NetMet Solutions
Your Trusted Learning Partner

CCIE Security v6.1 – Identity Service Engine (ISE)

Index

Lab1 - Configuring the Base Network

Lab2 - Configuring Passwords in ISE

Lab3 - Configuring Network Configuration of ISE

Lab4 - Initializing ISE – GUI

Lab5 - Create Admin User Creation

Lab6 - Radius Protocol for Device Authentication

Lab7 - Radius Protocol for Device Authentication Exec Level.

Lab8 – TACAS+ Protocol for Device Authentication

Lab9 - Backup of ISE

Lab10 - Configure Mab and Dot1x

Lab 11 - Integrate Active Directory On ISE

Lab12 - TrustSec on ISE

Lab13 - Guest Access

Lab14 - PxGrid on ISE and FTD

Lab 15 - Configure PxGrid on WSA and ISE

Lab16 - Configure profiling on ISE

Lab17 - BYOD on ISE

Lab18 - Visibility Setup Wizard BYOD on ISE on ISE

Lab19 - DNAC ISE Integration

Lab 20 - ISE Deployment Distributed Setup

Lab21 - ISE Posture Configuration

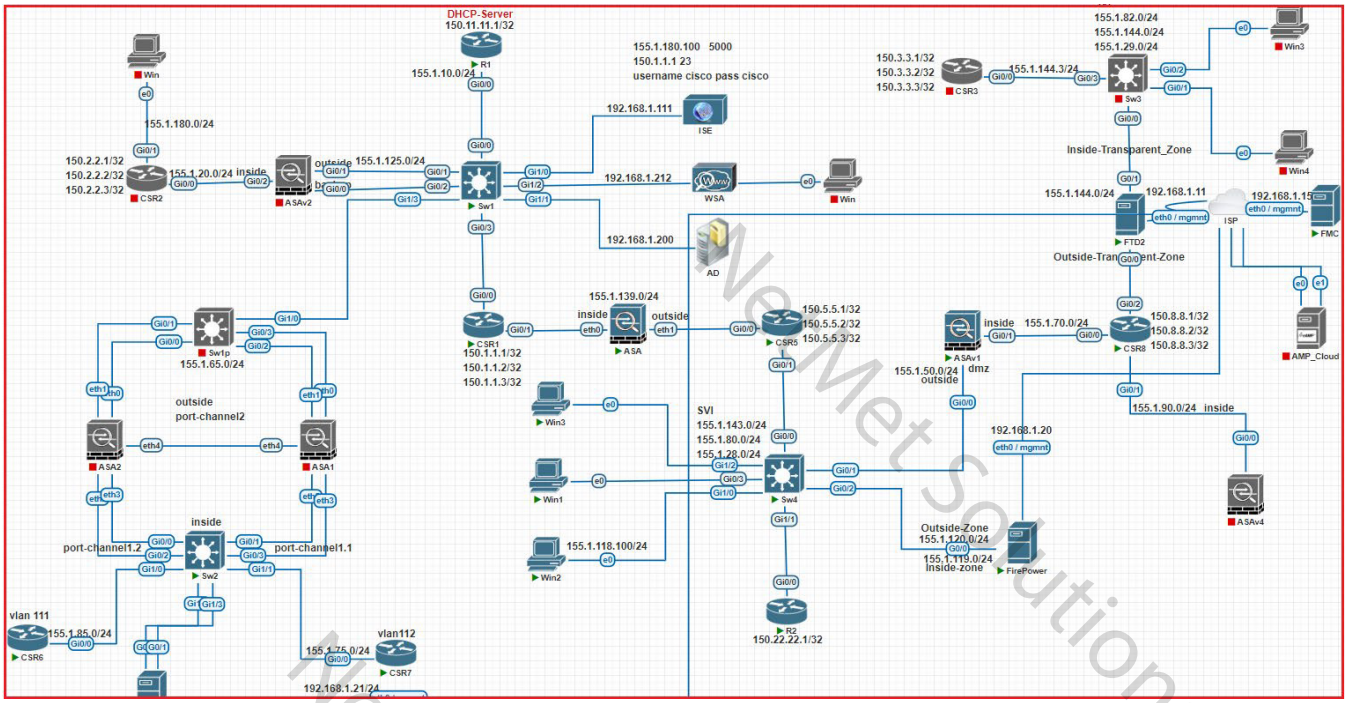
NetMet Solutions

NetMet Solutions

NetMet Solutions

NetMet Solutions
Your Trusted Learning Partner

Lab 1 – Configuring the Base Network



Lab Scenario:

➢ Configuring the Base Network with VLANs, IP Addressing & Routing

Initial Setup:

➢ Not required

Lab Tasks:

Task 1

Configure R1 g0/0 Sub Interface. Use Dot1q as the trunking encapsulation. And Configure R1 as DHCP Server. Configure Routing protocol OSPF.

R1

```
!
interface Loopback1
 ip address 150.11.11.1 255.255.255.255
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/0.1
 encapsulation dot1Q 1 native
 ip address 192.168.1.157 255.255.255.0
!
interface GigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 155.1.10.11 255.255.255.0
```

NetMet Solutions

```
!
interface GigabitEthernet0/0.65
 encapsulation dot1Q 65
 ip address 155.1.65.1 255.255.255.0
!

router ospf 1
 network 150.11.11.1 0.0.0.0 area 0
 network 155.1.10.0 0.0.0.255 area 0
 network 192.168.1.0 0.0.0.255 area 0
!
ip dhcp pool vlan80
 network 155.1.80.0 255.255.255.0
 default-router 155.1.80.250
!
ip dhcp pool vlan28
 network 155.1.28.0 255.255.255.0
!
ip dhcp pool vlan29
 network 155.1.29.0 255.255.255.0
 default-router 155.1.29.250
!
ip dhcp pool Sponsor
 network 155.1.120.0 255.255.255.0
 default-router 155.1.120.250
!
ip dhcp pool Geust-Portal
 network 155.1.130.0 255.255.255.0
 default-router 155.1.130.250
!
ip dhcp pool vlan82
 network 155.1.82.0 255.255.255.0
 default-router 155.1.82.250
!
ip dhcp pool vlan84
 network 155.1.84.0 255.255.255.0
 default-router 155.1.84.250
!
ip dhcp pool vlan85
 network 155.1.85.0 255.255.255.0
 default-router 155.1.85.250
!
ip dhcp pool vlan86
 network 155.1.86.0 255.255.255.0
 default-router 155.1.86.250
!
ip dhcp excluded-address 155.1.80.250
ip dhcp excluded-address 155.1.28.250
```

NetMet Solutions
NetMet Solutions
NetMet Solutions

NetMet Solutions
Your Trusted Learning Partner

```
ip dhcp excluded-address 155.1.29.250
ip dhcp excluded-address 155.1.20.250
ip dhcp excluded-address 155.1.130.250
ip dhcp excluded-address 155.1.82.250
ip dhcp excluded-address 155.1.84.250
ip dhcp excluded-address 155.1.85.250
ip dhcp excluded-address 155.1.86.250
```

Task 2

Configure SW1 g0/0 and g0/3 Interface as a Trunk towards R1 g0/0 and CSR1 g0/0 Interface. Use Dot1q as the trunking encapsulation.

SW1

```
!
interface GigabitEthernet0/0
switchport trunk encapsulation dot1q
switchport mode trunk
!
interface GigabitEthernet0/3
switchport trunk encapsulation dot1q
switchport mode trunk
```

Task 3

Configure VLANs on SW1 that will be used in the network. Create the following VLANS:

- ➢ VLAN 10
- ➢ VLAN 65
- ➢ VLAN 125
- ➢ VLAN 126

SW1

```
VLAN 10,65,125,126
```

Task 4

Configure CSR1 g0/0 Sub Interface. Use Dot1q as the trunking encapsulation. And Configure CSR1 g0/1 interface. Configure loopback also. And Routing protocol OSPF

CSR1

```
!
username admin privilege 15 password 0 cisco
!
interface Loopback1
ip address 150.1.1.1 255.255.255.255
interface Loopback2
ip address 150.1.1.2 255.255.255.255
interface Loopback3
ip address 150.1.1.3 255.255.255.255
!
interface GigabitEthernet0/0.10
encapsulation dot1Q 10
ip address 155.1.10.1 255.255.255.0
```

NetMet Solutions
NetMet Solutions
NetMet Solutions

```
!
interface GigabitEthernet0/1
ip address 155.1.139.1 255.255.255.0
no shut
!
interface GigabitEthernet0/2.111
encapsulation dot1Q 111
ip address 155.1.109.1 255.255.255.0
!
router ospf 1
router-id 1.1.1.1
network 155.1.10.0 0.0.0.255 area 0
network 155.1.30.0 0.0.0.255 area 0
network 155.1.40.0 0.0.0.255 area 0
network 155.1.139.0 0.0.0.255 area 0
```

Task 5

Configure ASA as transparent firewall. And configure BVI also. And allow TCP and UDP using Access-control List.

ASA

```
!
username admin password cisco privilege 15
!
interface BVI1
ip address 155.1.139.50 255.255.255.0
!
interface Ethernet0
nameif inside
bridge-group 1
security-level 100
!
interface Ethernet1
nameif outside
bridge-group 1
security-level 0
!
access-list outin extended permit ospf any any
access-list outin extended permit tcp any any eq www
access-list outin extended permit tcp any any eq https
access-list outin extended permit udp any any eq 1812
access-list outin extended permit udp any any eq 1813
access-list outin extended permit udp any any eq domain
access-list outin extended permit udp any any eq ntp
access-list outin extended permit tcp any any eq tacacs
access-list inout extended permit ip any any
!
access-group inout in interface inside
access-group outin in interface outside

firewall Transparent
```

Task 6

NetMet Solutions
NetMet Solutions
NetMet Solutions

Configure Loopback in CSR5. And interface g0/0. And Configure G0/1 sub interface following Requirement. Configure OSPF Routing Protocol.

CSR5

```
!
username admin privilege 15 password 0 cisco
!
interface Loopback1
ip address 150.5.5.1 255.255.255.255
!
interface Loopback2
ip address 150.5.5.2 255.255.255.255
!
interface Loopback3
ip address 150.5.5.3 255.255.255.255
!
interface GigabitEthernet0/0
ip address 155.1.139.5 255.255.255.0
no shut
!
interface GigabitEthernet0/1.50
encapsulation dot1Q 50
ip address 155.1.50.5 255.255.255.0
!
interface GigabitEthernet0/1.143
encapsulation dot1Q 143
ip address 155.1.143.5 255.255.255.0
!
router ospf 1
router-id 5.5.5.5
network 150.5.5.1 0.0.0.0 area 0
network 150.5.5.2 0.0.0.0 area 0
network 150.5.5.3 0.0.0.0 area 0
network 155.1.50.0 0.0.0.255 area 0
network 155.1.139.0 0.0.0.255 area 0
network 155.1.143.0 0.0.0.255 area 0
!
```

Task7

Configure VLANs on SW4 that will be used in the network. Create the following VLANS. Configure SW4 g0/0 Interface as a Trunk towards Use Dot1q as the trunking encapsulation. Configure SVI in SW4. And configure Routing protocol OSPF0.

- VLAN 29
- VLAN 82
- VLAN 84
- VLAN 85
- VLAN 86
- VLAN 143

Sw4.

Vlan 29,82,84,85,86,143

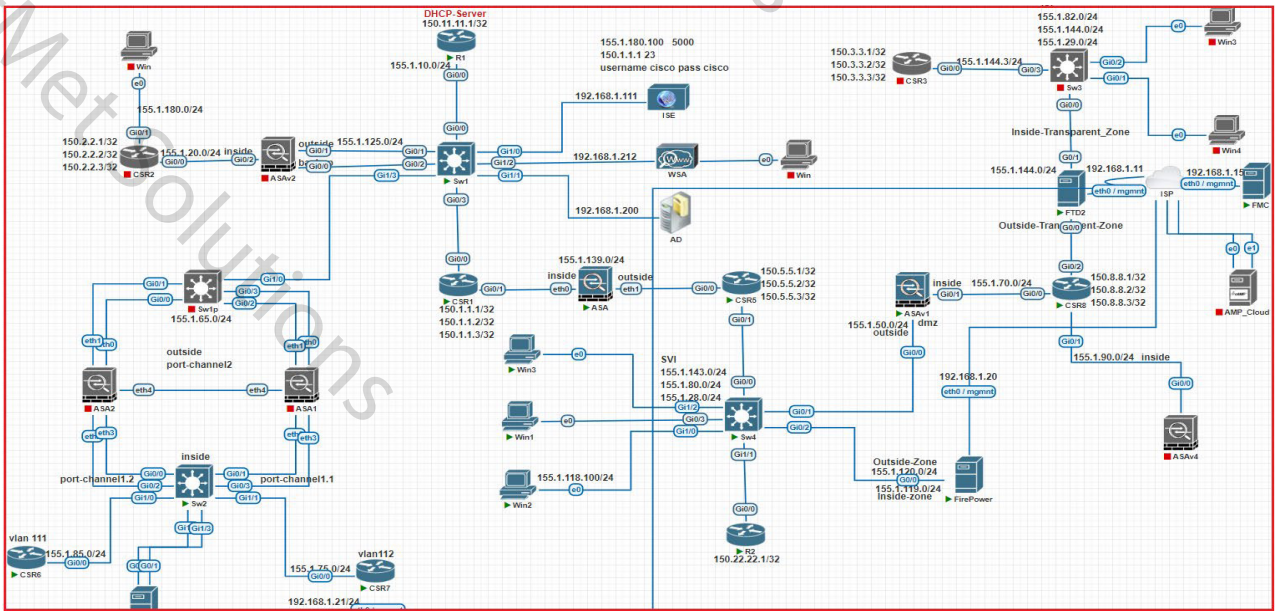
interface GigabitEthernet0/0

NetMet Solutions

NetMet Solutions
Your Trusted Learning Partner

```
 switchport trunk encapsulation dot1q
 switchport mode trunk
!
 interface Vlan29
 ip address 155.1.29.250 255.255.255.0
 !
 interface Vlan82
 ip address 155.1.82.250 255.255.255.0
 !
 interface Vlan84
 ip address 155.1.84.250 255.255.255.0
 !
 interface Vlan85
 ip address 155.1.85.250 255.255.255.0
 !
 interface Vlan86
 ip address 155.1.86.250 255.255.255.0
 !
 interface Vlan143
 ip address 155.1.143.250 255.255.255.0
!
router ospf 1
router-id 250.250.250.250
network 155.1.29.0 0.0.0.255 area 0
network 155.1.80.0 0.0.0.255 area 0
network 155.1.82.0 0.0.0.255 area 0
network 155.1.84.0 0.0.0.255 area 0
network 155.1.85.0 0.0.0.255 area 0
network 155.1.86.0 0.0.0.255 area 0
network 155.1.143.0 0.0.0.255 area 0
!
```

Lab 2 – Configuring Passwords in ISE



NetMet Solutions

NetMet Solutions
Your Trusted Learning Partner

Lab Scenario:

➢ Configuring Passwords in ISE

Initial Setup:

➢ **Based on the previous Lab**

Lab Tasks:

Task 1

Configure the ISE CLI Administrator password based on the following:

➢ The Default password on Eve-NG for ISE is Cisc0!@#.

➢ It will prompt you to change the password.

➢ Change it to Cisc01234

ISE

ISE3-0 login: admin
Password:
You are required to change your password immediately (password aged) Changing password for admin.
(current) UNIX password: Cisc0!@#
Enter new UNIX password: Cisc01234
Retype new UNIX password: Cisc01234

Task 2

Change the ISE CLI admin password to Sagir1234

ISE

ISE3-0/admin# **password**
Enter old password: **Cisc01234**
Enter new password: **Sagir1234**
Confirm new password: **Sagir1234**

Task 3

Reset the ISE GUI Admin password to **Sagir1234**.

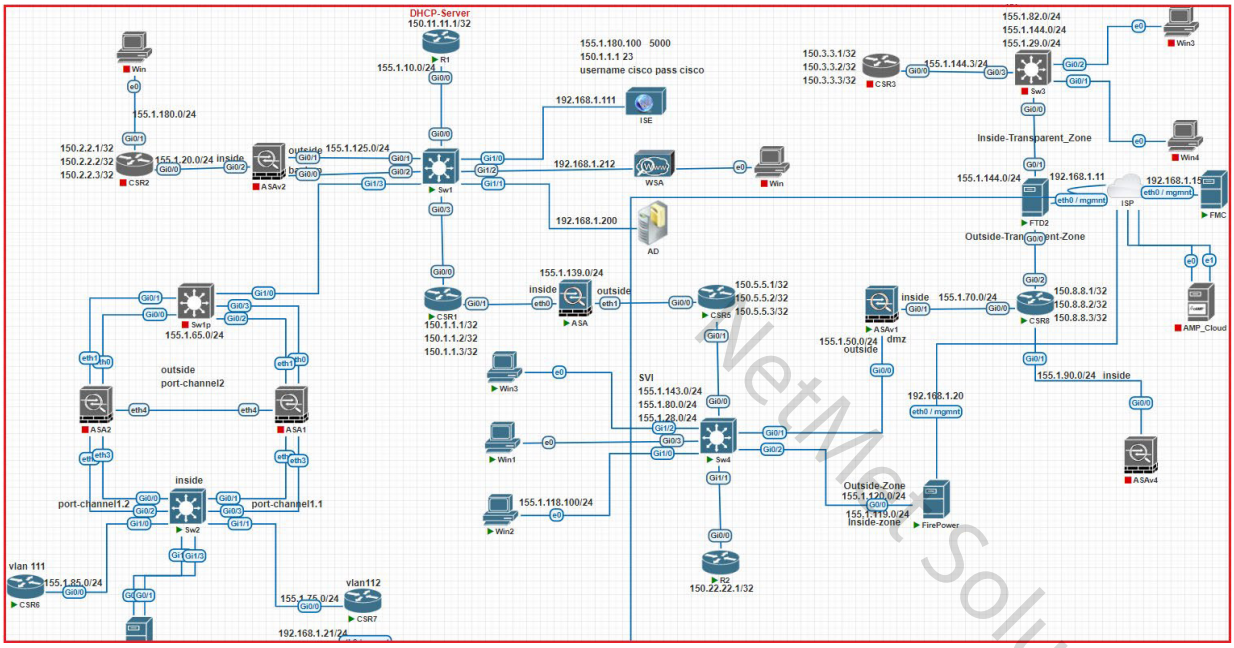
ISE

ISE3-0/admin# **application reset-passwd ise admin**
Enter new password: **Sagir1234**
Confirm new password: **Sagir1234**

Password reset successfully.

Lab 3 – Configuring Network Configuration of ISE

NetMet Solutions



Lab Scenario:

➢ Configuring Passwords in ISE

Initial Setup:

➢ **Based on the previous Lab**

Lab Tasks:

Task 1

Configure/Verify ISE Network Parameters based on the following:

➢ IP Address: 192.168.1.111/24

➢ Default-Gateway: 192.168.1.1

➢ DNS Server (Name Server): 192.168.1.200

➢ Domain Name: cisco.com

➢ Hostname: ISE

ISE

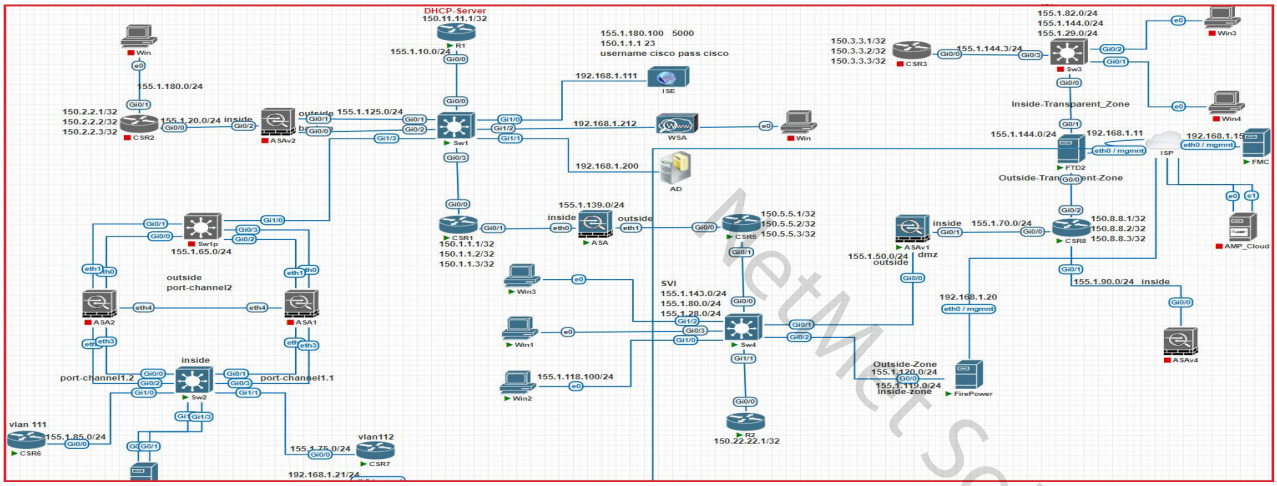
```
Config t
!
hostname ISE1
!
ip domain-name cisco.com
!
interface Gigabit Ethernet 0
ip address 192.168.1.111 255.255.255.0
!
ip default-gateway 192.168.1.1
!
ip name-server 192.168.1.200
!
```

Note: It will prompt you to restart the ISE Application. Type "**yes**" to process. It will take a bit to come back.

NetMet Solutions

NetMet Solutions
Your Trusted Learning Partner

Lab 4 – Initializing ISE – GUI



Lab Scenario:

➢ Configure RADIUS Log Settings in ISE.

➢ Enable Services.

Initial Setup:

➢ **Based on the previous Lab**

Lab Tasks:

Task 1

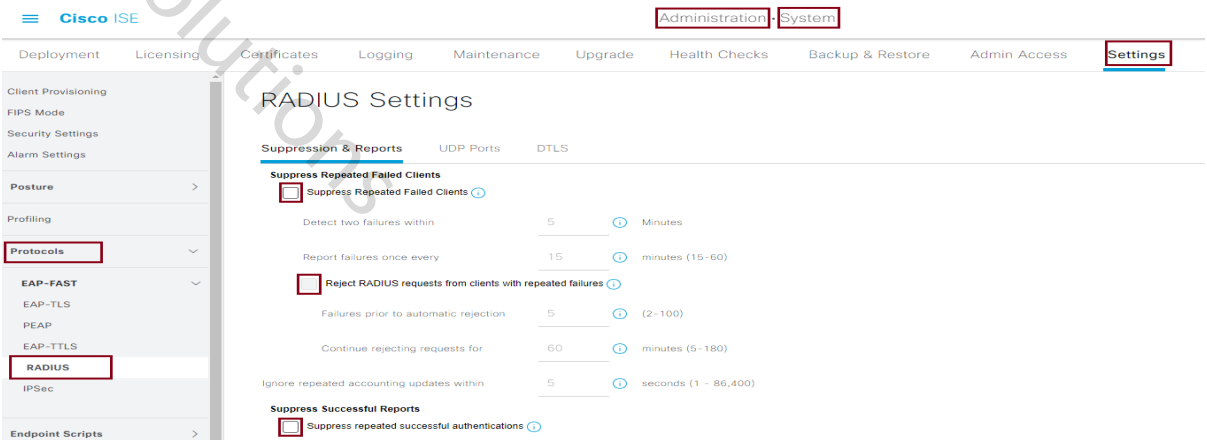
Configure RADIUS settings based on the following:

➢ Configure ISE RADIUS setting to allow repeated Failures & suppress failed attempts. This is done to see the logs as we are testing configurations.

➢ Configure ISE RADIUS to display all Successful authentications in the log even if they are repeated. This is done to see the logs as we are testing configurations.

ISE

1. Log into ISE using the admin/**Cisc01234** as the credentials.
2. Browse to **"Administration -> System -> Settings -> Protocols -> RADIUS"**
3. Uncheck "Reject RADIUS requests from clients with repeated failures".
4. Uncheck "Suppress repeated failed clients".
5. Uncheck "Suppress repeated successful authentications"
6. Click **Save.**



NetMet Solutions

NetMet Solutions
Your Trusted Learning Partner

Task 1

Configure RADIUS settings based on the following:

➢ Configure ISE to run the Device Administration and pxGrid services.

➢ We will be using TACACS+ for Device Administration in a later section.

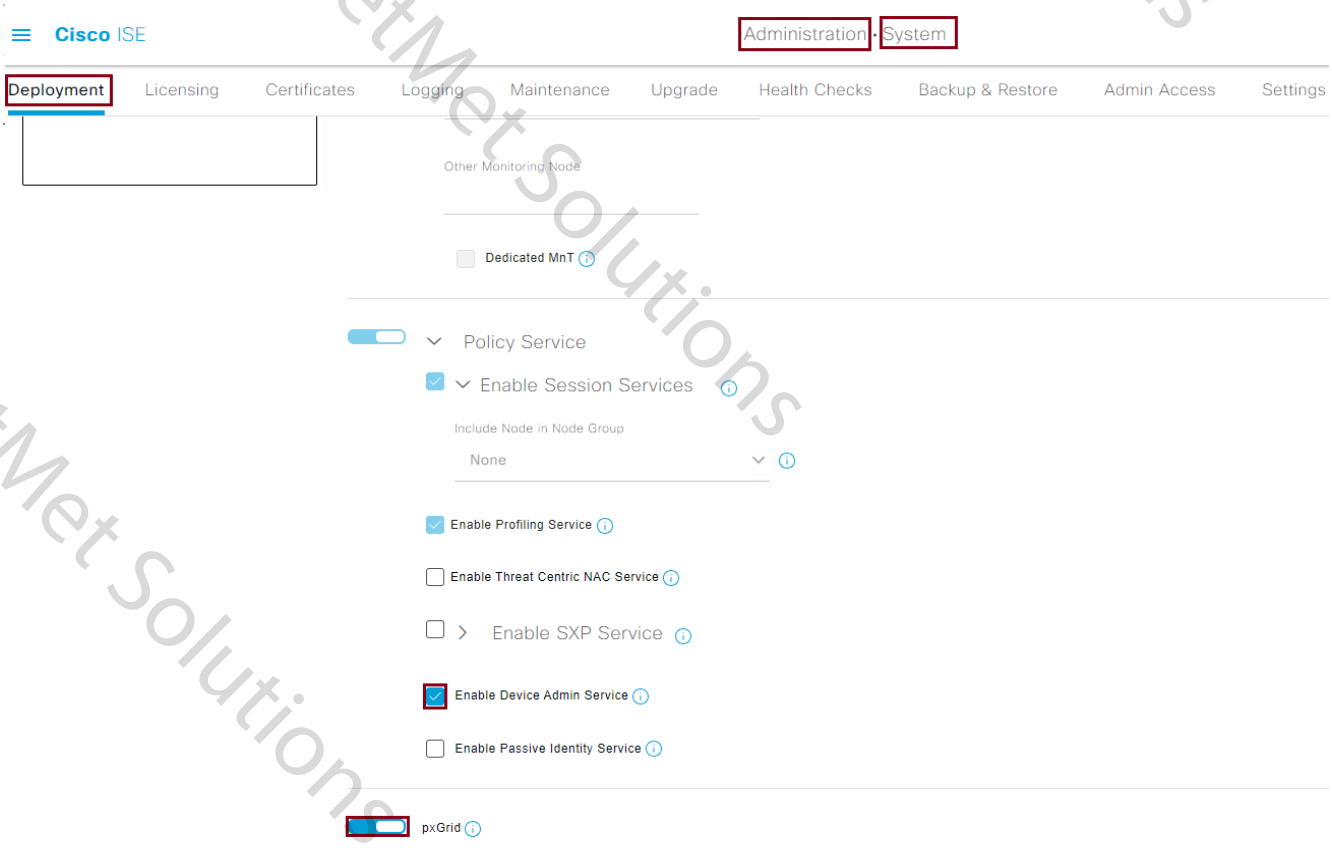
➢ We will be using pxGrid services for the ISE to FMC integration.

ISE

1. Browse to **"Administration -> System -> Deployment -> ISE1"**
2. Check to enable the following Services:

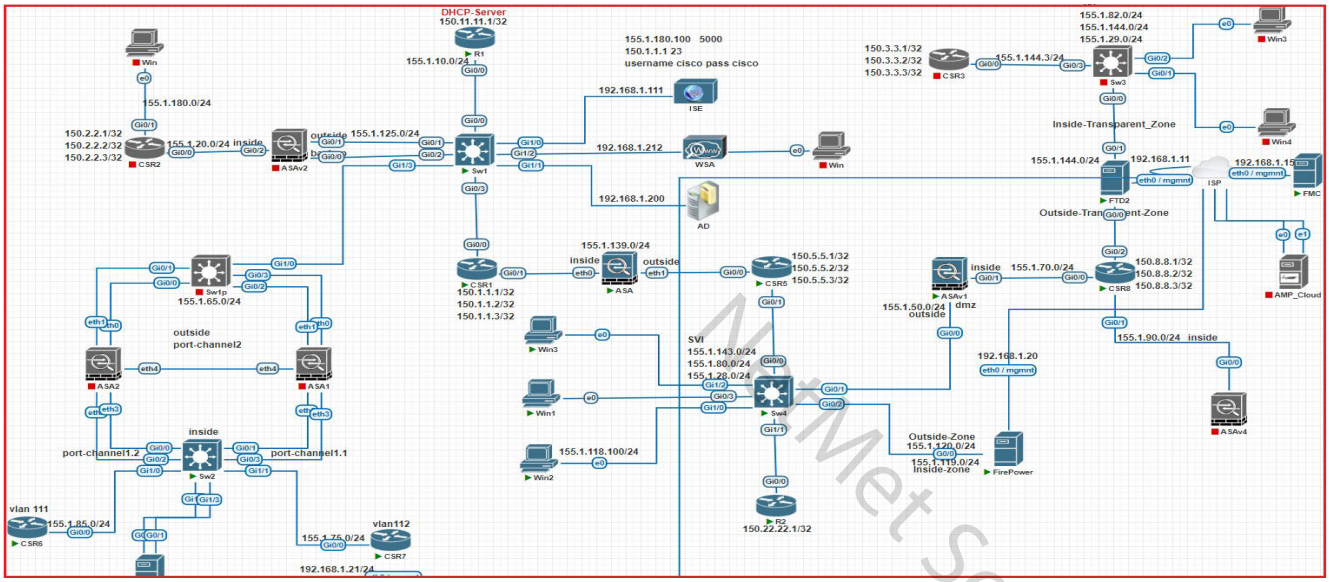
- pxGrid
- Enable Device Admin Service.

3. Click **Save.**



Lab 5 – Create Admin User Creation

NetMet Solutions



Lab Scenario:

➢ Configure Admin User Creation in ISE.

Initial Setup:

➢ **Based on the previous Lab**

Lab Tasks:

Task 1

Create New Admin User with the Following Credential.

Username: **Sagir**
Password: **Netmet@123**
User Information First Name – **Sagir**
User Information Last Name – **Khan**
Email -khansagir446@gmail.com
Admin Group –**Super Admin**

ISE

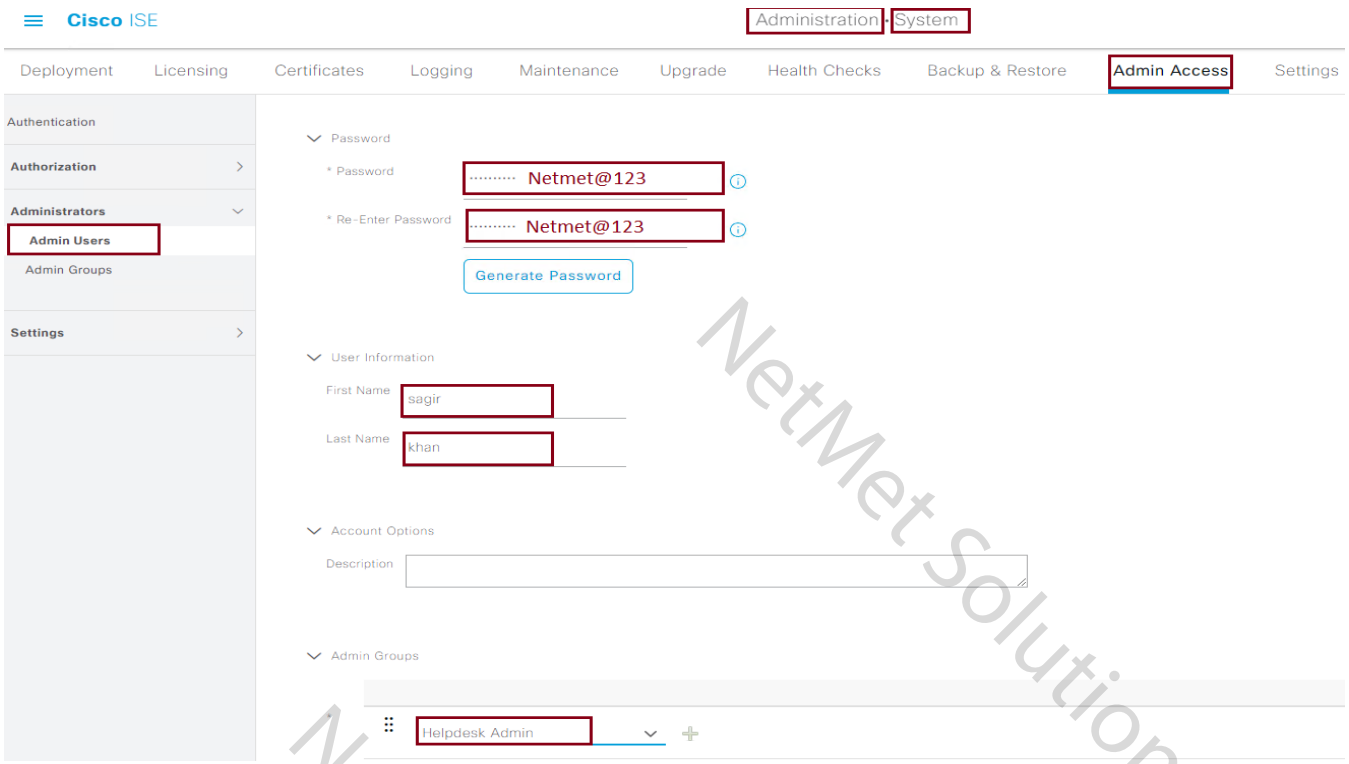
1. Browse to **"Administration -> Admin Access -> Admin User -> Add -> Creat AdminUser"**
   Name- **Sagir**
   Email- **khansagir446@gmail.com**
   Password- **Netmet@123** Re Enter Password- **Netmet@123**
   First name- **Sagir**
   Last Name- **Khan**

Admin Group

SuperAdmin

2. Click **Submit.**

NetMet Solutions



NetMet Solutions

Task 2

Create one more User with the Following Credential.

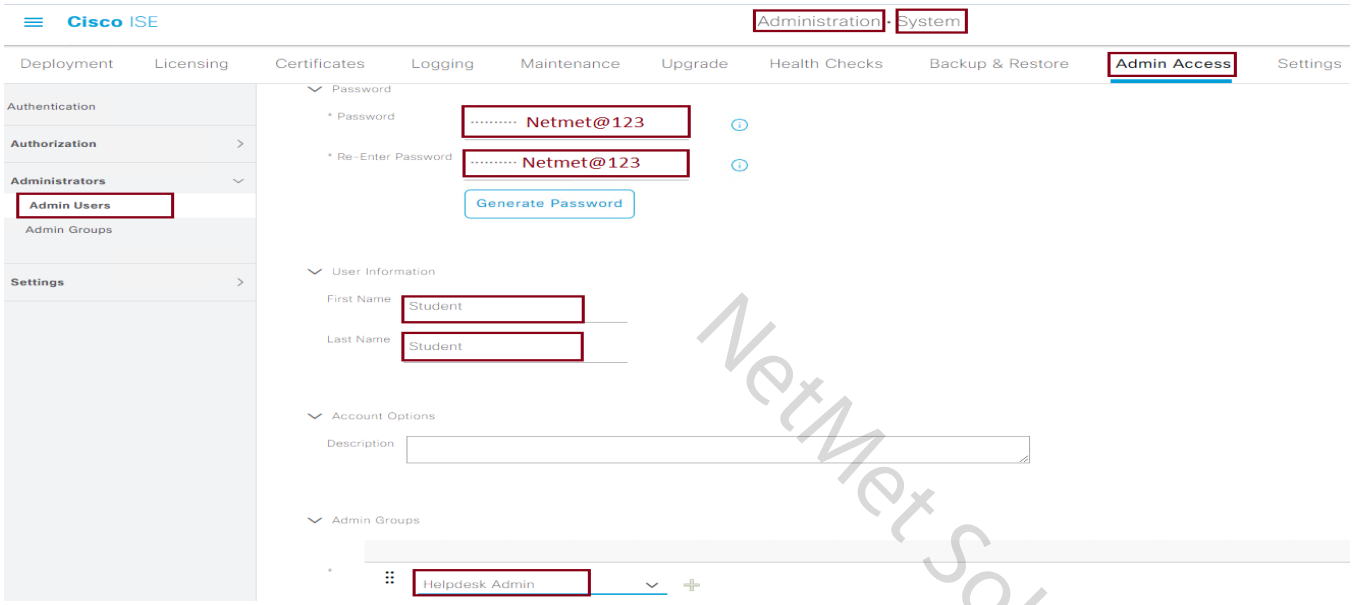
Username: **Student**
Password: **Student**
User Information First Name – **Student**
User Information Last Name – **Student**
Email – **student@gmail.com**
Admin Group – **HelpDesk Admin**

ISE

1. Browse to **"Administration -> Admin Access -> Admin User -> Add -> Creat AdminUser"**
   Name- **Student**
   Email- **student@gmail.com**
   Password- **Netmet@123** Re Enter Password- **Netmet@123**
   First name- **Student**
   Last Name- **Student**

Admin Group
HelpDesk Admin

2. Click **Submit**.

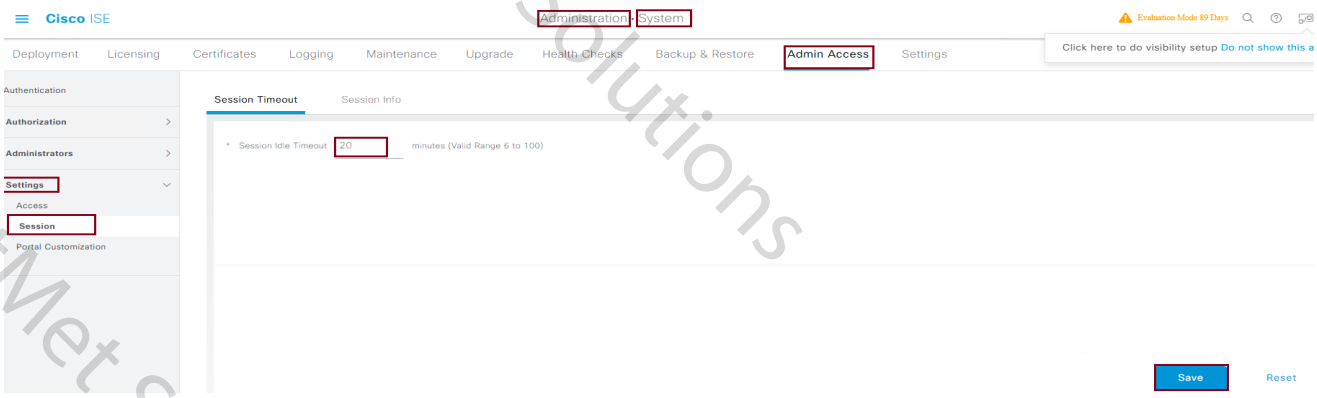


Task 3

Ensure that the idle Session timeout is set to 20 minutes for all users.

ISE

1. Browse to **"Administration -> Admin Access -> Setting -> Session"**
   Session Idle Timeout **20** minutes (Valid Range 6 to 100)
2. Click **Save**.



Task 4

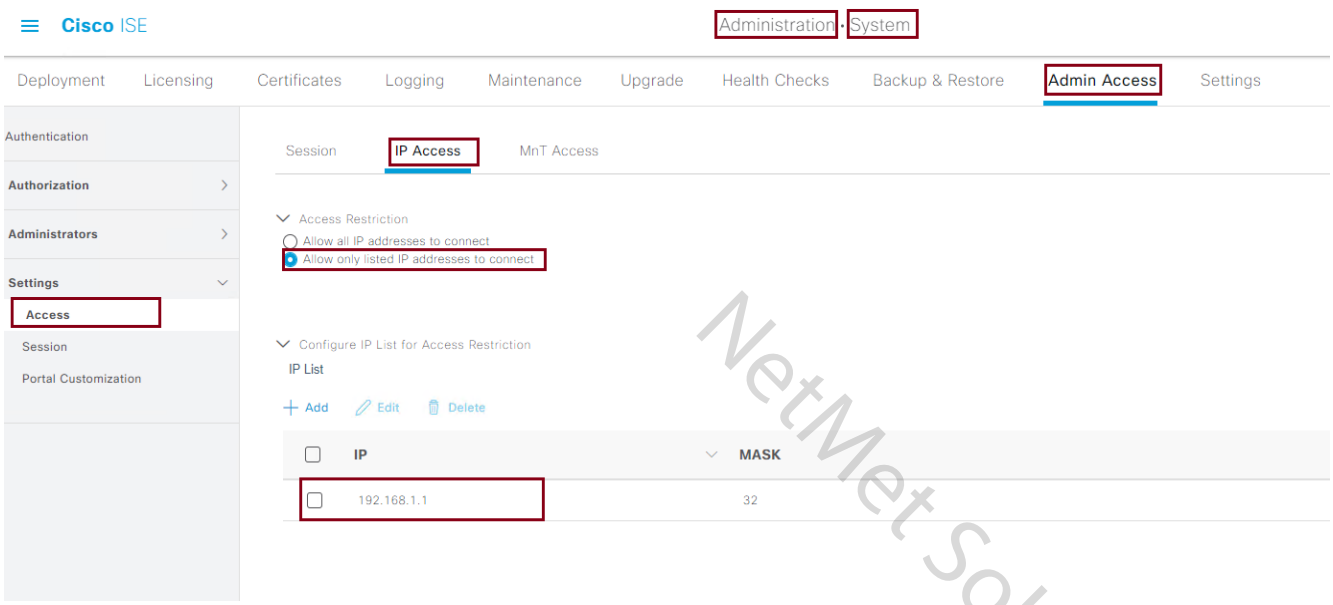
Ensure that ISE can only Access by the window machine using IP Address 192.168.1.1

ISE

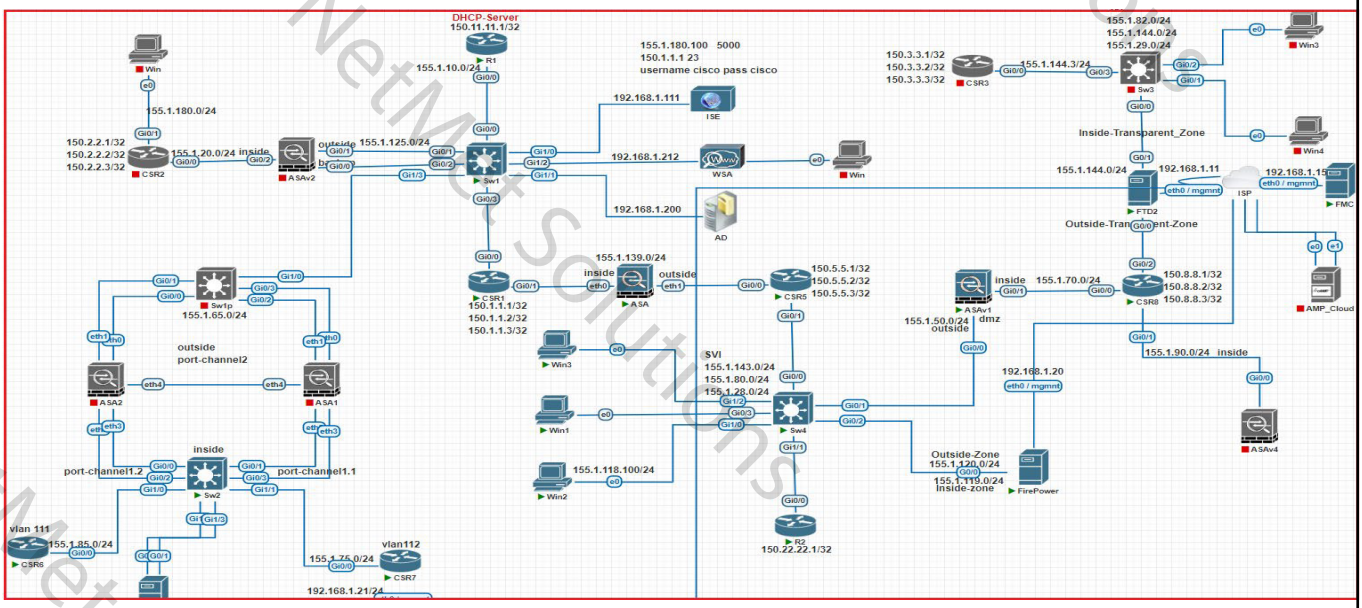
1. Browse to **"Administration -> System -> Settings -> Access -> IP Access ->**
   Select Allow only Listed IP Address to Control
   Click **Add"**

   IP Address- **192.168.1.1**
   Netmask in CIDR format- **32**
2. Click **Save**.

NetMet Solutions



Lab 6 – Radius Protocol for Device Authentication



Lab Scenario:

➢ Configure Authenticate All Console and Remote Login to CSR1 Using ISE.

Initial Setup:

➢ **Based on the previous Lab**

Lab Tasks:

Task 1

Create some NDG Groups in ISE

All Device Type- **All Router**

All Device Type- **All Switches**

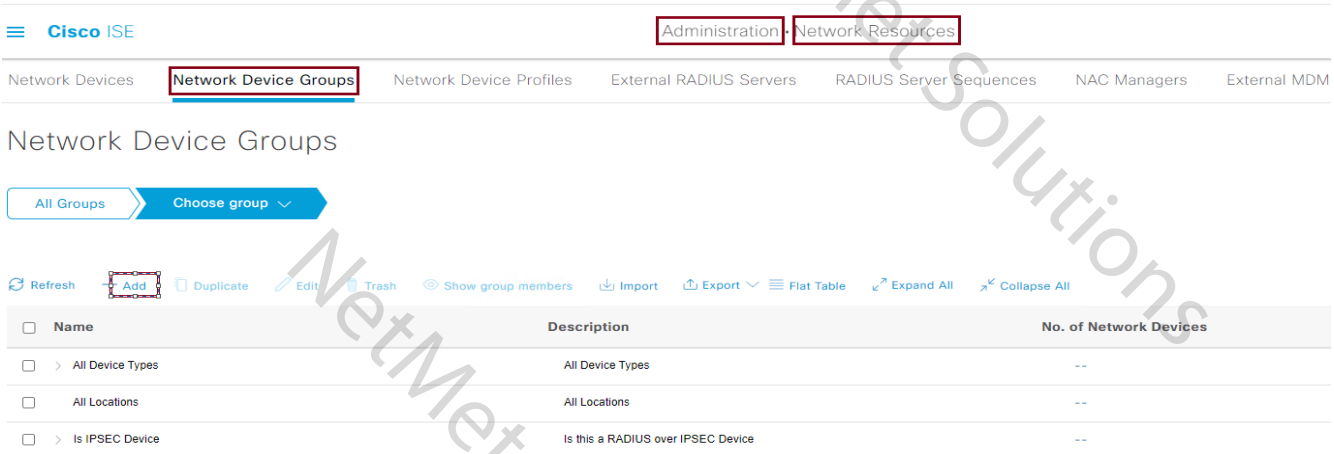
All Device Type – **Firewall**

NetMet Solutions

NetMet Solutions
Your Trusted Learning Partner

ISE

1. Browse to **"Administration -> Network Resources -> Network Device Groups -> Add**
   Name- **All Router**
   Parent Group- **All Device Type**
2. Click Again **"Add"**
   Name- **All Switches**
   Parent Group- **All Device Type**
3. Click Again **"Add"**
   Name- **All Switches**
   Parent Group- **All Device Type**
4. Click **"OK"**



Task 2

Create New User with Following Credentials in ISE.

Username: **Cisco**
Password: **Cisco**
Admin Group: **Device Admin**

- Device Admin Group users should only be Allowed to CSR1 Remotely.
- Create User Group in ISE.

ISE

1. Browse to **"Administration -> Identity Management -> Groups -> User Identity Groups -> Add**
   Name- **DeviceAdmin**
2. Click **"Submit"**

ISE

. Browse to **"Administration -> Identity Management -> Identities -> Add"**
2. Click **"Submit"**

Task 3

Create one more User with Following Credentials in ISE.

Username: **batman**
Password: **Cisco**

NetMet Solutions

Admin Group: **SuperHeros**

- Create User Group in ISE.

ISE
1. Browse to "Administration -> Identity Management -> Groups -> User Identity Groups -> Add
   Name- **SuperHeros**
2. Click **"Submit"**

ISE
. Browse to "Administration -> Identity Management -> Identities -> Add"
2. Click "Submit"

Task 4

Configure CSR-Router Client of ISE

Name- **CSR1**
IP Add- **155.1.146.1**
Device Type- **All Router**
Radius Authentication- **cisco**

ISE
1. Browse to "Administration -> Network Resources -> Network Device -> Add"
2. Click**"Submit"**

Task 4

- Super Heros Group user should be allowed to access CSR1 Remotely and should be allowed to Access CSR1 using Console.
- Use Radius as the protocol for Authentication.
- If the ISE is Unavailable the admin should still be allowed to access the console or Access CSR1 Remotely using a local user account "Admin" password as "default1A"

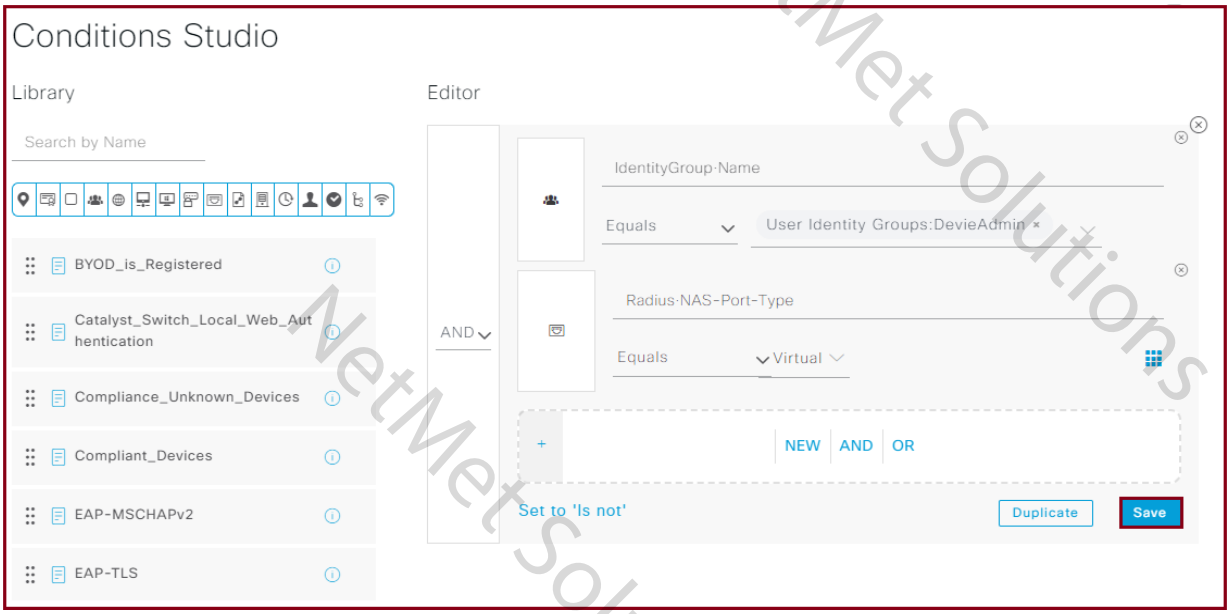
```
CSR1
!
Aaa new-model
Aaa authentication login Con group Radius LOCAL
Aaa authentication login VTY group radius LOCAL
Username Admin privilege 15 password default1A
!
Line Con 0
Login authentication Con
!
Line vty 0 15
Login authentication VTY
!
Radius Server Rad
Address IPv4 192.168.1.111 auth-port 1812 acct-port 1813
Key cisco
!
```

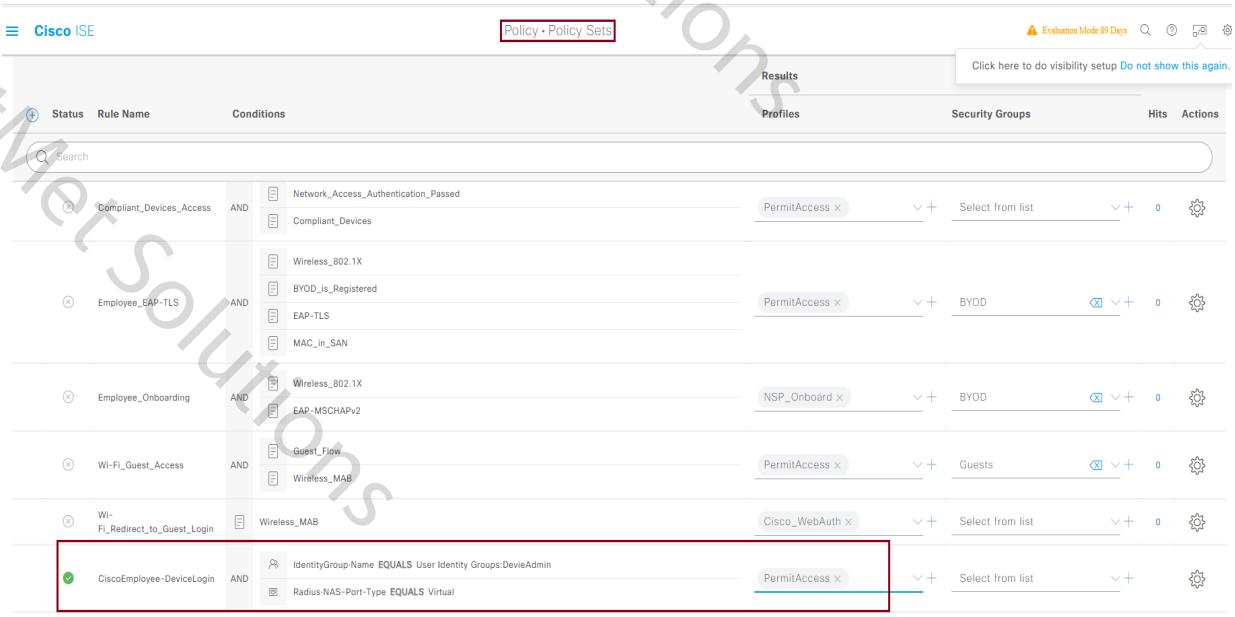
NetMet Solutions

Radius-Server attributes 6 on-for-login-auth
Radius-Server attributes 8 include-in Access-Request
Radius-Server attributes 25 access-request include
!

- Create Policy in ISE

ISE
1. Browse to " Policy -> Policy Stes->Default -> Authorization Policy"
2. Click "Save"

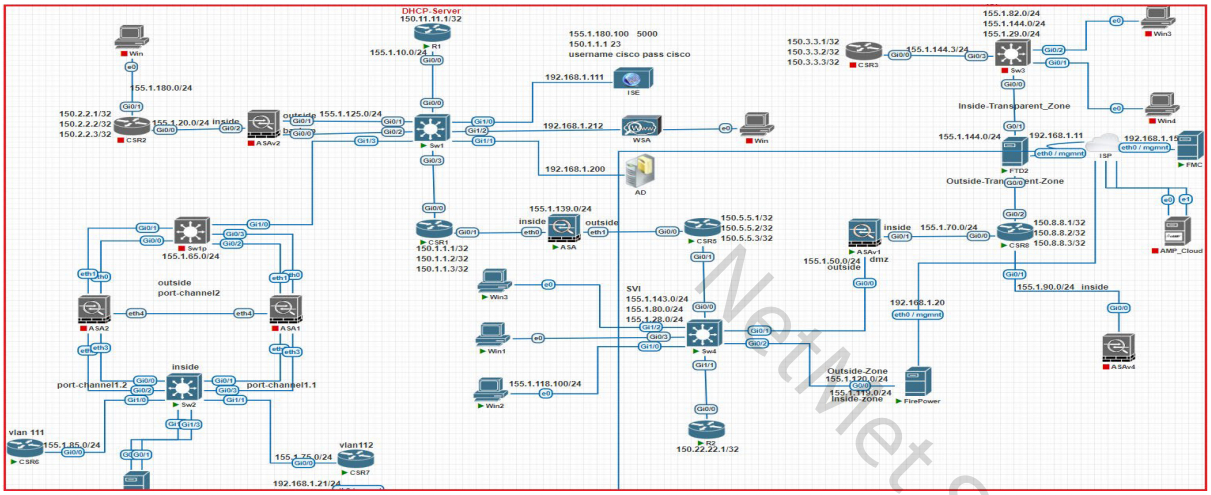




NetMet Solutions

NetMet Solutions
Your Trusted Learning Partner

Lab 7 – Radius Protocol for Device Authentication Exec Level.



Lab Scenario:

➢ Configure Authenticate All Console and Remote Login to CSR1 Using ISE.

Initial Setup:

➢ **Based on the previous Lab**

Lab Tasks:

Task 1

- **All console and Remote login to CSR should be Authorized with Respective Exec Level using ISE.**
- **User cisco should be Assigned privilege exec level2**
- **User batman should be Assigned exec level 15.**
- **Privilege exec level2 should be allowed to shut and no shut all interface.**
- **Permission for level2 or level 15 must be locally defined on CSR.**

CSR

Aaa authorization Authz1 group radius
Line vty 0 15
Authorization exec Authz1
Line console 0
Authorization exec Authz1
Exit
!
Aaa authorization exec Authz1

➢ Create Customization Authorization profile on ISE.

ISE

1.Brows to "Policy -> Policy Sets -> Result -> Authorization -> Authorization profile -> Add"

Name- AUTHZ-SH

Go to Attribute Settings

2.Click "Select on Item -> cisco -> cisco-av-pair-[1]

NetMet Solutions

NetMet Solutions

NetMet Solutions

NetMet Solutions
Your Trusted Learning Partner

Write- priv-lvl-15

3.Click "Submit"

ISE

1.Brows to "Policy -> Policy Sets -> Result -> Authorization -> Authorization profile -> Add"

Name- AUTHZ-DA

Go to Attribute Settings

2.Click "Select on Item -> cisco -> cisco-av-pair-[1]

Write- priv-lvl-2

3.Click "Submit"

➢ **Know this Customization profile Use in Policy**

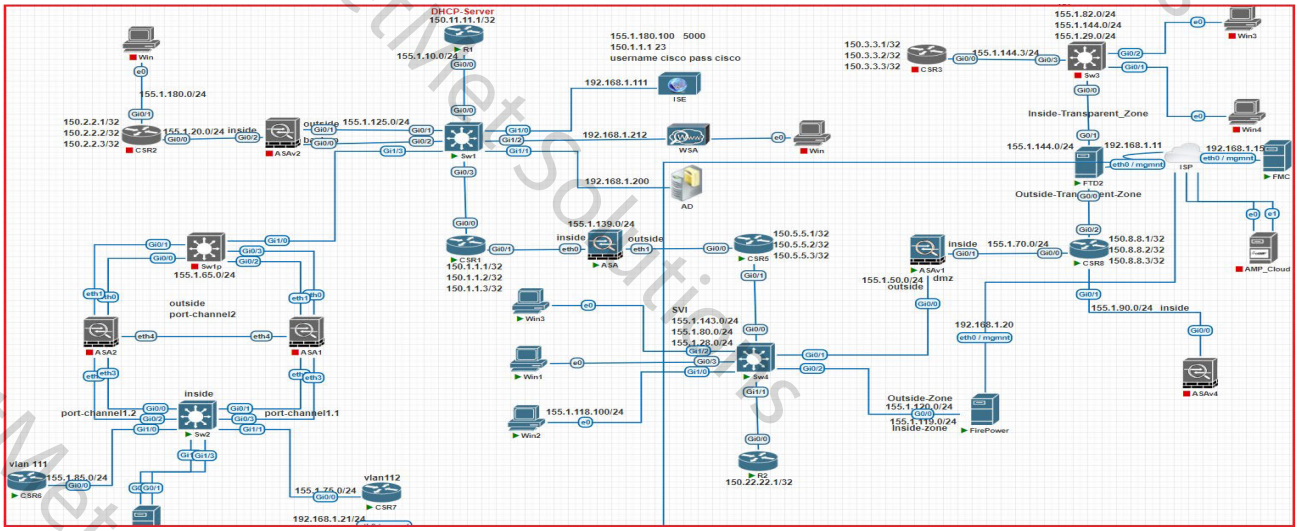
ISE

1.Brows to "policy -> Policy Sets -> Authorization policy -> edit -> edit policy"

Permit Access-AUTHZ-SH

2.Click "submit"

Lab 8 – TACAS+ Protocol for Device Authentication



Lab Scenario:

➢ Configure Authenticate All Console and Remote Login to SW1 Using ISE.

Initial Setup:

➢ **Based on the previous Lab**

Lab Tasks:

Task 1

Configure the ISE as per the Following Requirements.

- ➢ Create a Internal user on ISE with username as "Sagir" and Password as cisco.
- ➢ This user on ISE must belong to the local users group Avengers.
- ➢ Ensure switch1 authenticates all Telnet or SSH. Session from ISE using TACAS+ protocol.
- ➢ Network Device IP add of Sw1 is 10.0.0.254

NetMet Solutions