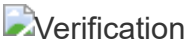
Detailed ESG Configuration Guide in Cisco ACI APIC

Prerequisites

- APIC admin access
- Target tenant permissions
- Planned ESG structure
- Identified endpoints and contracts

1. Initial Navigation
    APIC Login
2. Launch APIC GUI (https://{APIC-IP})
3. Login with admin credentials
4. Navigate: `Tenants > {your-tenant} > Application Profiles`
5. ESG Creation
    ESG Creation
6. Right-click "Endpoint Security Groups"
7. Select "Create Endpoint Security Group"
8. Fill in basic information:
   `Name: esg-prod-vmware Description: Production VMware Environment VRF: {select-appropriate-vrf}`
9. Advanced settings:
   - Intra ESG isolation: Disabled
   - Preferred Group Member: No
   - PCTag: Auto-assign
10. ESG Selector Configuration
     Selector Config
11. In ESG > Selectors tab: ```yaml
    Name: vmware-prod-selector
    Match Type: EPG
    EPG: epg-3378
    Additional Criteria:
    - MAC: 00:50:56:*
    - Subnet: 172.31.44.224/28 ```
12. Contract Configuration
     Contract Setup
13. Create Contract: ```yaml
    Name: prod-to-mgmt
    Scope: tenant
    Subject: mgmt-access
    Filters:

- https (TCP/443)
- ssh (TCP/22)
- snmp (UDP/161) ```

14. Apply to ESG:
    - Provided Contracts tab: `yaml Contract: prod-to-mgmt Type: provided`
    - Consumed Contracts tab: `yaml Contract: dmz-access Type: consumed`
15. Verification Steps
     Verification
16. Operational View: ```
    Navigate: Operations > EP Tracker
    Filter by:
    - ESG Name
    - MAC prefix
    - IP subnet ```
17. Check Endpoint Association: ```
    Navigate: Tenant > Application Profiles > ESGs
    Select ESG > Operational tab
    Verify:
    - Endpoint count
    - Contract status
    - Policy deployment ```
18. Common ESG Configurations

DMZ ESG

Management ESG

```yaml
Name: esg-mgmt
Selectors:
  - Match EPG: epg-1751
    Type: physical-only
Contracts:
  Provided:
    - mgmt-access
```

7. Troubleshooting
8. Endpoint not appearing in ESG:
    - Verify selector criteria
    - Check endpoint attributes
    - Confirm EPG association
9. Contract issues:

- Verify contract scope
- Check filter entries
- Confirm provider/consumer relationship

10. Common commands:

```
# Check ESG configuration
moquery -c fvESg

# Verify endpoint association
moquery -c fvCEp -f 'fvCEp.esg=="esg-prod-vmware"'

# Check contract deployment
moquery -c vzBrCP -f 'vzBrCP.name=="prod-to-mgmt"'
```

11. Best Practices
12. Naming Conventions:
    - Use consistent prefixes (esg-, contract-, filter-)
    - Include environment indicator (prod-, dev-, test-)
    - Add purpose suffix (-web, -db, -app)
13. Documentation:
    - Document all ESG configurations
    - Map contract relationships
    - Keep endpoint inventory updated
14. Security:
    - Follow least-privilege principle
    - Regular contract audit
    - Monitor ESG membership changes