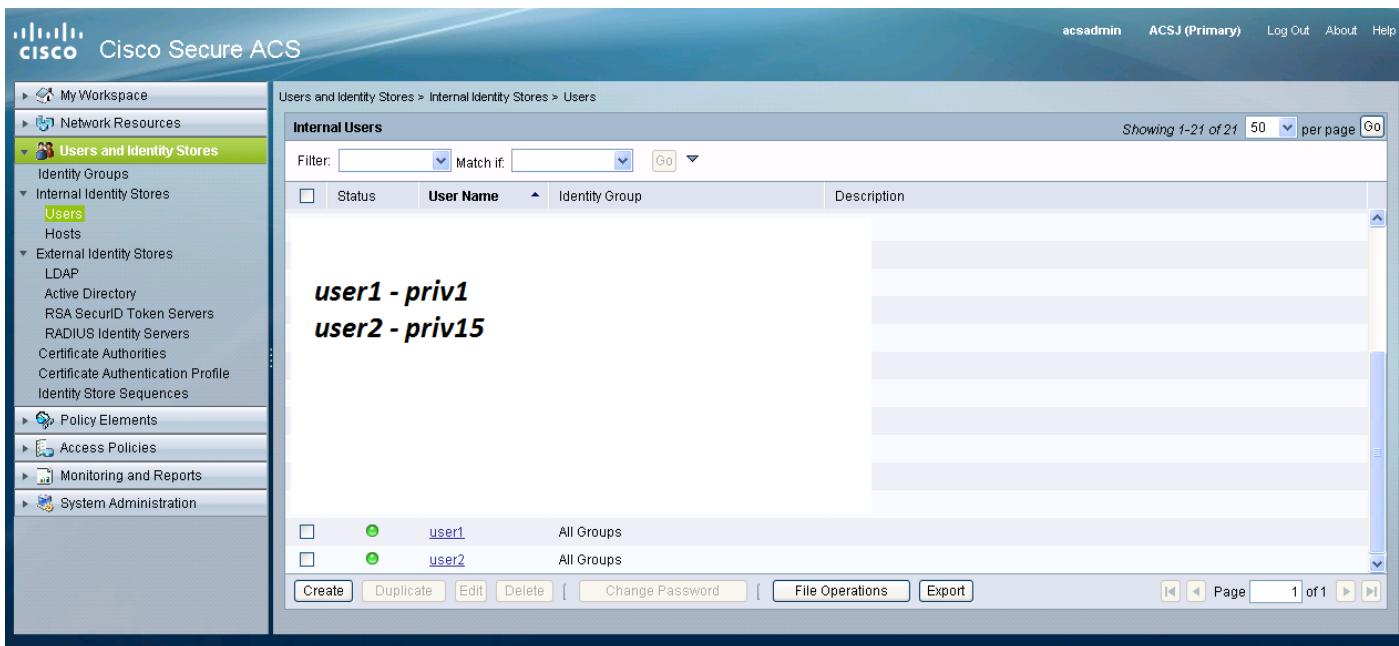
- Cisco convergiu o acesso 5760, a liberação 3.6.3
- Server do controle de Cisco Acess (ACS) 5.2

## Configuração

### Crie alguns usuários de teste no ACS

Clique sobre “usuários e a identidade armazena”, a seguir seleciona “usuários”.

Clique “criar” e configuram alguns usuários de teste tais como ilustrado abaixo.



### Estabelecendo elementos da política e perfis do shell

Você precisa de criar 2 perfis para os 2 tipos diferentes de acesso. O privilégio 15 no mundo dos tacacs de Cisco significa o fornecimento do acesso direto ao dispositivo sem nenhuma limitação. Privilegie 1 por outro lado permitirá que você entre e execute somente uma quantidade limitada de comandos. Está abaixo uma descrição breve dos níveis do acesso fornecidos por Cisco.

nível de privilégio 1 = NON-privilegiado (a alerta é Roteador>), o nível padrão para entrar

nível de privilégio 15 = privilegiado (o prompt é número de roteador), o nível depois que se entra no modo de ativação

o nível de privilégio 0 = usado raramente, mas inclui os comandos 5: **o desabilitação, permite, retira, ajuda, e saída**

Em 5760, os níveis 2-14 são considerados o mesmos que o nível 1. São dados o mesmo privilégio que 1. **Não configurar tacacs que os níveis de privilégio comandam com certeza nos 5760.** O acesso UI por abas não é apoiado em 5760. Você pode ter o acesso direto (priv15) ou somente o acesso à aba do monitor (priv1). Também, os usuários com nível de privilégio 0 não allowed para entrar.

### Criando o perfil nivelado do acesso do shell do privilégio 15

Usando a tela de impressão abaixo crie esse perfil:

Clique sobre da “elementos política”. Clique sobre o “shell perfila”.

Crie um novo.

Vá “nas tarefas comuns” aba e ajuste os níveis de privilégio do padrão e do máximo a 15.



## Criando conjuntos de comandos para o usuário admin

Os conjuntos de comandos são conjuntos de comandos usados por todos os dispositivos dos tacacs. Podem ser usados para restringir os comandos que é permitido a um usuário usar se atribuído esse perfil específico. Desde que nos 5760, a limitação é feita no código de Webui baseado no nível de privilégio passado, os conjuntos de comandos para ambos o privilégio level1 e 15 são os mesmos.

Cisco Secure ACS - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites

Address <https://9.10.40.56/acsadmin/>

acesadmin ACSJ (Primary)

**Cisco Secure ACS**

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
-------	---------	-----------

Add A Edit V Replace A Delete

Grant Command Arguments

Permit

Submit Cancel

## Criando o perfil do shell para o usuário do read only

Crie um outro perfil do shell para usuários de leitura apenas. Este perfil diferirá pelo fato que os níveis de privilégio são ajustados a 1.

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

General **Common Tasks** Custom Attributes

**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

Submit Cancel

## Crie uma regra de seleção do serviço combinar o protocolo dos tacacs

Segundo suas políticas e configuração, certifique-se de que você tem os tacacs de harmonização de uma regra que vêm dos 5760.

The screenshot shows the Cisco Secure ACS web interface. The main window displays the 'Service Selection Policy' configuration page. The 'Rule based result selection' radio button is selected. A table lists the policy rules:

	Status	Name	Protocol	Conditions	Results	Hit Count
1	<input checked="" type="checkbox"/>	Rule-1	match Tacacs		Default Device Admin	0

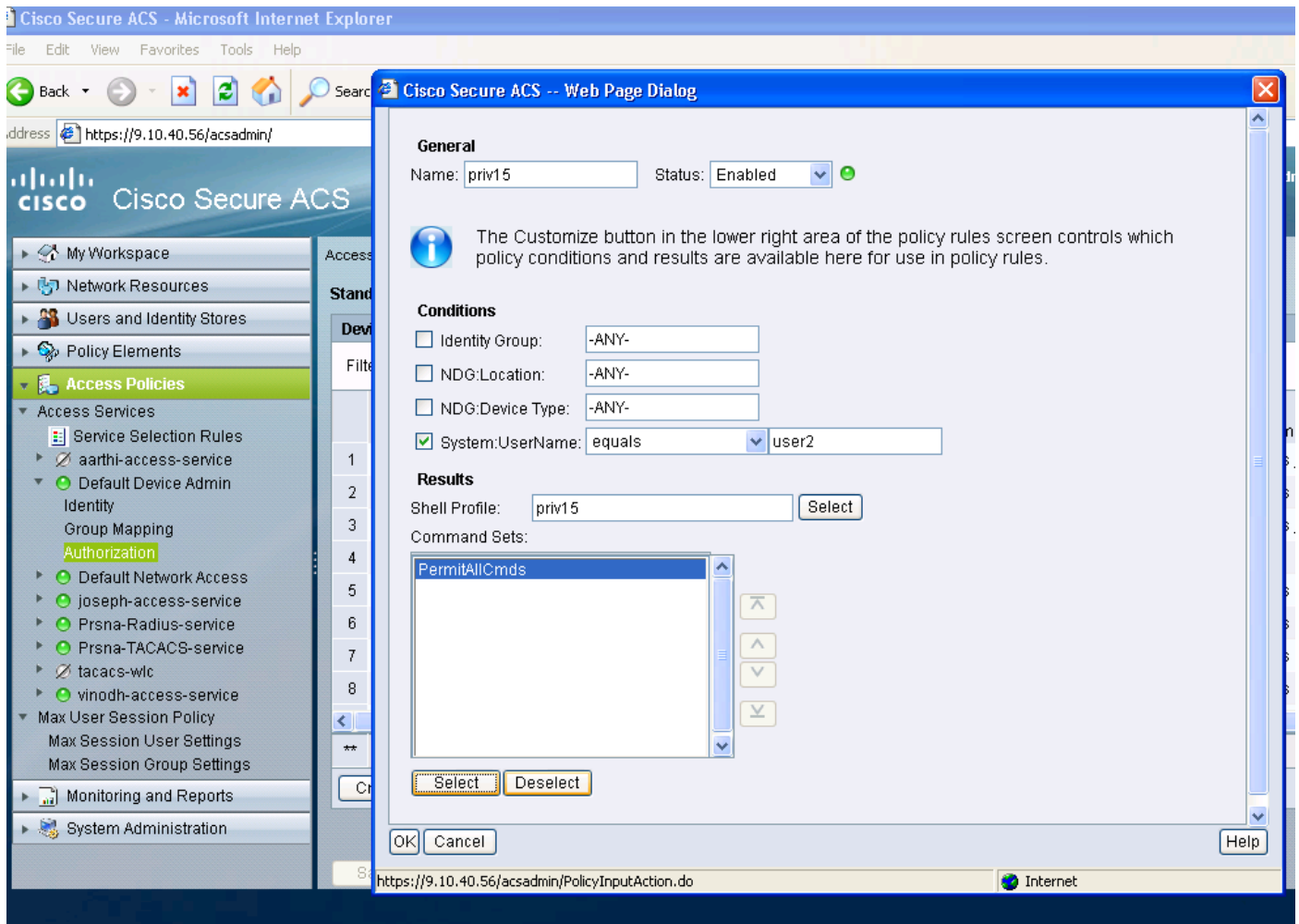
An inset window titled 'Cisco Secure ACS - Mozilla Firefox' shows the configuration details for 'Rule-1':

- General:** Name: Rule-1, Status: Enabled
- Conditions:** Protocol: match, Tacacs
- Results:** Service: Default Device Admin

A red text box on the left side of the screenshot contains the instruction: *Create service selection rule. Match protocol tacacs and map it to access service.*

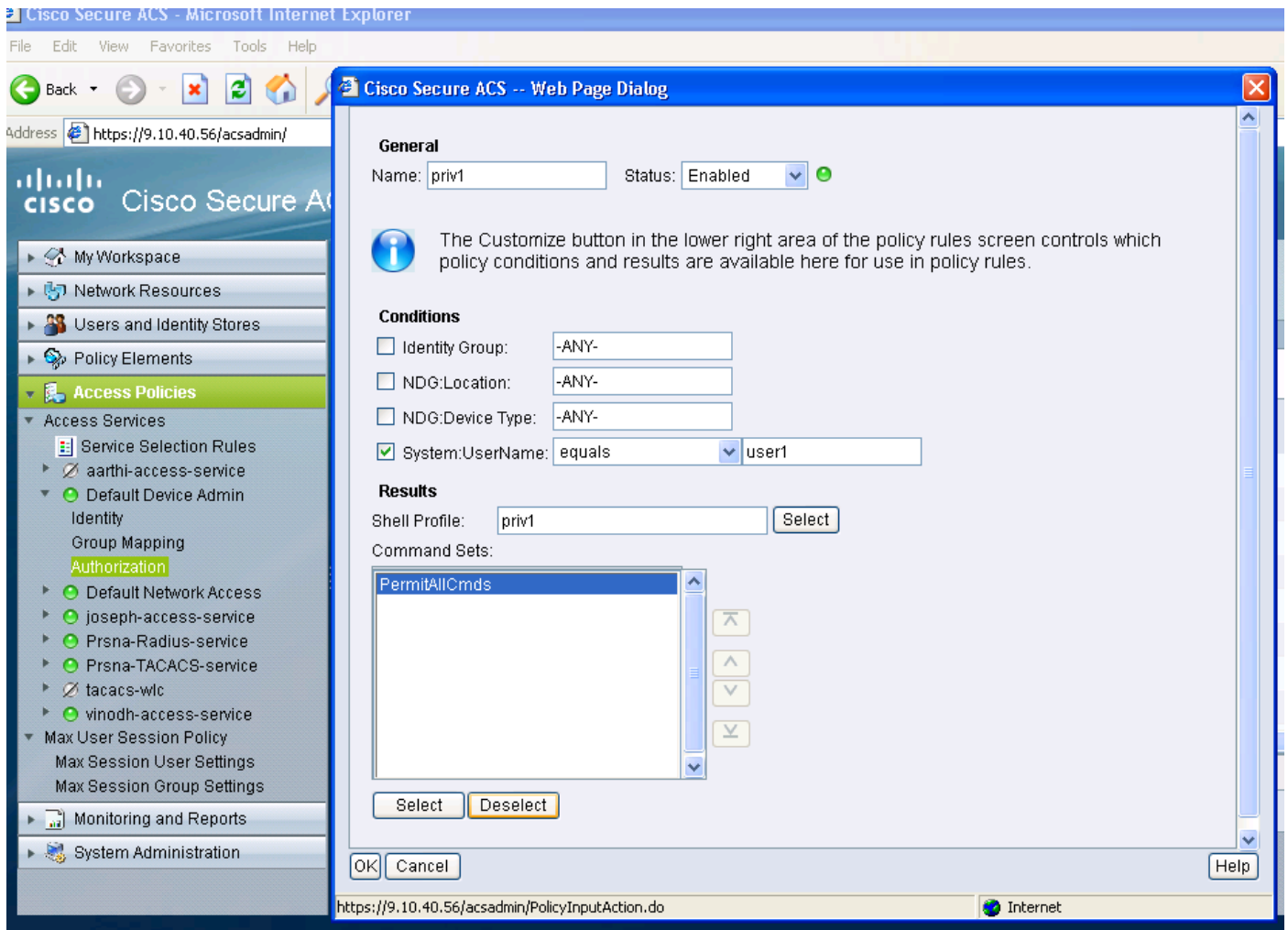
## Crie a política da autorização para o acesso completo da administração.

A política Admin do dispositivo do padrão usada com seleção de protocolo dos tacacs é selecionada como parte do processo da política da avaliação. Ao usar o protocolo dos tacacs para autenticar, a política de serviços selecionada é chamada política Admin do dispositivo do padrão. Que a política compreende em si mesmo 2 seções. Identity significa quem o usuário é e que grupo pertence (local ou externo) e o que é permitido fazer de acordo com o perfil da autorização configurado. Atribua o comando set relativo ao usuário que você está configurando.



**Crie a política da autorização para o acesso da administração do read only.**

O mesmo é feito para usuários de leitura apenas. Este os exemplos configuram o perfil do shell do nível de privilégio 1 para o usuário1 e o privilégio 15 ao usuário 2.



## Configurando os 5760 para tacacs

1. O raio/servidor de TACACS precisa de ser configurado.  
tac\_acct do servidor de TACACS

IPv4 9.1.0.100 do endereço

Cisco chave

2. Configurar o grupo de servidor  
gtac do server tacacs+ do grupo aaa

tac\_acct do nome do servidor

Não há nenhuma condição prévia até a etapa acima.

3. configurar listas de método da authentication e autorização  
<srv-grp> do grupo do <method-list> da autentificação de login aaa

srv-grp> do grupo do <method-list> do executivo da autorização aaa

<srv-grp> do grupo padrão do executivo da autorização aaa ----ação alternativa do à para obter tacacs no HTTP.



Os comandos 3 acima e todos parâmetros restantes da authentication e autorização devem usar o mesmo base de dados, raio/tacacs ou local

Por exemplo, se o comando authorization precisa permitido, igualmente precisa de apontar ao mesmo base de dados.

Para ex:

a autorização aaa comanda o <srv-grp> do grupo de 15 <method-list> — — > o grupo de servidor que aponta ao base de dados (tacacs/raio ou local) deve ser a mesma.

4. configurar o HTTP para usar as listas de método acima  
o <method-list> do início de uma sessão-AUTH aaa da autenticação do HTTP de IP — — — > a lista de método precisa especificado explicitamente aqui, mesmo se a lista de método é o “padrão”

<method-list> do EXEC-AUTH aaa da autenticação do HTTP de IP

\*\* Pontos a notar

- Não configurar nenhuma listas de método na “linha” parâmetros de configuração vty. Se as etapas acima e a linha vty têm configurações diferentes, a seguir a linha configurações vty tomaria a precedência.
- O base de dados deve ser o mesmo através de todos os tipos da configuração de gerenciamento como o ssh/telnet e o webui.
- A autenticação HTTP deve ter a lista de método definida explicitamente.

## Alcançando os mesmos 5760 com os 2 perfis diferentes

O abaixo é um acesso de um usuário do nível de privilégio 1 onde o acesso limitado seja dado

System Summary

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-CT5760
Up Time	9 hours, 28 minutes
Wireless Management IP	9.12.137.95
802.11 a/n/ac Network State	Enabled
802.11 b/g/n Network State	Enabled

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  Search

Top WLANs

Profile Name	Number of Clients
QM	0
jolouisan	0

AVC for WLAN : QM

AVC is not enabled on this WLAN

Rogue APs

Active Rogue APs 203 Detail

O abaixo é um acesso de um usuário do nível de privilégio 15 onde você seja dado o acesso direto

The screenshot shows the Cisco Wireless Controller web interface. The browser address bar displays `9.12.137.95/wireless`. The navigation menu includes **Home**, **Monitor**, **Configuration**, **Administration**, and **Help**. The main content area is divided into two columns.

**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	<a href="#">Detail</a>

**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
jolouisan	0

**AVC for WLAN : QM**

AVC is not enabled on this WLAN

**Rogue APs**

Active Rogue APs	207	<a href="#">Detail</a>
------------------	-----	------------------------