

Cisco Application Centric Infrastructure

Configuring ACI Fabric Access Policies

ACI Fabric Access Policies are used to configure parameters that relate to access *into* the fabric (i.e., configuring ports on leaf switches for servers, firewalls, network switches, and other devices). In addition, Fabric Access Policies are used to configure other parameters like SPEED, Enabling LLDP or CDP, LACP and more.

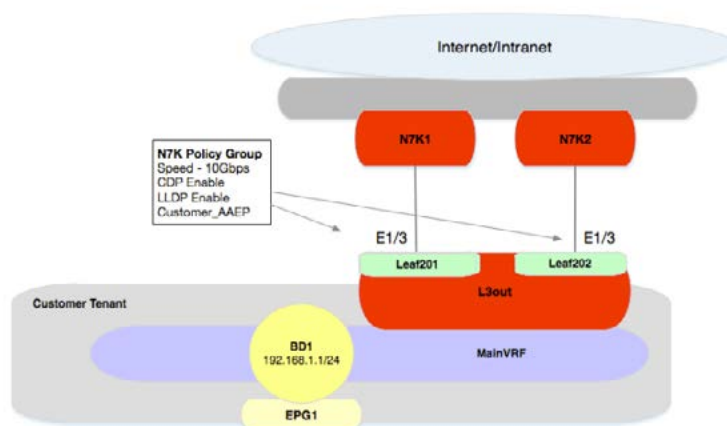
Assumptions

The workflow of this guide assumes that the customer has configured nothing in their Fabric Access Policies (i.e., no Switch Profiles, no Interface Profiles, no AAEP, no VPC domain).

What are you trying to accomplish?

Scenario 1 - Configuring L3out interfaces

You want to configure (2) interfaces (Leaf201 E1/3 and Leaf202 E1/3) and make them ready to be used with an L3out. For this scenario, you will be using routed interfaces, so this means from an ACI perspective, you will configure Leaf 201/202 E1/3 as access ports.



Configure Interface Leaf201 e1/3 as a routed Interface (access port, non-switched)
 Configure Interface Leaf202 e1/3 as a routed Interface (access port, non-switched)

How will you accomplish this?

The most important thing to remember when configuring Fabric Access Policies is that each policy has a reference (or pointer) to the next. If you forget to connect your Switch Profile to your Interface Profiles, or if you forget to tie your Interface Policy Group to your AAEP, the configuration will not be pushed correctly to the appropriate switch interface.



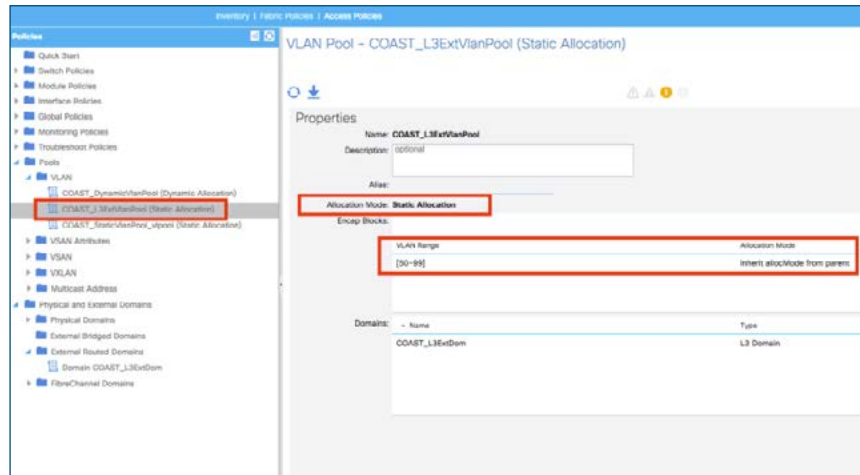
Fabric Access Policy Linkage

Configuration Steps

- 1. Create Vlan Pools** (which will belong to a External Routed Domain.) This is required for every L3out, even routed ports.
- 2. Create a External Routed Domain** (which defines the scope of the resources; in this case, external routers).
- 3. Create an AAEP** – This is the “glue” that connects our domains (i.e., Physical, VMM and External routed Domains) and our Vlan Pool to Switches and Switch Interfaces.
- 4. Create a VPC domain** for our Leaf Switches (optional)
- 5. Configure Policies** (CDP enable, LLDP enable, Speed)
- 6. Configure Policy Group(s)** – This is a grouping of policies (LLDP, CDP, AAEP, LACP, etc).
- 7. Select Interfaces** (Which interfaces will connect from the ACI fabric to the external device?)
- 8. Select Switches** (Which switches will connect from the ACI fabric to the external device?)

1. Creating a Vlan Pool – Go to **Fabric > Access Policies > Pools > VLAN**

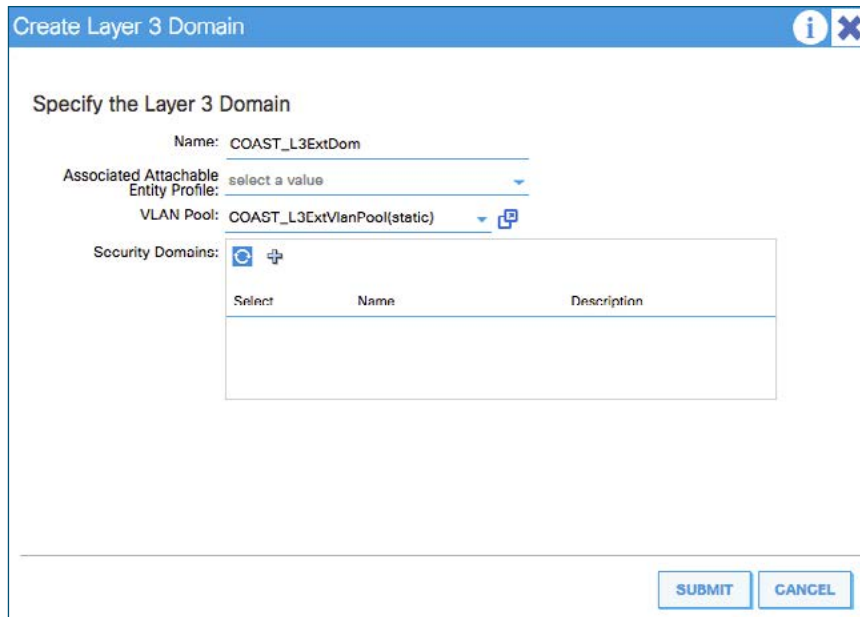
Create a Vlan Pool which will be used by your External Routed Domain. Enter a name for your Vlan pool, select a static allocation mode, and enter the range of Vlans to be allocated to the pool.



Fabric > Access Policies > Pools > VLAN

2. Create an External Routed Domain – Go to **Fabric > Access Policies > Physical and External Domains > External Routed Domains**

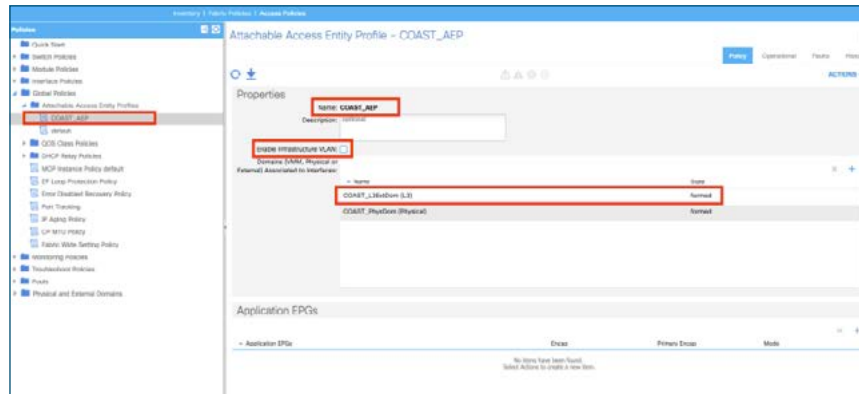
Create an External Routed Domain to associate with your Vlan Pool. Enter a name for your External Routed Domain, and select your Vlan Pool. Leave the Attachable Access Entity Profile (AAEP) blank.



Fabric > Access Policies > Physical and External Domains > External Routed Domains

3. Create an AAEP – Go to **Fabric > Access Policies > Global Policies > Attachable Access Entity Profile**

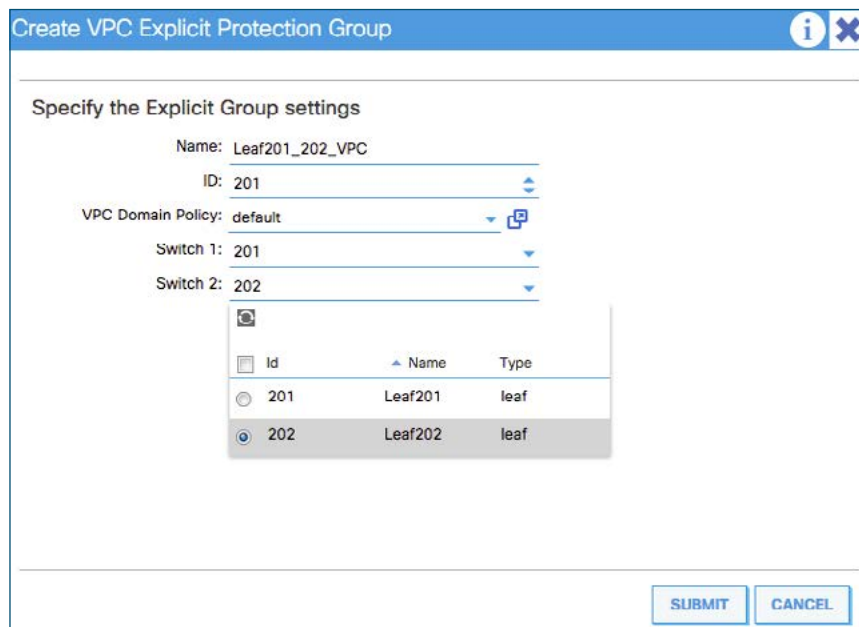
This is the “glue” that connects our domains (i.e., Physical, VMM and External routed Domains) and our Vlan Pool to Switches and Switch Interfaces. For the AAEP, we will configure the name of the AAEP and select the domain to attach to it. In this example, it’s the External Routed Domain.



Fabric > Access Policies > Global Policies > Attachable Access Entity Profile

4. Create VPC Domain (Note: This is optional for this scenario, but included as you should always have your VPC domain configured and pair up your leaf switches). Go to **Fabric > Access Policies > Switch Policies > Policies > VPC Port Channel default > Create VPC Explicit Protection Group.**

Provide a name, an ID (unique for each Leaf VPC Pair), select the default VPC Domain policy, and select your two VPC switches.



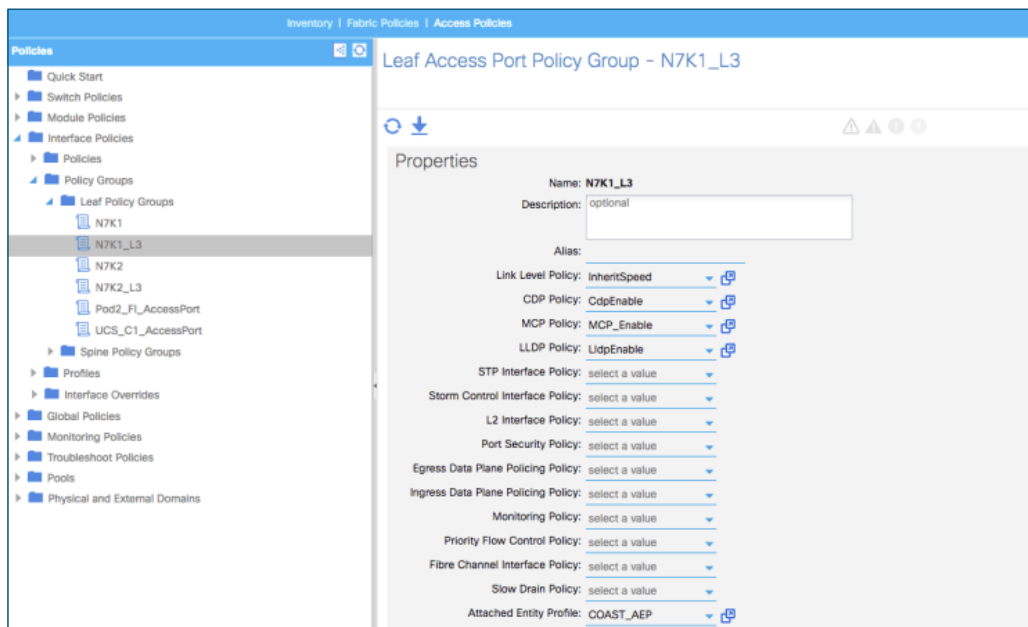
Fabric > Access Policies > Switch Policies > Policies > VPC Port Channel default > Create VPC Explicit Protection Group

5. Configure Policies – Go to **Fabric > Access Policies > Interface Policies > Policies.**

Use the GUI or other methods, such as [XML posts](#), to configure a set of policies that will be used (and re-used) to configure our interfaces. At a minimum, configure Speed, CDP enable, and LLDP enable.

6. Interface Policy Group – Go to **Fabric > Access Policies > Interface Policies > Policy Groups > Leaf Policy Groups > Create Access Port Policy Group.** A policy group is a grouping of policies (LLDP, CDP, SPEED) that will be used to configure a switch interface or interfaces.

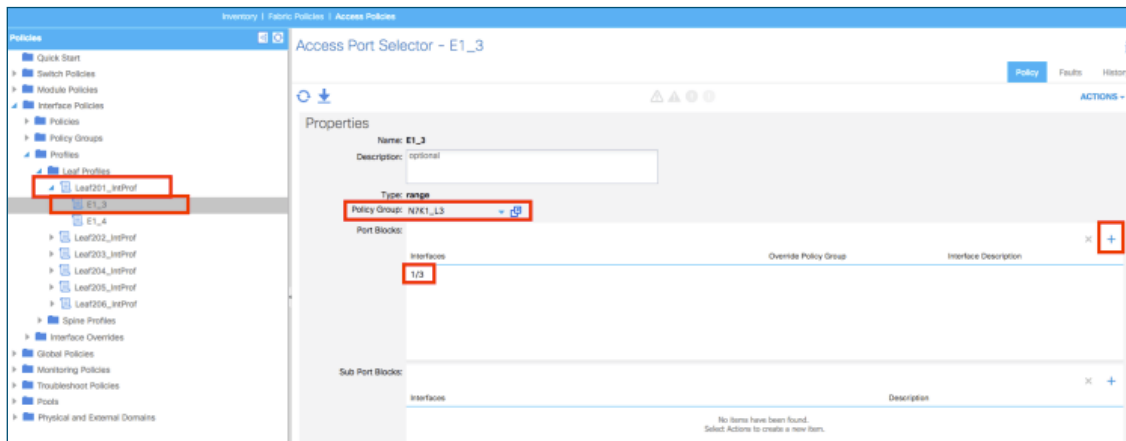
Enter a name for your Access Port Policy Group. For Access Policy groups, you can either RE-USE the Policy group for multiple interfaces, or create a separate Access Policy group for each and every port. Creating a shared Access Policy group will save time, however, it also means that you can impact multiple interfaces if you modify it incorrectly or delete it.



Fabric > Access Policies > Interface Policies > Policy Groups > Leaf Policy Groups > Create Access Port Policy Group

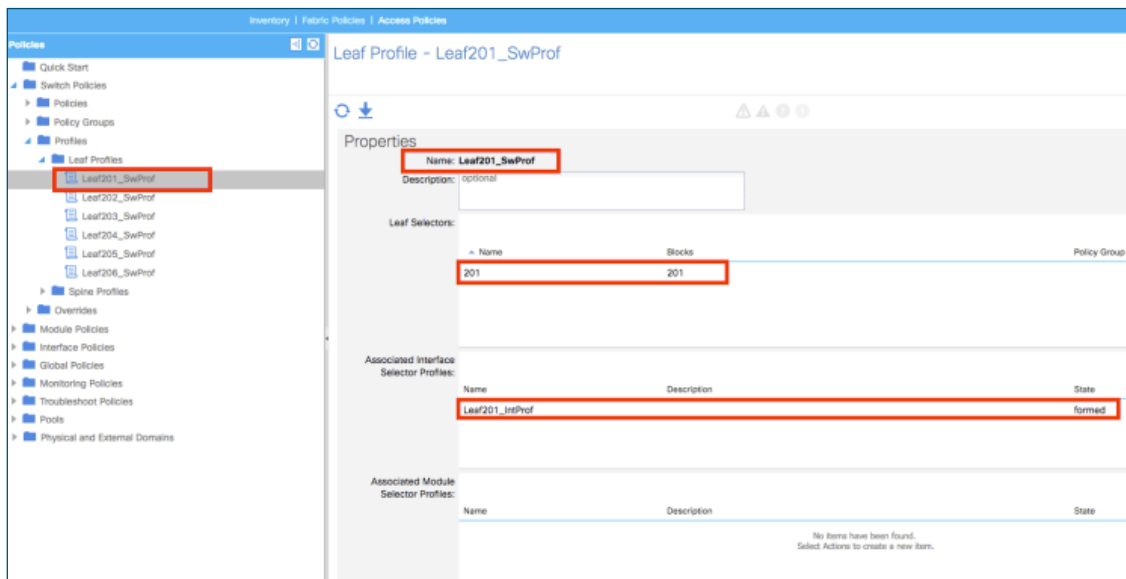
7. Select interfaces – Next, you will select the interfaces to apply the configuration to; in this case Ethernet1/3. **Go to Fabric > Access Policies > Interface Policies > Leaf Profiles > Create Leaf Interface Profile.**

Name your Interface Profile (Recommendation: Name your Interface Profile after your Leaf switch name, to make linking it with your Switch Profiles easy to remember). Next, select the interface to be used. Finally, select the access policy group that you created in Step 6.



Fabric > Access Policies > Interface Policies > Leaf Profiles > Create Leaf Interface Profile

8. Select switches – Finally, create the Switch Profiles (which will allow you to select your switches where configuration will be pushed) and associate them with the Interface Profiles that you just created. If this seems backwards, please remember, you can technically configure these policies in any order; the important thing is to ensure that all of the policies are connected. To configure your Switch, go to **Fabric > Access Policies > Switch Policies > Profiles > Leaf Profiles > Create Leaf Profile.** Note: It is recommended to name the Switch Leaf Profile after your Leaf switch.



Fabric > Access Policies > Switch Policies > Profiles > Leaf Profiles > Create Leaf Profile