

FORMAÇÃO EM CIBERSEGURANÇA

CISCO ISE - AAA
(COM RADIUS E TACACS)

CIBERSEGURANCA.CISCO.COM.BR

JANEIRO/2025

DISCLAIMER

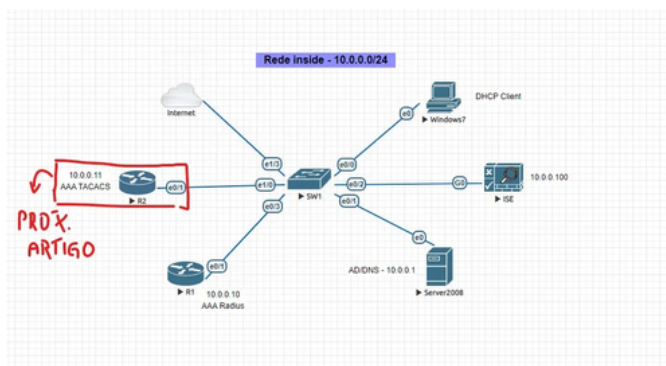
Esse material não tem qualquer relação oficial com a empresa CISCO. Ele foi criado por um profissional que trabalha há 20 anos com os equipamentos e soluções do fabricante.

A configuração mostrada não é uma recomendação. O autor não se responsabiliza por má utilização do material, que tem objetivo exclusivamente educativo (use-o para testar e aprender a ferramenta).

Esse ebook foi constituído a partir de artigos publicados de 2019 a 2021 no blog da TechRebels no medium.com pelo mesmo autor.

A versão utilizada do Cisco ISE na época era a 2.1, mas o conceito, telas e configuração continuam válidas para as versões atuais 3.x.

RADIUS



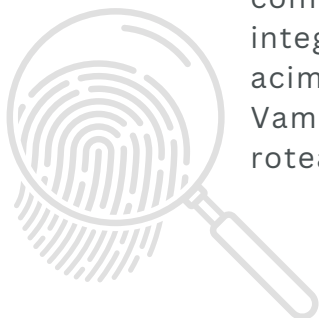
Vamos falar sobre um dos meus assuntos preferidos hoje: **AAA (Authentication, Authorization e Accounting)!**

Nosso objetivo é logar em um router via SSH, com um usuário do AD autenticando no ISE e obter privilégio 15 automaticamente.

Relembrando:

O ebook anterior mostra o processo de configurar o NAD (Router, Switch, etc.) no ISE e como fazer a integração entre o AD e o ISE.

Bom, nesse momento, temos nosso router configurado (servidor Radius) e o AD integrado ao ISE. Repare na topologia acima. Estamos configurando o R1. Vamos aplicar as configurações de AAA no roteador:



```
> aaa authentication login SEMAUTENTIC none
aaa authentication login ISE group ISE
aaa authorization exec ISE group ISE
```

O primeiro comando, cria um grupo de autenticação “sem autenticação”. SEMAUTENTIC é o nome que eu dei e associei a um método ‘none’. Vamos configurar esse método na line con do router, para não ficarmos presos “pra fora” do roteador caso algo dê errado.

O segundo comando cria um grupo de autenticação “ISE” e associa ao grupo “ISE”, que é o nome do servidor que eu criei no artigo com o link acima. Os nomes iguais foram preferência minha, ok? Eles não precisam ser iguais.

Agora que já sabemos “quem” é a pessoa que vai logar no router, veremos “o que” ela pode fazer. Essa parte é bem simples e menos granular do que usando o protocolo TACACS.



Nós já definimos os métodos de autenticação e autorização e apontamos eles para o grupo de servidores Radius chamado ISE. Agora, vamos linkar esses métodos no acesso aos eqtos.

```
> line con 0
  logging synchronous
  login authentication SEMAUTENTIC

line vty 0 4
  authorization exec ISE
  login authentication ISE
  transport input ssh
```

Repare na line vty que estou usando SSH. Portanto, não esqueça de gerar a chave rsa com o comando:

```
> crypto key generate rsa label MINHA-
CHAVE modulus 2048
```

Finalizamos a parte do router.

Vamos fazer um teste de autenticação agora sem nenhuma configuração adicional no ISE. Veja o resultado:




The screenshot shows the Cisco ISE GUI with a terminal window titled '3D0010 - PuTTY'. The terminal output shows a failed login attempt:

```





login as: fernando
Keyboard-interactive authentication prompt from server:
Password:
End of keyboard-interactive prompt from server
Access denied
Keyboard-interactive authentication prompt from server:
Password:

```

Olhando os logs do ISE:

 **Obs:** Pessoal, não vou ficar repetindo os menus ou como encontrar a informação na GUI do ISE. Está tudo explicado nos outros ebooks, ok?

The screenshot shows the 'Live Sessions' tab in the Cisco ISE GUI. The table below displays the details of active sessions:

Time	Status	Details	Repeat	Identity	Endpoint ID	Endpoint P...
Dec 21, 2020 07:04:22.794 PM				USER@NAME	Endpoint ID	Endpoint Prof
Dec 21, 2020 07:04:17.766 PM				USER@NAME		



Identity Services Engine

Overview


Event	5405 RADIUS Request dropped
Username	USERNAME ?
Endpoint Id	
Endpoint Profile	
Authentication Policy	Default >> Default
Authorization Policy	Default
Authorization Result	

Authentication Details

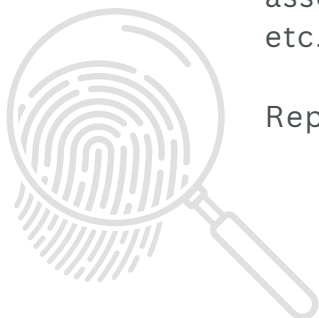
Source Timestamp	2020-12-21 19:04:22.794
Received Timestamp	2020-12-21 19:04:22.794
Policy Server	ise
Event	5405 RADIUS Request dropped
Failure Reason	24412: User not found in Active Directory

O padrão do ISE, é procurar em todas as bases de usuários configuradas. Portanto, ele procurou no AD, mas não encontrou meu usuário ‘fernando’.

Vou então criá-lo agora no AD (feito!) e também dentro do ISE, mas apontando a senha para o ‘AD’. Isso me permitirá adicionar esse user dentro de um grupo do próprio ISE.

 **Obs:** Tem inúmeras formas de fazer essas associações, seja por grupo no AD, no ISE, etc...

Reparem no “Password Type”:



Identity Services Engine

System > Identity Management > Network Resources > Device Portal Management > profind Services > Feed Service > Threat Centric NAC

Identities > Groups > External Identity Sources > Identity Source Sequences > Settings

Users

Latest Manual Network Scan Results

Network Access User

Name: fernando

Status: Enabled

Email:

Passwords

Password Type: **AD**

Password: Re-Enter Password:

* Login Password: ?

Enable Password: ?

User Information

First Name:

Last Name:

Fazemos outro teste de autenticação agora e vejam o resultado:

```

10.0.0.10 - PuTTY
login as: fernando
Keyboard-interactive authentication prompts from server:
| Password:
End of keyboard-interactive prompts from server
R1>

```

Identity Services Engine

Overview

Event	5200 Authentication succeeded
Username	fernando
Endpoint Id	
Endpoint Profile	
Authentication Policy	Default >> Default
Authorization Policy	Default >> Basic_Authenticated_Access
Authorization Result	PermitAccess

Authentication Details

Source Timestamp	2020-12-21 19:08:31.004
Received Timestamp	2020-12-21 19:08:31.004
Policy Server	ise
Event	5200 Authentication succeeded

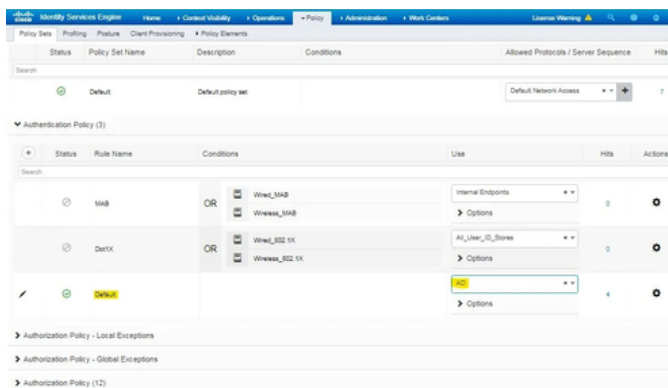


O usuário se autenticou com sucesso e bateu nas políticas padrão de autenticação e autorização.



Vamos agora fechar um pouco nossa política: Na autenticação, permitiremos apenas usuários do AD e, caso eles sejam membros do grupo AD-Admins (que criaremos no ISE), irão se logar e obter **privilégio 15 automaticamente (sem usar senha de enable)**.

Especificando o AD como única base de usuários para autenticação:



Criando grupo AD-Admins no ISE e adicionando o usuário fernando.



The screenshot shows the Cisco ISE configuration interface. The breadcrumb navigation at the top reads: System > Identity Management > Network Resources > Device Portal Management > pr0nd Services > Feed Service > Threat > Identities > Groups > External Identity Sources > Identity Source Sequences > Settings. The main content area is titled "Identity Group" and shows a form for configuring a group named "AD-Admin". The "Member Users" section contains a table with columns for "Status", "Email", and "Username". One user is listed with the status "Enabled", email "jremond", and username "jremond".

Vamos configurar um Authorization Profile e, usando o atributo **av-pair**, setar o privilégio (*priv-lvl*) 15:

The screenshot shows the Cisco ISE configuration interface for an Authorization Profile. The breadcrumb navigation at the top reads: Identity Services Engine > Home > Context Visibility > Operations > Policy > Administration > Work Center > Policy Sets > Profiling > Posture > Client Provisioning > Policy Elements. The main content area is titled "Results" and shows a list of "Common Tasks" and "Advanced Attributes Settings". Under "Advanced Attributes Settings", the attribute "Cisco:cisco-av-pair" is set to "priv-lvl=15". Under "Attributes Details", the "Access Type" is set to "ACCESS_ACCEPT" and the "Cisco:cisco-av-pair" attribute is set to "priv-lvl=15".



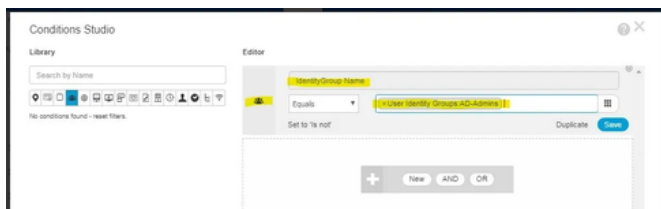
Na política de autorização, criamos uma nova regra e selecionamos esse profile nela:



Ah, reparem na condição *“Identity-AD-Admins”*. Essa condição fui eu que criei e ela simplesmente checa se o usuário faz parte do grupo AD-Admins que criamos acima.

Selecionando a condição *“IdentityGroup Name”*, ao clicar no box abaixo, você seleciona o grupo que você quer e pronto.

Veja como fica:



E, finalmente, tudo pronto!

Vamos testar? Reparem no privilégio que o usuário recebe ao se autenticar.



```

10.0.0.10 - PuTTY
login as: fernando
Keyboard-interactive authentication prompts from server:
| Password:
| End of keyboard-interactive prompts from server
R1#show priv
R1#show privilege
Current privilege level is 15
R1#

```

Identity Services Engine

Overview

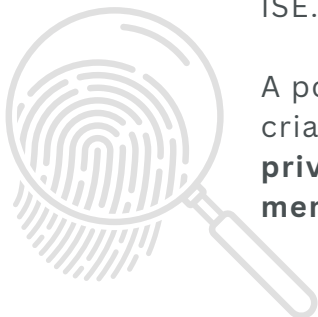
Event	5200 Authentication succeeded
Username	fernando
Endpoint Id	
Endpoint Profile	
Authentication Policy	Default >> Default
Authorization Policy	Default >> Network Admins (AD)
Authorization Result	PermitAccess

Authentication Details

Source Timestamp	2020-12-21 19:29:43.86
Received Timestamp	2020-12-21 19:29:43.86
Policy Server	ise
Event	5200 Authentication succeeded
Username	fernando
Authentication Identity Store	AD

A política de autenticação ainda é a “Default”, mas ela só puxa usuários do AD e não mais de todas as bases configuradas no ISE.

A política de autorização é que a nós criamos: **Network Admins (AD)**, e entrega **privilegio 15** automaticamente para os membros do grupo AD-Admins.



TACACS



Nosso objetivo é permitir que um usuário se logue automaticamente com privilégio 15 mas, de forma granular, permitir apenas alguns comandos específicos.

O primeiro passo é ativar o serviço no ISE. Fazemos isso nessa tela:

The screenshot shows the Cisco ISE configuration interface. The left sidebar shows a tree view with 'Deployments' and 'ise' selected. The main content area is titled 'Identity Services Engine' and shows configuration for a node. The 'Role' is 'STANDALONE' with a 'Make Primary' button. Under 'Monitoring', the role is 'PRIMARY'. Under 'Policy Service', several services are enabled: 'Enable Session Services', 'Enable Profiling Service', and 'Enable SXP Service'. The 'Use Interface' is set to 'GigabitEthernet 0'. The 'Enable Device Admin Service' is highlighted in yellow.

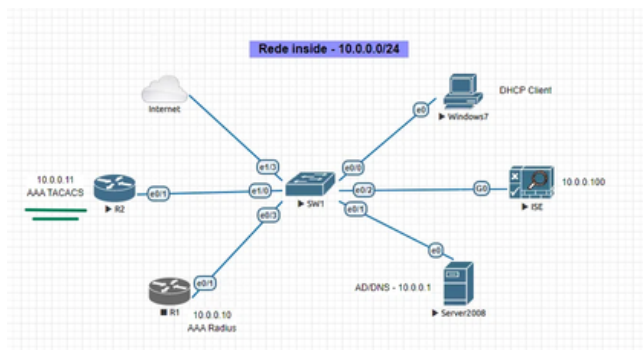
Em seguida, nesse menu, nessa visão geral dos passos necessários:



Device Administration Overview

- Prepare**
 - Authorization Roles**
Consider the roles your organization needs to manage its devices. Create Authorization Profiles and Command Sets to determine the operations admins may perform.
 - Migrating from ACS (4.2, 5.5 - 5.8 & 5.8.117)**
Use the migration tool available in the [Download Software Package](#) to import all your data and set default TACACS servers for all network devices.
 - Enable Deployment for TACACS**
To activate ISE Nodes for Device Administration, go to [Deployment Page](#).
- Define**
 - Configure Devices**
All the devices that will be controlled and audited by TACACS device administration, should have TACACS servers set.
 - Device Administrators**
All users who will perform device administration, whether internal or external, should have a common attribute or be assigned to a suitable group.
 - Policy**
Create a policy within the policy sets for your device administration service. First, set the authorization policy to select the identity roles that contain the device administrators.
Next use the authorization policy to select the Profiles and Command Sets, according to the relevant conditions, for example NODs and identity groups.
 - Settings**
Check the default settings for connections and password control suit your organization.
- Go Live & Monitor**
 - Real-time Monitoring**
View Liveing to monitor network events.
 - Auditing**
Examine reports to check access and authorization is as intended.

Primeiramente, vamos então adicionar o nosso network device (já fizemos isso nos outros ebooks):



Name	IP/Host	Profile Name	Location	Type	Device Types
R1	10.0.0.1032	Case	All Locations	All Device Types	
sw1	10.0.0.1102	Case	All Locations	All Device Types	

Pronto! Vamos criar agora o *command set* – grupo de comandos que iremos permitir o usuário dar no router. Atente-se à sintaxe, não pode haver erros! Não há checagem por parte do ISE.

The screenshot shows the 'TACACS Command Set' configuration page. The 'Commands' table is highlighted with a green box. The table has columns for 'Grant', 'Command', and 'Arguments'. The rows are:

Grant	Command	Arguments
PERMIT	router	any
PERMIT	show	ip route
PERMIT	configure	terminal
PERMIT	show	ip interface


Agora vamos criar o Profile. Repare nos menus. A única informação que vamos colocar é o privilégio 15 automático para o usuário.

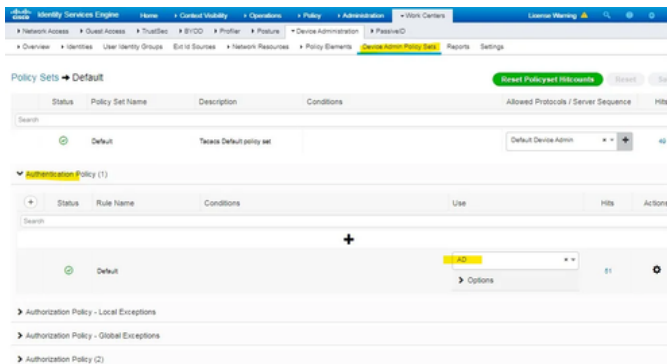
The screenshot shows the 'TACACS Profile' configuration page. The 'Common Tasks' section is highlighted. The 'Common Task Type' is set to 'Shell'. The 'Default Privilege' is set to '15' (Select 0 to 15). Other options include:

- Maximum Privilege (Select 0 to 15)
- Access Control List
- Auto Command
- No Escape (Select true or false)
- Timeout (Minutes (0-2000))
- Idle Time (Minutes (0-9999))

Feito isso, vamos editar a política de autenticação padrão para buscar o usuário apenas no AD que configuramos no artigo passado.

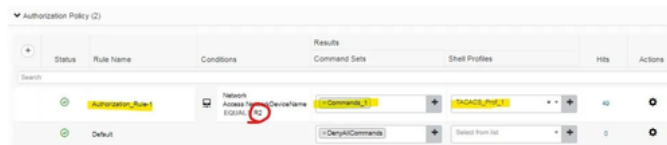


 **Obs:** Repare na estrutura de menu que se trata de outra Policy Set. É uma base de políticas diferente da utilizada pelo Radius. No entanto, elas possuem o mesmo formato.



The screenshot shows the Cisco ISE Policy Sets configuration interface. The 'Default' policy set is selected, and the 'Authorization Policy (1)' rule is expanded. The rule name is 'Default' and the condition is 'Network Access EQUAL R2'. The 'Use' column shows 'Default Device Admin'.

Na política de autorização, nós definimos o *Command Set* que criamos, o *Profile* e, na condição, seleccionei apenas o *Network Device* com o nome “R2”. Ou seja, essa condição não se aplica a nenhum outro eqto da rede, apenas a esse router em específico.



The screenshot shows the Cisco ISE Policy Sets configuration interface. The 'Authorization Policy (2)' rule is expanded. The rule name is 'Authorization_Rule1' and the condition is 'Network Access EQUAL R2'. The 'Command Sets' column shows 'DenyAllCommands'.



Testando:

Ao logar, o usuário fernando do AD, recebe direto o prompt privilegiado, mas não é possível entrar com o comando *show privilege*, já que não o permitimos no command set que criamos acima.

```

10.0.0.11 - PuTTY
login as: fernando
Keyboard-interactive authentication prompts from server:
Password:
End of keyboard-interactive prompts from server

R2#show privi
R2#show privilege
Command authorization failed.

R2#

```

Veja abaixo os comandos que permitimos e os que foram negados. Por ex: não permitimos o *router ospf*, mas permitimos o *router eigrp*.

```

10.0.0.11 - PuTTY

R2#
R2#show ip int brie
Interface                IP-Address      OK? Method Status          Protocol
Ethernet0/0              unassigned     YES unset  administratively down down
Ethernet0/1              10.0.0.11      YES manual up                up
Ethernet0/2              unassigned     YES unset  up                up
Ethernet0/3              unassigned     YES unset  administratively down down
R2#
R2#show int e0/0
Command authorization failed.

R2#show int e0/1
Command authorization failed.

R2#show ip route | i 10.
      10.0.0.0/24 is variably subnetted, 2 subnets, 2 masks
C       10.0.0.0/24 is directly connected, Ethernet0/1
L       10.0.0.11/32 is directly connected, Ethernet0/1
R2#
R2#show priv
Command authorization failed.

R2#confi_
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#router ospf 1
Command authorization failed.

R2(config)#router eigrp 1
R2(config-router)#
R2(config-router)#do show runn
Command authorization failed.

R2(config-router)#

```



Qto aos logs do TACACS, eles são consultados nesse menu:

Um exemplo de log de comando autorizado:

Um exemplo de log de comando não autorizado:



Identity Services Engine	
Overview	
Request Type	Authorization
Status	Fail
Session Key	isa207050134/00
Message Text	Failed-Attempt: Command Authorization failed
Username	terminal
Authorization Policy	Default >> Authorization_Rule-1
Shell Profile	
Matched Command Set	
Command From Device	router ospf 1
Authorization Details	
Generated Time	2020-12-22 14:20:31.796 -2:00
Logged Time	2020-12-22 13:20:31.796
Epoch Time (sec)	1606657031
ISE Node	ise
Message Text	Failed-Attempt: Command Authorization failed
Failure Reason	13025 Command failed to match a Permit rule

Por fim, mas igualmente importante a config toda do router(também já detalhada nos ebooks anteriores):



```
aaa new-model
!
!
aaa group server tacacs+ ISE_TACACS
  server name ISE_TACACS
!
aaa authentication login NOAUTH none
aaa authentication login ISE_TACACS group ISE_TACACS
aaa authorization config-commands
aaa authorization exec ISE_TACACS group ISE_TACACS
aaa authorization commands 1 ISE_TACACS group
ISE_TACACS
aaa authorization commands 15 ISE_TACACS group
ISE_TACACS
aaa accounting exec ISE_TACACS start-stop group
ISE_TACACS
aaa accounting commands 15 ISE_TACACS start-stop
group ISE_TACACS
!
interface Ethernet0/1
  ip address 10.0.0.11 255.255.255.0
!
tacacs server ISE_TACACS
  address ipv4 10.0.0.100
  key cisco123
!
line con 0
  logging synchronous
  login authentication NOAUTH
line aux 0
line vty 0 4
  authorization commands 1 ISE_TACACS
  authorization commands 15 ISE_TACACS
  authorization exec ISE_TACACS
  login authentication ISE_TACACS
  transport input ssh
```

Importante destacar 3 comandos nessa config:

```
> aaa authorization config-commands
```

“*Config-Commands*” significa que o network device precisa obter autorização para comandos dados dentro do prompt de configuração (configure terminal)

```
> aaa authorization commands 15  
ISE_TACACS group ISE_TACACS
```

O “15” significa autorização para comandos de usuários que possuem *privilege level 15*

```
> aaa accounting commands 15 ISE_TACACS  
start-stop group ISE_TACACS
```

E, finalmente, o *accounting commands 15*, que irá logar cada comando no nível de privilégio 15.



AGRADECIMENTOS

Gostaria de agradecer a todos os leitores e seguidores do blog TechRebels nesses anos todos. Foi sensacional ter tido a chance de conhecer alguns pessoalmente.

Espero que o conteúdo possa ajudar muito mais pessoas a aprender sobre essa solução que continua dominando o mercado e não para de crescer em funcionalidades e adoção!

Se você recebeu esse ebook de um amigo, dê uma olhada nos treinamentos que temos disponíveis no ciberseguranca.cisco.com.br.

Grande abraço e muito sucesso!!!



[linkedin.com/in/fmp7/](https://www.linkedin.com/in/fmp7/)

