{{title}}

Detailed ESG Configuration Guide in Cisco ACI APIC

Prerequisites

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

Initial Navigation[No Image: c:\Users\wkimand1\Downloads\F5\_Analysis\ESG\_MIGRATION\placeholder\_for\_login\_screenshot.png]

Launch APIC GUI (https://{APIC-IP})

Login with admin credentials

Navigate: Tenants > {your-tenant} > Application Profiles

ESG Creation[No Image: c:\Users\wkimand1\Downloads\F5\_Analysis\ESG\_MIGRATION\placeholder\_for\_esg\_creation.png]

Right-click "Endpoint Security Groups"

Select "Create Endpoint Security Group"

Fill in basic information: Name: esg-prod-vmware Description: Production VMware Environment VRF: {select-appropriate-vrf}

Advanced settings:

* + Intra ESG isolation: Disabled
  + Preferred Group Member: No
  + PCTag: Auto-assign

ESG Selector Configuration[No Image: c:\Users\wkimand1\Downloads\F5\_Analysis\ESG\_MIGRATION\placeholder\_for\_selector.png]

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 ```

Contract Configuration[No Image: c:\Users\wkimand1\Downloads\F5\_Analysis\ESG\_MIGRATION\placeholder\_for\_contract.png]

Create Contract: ```yaml Name: prod-to-mgmt Scope: tenant Subject: mgmt-access Filters:

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

Apply to ESG:

* + Provided Contracts tab: yaml Contract: prod-to-mgmt Type: provided
  + Consumed Contracts tab: yaml Contract: dmz-access Type: consumed

Verification Steps[No Image: c:\Users\wkimand1\Downloads\F5\_Analysis\ESG\_MIGRATION\placeholder\_for\_verify.png]

Operational View: ``` Navigate: Operations > EP Tracker Filter by:

* + ESG Name
  + MAC prefix
  + IP subnet ```

Check Endpoint Association: ``` Navigate: Tenant > Application Profiles > ESGs Select ESG > Operational tab Verify:

* + Endpoint count
  + Contract status
  + Policy deployment ```

Common ESG Configurations

DMZ ESG

Management ESG

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

Troubleshooting

Endpoint not appearing in ESG:

* + Verify selector criteria
  + Check endpoint attributes
  + Confirm EPG association

Contract issues:

* + Verify contract scope
  + Check filter entries
  + Confirm provider/consumer relationship

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"'

Best Practices

Naming Conventions:

* + Use consistent prefixes (esg-, contract-, filter-)
  + Include environment indicator (prod-, dev-, test-)
  + Add purpose suffix (-web, -db, -app)

Documentation:

* + Document all ESG configurations
  + Map contract relationships
  + Keep endpoint inventory updated

Security:

* + Follow least-privilege principle
  + Regular contract audit
  + Monitor ESG membership changes