

Load initials.

TASK 1: Admin user creation

Access the ISE gui on 172.16.3.100 using ServerA or directly from your laptop if you are connected to anyconnect, and achieve the following requirements:

- Create a new admin user with the following credentials:
 - ✓ Username=rohit
 - ✓ Password=Ine@123
 - ✓ User Information First Name=Rohit
 - ✓ User Information Last Name=Pardasani
 - ✓ Email=rpardasani@ine.com
 - ✓ Admin Groups=SuperAdmin
- ✓ Username=student
- ✓ Password=Ine@123
- ✓ User Information First Name=Student
- ✓ User Information Last Name=Student
- ✓ Email=student@ine.com
- ✓ Admin Groups=HelpDesk Admin
- Ensure that the idle session timeout is set to 20 minutes for all users.
- Ensure that ISE can only be accessed by the ServerA machine using the IP address 172.16.10.100/32 and 10.0.0.0/8 subnet.
- Password must contain minimum 6 characters.
- Password must not contain the admin name or words like cisco or test.
- Admin account must not be disabled automatically.
- Password must contain atleast one lowercase and one uppercase alphabetic character and one numeric character.

TASK 2: Device login using Radius Protocol

Authenticate all console and remote logins (telnet and ssh) to CSR1 using ISE.

- Create a new user with the following credentials:
 - ✓ Username=thor
 - ✓ Password=cisco
 - ✓ Admin Groups=marvel
- DeviceAdmin group users should only be allowed to access CSR1 remotely.
- Create another user with the following credentials:
 - ✓ Username=nickfury
 - ✓ Password=cisco
 - ✓ Admin Groups=shield
- Marvel group users should be allowed to access CSR1 remotely and should also be allowed to access CSR1 using console.
- Shield group users should only be allowed to access CSR1 remotely. (Telnet or SSH)
- Use radius as the protocol for authentication.
- If the ISE is unavailable, the administrator should still be allowed to access the console or access CSR1 remotely using a local user account "cisco" and password as "cisco".

TASK 3: DOT1x for pcA

Configure SW1 to authenticate pcA using DOT1x. pcA is connected to SW1 on port FastEthernet 1/0/18 through the IP Phone. Ensure the following requirements are met:

- pcA should be assigned vlan 82 from ISE.
- pcA should authenticate using username "loki" and password "loki".
- Loki belongs to the group SuperVillians.
- Enable Radius authentication, authorization and accounting on SW1 with a secret key of lne@123.
- Ensure radius packets are sourced from vlan 143.
- Once authenticated, pcA should receive an IP address from the DHCP server R1.
- Ensure that you support multiple authentications on DATA vlan and one authentication on Voice vlan.

- Once connected loki should only be allowed to telnet 155.1.82.250 and ping 155.1.0.0/16.
- Ensure both Anyconnect and windows supplicant works.

TASK 4: MAB for IP Phone

Configure SW1 to authenticate the IP Phone using MAB.

- The IP Phone should be assigned to voice vlan 28 locally on the switch.
- After successful authentication, the IP Phone should register to the CUCM.
- DHCP server has been pre-configured on R1.
- Once authenticated, the IP Phone should automatically profile as “Cisco IP Phone” and should also download the default DACL as per the default Authorization Policy “Cisco IP Phone”.

TASK 5: Profiling for IP Phone and pcA

Configure ISE to profile IP Phone and pcA as per the following requirements:

- Configure SW1 to allow ISE to do CoA based on port-bounce using SNMP. Use community string as cisco.
- The IP Phone should be profiled as “Approved_Phones” based on the conditions given below:
 1. If the OUI contains “Cisco Systems”, then the Certainty Factor Increases by 50.
 2. If the IP address contains voice vlan subnet “155.1.28.X”, then the Certainty Factor Increases by 20.
 3. If the cdp cached Platform contains “Cisco IP Phone”, then the Certainty Factor Increases by 50.
 4. If the cdp cached Device Id starts with “SEP”, then the Certainty Factor Increases by 20.
 5. If the DHCP class identifier contains Cisco Systems, then the Certainty Factor Increases by 50.
- The pcA should be profiled as “Approved_Machines” based on the conditions given below:

1. If the IP address contains DATA vlan subnet "155.1.82.X", then the Certainty Factor Increases by 60.
 2. If the "ifDescr" contains "FastEthernet1/0/18", then the Certainty Factor Increases by 70.
 3. If username contains "loki", then the Certainty Factor increases by 30.
- After successful authentication, the IP Phone should register to the CME pre-configured as R1.
 - DHCP server has been pre-configured on R1.
 - Once authenticated, the IP Phone should also download a DACL with "permit ip any any" and the Authorization Profile must be called "Authz_Cisco_IP_Phone" and Authorization Policy must be named as "Approved_Phones". The match criteria in the Authorization Policy must match based on the profile "Approved_Phones" which was created earlier.
 - Once authenticated, the pcA should be assigned to the Authorization profile named "Approved_Machines".

TASK 6: Wired Central WebAuth, Employee BYOD, Self and Sponsored Guest

Company has provided a port for remote employees to connect to the corporate network using DOT1x. If the remote employees do not have DOT1X capabilities, they should then be authenticated using central webauth, processed by the ISE. Configure ISE and SW1 as per the following requirements:

- Configure SW1 port FastEthernet 1/0/18 to allow DOT1X capable users to be authenticated.
- Employees are authenticated to vlan 82 with unrestricted access if they are using dot1x.
- Employees that webauth, should be assigned to vlan 82 with all access to internal network (155.1.0.0/16) and internet access.
- Self Provisioned guest users will go to vlan 83 with internet access only.
- Sponsored guest, go to vlan 84 with internet access only.
- For testing DOT1X, create a user named "CaptAmerica" and assign him to the group "Employee".
- For testing BYOD, CaptAmerica should be assigned to endpoint group "Employee_BYOD" group.

- For testing Self Registration, register a new user “Spiderman” and he should be assigned to endpoint group “SelfRegistered” group.
- For testing Sponsored Registration, register a new user “Ironman” and he should be assigned to endpoint group “SponsorRegistered” group.