Understand ACI Enforce Domain Validation

Contents

Introduction

This document describes Enforce Domain Validation setting and its benefits.

Enforce Domain Validation Explained

By default, Enforce Domain Validation is not enabled, so if an EPG is configured with a static {port, VLAN} where a domain containing this VLAN is not present, then this happens:

- Application Centric Infrastructure (ACI) raises Fault F0467 "Configuration failed for <path> due to Invalid Path Configuration".
- Vlan is deployed on the interface.
- Traffic is forwarded on the specific interface.

This misconfiguration can be prevented by Enforce Domain Validation.

Caution: DO NOT ENABLE THIS FEATURE ON AN EXISTING FABRIC WITHOUT PROPER DUE DILIGENCE.

This feature cannot be disabled once you enable it. You can have existing configurations that were working even if they were incorrect. Before enabling it, make sure you verify the domain assignment to the EPGs and the associated AEPs.

Enforce Domain Validation: Disabled (Default Behavior)

APIC CLI Enforce Domain Validation verification. Default state indicates that domain validation is disabled.

<#root>

```
APIC# moquery -c infraSetPol | egrep"domainValidation"
domainValidation               :

no
```

Assume encap vlan 420 is not tied to the domain/AEP associated to the EPG. Vlan 420 is still deployed on the expected interface.

<#root>

```
leaf# show vlan encap-id

420

 extended
 VLAN Name                             Encap            Ports
 ---- -------------------------------- ---------------- ------------------------

1

    lc_TN:lc_APP:lc_EPG              vlan-420

Eth1/13
```

Platform Independent (PI) Vlans (1,19) for EPG and BD are deployed and allowed to trunk on the expected interface.

<#root>

```
"
 VLAN Name                             Encap            Ports
 ---- -------------------------------- ---------------- ------------------------

1

    lc_TN:lc_APP:lc_EPG              vlan-420         Eth1/13

19

   lc_TN:lc_BD                       vxlan-16416666   Eth1/13
```

Vlans for BD and EPG are deployed on the expected interface.

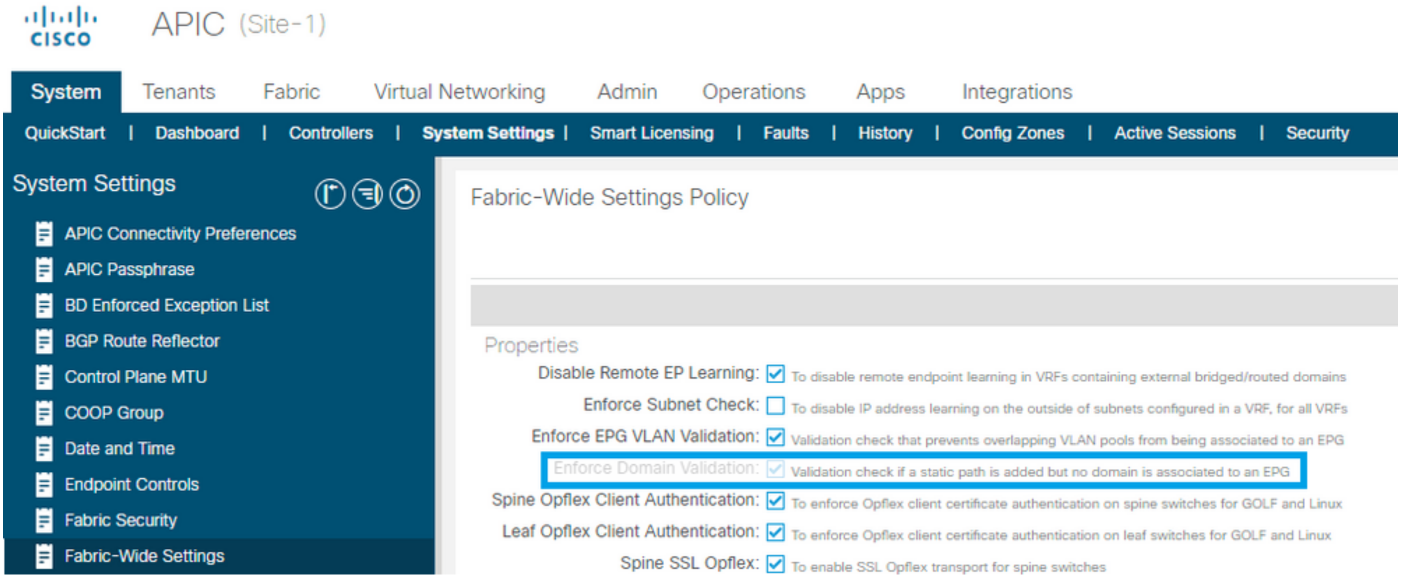
<#root>

```
leaf# show int eth

1/13

 trunk | grep -A Allowed
 Port          Vlans Allowed on Trunk
--------------------------------------------------------------------------------

Eth1/

13

        1,19
```

Enforce Domain Validation: Enabled

If Enforce Domain Validation is Enabled, you can create a Static Path on an EPG with a VLAN ID that is not linked to the respective access policy path. The fabric raises a fault, and the VLAN is NOT programmed on the interface.

APIC GUI Enforcing Domain Validation verification **System** > **System Settings** > **Enforce Domain Validation**.



Fabric-Wide Settings Policy

Properties

Disable Remote EP Learning: ☑ To disable remote endpoint learning in VRFs containing external bridged/routed domains

Enforce Subnet Check: □ To disable IP address learning on the outside of subnets configured in a VRF, for all VRFs

Enforce EPG VLAN Validation: ☑ Validation check that prevents overlapping VLAN pools from being associated to an EPG

Enforce Domain Validation: ☑ Validation check if a static path is added but no domain is associated to an EPG

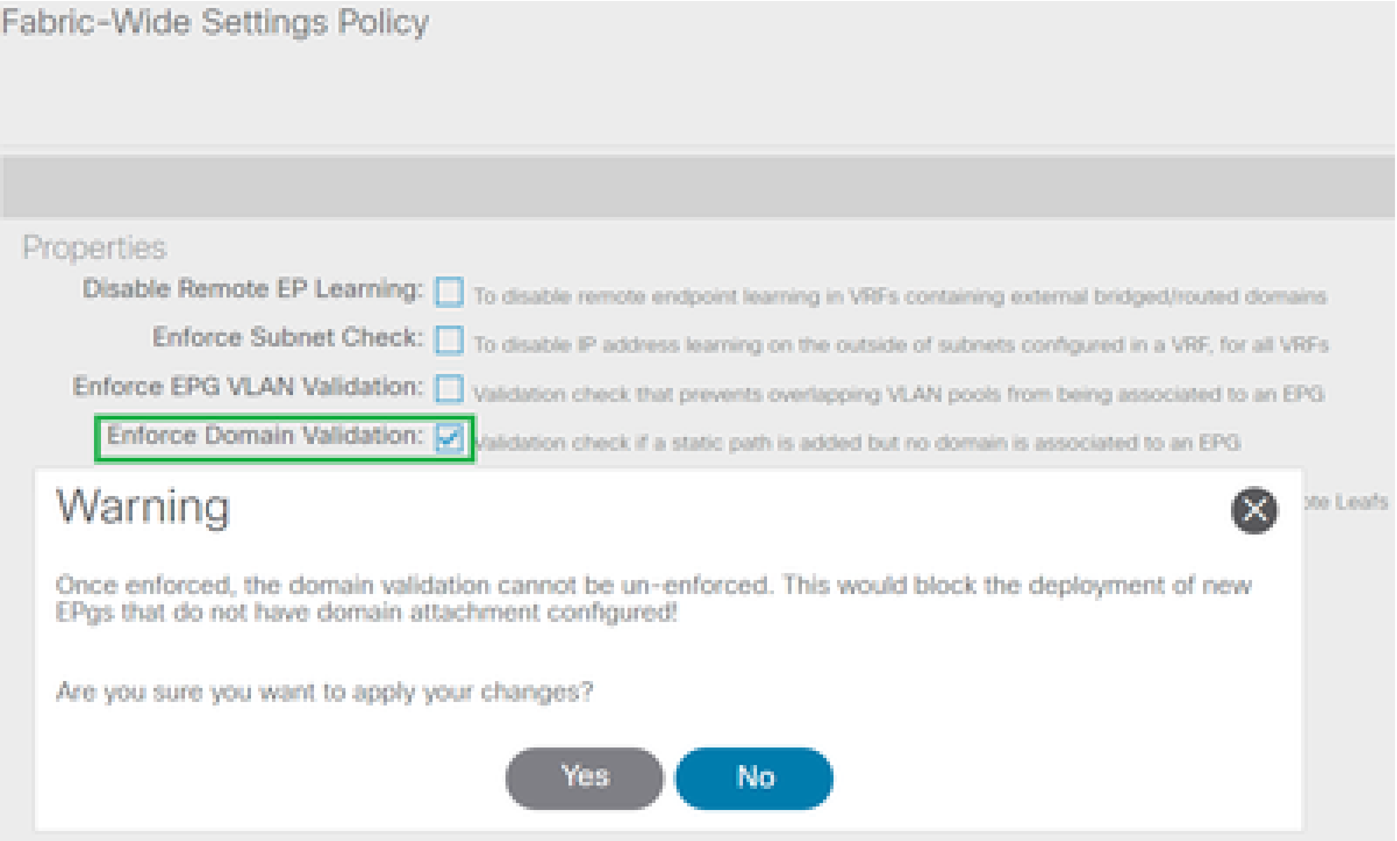
Spine Opflex Client Authentication: ☑ To enforce Opflex client certificate authentication on spine switches for GOLF and Linux

Leaf Opflex Client Authentication: ☑ To enforce Opflex client certificate authentication on leaf switches for GOLF and Linux

Spine SSL Opflex: ☑ To enable SSL Opflex transport for spine switches

Enabled Enforce Domain Validation

Confirmation Verification Warning



Fabric-Wide Settings Policy

Properties

Disable Remote EP Learning: □ To disable remote endpoint learning in VRFs containing external bridged/routed domains

Enforce Subnet Check: □ To disable IP address learning on the outside of subnets configured in a VRF, for all VRFs

Enforce EPG VLAN Validation: □ Validation check that prevents overlapping VLAN pools from being associated to an EPG

Enforce Domain Validation: ☑ Validation check if a static path is added but no domain is associated to an EPG

Warning

Once enforced, the domain validation cannot be un-enforced. This would block the deployment of new EPgs that do not have domain attachment configured!

Are you sure you want to apply your changes?

Once Enforced, the Domain Validation Cannot be Un-enforced

Once the setting is enabled, the option is grayed out so you cannot undo the action.

APIC CLI: Enforce Domain Validation verification

<#root>

```
APIC# moquery -c infraSetPol | egrep "domainValidation"
domainValidation               :
```

```
yes
```

This validation kicks in for existing configuration ONLY when the policy has to be downloaded to the switch.

Typically, this can occur during a switch upgrade, clean reload, or snapshot/backup restore of configuration.

Example of a clean reload step:

<#root>

```
leaf#
```

```
acidiag  touch clean
```

```

This command can wipe out this device, Proceed? [y/N] y
leaf# reload


This command can reload the chassis, Proceed (y/n)? [n]: y
```

Vlan 420, which originally got deployed, is NOT on the expected interface at this time.

<#root>

```
leaf# show int eth
```

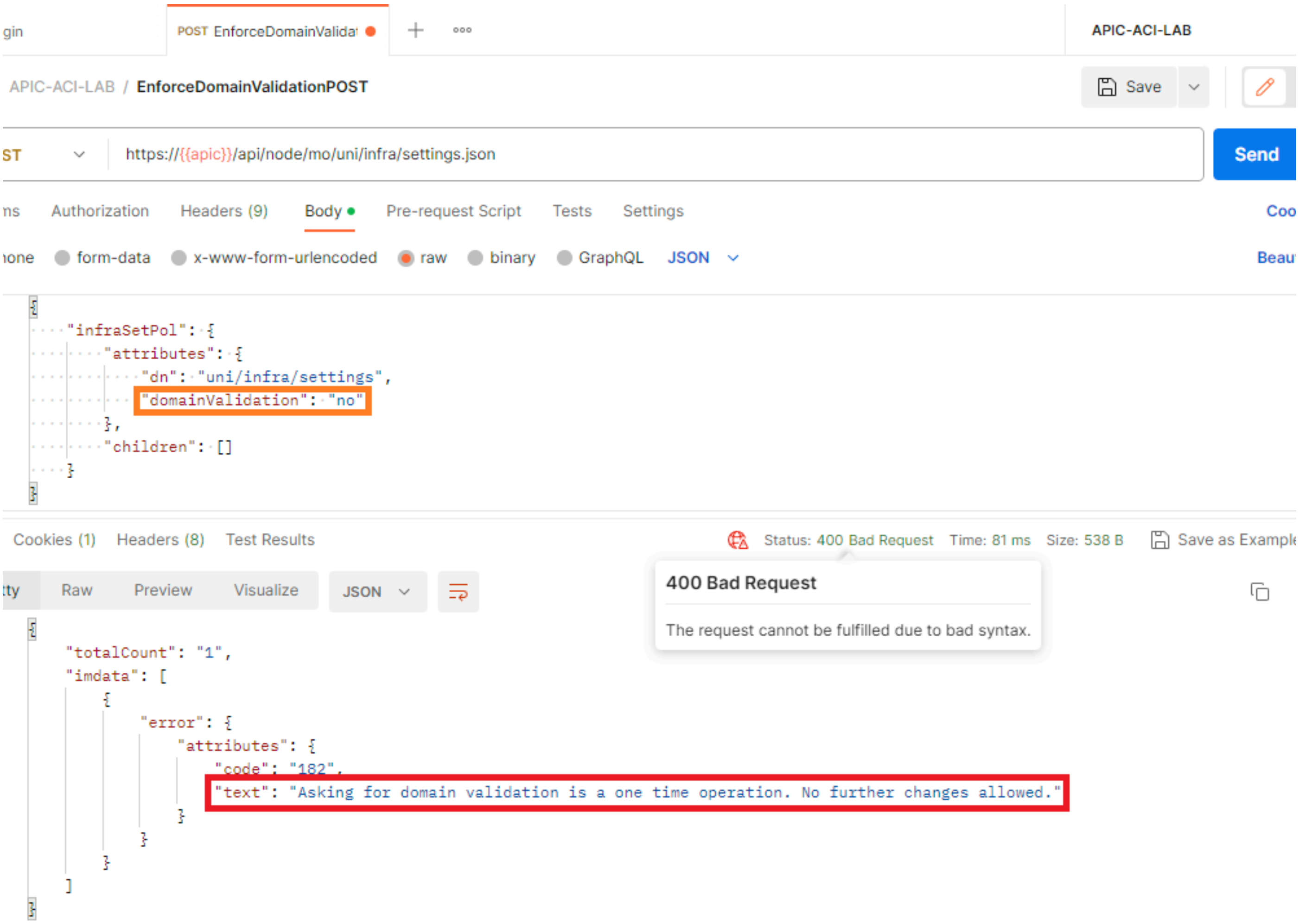
```
1/13
```

```
 trunk | grep -A 2 Allowed
 Port           Vlans Allowed on Trunk
--------------------------------------------------------------------------------
 Eth1/13
```

```
none
```

Enabling domain validation is considered a best practice, hence once enabled, there is no option to revert the change.

A POSTMAN API shows the post to change the setting is not successful.



https://{{apic}}/api/node/mo/uni/infra/settings.json

```
{
    "infraSetPol": {
        "attributes": {
            "dn": "uni/infra/settings",
            "domainValidation": "no"
        },
        "children": []
    }
}
```

Status: 400 Bad Request Time: 81 ms Size: 538 B

400 Bad Request

The request cannot be fulfilled due to bad syntax.

```
{
    "totalCount": "1",
    "imdata": [
        {
            "error": {
                "attributes": {
                    "code": "182",
                    "text": "Asking for domain validation is a one time operation. No further changes allowed."
                }
            }
        }
    ]
}
```

Asking for Domain Validation is a One Time Operation. No Further Changes Allowed.

Because this setting was not a default during initial release, any future enforced change in the default setting can cause incorrect configuration to fail, resulting in outages.

Due to this reason, the setting is user configurable.

Troubleshooting

Fault F0467 is raised for affected EPGs with missing access policies associations.

Reference this article Quick Start Isolation on how to troubleshoot the fault.

Related Information

- Address ACI Fault Code F0467: invalid-vlan, invalid-path, encap-already-in-use
- Setting Up an ACI Fabric: Initial Setup Configuration Example > System Settings
- Cisco Application Centric Infrastructure (ACI) Design Guide > EPG Domain Validation