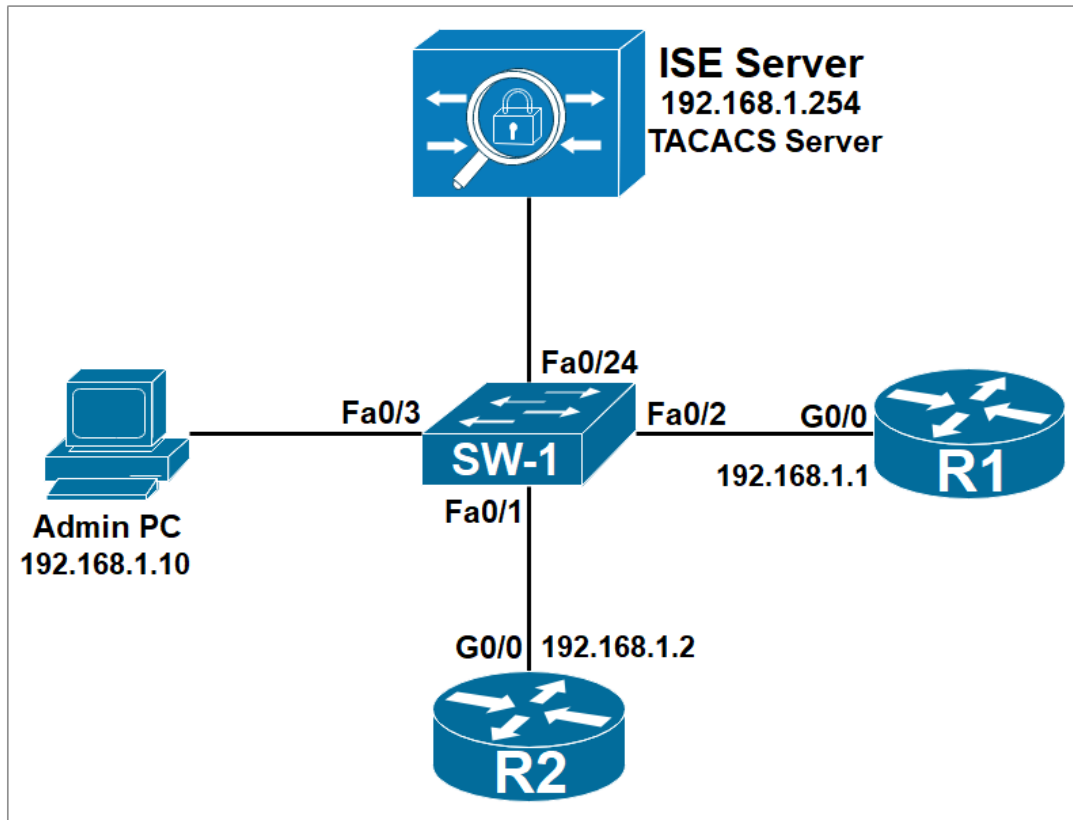
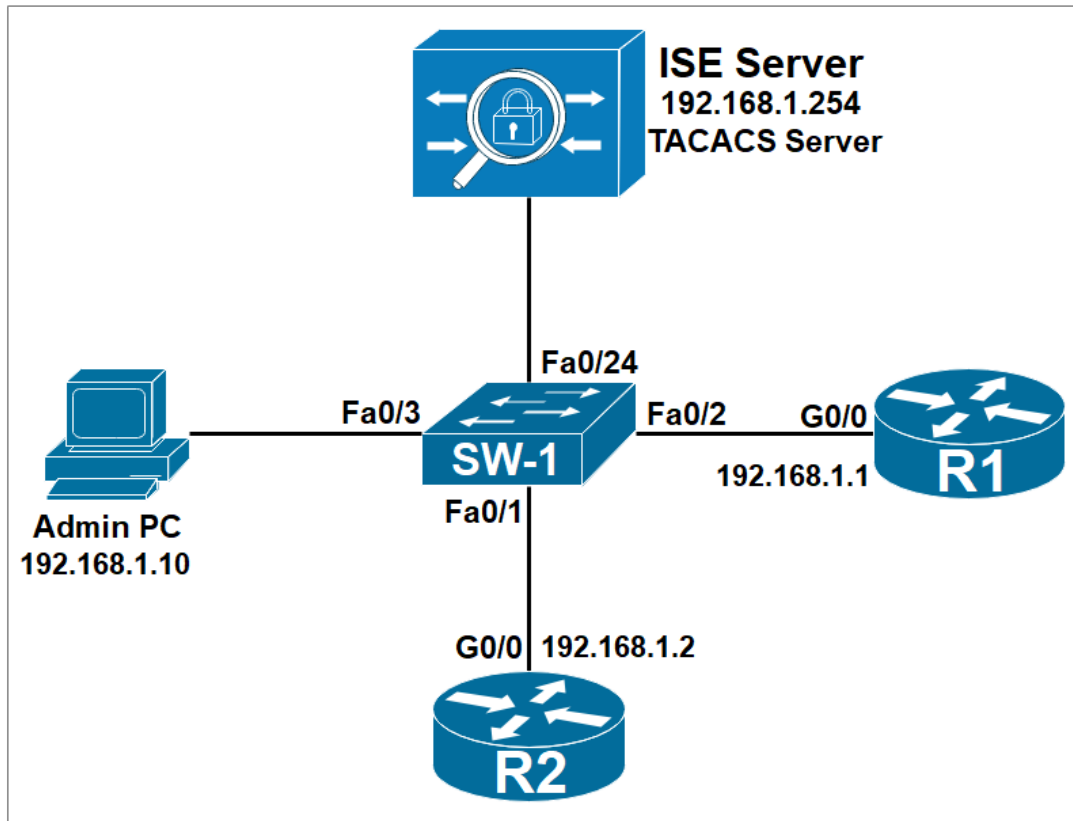


TACACS+ Protocol IOS Switch commands and Cisco ISE Demystified



Redouane MEDDANE
CCSI 35458
3 CCNP Collaboration Security and Enterprise
www.ipdemystify.com

Device Admin using TACACS Scenario 1



Activate the AAA process on the router:
Configure the TACACS service with the following commands:

```
SW-1(config)#aaa new-model
SW-1(config)#aaa authentication login default group tacacs+ local
SW-1(config)#aaa authorization config-commands
SW-1(config)#aaa authorization exec default group tacacs+ local
```

```
R1(config)#tacacs server ISE-SRV
R1(config-server-tacacs)#address ipv4 192.168.1.254
R1(config-server-tacacs)#key cisco
```

Create Network Device Group

Navigate to **Administration > Network Resources > Network Device Groups**.

Click **Add** and Type **San-Jose** as the Name.
Select **All Locations** in the **Parent Group** field.
Click **Save**.

Network Device Groups

All Groups Choose group ▾

Refresh Add Duplicate Edit Trash Show group members Import Export Flat Table Expand All Collapse All

Name	Description	No. of Network Devices
▾ All Device Types	All Device Types	--
▾ All Locations	All Locations	--
▾ ▾ Is IPSEC Device	Is this a RADIUS over IPSEC Device	--

Add Group



Name * San-Jose

Description

Parent Group * All Locations x ▾

Cancel

Save

Click **Add** and Type **New-York** as the Name.
Select **All Locations** in the **Parent Group** field.
Click **Save**.

Add Group



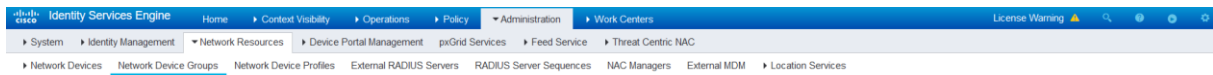
Name * New-York

Description

Parent Group * All Locations x ▾

Cancel

Save



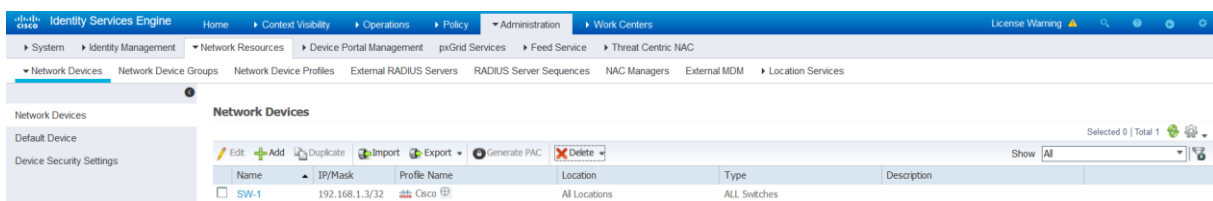
Network Device Groups

All Groups Choose group ▾

Name	Description	No. of Network Devices
▶ All Device Types	All Device Types	--
▶ All Locations	All Locations	--
▶ New-York		0
▶ San-Jose		0
▶ Is IPSEC Device	Is this a RADIUS over IPSEC Device	--

Add the routers as AAA Client in the Cisco ISE

Navigate to **Administration > Network Resources > Network Devices**. The **Network Devices** window will open.



In the right section window, click **Add**. The AAA Client window opens.

In the **Name** field, type **R1** as the name.

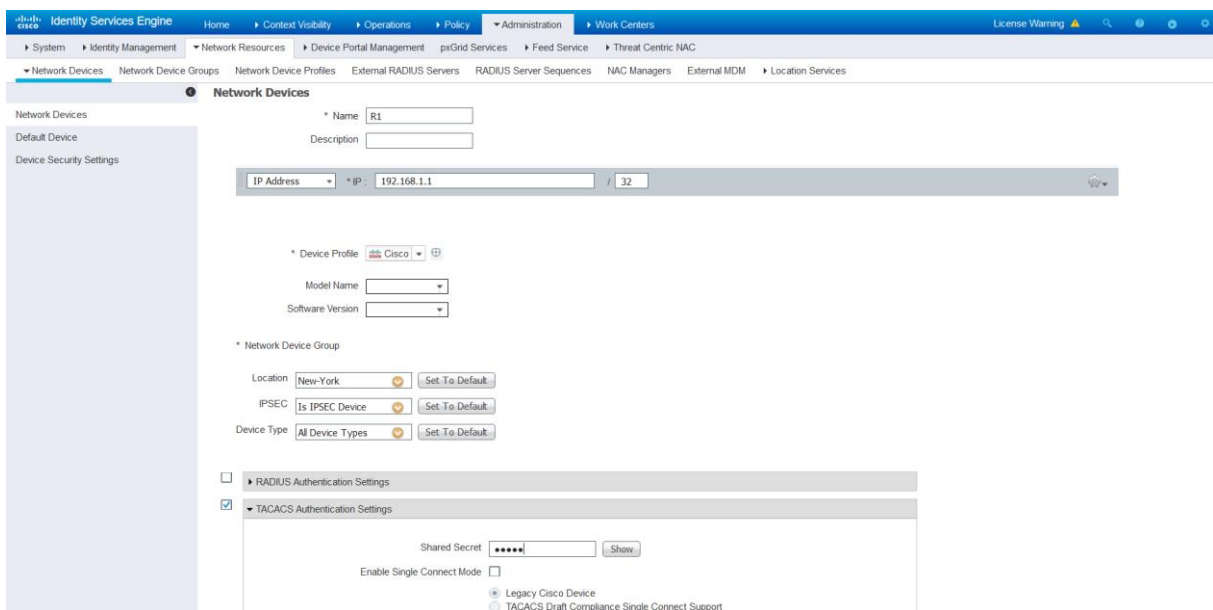
In the **IP Address** field, enter **192.168.1.1/32**. this the IP address of the router interface that will forward TACACS packets to Cisco ISE.

From the **Location** drop-down menu, select **New-York**.

To activate **TACACS Authentication Settings**, click the check box.

In the **Shared Secret** field, enter a shared secret of **cisco**.

Click the **Submit** button.



Click **Add** once again. The AAA Client window opens.

In the **Name** field, type **R2** as the name.

In the **IP Address** field, enter **192.168.1.2/32**. this the IP address of the router interface that will forward TACACS packets to Cisco ISE.
From the **Location** drop-down menu, select **San-Jose**.

To activate **TACACS Authentication Settings**, click the check box.
In the **Shared Secret** field, enter a shared secret of **cisco**.
Click the **Submit** button.

The screenshot shows the configuration page for a Network Device in Cisco ISE. The configuration includes:

- Name: R2
- Description: (empty)
- IP Address: 192.168.1.2 / 32
- Device Profile: Cisco
- Model Name: (empty)
- Software Version: (empty)
- Network Device Group:
 - Location: San-Jose
 - IPSEC: Is IPSEC Device
 - Device Type: All Device Types
- TACACS Authentication Settings:
 - Shared Secret: cisco
 - Enable Single Connect Mode: (unchecked)
 - Legacy Cisco Device: (checked)
 - TACACS Draft Compliance Single Connect Support: (unchecked)

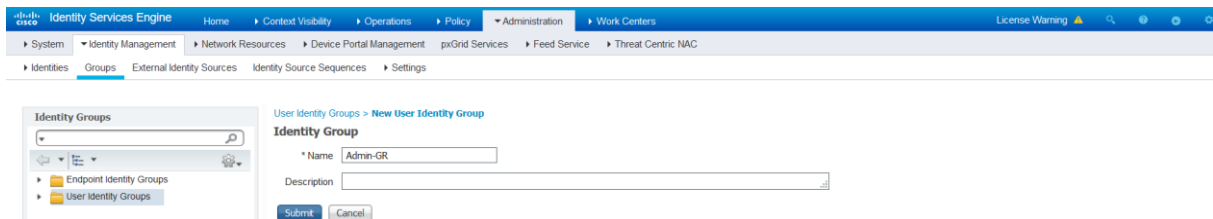
Name	IP/Mask	Profile Name	Location	Type	Description
R1	192.168.1.1/32	Cisco	New-York	All Device Types	
R2	192.168.1.2/32	Cisco	San-Jose	All Device Types	
SW-1	192.168.1.3/32	Cisco	All Locations	All Switches	

Create two user groups.

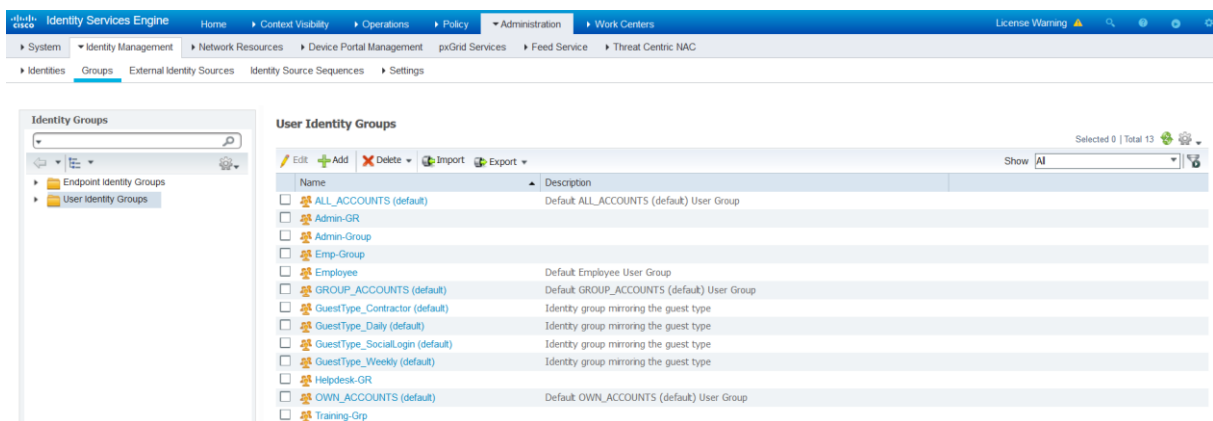
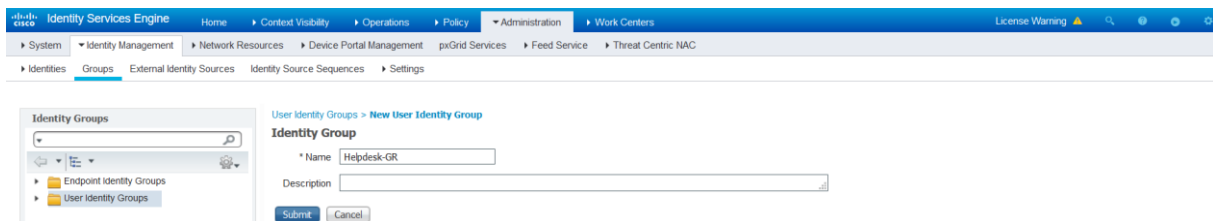
Navigate to **Administration > Identity Management > Groups**.
Under the **User Identity Groups**, click **Add**.

Name	Description
ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group
Admin-Group	
Emp-Group	
Employee	Default Employee User Group
GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Group
GuestType_Contractor (default)	Identity group mirroring the guest type
GuestType_Daily (default)	Identity group mirroring the guest type
GuestType_SocialLogin (default)	Identity group mirroring the guest type
GuestType_Weekly (default)	Identity group mirroring the guest type
OWN_ACCOUNTS (default)	Default OWN_ACCOUNTS (default) User Group
Training-Grp	

In the **Name** field, enter **Admin-GR**.
Click **Submit**.

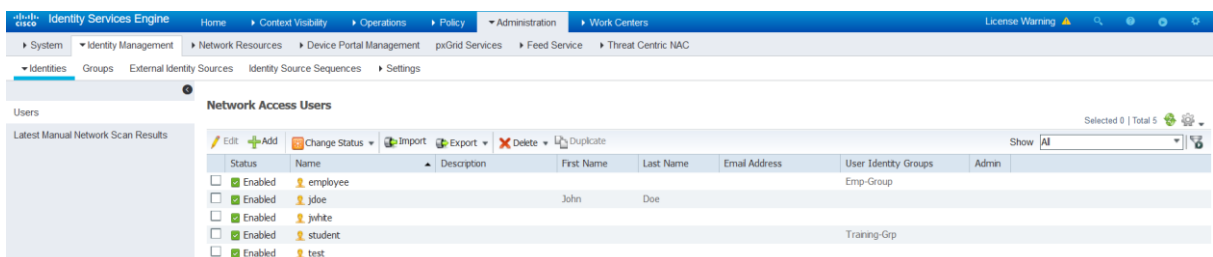


Create another **User Identity Groups**.
In the **Name** field, enter **Helpdesk-GR**.
Click **Submit**.



Create Two users.

Navigate to **Administration > Identity Management > Identities**.



Create a user **administrator** with password **Admin123**. In the **User Groups** field, select **Admin-GR**.
Click **Submit**.

Identity Services Engine Administration Work Centers

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

Identities Groups External Identity Sources Identity Source Sequences Settings

Users Latest Manual Network Scan Results

Network Access Users List > New Network Access User

Network Access User

* Name: administrator

Status: Enabled

Email:

Passwords

Password Type: Internal Users

Password: Re-Enter Password:

* Login Password: (i)

Enable Password: (i)

User Information

Account Options

Account Disable Policy

User Groups

Admin-GR

Create a user **helpdesk** with password **Help123**. In the **User Groups** field, select **Helpdesk-GR**.
Click **Submit**.

Identity Services Engine Administration Work Centers

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

Identities Groups External Identity Sources Identity Source Sequences Settings

Users Latest Manual Network Scan Results

Network Access Users List > New Network Access User

Network Access User

* Name: helpdesk

Status: Enabled

Email:

Passwords

Password Type: Internal Users

Password: Re-Enter Password:

* Login Password: (i)

Enable Password: (i)

User Information

Account Options

Account Disable Policy

User Groups

Helpdesk-GR

Identity Services Engine Administration Work Centers

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

Identities Groups External Identity Sources Identity Source Sequences Settings

Users Latest Manual Network Scan Results

Network Access Users

Selected 0 | Total 7

Status	Name	Description	First Name	Last Name	Email Address	User Identity Groups	Admin
<input checked="" type="checkbox"/>	administrator					Admin-GR	
<input checked="" type="checkbox"/>	employee					Emp-Group	
<input checked="" type="checkbox"/>	helpdesk					Helpdesk-GR	
<input checked="" type="checkbox"/>	jdoe		John	Doe			
<input checked="" type="checkbox"/>	jwhite						
<input checked="" type="checkbox"/>	student					Training-Grp	
<input checked="" type="checkbox"/>	test						

To add policy elements, navigate to **Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles**.

You will add two different TACACS profiles with different privilege levels.

Click **Add** to create a new profile named **Privilege_1** where the **default**

Copyright 2021 Redouane Meddane. Consumers may download and use this document for personal use only. Downloading and editing this document for redistribution is prohibited. All rights reserved.

privilege level is 8, and maximum privilege level is 8. Click **Submit**.

The screenshot shows the Cisco Identity Services Engine interface. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The left sidebar shows a tree view with 'Results' > 'TACACS Profiles' selected. The main content area displays a table of TACACS Profiles:

Name	Type	Description
Default Shell Profile	Shell	Default Shell Profile
Deny All Shell Profile	Shell	Deny All Shell Profile
WLC ALL	WLC	WLC ALL
WLC MONITOR	WLC	WLC MONITOR

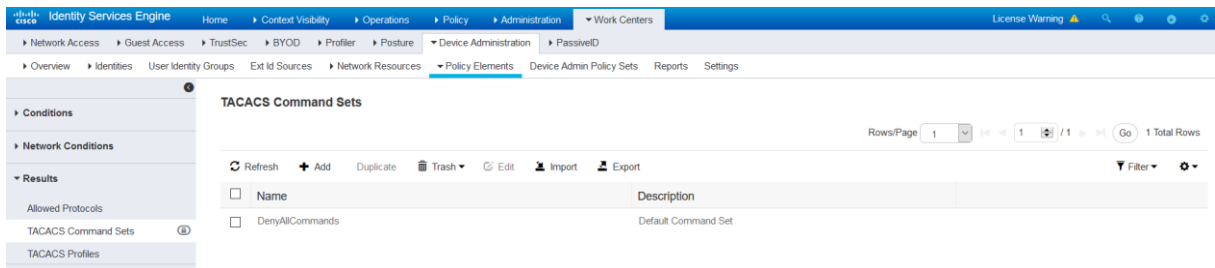
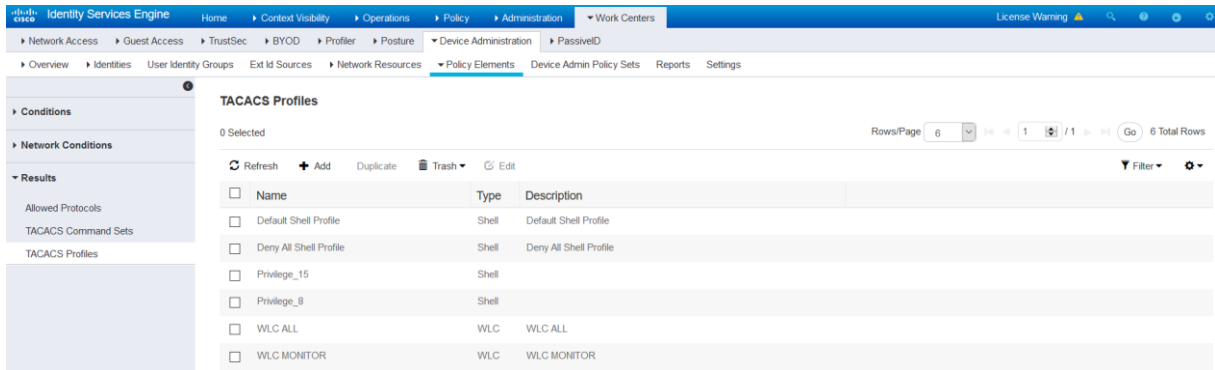
The screenshot shows the 'New TACACS Profile' configuration page. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The left sidebar shows 'Results' > 'TACACS Profiles' selected. The main content area shows the configuration for a profile named 'Privilege_8':

- Name: Privilege_8
- Description: (empty)
- Task Attribute View / Raw View tabs
- Common Tasks section:
 - Common Task Type: Shell
 - Default Privilege: 8 (Select 0 to 15)
 - Maximum Privilege: 8 (Select 0 to 15)
 - Access Control List: (empty)
 - Auto Command: (empty)
 - No Escape: (empty) (Select true or false)
 - Timeout: (empty) Minutes (0-9999)
 - Idle Time: (empty) Minutes (0-9999)

Add a second profile named **Privilege_15**, with a **default privilege level 15** and **maximum privilege level 15**. Click **Submit**.

The screenshot shows the 'New TACACS Profile' configuration page for a profile named 'Privilege_15'. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The left sidebar shows 'Results' > 'TACACS Profiles' selected. The main content area shows the configuration for a profile named 'Privilege_15':

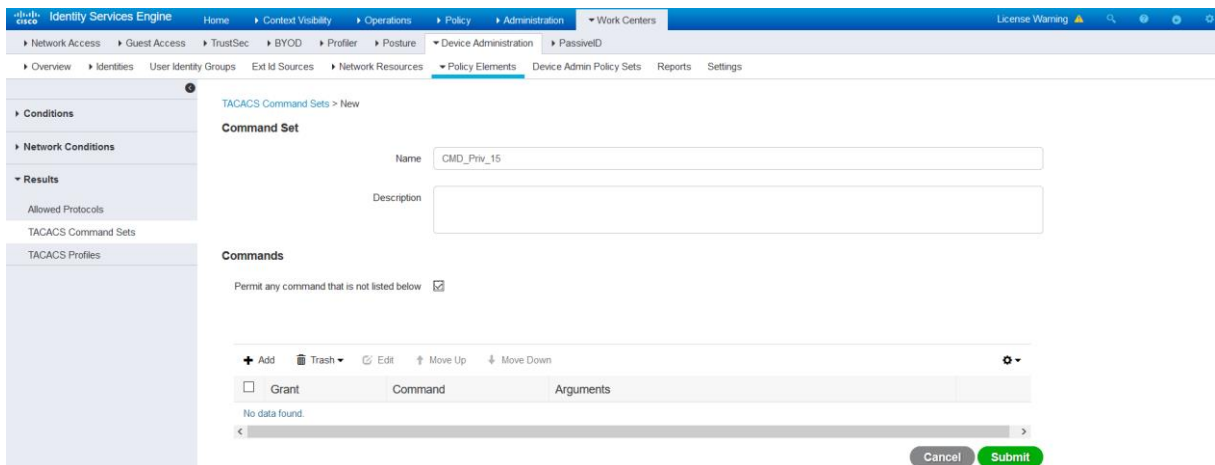
- Name: Privilege_15
- Description: (empty)
- Task Attribute View / Raw View tabs
- Common Tasks section:
 - Common Task Type: Shell
 - Default Privilege: 15 (Select 0 to 15)
 - Maximum Privilege: 15 (Select 0 to 15)
 - Access Control List: (empty)
 - Auto Command: (empty)
 - No Escape: (empty) (Select true or false)
 - Timeout: (empty) Minutes (0-9999)
 - Idle Time: (empty) Minutes (0-9999)



Navigate to **Work Centers > Device Administration > Policy Elements > Results > TACACS Command Sets**. Create two command sets, one with full access, and one with limited access to a specific set of commands.

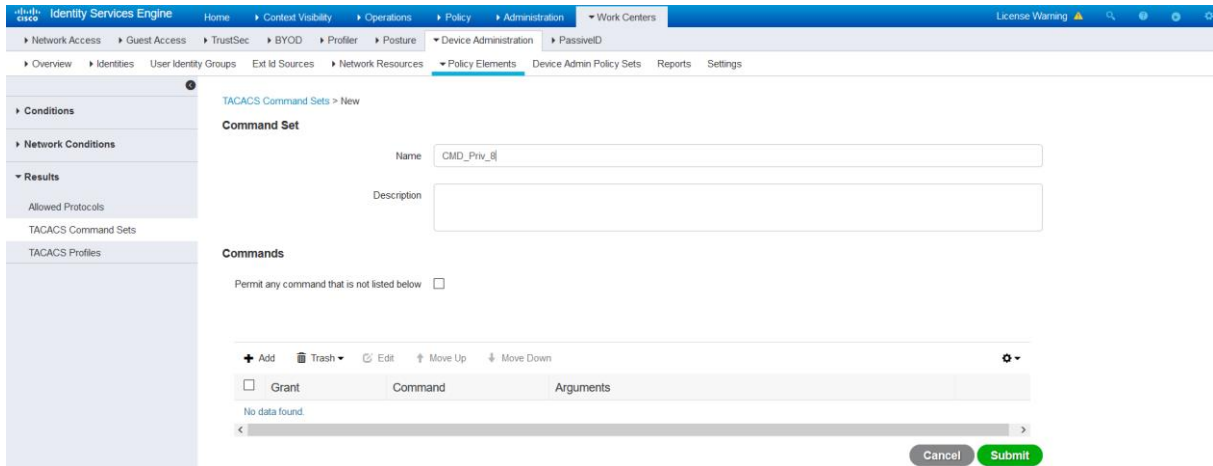
Click **Add** to create a new command set. Configure the name as **CMD_Priv_15**, and click the checkbox for **Permit any command that is not listed below**.

Click **Submit**.

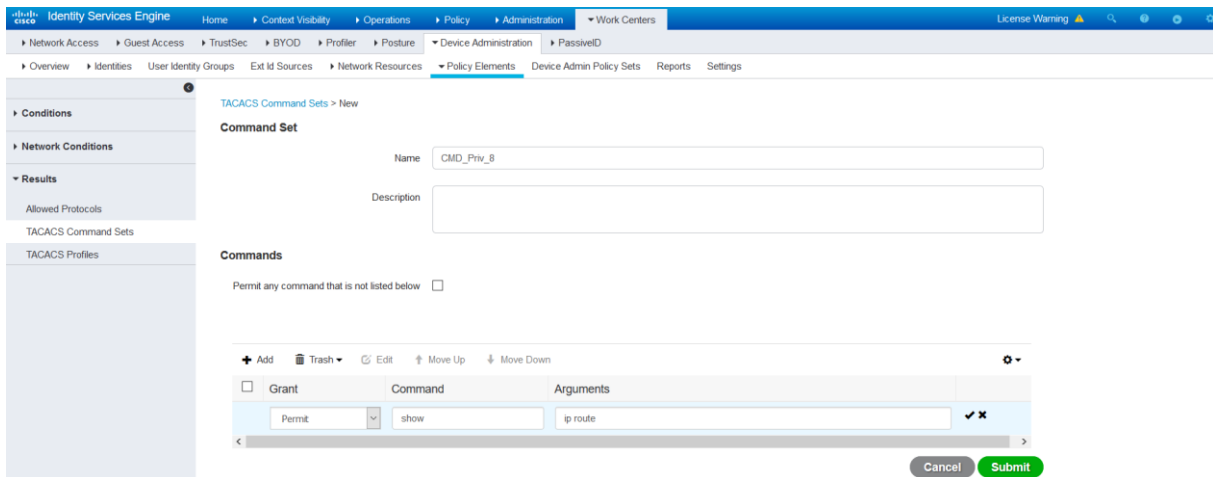


Create a new command set named **CMD_Priv_15** to permit the following commands:

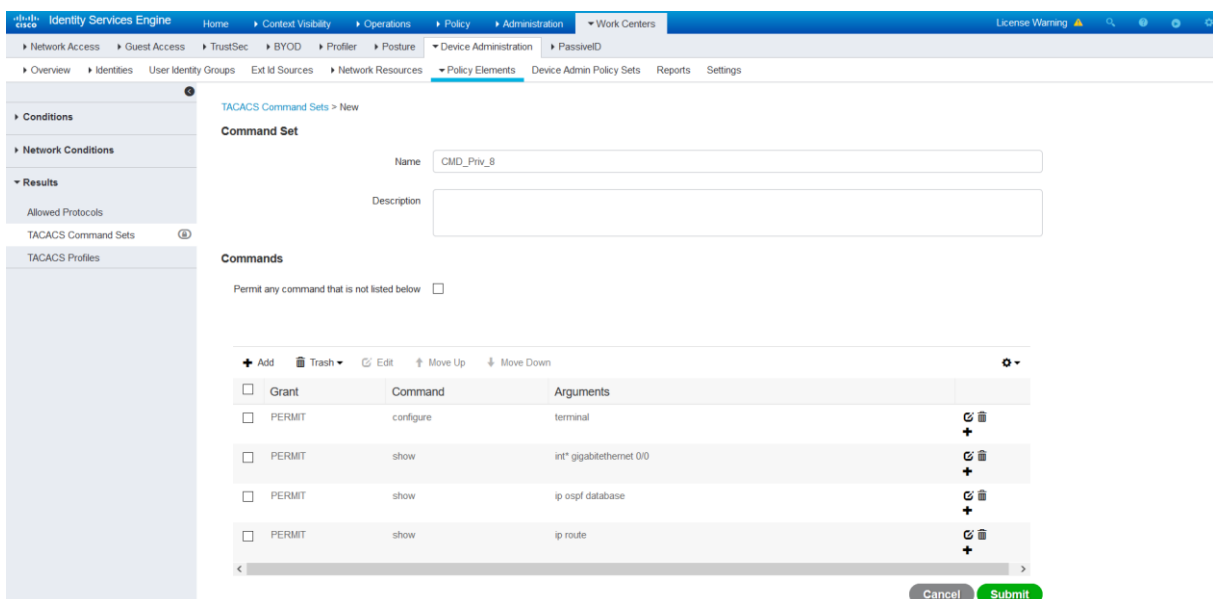
Configure terminal
Show interface g0/0
Show ip ospf database
Show ip route

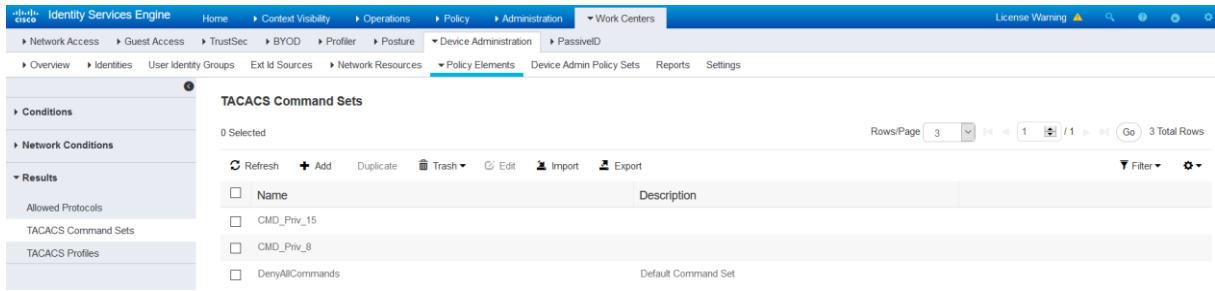


Click the **Add** button to add each command. After entering each command, make sure to click the checkmark at the end of the line to save the command.



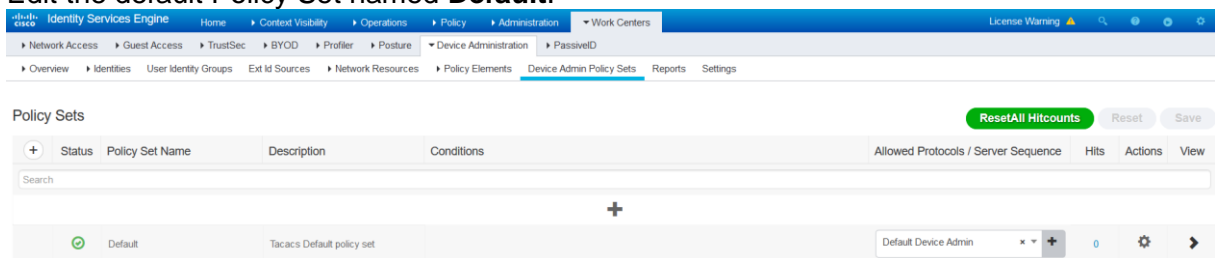
Click **Submit**.





For policy creation, navigate to **Work Centers > Device Administration > Device Admin Policy Sets**.

Edit the default Policy Set named **Default**.



Edit the **Authentication Policy** to use **Internal Users** as the Identity Store. Next edit the **Authorization Policy**, insert a new authorization policy above the Default authorization policy.

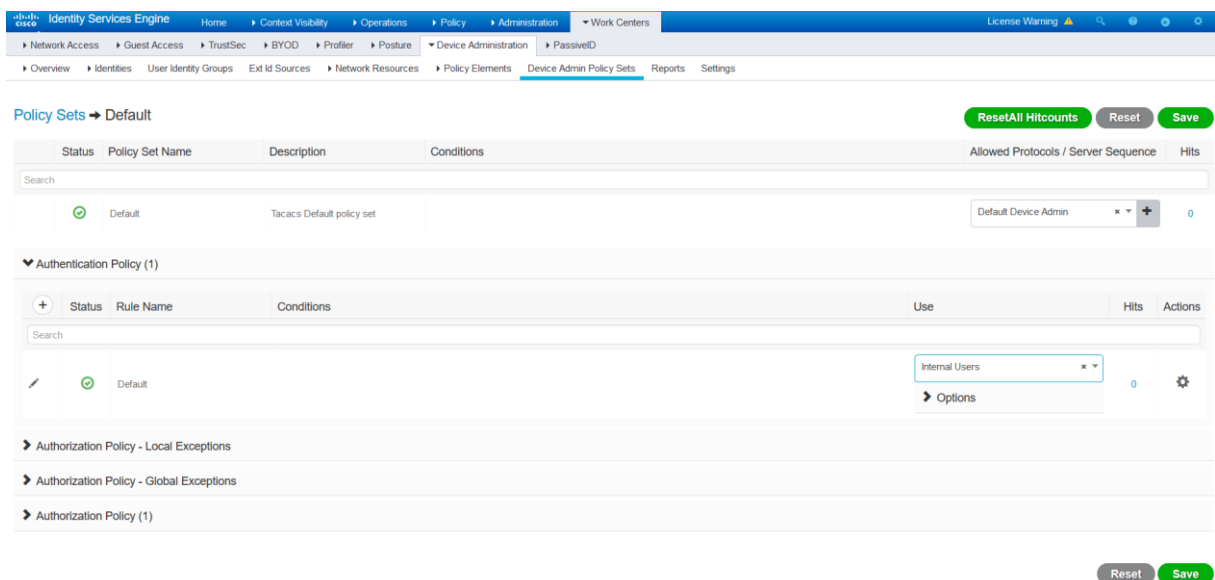
Configure this new rule according to the chart below.

Rule Name: Admin-AuthoZ

Conditions: IdentityGroup Name EQUALS User Identity Groups:Admin-GR

Command Sets: CMD_Priv_15

Shell Profiles: Privilege_15



Conditions Studio

Library

Search by Name

- EAP-MSCHAPv2 (i)
- EAP-TLS (i)
- Guest_Flow (i)
- Network_Access_Authentication_Passed (i)

Editor

IdentityGroup:Name

⋮

Set to 'Is not' Duplicate Save

+ New AND OR

Close Use

Identity Services Engine

Home > Context Visibility > Operations > Policy > Administration > Work Centers

License Warning

Network Access > Guest Access > TrustSec > BYOD > Profiler > Posture

Device Administration > PasswdID

Overview > Identities > User Identity Groups > Ext Id Sources > Network Resources > Policy Elements > Device Admin Policy Sets > Reports > Settings

Default Tacacs Default policy set

Default Device Admin 0

Authentication Policy (1)
 Authorization Policy - Local Exceptions
 Authorization Policy - Global Exceptions
 Authorization Policy (2)

+	Status	Rule Name	Conditions	Results		Hits	Actions
				Command Sets	Shell Profiles		
		Admin-AuthoZ	IdentityGroup:Name EQUALS User Identity Groups:Admin-GR	*CMD_Priv_15	Privilege_15		
	Default			*DenyAllCommands	Deny All Shell Profile	0	

Reset Save

Now add an Authorization Policy for **Helpdesk**. Start by clicking the **gear** icon at the end of the **Admin-AuthoZ** policy, and choose **Insert New Rule Below**. Configure this new rule according to the chart below.

Rule Name: Helpdesk-AuthoZ

Conditions: IdentityGroup Name EQUALS User Identity Groups:Helpdesk-GR

Command Sets: CMD_Priv_8

Shell Profiles: Privilege_8

Conditions Studio



Library

Search by Name

- EAP-MSCHAPv2
- EAP-TLS
- Guest_Flow
- Network_Access_Authentication_Passed

Editor

IdentityGroup Name

Set to 'Is not' Save

Remove this item, to select or type another item.

+
New
AND
OR

Close
Use

Identity Services Engine | Home | Context Visibility | Operations | Policy | Administration | Work Centers | License Warning

Network Access | Guest Access | TrustSec | BYOD | Profiler | Posture | Device Administration | PassiveID

Overview | Identities | User Identity Groups | Ext Id Sources | Network Resources | Policy Elements | **Device Admin Policy Sets** | Reports | Settings

Default | Tacacs Default policy set | Default Device Admin x 0

Authentication Policy (1)
 Authorization Policy - Local Exceptions
 Authorization Policy - Global Exceptions
 Authorization Policy (3)

+	Status	Rule Name	Conditions	Results		Hits	Actions
				Command Sets	Shell Profiles		
		Admin_AuthoZ	IdentityGroup Name EQUALS User Identity Groups:Admin-GR	<input type="text" value="CMD_Priv_15"/>	Privilege_15		
		Helpdesk_AuthoZ	IdentityGroup Name EQUALS User Identity Groups:Helpdesk-GR	<input type="text" value="CMD_Priv_8"/>	Privilege_8		
		Default		<input type="text" value="DenyAllCommands"/>	Deny All Shell Profile	0	

Reset
Save

The screenshot shows the Identity Services Engine (ISE) Work Centers interface. The top navigation bar includes Home, Context Visibility, Operations, Policy, Administration, and Work Centers. The main content area is divided into two sections:

- Authentication Policy (1):** A table with columns for Status, Rule Name, Conditions, Use, Hits, and Actions. A search bar is present. A single rule named "Default" is listed with a status of "On" and 0 hits.
- Authorization Policy (3):** A table with columns for Status, Rule Name, Conditions, Results (Command Sets, Shell Profiles), Hits, and Actions. A search bar is present. Three rules are listed:
 - Admin-AuthoZ:** IdentityGroup Name EQUALS User Identity Groups:Admin-GR. Command Set: CMD_Priv_15. Shell Profile: Privilege_15. Hits: 0.
 - Helpdesk-AuthoZ:** IdentityGroup Name EQUALS User Identity Groups:Helpdesk-GR. Command Set: CMD_Priv_8. Shell Profile: Privilege_8. Hits: 0.
 - Default:** Command Set: DenyAllCommands. Shell Profile: Deny All Shell Profile. Hits: 0.

Return to your **Admin PC**, and use PUTTY to open an SSH session to **R1** router (**192.168.1.1**).

Login using the credentials **administrator / Admin123**. This should succeed.

The screenshot shows the PuTTY Configuration dialog box. The "Category:" list on the left includes Session, Logging, Terminal, Keyboard, Bell, Features, Window, Appearance, Behaviour, Translation, Selection, Colours, Connection, Data, Proxy, Telnet, Rlogin, SSH, and Serial. The "SSH" category is selected.

The "Basic options for your PuTTY session" section contains the following fields and options:

- Specify the destination you want to connect to:**
 - Host Name (or IP address): 192.168.1.1
 - Port: 22
- Connection type:**
 - Raw
 - Telnet
 - Rlogin
 - SSH
 - Serial
- Load, save or delete a stored session:**
 - Saved Sessions: (Empty list)
 - Default Settings: (Selected)
 - Buttons: Load, Save, Delete
- Close window on exit:**
 - Always
 - Never
 - Only on clean exit

At the bottom, there are buttons for "About", "Help", "Open", and "Cancel".

```

192.168.1.1 - PuTTY
login as: administrator
Keyboard-interactive authentication prompts from server:
| Password:
| End of keyboard-interactive prompts from server

R1#

```

Navigate to **Operations > TACACS > Live Logs** to see that the authentication and authorization are successful.

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Device ...	Network Device I
Jan 07, 2020 08:35:46:417 PM	✓	🔒	administrator	Authorization		Default >> Admin-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 08:35:46:391 PM	✓	🔒	administrator	Authentication	Default >> Default		ISE	R1	192.168.1.1
Jan 07, 2020 08:34:41:024 PM	✗	🔒	INVALID	Authentication	Default >> Default		ISE	R1	192.168.1.1
Jan 07, 2020 08:32:18:764 PM	✓	🔒	administrator	Authorization		Default >> Admin-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 08:32:18:711 PM	✓	🔒	administrator	Authentication	Default >> Default		ISE	R1	192.168.1.1

For the successful **Administrator** entry, click the **Details** icon, as shown above. You can analyze the details of each session. Some of the more pertinent information includes the Authorization details.

The ISE TACACS Logs confirms Authentication and Authorization succeed, matching the correct Authorization Profile ***Privilege_15***.

Overview

Request Type	Authentication
Status	Pass
Session Key	ISE/363103442/188
Message Text	Passed-Authentication: Authentication succeeded
Username	administrator
Authentication Policy	Default >> Default
Selected Authorization Profile	Privilege_15

Authentication Details

Generated Time	2020-01-07 20:35:46.391000 +00:00
Logged Time	2020-01-07 20:35:46.391
Epoch Time (sec)	1578429346
ISE Node	ISE
Message Text	Passed-Authentication: Authentication succeeded
Failure Reason	

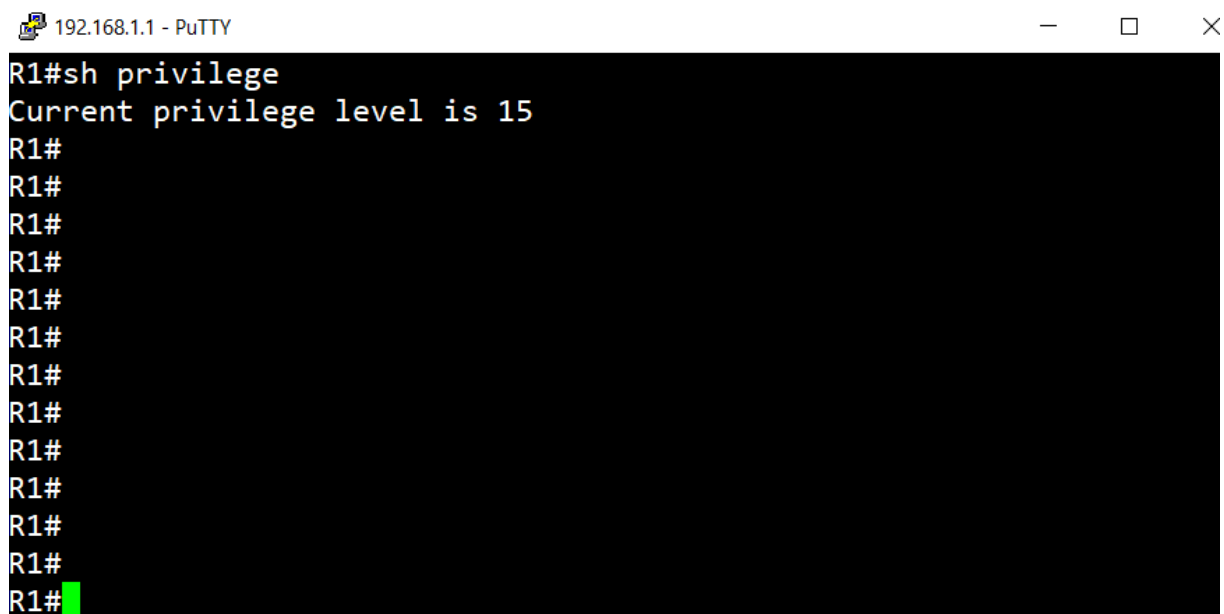
Overview

Request Type	Authorization
Status	Pass
Session Key	ISE/363103442/189
Message Text	Device-Administration: Session Authorization succeeded
Username	administrator
Authorization Policy	Default >> Admin-AuthoZ
Shell Profile	Privilege_15
Matched Command Set	
Command From Device	

Authorization Details

Generated Time	2020-01-07 20:35:46.417 +0:00
Logged Time	2020-01-07 20:35:46.417
Epoch Time (sec)	1578429346
ISE Node	ISE
Message Text	Device-Administration: Session Authorization succeeded

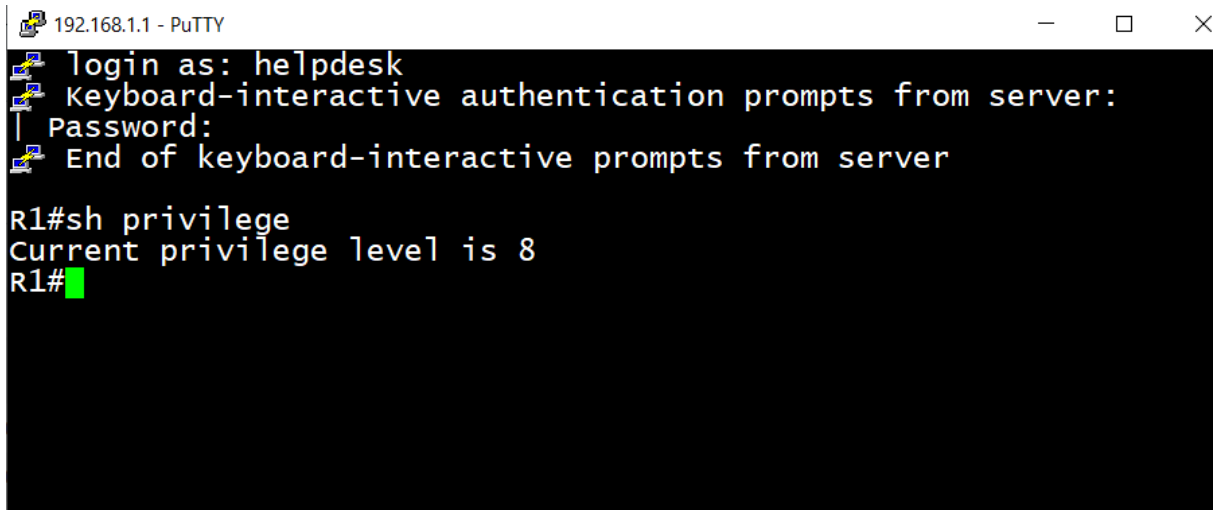
From Putty, type the **show privilege** command, you should see the level of 15.



```
192.168.1.1 - PuTTY
R1#sh privilege
Current privilege level is 15
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
R1#
```

Return to your Admin PC, and use PUTTY to open a SSH session to **R1** router (**192.168.1.1**) Login using the credentials **helpdesk / Help123**. This should succeed.

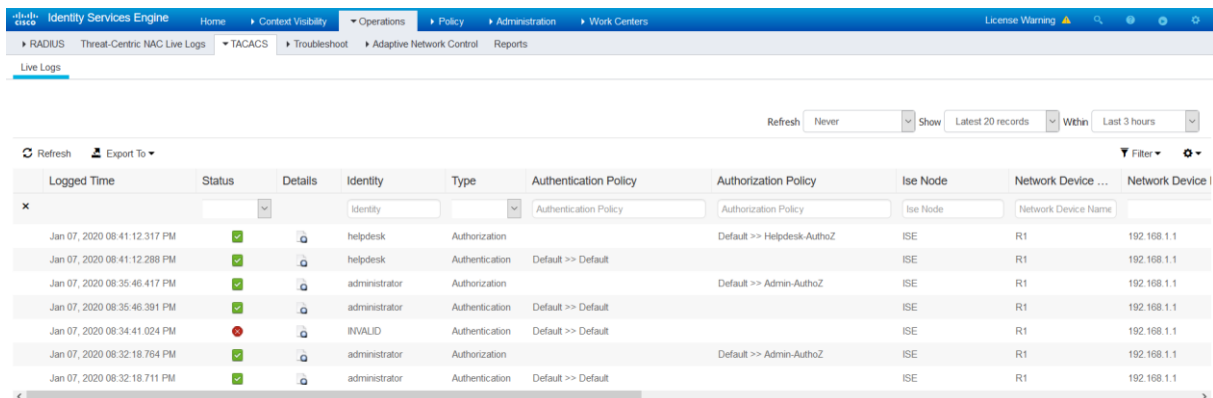
Type the **show privilege** command, the level should be 8.



```
192.168.1.1 - PuTTY
login as: helpdesk
Keyboard-interactive authentication prompts from server:
Password:
End of keyboard-interactive prompts from server

R1#sh privilege
Current privilege level is 8
R1#
```

Navigate to **Operations > TACACS > Live Logs** to see that the authentication and authorization are successful.



Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Device ...	Network Device
Jan 07, 2020 08:41:12:317 PM	✓		helpdesk	Authorization	Default >> Default	Default >> Helpdesk-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 08:41:12:288 PM	✓		helpdesk	Authentication	Default >> Default		ISE	R1	192.168.1.1
Jan 07, 2020 08:35:46:417 PM	✓		administrator	Authorization	Default >> Admin-AuthoZ	Default >> Admin-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 08:35:46:391 PM	✓		administrator	Authentication	Default >> Default		ISE	R1	192.168.1.1
Jan 07, 2020 08:34:41:024 PM	✗		INVALID	Authentication	Default >> Default		ISE	R1	192.168.1.1
Jan 07, 2020 08:32:18:764 PM	✓		administrator	Authorization	Default >> Admin-AuthoZ	Default >> Admin-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 08:32:18:711 PM	✓		administrator	Authentication	Default >> Default		ISE	R1	192.168.1.1

For the **helpdesk** entry, click the **Details** icon, as shown above. You can analyze the details of each session. Some of the more pertinent information includes the Authorization details, as shown below.

The ISE TACACS Logs confirms authentication and authorization succeed, matching the correct Authorization Profile **Privilege_8**.

Overview

Request Type	Authentication
Status	Pass
Session Key	ISE/363103442/192
Message Text	Passed-Authentication: Authentication succeeded
Username	helpdesk
Authentication Policy	Default >> Default
Selected Authorization Profile	Privilege_8

Authentication Details

Generated Time	2020-01-07 20:41:12.288000 +00:00
Logged Time	2020-01-07 20:41:12.288
Epoch Time (sec)	1578429672
ISE Node	ISE
Message Text	Passed-Authentication: Authentication succeeded
Failure Reason	

Overview

Request Type	Authorization
Status	Pass
Session Key	ISE/363103442/193
Message Text	Device-Administration: Session Authorization succeeded
Username	helpdesk
Authorization Policy	Default >> Helpdesk-AuthoZ
Shell Profile	Privilege_8
Matched Command Set	
Command From Device	

Authorization Details

Generated Time	2020-01-07 20:41:12.317 +0:00
Logged Time	2020-01-07 20:41:12.317
Epoch Time (sec)	1578429672
ISE Node	ISE
Message Text	Device-Administration: Session Authorization succeeded

Enable the **debug aaa authorization** command on the router R1.

```
R1#debug aaa authorization
AAA Authorization debugging is on
R1#
```

```
R1#debug aaa authorization
AAA Authorization debugging is on
R1#
R1#
Jan  7 20:39:13.979: AAA/BIND(00000014): Bind i/f
Jan  7 20:39:18.771: AAA/AUTHOR (0x14): Pick method list 'default'
Jan  7 20:39:18.803: AAA/AUTHOR/EXEC(00000014): processing AV cmd=
Jan  7 20:39:18.803: AAA/AUTHOR/EXEC(00000014): processing AV priv-lvl=8
Jan  7 20:39:18.803: AAA/AUTHOR/EXEC(00000014): Authorization successful
R1#
```

```

R1#debug aaa authorization
AAA Authorization debugging is on
R1#
R1#
Jan 7 20:39:13.979: AAA/BIND(00000014): Bind i/f
Jan 7 20:39:18.771: AAA/AUTHOR (0x14): Pick method list 'default'
Jan 7 20:39:18.803: AAA/AUTHOR/EXEC(00000014): processing AV cmd=
Jan 7 20:39:18.803: AAA/AUTHOR/EXEC(00000014): processing AV priv-lvl=8
Jan 7 20:39:18.803: AAA/AUTHOR/EXEC(00000014): Authorization successful
R1#
R1#
R1#
Jan 7 20:40:08.463: AAA/AUTHOR: auth_need : user= 'helpdesk' ruser= 'R1'rem_addr= '192.168.1.10' priv= 1 list= '
AUTHOR-TYPE= 'commands'
R1#

```

From the SSH Session with **helpdesk** user, execute the **show privilege** and **show version** commands.

The **show privilege** command is successfully executed even if the Command Sets **CM_Priv_8** does not include this command, this is not what we should expect.

```

192.168.1.1 - PuTTY
Login as: helpdesk
Keyboard-interactive authentication prompts from server:
| Password:
End of keyboard-interactive prompts from server

R1#sh privilege
Current privilege level is 8
R1#

```

The **show version** command is successfully executed, even if the Command Sets **CM_Priv_8** does not include this command, this is not what we should expect.

```

192.168.1.1 - PuTTY
R1#sh version
Cisco IOS Software, c2900 Software (C2900-UNIVERSALK9-M), Version 15.3(3)M4, REL
EASE SOFTWARE (fc2)
Technical support: http://www.cisco.com/techsupport
Copyright (c) 1986-2014 by Cisco Systems, Inc.
Compiled wed 24-Sep-14 06:53 by prod_rel_team

ROM: System Bootstrap, Version 15.0(1r)M15, RELEASE SOFTWARE (fc1)

R1 uptime is 3 hours, 28 minutes
System returned to ROM by power-on
System restarted at 17:12:36 UTC Tue Jan 7 2020
System image file is "flash0:c2900-universalk9-mz.SPA.153-3.M4.bin"
Last reload type: Normal Reload
Last reload reason: power-on

This product contains cryptographic features and is subject to United
States and local country laws governing import, export, transfer and
use. Delivery of Cisco cryptographic products does not imply
third-party authority to import, export, distribute or use encryption.
Importers, exporters, distributors and users are responsible for
compliance with U.S. and local country laws. By using this product you

```

What's wrong here ?

Let's see the debugging on router R1, we can see that the router does not contact the ISE server for command authorization, the router shown that these commands are available at the privilege level 1, the higher privilege level 8 can also access the commands sets at lower level.

```
R1#
Jan 7 20:40:08.463: AAA/AUTHOR: auth_need : user= 'helpdesk' ruser= 'R1' rem_addr= '192.168.1.10' priv= 1 list= ''
AUTHOR-TYPE= 'commands'
R1#
R1#
R1#
Jan 7 20:41:19.419: AAA/AUTHOR: auth_need : user= 'helpdesk' ruser= 'R1' rem_addr= '192.168.1.10' priv= 1 list= ''
AUTHOR-TYPE= 'commands'
```

Let's enable the command authorization for level 1.

```
R1(config)#aaa authorization commands 1 default group tacacs+ local
```

for each command run on the CLI, the router will check with the TACACS server to confirm the user is allowed to run the command.

Execute the **show privilege** command using the SSH session of **helpdesk** user, now the authorization failed.



```
192.168.1.1 - PuTTY
R1#
R1#
R1#
R1#show privileg
Command authorization failed.

R1#
R1#
R1#
R1#
```

On the router R1, a request for authorization is sent to ISE server, since this command is not configured under the Command Sets **CMD_Priv_8**, the **Helpdesk** user is not allowed to type this command.

```
R1#DEBUg Aaa AuthOrization
AAA Authorization debugging is on
R1#
Jan 7 20:53:40.547: AAA/AUTHOR: auth_need : user= 'helpdesk' ruser= 'R1' rem_addr= '192.168.1.10' priv= 1 list= ''
AUTHOR-TYPE= 'commands'
Jan 7 20:53:40.547: AAA: parse name=tty388 idb type=-1 tty=-1
Jan 7 20:53:40.547: AAA: name=tty388 flags=0x11 type=5 shelf=0 slot=0 adapter=0 port=388 channel=0
Jan 7 20:53:40.547: AAA/MEMORY: create_user (0x3C4437DC) user='helpdesk' ruser='R1' ds0=0 port='tty388' rem_addr='
192.168.1.10' authen_type=ASCII service=NONE priv=1 initial_task_id='0', vrf= (id=0)
Jan 7 20:53:40.547: tty388 AAA/AUTHOR/CMD (1655813791): Port='tty388' list='' service=CMD
Jan 7 20:53:40.547: AAA/AUTHOR/CMD: tty388 (1655813791) user='helpdesk'
Jan 7 20:53:40.547: tty388 AAA/AUTHOR/CMD (1655813791): send AV service=shell
Jan 7 20:53:40.547: tty388 AAA/AUTHOR/CMD (1655813791): send AV cmd=show
Jan 7 20:53:40.547: tty388 AAA/AUTHOR/CMD (1655813791): send AV cmd-arg=privilege
Jan 7 20:53:40.547: tty388 AAA/AUTHOR/CMD (1655813791): send AV cmd-arg=<cr>
Jan 7 20:53:40.547: tty388 AAA/AUTHOR/CMD (1655813791): found list "default"
Jan 7 20:53:40.547: tty388 AAA/AUTHOR/CMD (1655813791): Method=tacacs+ (tacacs+)
Jan 7 20:53:40.547: AAA/AUTHOR/TAC+: (1655813791): user=helpdesk
Jan 7 20:53:40.547: AAA/AUTHOR/TAC+: (1655813791): send AV service=shell
Jan 7 20:53:40.547: AAA/AUTHOR/TAC+: (1655813791): send AV cmd=show
Jan 7 20:53:40.547: AAA/AUTHOR/TAC+: (1655813791): send AV cmd-arg=privilege
Jan 7 20:53:40.547: AAA/AUTHOR/TAC+: (1655813791): send AV cmd-arg=<cr>
Jan 7 20:53:40.747: AAA/AUTHOR (1655813791): Post authorization status = FAIL
Jan 7 20:53:40.747: AAA/MEMORY: free_user (0x3C4437DC) user='helpdesk' ruser='R1' port='tty388' rem_addr='192.168.
1.10' authen_type=ASCII service=NONE priv=1 vrf= (id=0)
```

Navigate to **Operations > TACACS > Live Logs** to see that the authentication and authorization.

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Device ...	Network Device
Jan 07, 2020 08:58:45.185 PM	●		helpdesk	Authorization	Authentication Policy	Authorization Policy	ISE	R1	192.168.1.1
Jan 07, 2020 08:54:07.202 PM	●		helpdesk	Authorization	Default >> Helpdesk-AuthoZ	Default >> Helpdesk-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 08:54:07.169 PM	●		helpdesk	Authentication	Default >> Default	Default >> Helpdesk-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 08:46:02.049 PM	●		helpdesk	Authorization	Default >> Default	Default >> Helpdesk-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 08:46:02.015 PM	●		helpdesk	Authentication	Default >> Default	Default >> Helpdesk-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 08:41:12.317 PM	●		helpdesk	Authorization	Default >> Default	Default >> Helpdesk-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 08:41:12.288 PM	●		helpdesk	Authentication	Default >> Default	Default >> Admin-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 08:35:46.417 PM	●		administrator	Authorization	Default >> Default	Default >> Admin-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 08:35:46.391 PM	●		administrator	Authentication	Default >> Default	Default >> Admin-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 08:34:41.024 PM	●		INVALID	Authentication	Default >> Default	Default >> Admin-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 08:32:18.764 PM	●		administrator	Authorization	Default >> Default	Default >> Admin-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 08:32:18.711 PM	●		administrator	Authentication	Default >> Default	Default >> Admin-AuthoZ	ISE	R1	192.168.1.1

For the failed **helpdesk** entry, click the **Details** icon. You can analyze the details of each session. Some of the more pertinent information includes the Authorization details, as shown below.

Overview

Request Type	Authorization
Status	Fail
Session Key	ISE/363103442/204
Message Text	Failed-Attempt: Command Authorization failed
Username	helpdesk
Authorization Policy	Default >> Helpdesk-AuthoZ
Shell Profile	
Matched Command Set	
Command From Device	show privilege

Authorization Details

Generated Time	2020-01-07 20:58:45.185 +0:00
Logged Time	2020-01-07 20:58:45.185
Epoch Time (sec)	1578430725
ISE Node	ISE
Message Text	Failed-Attempt: Command Authorization failed
Failure Reason	13025 Command failed to match a Permit rule
Resolution	Check the SelectedCommandSet attributes to verify that the expected Command Sets were selected by the Authorization policy
Root Cause	The requested command failed to match a Permit rule in any of the Command Sets
Username	helpdesk
Network Device Name	R1
Network Device IP	192.168.1.1
Network Device Groups	IPSEC#s IPSEC Device#No,Location#All Locations#New-York,Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations#New-York
Device Port	tty388
Remote Address	192.168.1.10

Execute the **show version** command, now the **helpdesk** user is not able to execute this command, and the authorization failed.

```
192.168.1.1 - PuTTY
R1#
R1#
R1#
R1#show version
Command authorization failed.
R1#
R1#
R1#
R1#
```

On the router R1, a request for authorization is sent to ISE server, since this command is not configured under the Command Sets **CMD_Priv_8**, the **Helpdesk** user is not allowed to type this command. You get the **Post authorization status = Fail** message from the output.


```

R1#DEBUg AAa AUTHorization
AAA Authorization debugging is on
R1#
R1#
Jan 7 20:57:22.567: AAA/AUTHOR: auth_need : user= 'helpdesk' ruser= 'R1' rem_addr= '192.168.1.10' priv= 1 list= ''
AUTHOR-TYPE= 'commands'
Jan 7 20:57:22.567: AAA: parse name=tty388 idb type=-1 tty=-1
Jan 7 20:57:22.567: AAA: name=tty388 flags=0x11 type=5 shelf=0 slot=0 adapter=0 port=388 channel=0
Jan 7 20:57:22.567: AAA/MEMORY: create_user (0x3C4437DC) user='helpdesk' ruser='R1' ds0=0 port='tty388' rem_addr='
192.168.1.10' authen_type=ASCII service=NONE priv=1 initial_task_id='0', vrf= (id=0)
Jan 7 20:57:22.567: tty388 AAA/AUTHOR/CMD (460520163): Port='tty388' list='' service=CMD
Jan 7 20:57:22.567: AAA/AUTHOR/CMD: tty388 (460520163) user='helpdesk'
Jan 7 20:57:22.567: tty388 AAA/AUTHOR/CMD (460520163): send AV service=shell
Jan 7 20:57:22.567: tty388 AAA/AUTHOR/CMD (460520163): send AV cmd=show
Jan 7 20:57:22.567: tty388 AAA/AUTHOR/CMD (460520163): send AV cmd-arg=version
Jan 7 20:57:22.567: tty388 AAA/AUTHOR/CMD (460520163): send AV cmd-arg=<cr>
Jan 7 20:57:22.567: tty388 AAA/AUTHOR/CMD(460520163): found list "default"
Jan 7 20:57:22.567: tty388 AAA/AUTHOR/CMD (460520163): Method=tacacs+ (tacacs+)
Jan 7 20:57:22.567: AAA/AUTHOR/TAC+: (460520163): user=helpdesk
Jan 7 20:57:22.567: AAA/AUTHOR/TAC+: (460520163): send AV service=shell
Jan 7 20:57:22.567: AAA/AUTHOR/TAC+: (460520163): send AV cmd=show
Jan 7 20:57:22.567: AAA/AUTHOR/TAC+: (460520163): send AV cmd-arg=version
Jan 7 20:57:22.567: AAA/AUTHOR/TAC+: (460520163): send AV cmd-arg=<cr>
Jan 7 20:57:22.767: AAA/AUTHOR (460520163): Post authorization status = FAIL
Jan 7 20:57:22.767: AAA/MEMORY: free_user (0x3C4437DC) user='helpdesk' ruser='R1' port='tty388' rem_addr='192.168.
1.10' authen_type=ASCII service=NONE priv=1 vrf= (id=0)

```

For the failed **helpdesk** entry, click the **Details** icon. You can analyze the details and see the **Status**, the **Failure Reason** and **Root Cause**.

By attempting to use a command not permitted in the TACACS Command Set, results in failure

Overview

Request Type	Authorization
Status	Fail
Session Key	ISE/363103442/207
Message Text	Failed-Attempt: Command Authorization failed
Username	helpdesk
Authorization Policy	Default >> Helpdesk-AuthoZ
Shell Profile	
Matched Command Set	
Command From Device	show version

Authorization Details

Generated Time	2020-01-07 21:04:05.929 +0:00
Logged Time	2020-01-07 21:04:05.929
Epoch Time (sec)	1578431045
ISE Node	ISE
Message Text	Failed-Attempt: Command Authorization failed
Failure Reason	13025 Command failed to match a Permit rule
Resolution	Check the SelectedCommandSet attributes to verify that the expected Command Sets were selected by the Authorization policy
Root Cause	The requested command failed to match a Permit rule in any of the Command Sets
Username	helpdesk
Network Device Name	R1
Network Device IP	192.168.1.1
Network Device Groups	IPSEC#Is IPSEC Device#No,Location#All Locations#New-York,Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations#New-York
Device Port	tty388
Remote Address	192.168.1.10

From the SSH session, execute the **show ip ospf database** command, since this command is included in the Command Sets **CMD_Priv_8**, the **helpdesk** user is able to run this command.



```
192.168.1.1 - PuTTY
R1#
R1#
R1#
R1#show ip ospf database
R1#
R1#
R1#
R1#
```

The **Post authorization status = PASS_ADD** is displayed in the debug output.

```

Jan 7 20:59:10.067: AAA/AUTHOR: auth_need : user= 'helpdesk' ruser= 'R1' rem_addr= '192.168.1.10' priv=1 list=
AUTHOR-TYPE= 'commands'
Jan 7 20:59:10.067: AAA: parse name=tty388 idb type=-1 tty=-1
Jan 7 20:59:10.067: AAA: name=tty388 flags=0x11 type=5 shelf=0 slot=0 adapter=0 port=388 channel=0
Jan 7 20:59:10.067: AAA/MEMORY: create_user (0x3C4437DC) user='helpdesk' ruser='R1' ds0=0 port='tty388' rem_addr='
192.168.1.10' authen_type=ASCII service=NONE priv=1 initial_task_id='0', vrf= (id=0)
Jan 7 20:59:10.067: tty388 AAA/AUTHOR/CMD (853050497): Port='tty388' list=' service=CMD
Jan 7 20:59:10.067: AAA/AUTHOR/CMD: tty388 (853050497) user='helpdesk'
Jan 7 20:59:10.067: tty388 AAA/AUTHOR/CMD (853050497): send AV service=shell
Jan 7 20:59:10.067: tty388 AAA/AUTHOR/CMD (853050497): send AV cmd=show
Jan 7 20:59:10.067: tty388 AAA/AUTHOR/CMD (853050497): send AV cmd-arg=ip
Jan 7 20:59:10.067: tty388 AAA/AUTHOR/CMD (853050497): send AV cmd-arg=ospf
Jan 7 20:59:10.067: tty388 AAA/AUTHOR/CMD (853050497): send AV cmd-arg=database
Jan 7 20:59:10.067: tty388 AAA/AUTHOR/CMD (853050497): send AV cmd-arg=<cr>
Jan 7 20:59:10.067: tty388 AAA/AUTHOR/CMD (853050497): found list "default"
Jan 7 20:59:10.067: tty388 AAA/AUTHOR/CMD (853050497): Method=tacacs+ (tacacs+)
Jan 7 20:59:10.067: AAA/AUTHOR/TAC+: (853050497): user=helpdesk
Jan 7 20:59:10.067: AAA/AUTHOR/TAC+: (853050497): send AV service=shell
Jan 7 20:59:10.067: AAA/AUTHOR/TAC+: (853050497): send AV cmd=show
Jan 7 20:59:10.067: AAA/AUTHOR/TAC+: (853050497): send AV cmd-arg=ip
Jan 7 20:59:10.067: AAA/AUTHOR/TAC+: (853050497): send AV cmd-arg=ospf
Jan 7 20:59:10.067: AAA/AUTHOR/TAC+: (853050497): send AV cmd-arg=database
Jan 7 20:59:10.067: AAA/AUTHOR/TAC+: (853050497): send AV cmd-arg=<cr>
Jan 7 20:59:10.267: AAA/AUTHOR (853050497): Post authorization status = PASS_ADD
Jan 7 20:59:10.267: AAA/MEMORY: free_user (0x3C4437DC) user='helpdesk' ruser='R1' port='tty388' rem_addr='192.168.
1.10' authen_type=ASCII service=NONE priv=1 vrf= (id=0)

```

The ISE TACACS Logs confirms authentication and authorization succeed, matching the correct Authorization Policy **Helpdesk-AuthoZ**.

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Device ...	Network Device ID
Jan 07, 2020 09:05:53.431 PM	✓	🔒	helpdesk	Authorization	Authentication Policy	Authorization Policy	ISE	R1	192.168.1.1
Jan 07, 2020 09:04:05.929 PM	✗	🔒	helpdesk	Authorization	Default >> Helpdesk-AuthoZ	Default >> Helpdesk-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 09:03:20.922 PM	✗	🔒	helpdesk	Authorization	Default >> Helpdesk-AuthoZ	Default >> Helpdesk-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 09:00:23.914 PM	✗	🔒	helpdesk	Authorization	Default >> Helpdesk-AuthoZ	Default >> Helpdesk-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 08:58:45.185 PM	✗	🔒	helpdesk	Authorization	Default >> Helpdesk-AuthoZ	Default >> Helpdesk-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 08:54:07.202 PM	✓	🔒	helpdesk	Authorization	Default >> Default	Default >> Helpdesk-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 08:54:07.169 PM	✓	🔒	helpdesk	Authentication	Default >> Default	Default >> Helpdesk-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 08:46:02.049 PM	✓	🔒	helpdesk	Authorization	Default >> Default	Default >> Helpdesk-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 08:46:02.015 PM	✓	🔒	helpdesk	Authentication	Default >> Default	Default >> Helpdesk-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 08:41:12.317 PM	✓	🔒	helpdesk	Authorization	Default >> Default	Default >> Helpdesk-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 08:41:12.288 PM	✓	🔒	helpdesk	Authentication	Default >> Default	Default >> Helpdesk-AuthoZ	ISE	R1	192.168.1.1

Overview

Request Type	Authorization
Status	Pass
Session Key	ISE/363103442/208
Message Text	Device-Administration: Command Authorization succeeded
Username	helpdesk
Authorization Policy	Default >> Helpdesk-AuthoZ
Shell Profile	
Matched Command Set	CMD_Priv_8
Command From Device	show ip ospf database

Authorization Details

Generated Time	2020-01-07 21:05:53.431 +0:00
Logged Time	2020-01-07 21:05:53.431
Epoch Time (sec)	1578431153
ISE Node	ISE
Message Text	Device-Administration: Command Authorization succeeded
Failure Reason	
Resolution	
Root Cause	
Username	helpdesk
Network Device Name	R1
Network Device IP	192.168.1.1
Network Device Groups	IPSEC#Is IPSEC Device#No_Location#All Locations#New-York,Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations#New-York
Device Port	tty388
Remote Address	192.168.1.10

Type the **show ip route** command from the SSH session, the command is executed successfully.

```
192.168.1.1 - PuTTY
R1#
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default, U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
       a - application route
       + - replicated route, % - next hop override

Gateway of last resort is not set

 10.0.0.0/24 is subnetted, 1 subnets
 D    10.1.6.0 [90/284160] via 192.168.1.2, 03:25:30, GigabitEthernet0/0
 192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
 C    192.168.1.0/24 is directly connected, GigabitEthernet0/0
 L    192.168.1.1/32 is directly connected, GigabitEthernet0/0
R1#
```

The **Post authorization status = PASS_ADD** is displayed in the debug output.

Copyright 2021 Redouane Meddane. Consumers may download and use this document for personal use only. Downloading and editing this document for redistribution is prohibited. All rights reserved.

```

R1#
Jan 7 21:02:18.507: AAA/AUTHOR: auth_need : user= 'helpdesk' ruser= 'R1' rem_addr= '192.168.1.10' priv= 1 list= ''
AUTHOR-TYPE= 'commands'
Jan 7 21:02:18.507: AAA: parse name=tty388 idb type=-1 tty=-1
Jan 7 21:02:18.507: AAA: name=tty388 flags=0x11 type=5 shelf=0 slot=0 adapter=0 port=388 channel=0
Jan 7 21:02:18.507: AAA/MEMORY: create_user (0x3C4437DC) user='helpdesk' ruser='R1' ds0=0 port='tty388' rem_addr='
192.168.1.10' authen_type=ASCII service=NONE priv=1 initial_task_id='0' vrf=(id=0)
Jan 7 21:02:18.507: tty388 AAA/AUTHOR/CMD (2576375961): Port='tty388' list='' service=CMD
Jan 7 21:02:18.507: AAA/AUTHOR/CMD: tty388 (2576375961) user='helpdesk'
Jan 7 21:02:18.507: tty388 AAA/AUTHOR/CMD (2576375961): send AV service=shell
Jan 7 21:02:18.507: tty388 AAA/AUTHOR/CMD (2576375961): send AV cmd=show
Jan 7 21:02:18.507: tty388 AAA/AUTHOR/CMD (2576375961): send AV cmd-arg=ip
Jan 7 21:02:18.507: tty388 AAA/AUTHOR/CMD (2576375961): send AV cmd-arg=route
Jan 7 21:02:18.507: tty388 AAA/AUTHOR/CMD (2576375961): send AV cmd-arg=<cr>
Jan 7 21:02:18.507: tty388 AAA/AUTHOR/CMD (2576375961): found list "default"
Jan 7 21:02:18.507: tty388 AAA/AUTHOR/CMD (2576375961): Method=tacacs+ (tacacs+)
Jan 7 21:02:18.507: AAA/AUTHOR/TAC+: (2576375961): user=helpdesk
Jan 7 21:02:18.507: AAA/AUTHOR/TAC+: (2576375961): send AV service=shell
Jan 7 21:02:18.507: AAA/AUTHOR/TAC+: (2576375961): send AV cmd=show
Jan 7 21:02:18.507: AAA/AUTHOR/TAC+: (2576375961): send AV cmd-arg=ip
Jan 7 21:02:18.507: AAA/AUTHOR/TAC+: (2576375961): send AV cmd-arg=route
Jan 7 21:02:18.507: AAA/AUTHOR/TAC+: (2576375961): send AV cmd-arg=<cr>
Jan 7 21:02:18.711: AAA/AUTHOR (2576375961): Post authorization status = PASS_ADD
Jan 7 21:02:18.711: AAA/MEMORY: free_user (0x3C4437DC) user='helpdesk' ruser='R1' port='tty388' rem_addr='192.168.
1.10' authen_type=ASCII service=NONE priv=1 vrf=(id=0)
R1#

```

The ISE TACACS Logs confirms Authentication and authorization succeed, matching the correct Authorization Policy **Helpdesk-AuthoZ** and correct Command Sets **CMD_Priv_8**.

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Device ...	Network Device
Jan 07, 2020 09:09:01 903 PM	✓	🔒	helpdesk	Authorization	Authentication Policy	Authorization Policy	ISE	R1	192.168.1.1
Jan 07, 2020 09:05:53 431 PM	✓	🔒	helpdesk	Authorization	Default >> Helpdesk-AuthoZ	Default >> Helpdesk-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 09:04:05 929 PM	✗	🔒	helpdesk	Authorization	Default >> Helpdesk-AuthoZ	Default >> Helpdesk-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 09:03:20 922 PM	✗	🔒	helpdesk	Authorization	Default >> Helpdesk-AuthoZ	Default >> Helpdesk-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 09:00:23 914 PM	✗	🔒	helpdesk	Authorization	Default >> Helpdesk-AuthoZ	Default >> Helpdesk-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 08:58:45 185 PM	✗	🔒	helpdesk	Authorization	Default >> Helpdesk-AuthoZ	Default >> Helpdesk-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 08:54:07 202 PM	✓	🔒	helpdesk	Authorization	Default >> Helpdesk-AuthoZ	Default >> Helpdesk-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 08:54:07 169 PM	✓	🔒	helpdesk	Authentication	Default >> Default	Default >> Default	ISE	R1	192.168.1.1
Jan 07, 2020 08:46:02 049 PM	✓	🔒	helpdesk	Authorization	Default >> Helpdesk-AuthoZ	Default >> Helpdesk-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 08:46:02 015 PM	✓	🔒	helpdesk	Authentication	Default >> Default	Default >> Default	ISE	R1	192.168.1.1
Jan 07, 2020 08:41:12 317 PM	✓	🔒	helpdesk	Authorization	Default >> Helpdesk-AuthoZ	Default >> Helpdesk-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 08:41:12 288 PM	✓	🔒	helpdesk	Authentication	Default >> Default	Default >> Default	ISE	R1	192.168.1.1

Overview

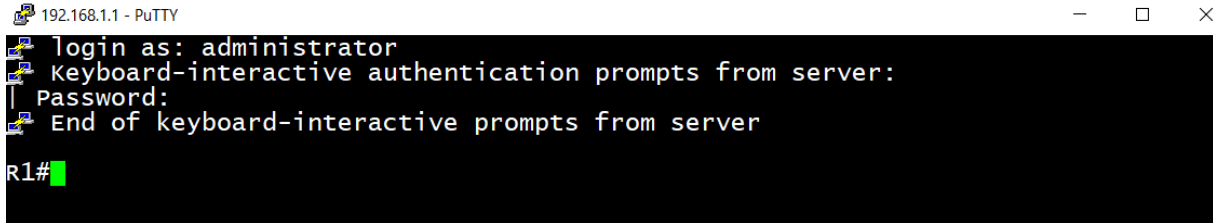
Request Type	Authorization
Status	Pass
Session Key	ISE/363103442/209
Message Text	Device-Administration: Command Authorization succeeded
Username	helpdesk
Authorization Policy	Default >> Helpdesk-AuthoZ
Shell Profile	
Matched Command Set	CMD_Priv_8
Command From Device	show ip route

Authorization Details

Generated Time	2020-01-07 21:09:01.903 +0:00
Logged Time	2020-01-07 21:09:01.903
Epoch Time (sec)	1578431341
ISE Node	ISE
Message Text	Device-Administration: Command Authorization succeeded
Failure Reason	
Resolution	
Root Cause	
Username	helpdesk
Network Device Name	R1
Network Device IP	192.168.1.1
Network Device Groups	IPSEC#s IPSEC Device#No,Location#All Locations#New-York,Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations#New-York
Device Port	tty388
Remote Address	192.168.1.10

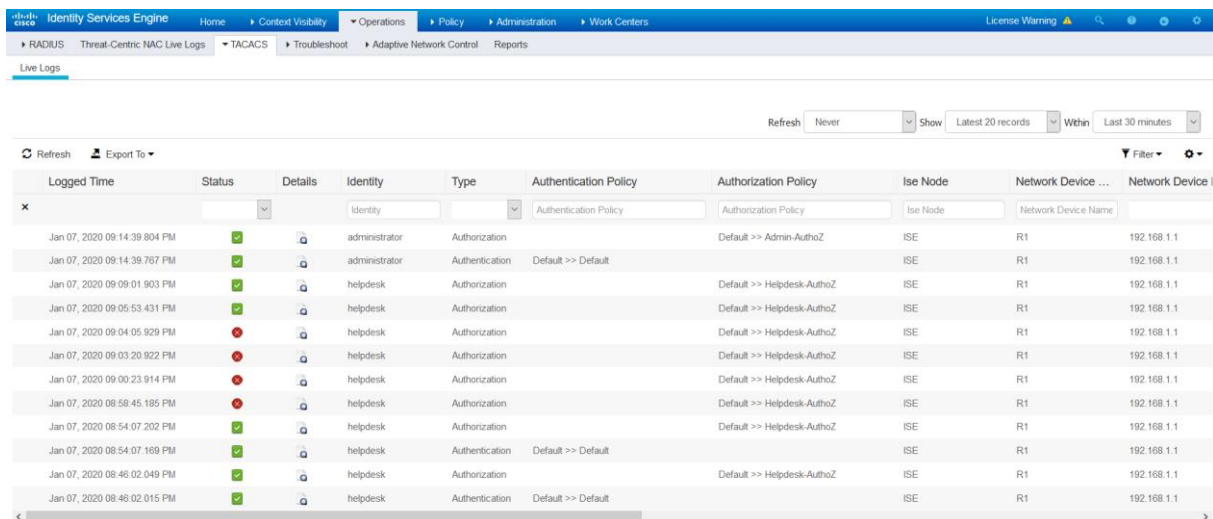
Return to your **Admin PC**, and use PUTTY to open an SSH session to **R1** router (**192.168.1.1**).

Login using the credentials **administrator / Admin123**.



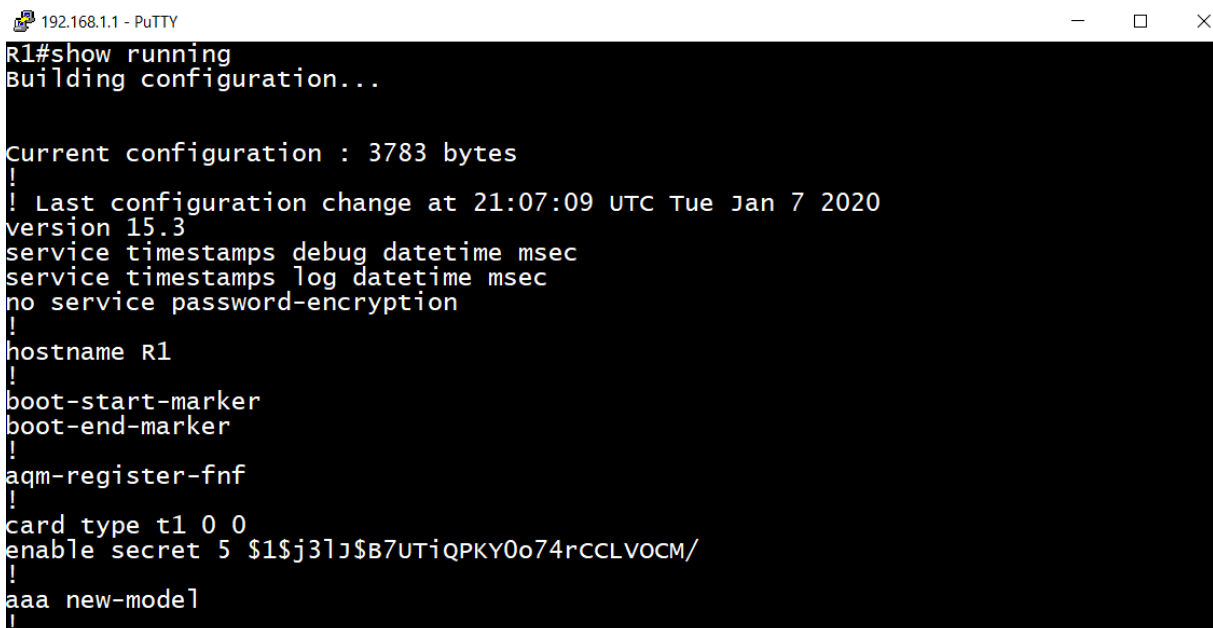
```
192.168.1.1 - PuTTY
login as: administrator
Keyboard-interactive authentication prompts from server:
Password:
End of keyboard-interactive prompts from server
R1#
```

Navigate to **Operations > TACACS > Live Logs** to see that the authentication and authorization are successful.



Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Device ...	Network Device
Jan 07, 2020 09:14:39 804 PM	✓	🔒	administrator	Authorization	Default >> Default	Default >> Admin-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 09:14:39 767 PM	✓	🔒	administrator	Authentication	Default >> Default		ISE	R1	192.168.1.1
Jan 07, 2020 09:09:01 903 PM	✓	🔒	helpdesk	Authorization	Default >> Helpdesk-AuthoZ	Default >> Helpdesk-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 09:05:53 431 PM	✓	🔒	helpdesk	Authorization	Default >> Helpdesk-AuthoZ	Default >> Helpdesk-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 09:04:05 929 PM	✗	🔒	helpdesk	Authorization	Default >> Helpdesk-AuthoZ	Default >> Helpdesk-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 09:03:20 922 PM	✗	🔒	helpdesk	Authorization	Default >> Helpdesk-AuthoZ	Default >> Helpdesk-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 09:00:23 914 PM	✗	🔒	helpdesk	Authorization	Default >> Helpdesk-AuthoZ	Default >> Helpdesk-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 08:58:45 185 PM	✗	🔒	helpdesk	Authorization	Default >> Helpdesk-AuthoZ	Default >> Helpdesk-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 08:54:07 202 PM	✓	🔒	helpdesk	Authorization	Default >> Helpdesk-AuthoZ	Default >> Helpdesk-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 08:54:07 169 PM	✓	🔒	helpdesk	Authentication	Default >> Default		ISE	R1	192.168.1.1
Jan 07, 2020 08:46:02 049 PM	✓	🔒	helpdesk	Authorization	Default >> Helpdesk-AuthoZ	Default >> Helpdesk-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 08:46:02 015 PM	✓	🔒	helpdesk	Authentication	Default >> Default		ISE	R1	192.168.1.1

From the SSH session, execute the **show running** command, the authorization is successful because the **administrator** user has full access to all commands.



```
R1#show running
Building configuration...

current configuration : 3783 bytes
!
! Last configuration change at 21:07:09 UTC Tue Jan 7 2020
version 15.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
aqm-register-fnf
!
card type t1 0 0
enable secret 5 $1$j3lJ$B7UTiQPKY0o74rcCLVOCM/
!
aaa new-model
!
```

Let's check the **debug aaa authorization** output, it seems that the router does not request the ISE server for command authorization.

```
R1#
Jan 7 21:09:20.879: AAA/AUTHOR: auth_need : user= 'administrator' ruser= 'R1' rem_addr= '192.168.1.10' priv= 15 list= '' AUTHOR-TYPE= 'commands'
R1#
```

In the TACACS Live Logs, there is no authorization request received by the ISE server from the router R1.

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Device Name	Network Device IP
Jan 07, 2020 09:14:39 804 PM	✓	🔒	administrator	Authorization	Authentication Policy	Authorization Policy	ISE	R1	192.168.1.1
Jan 07, 2020 09:14:39 767 PM	✓	🔒	administrator	Authentication	Default >> Default		ISE	R1	192.168.1.1
Jan 07, 2020 09:09:01 903 PM	✓	🔒	helpdesk	Authorization	Default >> Helpdesk-AuthoZ		ISE	R1	192.168.1.1
Jan 07, 2020 09:05:53 431 PM	✓	🔒	helpdesk	Authorization	Default >> Helpdesk-AuthoZ		ISE	R1	192.168.1.1
Jan 07, 2020 09:04:05 929 PM	✗	🔒	helpdesk	Authorization	Default >> Helpdesk-AuthoZ		ISE	R1	192.168.1.1
Jan 07, 2020 09:03:20 922 PM	✗	🔒	helpdesk	Authorization	Default >> Helpdesk-AuthoZ		ISE	R1	192.168.1.1
Jan 07, 2020 09:00:23 914 PM	✗	🔒	helpdesk	Authorization	Default >> Helpdesk-AuthoZ		ISE	R1	192.168.1.1
Jan 07, 2020 08:58:45 185 PM	✗	🔒	helpdesk	Authorization	Default >> Helpdesk-AuthoZ		ISE	R1	192.168.1.1
Jan 07, 2020 08:54:07 202 PM	✓	🔒	helpdesk	Authorization	Default >> Helpdesk-AuthoZ		ISE	R1	192.168.1.1
Jan 07, 2020 08:54:07 169 PM	✓	🔒	helpdesk	Authentication	Default >> Default		ISE	R1	192.168.1.1

Let's do a deep inspection, from the SSH session let's execute the **show ip route** command, the action succeeds.

```
192.168.1.1 - PuTTY
R1#
R1#
R1#show ip route
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
o - ODR, P - periodic downloaded static route, H - NHRP, l - LISP
a - application route
+ - replicated route, % - next hop override

Gateway of last resort is not set

10.0.0.0/24 is subnetted, 1 subnets
D 10.1.6.0 [90/284160] via 192.168.1.2, 03:34:18, GigabitEthernet0/0
192.168.1.0/24 is variably subnetted, 2 subnets, 2 masks
C 192.168.1.0/24 is directly connected, GigabitEthernet0/0
L 192.168.1.1/32 is directly connected, GigabitEthernet0/0
R1#
R1#
```

Let's verify the debug output, unlike with the **show running** command, the **show ip route** command authorization is sent to the ISE server. The output shown **Post authorization status=PASS_ADD**.


```

R1#
Jan 7 21:11:06.227: AAA/AUTHOR: auth_need : user= 'administrator' ruser= 'R1' rem_addr= '192.168.1.10' priv= 1 list
= '
AUTHOR-TYPE= 'commands'
Jan 7 21:11:06.227: AAA: parse name=tty388 idb type=-1 tty=-1
Jan 7 21:11:06.227: AAA: name=tty388 flags=0x11 type=5 shelf=0 slot=0 adapter=0 port=388 channel=0
Jan 7 21:11:06.227: AAA/MEMORY: create_user (0x3C4437DC) user='administrator' ruser='R1' ds0=0 port='tty388' rem_a
ddr='192.168.1.10' authen_type=ASCII service=NONE priv=1 initial_task_id='0', vrf= (id=0)
Jan 7 21:11:06.227: tty388 AAA/AUTHOR/CMD (4049124404): Port='tty388' list=' service=CMD
Jan 7 21:11:06.227: AAA/AUTHOR/CMD: tty388 (4049124404) user='administrator'
Jan 7 21:11:06.227: tty388 AAA/AUTHOR/CMD (4049124404): send AV service=shell
Jan 7 21:11:06.227: tty388 AAA/AUTHOR/CMD (4049124404): send AV cmd=show
Jan 7 21:11:06.227: tty388 AAA/AUTHOR/CMD (4049124404): send AV cmd-arg=ip
Jan 7 21:11:06.227: tty388 AAA/AUTHOR/CMD (4049124404): send AV cmd-arg=route
Jan 7 21:11:06.227: tty388 AAA/AUTHOR/CMD (4049124404): send AV cmd-arg=<cr>
Jan 7 21:11:06.227: tty388 AAA/AUTHOR/CMD (4049124404): found list "default"
Jan 7 21:11:06.227: tty388 AAA/AUTHOR/CMD (4049124404): Method=tacacs+ (tacacs+)
Jan 7 21:11:06.227: AAA/AUTHOR/TAC+: (4049124404): user=administrator
Jan 7 21:11:06.227: AAA/AUTHOR/TAC+: (4049124404): send AV service=shell
Jan 7 21:11:06.227: AAA/AUTHOR/TAC+: (4049124404): send AV cmd=show
Jan 7 21:11:06.227: AAA/AUTHOR/TAC+: (4049124404): send AV cmd-arg=ip
Jan 7 21:11:06.227: AAA/AUTHOR/TAC+: (4049124404): send AV cmd-arg=route
Jan 7 21:11:06.227: AAA/AUTHOR/TAC+: (4049124404): send AV cmd-arg=<cr>
Jan 7 21:11:06.527: AAA/AUTHOR (4049124404): Post authorization status = PASS_ADD
Jan 7 21:11:06.527: AAA/MEMORY: free_user (0x3C4437DC) user='administrator' ruser='R1' port='tty388' rem_addr='192
.168.1.10' authen_type=ASCII service=NONE priv=1 vrf= (id=0)
R1#

```

Navigate to **Operations > TACACS > Live Logs** to see that the authentication and authorization are successful.

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Device	Network Device ID
Jan 07, 2020 09:17:49.727 PM	✓		administrator	Authorization	Default >> Admin-AuthoZ	Default >> Admin-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 09:14:39.804 PM	✓		administrator	Authorization	Default >> Admin-AuthoZ	Default >> Admin-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 09:14:39.767 PM	✓		administrator	Authentication	Default >> Default	Default >> Admin-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 09:09:01.903 PM	✓		helpdesk	Authorization	Default >> Helpdesk-AuthoZ	Default >> Helpdesk-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 09:05:53.431 PM	✓		helpdesk	Authorization	Default >> Helpdesk-AuthoZ	Default >> Helpdesk-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 09:04:05.929 PM	✗		helpdesk	Authorization	Default >> Helpdesk-AuthoZ	Default >> Helpdesk-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 09:03:20.922 PM	✗		helpdesk	Authorization	Default >> Helpdesk-AuthoZ	Default >> Helpdesk-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 09:00:23.914 PM	✗		helpdesk	Authorization	Default >> Helpdesk-AuthoZ	Default >> Helpdesk-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 08:58:45.185 PM	✗		helpdesk	Authorization	Default >> Helpdesk-AuthoZ	Default >> Helpdesk-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 08:54:07.202 PM	✓		helpdesk	Authorization	Default >> Helpdesk-AuthoZ	Default >> Helpdesk-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 08:54:07.169 PM	✓		helpdesk	Authentication	Default >> Default	Default >> Helpdesk-AuthoZ	ISE	R1	192.168.1.1

The ISE TACACS Logs confirms Authentication and Authorization succeed, matching the correct Authorization Policy **Admin-AuthoZ** and correct Command Sets **CMD_Priv_15**.

Overview

Request Type	Authorization
Status	Pass
Session Key	ISE/363103442/214
Message Text	Device-Administration: Command Authorization succeeded
Username	administrator
Authorization Policy	Default >> Admin-AuthoZ
Shell Profile	
Matched Command Set	CMD_Priv_15
Command From Device	show ip route

Authorization Details

Generated Time	2020-01-07 21:17:49.727 +0:00
Logged Time	2020-01-07 21:17:49.727
Epoch Time (sec)	1578431869
ISE Node	ISE
Message Text	Device-Administration: Command Authorization succeeded
Failure Reason	
Resolution	
Root Cause	
Username	administrator
Network Device Name	R1
Network Device IP	192.168.1.1
Network Device Groups	IPSEC#s IPSEC Device#No,Location#All Locations#New-York,Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations#New-York
Device Port	tty388
Remote Address	192.168.1.10

Let's confirm, from the SSH session let's execute the **show ip ospf database** command, the action succeeds.

```

192.168.1.1 - PuTTY
R1#
R1#
R1#
R1#
R1#show ip ospf data
R1#
R1#
R1#

```

Let's verify the debug output. The output shown **Post authorization status=PASS_ADD**.

```

Jan 7 21:13:39.475: AAA/AUTHOR: auth_need : user= 'administrator' ruser= 'R1' rem_addr= '192.168.1.10' priv=1 list
= ' ' AUTHOR-TYPE= 'commands'
Jan 7 21:13:39.475: AAA: parse name=tty388 idb type=-1 tty=-1
Jan 7 21:13:39.475: AAA: name=tty388 flags=0x11 type=5 shelf=0 slot=0 adapter=0 port=388 channel=0
Jan 7 21:13:39.475: AAA/MEMORY: create_user (0x224E6570) user='administrator' ruser='R1' ds0=0 port='tty388' rem_a
ddr='192.168.1.10' authen_type=ASCII service=NONE priv=1 initial_task_id='0', vrf= (id=0)
Jan 7 21:13:39.475: tty388 AAA/AUTHOR/CMD (1276788080): Port='tty388' list=' ' service=CMD
Jan 7 21:13:39.475: tty388 AAA/AUTHOR/CMD (1276788080) user= 'administrator'
Jan 7 21:13:39.475: tty388 AAA/AUTHOR/CMD (1276788080): send AV service=shell
Jan 7 21:13:39.475: tty388 AAA/AUTHOR/CMD (1276788080): send AV cmd=show
Jan 7 21:13:39.475: tty388 AAA/AUTHOR/CMD (1276788080): send AV cmd-arg=ip
Jan 7 21:13:39.475: tty388 AAA/AUTHOR/CMD (1276788080): send AV cmd-arg=ospf
Jan 7 21:13:39.475: tty388 AAA/AUTHOR/CMD (1276788080): send AV cmd-arg=database
Jan 7 21:13:39.475: tty388 AAA/AUTHOR/CMD (1276788080): send AV cmd-arg=<cr>
Jan 7 21:13:39.475: tty388 AAA/AUTHOR/CMD (1276788080): found list "default"
Jan 7 21:13:39.475: tty388 AAA/AUTHOR/CMD (1276788080): Method=tacacs+ (tacacs+)
Jan 7 21:13:39.475: AAA/AUTHOR/TAC+: (1276788080): user=administrator
Jan 7 21:13:39.475: AAA/AUTHOR/TAC+: (1276788080): send AV service=shell
Jan 7 21:13:39.475: AAA/AUTHOR/TAC+: (1276788080): send AV cmd=show
Jan 7 21:13:39.475: AAA/AUTHOR/TAC+: (1276788080): send AV cmd-arg=ip
Jan 7 21:13:39.475: AAA/AUTHOR/TAC+: (1276788080): send AV cmd-arg=ospf
Jan 7 21:13:39.475: AAA/AUTHOR/TAC+: (1276788080): send AV cmd-arg=database
Jan 7 21:13:39.475: AAA/AUTHOR/TAC+: (1276788080): send AV cmd-arg=<cr>
Jan 7 21:13:39.679: AAA/AUTHOR (1276788080): Post authorization status = PASS_ADD
Jan 7 21:13:39.679: AAA/MEMORY: free_user (0x224E6570) user='administrator' ruser='R1' port='tty388' rem_addr='192
.168.1.10' authen_type=ASCII service=NONE priv=1 vrf= (id=0)

```

The ISE TACACS Logs confirms Authentication and Authorization succeed, matching the correct Authorization Policy **Admin-AuthoZ** and correct Command Sets **CMD_Priv_15**.

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Device ...	Network Device
Jan 07, 2020 09:20:22 843 PM	✓		administrator	Authorization	Authentication Policy	Authorization Policy	Ise Node	R1	192.168.1.1
Jan 07, 2020 09:17:49 727 PM	✓		administrator	Authorization	Default >> Admin-AuthoZ	Default >> Admin-AuthoZ	Ise	R1	192.168.1.1
Jan 07, 2020 09:14:39 804 PM	✓		administrator	Authorization	Default >> Admin-AuthoZ	Default >> Admin-AuthoZ	Ise	R1	192.168.1.1
Jan 07, 2020 09:14:39 767 PM	✓		administrator	Authentication	Default >> Default		Ise	R1	192.168.1.1
Jan 07, 2020 09:05:53 903 PM	✓		helpdesk	Authorization	Default >> Helpdesk-AuthoZ	Default >> Helpdesk-AuthoZ	Ise	R1	192.168.1.1
Jan 07, 2020 09:05:53 431 PM	✓		helpdesk	Authorization	Default >> Helpdesk-AuthoZ	Default >> Helpdesk-AuthoZ	Ise	R1	192.168.1.1
Jan 07, 2020 09:04:05 929 PM	✗		helpdesk	Authorization	Default >> Helpdesk-AuthoZ	Default >> Helpdesk-AuthoZ	Ise	R1	192.168.1.1
Jan 07, 2020 09:03:20 922 PM	✗		helpdesk	Authorization	Default >> Helpdesk-AuthoZ	Default >> Helpdesk-AuthoZ	Ise	R1	192.168.1.1
Jan 07, 2020 09:00:23 914 PM	✗		helpdesk	Authorization	Default >> Helpdesk-AuthoZ	Default >> Helpdesk-AuthoZ	Ise	R1	192.168.1.1
Jan 07, 2020 08:58:45 185 PM	✗		helpdesk	Authorization	Default >> Helpdesk-AuthoZ	Default >> Helpdesk-AuthoZ	Ise	R1	192.168.1.1
Jan 07, 2020 08:54:07 202 PM	✓		helpdesk	Authorization	Default >> Helpdesk-AuthoZ	Default >> Helpdesk-AuthoZ	Ise	R1	192.168.1.1
Jan 07, 2020 08:54:07 169 PM	✓		helpdesk	Authentication	Default >> Default		Ise	R1	192.168.1.1

Overview

Request Type	Authorization
Status	Pass
Session Key	ISE/363103442/215
Message Text	Device-Administration: Command Authorization succeeded
Username	administrator
Authorization Policy	Default >> Admin-AuthoZ
Shell Profile	
Matched Command Set	CMD_Priv_15
Command From Device	show ip ospf database

Authorization Details

Generated Time	2020-01-07 21:20:22.843 +0:00
Logged Time	2020-01-07 21:20:22.843
Epoch Time (sec)	1578432022
ISE Node	ISE
Message Text	Device-Administration: Command Authorization succeeded
Failure Reason	
Resolution	
Root Cause	
Username	administrator
Network Device Name	R1
Network Device IP	192.168.1.1
Network Device Groups	IPSEC#s IPSEC Device#No,Location#All Locations#New-York,Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations#New-York
Device Port	tty388
Remote Address	192.168.1.10

To confirm let's execute the **configure terminal** command.

```
192.168.1.1 - PuTTY
R1#
R1#
R1#
R1#
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#
R1(config)#
```

From the debug output, the router shown that it does not request the ISE server for command authorization.

```
R1#
Jan  8 07:02:32.691: AAA/AUTHOR: auth_need : user= 'administrator' ruser= 'R1' rem_addr= '192.168.1.10' priv= 15 lis
t= '' AUTHOR-TYPE= 'commands'
R1#
```

The reason is that the **show running** and **configure terminal** commands are available at the privilege level 15 and the router is not yet configured to send the commands at the level 15 to ISE server.

Configure the router so that the Authorization for all commands at specified level 15 will be sent to ISE server

```
R1(config)#aaa authorization commands 15 default group tacacs+ local
```

From the SSH session, execute the **show running** command.

```
192.168.1.1 - PuTTY
R1#
R1#sh running
Building configuration...

Current configuration : 3859 bytes
!
! Last configuration change at 21:20:55 UTC Tue Jan 7 2020 by administrator
version 15.3
service timestamps debug datetime msec
service timestamps log datetime msec
no service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
aqm-register-fnf
!
card type t1 0 0
enable secret 5 $1$j3l1j$B7UTiQPKY0o74rCCLVOCM/
!
aaa new-model
!
!
aaa authentication login default group tacacs+ local
--More--
```

Notice the debug output, the console message shown that the router sent a request for command authorization with **Post authorization status=PASS_ADD**.

```

R1#
Jan 7 21:21:07.346: AAA/AUTHOR: auth_need : user= 'administrator' ruser= 'R1' rem_addr= '192.168.1.10' priv= 15 lis
t= ' ' AUTHOR-TYPE= 'commands'
Jan 7 21:21:07.346: AAA: parse name=tty388 idb type=-1 tty=-1
Jan 7 21:21:07.346: AAA: name=tty388 flags=0x11 type=5 shelf=0 slot=0 adapter=0 port=388 channel=0
Jan 7 21:21:07.346: AAA/MEMORY: create_user (0x3C4437DC) user='administrator' ruser='R1' ds0=0 port='tty388' rem_a
ddr='192.168.1.10' authen_type=ASCII service=NONE priv=15 initial_task_id='0'; vrf= (id=0)
Jan 7 21:21:07.346: tty388 AAA/AUTHOR/CMD (1086455481): Port='tty388' list=' ' service=CMD
Jan 7 21:21:07.346: AAA/AUTHOR/CMD: tty388 (1086455481) user='administrator'
Jan 7 21:21:07.346: tty388 AAA/AUTHOR/CMD (1086455481): send AV service=shell
Jan 7 21:21:07.346: tty388 AAA/AUTHOR/CMD (1086455481): send AV cmd=show
Jan 7 21:21:07.346: tty388 AAA/AUTHOR/CMD (1086455481): send AV cmd-arg=running-config
Jan 7 21:21:07.346: tty388 AAA/AUTHOR/CMD (1086455481): send AV cmd-arg=<cr>
Jan 7 21:21:07.346: tty388 AAA/AUTHOR/CMD (1086455481): found list "default"
Jan 7 21:21:07.346: tty388 AAA/AUTHOR/CMD (1086455481): Method=tacacs+ (tacacs+)
Jan 7 21:21:07.346: AAA/AUTHOR/TAC+: (1086455481): user=administrator
Jan 7 21:21:07.346: AAA/AUTHOR/TAC+: (1086455481): send AV service=shell
Jan 7 21:21:07.346: AAA/AUTHOR/TAC+: (1086455481): send AV cmd=show
Jan 7 21:21:07.346: AAA/AUTHOR/TAC+: (1086455481): send AV cmd-arg=running-config
Jan 7 21:21:07.346: AAA/AUTHOR/TAC+: (1086455481): send AV cmd-arg=<cr>
Jan 7 21:21:07.550: AAA/AUTHOR (1086455481): Post authorization status = PASS_ADD
Jan 7 21:21:07.550: AAA/MEMORY: free_user (0x3C4437DC) user='administrator' ruser='R1' port='tty388' rem_addr='192
.168.1.10' authen_type=ASCII service=NONE priv=15 vrf= (id=0)
R1#

```

The ISE TACACS Logs confirms Authentication and Authorization succeed, matching the correct Authorization Policy **Admin-AuthoZ** and correct Command Sets **CMD_Priv_15**.

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Device ...	Network Device I
Jan 07, 2020 09:27:50.714 PM	✓		administrator	Authorization	Default >> Admin-AuthoZ	Admin-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 09:23:46.693 PM	✓		administrator	Authorization	Default >> Admin-AuthoZ	Admin-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 09:23:19.415 PM	✓		administrator	Authorization	Default >> Admin-AuthoZ	Admin-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 09:20:22.843 PM	✓		administrator	Authorization	Default >> Admin-AuthoZ	Admin-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 09:17:49.727 PM	✓		administrator	Authorization	Default >> Admin-AuthoZ	Admin-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 09:14:39.804 PM	✓		administrator	Authorization	Default >> Admin-AuthoZ	Admin-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 09:14:39.767 PM	✓		administrator	Authentication	Default >> Default		ISE	R1	192.168.1.1
Jan 07, 2020 09:09:01.903 PM	✓		helpdesk	Authorization	Default >> Helpdesk-AuthoZ	Helpdesk-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 09:05:53.431 PM	✓		helpdesk	Authorization	Default >> Helpdesk-AuthoZ	Helpdesk-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 09:04:05.929 PM	✗		helpdesk	Authorization	Default >> Helpdesk-AuthoZ	Helpdesk-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 09:03:20.922 PM	✗		helpdesk	Authorization	Default >> Helpdesk-AuthoZ	Helpdesk-AuthoZ	ISE	R1	192.168.1.1
Jan 07, 2020 09:00:23.914 PM	✗		helpdesk	Authorization	Default >> Helpdesk-AuthoZ	Helpdesk-AuthoZ	ISE	R1	192.168.1.1

Overview

Request Type	Authorization
Status	Pass
Session Key	ISE/363103442/218
Message Text	Device-Administration: Command Authorization succeeded
Username	administrator
Authorization Policy	Default >> Admin-AuthoZ
Shell Profile	
Matched Command Set	CMD_Priv_15
Command From Device	show running-config

Authorization Details

Generated Time	2020-01-07 21:27:50.714 +0:00
Logged Time	2020-01-07 21:27:50.714
Epoch Time (sec)	1578432470
ISE Node	ISE
Message Text	Device-Administration: Command Authorization succeeded
Failure Reason	
Resolution	
Root Cause	
Username	administrator
Network Device Name	R1
Network Device IP	192.168.1.1
Network Device Groups	IPSEC#Is IPSEC Device#No,Location#All Locations#New-York,Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations#New-York
Device Port	tty388
Remote Address	192.168.1.10

Return to the SSH session and execute the **configure terminal** command.

```
192.168.1.1 - PuTTY
R1#
R1#
R1#
R1#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R1(config)#
R1(config)#
R1(config)#
R1(config)#
```

Notice the debug output, the console message shown that the router sent a request for command authorization with **Post authorization status=PASS_ADD**.

```

R1#
Jan 7 21:24:26.878: AAA/AUTHOR: auth_need : user= 'administrator' ruser= 'R1' rem_addr= '192.168.1.10' priv= 15 lis
t= ' ' AUTHOR-TYPE= 'commands'
Jan 7 21:24:26.878: AAA: parse name=tty388 idb type=-1 tty=-1
Jan 7 21:24:26.878: AAA: name=tty388 flags=0x11 type=5 shelf=0 slot=0 adapter=0 port=388 channel=0
Jan 7 21:24:26.878: AAA/MEMORY: create_user (0x3C4437DC) user='administrator' ruser='R1' ds0=0 port='tty388' rem_a
ddr='192.168.1.10' authen_type=ASCII service=NONE priv=15 initial_task_id='0', vrf= (id=0)
Jan 7 21:24:26.878: tty388 AAA/AUTHOR/CMD (527014365): Port='tty388' list=' ' service=CMD
Jan 7 21:24:26.878: AAA/AUTHOR/CMD: tty388 (527014365) user='administrator'
Jan 7 21:24:26.878: tty388 AAA/AUTHOR/CMD (527014365): send AV service=shell
Jan 7 21:24:26.878: tty388 AAA/AUTHOR/CMD (527014365): send AV cmd=configure
Jan 7 21:24:26.878: tty388 AAA/AUTHOR/CMD (527014365): send AV cmd-arg=terminal
Jan 7 21:24:26.878: tty388 AAA/AUTHOR/CMD (527014365): send AV cmd-arg=<cr>
Jan 7 21:24:26.878: tty388 AAA/AUTHOR/CMD (527014365): found list "default"
Jan 7 21:24:26.878: tty388 AAA/AUTHOR/CMD (527014365): Method=tacacs+ (tacacs+)
Jan 7 21:24:26.878: AAA/AUTHOR/TAC+: (527014365): user=administrator
Jan 7 21:24:26.878: AAA/AUTHOR/TAC+: (527014365): send AV service=shell
Jan 7 21:24:26.882: AAA/AUTHOR/TAC+: (527014365): send AV cmd=configure
Jan 7 21:24:26.882: AAA/AUTHOR/TAC+: (527014365): send AV cmd-arg=terminal
Jan 7 21:24:26.882: AAA/AUTHOR/TAC+: (527014365): send AV cmd-arg=<cr>
Jan 7 21:24:27.082: AAA/AUTHOR (527014365): Post authorization status = PASS_ADD
Jan 7 21:24:27.082: AAA/MEMORY: free_user (0x3C4437DC) user='administrator' ruser='R1' port='tty388' rem_addr='192
.168.1.10' authen_type=ASCII service=NONE priv=15 vrf= (id=0)
R1#

```

The ISE TACACS Logs confirms Authentication and Authorization succeed, matching the correct Authorization Policy **Admin-AuthoZ** and correct Command Sets **CMD_Priv_15**.

Overview	
Request Type	Authorization
Status	Pass
Session Key	ISE/363103442/219
Message Text	Device-Administration: Command Authorization succeeded
Username	administrator
Authorization Policy	Default >> Admin-AuthoZ
Shell Profile	
Matched Command Set	CMD_Priv_15
Command From Device	configure terminal

Authorization Details

Generated Time	2020-01-07 21:31:10.241 +0:00
Logged Time	2020-01-07 21:31:10.241
Epoch Time (sec)	1578432670
ISE Node	ISE
Message Text	Device-Administration: Command Authorization succeeded
Failure Reason	
Resolution	
Root Cause	
Username	administrator
Network Device Name	R1
Network Device IP	192.168.1.1
Network Device Groups	IPSEC#Is IPSEC Device#No,Location#All Locations#New-York,Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations#New-York
Device Port	tty388
Remote Address	192.168.1.10

What about the commands at the global configuration mode?
From the SSH session, access the global configuration mode.
Type the **router ospfv3 1** and **ipv6 unicast-routing** commands.

```
192.168.1.1 - PuTTY
R1(config)#
R1(config)#
R1(config)#
R1(config)#router OSPFv3 1
%OSPFv3: IPv6 routing not enabled
R1(config)#ipv6 unicast-routing
R1(config)#
R1(config)#router OSPFv3 1
R1(config-router)#
R1(config-router)#
```

From the console session, the router shown that no authorization request is sent to the ISE server, and a console message shown the authorization for config command are not enable.
Config command authorization not enabled

```

R1#
Jan 7 21:26:31.598: AAA/AUTHOR: auth_need : user= 'administrator' ruser= 'R1' rem_addr= '192.168.1.10' priv= 15 lis
t= 'AUTHOR-TYPE= 'commands'
Jan 7 21:26:31.598: AAA/AUTHOR: config command authorization not enabled
Jan 7 21:26:51.282: AAA/AUTHOR: auth_need : user= 'administrator' ruser= 'R1' rem_addr= '192.168.1.10' priv= 15 lis
t= 'AUTHOR-TYPE= 'commands'
Jan 7 21:26:51.282: AAA/AUTHOR: config command authorization not enabled
Jan 7 21:26:56.102: AAA/AUTHOR: auth_need : user= 'administrator' ruser= 'R1' rem_addr= '192.168.1.10' priv= 15 lis
t= 'AUTHOR-TYPE= 'commands'
Jan 7 21:26:56.102: AAA/AUTHOR: config command authorization not enabled
R1#

```

The screenshot shows the Cisco Identity Services Engine (ISE) Live Logs interface. The table displays the following data:

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Device ...	Network Device
Jan 07, 2020 09:31:10.241 PM	✓		administrator	Authorization	Default >> Admin-AuthoZ	Authorization Policy	ISE	R1	192.168.1.1
Jan 07, 2020 09:27:50.714 PM	✓		administrator	Authorization	Default >> Admin-AuthoZ		ISE	R1	192.168.1.1
Jan 07, 2020 09:23:46.683 PM	✓		administrator	Authorization	Default >> Admin-AuthoZ		ISE	R1	192.168.1.1
Jan 07, 2020 09:23:19.415 PM	✓		administrator	Authorization	Default >> Admin-AuthoZ		ISE	R1	192.168.1.1
Jan 07, 2020 09:20:22.843 PM	✓		administrator	Authorization	Default >> Admin-AuthoZ		ISE	R1	192.168.1.1
Jan 07, 2020 09:17:49.727 PM	✓		administrator	Authorization	Default >> Admin-AuthoZ		ISE	R1	192.168.1.1
Jan 07, 2020 09:14:39.804 PM	✓		administrator	Authorization	Default >> Admin-AuthoZ		ISE	R1	192.168.1.1
Jan 07, 2020 09:14:39.767 PM	✓		administrator	Authentication	Default >> Default		ISE	R1	192.168.1.1
Jan 07, 2020 09:09:01.903 PM	✓		helpdesk	Authorization	Default >> Helpdesk-AuthoZ		ISE	R1	192.168.1.1
Jan 07, 2020 09:05:53.431 PM	✓		helpdesk	Authorization	Default >> Helpdesk-AuthoZ		ISE	R1	192.168.1.1

To force the router to send a request to ISE server for command authorization at the global configuration mode level, enter the following command.

```
R1(config)#aaa authorization config-commands
```

From the SSH session, access the global configuration mode. Type the **router ospfv3 1** and **ipv6 unicast-routing** commands.

```

192.168.1.1 - PuTTY
R1(config)#
R1(config)#
R1(config)#
R1(config)#router OSPFv3 1
%OSPFV3: IPv6 routing not enabled
R1(config)#ipv6 unicast-routing
R1(config)#
R1(config)#router OSPFv3 1
R1(config-router)#
R1(config-router)#

```

From the console session.

Notice the debug output, the console message shown that the router sent a request for command authorization with **Post authorization status=PASS_ADD**.

```

R1#
Jan 7 21:30:15.638: AAA/AUTHOR: auth_need : user= 'administrator' ruser= 'R1' rem_addr= '192.168.1.10' priv= 15 list= ''
AUTHOR-TYPE= 'commands'
Jan 7 21:30:15.638: AAA: parse name=tty388 idb type=-1 tty=-1
Jan 7 21:30:15.638: AAA: name=tty388 flags=0x11 type=5 shelf=0 slot=0 adapter=0 port=388 channel=0
Jan 7 21:30:15.638: AAA/MEMORY: create_user (0x24080FB0) user='administrator' ruser='R1' ds0=0 port='tty388' rem_addr='192.168.1.10'
authen_type=ASCII service=NONE priv=15 initial_task_id='0' vrf= (id=0)
Jan 7 21:30:15.638: AAA/AUTHOR/CMD (1775872431): Port='tty388' list=' service=CMD
Jan 7 21:30:15.638: AAA/AUTHOR/CMD: tty388 (1775872431) user='administrator'
Jan 7 21:30:15.638: tty388 AAA/AUTHOR/CMD (1775872431): send AV service=shell
Jan 7 21:30:15.638: tty388 AAA/AUTHOR/CMD (1775872431): send AV cmd=router
Jan 7 21:30:15.638: tty388 AAA/AUTHOR/CMD (1775872431): send AV cmd-arg=ospfv3
Jan 7 21:30:15.638: tty388 AAA/AUTHOR/CMD (1775872431): send AV cmd-arg=1
Jan 7 21:30:15.638: tty388 AAA/AUTHOR/CMD (1775872431): send AV cmd-arg=<cr>
Jan 7 21:30:15.638: tty388 AAA/AUTHOR/CMD (1775872431): found list "default"
Jan 7 21:30:15.638: tty388 AAA/AUTHOR/CMD (1775872431): Method=tacacs+ (tacacs+)
Jan 7 21:30:15.638: AAA/AUTHOR/TAC+: (1775872431): user=administrator
Jan 7 21:30:15.638: AAA/AUTHOR/TAC+: (1775872431): send AV service=shell
Jan 7 21:30:15.638: AAA/AUTHOR/TAC+: (1775872431): send AV cmd=router
Jan 7 21:30:15.638: AAA/AUTHOR/TAC+: (1775872431): send AV cmd-arg=ospfv3
Jan 7 21:30:15.638: AAA/AUTHOR/TAC+: (1775872431): send AV cmd-arg=1
Jan 7 21:30:15.638: AAA/AUTHOR/TAC+: (1775872431): send AV cmd-arg=<cr>
Jan 7 21:30:15.842: AAA/AUTHOR (1775872431): Post authorization status = PASS_ADD
Jan 7 21:30:15.842: AAA/MEMORY: free_user (0x24080FB0) user='administrator' ruser='R1' port='tty388' rem_addr='192.168.1.10'
authen_type=ASCII service=NONE priv=15 vrf= (id=0)
R1#

```

The ISE TACACS Logs confirms Authentication and Authorization succeed, matching the correct Authorization Policy **Admin-AuthoZ** and correct Command Sets **CMD_Priv_15**.

Overview

Request Type	Authorization
Status	Pass
Session Key	ISE/363103442/221
Message Text	Device-Administration: Command Authorization succeeded
Username	administrator
Authorization Policy	Default >> Admin-AuthoZ
Shell Profile	
Matched Command Set	CMD_Priv_15
Command From Device	router ospfv3 1

Authorization Details

Generated Time	2020-01-07 21:36:59.001 +0:00
Logged Time	2020-01-07 21:36:59.001
Epoch Time (sec)	1578433019
ISE Node	ISE
Message Text	Device-Administration: Command Authorization succeeded
Failure Reason	
Resolution	
Root Cause	
Username	administrator
Network Device Name	R1
Network Device IP	192.168.1.1
Network Device Groups	IPSEC#Is IPSEC Device#No_Location#All Locations#New-York,Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations#New-York
Device Port	tty388
Remote Address	192.168.1.10

Return to the SSH session, under the router configuration mode, execute the **compatible rfc1587** command.

```
192.168.1.1 - PuTTY
R1(config-router)#
R1(config-router)#exit
R1(config)#
R1(config)#
R1(config)#router OSPFv3 1
R1(config-router)#compatible rfc1587
R1(config-router)#
R1(config-router)#
R1(config-router)#
```

From the console session.

Notice the debug output, the console message shown that the router sent a request for command authorization with **Post authorization status=PASS_ADD** for the **compatible rfc1587** command.

```

RI#
Jan 7 21:32:57.282: AAA/AUTHOR: auth_need : user= 'administrator' ruser= 'R1' rem_addr= '192.168.1.10' priv= 15 list= ''
AUTHOR-TYPE= 'commands'
Jan 7 21:32:57.286: AAA: parse name=tty388 idb type=-1 tty=-1
Jan 7 21:32:57.286: AAA: name=tty388 flags=0x11 type=5 shelf=0 slot=0 adapter=0 port=388 channel=0
Jan 7 21:32:57.286: AAA/MEMORY: create_user (0x24080FB0) user='administrator' ruser='R1' ds0=0 port='tty388' rem_addr='192.168.1.10'
authen_type=ASCII service=NONE priv=15 initial_task_id='0' vrf= (id=0)
Jan 7 21:32:57.286: tty388 AAA/AUTHOR/CMD (4291384701): Port='tty388' list=''; service=CMD
Jan 7 21:32:57.286: AAA/AUTHOR/CMD: tty388 (4291384701) user='administrator'
Jan 7 21:32:57.286: tty388 AAA/AUTHOR/CMD (4291384701): send AV service=shell
Jan 7 21:32:57.286: tty388 AAA/AUTHOR/CMD (4291384701): send AV cmd=compatible
Jan 7 21:32:57.286: tty388 AAA/AUTHOR/CMD (4291384701): send AV cmd-arg=rfc1587
Jan 7 21:32:57.286: tty388 AAA/AUTHOR/CMD (4291384701): send AV cmd-arg=<cr>
Jan 7 21:32:57.286: tty388 AAA/AUTHOR/CMD (4291384701): found list "default"
Jan 7 21:32:57.286: tty388 AAA/AUTHOR/CMD (4291384701): Method=tacacs+ (tacacs+)
Jan 7 21:32:57.286: AAA/AUTHOR/TAC+: (4291384701): user=administrator
Jan 7 21:32:57.286: AAA/AUTHOR/TAC+: (4291384701): send AV service=shell
Jan 7 21:32:57.286: AAA/AUTHOR/TAC+: (4291384701): send AV cmd=compatible
Jan 7 21:32:57.286: AAA/AUTHOR/TAC+: (4291384701): send AV cmd-arg=rfc1587
Jan 7 21:32:57.286: AAA/AUTHOR/TAC+: (4291384701): send AV cmd-arg=<cr>
Jan 7 21:32:57.486: AAA/AUTHOR (4291384701): Post authorization status = PASS_ADD
Jan 7 21:32:57.486: AAA/MEMORY: free_user (0x24080FB0) user='administrator' ruser='R1' port='tty388' rem_addr='192.168.1.10'
authen_type=ASCII service=NONE priv=15 vrf= (id=0)
RI#

```

The ISE TACACS Logs confirms Authentication and Authorization succeed, matching the correct Authorization Policy **Admin-AuthoZ** and correct Command Sets **CMD_Priv_15**.

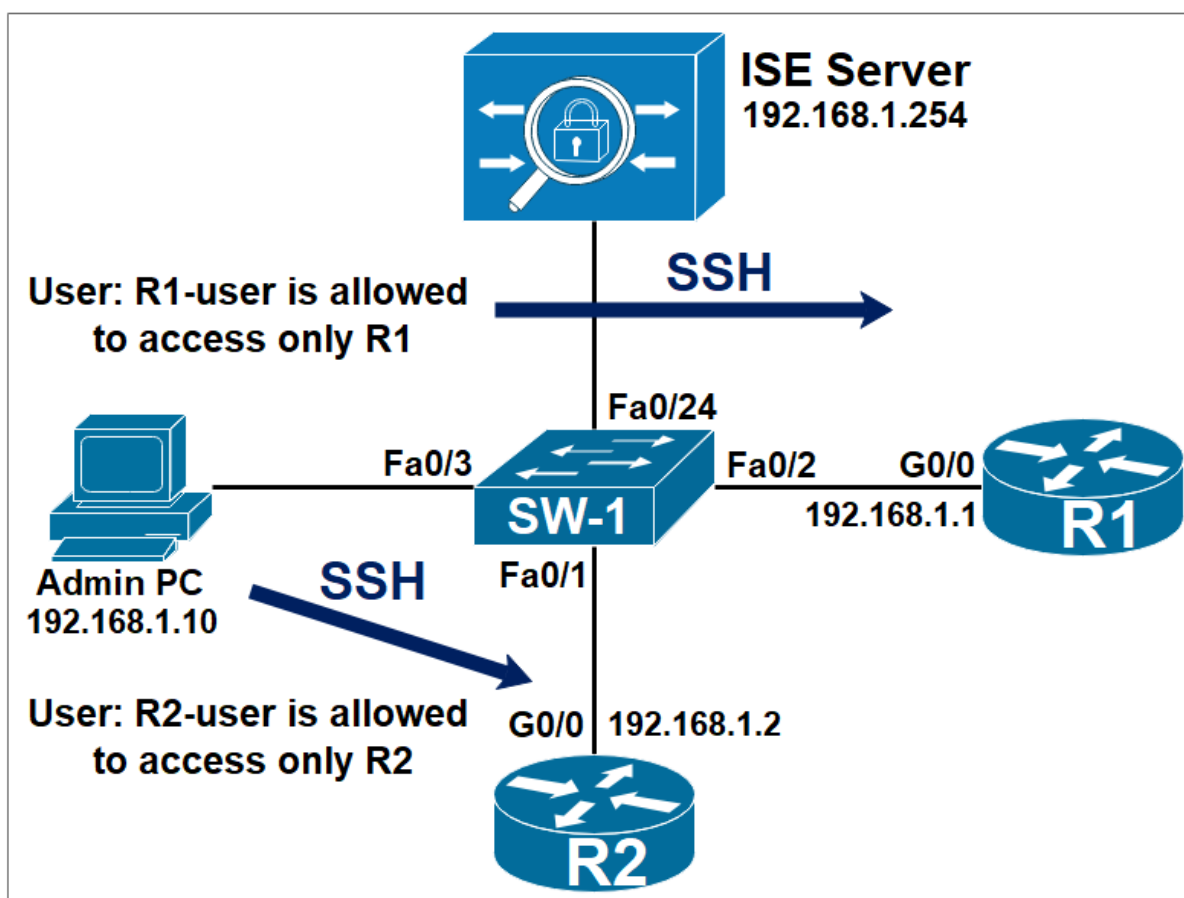
Overview

Request Type	Authorization
Status	Pass
Session Key	ISE/363103442/223
Message Text	Device-Administration: Command Authorization succeeded
Username	administrator
Authorization Policy	Default >> Admin-AuthoZ
Shell Profile	
Matched Command Set	CMD_Priv_15
Command From Device	compatible rfc1587

Authorization Details

Generated Time	2020-01-07 21:39:40.687 +0:00
Logged Time	2020-01-07 21:39:40.687
Epoch Time (sec)	1578433180
ISE Node	ISE
Message Text	Device-Administration: Command Authorization succeeded
Failure Reason	
Resolution	
Root Cause	
Username	administrator
Network Device Name	R1
Network Device IP	192.168.1.1
Network Device Groups	IPSEC#Is IPSEC Device#No,Location#All Locations#New-York,Device Type#All Device Types
Device Type	Device Type#All Device Types
Location	Location#All Locations#New-York
Device Port	tty388
Remote Address	192.168.1.10

Advanced Device Admin TACACS Scenario 2



Task:

The user **R1-user** is allowed to access the router **R1**. The user **R2-user** should be denied. The user **R2-user** is allowed to access the router **R2**. The user **R1-user** should be denied.

Activate the AAA process on the router:

Configure the TACACS service with the following commands:

R1:

```
R1(config)#aaa new-model
R1(config)#aaa authentication login default group tacacs+ local
R1(config)#aaa authorization config-commands
R1(config)#aaa authorization exec default group tacacs+ local
R1(config)#aaa authorization commands 1 default group tacacs+ local
R1(config)#aaa authorization commands 15 default group tacacs+ local
R1(config)#aaa accounting exec default start-stop group tacacs+
R1(config)#aaa accounting commands 1 default start-stop group tacacs+
R1(config)#aaa accounting commands 15 default start-stop group tacacs+
```

```
R1(config)#tacacs server ISE-SRV
```

```
R1(config-server-tacacs)#address ipv4 192.168.1.254
R1(config-server-tacacs)#key cisco
```

R2:

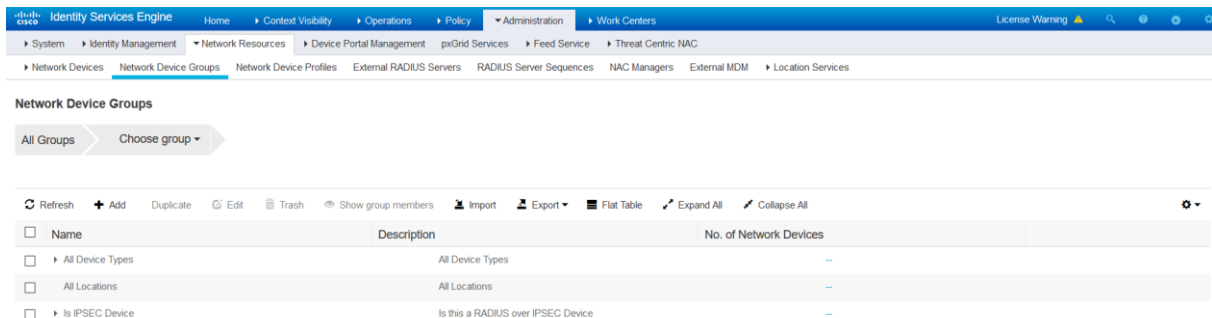
```
R2(config)#aaa new-model
R2(config)#aaa authentication login default group tacacs+ local
R2(config)#aaa authorization config-commands
R2(config)#aaa authorization exec default group tacacs+ local
R2(config)#aaa authorization commands 1 default group tacacs+ local
R2(config)#aaa authorization commands 15 default group tacacs+ local
R2(config)#aaa accounting exec default start-stop group tacacs+
R2(config)#aaa accounting commands 1 default start-stop group tacacs+
R2(config)#aaa accounting commands 15 default start-stop group tacacs+
```

```
R2(config)#tacacs server ISE-SRV
R2(config-server-tacacs)#address ipv4 192.168.1.254
R2(config-server-tacacs)#key cisco
```

Create Network Device Group

Navigate to **Administration > Network Resources > Network Device Groups**.

Click **Add** and Type **San-Jose** as the Name.
Select **All Locations** in the **Parent Group** field.
Click **Save**.



The screenshot shows the Cisco Identity Services Engine (ISE) interface. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers > Network Resources > Network Device Groups. The page title is "Network Device Groups". There are buttons for "All Groups" and "Choose group". Below the navigation, there are action buttons: Refresh, Add, Duplicate, Edit, Trash, Show group members, Import, Export, Flat Table, Expand All, and Collapse All. The main content is a table with the following data:

Name	Description	No. of Network Devices
All Device Types	All Device Types	--
All Locations	All Locations	--
Is IPSEC Device	Is this a RADIUS over IPSEC Device	--

Add Group



Name *

Description

Parent Group *

Cancel

Save

Click **Add** and Type **New-York** as the Name.
Select **All Locations** in the **Parent Group** field.
Click **Save**.

Add Group



Name *

Description

Parent Group *

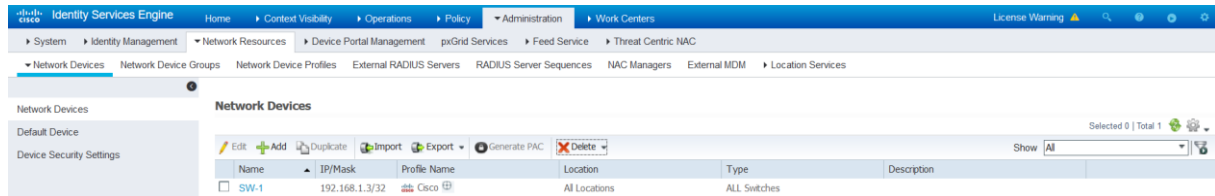
Cancel

Save

Name	Description	No. of Network Devices
All Device Types	All Device Types	--
All Locations	All Locations	--
New-York		0
San-Jose		0
Is IPSEC Device	Is this a RADIUS over IPSEC Device	--

Add the routers as AAA Client in the Cisco ISE

Navigate to **Administration > Network Resources > Network Devices**. The **Network Devices** window will open.



In the right section window, click **Add**. The AAA Client window opens.

In the **Name** field, type **R1** as the name.

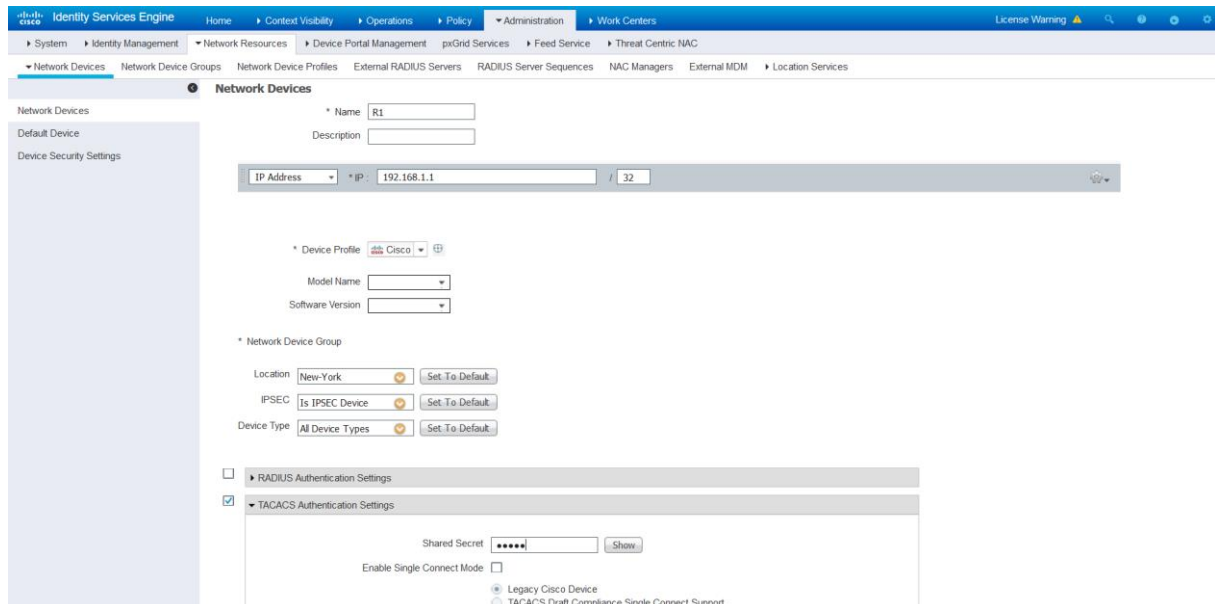
In the **IP Address** field, enter **192.168.1.1/32**. this the IP address of the router interface that will forward TACACS packets to Cisco ISE.

From the **Location** drop-down menu, select **New-York**.

To activate **TACACS Authentication Settings**, click the check box.

In the **Shared Secret** field, enter a shared secret of **cisco**.

Click the **Submit** button.



Click **Add** once again. The AAA Client window opens.

In the **Name** field, type **R2** as the name.

In the **IP Address** field, enter **192.168.1.2/32**. this the IP address of the router interface that will forward TACACS packets to Cisco ISE.

From the **Location** drop-down menu, select **San-Jose**.

To activate **TACACS Authentication Settings**, click the check box.

In the **Shared Secret** field, enter a shared secret of **cisco**.

Click the **Submit** button.

Network Devices

Name: R2
Description:

IP Address: 192.168.1.2 / 32

Device Profile: Cisco
Model Name:
Software Version:

Network Device Group: San-Jose
Location: San-Jose
IPSEC: Is IPSEC Device
Device Type: All Device Types

RADIUS Authentication Settings
 TACACS Authentication Settings

Shared Secret: Show
Enable Single Connect Mode:
Legacy Cisco Device:
TACACS Draft Compliance Single Connect Support:

Name	IP/Mask	Profile Name	Location	Type	Description
<input type="checkbox"/> R1	192.168.1.1/32	Cisco	New-York	All Device Types	
<input type="checkbox"/> R2	192.168.1.2/32	Cisco	San-Jose	All Device Types	
<input type="checkbox"/> SW-1	192.168.1.3/32	Cisco	All Locations	All Switches	

Create two user groups.

Navigate to **Administration > Identity Management > Groups**.
Under the **User Identity Groups**, click **Add**.

Name	Description
<input type="checkbox"/> ALL_ACCOUNTS (default)	Default ALL_ACCOUNTS (default) User Group
<input type="checkbox"/> Admin-GR	
<input type="checkbox"/> Admin-Group	
<input type="checkbox"/> Emp-Group	
<input type="checkbox"/> Employee	Default Employee User Group
<input type="checkbox"/> GROUP_ACCOUNTS (default)	Default GROUP_ACCOUNTS (default) User Group
<input type="checkbox"/> GuestType_Contractor (default)	Identity group mirroring the guest type
<input type="checkbox"/> GuestType_Daily (default)	Identity group mirroring the guest type
<input type="checkbox"/> GuestType_Social_login (default)	Identity group mirroring the guest type
<input type="checkbox"/> GuestType_Weekly (default)	Identity group mirroring the guest type
<input type="checkbox"/> Helpdesk-GR	
<input type="checkbox"/> OWN_ACCOUNTS (default)	Default OWN_ACCOUNTS (default) User Group
<input type="checkbox"/> Training-Grp	

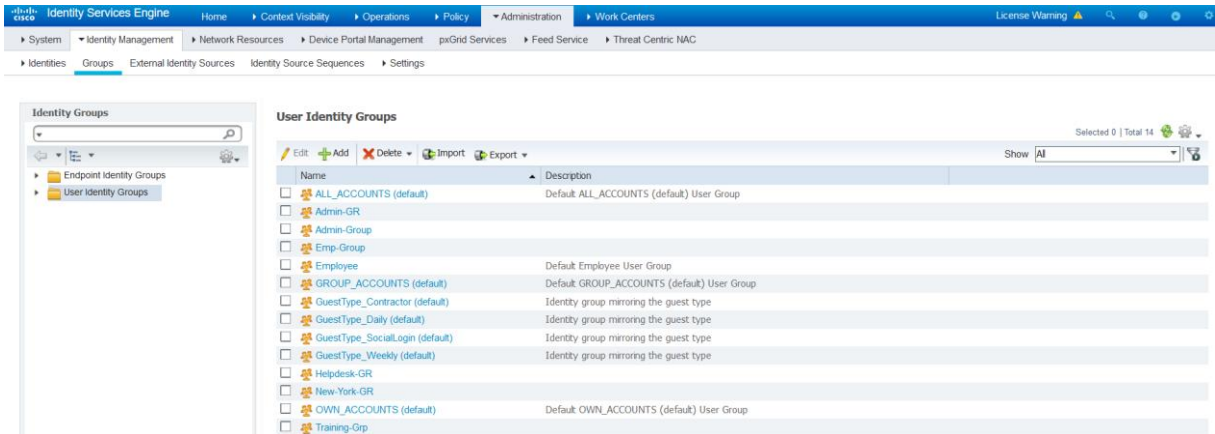
In the **Name** field, enter **New-York-GR**.
Click **Submit**.

User Identity Groups > New User Identity Group

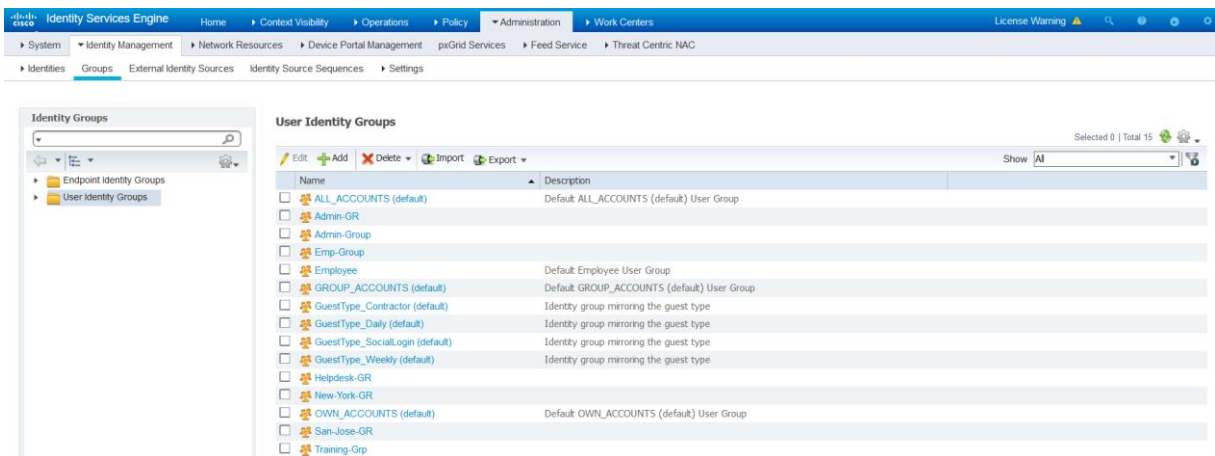
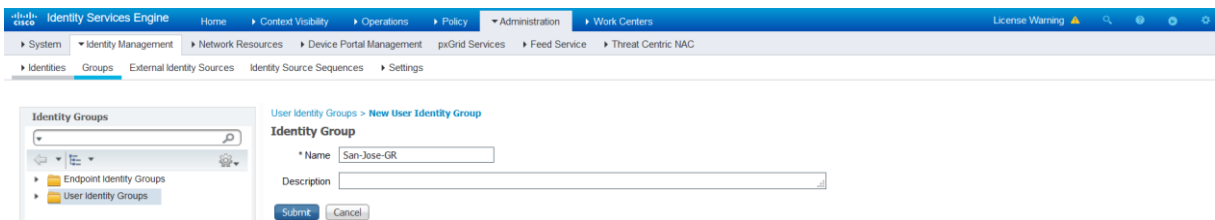
Identity Group

Name: New-York-GR
Description:

Submit Cancel

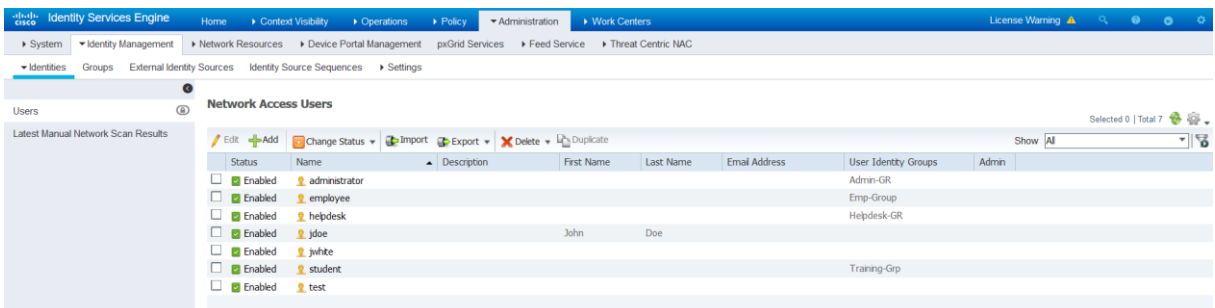


Create another **User Identity Groups**.
 In the **Name** field, enter **San-Jose-GR**.
 Click **Submit**.



Create Two users.

Navigate to **Administration > Identity Management > Identities**.



Create a user **R1-user** with password **Cisco1234**. In the **User Groups** field, select **New York-GR**.
Click **Submit**.

Identity Services Engine Administration Work Centers

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

Identities Groups External Identity Sources Identity Source Sequences Settings

Users

Network Access Users List > New Network Access User

Network Access User

* Name: R1-user

Status: Enabled

Email:

Passwords

Password Type: Internal Users

Password: Re-Enter Password:

* Login Password:

Enable Password:

User Information

Account Options

Account Disable Policy

User Groups

New-York-GR

Identity Services Engine Administration Work Centers

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

Identities Groups External Identity Sources Identity Source Sequences Settings

Users

Network Access Users

Selected 0 | Total 8

Edit Add Change Status Import Export Delete Duplicate Show All

Status	Name	Description	First Name	Last Name	Email Address	User Identity Groups	Admin
<input checked="" type="checkbox"/>	administrator					Admin-GR	
<input checked="" type="checkbox"/>	employee					Emp-Group	
<input checked="" type="checkbox"/>	helpdesk					Helpdesk-GR	
<input checked="" type="checkbox"/>	john		John	Doe			
<input checked="" type="checkbox"/>	juhite						
<input checked="" type="checkbox"/>	R1-user					New-York-GR	
<input checked="" type="checkbox"/>	student					Training-Gp	
<input checked="" type="checkbox"/>	test						

Identity Services Engine Administration Work Centers

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

Identities Groups External Identity Sources Identity Source Sequences Settings

Users

Network Access Users List > New Network Access User

Network Access User

* Name: R2-user

Status: Enabled

Email:

Passwords

Password Type: Internal Users

Password: Re-Enter Password:

* Login Password:

Enable Password:

User Information

Account Options

Account Disable Policy

User Groups

San-Jose-GR

Create a user **R2-user** with password **Cisco12345**. In the **User Groups** field, select **San-Jose-GR**.
Click **Submit**.

Status	Name	Description	First Name	Last Name	Email Address	User Identity Groups	Admin
<input type="checkbox"/> Enabled	administrator					Admin-GR	
<input type="checkbox"/> Enabled	employee					Emp-Group	
<input type="checkbox"/> Enabled	helpdesk					Helpdesk-GR	
<input type="checkbox"/> Enabled	jdoe		John	Doe			
<input type="checkbox"/> Enabled	juhite						
<input type="checkbox"/> Enabled	R1-user					New-York-GR	
<input type="checkbox"/> Enabled	R2-user					San-Jose-GR	
<input type="checkbox"/> Enabled	student					Training-GR	
<input type="checkbox"/> Enabled	test						

To add policy elements, navigate to **Work Centers > Device Administration > Policy Elements > Network Condition > Device Network Conditions**. You will add two different Device Network Conditions. Click **Add** to create a new **Device Network Conditions**.

Enter as Name **R1_IP_Address**.

In the **Devices** field, click the **Insert Device** button, then click the **Select** button.

Device Network Conditions > R1_IP_Address

Devices

Name:

Description:

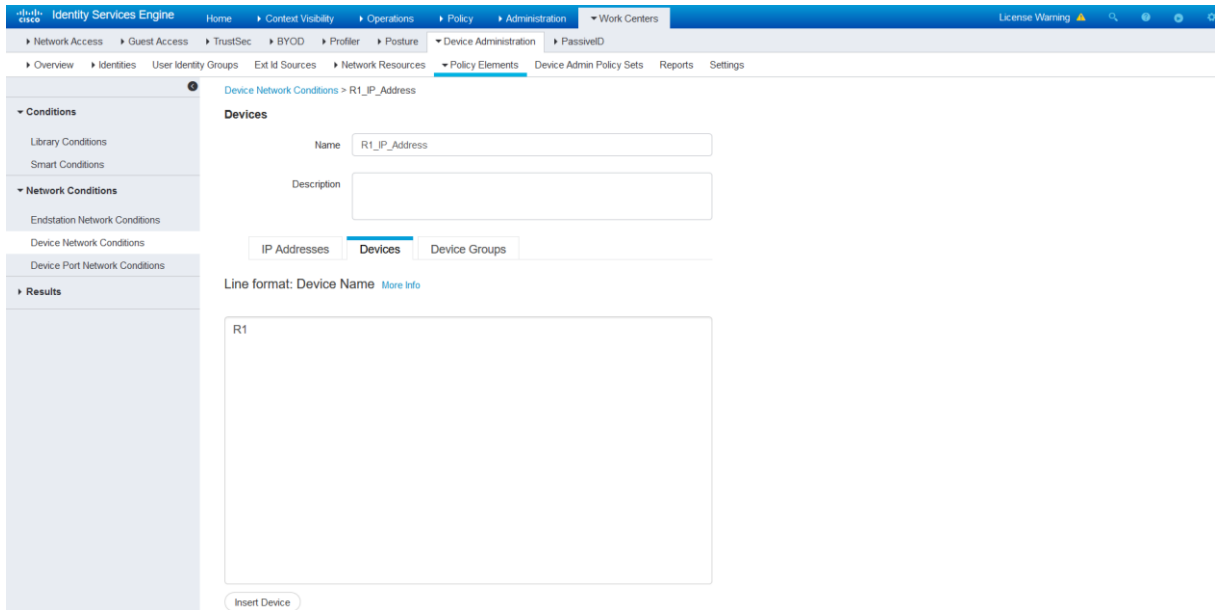
IP Addresses | **Devices** | Device Groups

Line format: Device Name [More Info](#)

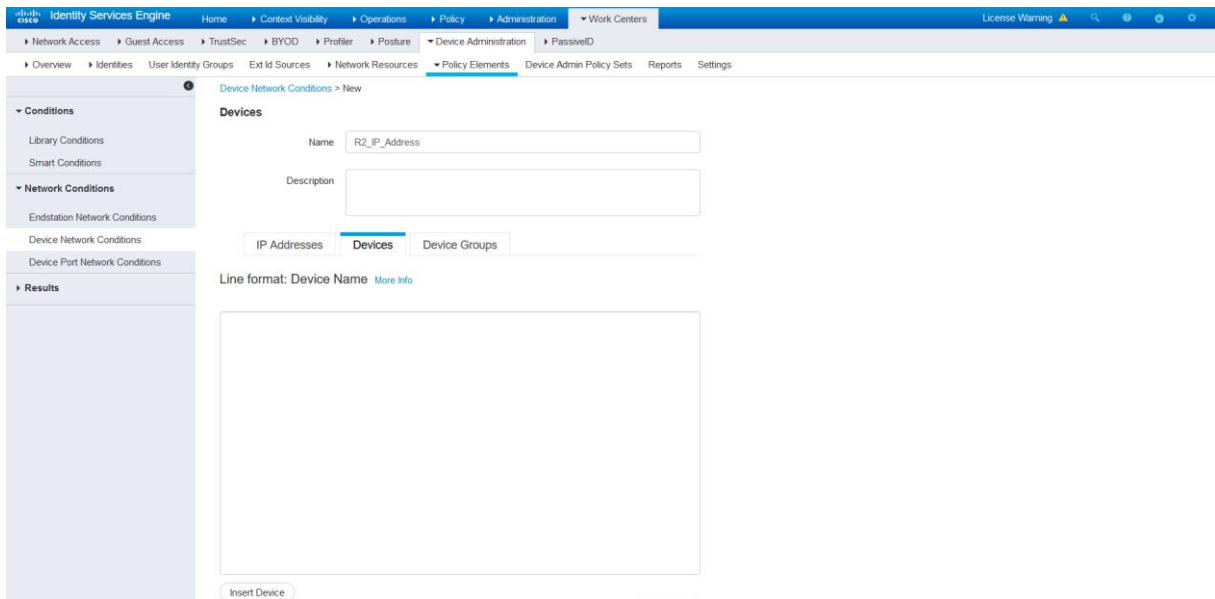
In the Select Device field, select **R1**, the Device Name condition identifies the devices added in the ISE, in this case **R1** and **R2**.

Click the **Insert** button and click **Submit**.

Select Device ✕



Click **Add** to create a new Device Network Conditions.
 Enter as Name **R2_IP_Address**.
 In the **Devices** field, click the **Insert Device** button, then click the **Select** button.



In the Select Device field, select **R2**, the Device Name condition identifies the devices added in the ISE, in this case **R1** and **R2**.
 Click the **Insert** button and click **Submit**.

Select Device



R2

Cancel

Insert

Identity Services Engine

Home > Context Visibility > Operations > Policy > Administration > Work Centers

License Warning

Network Access > Guest Access > TrustSec > BYOD > Profiler > Posture > Device Administration > PassivelD

Overview > Identities > User Identity Groups > Ext Id Sources > Network Resources > Policy Elements > Device Admin Policy Sets > Reports > Settings

Device Network Conditions > New

Conditions

- Library Conditions
- Smart Conditions

Network Conditions

- Endstation Network Conditions
- Device Network Conditions
- Device Port Network Conditions

Results

Devices

Name: R2_IP_Address

Description:

IP Addresses | **Devices** | Device Groups

Line format: Device Name [More Info](#)

R2

Insert Device

Identity Services Engine

Home > Context Visibility > Operations > Policy > Administration > Work Centers

License Warning

Network Access > Guest Access > TrustSec > BYOD > Profiler > Posture > Device Administration > PassivelD

Overview > Identities > User Identity Groups > Ext Id Sources > Network Resources > Policy Elements > Device Admin Policy Sets > Reports > Settings

Device Network Conditions

0 Selected

Rows/Page: 2

1 / 1

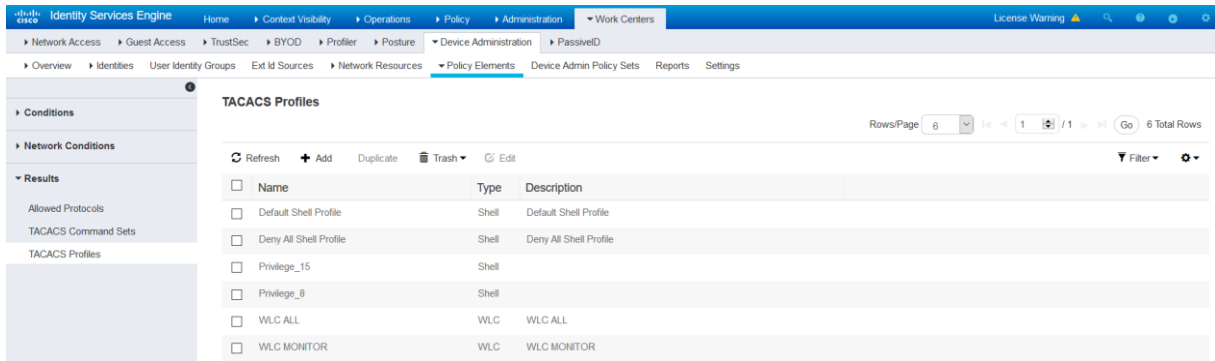
Go 2 Total Rows

Refresh + Add Duplicate Trash Edit Filter

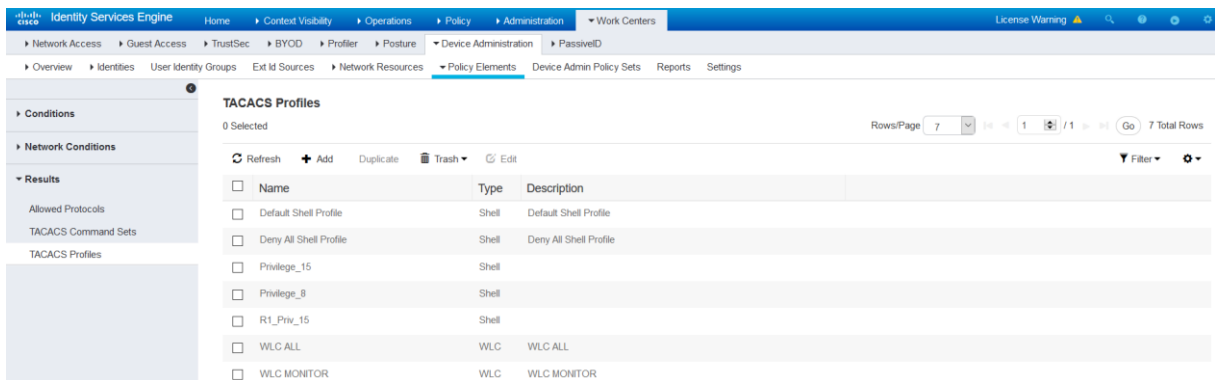
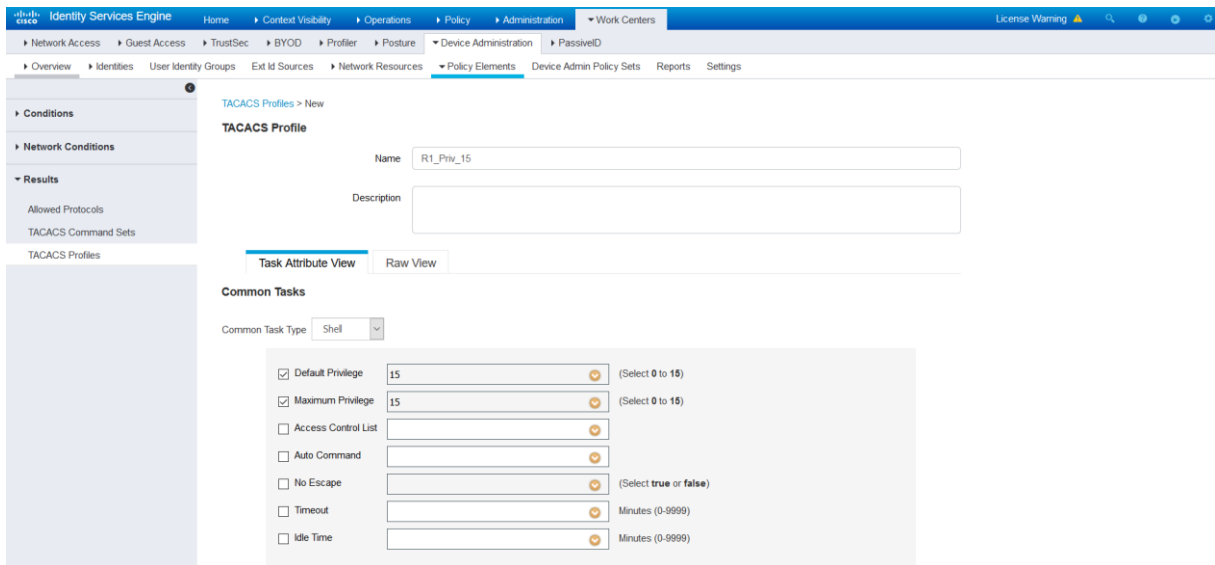
Name	Description
<input type="checkbox"/> R1_IP_Address	
<input type="checkbox"/> R2_IP_Address	

Navigate to **Work Centers > Device Administration > Policy Elements > Results > TACACS Profiles.**

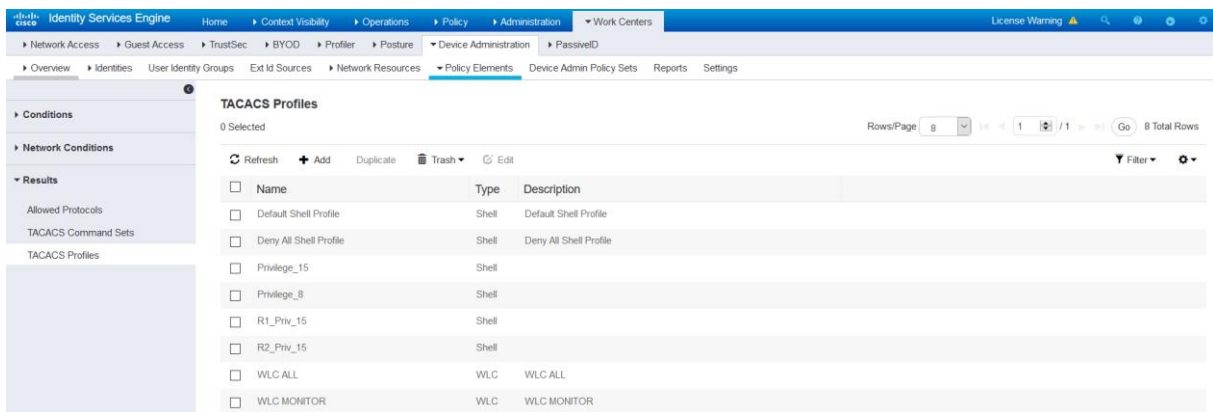
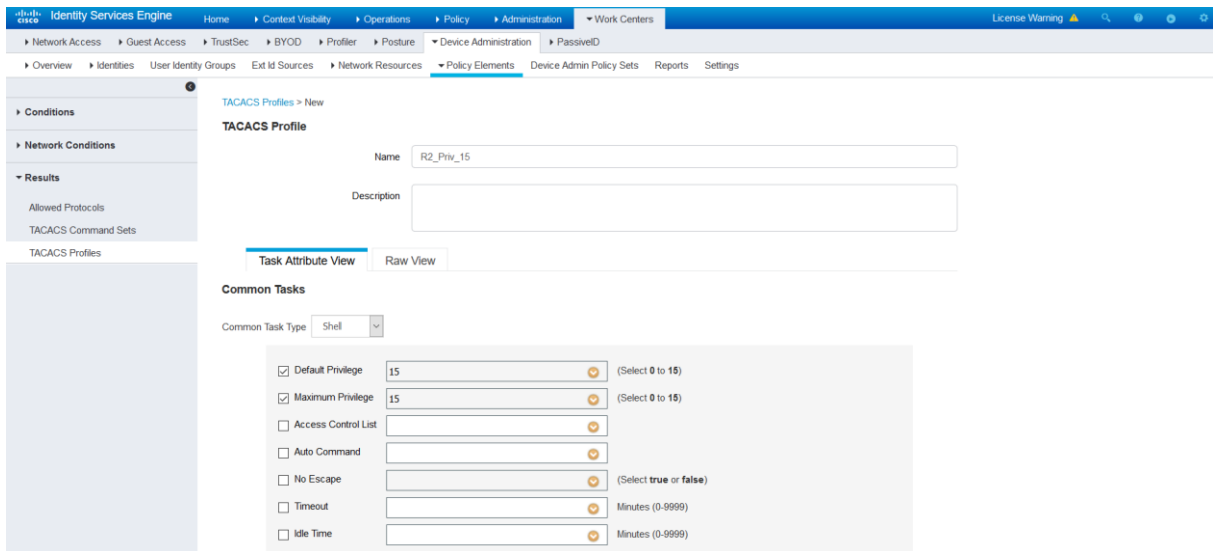
You will add two different TACACS profiles with different privilege levels.



Click **Add** to create a new profile named **R1_Priv_1** where the **default privilege level is 15**, and **maximum privilege level is 15**. Click **Submit**.

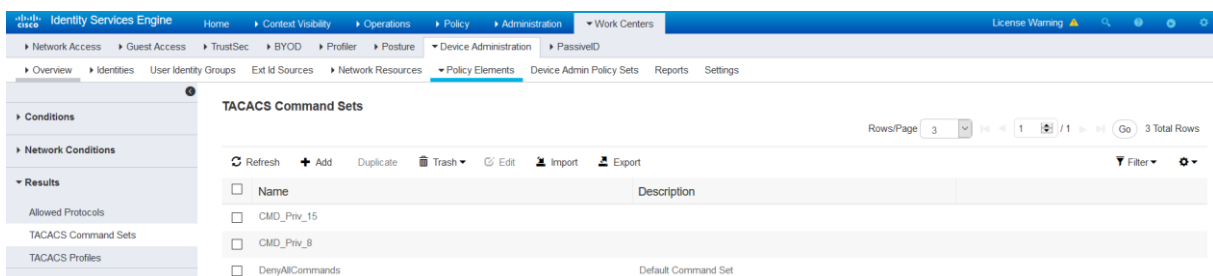


Add a second profile named **R2_Priv_15**, with a **default privilege level 15** and **maximum privilege level 15**. Click **Submit**.



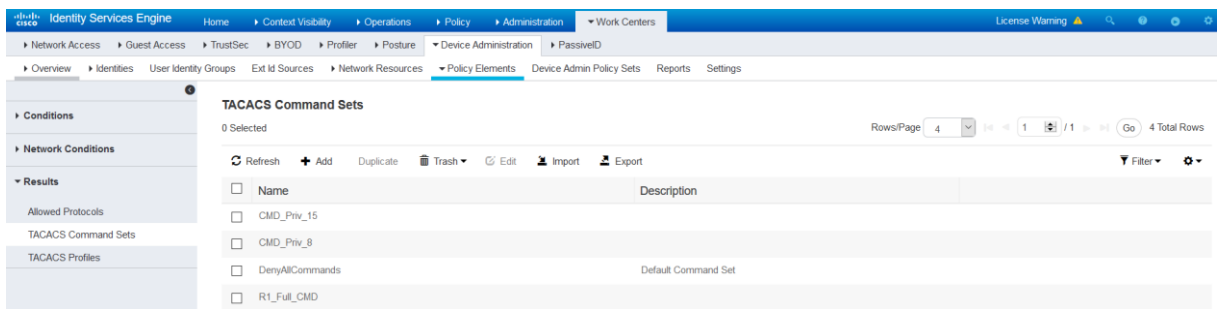
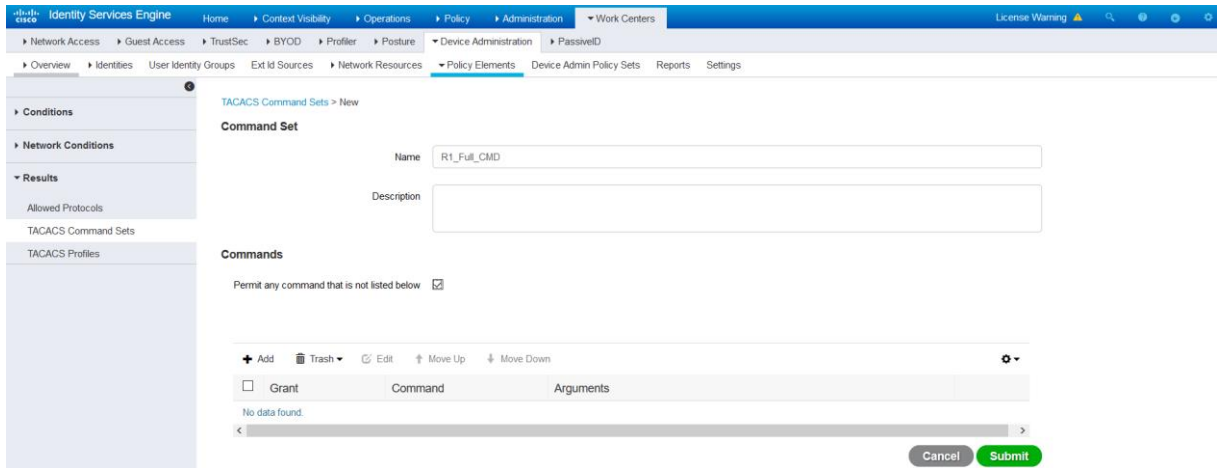
Navigate to **Work Centers > Device Administration > Policy Elements > Results > TACACS Command Sets**. Create two command sets, with full access.

Click **Add** to create a new command set.



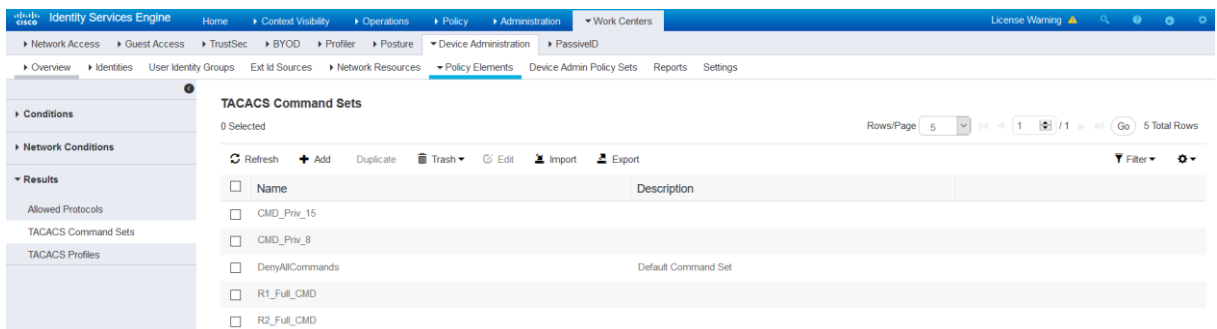
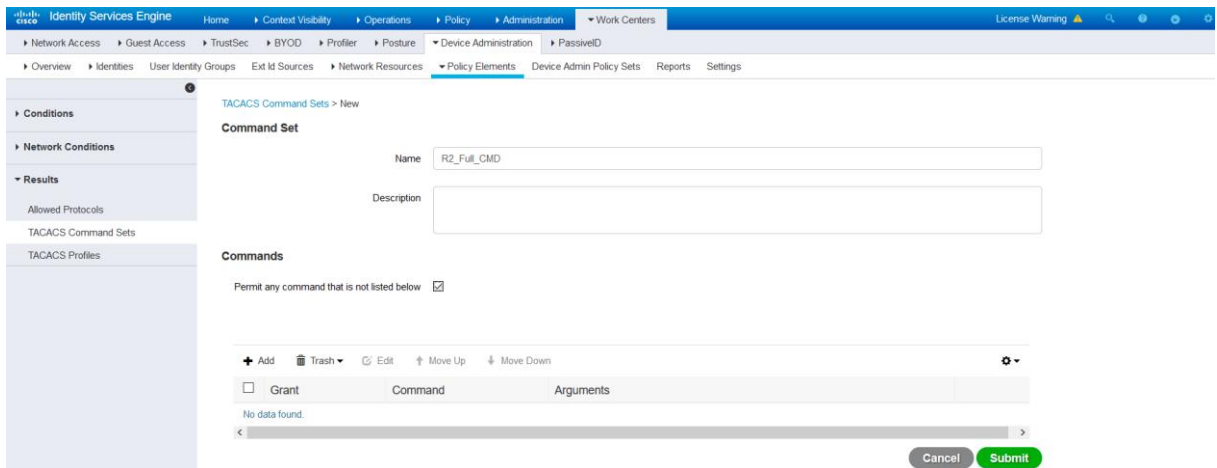
Configure the name as **R1_Full_CMD**, and click the checkbox for **Permit any command that is not listed below**.

Click **Submit**.



Create a new command set named **R2_Full_CMD**, and click the checkbox for **Permit any command that is not listed below**.

Click **Submit**.

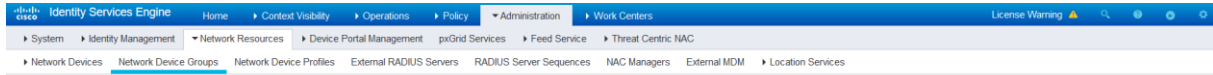


Create Network Device Group

Copyright 2021 Redouane Meddane. Consumers may download and use this document for personal use only. Downloading and editing this document for redistribution is prohibited. All rights reserved.

Navigate to **Administration > Network Resources > Network Device Groups**.

Click **Add** and Type **ALL Routers** as the Name.
Select **All Device Types** in the **Parent Group** field.
Click **Save**.



Network Device Groups

All Groups > Choose group ▾

Refresh Add Duplicate Edit Trash Show group members Import Export Flat Table Expand All Collapse All

Name	Description	No. of Network Devices
All Device Types	All Device Types	--
All Locations	All Locations	--
Is IPSEC Device	Is this a RADIUS over IPSEC Device	--

Add Group

Name *

All Routers

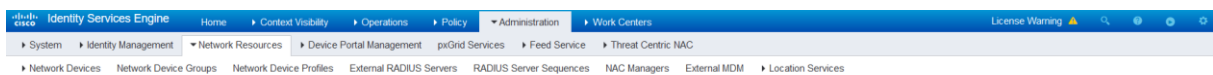
Description

Parent Group *

All Device Types

Cancel

Save



Network Device Groups

All Groups > Choose group ▾

Refresh Add Duplicate Edit Trash Show group members Import Export Flat Table Expand All Collapse All

Name	Description	No. of Network Devices
All Device Types	All Device Types	--
ALL Switches		1
All Routers		0
All Locations	All Locations	--
Is IPSEC Device	Is this a RADIUS over IPSEC Device	--

Navigate to **Administration > Network Resources > Network Devices**.
Edit the device **R1**, from the **Device Type** drop-down menu, select **All Routers**.

Identity Services Engine Administration Work Centers

Network Devices

Name	IP/Mask	Profile Name	Location	Type	Description
<input type="checkbox"/> R1	192.168.1.1/32	Cisco	New-York	All Device Types	
<input type="checkbox"/> R2	192.168.1.2/32	Cisco	San-Jose	All Device Types	
<input type="checkbox"/> SW-1	192.168.1.3/32	Cisco	All Locations	All Switches	

Identity Services Engine Administration Work Centers

Network Devices List > R1

Network Devices

Name: R1

Description:

IP Address: 192.168.1.1 / 32

Device Profile: Cisco

Model Name:

Software Version:

Network Device Group

Location: New-York (Set To Default)

IPSEC: No (Set To Default)

Device Type: All Routers (Set To Default)

RADIUS Authentication Settings

TACACS Authentication Settings

Shared Secret: ***** (Show/Retire)

Edit the device R2, from the **Device Type** drop-down menu, select **All Routers**.

Identity Services Engine Administration Work Centers

Network Devices List > R2

Network Devices

Name: R2

Description:

IP Address: 192.168.1.2 / 32

Device Profile: Cisco

Model Name:

Software Version:

Network Device Group

Location: San-Jose (Set To Default)

IPSEC: No (Set To Default)

Device Type: All Routers (Set To Default)

RADIUS Authentication Settings

TACACS Authentication Settings

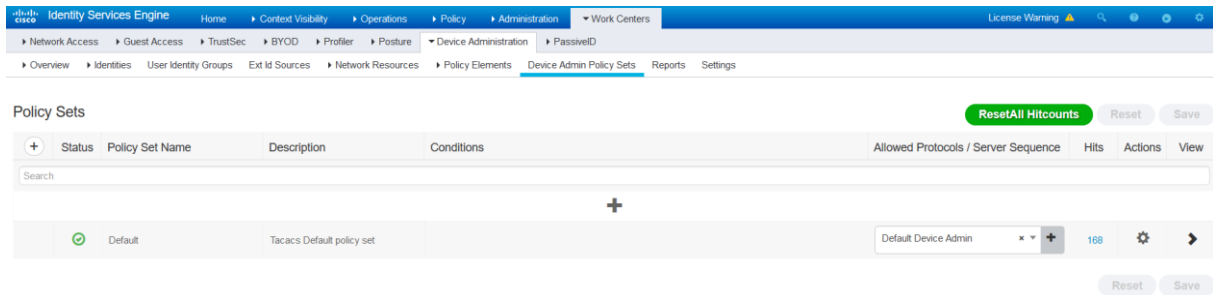
Shared Secret: ***** (Show/Retire)

Identity Services Engine Administration Work Centers

Network Devices

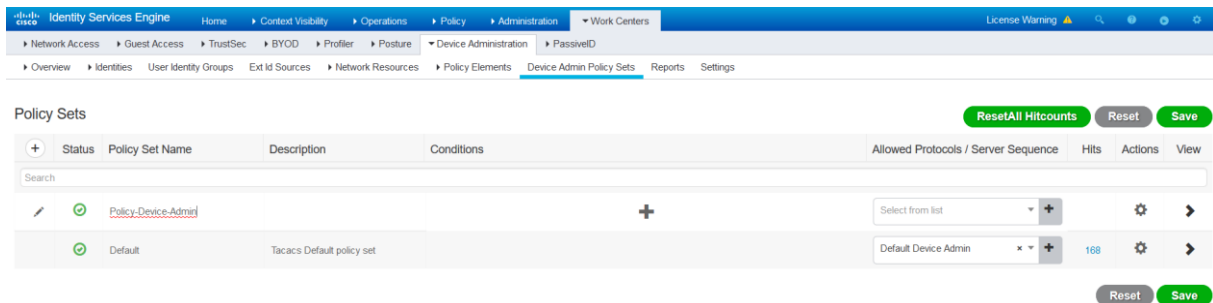
Name	IP/Mask	Profile Name	Location	Type	Description
<input type="checkbox"/> R1	192.168.1.1/32	Cisco	New-York	All Routers	
<input type="checkbox"/> R2	192.168.1.2/32	Cisco	San-Jose	All Routers	
<input type="checkbox"/> SW-1	192.168.1.3/32	Cisco	All Locations	All Switches	

For policy creation, navigate to **Work Centers > Device Administration > Device Admin Policy Sets**.



Create a new Policy Set named **Policy-Device-Admin**, Click the **Plus** icon or click the **gear** icon and select **Insert new row above** to create a new Policy Set above the Default Policy Set.

Create a new Condition of **Device: Device Type EQUALS All Device Types#ALL Routers**.



Create a new Condition of **Device: Device Type EQUALS All Device Types#ALL Routers**.

Conditions Studio

Library

Search by Name

No conditions found - reset filters.

Editor

DEVICE-Device Type

Equals All Device Types#All Routers

Set to 'Is not'

Duplicate Save

+ New AND OR

Close Use

Select **Default Device Admin** from the Drop-Down Menu under **Allowed Protocols/Server Sequence**.
Click **Save**.

Policy Sets

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✓	Policy-Device-Admin		DEVICE Device Type EQUALS All Device Types#All Routers	Default Device Admin		⚙️	➔
✓	Default	Tacacs Default policy set		Default Device Admin	168	⚙️	➔

Policy Sets

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
✓	Policy-Device-Admin		DEVICE Device Type EQUALS All Device Types#All Routers	Default Device Admin	0	⚙️	➔
✓	Default	Tacacs Default policy set		Default Device Admin	168	⚙️	➔

Next, edit the Authentication Policy.

Policy Sets → Policy-Device-Admin

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Policy-Device-Admin		DEVICE Device Type EQUALS All Device Types#All Routers	Default Device Admin	0

- ➔ Authentication Policy (1)
- ➔ Authorization Policy - Local Exceptions
- ➔ Authorization Policy - Global Exceptions
- ➔ Authorization Policy (1)

Use **Internal Users** as the Identity Store instead of **All_AD_Join_Points**.
Click **Done** and click **Save**.

Identity Services Engine Administration Work Centers

Policy Administration Device Admin Policy Sets

Policy Sets → Policy-Device-Admin

ResetAll Hitcounts Reset Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✔	Policy-Device-Admin		DEVICE Device Type EQUALS All Device Types#All Routers	Default Device Admin	0

Authentication Policy (1)

Status	Rule Name	Conditions	Use	Hits	Actions
✔	Default		All_User_ID_Stores	0	Options

Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

Authorization Policy (1)

Identity Services Engine Administration Work Centers

Policy Administration Device Admin Policy Sets

Policy Sets → Policy-Device-Admin

ResetAll Hitcounts Reset Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✔	Policy-Device-Admin		DEVICE Device Type EQUALS All Device Types#All Routers	Default Device Admin	0

Authentication Policy (1)

Status	Rule Name	Conditions	Use	Hits	Actions
✔	Default		Internal Users	0	Options

Authorization Policy - Local Exceptions

Authorization Policy - Global Exceptions

Authorization Policy (1)

Identity Services Engine Administration Work Centers

Policy Administration Device Admin Policy Sets

Policy Sets → Policy-Device-Admin

ResetAll Hitcounts Reset Save

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✔	Policy-Device-Admin		DEVICE Device Type EQUALS All Device Types#All Routers	Default Device Admin	0

Authentication Policy (1)

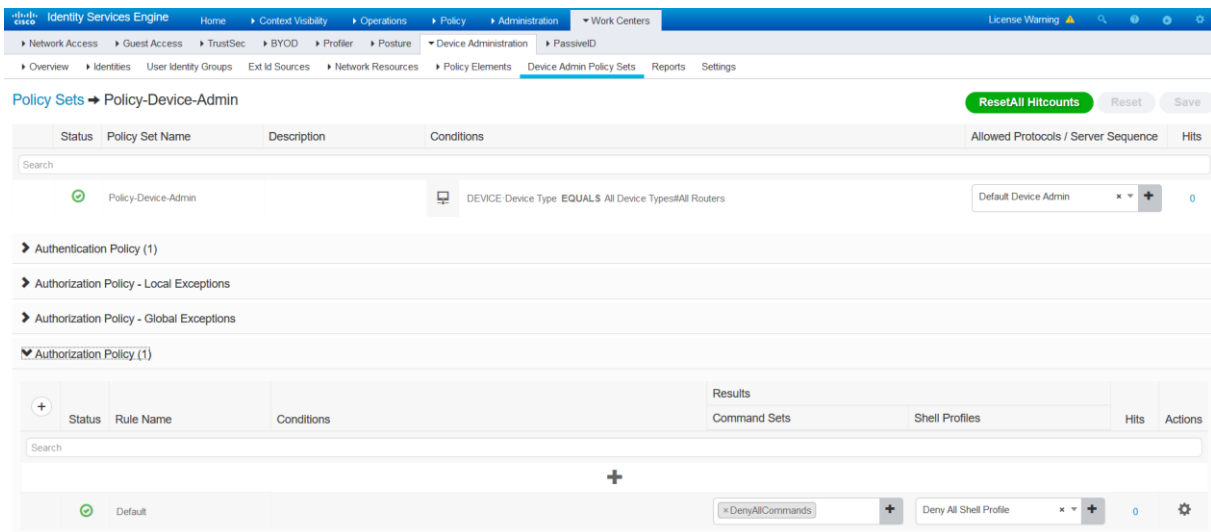
Status	Rule Name	Conditions	Use	Hits	Actions
✔	Default		Internal Users	0	Options

Authorization Policy - Local Exceptions

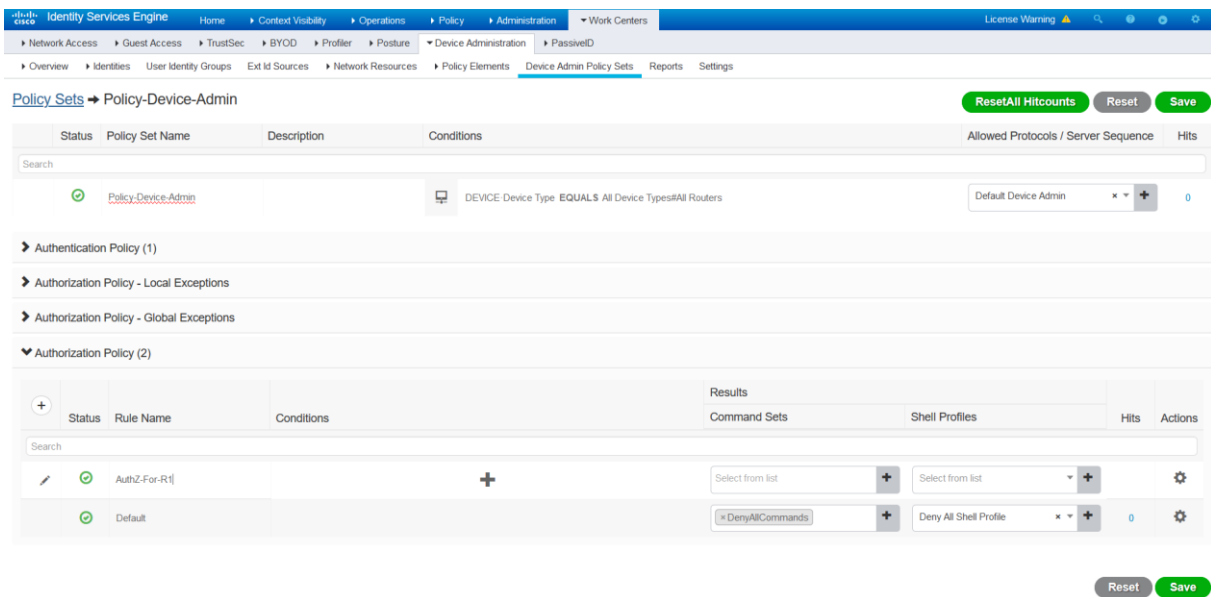
Authorization Policy - Global Exceptions

Authorization Policy (1)

Next edit the **Authorization Policy**, insert a new authorization policy above the Default authorization policy.



Enter the name **AuthZ-For-R1**.
Click in the **Conditions** field to create a new condition.



Under **Editor**, define a condition as **TACACS: User Equals R1-user**. Click new with **AND** operator, define a condition as **Network Condition: R1_IP_Address Equals True**.

Conditions Studio

Library

Search by Name

- EAP-MSCHAPV2
- EAP-TLS
- Guest_Flow
- Network_Access_Authentication_Passed

Editor

TACACS-User
Equals R1-user
Set to 'Is not' Duplicate Save

AND
Network Condition-R1_IP_Address
Equals true
Set to 'Is not' Duplicate Save

+ New AND OR

Close Use

Select the following Results:
Command Sets: **R1_Full_CMD**
Shell Profiles: **R1_Priv_15**
Click **Save**.

The screenshot shows the Cisco ISE Policy Administration console. The breadcrumb navigation is: Home > Context Visibility > Operations > Policy > Administration > Work Centers. The current page is 'Policy Sets > Policy-Device-Admin'. A table lists policy sets, with 'AuthZ-For-R1' selected. The 'Conditions' field for 'AuthZ-For-R1' is expanded, showing two conditions: 'TACACS User EQUALS R1-user' and 'Network Condition R1_IP_Address EQUALS true', connected by an 'AND' operator. The 'Results' section shows 'Command Sets' with 'R1_Full_CMD' selected and 'Shell Profiles' with 'R1_Priv_15' selected. The 'Hits' column shows 2 hits for this rule.

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✔	Policy-Device-Admin		DEVICE Device Type: EQUALS All Device Types#All Routers	Default Device Admin x +	15
▶	Authentication Policy (1)				
▶	Authorization Policy - Local Exceptions				
▶	Authorization Policy - Global Exceptions				
▼	Authorization Policy (3)				
+	Status	Rule Name	Conditions	Results	
✔		AuthZ-For-R1	AND TACACS User EQUALS R1-user Network Condition R1_IP_Address EQUALS true	R1_Full_CMD R1_Priv_15	2
✎		AuthZ-For-R2	+	Select from list Select from list	
✔		Default		DenyAllCommands Deny All Shell Profile	3

Now add an Authorization Policy. Start by clicking the **gear** icon at the end of the **AuthZ-For-R1** policy, and choose **Insert New Rule Below**. Enter the name **AuthZ-For-R2**.

Click in the Conditions field to create a new condition.

Under **Editor**, define a condition as **TACACS: User Equals R1-user**. Click new with **AND** operator, define a condition as **Network Condition: R1_IP_Address Equals True**.

Conditions Studio



Library

Search by Name

- EAP-MSCHAPv2
- EAP-TLS
- Guest_Flow
- Network_Access_Authentication_Passed

Editor

TACACS-User

Set to 'Is not'

AND

Network Condition-R2_IP_Address

Set to 'Is not'

Select the following Results:
 Command Sets: **R2_Full_CMD**
 Shell Profiles: **R2_Priv_15**
 Click **Save**.

Identity Services Engine

Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
	Policy-Device-Admin		DEVICE Device Type EQUALS All Device TypesAll Routers	Default Device Admin	15
Authentication Policy (1)					
Authorization Policy - Local Exceptions					
Authorization Policy - Global Exceptions					
Authorization Policy (4)					
Status	Rule Name	Conditions	Results	Hits	Actions
	AuthZ-For-R1	AND <ul style="list-style-type: none"> TACACS User EQUALS R1-user Network Condition R1_IP_Address EQUALS true 	<input type="text" value="R1_Full_CMD"/> <input type="button" value="+"/> <input type="text" value="R1_Priv_15"/> <input type="button" value="x"/> <input type="button" value="+"/>	2	
	AuthZ-For-R2	AND <ul style="list-style-type: none"> TACACS User EQUALS R2-user Network Condition R2_IP_Address EQUALS true 	<input type="text" value="R2_Full_CMD"/> <input type="button" value="+"/> <input type="text" value="R2_Priv_15"/> <input type="button" value="x"/> <input type="button" value="+"/>		

The screenshot shows the Cisco ISE Policy Sets configuration page. The main table lists the Policy Set Name 'Policy-Device-Admin' with a status of 'OK' and 15 hits. Below this, several authorization policies are listed, including 'AuthZ-For-R1' and 'AuthZ-For-R2'. The 'AuthZ-For-R1' policy is expanded to show its conditions: 'TACACS User EQUALS R1-user' and 'Network Condition R1_IP_Address EQUALS true'. The results for this policy show 'R1_Full_CMD' and 'R1_Priv_15' with 2 hits.

Return to your **Admin PC**, and use PUTTY to open an SSH session to **R1** router (**192.168.1.1**).

Login using the credentials **R1-user / Cisco1234**. This should succeed.

```

192.168.1.1 - PuTTY
login as: R1-user
Keyboard-interactive authentication prompts from server:
Password:
End of keyboard-interactive prompts from server
R1#
  
```

Navigate to **Operations > TACACS > Live Logs** to see that the authentication and authorization are successful.

The screenshot shows the Cisco ISE Live Logs page. The table displays two log entries for 'R1-user' authentication on 'R1' router. Both entries have a status of 'Success' and are associated with the 'Policy-Device-Admin' policy set.

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Device ...	Network Device
Jan 09, 2020 03:51:09 071 PM	Success		R1-user	Authentication	Policy-Device-Admin >> Default	Policy-Device-Admin >> AuthZ-For-R1	ISE	R1	192.168.1.1
Jan 09, 2020 03:51:08 879 PM	Success		R1-user	Authentication	Policy-Device-Admin >> Default	Policy-Device-Admin >> AuthZ-For-R1	ISE	R1	192.168.1.1

For the successful **R1-user** entry, click the **Details** icon. You can analyze the details of each session. Some of the more pertinent information includes the Authorization details.

The ISE TACACS Logs confirms Authentication succeed matching the correct **Default** Authentication Policy of the Policy Set **Policy-Device-Admin**.

Overview

Request Type	Authentication
Status	Pass
Session Key	ISE/363103442/365
Message Text	Passed-Authentication: Authentication succeeded
Username	R1-user
Authentication Policy	Policy-Device-Admin >> Default
Selected Authorization Profile	R1_Priv_15

Authentication Details

Generated Time	2020-01-09 15:51:08.879000 +00:00
Logged Time	2020-01-09 15:51:08.879
Epoch Time (sec)	1578585068
ISE Node	ISE
Message Text	Passed-Authentication: Authentication succeeded
Failure Reason	
Resolution	
Root Cause	
Username	R1-user
Network Device Name	R1
Network Device IP	192.168.1.1
Network Device Groups	IPSEC#Is IPSEC Device#No,Location#All Locations#New-York,Device Type#All Device Types#All Routers
Device Type	Device Type#All Device Types#All Routers
Location	Location#All Locations#New-York
Device Port	tty388
Remote Address	192.168.1.10

Steps

13013 Received TACACS+ Authentication START Request
15049 Evaluating Policy Group
15008 Evaluating Service Selection Policy
15048 Queried PIP - DEVICE.Device Type
15041 Evaluating Identity Policy
15013 Selected Identity Source - Internal Users
13045 TACACS+ will use the password prompt from global TACACS+ configuration
13015 Returned TACACS+ Authentication Reply
13014 Received TACACS+ Authentication CONTINUE Request (🕒 Step latency=3772ms)
15041 Evaluating Identity Policy
15013 Selected Identity Source - Internal Users
24210 Looking up User in Internal Users IDStore
24212 Found User in Internal Users IDStore
22037 Authentication Passed
15036 Evaluating Authorization Policy
15048 Queried PIP - TACACS.User
15048 Queried PIP - Network Condition.R1_IP_Address
13015 Returned TACACS+ Authentication Reply

The ISE TACACS Logs confirms Authorization succeed, matching the correct Authorization Policy **AuthZ-For-R1** and correct Tacacs Profile **R1_Priv_15**.

Overview

Request Type	Authorization
Status	Pass
Session Key	ISE/363103442/366
Message Text	Device-Administration: Session Authorization succeeded
Username	R1-user
Authorization Policy	Policy-Device-Admin >> AuthZ-For-R1
Shell Profile	R1_Priv_15
Matched Command Set	
Command From Device	

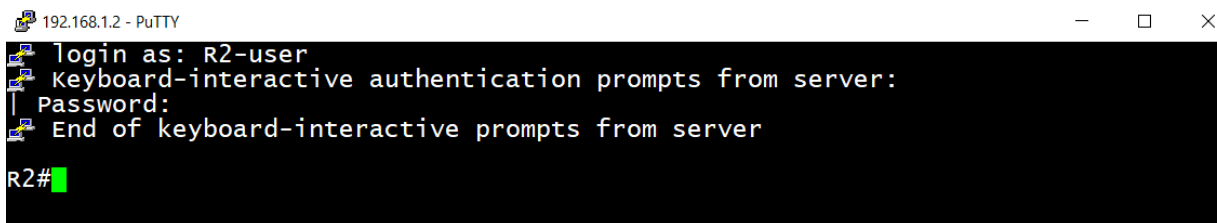
Authorization Details

Generated Time	2020-01-09 15:51:09.071 +0:00
Logged Time	2020-01-09 15:51:09.071
Epoch Time (sec)	1578585069
ISE Node	ISE
Message Text	Device-Administration: Session Authorization succeeded
Failure Reason	
Resolution	
Root Cause	
Username	R1-user
Network Device Name	R1
Network Device IP	192.168.1.1
Network Device Groups	IPSEC#s IPSEC Device#No,Location#All Locations#New-York,Device Type#All Device Types#All Routers
Device Type	Device Type#All Device Types#All Routers
Location	Location#All Locations#New-York
Device Port	tty388
Remote Address	192.168.1.10

Steps

```
13005 Received TACACS+ Authorization Request
15049 Evaluating Policy Group
15008 Evaluating Service Selection Policy
15048 Queried PIP - DEVICE.Device Type
15041 Evaluating Identity Policy
15013 Selected Identity Source - Internal Users
24210 Looking up User in Internal Users IDStore
24212 Found User in Internal Users IDStore
22037 Authentication Passed
15036 Evaluating Authorization Policy
15048 Queried PIP - TACACS.User
15048 Queried PIP - Network Condition.R1_IP_Address
15017 Selected Shell Profile
22081 Max sessions policy passed
22080 New accounting session created in Session cache
13034 Returned TACACS+ Authorization Reply
```

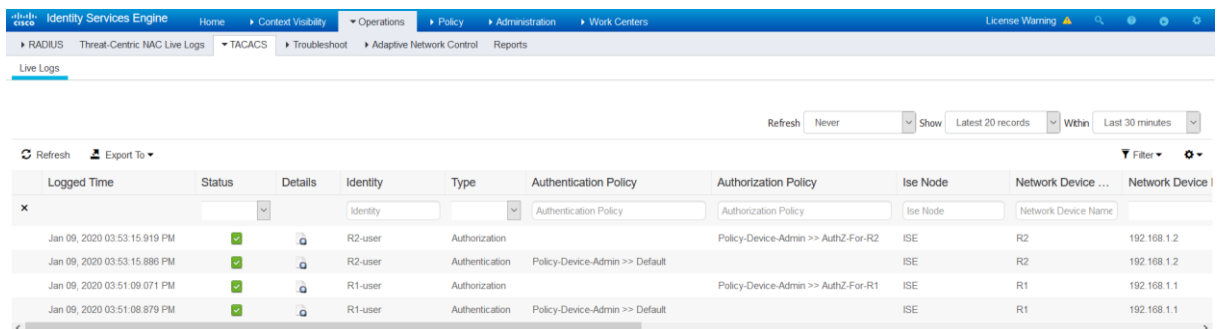
Return to your **Admin PC**, and use **PUTTY** to open an **SSH** session to **R2** router (**192.168.1.2**).
Login using the credentials **R2-user / Cisco12345**. This should succeed.



```
192.168.1.2 - PuTTY
login as: R2-user
keyboard-interactive authentication prompts from server:
Password:
End of keyboard-interactive prompts from server
R2#
```

Navigate to **Operations > TACACS > Live Logs** to see that the authentication and authorization are successful.

For the successful **R2-user** entry, click the **Details** icon. You can analyze the details of each session. Some of the more pertinent information includes the Authorization details.



Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Device ...	Network Device
Jan 09, 2020 03:53:15.919 PM	✓	🔒	R2-user	Authorization	Authentication Policy	Authorization Policy	Ise Node	Network Device Name	
Jan 09, 2020 03:53:15.886 PM	✓	🔒	R2-user	Authorization	Policy-Device-Admin >> Default	Policy-Device-Admin >> AuthZ-For-R2	ISE	R2	192.168.1.2
Jan 09, 2020 03:51:09.071 PM	✓	🔒	R1-user	Authorization	Policy-Device-Admin >> Default	Policy-Device-Admin >> AuthZ-For-R1	ISE	R1	192.168.1.1
Jan 09, 2020 03:51:08.879 PM	✓	🔒	R1-user	Authorization	Policy-Device-Admin >> Default		ISE	R1	192.168.1.1

The ISE TACACS Logs confirms Authentication succeed matching the correct **Default** Authentication Policy of the Policy Set **Policy-Device-Admin**.

Overview

Request Type	Authentication
Status	Pass
Session Key	ISE/363103442/368
Message Text	Passed-Authentication: Authentication succeeded
Username	R2-user
Authentication Policy	Policy-Device-Admin >> Default
Selected Authorization Profile	R2_Priv_15

Authentication Details

Generated Time	2020-01-09 15:53:15.886000 +00:00
Logged Time	2020-01-09 15:53:15.886
Epoch Time (sec)	1578585195
ISE Node	ISE
Message Text	Passed-Authentication: Authentication succeeded
Failure Reason	
Resolution	
Root Cause	
Username	R2-user
Network Device Name	R2
Network Device IP	192.168.1.2
Network Device Groups	IPSEC#Is IPSEC Device#No,Location#All Locations#San-Jose,Device Type#All Device Types#All Routers
Device Type	Device Type#All Device Types#All Routers
Location	Location#All Locations#San-Jose
Device Port	tty388
Remote Address	192.168.1.10

Steps

13013 Received TACACS+ Authentication START Request
15049 Evaluating Policy Group
15008 Evaluating Service Selection Policy
15048 Queried PIP - DEVICE.Device Type
15041 Evaluating Identity Policy
15013 Selected Identity Source - Internal Users
13045 TACACS+ will use the password prompt from global TACACS+ configuration
13015 Returned TACACS+ Authentication Reply
13014 Received TACACS+ Authentication CONTINUE Request (🕒 Step latency=4753ms)
15041 Evaluating Identity Policy
15013 Selected Identity Source - Internal Users
24210 Looking up User in Internal Users IDStore
24212 Found User in Internal Users IDStore
22037 Authentication Passed
15036 Evaluating Authorization Policy
15048 Queried PIP - TACACS.User
15048 Queried PIP - Network Condition.R2_IP_Address
13015 Returned TACACS+ Authentication Reply

The ISE TACACS Logs confirms Authorization succeed, matching the correct Authorization Policy **AuthZ-For-R2** and correct Tacacs Profile **R2_Priv_15**.

Overview

Request Type	Authorization
Status	Pass
Session Key	ISE/363103442/369
Message Text	Device-Administration: Session Authorization succeeded
Username	R2-user
Authorization Policy	Policy-Device-Admin >> AuthZ-For-R2
Shell Profile	R2_Priv_15
Matched Command Set	
Command From Device	

Authorization Details

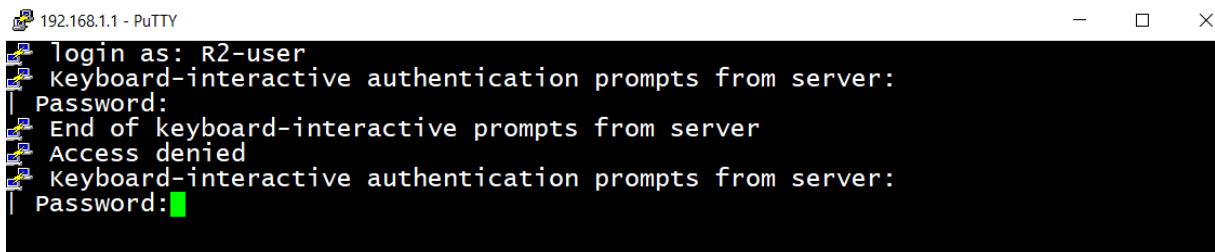
Generated Time	2020-01-09 15:53:15.919 +0:00
Logged Time	2020-01-09 15:53:15.919
Epoch Time (sec)	1578585195
ISE Node	ISE
Message Text	Device-Administration: Session Authorization succeeded
Failure Reason	
Resolution	
Root Cause	
Username	R2-user
Network Device Name	R2
Network Device IP	192.168.1.2
Network Device Groups	IPSEC#s IPSEC Device#No,Location#All Locations#San-Jose,Device Type#All Device Types#All Routers
Device Type	Device Type#All Device Types#All Routers
Location	Location#All Locations#San-Jose
Device Port	tty388
Remote Address	192.168.1.10

Steps

- 13005 Received TACACS+ Authorization Request
- 15049 Evaluating Policy Group
- 15008 Evaluating Service Selection Policy
- 15048 Queried PIP - DEVICE.Device Type
- 15041 Evaluating Identity Policy
- 15013 Selected Identity Source - Internal Users
- 24210 Looking up User in Internal Users IDStore
- 24212 Found User in Internal Users IDStore
- 22037 Authentication Passed
- 15036 Evaluating Authorization Policy
- 15048 Queried PIP - TACACS.User
- 15048 Queried PIP - Network Condition.R2_IP_Address
- 15017 Selected Shell Profile
- 22081 Max sessions policy passed
- 22080 New accounting session created in Session cache
- 13034 Returned TACACS+ Authorization Reply

Return to your **Admin PC**, and use **PUTTY** to open an **SSH** session to **R1** router (**192.168.1.1**).

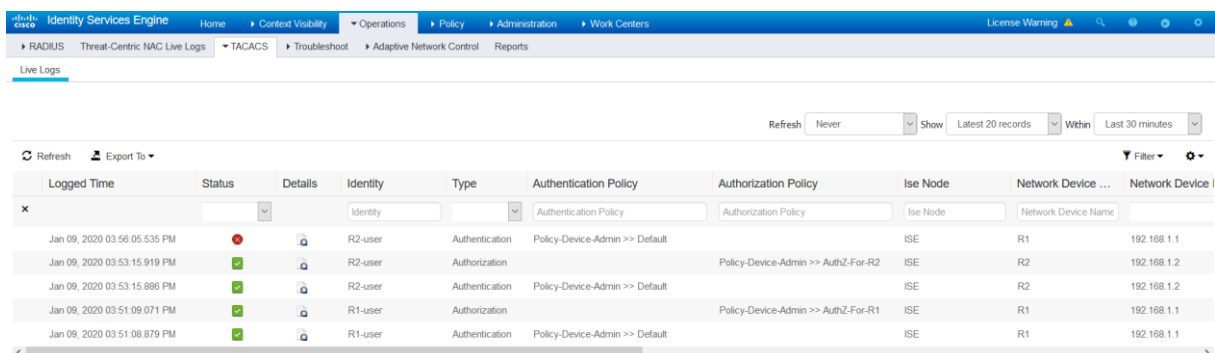
Login using the credentials **R2-user / Cisco12345**. This should fail.



```
192.168.1.1 - PuTTY
login as: R2-user
Keyboard-interactive authentication prompts from server:
Password:
End of keyboard-interactive prompts from server
Access denied
Keyboard-interactive authentication prompts from server:
Password:
```

Navigate to **Operations > TACACS > Live Logs** to see that the authentication and authorization failed.

For the failed **R2-user** entry, click the **Details** icon.



Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Device ...	Network Device IP
Jan 09, 2020 03:56:05.535 PM	Failed		R2-user	Authentication	Policy-Device-Admin >> Default		ISE	R1	192.168.1.1
Jan 09, 2020 03:53:15.919 PM	Success		R2-user	Authentication		Policy-Device-Admin >> AuthZ-For-R2	ISE	R2	192.168.1.2
Jan 09, 2020 03:53:15.896 PM	Success		R2-user	Authentication	Policy-Device-Admin >> Default		ISE	R2	192.168.1.2
Jan 09, 2020 03:51:09.071 PM	Success		R1-user	Authentication		Policy-Device-Admin >> AuthZ-For-R1	ISE	R1	192.168.1.1
Jan 09, 2020 03:51:08.879 PM	Success		R1-user	Authentication	Policy-Device-Admin >> Default		ISE	R1	192.168.1.1

The ISE TACACS Logs confirms Authorization failed, matching the default Authorization Policy **Default** and default TACACS Profile **Deny All Shell Profile**.

Overview

Request Type	Authentication
Status	Fail
Session Key	ISE/363103442/373
Message Text	Failed-Attempt: Authentication failed
Username	R2-user
Authentication Policy	Policy-Device-Admin >> Default
Selected Authorization Profile	Deny All Shell Profile

Authentication Details

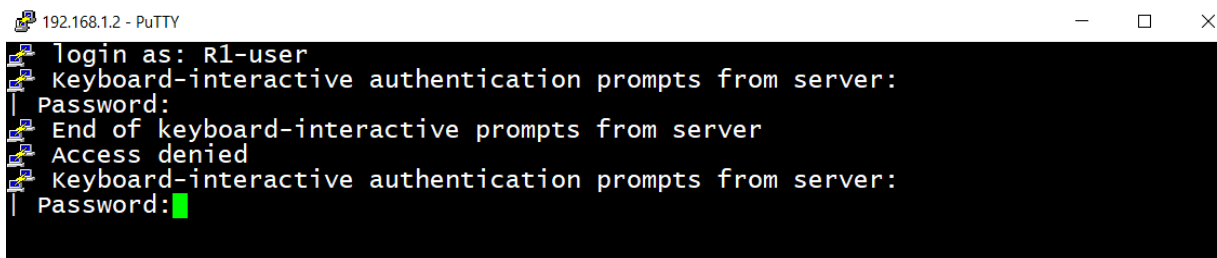
Generated Time	2020-01-09 15:56:05.535000 +00:00
Logged Time	2020-01-09 15:56:05.535
Epoch Time (sec)	1578585365
ISE Node	ISE
Message Text	Failed-Attempt: Authentication failed
Failure Reason	13036 Selected Shell Profile is DenyAccess
Resolution	Check whether the Device Administration Authorization Policy rules are correct
Root Cause	Selected Shell Profile fails for thsi request
Username	R2-user
Network Device Name	R1
Network Device IP	192.168.1.1
Network Device Groups	IPSEC#s IPSEC Device#No,Location#All Locations#New-York,Device Type#All Device Types#All Routers
Device Type	Device Type#All Device Types#All Routers
Location	Location#All Locations#New-York
Device Port	tty388
Remote Address	192.168.1.10

Steps

13013 Received TACACS+ Authentication START Request
15049 Evaluating Policy Group
15008 Evaluating Service Selection Policy
15048 Queried PIP - DEVICE.Device Type
15041 Evaluating Identity Policy
15013 Selected Identity Source - Internal Users
13045 TACACS+ will use the password prompt from global TACACS+ configuration
13015 Returned TACACS+ Authentication Reply
13014 Received TACACS+ Authentication CONTINUE Request (🕒 Step latency=4593ms)
15041 Evaluating Identity Policy
15013 Selected Identity Source - Internal Users
24210 Looking up User in Internal Users IDStore
24212 Found User in Internal Users IDStore
22037 Authentication Passed
15036 Evaluating Authorization Policy
15048 Queried PIP - TACACS.User
15048 Queried PIP - Network Condition.R2_IP_Address
13036 Selected Shell Profile is DenyAccess
13015 Returned TACACS+ Authentication Reply

Return to your **Admin PC**, and use PUTTY to open an SSH session to **R2** router (**192.168.1.2**).

Login using the credentials **R1-user / Cisco1234**. This should fail.



```
192.168.1.2 - PuTTY
Login as: R1-user
Keyboard-interactive authentication prompts from server:
Password:
End of keyboard-interactive prompts from server
Access denied
Keyboard-interactive authentication prompts from server:
Password:█
```

Navigate to **Operations > TACACS > Live Logs** to see that the authentication and authorization failed.

For the failed **R1-user** entry, click the **Details** icon.

Logged Time	Status	Details	Identity	Type	Authentication Policy	Authorization Policy	Ise Node	Network Device ...	Network Device
Jan 09, 2020 03:58:34.561 PM	✖		R1-user	Authentication	Policy-Device-Admin >> Default		ISE	R2	192.168.1.2
Jan 09, 2020 03:56:05.535 PM	✖		R2-user	Authentication	Policy-Device-Admin >> Default		ISE	R1	192.168.1.1
Jan 09, 2020 03:53:15.919 PM	✔		R2-user	Authorization		Policy-Device-Admin >> AuthZ-For-R2	ISE	R2	192.168.1.2
Jan 09, 2020 03:53:15.888 PM	✔		R2-user	Authentication	Policy-Device-Admin >> Default		ISE	R2	192.168.1.2
Jan 09, 2020 03:51:09.071 PM	✔		R1-user	Authorization		Policy-Device-Admin >> AuthZ-For-R1	ISE	R1	192.168.1.1
Jan 09, 2020 03:51:08.879 PM	✔		R1-user	Authentication	Policy-Device-Admin >> Default		ISE	R1	192.168.1.1

The ISE TACACS Logs confirms Authorization failed, matching the default Authorization Policy **Default** and default Tacacs Profile **Deny All Shell Profile**.

Overview

Request Type	Authentication
Status	Fail
Session Key	ISE/363103442/375
Message Text	Failed-Attempt: Authentication failed
Username	R1-user
Authentication Policy	Policy-Device-Admin >> Default
Selected Authorization Profile	Deny All Shell Profile

Authentication Details

Generated Time	2020-01-09 15:58:34.561000 +00:00
Logged Time	2020-01-09 15:58:34.561
Epoch Time (sec)	1578585514
ISE Node	ISE
Message Text	Failed-Attempt: Authentication failed
Failure Reason	13036 Selected Shell Profile is DenyAccess
Resolution	Check whether the Device Administration Authorization Policy rules are correct
Root Cause	Selected Shell Profile fails for thsi request
Username	R1-user
Network Device Name	R2
Network Device IP	192.168.1.2
Network Device Groups	IPSEC#Is IPSEC Device#No,Location#All Locations#San-Jose,Device Type#All Device Types#All Routers
Device Type	Device Type#All Device Types#All Routers
Location	Location#All Locations#San-Jose
Device Port	tty388
Remote Address	192.168.1.10

Steps

- 13013 Received TACACS+ Authentication START Request
- 15049 Evaluating Policy Group
- 15008 Evaluating Service Selection Policy
- 15048 Queried PIP - DEVICE.Device Type
- 15041 Evaluating Identity Policy
- 15013 Selected Identity Source - Internal Users
- 13045 TACACS+ will use the password prompt from global TACACS+ configuration
- 13015 Returned TACACS+ Authentication Reply
- 13014 Received TACACS+ Authentication CONTINUE Request (🕒 Step latency=4405ms)
- 15041 Evaluating Identity Policy
- 15013 Selected Identity Source - Internal Users
- 24210 Looking up User in Internal Users IDStore
- 24212 Found User in Internal Users IDStore
- 22037 Authentication Passed
- 15036 Evaluating Authorization Policy
- 15048 Queried PIP - TACACS.User
- 15048 Queried PIP - Network Condition.R1_IP_Address
- 13036 Selected Shell Profile is DenyAccess
- 13015 Returned TACACS+ Authentication Reply