EXTREME NETWORKS

# XIQ-C Enforce

Ludovico Stevens

Solutions Engineering

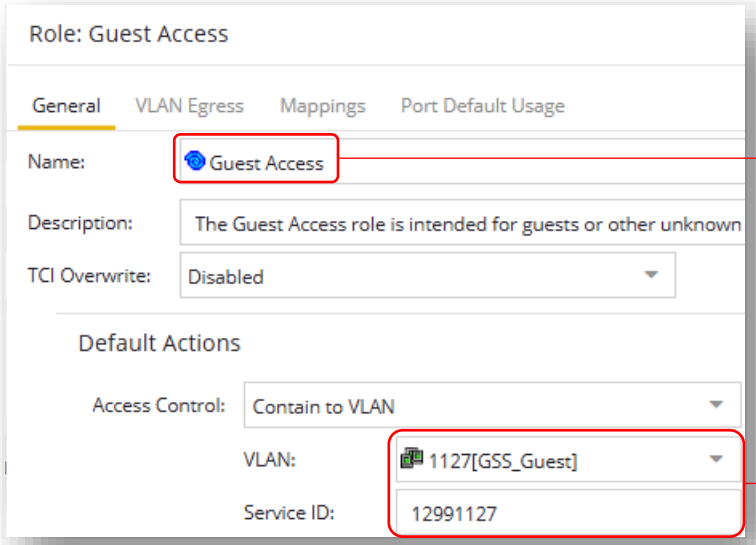
August 2025

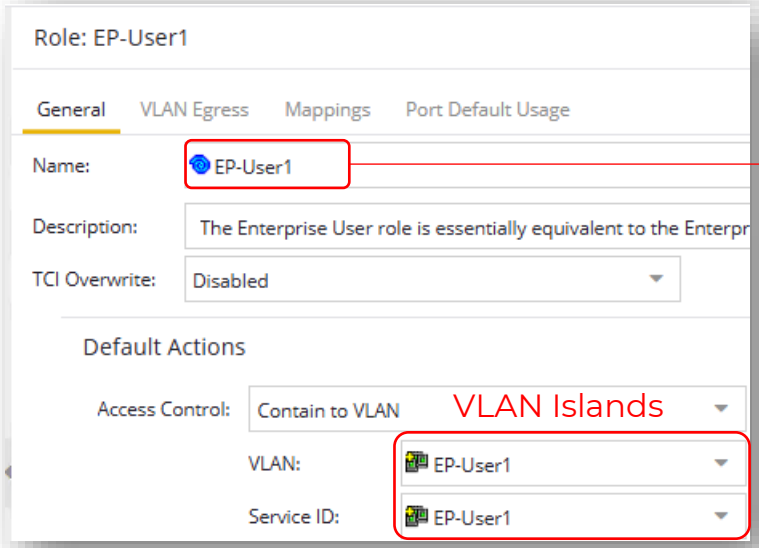
ADVANCE WITH US

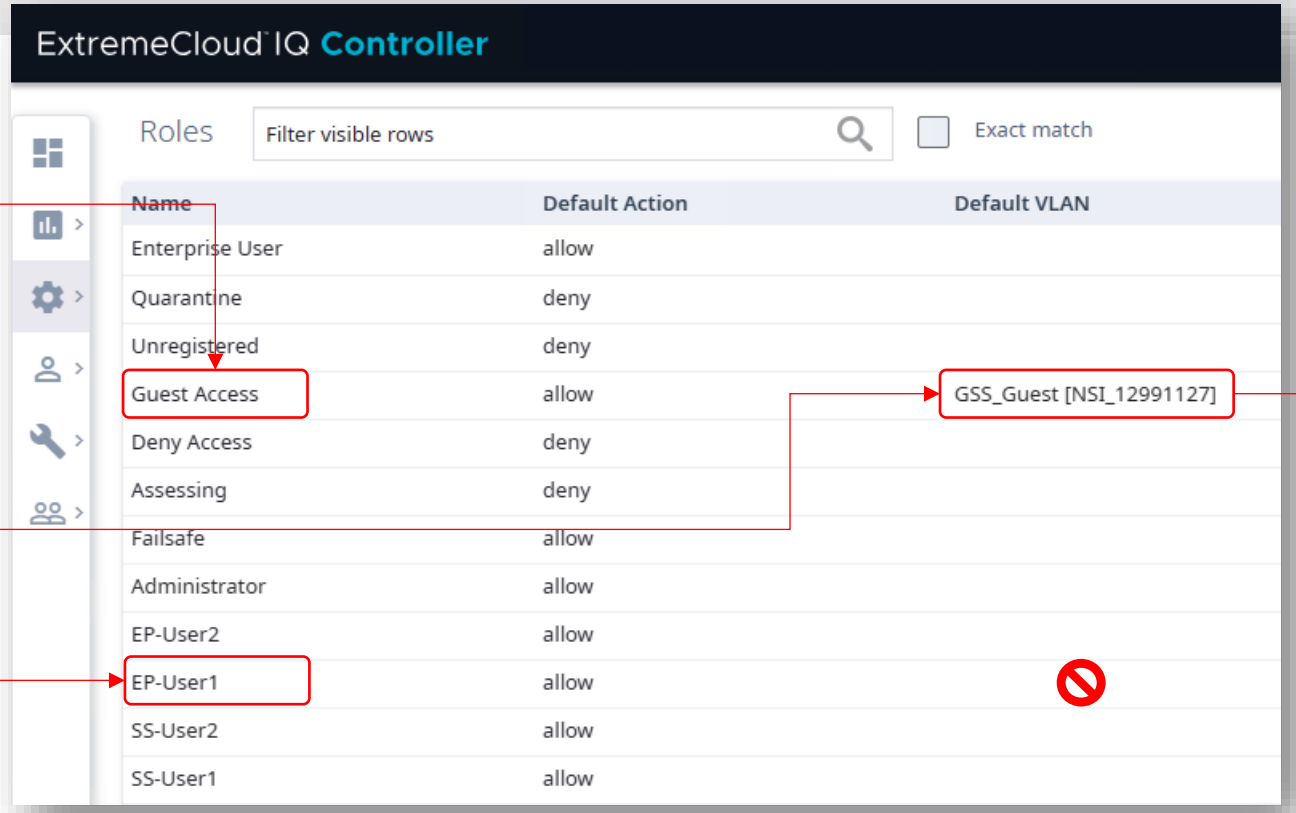
# XIQ-C Enforce VLAN Islands

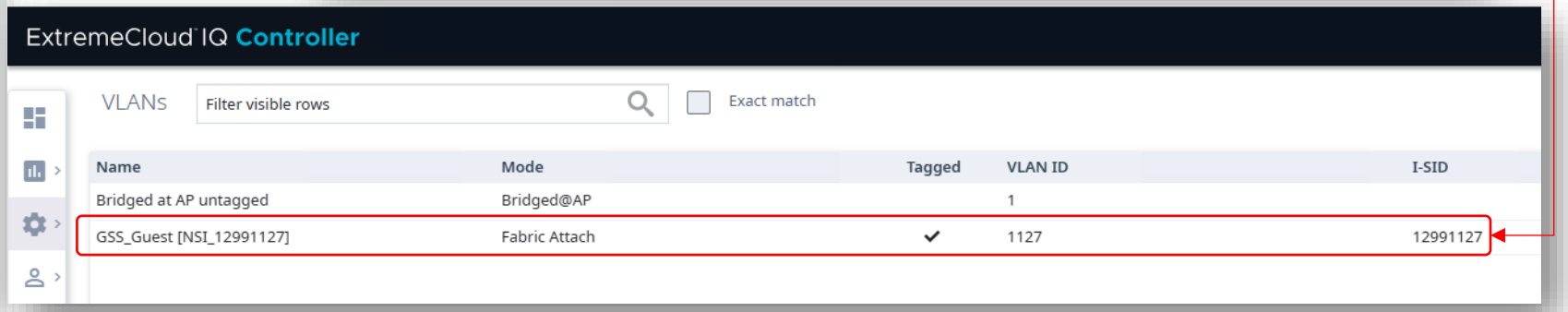
- Workflow to integrate XIQ-SE Policy VLAN Islands with XIQ-C
- XIQ-C does support XIQ-SE Policy. When an XIQ-SE Policy Enforce is performed, all the policy roles are pushed to XIQ-C with their respective VLAN-id and I-SID.
  - However, this only works if the Policy role is not using a VLAN Island reference (see next slide)
  - If the Policy role is using a VLAN Island, then only the Role is created on XIQ-C, but it is not linked to any VLAN topology information; this is where this workflow must be used
- This workflow is able to extract the XIQ-SE Policy VLAN Island data and push it via RESTCONF API into the XIQ-C VLAN topology table, and also associate it with XIQ-C device group profiles which need to be unique per XIQ-C Site
- XIQ-SE NAC Control then needs to also send back RFC 3580 VLAN-id RADIUS attribute for wireless authentications

# XIQ-C Native support of XIQ-SE Policies



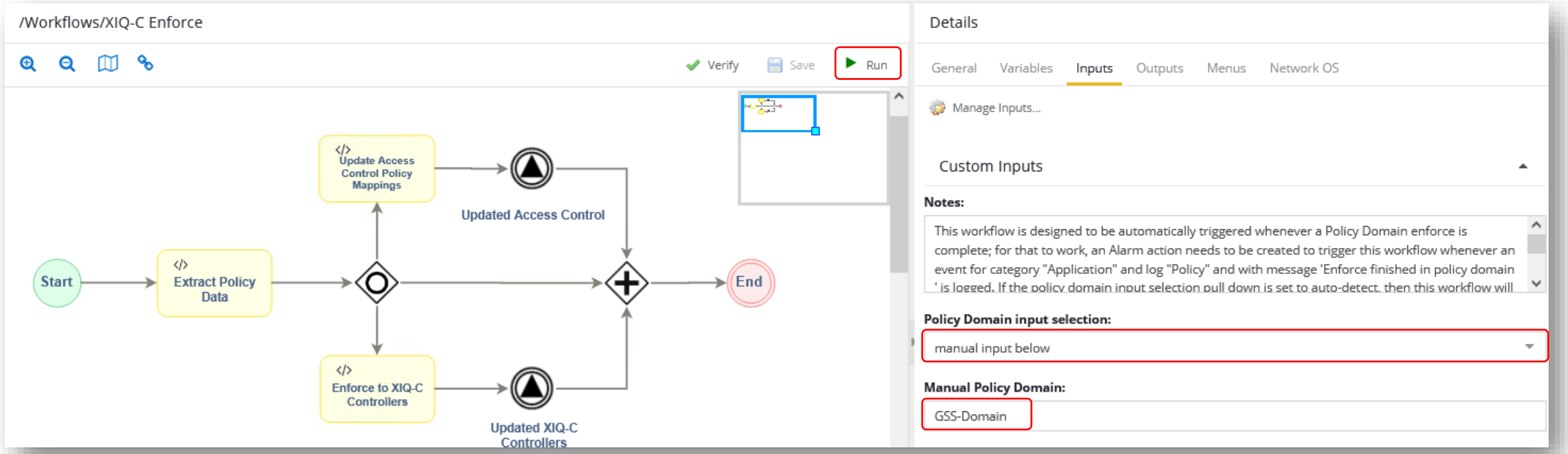



# XIQ-C Enforce Role ACL rules not supported by XIQ-SE

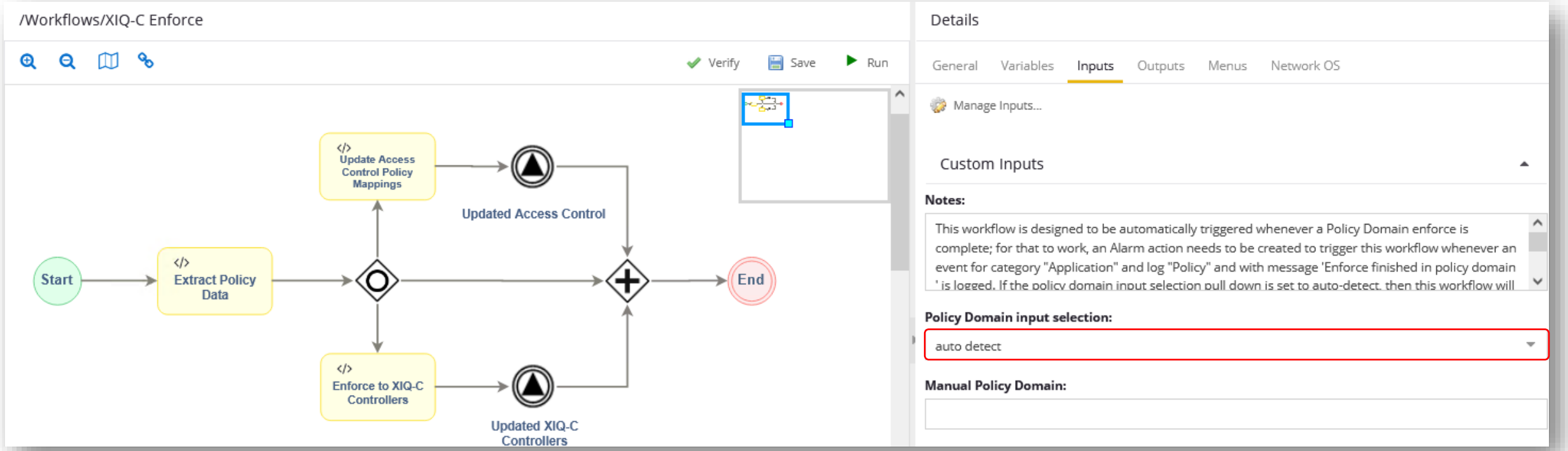
- Workflow to integrate XIQ-SE Policy with XIQ-C allowing role rules not natively supported in XIQ-SE for XIQ-C
- Some Role rule types necessary for Captive Web Portal cannot be pushed from XIQ-SE
  - L3 FQDN Rules
  - Egress any source rules
  - HTTP/HTTPS redirect rules
- XIQ-SE will either not allow the above rules at all, or it will not allow them for device type “XIQ-Controller” or it will allow them for “All Devices” but with then error if/when enforced to XIQ-C
- Manually adding these rules to the roles directly in XIQ-C is futile as on the next Policy enforce they get wiped.
- Workflow workaround. Configure the desired role rules in XIQ-SE and label them for device “Wireless Controller” (older version of XIQ-C with which those rules are still allowed in XIQ-SE)
- This workflow parses all the Policy roles and inspects all the rules (services) associated. If a Role is found to have “Wireless Controller” rules, all rules for the role are extracted. Next the workflow will update the same role on XIQ-C. Since this workflow runs after a normal Policy enforce, rules supported by XIQ-SE for XIQ-C will already have been pushed to XIQ-C. While any “Wireless Controller” rules will not have been pushed. This workflow will go insert the “Wireless Controller” rules to the intended roles and in the order expected including if some supported rules were already pushed by Policy enforce.

# Running the workflow manually



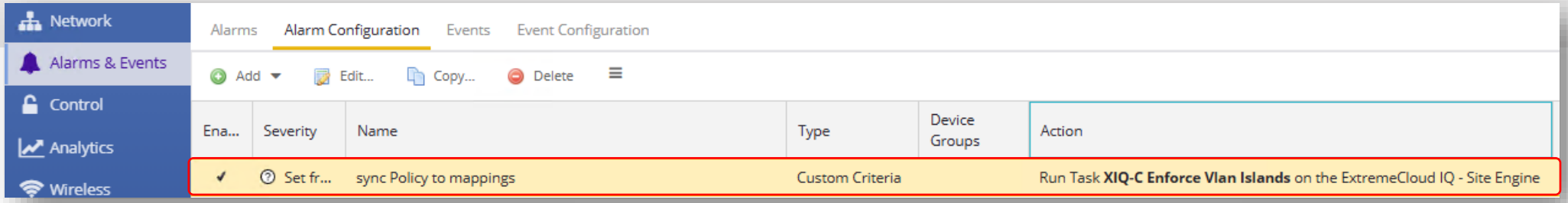

- Set the Policy Domain input selection to “manual input below”
- Provide the policy domain as input
- Run the workflow

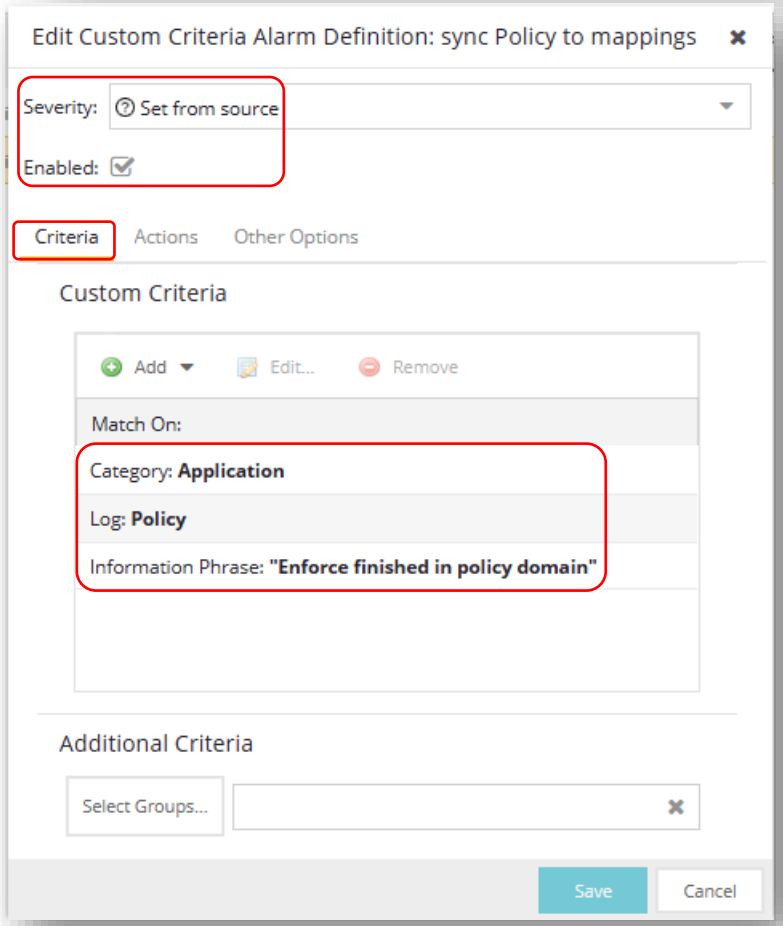
# Automatically running the workflow on Policy Enforce

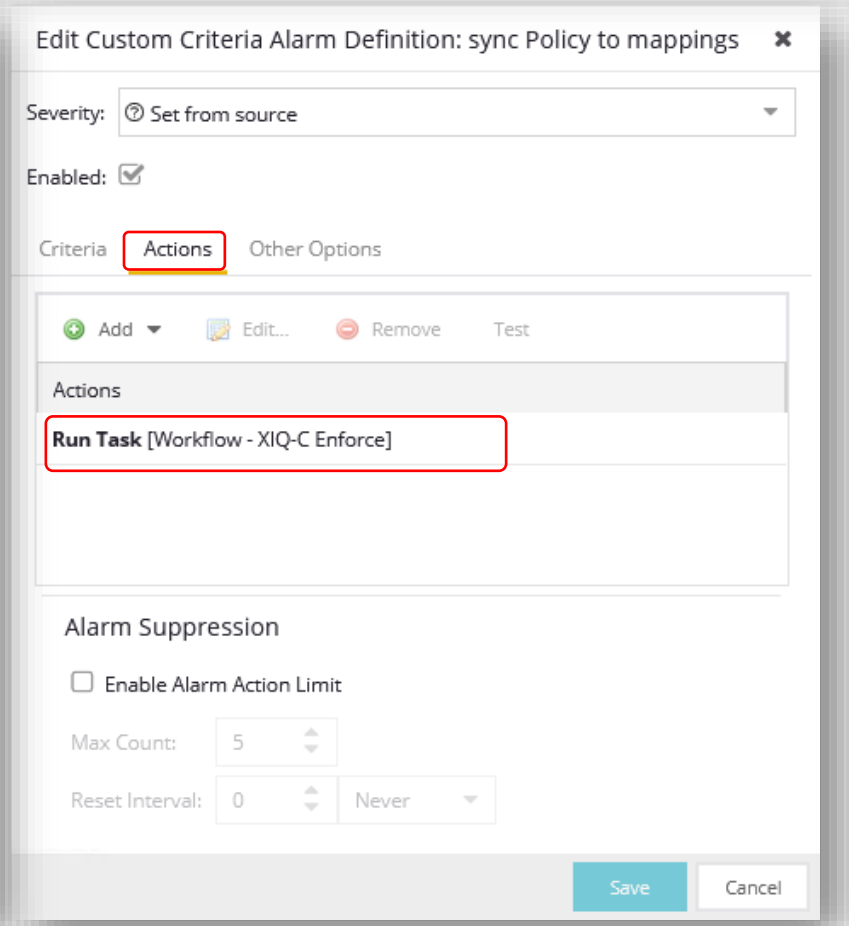


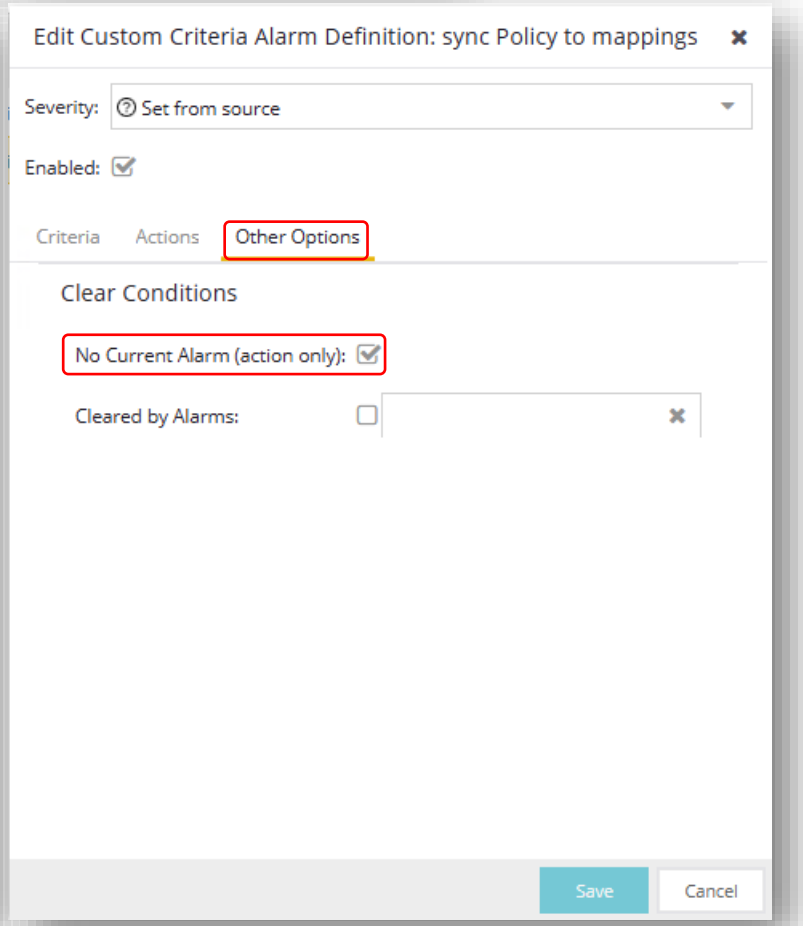

- Set the Policy Domain input selection to “auto-detect”
- Configure an Alarm as shown in next slide

# Triggering workflow on Alarm (completion of Policy Domain enforce)



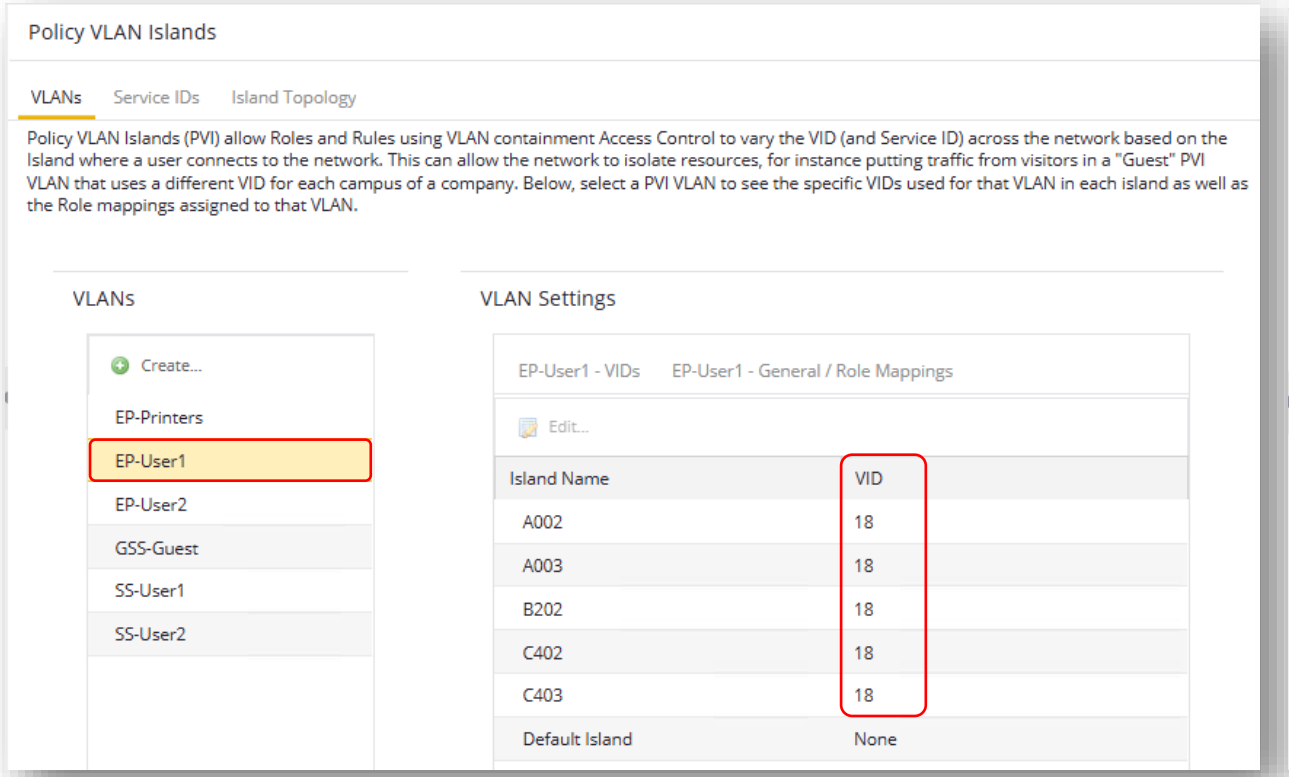



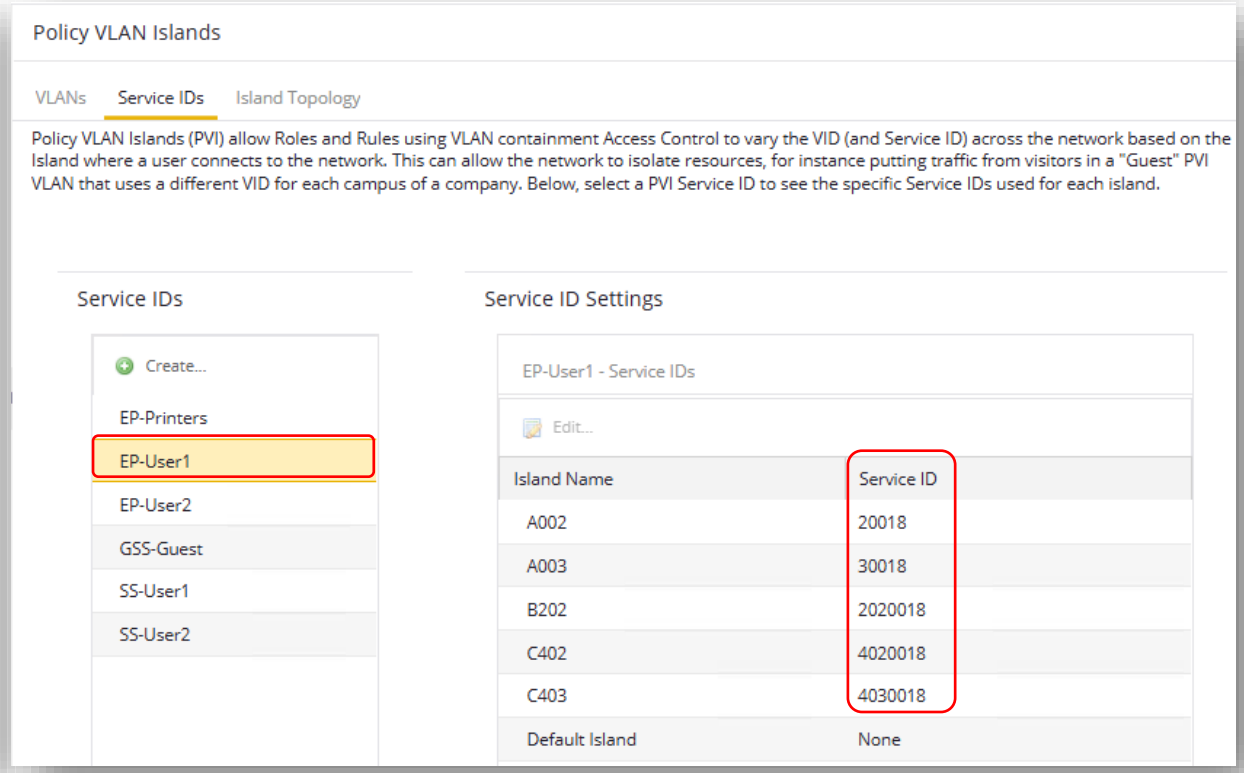



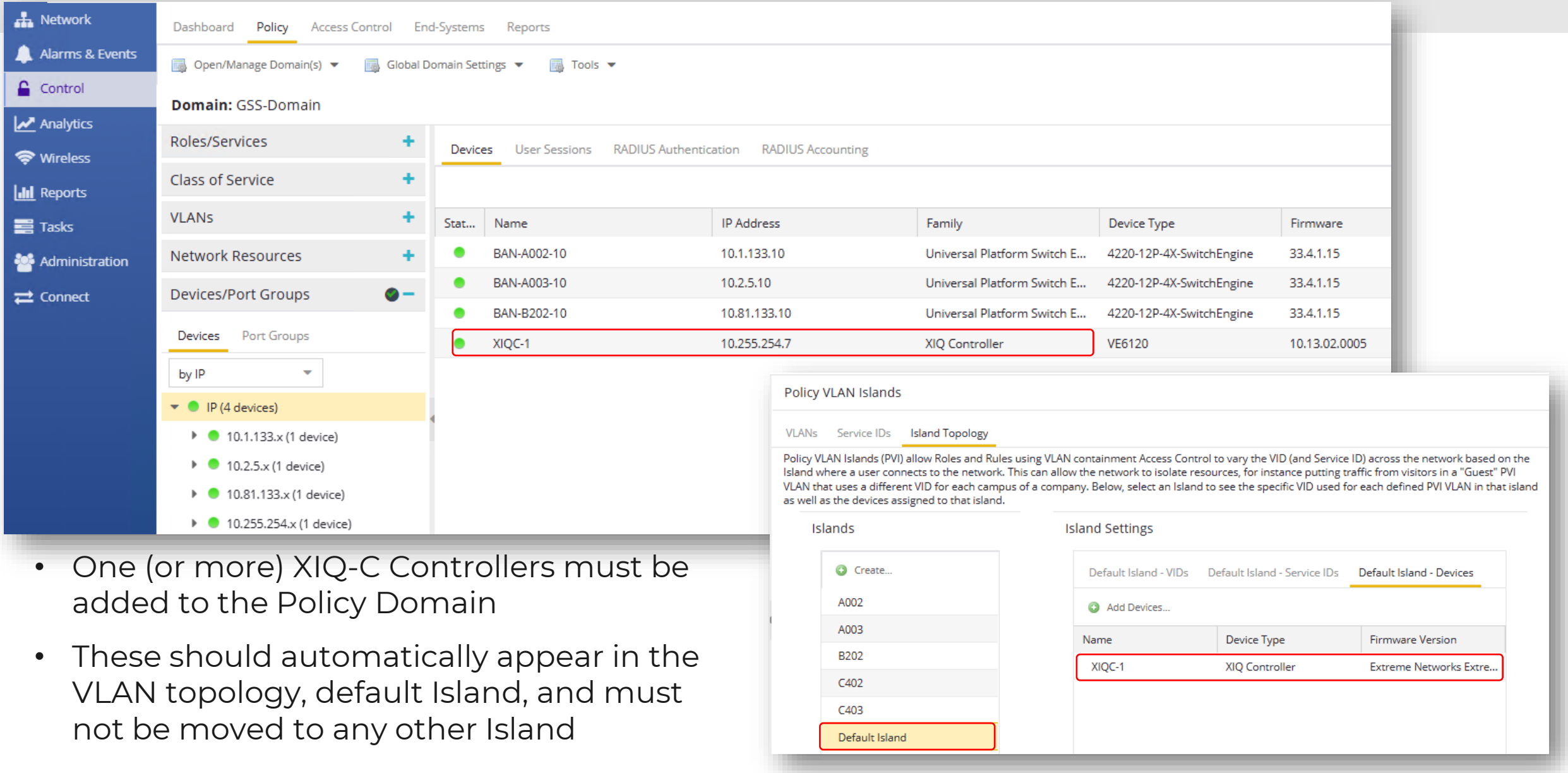
# Requirement - 1

- The workflow will only look at Policy roles where the VLAN-id is the same across all island topologies, but the I-SID value is unique and different across all island topologies
- The desire is to re-use the VLAN-id in the branch locations, but in reality, a different I-SID (IP subnet)
- As will be seen later, the VLAN-id is provided via RADIUS RFC3580, so must be the same everywhere for a given role



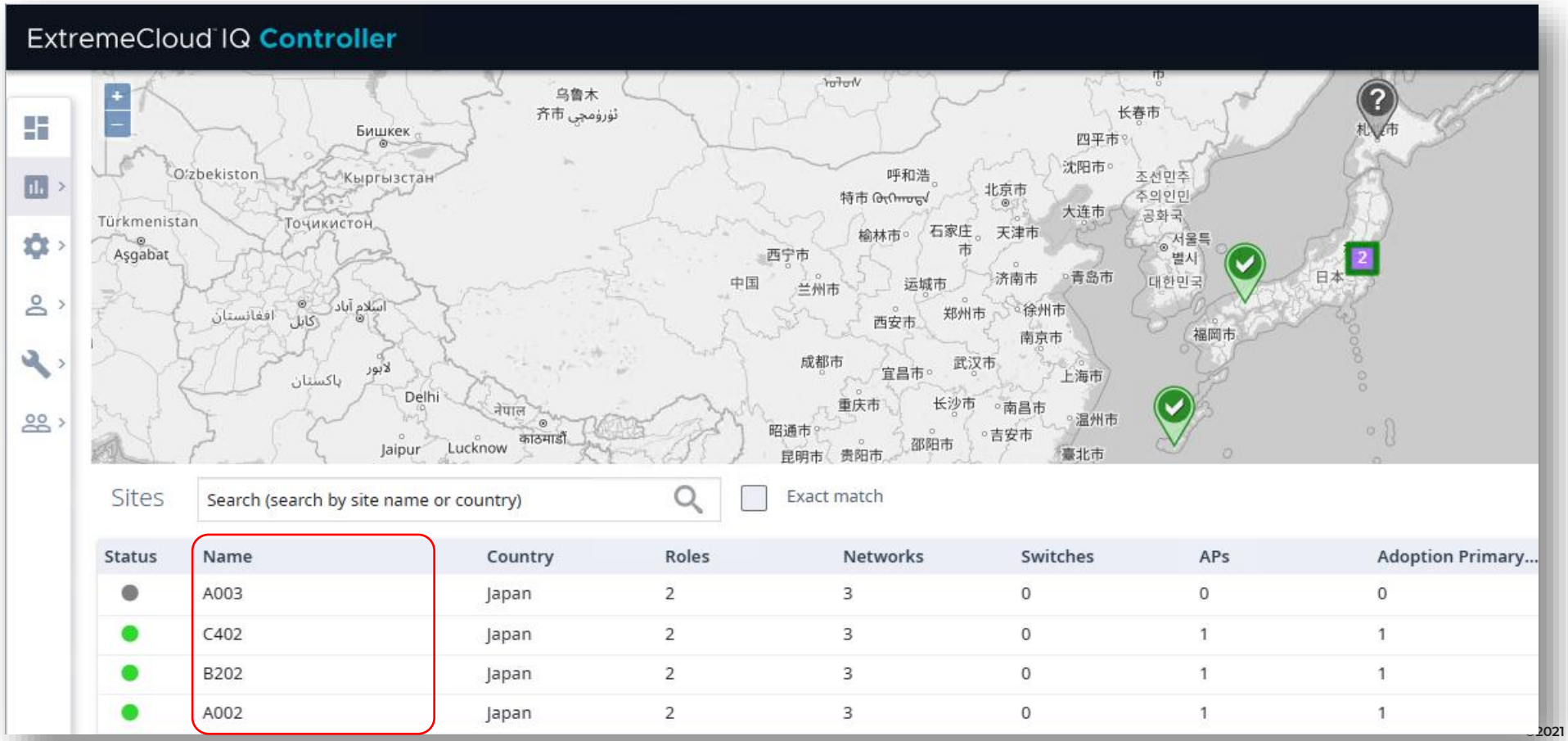
# Requirement - 2




- One (or more) XIQ-C Controllers must be added to the Policy Domain
- These should automatically appear in the VLAN topology, default Island, and must not be moved to any other Island

# Requirement - 3

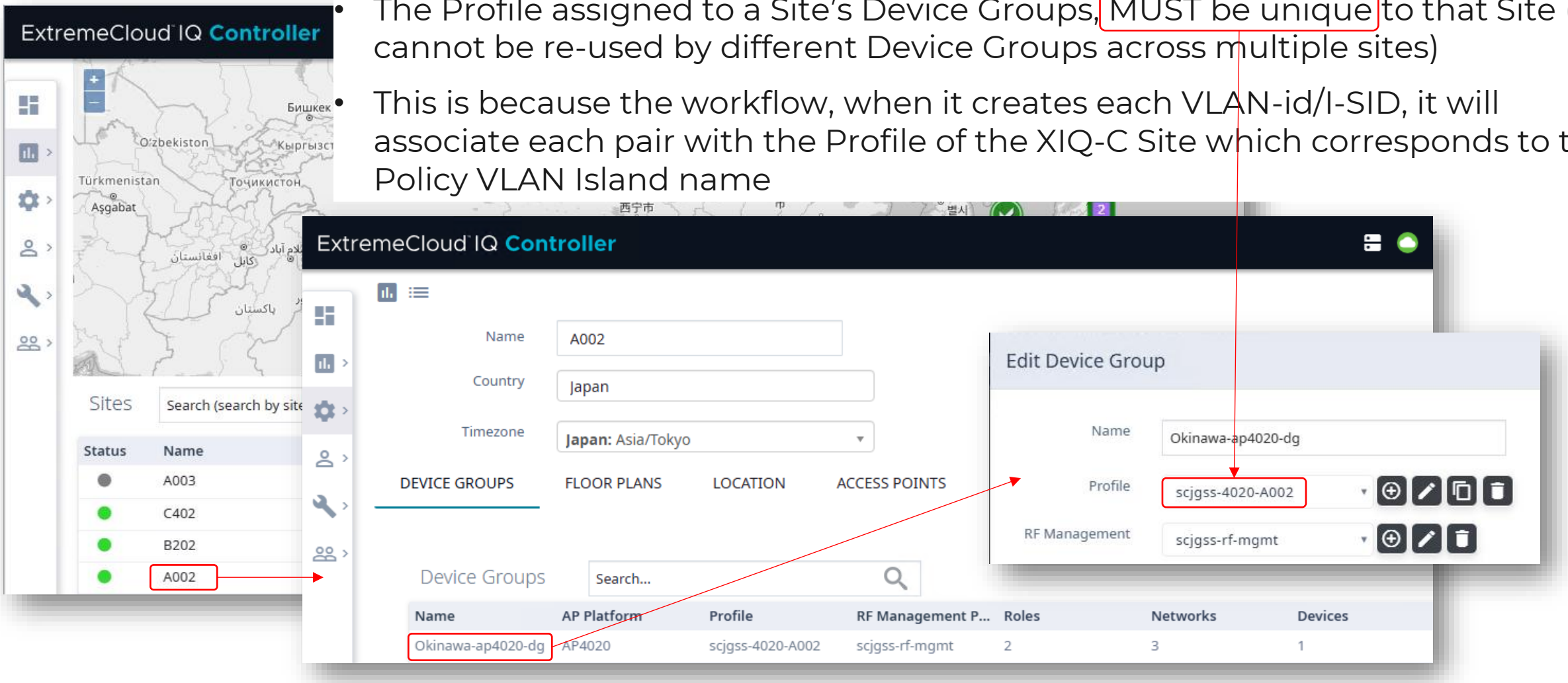
- The workflow needs to be able to link the Policy VLAN Island names , to XIQ-C Site Names
- So, the XIQ-C Site Names either have to be made identical to the XIQ-SE Policy VLAN Island names (as in screen shot below), or they must contain the latter (e.g. “Okinawa-A002”)



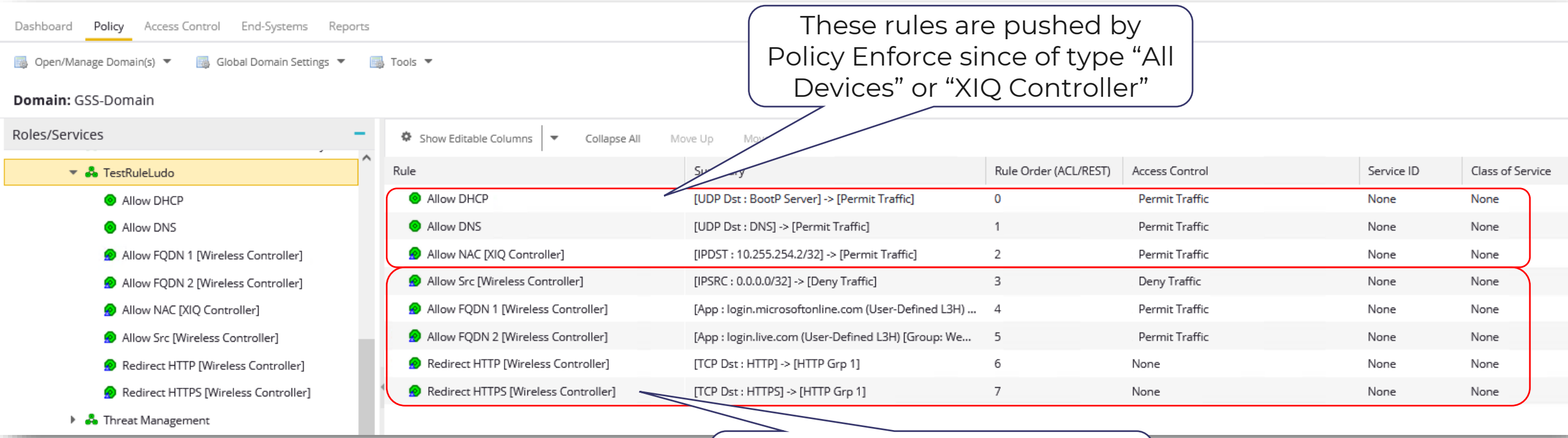

| Status | Name | Country | Roles | Networks | Switches | APs | Adoption Primary... |
|---|---|---|---|---|---|---|---|
| ● | A003 | Japan | 2 | 3 | 0 | 0 | 0 |
| ● | C402 | Japan | 2 | 3 | 0 | 1 | 1 |
| ● | B202 | Japan | 2 | 3 | 0 | 1 | 1 |
| ● | A002 | Japan | 2 | 3 | 0 | 1 | 1 |

# Requirement - 4

- The Profile assigned to a Site's Device Groups, MUST be unique to that Site (it cannot be re-used by different Device Groups across multiple sites)
- This is because the workflow, when it creates each VLAN-id/I-SID, it will associate each pair with the Profile of the XIQ-C Site which corresponds to the Policy VLAN Island name



# Creating “Wireless Controller” rules

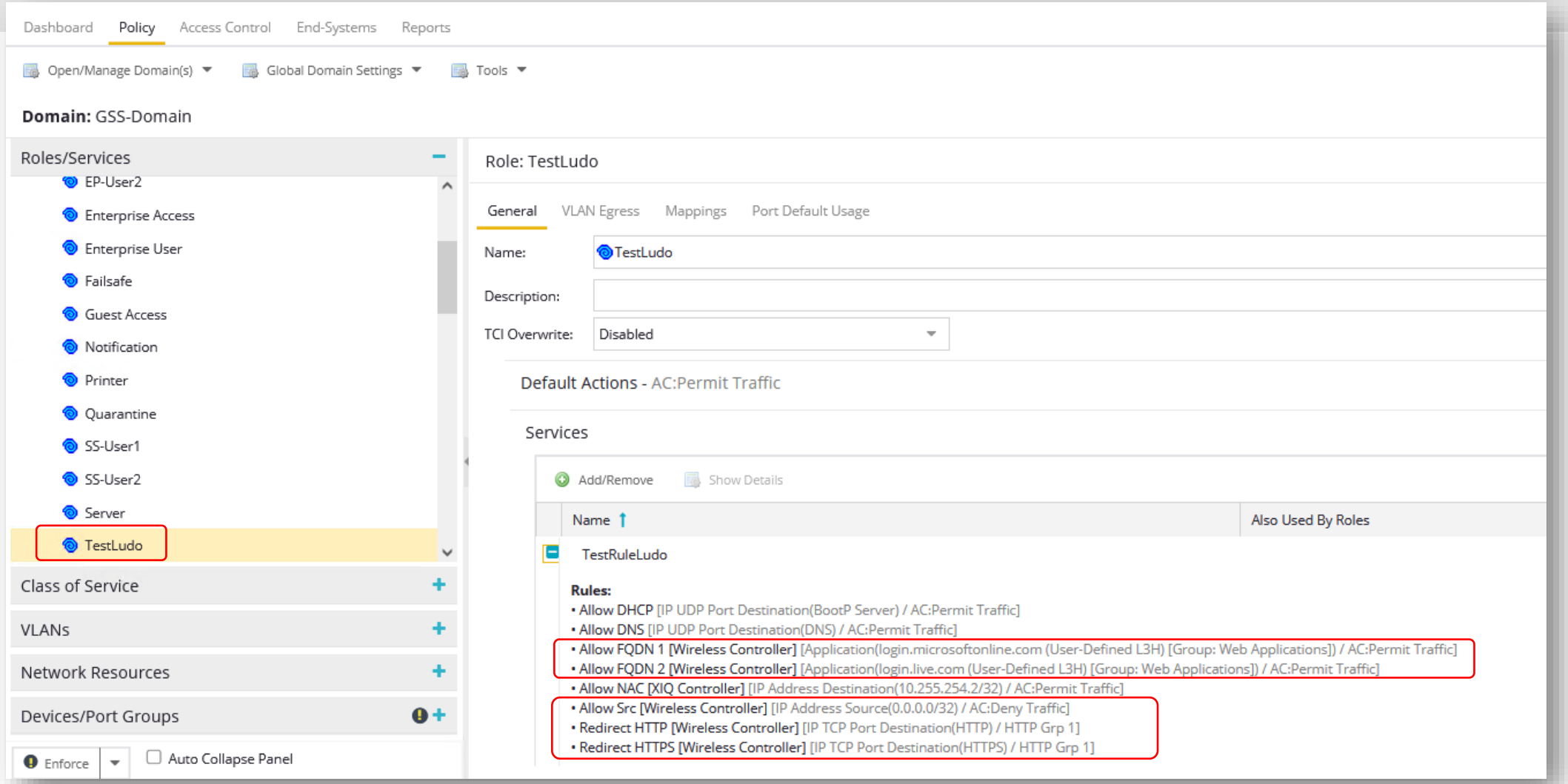



These rules are pushed by Policy Enforce since of type “All Devices” or “XIQ Controller”

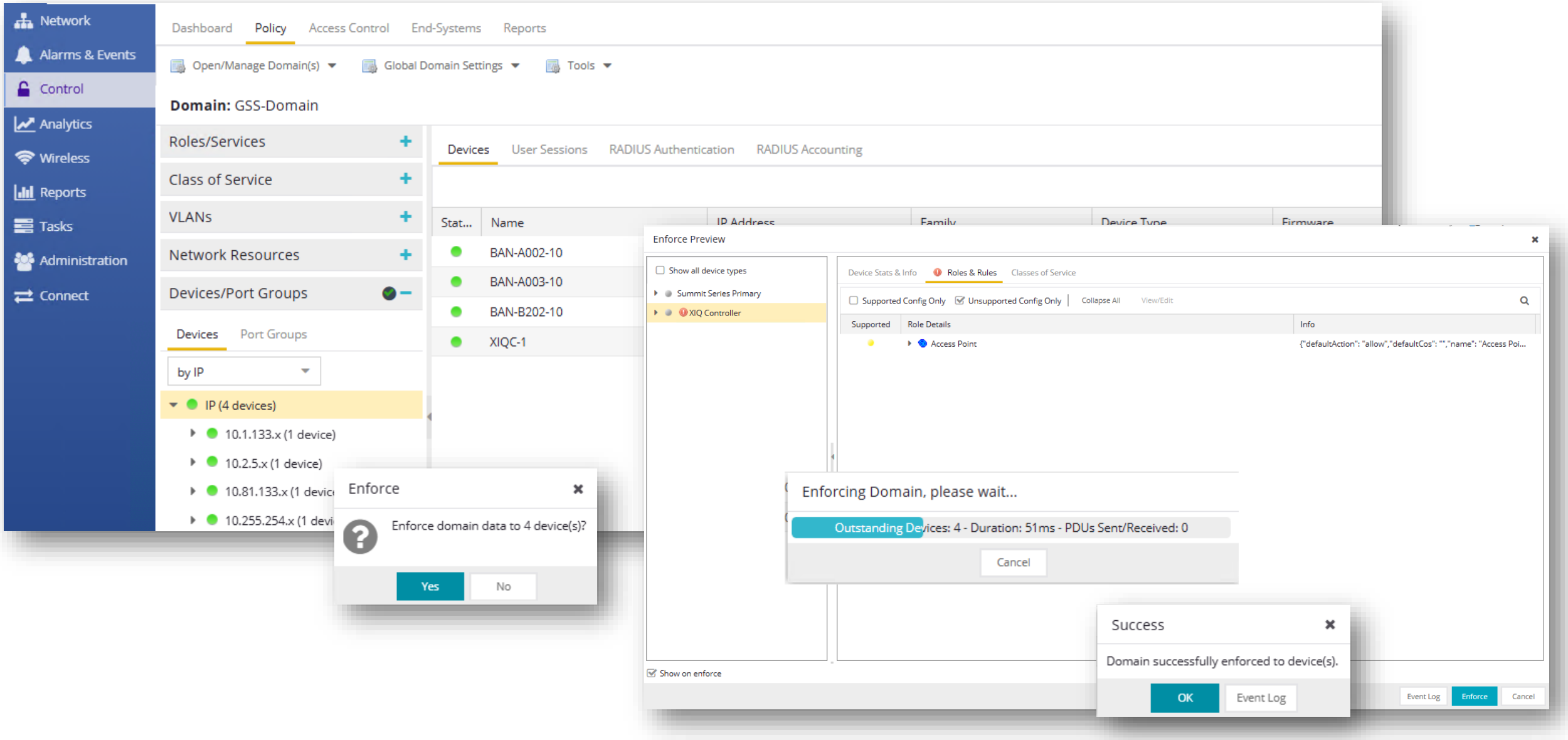
These rules are pushed by the workflow since of type “Wireless Controller”

- Make sure rule order is set as required in this screen

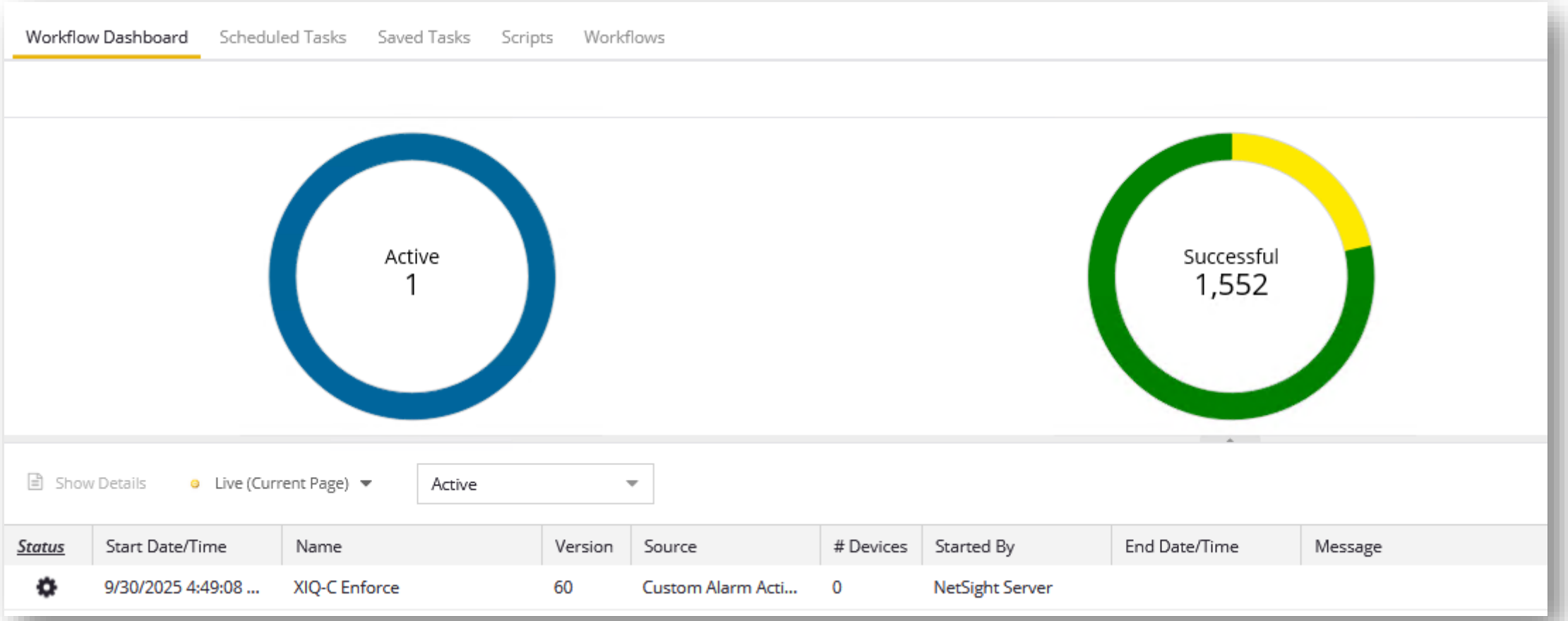
# “Wireless Controller” rules assigned to a Role



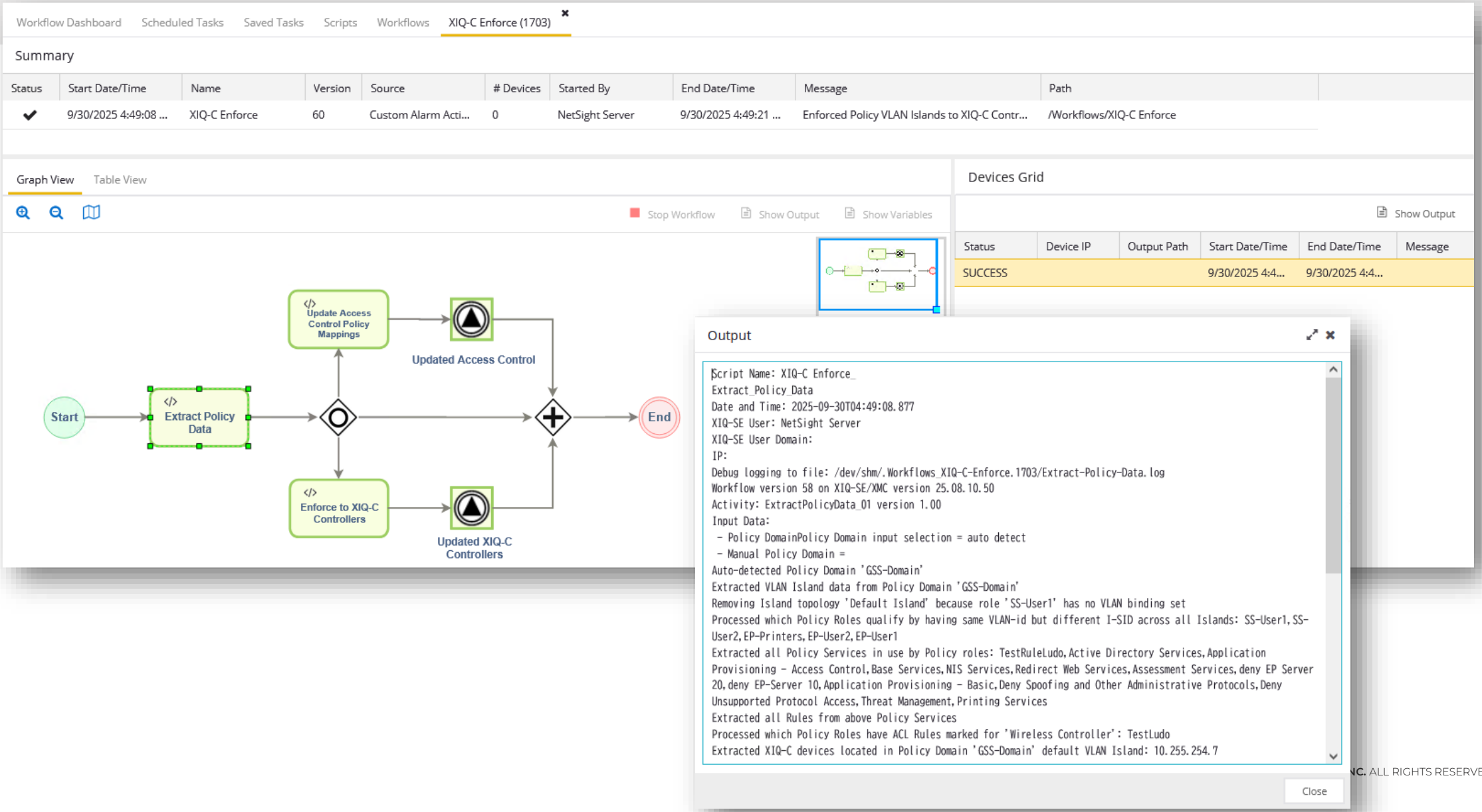
# Enforce Policy Domain



# Workflow automatically executes

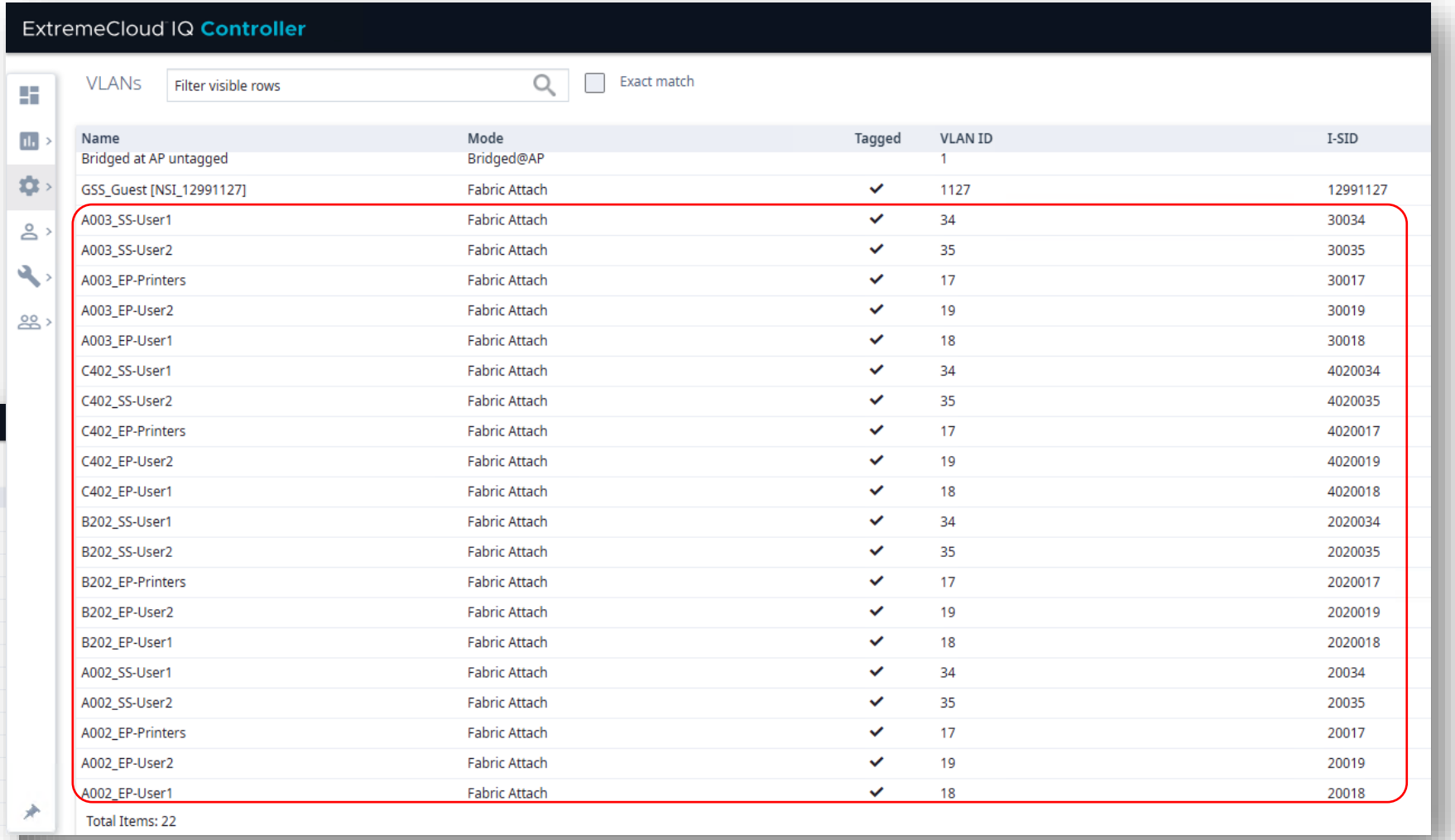


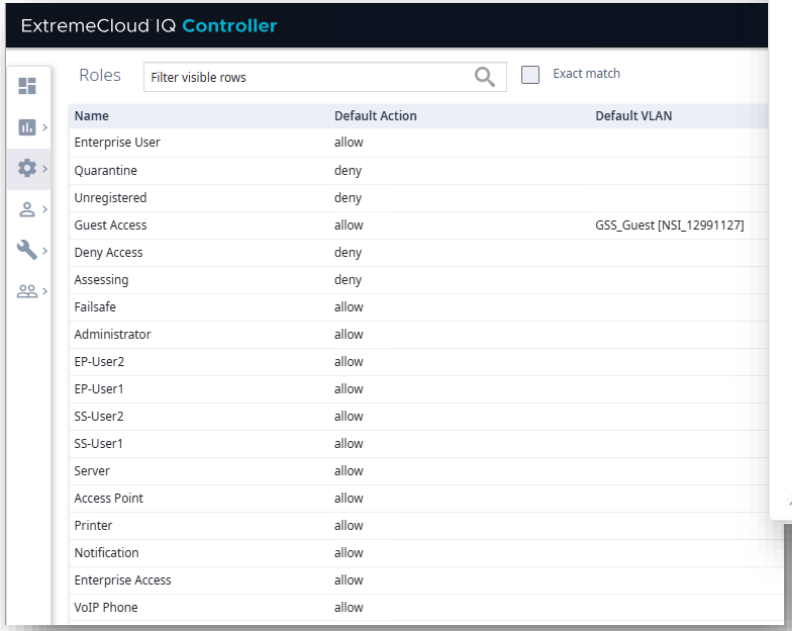
# Workflow automatically executes



# What workflow did - 1

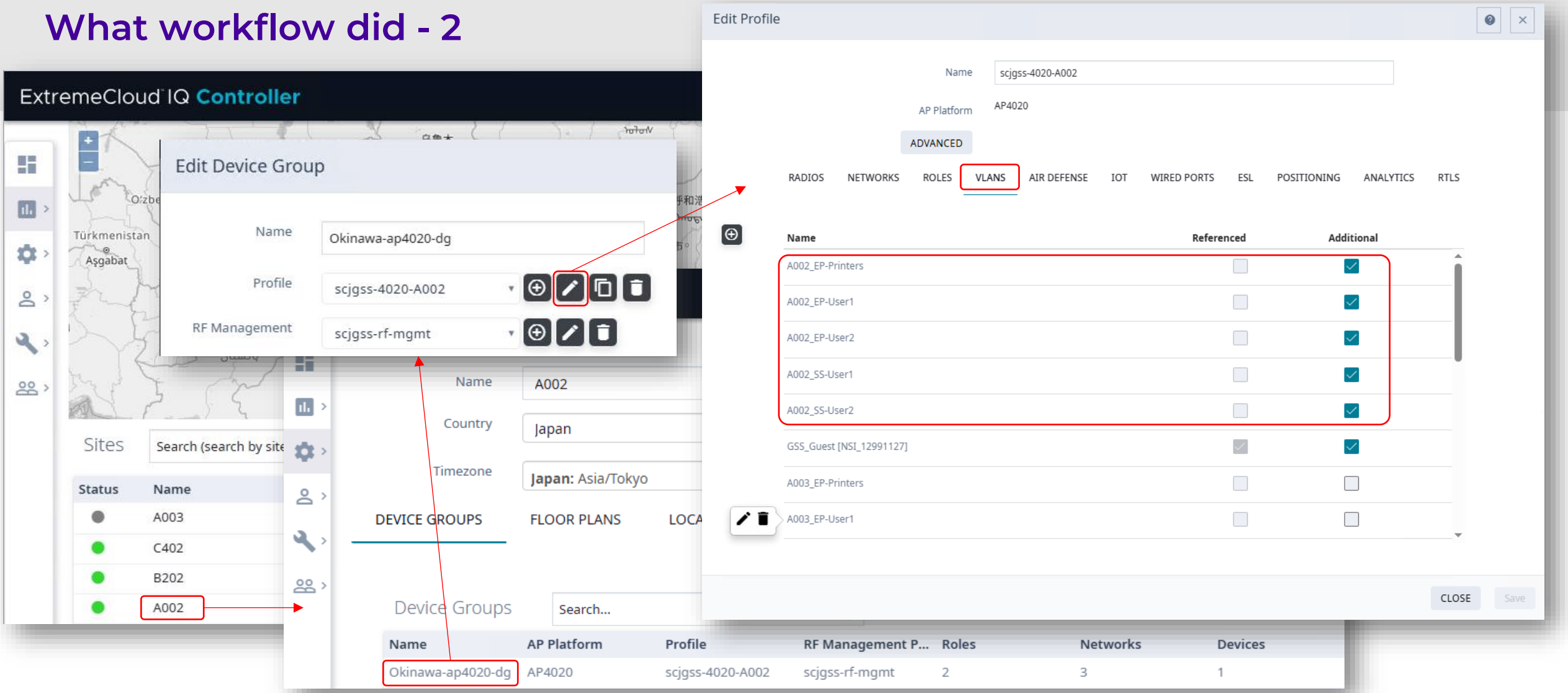
- Workflow created all the VLAN topologies on XIQ-C, each VLAN takes name the Island name + Role name
- Note that the XIQ-C Roles (pushed by native XIQ-SE Policy Enforce) still cannot reference these VLAN topologies…



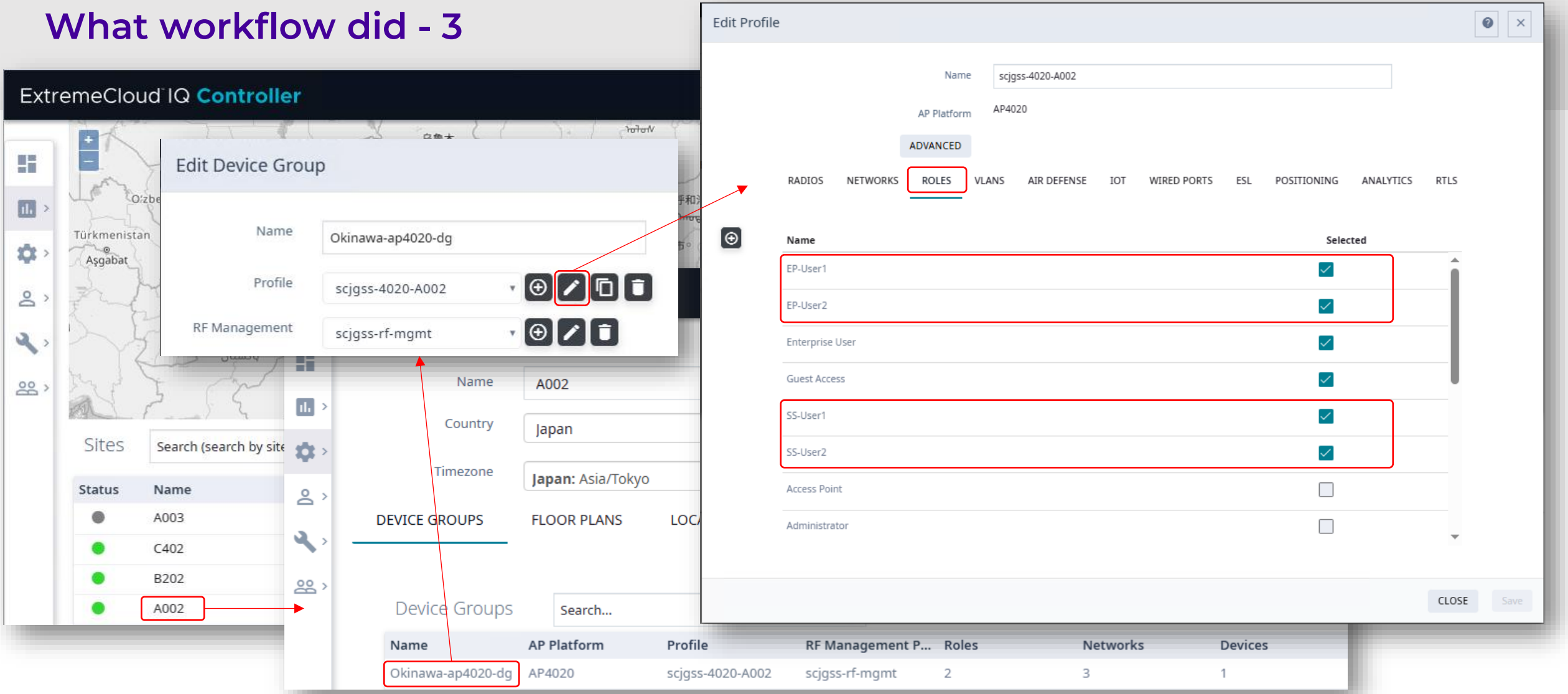

 

# What workflow did - 2



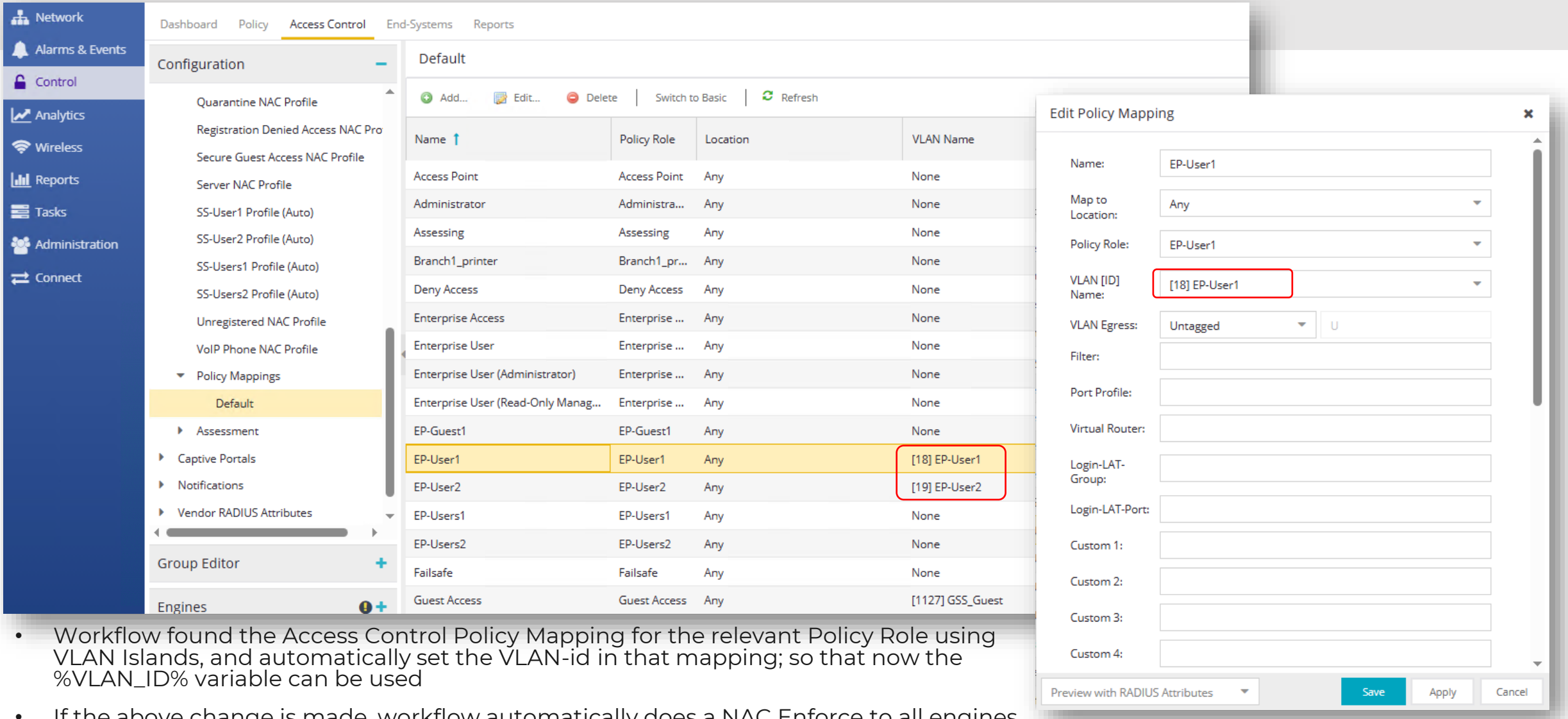

- Note that VLAN topologies for Island name “A002” have automatically been added into the XIQ-C Site’s Device Group assigned Profile
- Bingo! Now it is enough for XIQ-SE Control to return just the RFC3580 VLAN-id RADIUS attribute, and wireless users will automatically get the VLAN topology with that VLAN-id assigned to the Profile the AP is in

# What workflow did - 3




- All Roles are also added to the same Profile (the ones which use VLAN Islands were added by the workflow; the ones not using VLAN Islands were already added)

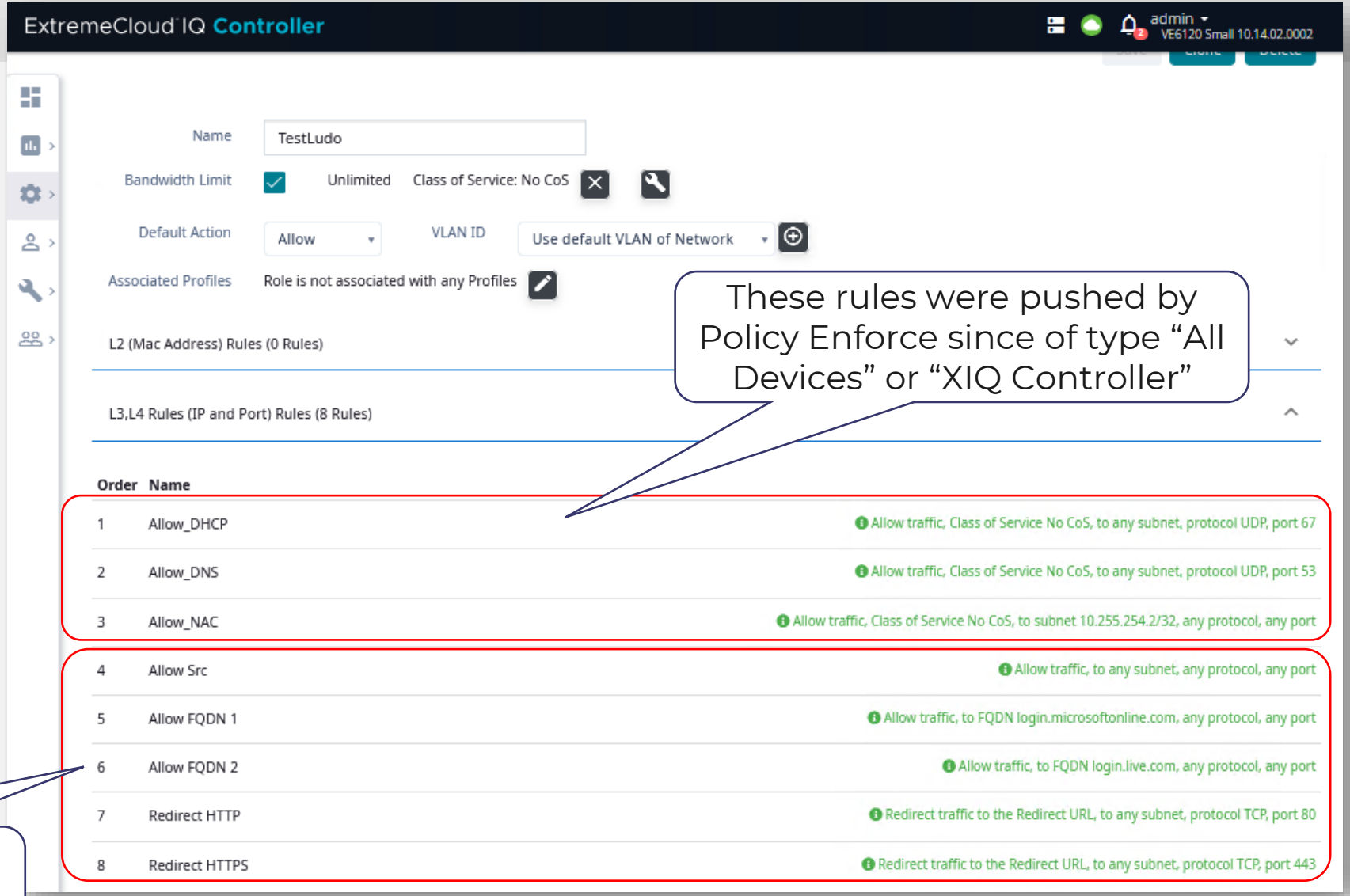
# What workflow did - 4




- Workflow found the Access Control Policy Mapping for the relevant Policy Role using VLAN Islands, and automatically set the VLAN-id in that mapping; so that now the %VLAN_ID% variable can be used
- If the above change is made, workflow automatically does a NAC Enforce to all engines

# What workflow did - 5

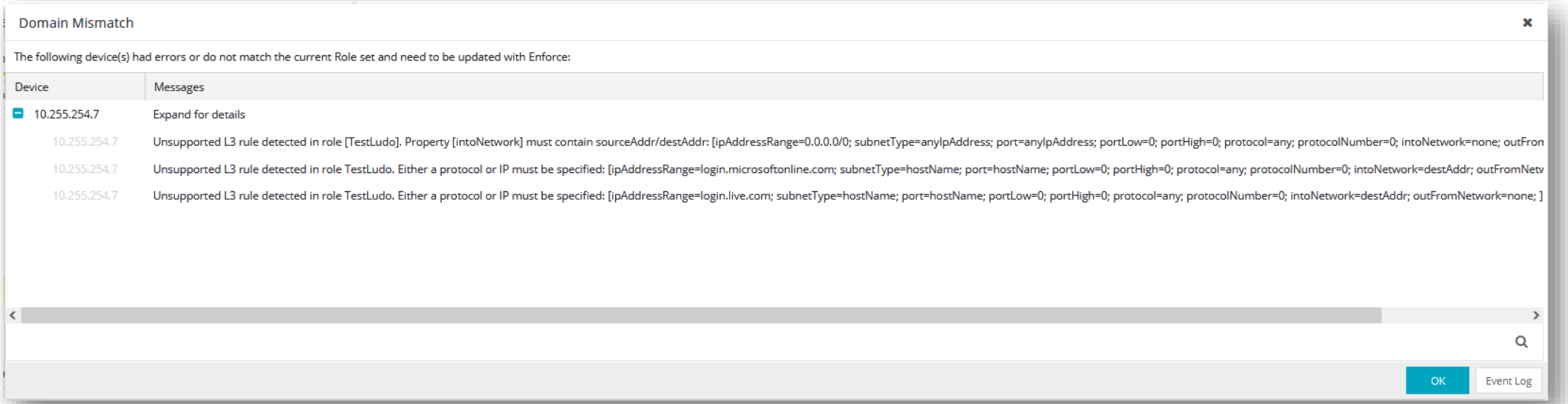
- Workflow preserved the rules already pushed by the Policy enforce and added the extra “Wireless Controller” rules
- Workflow also ensures that both rule types are created in the correct order as defined in Policy




These rules were pushed by Policy Enforce since of type “All Devices” or “XIQ Controller”

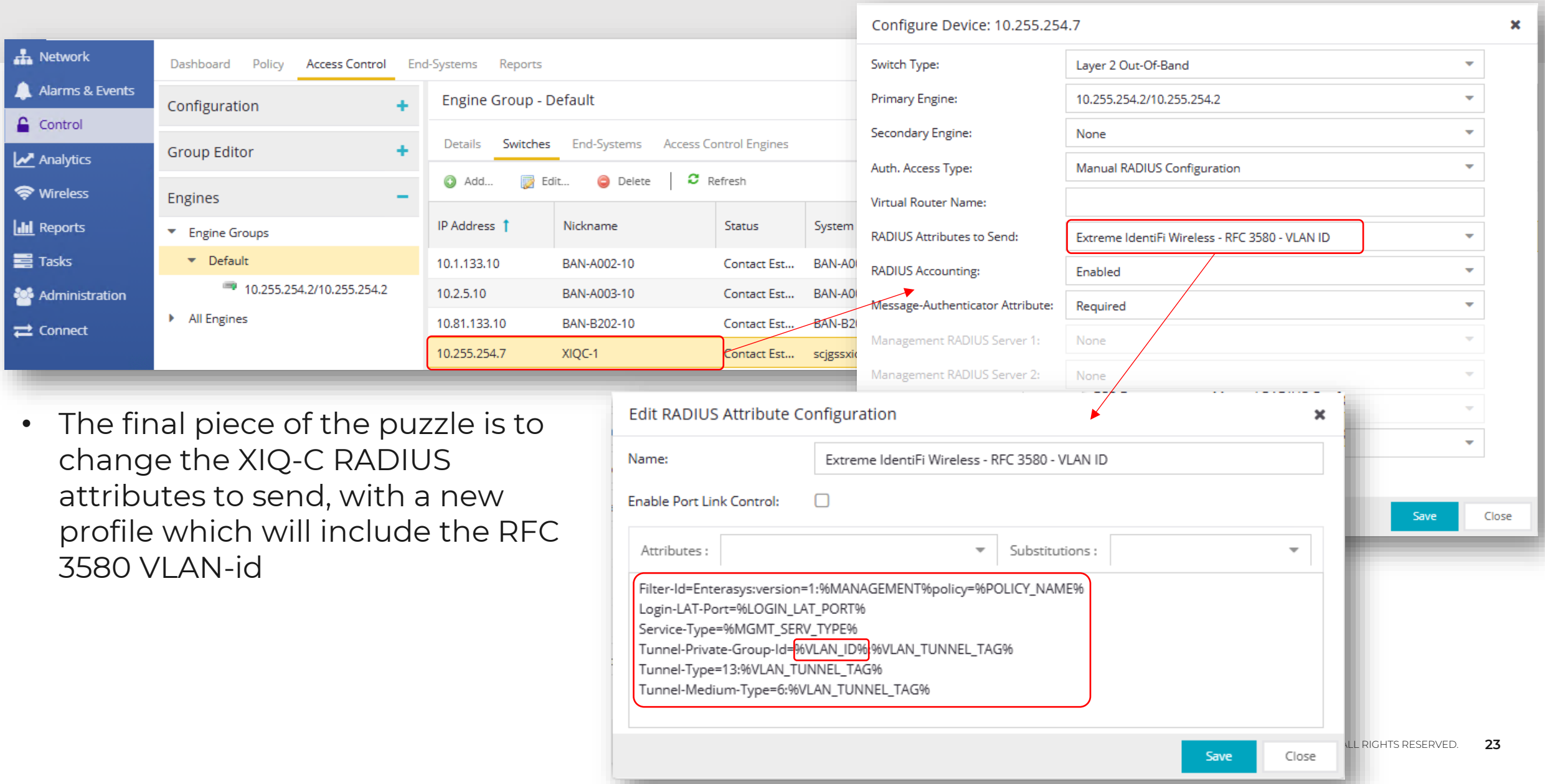
These rules were pushed by the workflow since of type “Wireless Controller”

# Limitation




- Doing a Policy Verify against the XIQ-C devices will pickup the extra rules pushed by the workflow and report them as unsupported / unexpected

# Changing the RADIUS template for XIQ-C




- The final piece of the puzzle is to change the XIQ-C RADIUS attributes to send, with a new profile which will include the RFC 3580 VLAN-id