



## Verify the ACI Endpoint Update App

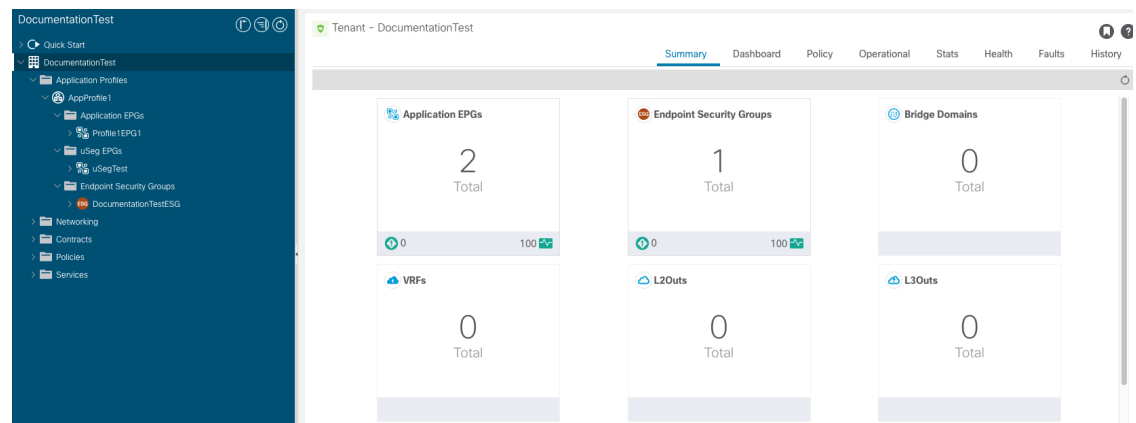
Verify the ACI endpoint update app is working properly by checking the network objects in the management center.

- [Verify the ACI Endpoint Update App in the Management Center, on page 1](#)
- [Verify the Endpoint Update App in the ASA, on page 3](#)

## Verify the ACI Endpoint Update App in the Management Center

When an APIC endpoint is pulled and pushed to the management center, it's put into either a dynamic object or a network object. The object is named *SitePrefix\_TenantName\_ApplicationProfileName\_ApplicationEPGName*.

Following is an example APIC tenant on which the information in this section is based.



**Step 1** Log in to the management center.

**Step 2** Click one of the following:

- Network object: Click **Objects > Object Management > Network**.
- Dynamic object: Click **Objects > Object Management > External Attributes > Dynamic Objects**.

Network

Add Network  Filter





Show Unused Objects

A network object represents one or more IP addresses. Network objects are used in various places, including access control policies, network variables, intrusion rules, identity rules, network discovery rules, event searches, reports, and so on.

Name	Domain	Value	Type	Override
any	Global	0.0.0.0/0 ::/0	Group	<input type="checkbox"/>
any-ipv4	Global	0.0.0.0/0	Network	<input type="checkbox"/>
any-ipv6	Global	::/0	Host	<input type="checkbox"/>
AP143_DOCUMENTATIONTEST_APPPROFILE1_ESG-DOCUMENTATIONTESTES	Global	127.0.0.1	Group	<input type="checkbox"/>
AP143_DOCUMENTATIONTEST_APPPROFILE1_PROFILE1EPG1	Global	127.0.0.1	Group	<input type="checkbox"/>
AP143_DOCUMENTATIONTEST_APPPROFILE1_USEGTEST	Global	127.0.0.1	Group	<input type="checkbox"/>


## What to do next

For troubleshooting purposes, you can track endpoints in the APIC's EP Tracker and Object Store Browser:

CISCO APIC admin    

System Tenants Fabric Virtual Networking L4-L7 Services Admin **Operations** Apps Integrations

Visibility & Troubleshooting | Capacity Dashboard | **EP Tracker** | Visualization

EP Tracker 

End Point Search

Learned At	Tenant	Application	EPG	IP
Pod:1, Leaf:104, Port:eth1/32	T1	app-prof	web	70.0.0.100

State Transitions

Date	IP	MAC	EPG	VRF	Action	Node	Interface	Encap
Page 0 of 0								
Objects Per Page: 15								
No Objects Found								

The screenshot shows the Cisco Object Store interface. At the top, there is a search bar with the following fields: "Class or DN or URL" containing "fvCEp", "Property" (empty), "Operation" set to "=", and "Value" (empty). A "Run Query" button is to the right. Below the search bar, it indicates "2 objects found" and provides a "Show URL and response of last query" button. There are also "Empty Properties: Show Hide" buttons. The main content area displays the object "fvCEp" with a table of properties:

Property	Value
dn	< uni/tn-T1/ap-app-prof/epg-app/cep-BC:16:65:B4:7A:76 >
annotation	
childAction	
contName	
encap	vlan-3002
extMngdBy	
id	0
idepdn	
ip	80.0.0.100
lcC	learned
lcOwn	local
mac	BC:16:65:B4:7A:76
mcastAddr	not-applicable

Additional notes:

- During the push process, the REST operation (POST, PUT, or DELETE) is determined based on the comparison of what data is on the APIC and what is on the management center.
- For diff calculation, each tenant updates only the data of its own tenant.
- When all endpoints are deleted from an APIC endpoint group (EPG), the corresponding object group on the management center gets deleted too. But if the object group is referenced or used in any access rule on the management center, because there is a dependency, the object group cannot get deleted. In this case, we keep the group name and put the localhost IP address, 127.0.0.1, inside the group instead.

## Verify the Endpoint Update App in the ASA

When an APIC endpoint is pushed to the ASA, it's put into a network object group named *SitePrefix#TenantName#ApplicationProfileName#ApplicationEPGName*.

**Step 1** Start ASDM.

- Step 2** Log in to the ASA.
- Step 3** Click **Configuration > Firewall**.
- Step 4** In the right pane, expand **Network Objects**.
- Step 5** Network objects created by the Endpoint Update App are displayed under **Network Object Groups**, similar to the following.

The screenshot displays the Cisco ASDM 7.16(1) for ASA interface. The main window shows the 'Configuration > Firewall > Access Rules' page. The left pane shows the 'Firewall' configuration tree with 'Access Rules' selected. The right pane shows the 'Addresses' configuration tree with 'Network Object Groups' expanded. A red arrow points to the object 'SITE1#TenantTest#coke\_prof#EPC\_COKE\_EXT' in the 'Network Object Groups' list.

#	Enabled	Source Criteria	User	Security Group	Source Service
1		Global (1 implicit rule)	any		

Network Object Groups:

- SITE1#TenantTest#AP\_Test#APP
- SITE1#TenantTest#AP\_Test#WEB
- SITE1#TenantTest#coke\_prof#EPC\_COKE\_EXT
- SITE1#TenantTest#coke\_prof#EPC\_COKE\_INT
- SITE1#TenantTest#testspan#targetEPC
- SITE2\_TENANTFAYAZ\_APTENANTFAYAZ\_APP
- SITE2\_TENANTFAYAZ\_APTENANTFAYAZ\_WEB