

CISCO ISE TACACS CONFIGURATION

CREATE USERS



IDENTITY SERVICES ENGINE

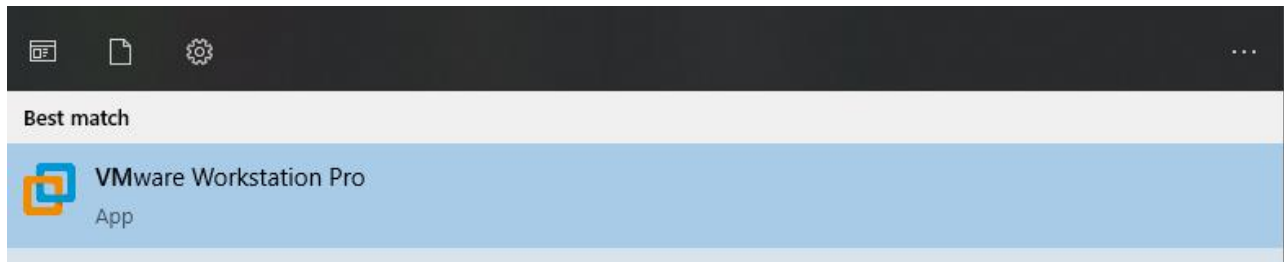
VMWARE WORKSTATION

WINDOWS SERVER 2022

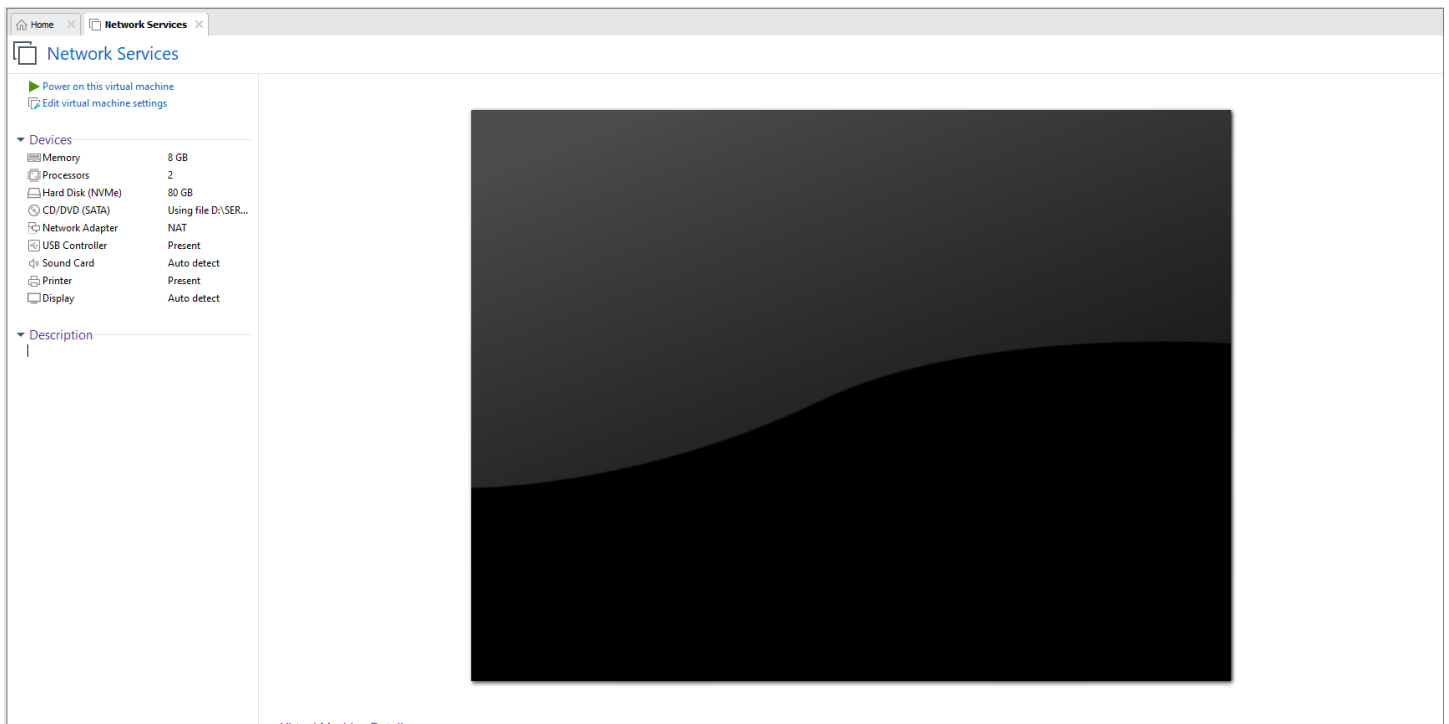
ISE-2.6.0.156-virtual-SNS3615-SNS3655-200.ova

CSR1000v

1.OPEN VMWARE WORKSTATION



2.CHEK IF YOU HAVE WINDOWS SERVE 2022



SET THE NETWORK ADAPTER TO NAT

RAM 8 GB

THEN POWER IT ON

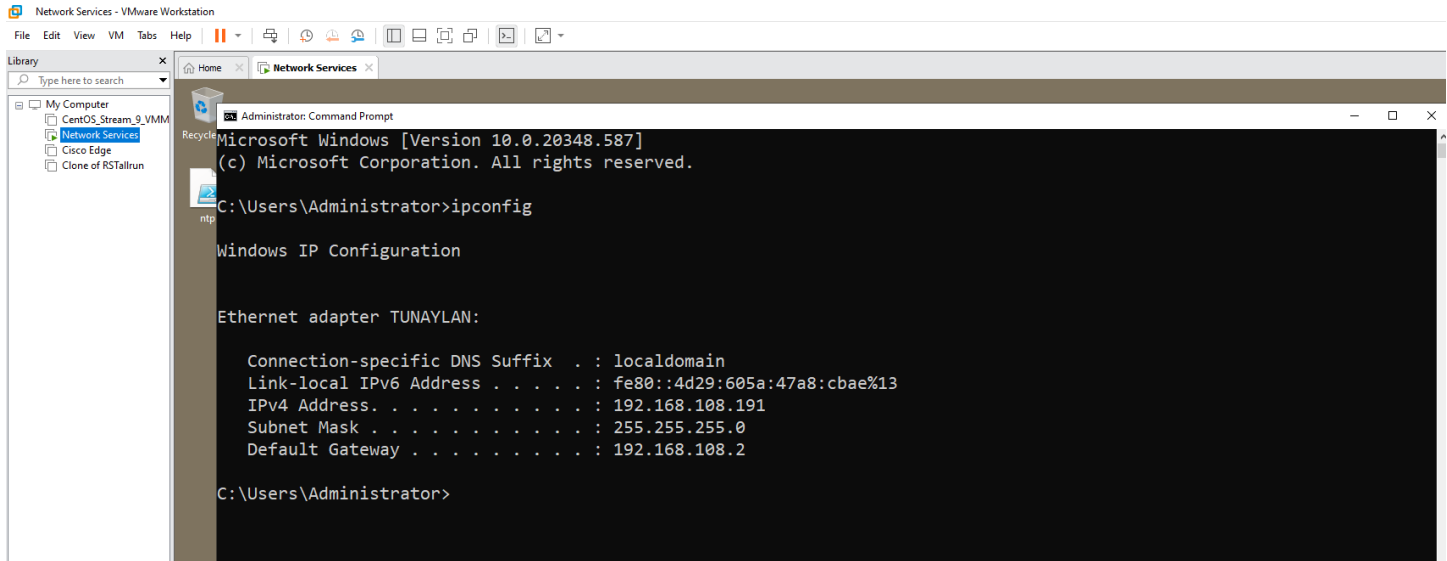
3.CHECK THE IP ADDRESS OF VIRTUAL WINDOWS SERVER

OPEN CMD

TYPE: ipconfig

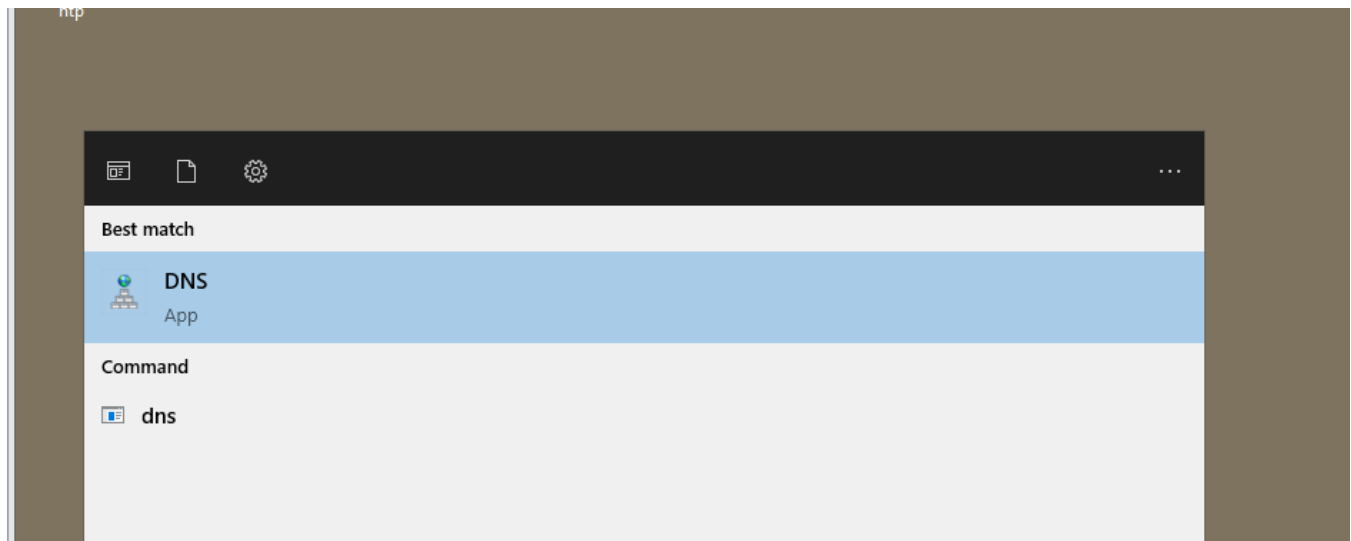
REMEMBER THE IP ADDRESS

192.168.108.191



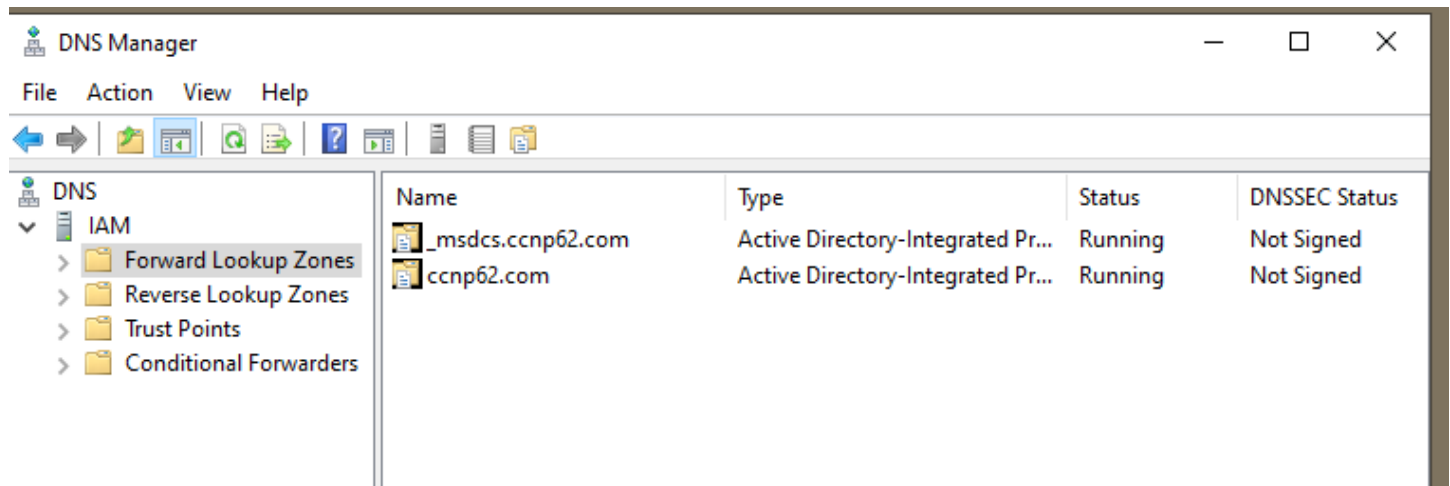
4.CHECK DNS – Domain Name Server

PRESS Windows KEY then type DNS

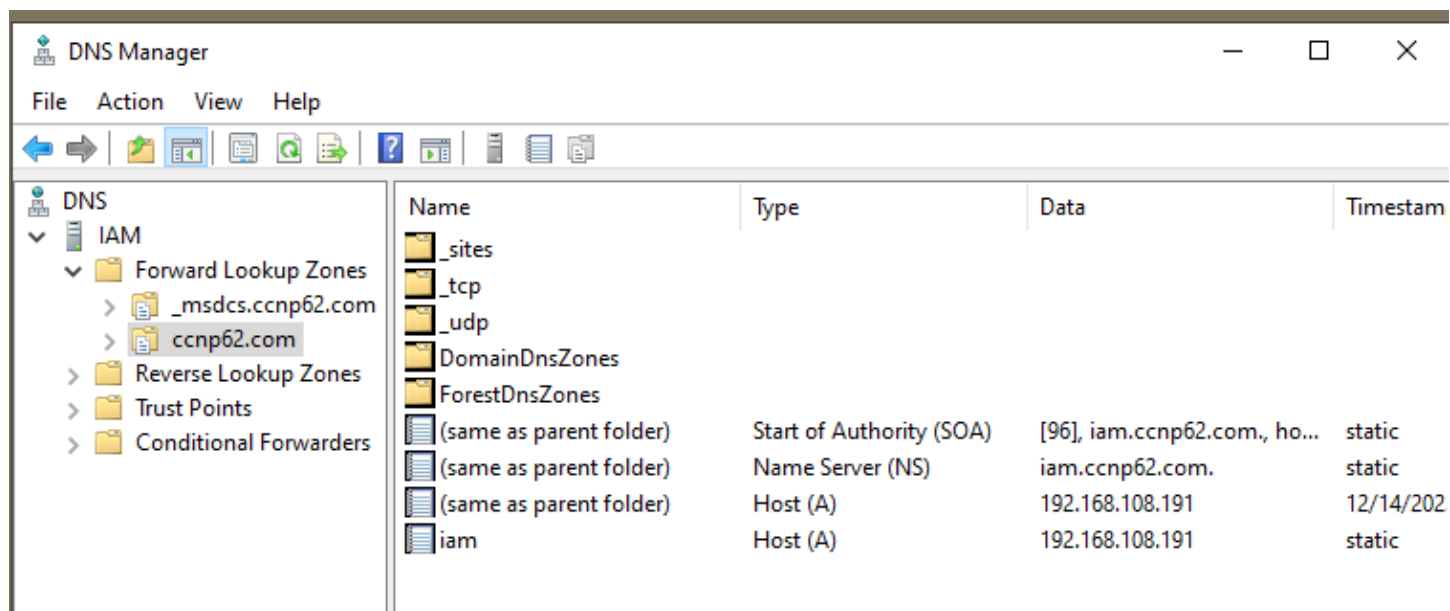


CHECK IF MAY DNS NA ccnpM.com

THEN DOUBEL CLICK ON IT

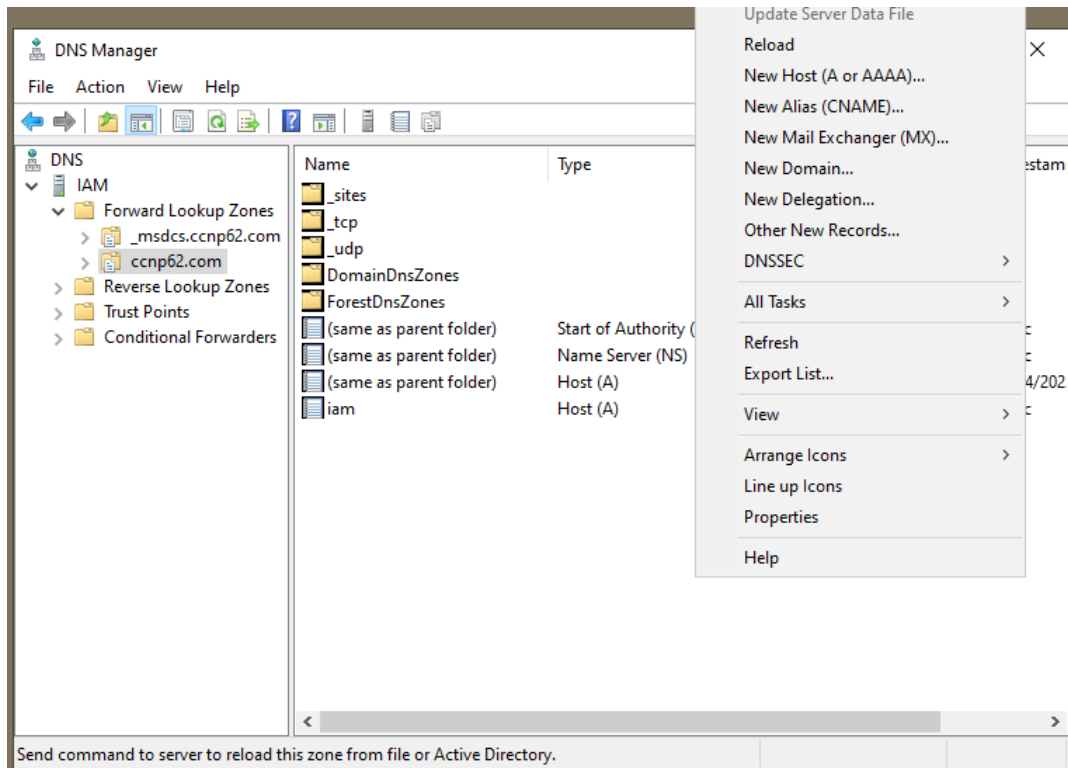


CHECK THE IP ADDRES IF THE SAME SILA SA IPCONFIG sa CMD

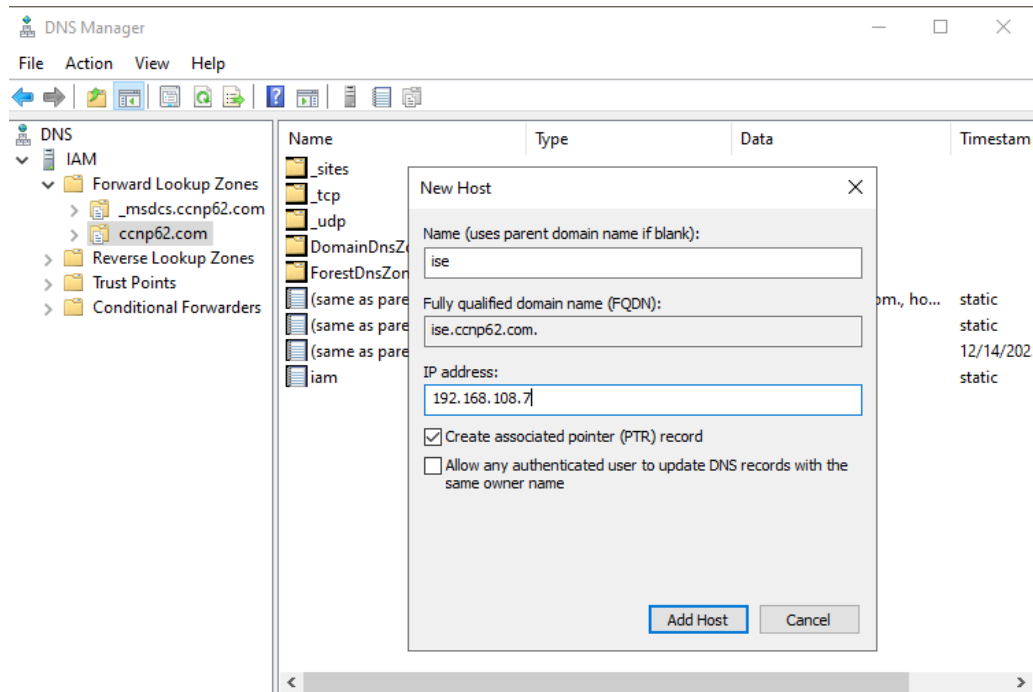


ADD ONE HOST NAME

RIGHT CLICK ON THE CCNPM.COM

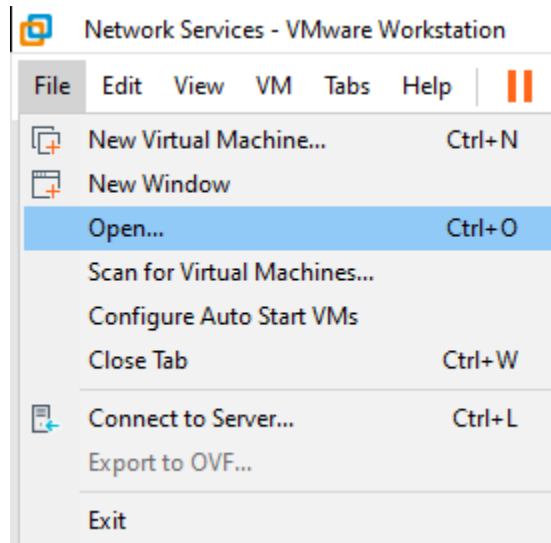


CLICK New Host (A or AAA) THEN FOLLOW THE INFO BELOW ADD HOST



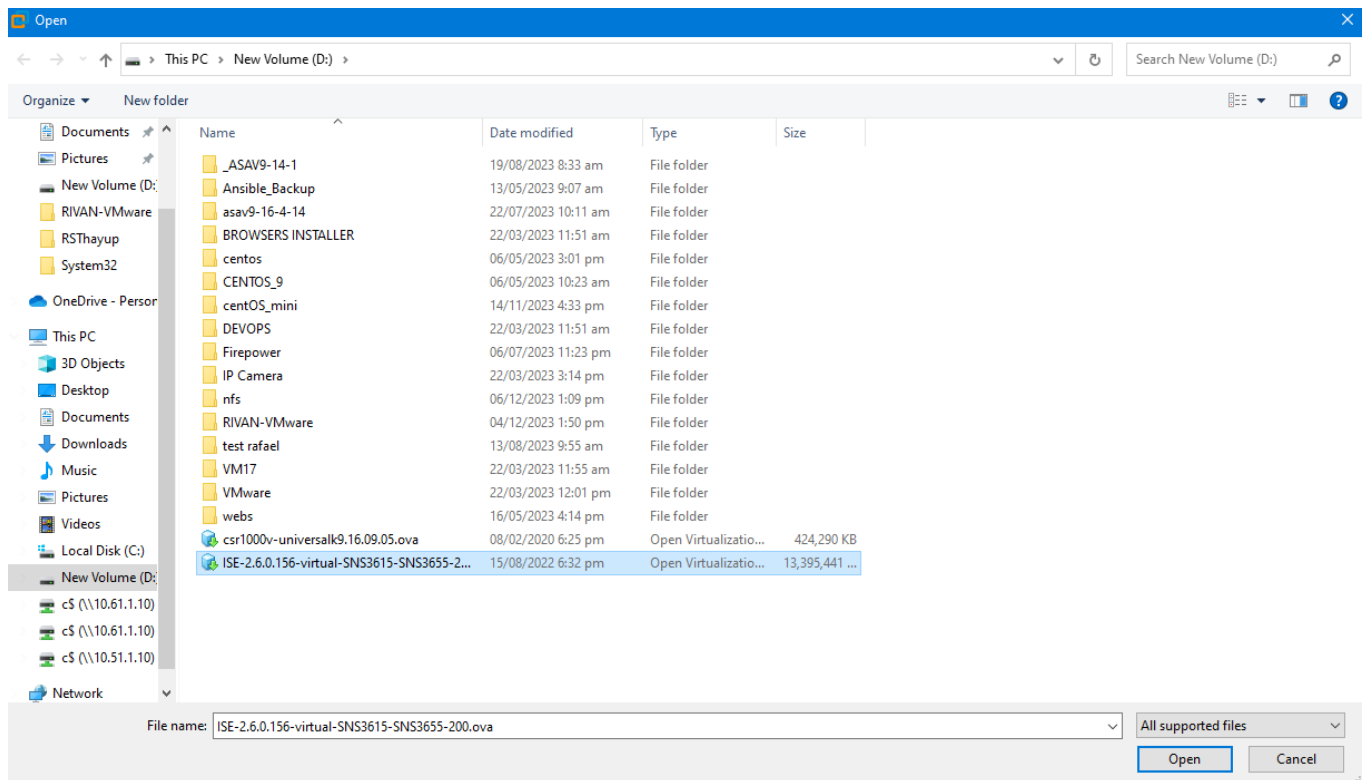
6.DEPLOY THE ISE.ova

CLICK FILE -> OPEN



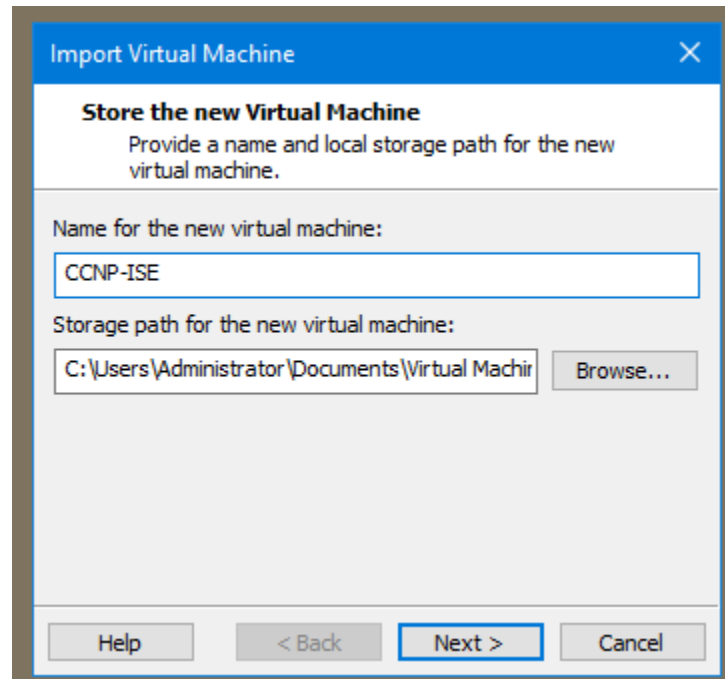
FIND THE ISE

Drive D -> ISE



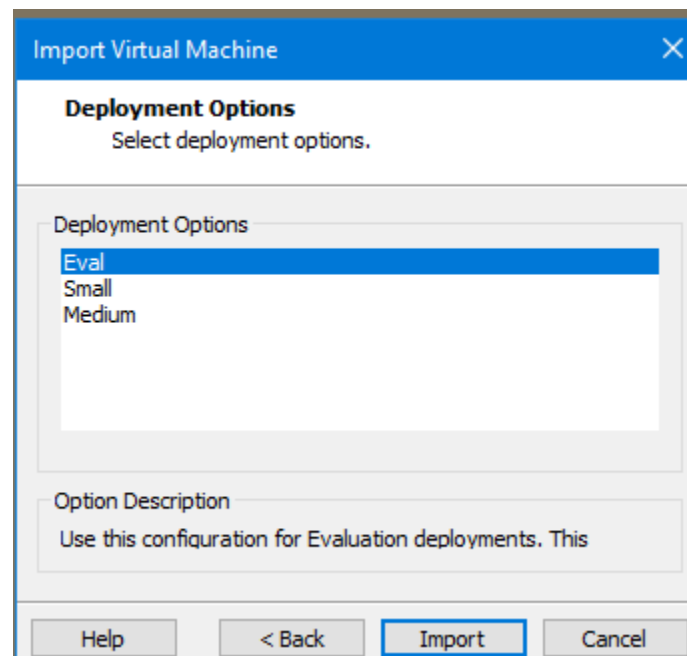
7.DEPLOY THE ISE.ova

Name: CCNP-ISE then CLICK Next



The 'Import Virtual Machine' dialog box has a blue title bar with a close button. The main section is titled 'Store the new Virtual Machine' with the instruction 'Provide a name and local storage path for the new virtual machine.' It contains two input fields: 'Name for the new virtual machine:' with the text 'CCNP-ISE' and 'Storage path for the new virtual machine:' with the text 'C:\Users\Administrator\Documents\Virtual Machir'. A 'Browse...' button is next to the storage path field. At the bottom are buttons for 'Help', '< Back', 'Next >' (highlighted with a blue border), and 'Cancel'.

Import



The 'Import Virtual Machine' dialog box shows the 'Deployment Options' section. It has a blue title bar with a close button. The section is titled 'Deployment Options' with the instruction 'Select deployment options.' It contains a list box with three options: 'Eval' (selected and highlighted in blue), 'Small', and 'Medium'. Below the list box is a text area labeled 'Option Description' with the text 'Use this configuration for Evaluation deployments. This'. At the bottom are buttons for 'Help', '< Back', 'Import' (highlighted with a blue border), and 'Cancel'.



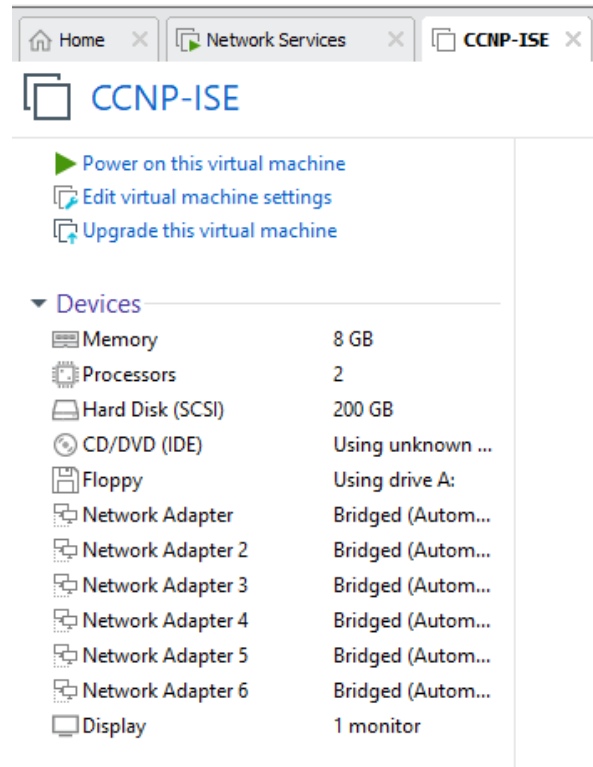
The 'VMware Workstation' progress bar shows the status 'Importing CCNP-ISE'. It features a progress bar with a green indicator on the left and a 'Cancel' button on the right.

8.EDIT THE SETTINGS OF ISE VIRTUAL MACHINE

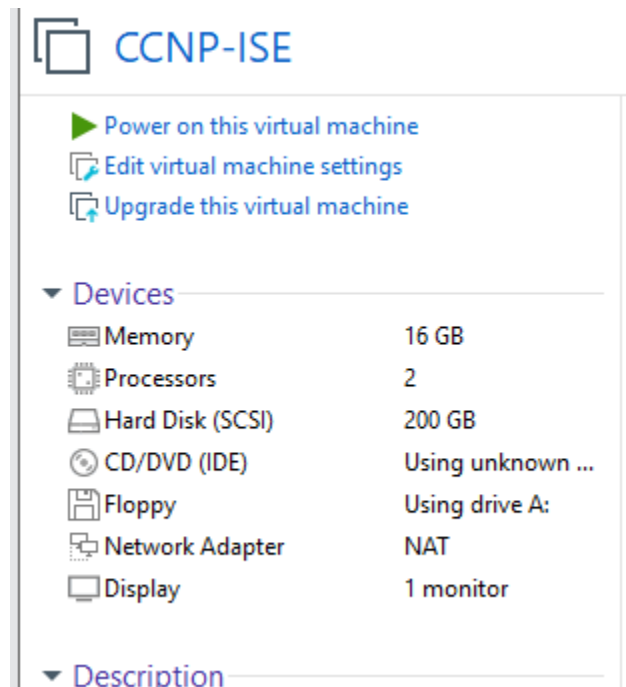
SET THE RAM TO 16 GB

SET THE NETWORK ADAPTER TO NAT

REMOVE THE NETWORK 2-6



UPDATED



THEN POWER IT ON

9.TYPE "setup"

```
Network Services x CCNP-ISE x
*****
Please type 'setup' to configure the appliance
*****
localhost login: setup_
```

```
Press 'Ctrl-C' to abort setup
Enter hostname[]: ISE62
Enter IP address[]: 192.168.108.7
Enter IP netmask[]: 255.255.255.0
Enter IP default gateway[]: 192.168.108.2
Do you want to configure IPv6 address? Y/N [N]: N
Enter default DNS domain[]: ccnp62.com
Enter primary nameserver[]: 192.168.108.191
Add secondary nameserver? Y/N [N]: N
Enter NTP server[time.nist.gov]: 192.168.108.191
Add another NTP server? Y/N [N]: N
Enter system timezone[UTC]: UTC
Enable SSH service? Y/N [N]: Y
Enter username[admin]: admin
Enter password:
Enter password again: _
```

192.168.108.191 – IP ADD OF MY Windows Server Virtual (NTP,NAME SERVER)

```
Home x Network Services x CCNP-ISE x
ISE62 login: admin
Password:
Failed to log in 0 time(s)
ISE62/admin# _
```

Admin

C1sc0123

10.OPEN CMD THEN PING THE IP ADDRESS OF ISE – 192.168.108.7

```
Administrator: Command Prompt
Microsoft Windows [Version 10.0.20348.587]
(c) Microsoft Corporation. All rights reserved.

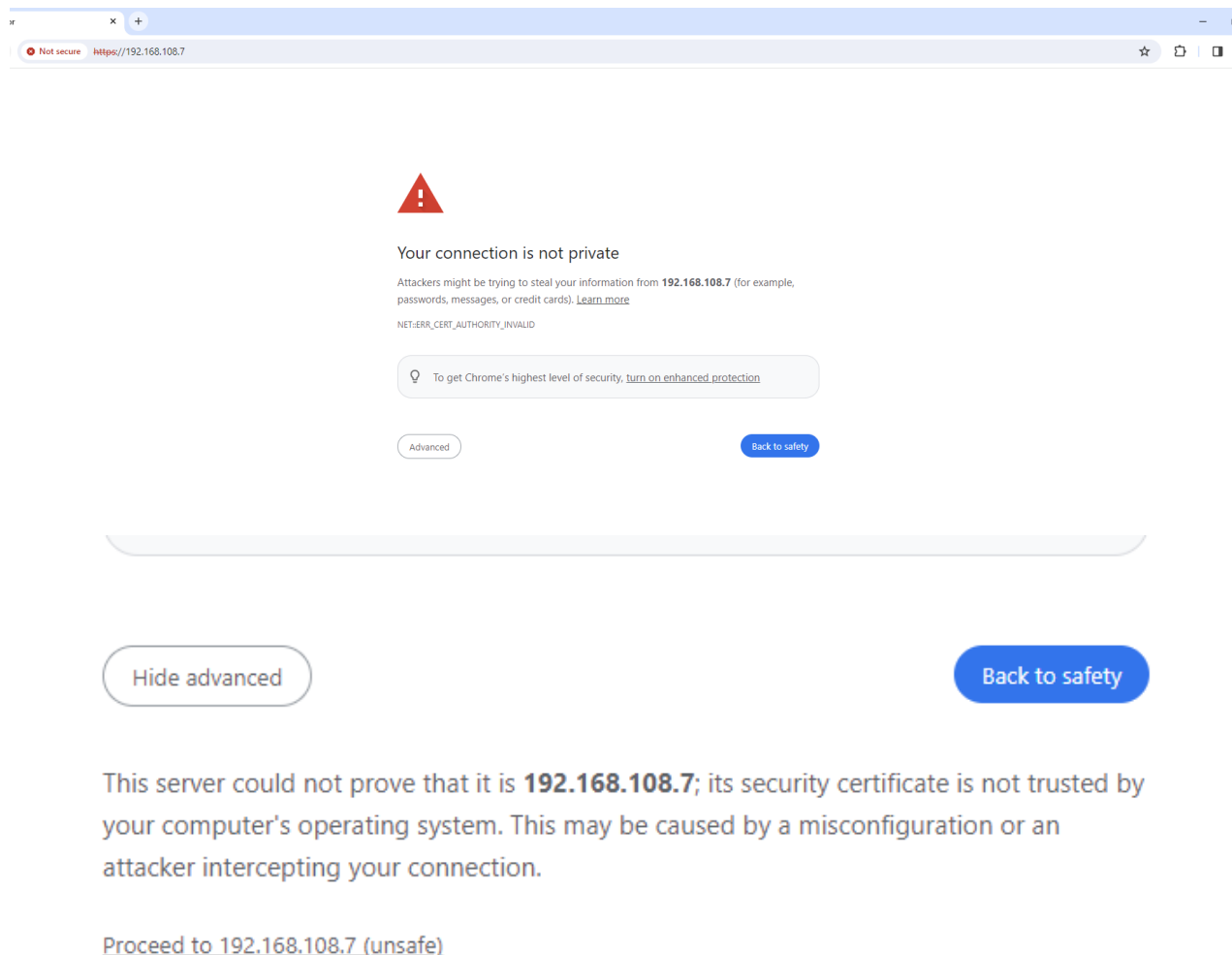
C:\Users\Administrator>ping 192.168.108.7

Pinging 192.168.108.7 with 32 bytes of data:
Reply from 192.168.108.7: bytes=32 time<1ms TTL=64
Reply from 192.168.108.7: bytes=32 time<1ms TTL=64
Reply from 192.168.108.7: bytes=32 time<1ms TTL=64
Reply from 192.168.108.7: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.108.7:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Users\Administrator>
```

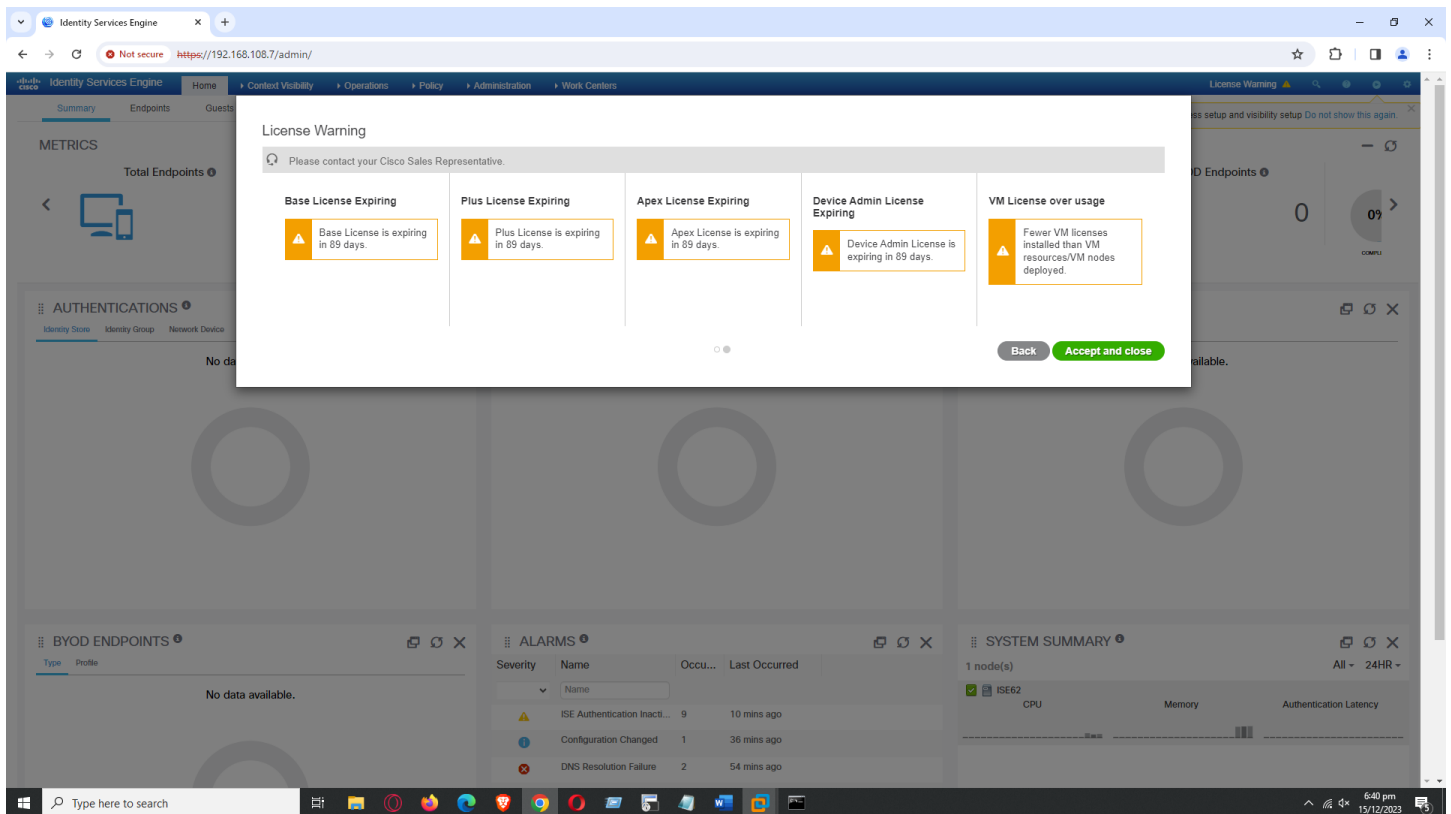
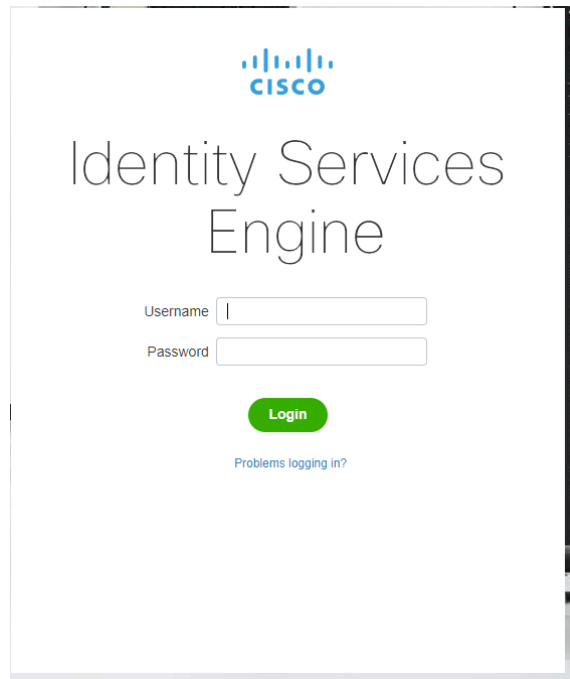
11.OPEN ANY BROWSER TYPE : <https://192.168.108.7>



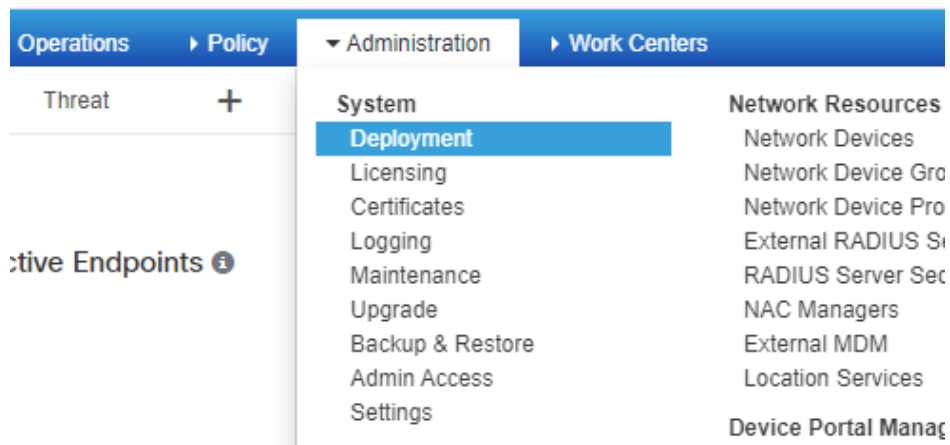
12.GUI OF ISE

admin

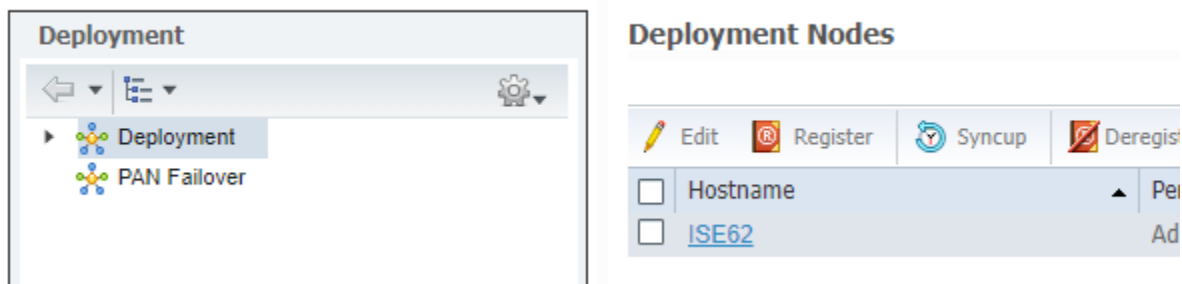
C1sc0123



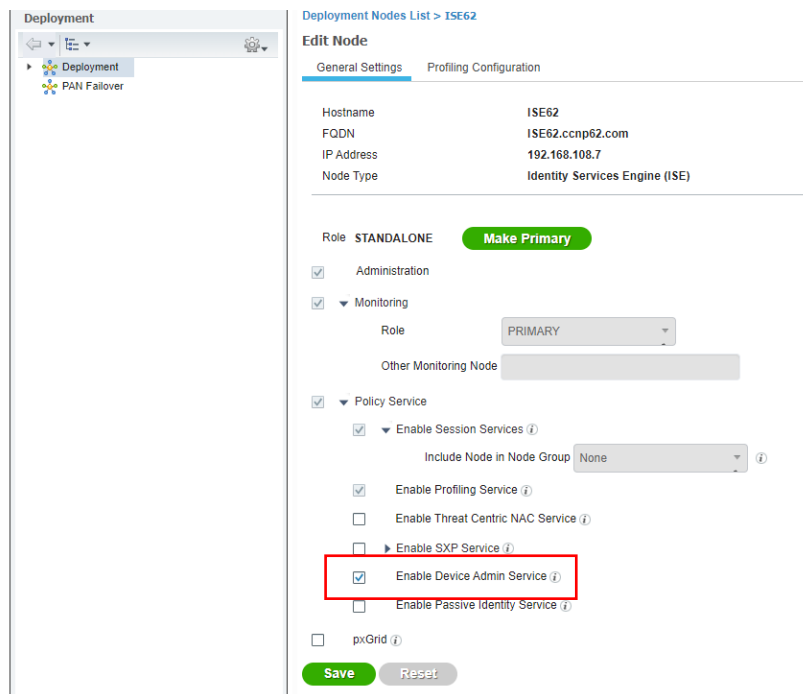
13.GO TO ADMINISTRATION - DEPLOYMENT



CLICK ISE-M



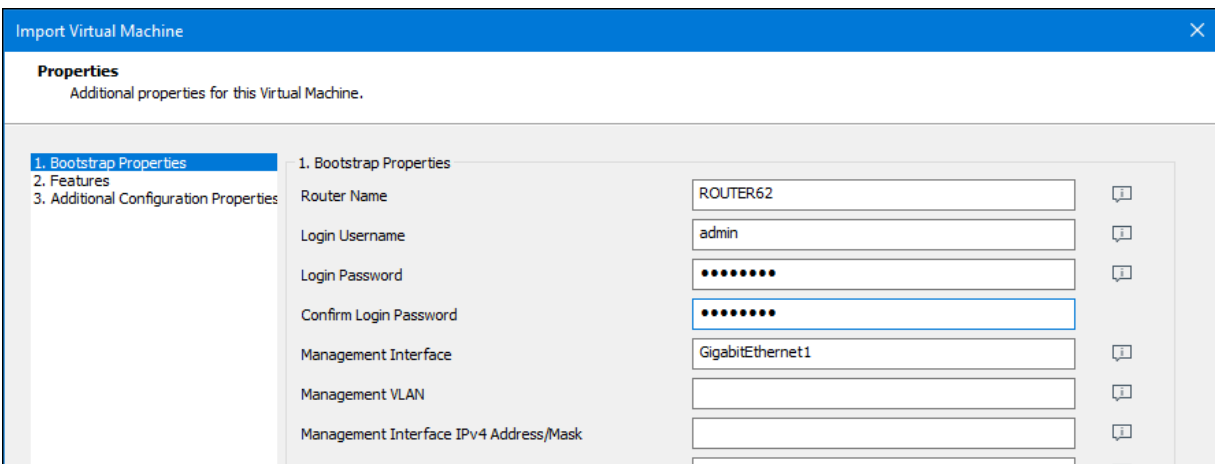
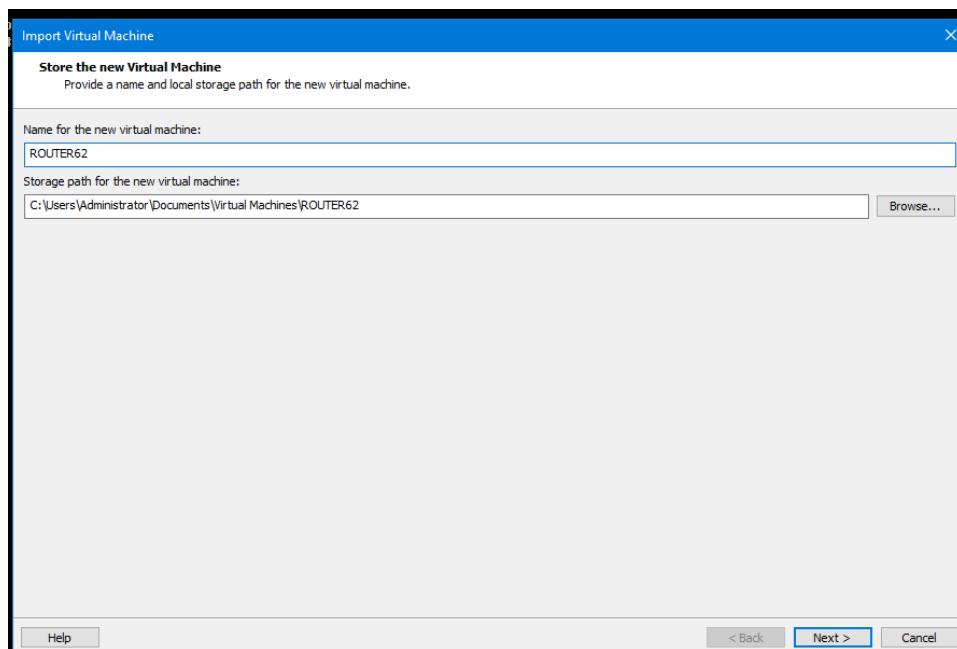
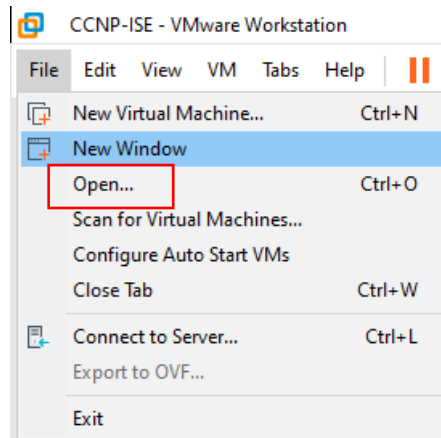
14. ENABLE DEVICE ADMIN SERVICE



CLICK SAVE

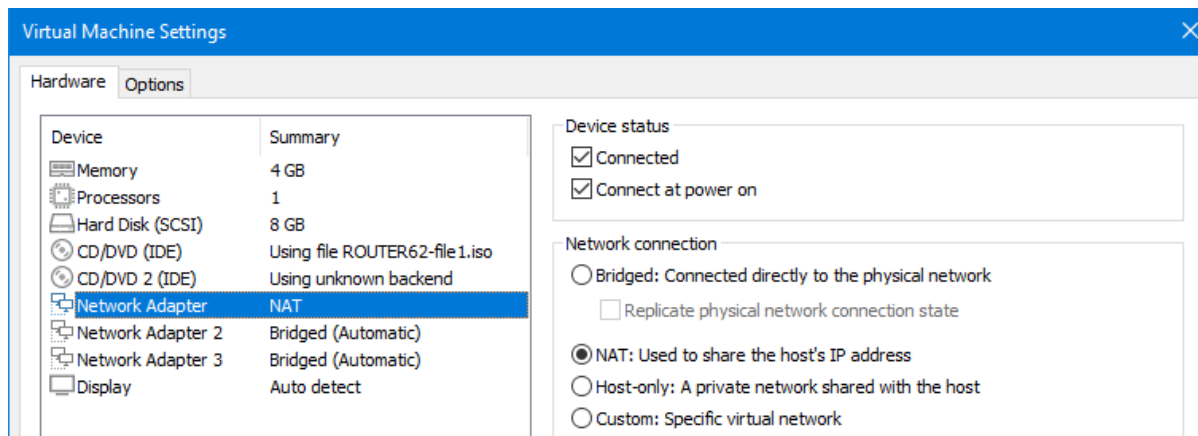
15. DEPLOY A CSR 1000v

File – OPEN – FIND THE CSR1000v (D-Rivanapp-IOS)



THEN CLICK IMPORT

Set the Network Adapter of CSR 1000v to NAT



16. TYPE THIS COMMAND TO CSR1000v AFTER BOOTING

Enable

Conf t

Int gi 1

Ip add 192.168.108.100 255.255.255.0

No shut

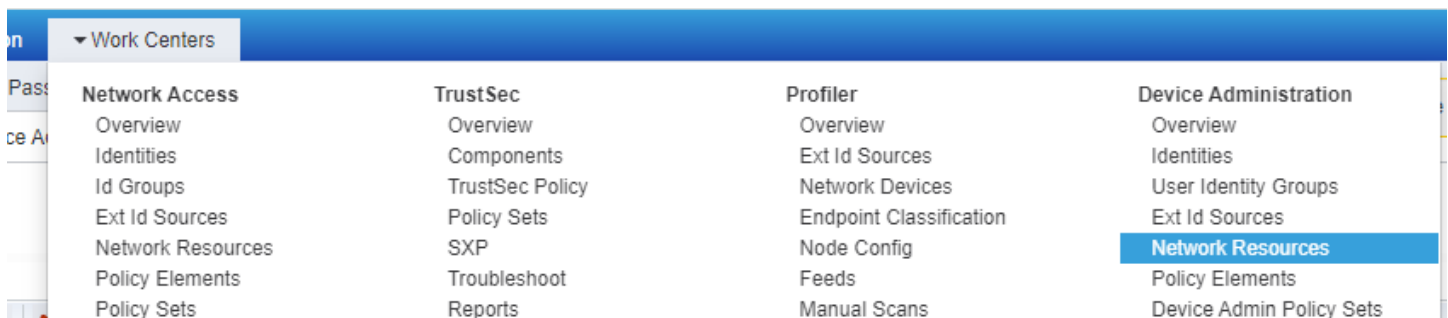
THEN PING THE IP ADDRESS OF 192.168.108.100 TO CMD TUNAY NA PC

```
C:\Users\Administrator>ping 192.168.108.100

Pinging 192.168.108.100 with 32 bytes of data:
Request timed out.
Reply from 192.168.108.100: bytes=32 time=1ms TTL=255
Reply from 192.168.108.100: bytes=32 time=1ms TTL=255
Reply from 192.168.108.100: bytes=32 time=1ms TTL=255

Ping statistics for 192.168.108.100:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

17. GO BACK THE GUI OF ISE – GO TO WORK CENTERS – DEVICE ADMINISTRATION – NETWORK RESOURCES



CLICK ADD

Network Devices

Network Device Groups

Default Devices

TACACS External Servers

TACACS Server Sequence

Network Devices

Edit

Add

Duplicate

Import

Export

Generate PAC

Delete

Name	IP/Mask	Profile Name	Location
------	---------	--------------	----------

FOLLOW THIS SETTINGS

Network Devices

Network Device Groups

Default Devices

TACACS External Servers

TACACS Server Sequence

Network Devices List > New Network Device

Network Devices

Name

CSR1

Description

IP Address

* IP : 192.168.108.100 / 32

Device Profile

Cisco

Model Name

Unknown

Software Version

Unknown

* Network Device Group

Location

All Locations

Set To Default

IPSEC

No

Set To Default

Device Type

All Device Types

Set To Default

RADIUS Authentication Settings

TACACS Authentication Settings

Shared Secret

C1sc0123

Hide

Enable Single Connect Mode

Legacy Cisco Device

TACACS Draft Compliance Single Connec

SNMP Settings

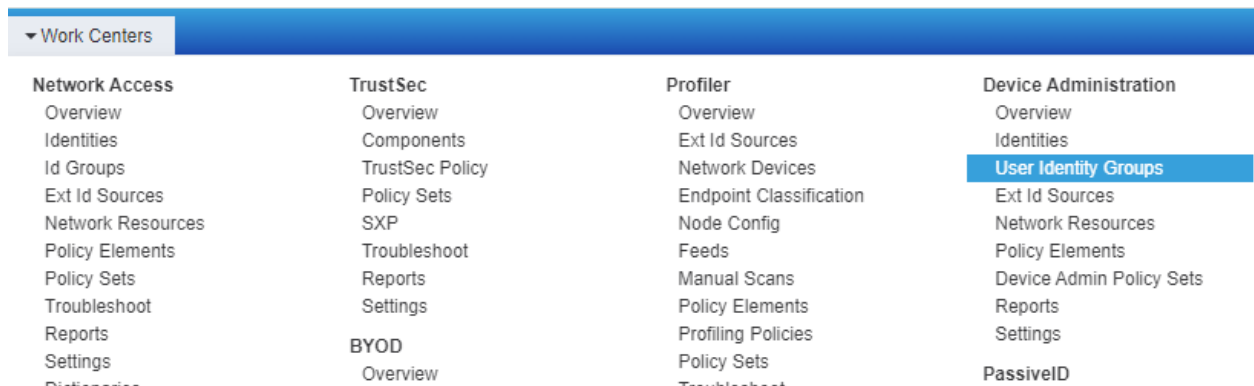
Advanced TrustSec Settings

Submit

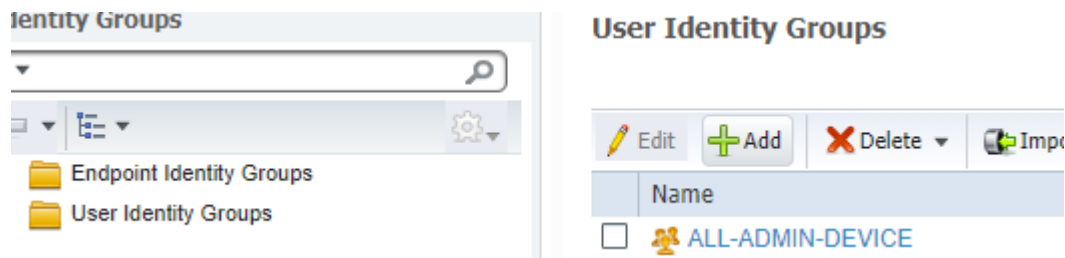
Cancel

THEN CLICK SUBMIT

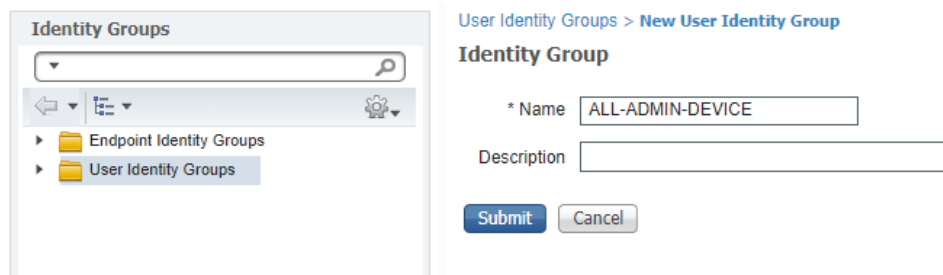
18. GO TO – WORK CENTERS – DEVICE ADMINISTRATION – USER IDENTITY GROUPS



CLICK ADD

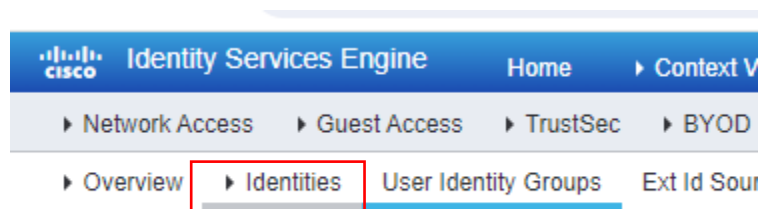


NAME: ALL-ADMIN-DEVICE



THEN CLICK SUBMIT

19. CLICK IDENTITIES



CLICK “ADD”

Users

Network Access Users

Edit

Add

Change Status

Status	Name
--------	------

FOLLOW THIS SETUP

Users

Network Access Users List > New Network Access User

Network Access User

* Name

ccnp62

Status

☒ Enabled

Email

Passwords

Password Type:

Internal Users

Password

Re-Enter Password

Generate Password

Enable Password

Generate Password

User Information

First Name

Last Name

Account Options

Description

Change password on next login

☐

Account Disable Policy

☐ Disable account if date exceeds

2024-02-13

(yyyy-mm-dd)

User Groups

ALL-ADMIN-DEVICE

Submit

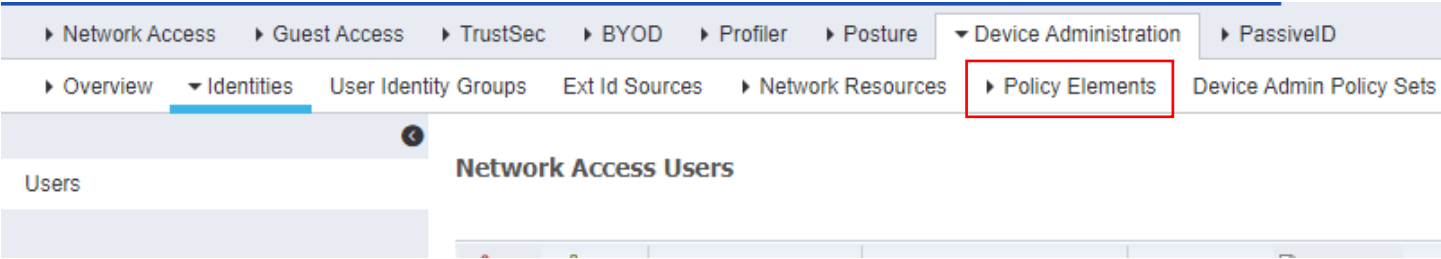
Cancel

THEN CLICK “SUBMIT”

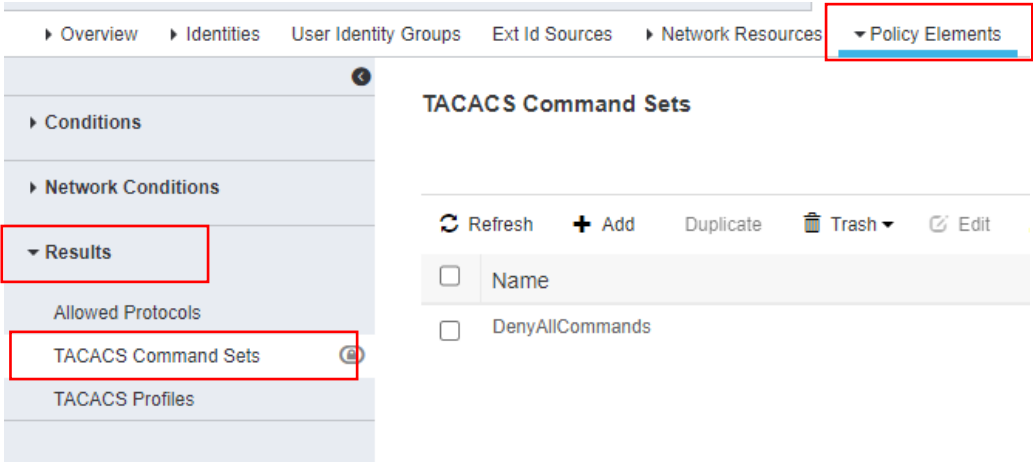
Users

Status	Name	Description	First Name	Last Name	Email Address	User Identity Groups	Admin
<input checked="" type="checkbox"/> Enabled	ccnp62					ALL-ADMIN-DEVICE	

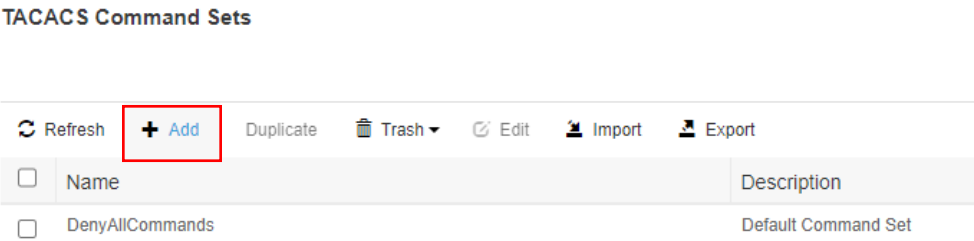
20. CLICK POLICY ELEMENTS



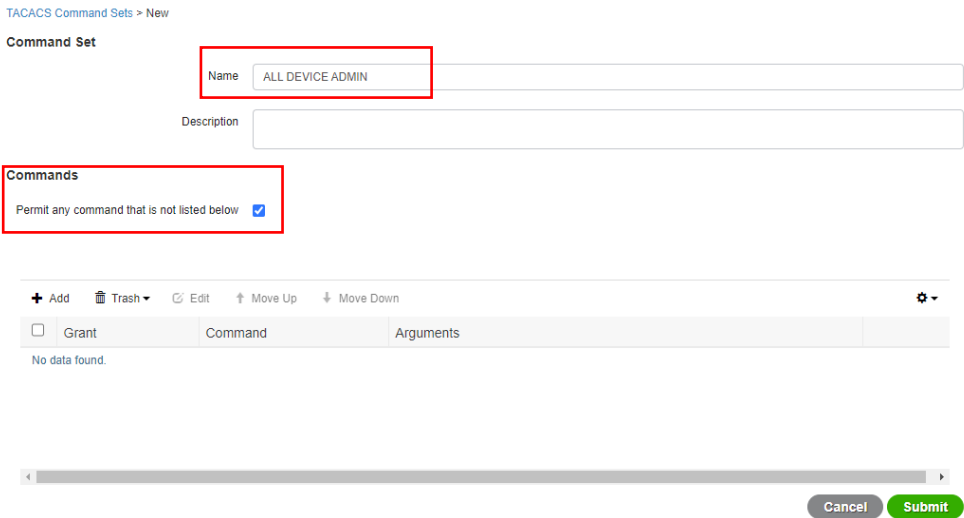
Policy Elements – Results – TACACS Command Sets



CLICK “ADD”

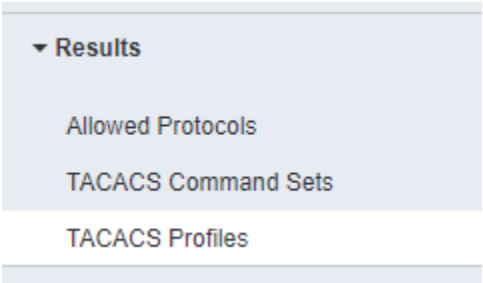


FOLLOW THIS SETUP



CLICK SUBMIT

21. GO TO TACACS PROFILE



CLICK ADD

TACACS Profiles

Refresh

+

Add

Duplicate

Trash

Edit

<input type="checkbox"/>	Name	Type	Description
<input type="checkbox"/>	Default Shell Profile	Shell	Default Shell Profile
<input type="checkbox"/>	Deny All Shell Profile	Shell	Deny All Shell Profile
<input type="checkbox"/>	WLC ALL	WLC	WLC ALL
<input type="checkbox"/>	WLC MONITOR	WLC	WLC MONITOR

FOLLOW THIS SETUP

TACACS Profile

Name

ALL_DEVICE_ADMIN

Description

Task Attribute View

Raw View

Common Tasks

Common Task Type

Shell

☒ Default Privilege

15

(Select 0 to 15)

☒ Maximum Privilege

15

(Select 0 to 15)

☐ Access Control List

☐ Auto Command

☐ No Escape

(Select true or false)

☐ Timeout

Minutes (0-9999)

☐ Idle Time

Minutes (0-9999)

Custom Attributes

+

Add

Trash

Edit

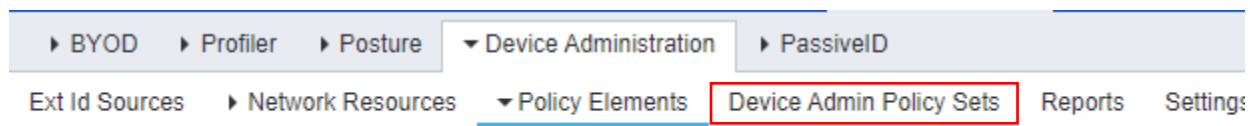
<input type="checkbox"/>	Type	Name	Value
No data found.			

Cancel

Submit

CLICK SUBMIT

22. GO TO DEVICE ADMIN POLICY SETS



CLICK THE + SIGN

Policy Sets

	Status	Policy Set Name	Description	Conditions
<input type="text" value="Search"/>				

NAME: Cisco Devices

	Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
<input type="text" value="Search"/>								
		Cisco Devices			<input type="text" value="Select from list"/>			

CLICK THE + SIGN

THEN FOLLOW THIS SETUP

Conditions Studio

Library

No conditions found - reset filters.

Editor

TACACS-User

In

Network Access-UserName

Set to 'is not'

Duplicate

Save

New

AND

OR

Close

Use

THEN CLICK “USE”

SELECT : DEFAULT DEVICE ADMINS

+	Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
Search								
		Cisco Devices		TACACS User IN Network Access-UserName	Default Device Admin			

CLICK SAVE

Default Device Admin

Default Device Admin

0

Reset

Save

CLICK THE GREATER THAN SIGN “>”

Default Device Admin

Save or reset before navigation

Expand “Authentication Policy (1)”

Internal Users

▼ Authentication Policy (1)

+

Status

Rule Name

Conditions

Use

Hits

Search

Default

Internal Users

Options

0

THEN EXPAND “ Authorization Policy (1)”

CLICK THE + Sign

➤ Authorization Policy - Local Exceptions

➤ Authorization Policy - Global Exceptions

▼ Authorization Policy (1)

+	Status	Rule Name	Conditions	Results		Hits	Actions
				Command Sets	Shell Profiles		
<div>Search</div>							
+							
✔	Default			DenyAllCommands	Deny All Shell Profile	0	⚙

Reset

Save

CLIK THE + SIGN

▼ Authorization Policy (2)									
+	Status	Rule Name	Conditions	Results		Hits	Actions		
				Command Sets	Shell Profiles				
Search									
		ALL-DEVICE-ADMIN		Select from list					
	Default			DenyAllCommands			Deny All Shell Profile		

FOLLOW THIS SETUP

The screenshot shows the Cisco Conditions Studio interface. On the left is the 'Library' pane with a search bar and a list of conditions: EAP-MSCHAPv2, EAP-TLS, Guest_Flow, and Network_Access_Authentication_Passed. The main 'Editor' pane shows a configuration for the 'InternalUser: IdentityGroup' field. The operator is set to 'Equals'. The value is 'User Identity Groups:ALL-ADMIN-DEVICE', which is highlighted with a red box. Below the value field is a 'Save' button. At the bottom of the editor is a dashed box containing a '+ New AND OR' button. Below the editor is a table with columns: Status, Rule Name, Conditions, Results, Command Sets, Shell Profiles, Hits, and Actions. The table contains one row with the rule name 'ALL-DEVICE-ADMIN' and the condition 'InternalUser: IdentityGroup EQUALS User Identity Groups:ALL-ADMIN-DEVICE'.

THEN CLICK SAVE

23. GO BACK TO CSR1000v TYPE THIS COMMAND

config t

aaa new-model

tacacs-server host 192.168.108.7

tacacs-server key C1sc0123

aaa authentication login default group tacacs+ local

do debug aaa authentication

do debug tacacs

end

conf t

enable secret pass

service password-encryption

end

OPEN PUTTY THEN TRY TO LOGIN – 192.168.108.100

OPTIONAL #do test aaa group tacacs+ testadmin cisco legacy