

EXTREME NETWORKS

# XIQ-C Enforce

Ludovico Stevens

Solutions Engineering

August 2025

- 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



Role: Guest Access

General | VLAN Egress | Mappings | Port Default Usage

Name: **Guest Access**

Description: The Guest Access role is intended for guests or other unknown

TCI Overwrite: Disabled

Default Actions

Access Control: Contain to VLAN

VLAN: **1127[GSS\_Guest]**

Service ID: 12991127

Role: EP-User1

General | VLAN Egress | Mappings | Port Default Usage

Name: **EP-User1**

Description: The Enterprise User role is essentially equivalent to the Enterpr

TCI Overwrite: Disabled

Default Actions

Access Control: Contain to VLAN **VLAN Islands**

VLAN: **EP-User1**

Service ID: **EP-User1**

ExtremeCloud IQ Controller

Roles

Filter visible rows

Exact match

| Name                | Default Action | Default VLAN                    |
|---------------------|----------------|---------------------------------|
| Enterprise User     | allow          |                                 |
| Quarantine          | deny           |                                 |
| Unregistered        | deny           |                                 |
| <b>Guest Access</b> | allow          | <b>GSS_Guest [NSI_12991127]</b> |
| Deny Access         | deny           |                                 |
| Assessing           | deny           |                                 |
| Failsafe            | allow          |                                 |
| Administrator       | allow          |                                 |
| EP-User2            | allow          |                                 |
| <b>EP-User1</b>     | allow          |                                 |
| SS-User2            | allow          |                                 |
| SS-User1            | allow          |                                 |

ExtremeCloud IQ Controller

VLANs

Filter visible rows

Exact match

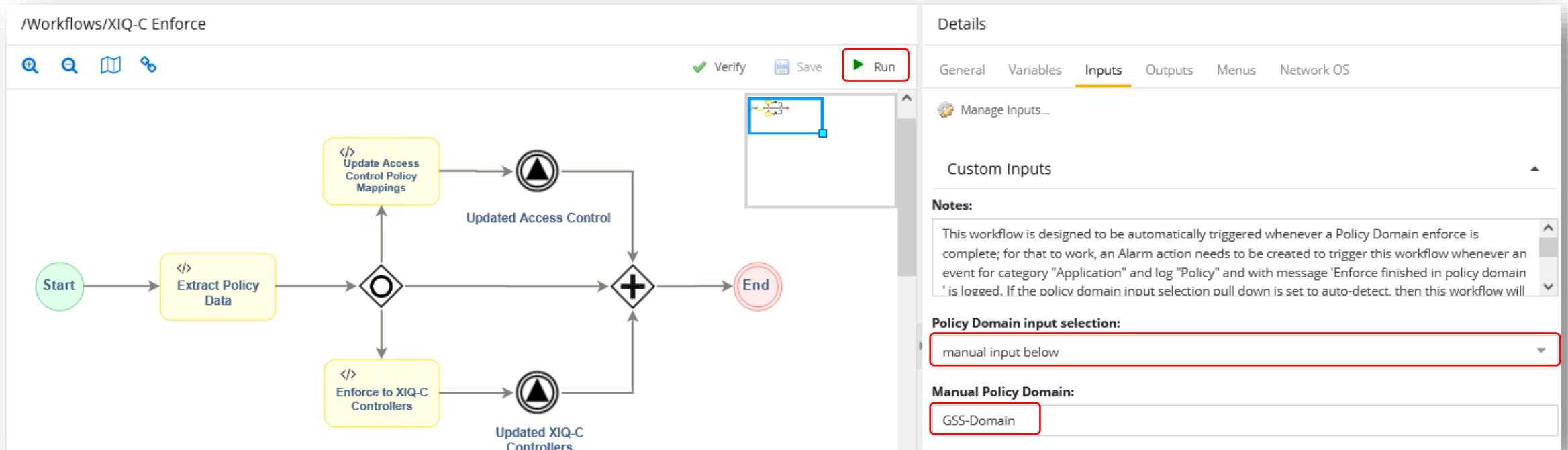
| Name                            | Mode          | Tagged | VLAN ID | I-SID    |
|---------------------------------|---------------|--------|---------|----------|
| Bridged at AP untagged          | Bridged@AP    |        | 1       |          |
| <b>GSS_Guest [NSI_12991127]</b> | Fabric Attach | ✓      | 1127    | 12991127 |

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



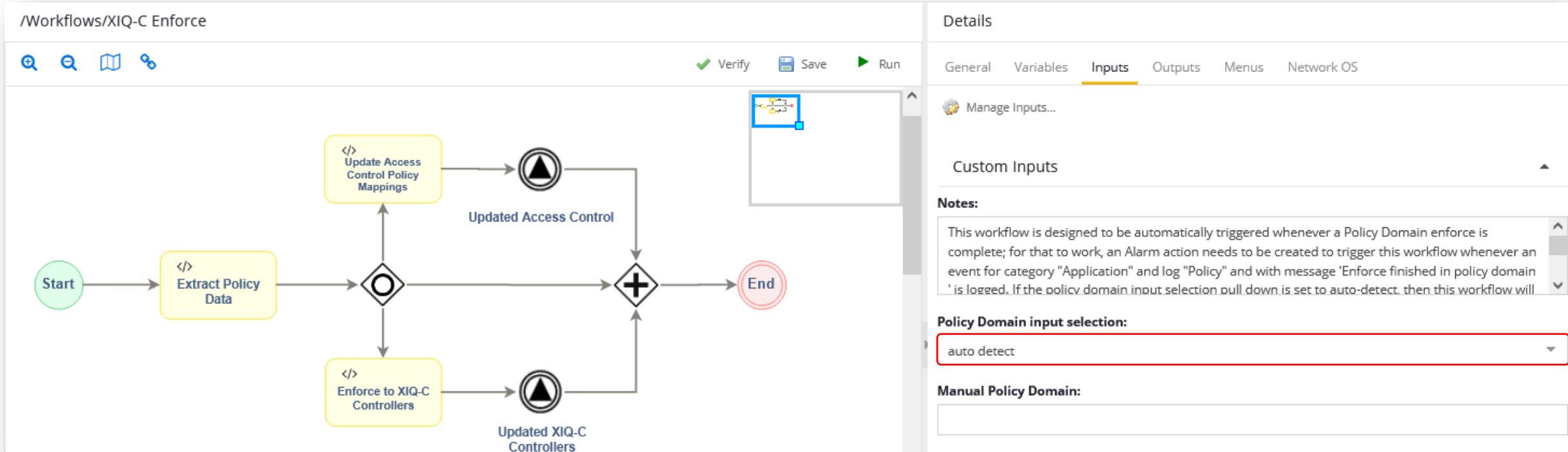
- Workflow to integrate XIQ-SE Policy with XIQ-C allowing role rules not natively supported in XIQ-SE for XIQ-C
- Some Role rule types necessary for Captive Web Portal cannot be pushed from XIQ-SE
  - L3 FQDN Rules
  - Egress any source rules
  - HTTP/HTTPS redirect rules
- XIQ-SE will either not allow 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)



|   |           |                         |                 |               |  |
|---|-----------|-------------------------|-----------------|---------------|--|
| Network   |           |                         |                 |               |  |
| Alarms & Events                                       |           |                         |                 |               |  |
| Control   |           |                         |                 |               |  |
| Analytics   |           |                         |                 |               |  |
| Wireless  |           |                         |                 |               |  |
| Alarms Alarm Configuration Events Event Configuration |           |                         |                 |               |  |
| Add Edit... Copy... Delete                            |           |                         |                 |               |  |
| Ena...  | Severity  | Name                    | Type            | Device Groups | Action   |
| ✓   | Set fr... | sync Policy to mappings | Custom Criteria |               | Run Task XIQ-C Enforce Vlan Islands on the ExtremeCloud IQ - Site Engine |

Edit Custom Criteria Alarm Definition: sync Policy to mappings

Severity: Set from source

Enabled: ☒

Criteria Actions Other Options

Custom Criteria

Add Edit... Remove

Match On:

Category: **Application**

Log: **Policy**

Information Phrase: **"Enforce finished in policy domain"**

Additional Criteria

Select Groups...

Save Cancel

Edit Custom Criteria Alarm Definition: sync Policy to mappings

Severity: Set from source

Enabled: ☒

Criteria Actions Other Options

Actions

Add Edit... Remove Test

Run Task [Workflow - XIQ-C Enforce]

Alarm Suppression

☐ Enable Alarm Action Limit

Max Count: 5

Reset Interval: 0 Never

Save Cancel

Edit Custom Criteria Alarm Definition: sync Policy to mappings

Severity: Set from source

Enabled: ☒

Criteria Actions Other Options

Clear Conditions

No Current Alarm (action only): ☒

Cleared by Alarms: ☐

Save Cancel

# 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

Policy VLAN Islands

VLANs

Service IDs

Island Topology

Policy VLAN Islands (PVI) allow Roles and Rules using VLAN containment Access Control to vary the VID (and Service ID) across the network based on the Island where a user connects to the network. This can allow the network to isolate resources, for instance putting traffic from visitors in a "Guest" PVI VLAN that uses a different VID for each campus of a company. Below, select a PVI VLAN to see the specific VIDs used for that VLAN in each island as well as the Role mappings assigned to that VLAN.

VLANs

Create...

EP-Printers

EP-User1

EP-User2

GSS-Guest

SS-User1

SS-User2

VLAN Settings

EP-User1 - VIDs

EP-User1 - General / Role Mappings

Edit...

| Island Name    | VID  |
|----------------|------|
| A002           | 18   |
| A003           | 18   |
| B202           | 18   |
| C402           | 18   |
| C403           | 18   |
| Default Island | None |

Policy VLAN Islands

VLANs

Service IDs

Island Topology

Policy VLAN Islands (PVI) allow Roles and Rules using VLAN containment Access Control to vary the VID (and Service ID) across the network based on the Island where a user connects to the network. This can allow the network to isolate resources, for instance putting traffic from visitors in a "Guest" PVI VLAN that uses a different VID for each campus of a company. Below, select a PVI Service ID to see the specific Service IDs used for each island.

Service IDs

Create...

EP-Printers

EP-User1

EP-User2

GSS-Guest

SS-User1

SS-User2

Service ID Settings

EP-User1 - Service IDs

Edit...

| Island Name    | Service ID |
|----------------|------------|
| A002           | 20018      |
| A003           | 30018      |
| B202           | 2020018    |
| C402           | 4020018    |
| C403           | 4030018    |
| Default Island | None       |



# Requirement - 2



Dashboard Policy Access Control End-Systems Reports

Open/Manage Domain(s) Global Domain Settings Tools

Domain: GSS-Domain

Roles/Services +

Class of Service +

VLANs +

Network Resources +

Devices/Port Groups -

Devices Port Groups

by IP

IP (4 devices)

- 10.1.133.x (1 device)
- 10.2.5.x (1 device)
- 10.81.133.x (1 device)
- 10.255.254.x (1 device)

| Stat... | Name        | IP Address   | Family                         | Device Type              | Firmware      |
|---------|-------------|--------------|--------------------------------|--------------------------|---------------|
| ●       | BAN-A002-10 | 10.1.133.10  | Universal Platform Switch E... | 4220-12P-4X-SwitchEngine | 33.4.1.15     |
| ●       | BAN-A003-10 | 10.2.5.10    | Universal Platform Switch E... | 4220-12P-4X-SwitchEngine | 33.4.1.15     |
| ●       | BAN-B202-10 | 10.81.133.10 | Universal Platform Switch E... | 4220-12P-4X-SwitchEngine | 33.4.1.15     |
| ●       | XIQ-C-1     | 10.255.254.7 | XIQ Controller                 | VE6120                   | 10.13.02.0005 |

- 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

Policy VLAN Islands

VLANs Service IDs Island Topology

Policy VLAN Islands (PVI) allow Roles and Rules using VLAN containment Access Control to vary the VID (and Service ID) across the network based on the Island where a user connects to the network. This can allow the network to isolate resources, for instance putting traffic from visitors in a "Guest" PVI VLAN that uses a different VID for each campus of a company. Below, select an Island to see the specific VID used for each defined PVI VLAN in that island as well as the devices assigned to that island.

Islands

Create...

A002

A003

B202

C402

C403

Default Island

Island Settings

Default Island - VLANs Default Island - Service IDs Default Island - Devices

Add Devices...

| Name    | Device Type    | Firmware Version          |
|---------|----------------|---------------------------|
| XIQ-C-1 | XIQ Controller | Extreme Networks Extre... |

## 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”)

ExtremeCloud IQ Controller

| 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

The screenshot displays the ExtremeCloud IQ Controller interface. On the left, a sidebar shows a map and a list of sites. The 'Sites' list includes A003, C402, B202, and A002, with A002 highlighted. The main panel shows the configuration for site A002, including Name (A002), Country (Japan), and Timezone (Japan: Asia/Tokyo). Below this, there are tabs for DEVICE GROUPS, FLOOR PLANS, LOCATION, and ACCESS POINTS. The 'Edit Device Group' modal is open, showing the configuration for 'Okinawa-ap4020-dg'. The 'Profile' field is set to 'scjgss-4020-A002', which is highlighted with a red box. A red arrow points from this box to the 'Profile' column in the 'Device Groups' table below. The table has columns: Name, AP Platform, Profile, RF Management P..., Roles, Networks, and Devices. The row for 'Okinawa-ap4020-dg' shows AP Platform 'AP4020', Profile 'scjgss-4020-A002', RF Management P... 'scjgss-rf-mgmt', Roles '2', Networks '3', and Devices '1'. The 'Name' and 'Profile' fields in this row are also highlighted with red boxes.

| Name              | AP Platform | Profile          | RF Management P... | Roles | Networks | Devices |
|-------------------|-------------|------------------|--------------------|-------|----------|---------|
| Okinawa-ap4020-dg | AP4020      | scjgss-4020-A002 | scjgss-rf-mgmt     | 2     | 3        | 1       |

# Creating “Wireless Controller” rules



Dashboard Policy Access Control End-Systems Reports

Open/Manage Domain(s) Global Domain Settings Tools

Domain: GSS-Domain

Roles/Services

- TestRuleLudo
  - Allow DHCP
  - Allow DNS
  - Allow FQDN 1 [Wireless Controller]
  - Allow FQDN 2 [Wireless Controller]
  - Allow NAC [XIQ Controller]
  - Allow Src [Wireless Controller]
  - Redirect HTTP [Wireless Controller]
  - Redirect HTTPS [Wireless Controller]
- Threat Management

| Rule                                 | Summary   | Rule Order (ACL/REST) | Access Control | Service ID | Class of Service |
|--------------------------------------|---|-----------------------|----------------|------------|------------------|
| Allow DHCP                           | [UDP Dst : BootP Server] -> [Permit Traffic]            | 0                     | Permit Traffic | None       | None             |
| Allow DNS                            | [UDP Dst : DNS] -> [Permit Traffic]                     | 1                     | Permit Traffic | None       | None             |
| Allow NAC [XIQ Controller]           | [IPDST : 10.255.254.2/32] -> [Permit Traffic]           | 2                     | Permit Traffic | None       | None             |
| Allow Src [Wireless Controller]      | [IPSRC : 0.0.0.0/32] -> [Deny Traffic]                  | 3                     | Deny Traffic   | None       | None             |
| Allow FQDN 1 [Wireless Controller]   | [App : login.microsoftonline.com (User-Defined L3H) ... | 4                     | Permit Traffic | None       | None             |
| Allow FQDN 2 [Wireless Controller]   | [App : login.live.com (User-Defined L3H) [Group: We...  | 5                     | Permit Traffic | None       | None             |
| Redirect HTTP [Wireless Controller]  | [TCP Dst : HTTP] -> [HTTP Grp 1]                        | 6                     | None           | None       | None             |
| Redirect HTTPS [Wireless Controller] | [TCP Dst : HTTPS] -> [HTTP Grp 1]                       | 7                     | None           | None       | None             |

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



Dashboard Policy Access Control End-Systems Reports

Open/Manage Domain(s) Global Domain Settings Tools

Domain: GSS-Domain

Roles/Services

- EP-User2
- Enterprise Access
- Enterprise User
- Failsafe
- Guest Access
- Notification
- Printer
- Quarantine
- SS-User1
- SS-User2
- Server
- TestLudo**

Class of Service +

VLANs +

Network Resources +

Devices/Port Groups ! +

Enforce Auto Collapse Panel

Role: TestLudo

General VLAN Egress Mappings Port Default Usage

Name: TestLudo

Description:

TCI Overwrite: Disabled

Default Actions - AC:Permit Traffic

Services

Add/Remove Show Details

| Name ↑   | Also Used By Roles |
|--|--------------------|
| TestRuleLudo   |                    |
| <b>Rules:</b>  |                    |
| • Allow DHCP [IP UDP Port Destination(BootP Server) / AC:Permit Traffic]   |                    |
| • Allow DNS [IP UDP Port Destination(DNS) / AC:Permit Traffic]   |                    |
| • Allow FQDN 1 [Wireless Controller] [Application(login.microsoftonline.com (User-Defined L3H) [Group: Web Applications]) / AC:Permit Traffic] |                    |
| • Allow FQDN 2 [Wireless Controller] [Application(login.live.com (User-Defined L3H) [Group: Web Applications]) / AC:Permit Traffic]            |                    |
| • Allow NAC [XIQ Controller] [IP Address Destination(10.255.254.2/32) / AC:Permit Traffic]   |                    |
| • Allow Src [Wireless Controller] [IP Address Source(0.0.0.0/32) / AC:Deny Traffic]  |                    |
| • Redirect HTTP [Wireless Controller] [IP TCP Port Destination(HTTP) / HTTP Grp 1]   |                    |
| • Redirect HTTPS [Wireless Controller] [IP TCP Port Destination(HTTPS) / HTTP Grp 1]   |                    |

# Enforce Policy Domain



Network

Alarms & Events

Control

Analytics

Wireless

Reports

Tasks

Administration

Connect

Dashboard

Policy

Access Control

End-Systems

Reports

Open/Manage Domain(s)

Global Domain Settings

Tools

Domain: GSS-Domain

Roles/Services

Class of Service

VLANs

Network Resources

Devices/Port Groups

Devices

Port Groups

by IP

IP (4 devices)

10.1.133.x (1 device)

10.2.5.x (1 device)

10.81.133.x (1 device)

10.255.254.x (1 device)

Devices

User Sessions

RADIUS Authentication

RADIUS Accounting

| Stat... | Name        | IP Address | Family | Device Type | Firmware |
|---------|-------------|------------|--------|-------------|----------|
| ●       | BAN-A002-10 |            |        |             |          |
| ●       | BAN-A003-10 |            |        |             |          |
| ●       | BAN-B202-10 |            |        |             |          |
| ●       | XIQC-1      |            |        |             |          |

Enforce Preview

Show all device types

Summit Series Primary

XIQ Controller

Device Stats & Info

Roles & Rules

Classes of Service

Supported Config Only

Unsupported Config Only

Collapse All

View/Edit

| Supported | Role Details | Info   |
|-----------|--------------|--|
| ●         | Access Point | { "defaultAction": "allow", "defaultCos": "", "name": "Access Poi... |

Enforcing Domain, please wait...

Outstanding Devices: 4 - Duration: 51 ms - PDUs Sent/Received: 0

Cancel

Enforce

Enforce domain data to 4 device(s)?

Yes

No

Success

Domain successfully enforced to device(s).

OK

Event Log

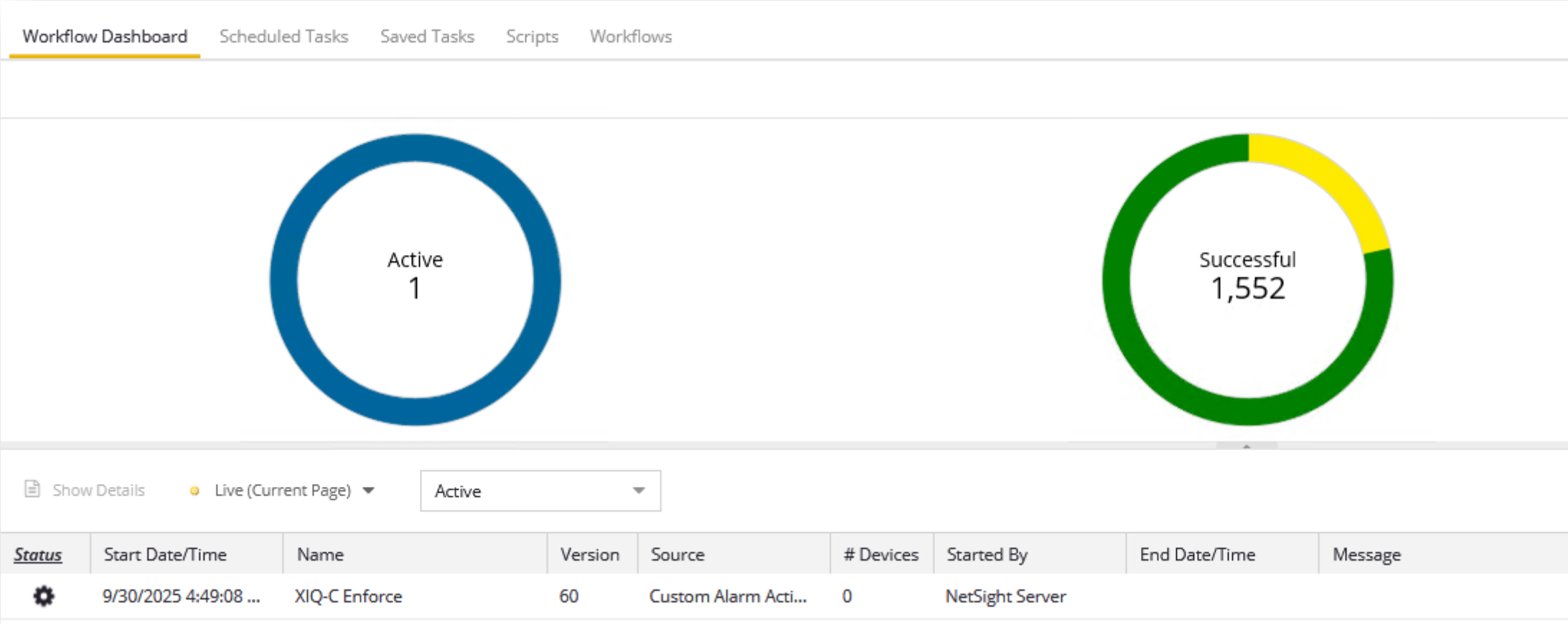
Show on enforce

Event Log

Enforce

Cancel

# Workflow automatically executes



# Workflow automatically executes



Workflow Dashboard

Scheduled Tasks

Saved Tasks

Scripts

Workflows

XIQ-C Enforce (1703)

Summary

| Status | Start Date/Time       | Name          | Version | Source               | # Devices | Started By      | End Date/Time         | Message  | Path                     |
|--------|-----------------------|---------------|---------|----------------------|-----------|-----------------|-----------------------|--|--------------------------|
| ✓      | 9/30/2025 4:49:08 ... | XIQ-C Enforce | 60      | Custom Alarm Acti... | 0         | NetSight Server | 9/30/2025 4:49:21 ... | Enforced Policy VLAN Islands to XIQ-C Contr... | /Workflows/XIQ-C Enforce |

Graph View

Table View

Stop Workflow

Show Output

Show Variables

Devices Grid

Show Output

| Status  | Device IP | Output Path | Start Date/Time  | End Date/Time    | Message |
|---------|-----------|-------------|------------------|------------------|---------|
| SUCCESS |           |             | 9/30/2025 4:4... | 9/30/2025 4:4... |         |

Output

```
Script Name: XIQ-C Enforce_
Extract_Policy_Data
Date and Time: 2025-09-30T04:49:08.877
XIQ-SE User: NetSight Server
XIQ-SE User Domain:
IP:
Debug logging to file: /dev/shm/.Workflows_XIQ-C-Enforce.1703/Extract-Policy-Data.log
Workflow version 58 on XIQ-SE/XMC version 25.08.10.50
Activity: ExtractPolicyData_01 version 1.00
Input Data:
- Policy DomainPolicy Domain input selection = auto detect
- Manual Policy Domain =
Auto-detected Policy Domain 'GSS-Domain'
Extracted VLAN Island data from Policy Domain 'GSS-Domain'
Removing Island topology 'Default Island' because role 'SS-User1' has no VLAN binding set
Processed which Policy Roles qualify by having same VLAN-id but different I-SID across all Islands: SS-User1, SS-User2, EP-Printers, EP-User2, EP-User1
Extracted all Policy Services in use by Policy roles: TestRuleLudo, Active Directory Services, Application Provisioning - Access Control, Base Services, NIS Services, Redirect Web Services, Assessment Services, deny EP Server 20, deny EP-Server 10, Application Provisioning - Basic, Deny Spoofing and Other Administrative Protocols, Deny Unsupported Protocol Access, Threat Management, Printing Services
Extracted all Rules from above Policy Services
Processed which Policy Roles have ACL Rules marked for 'Wireless Controller': TestLudo
Extracted XIQ-C devices located in Policy Domain 'GSS-Domain' default VLAN Island: 10.255.254.7
```

Close



# 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...

ExtremeCloud IQ Controller

Roles  ☐ Exact match

| Name              | Default Action | Default VLAN             |
|-------------------|----------------|--------------------------|
| Enterprise User   | allow          |                          |
| Quarantine        | deny           |                          |
| Unregistered      | deny           |                          |
| Guest Access      | allow          | GSS_Guest [NSI_12991127] |
| Deny Access       | deny           |                          |
| Assessing         | deny           |                          |
| Failsafe          | allow          |                          |
| Administrator     | allow          |                          |
| EP-User2          | allow          |                          |
| EP-User1          | allow          |                          |
| SS-User2          | allow          |                          |
| SS-User1          | allow          |                          |
| Server            | allow          |                          |
| Access Point      | allow          |                          |
| Printer           | allow          |                          |
| Notification      | allow          |                          |
| Enterprise Access | allow          |                          |
| VoIP Phone        | allow          |                          |

ExtremeCloud IQ Controller

VLANs  ☐ Exact match

| Name                     | Mode          | Tagged | VLAN ID | I-SID    |
|--------------------------|---------------|--------|---------|----------|
| Bridged at AP untagged   | Bridged@AP    |        | 1       |          |
| GSS_Guest [NSI_12991127] | Fabric Attach | ✓      | 1127    | 12991127 |
| A003_SS-User1            | Fabric Attach | ✓      | 34      | 30034    |
| A003_SS-User2            | Fabric Attach | ✓      | 35      | 30035    |
| A003_EP-Printers         | Fabric Attach | ✓      | 17      | 30017    |
| A003_EP-User2            | Fabric Attach | ✓      | 19      | 30019    |
| A003_EP-User1            | Fabric Attach | ✓      | 18      | 30018    |
| C402_SS-User1            | Fabric Attach | ✓      | 34      | 4020034  |
| C402_SS-User2            | Fabric Attach | ✓      | 35      | 4020035  |
| C402_EP-Printers         | Fabric Attach | ✓      | 17      | 4020017  |
| C402_EP-User2            | Fabric Attach | ✓      | 19      | 4020019  |
| C402_EP-User1            | Fabric Attach | ✓      | 18      | 4020018  |
| B202_SS-User1            | Fabric Attach | ✓      | 34      | 2020034  |
| B202_SS-User2            | Fabric Attach | ✓      | 35      | 2020035  |
| B202_EP-Printers         | Fabric Attach | ✓      | 17      | 2020017  |
| B202_EP-User2            | Fabric Attach | ✓      | 19      | 2020019  |
| B202_EP-User1            | Fabric Attach | ✓      | 18      | 2020018  |
| A002_SS-User1            | Fabric Attach | ✓      | 34      | 20034    |
| A002_SS-User2            | Fabric Attach | ✓      | 35      | 20035    |
| A002_EP-Printers         | Fabric Attach | ✓      | 17      | 20017    |
| A002_EP-User2            | Fabric Attach | ✓      | 19      | 20019    |
| A002_EP-User1            | Fabric Attach | ✓      | 18      | 20018    |

Total Items: 22

# What workflow did - 2

**ExtremeCloud IQ Controller**

**Edit Device Group**

Name: Okinawa-ap4020-dg

Profile: scjgss-4020-A002

RF Management: scjgss-rf-mgmt

**Sites**

| Status | Name |
|--------|------|
| ●      | A003 |
| ●      | C402 |
| ●      | B202 |
| ●      | A002 |

**DEVELOPER GROUPS**

Name: A002

Country: Japan

Timezone: Japan: Asia/Tokyo

**Device Groups**

| Name              | AP Platform | Profile          | RF Management P... | Roles | Networks | Devices |
|-------------------|-------------|------------------|--------------------|-------|----------|---------|
| Okinawa-ap4020-dg | AP4020      | scjgss-4020-A002 | scjgss-rf-mgmt     | 2     | 3        | 1       |

**Edit Profile**

Name: scjgss-4020-A002

AP Platform: AP4020

**ADVANCED**

**VLANs**

| Name                     | Referenced                          | Additional                          |
|--------------------------|-------------------------------------|-------------------------------------|
| A002_EP-Printers         | <input type="checkbox"/>            | <input checked="" type="checkbox"/> |
| A002_EP-User1            | <input type="checkbox"/>            | <input checked="" type="checkbox"/> |
| A002_EP-User2            | <input type="checkbox"/>            | <input checked="" type="checkbox"/> |
| A002_SS-User1            | <input type="checkbox"/>            | <input checked="" type="checkbox"/> |
| A002_SS-User2            | <input type="checkbox"/>            | <input checked="" type="checkbox"/> |
| GSS_Guest [NSI_12991127] | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| A003_EP-Printers         | <input type="checkbox"/>            | <input type="checkbox"/>            |
| A003_EP-User1            | <input type="checkbox"/>            | <input type="checkbox"/>            |

- 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

ExtremeCloud IQ Controller

**Edit Device Group**

Name: Okinawa-ap4020-dg

Profile: scjgss-4020-A002

RF Management: scjgss-rf-mgmt

**Sites**

| Status | Name |
|--------|------|
| ●      | A003 |
| ●      | C402 |
| ●      | B202 |
| ●      | A002 |

**DEVICE GROUPS**

| Name              | AP Platform | Profile |
|-------------------|-------------|---------|
| Okinawa-ap4020-dg | AP4020      | scjgss  |

Edit Profile

Name

scjgss-4020-A002

AP Platform

AP4020

ADVANCED

RADIOS

NETWORKS

ROLES

VLANs

AIR DEFENSE

IOT

WIRED PORTS

ESL

POSITIONING

ANALYTICS

RTLs

Name

Selected

EP-User1

☒

EP-User2

☒

Enterprise User

☒

Guest Access

☒

SS-User1

☒

SS-User2

☒

Access Point

☐

Administrator

☐

CLOSE

Save

| Name              | AP Platform | Profile          | RF Management P... | Roles | Networks | Devices |
|-------------------|-------------|------------------|--------------------|-------|----------|---------|
| Okinawa-ap4020-dg | AP4020      | scjgss-4020-A002 | scjgss-rf-mgmt     | 2     | 3        | 1       |

- ©2021 EXTREME NETWORKS, INC. ALL RIGHTS RESERVED. 19

# What workflow did - 4



The screenshot displays the Extreme Networks configuration interface. The left sidebar shows the navigation menu with 'Control' selected. The main area shows the 'Access Control' configuration page. The 'Policy Mappings' section is expanded, and the 'Default' mapping is selected. The 'Edit Policy Mapping' dialog is open, showing the 'VLAN [ID] Name' field set to '[18] EP-User1'.

| Name                                | Policy Role    | Location | VLAN Name        |
|-------------------------------------|----------------|----------|------------------|
| Access Point                        | Access Point   | Any      | None             |
| Administrator                       | Administra...  | Any      | None             |
| Assessing                           | Assessing      | Any      | None             |
| Branch1_printer                     | Branch1_pr...  | Any      | None             |
| Deny Access                         | Deny Access    | Any      | None             |
| Enterprise Access                   | Enterprise ... | Any      | None             |
| Enterprise User                     | Enterprise ... | Any      | None             |
| Enterprise User (Administrator)     | Enterprise ... | Any      | None             |
| Enterprise User (Read-Only Manag... | Enterprise ... | Any      | None             |
| EP-Guest1                           | EP-Guest1      | Any      | None             |
| EP-User1                            | EP-User1       | Any      | [18] EP-User1    |
| EP-User2                            | EP-User2       | Any      | [19] EP-User2    |
| EP-Users1                           | EP-Users1      | Any      | None             |
| EP-Users2                           | EP-Users2      | Any      | None             |
| Failsafe                            | Failsafe       | Any      | None             |
| Guest Access                        | Guest Access   | Any      | [1127] GSS_Guest |

**Edit Policy Mapping**

Name: EP-User1

Map to Location: Any

Policy Role: EP-User1

VLAN [ID] Name: [18] EP-User1

VLAN Egress: Untagged U

Filter:

Port Profile:

Virtual Router:

Login-LAT-Group:

Login-LAT-Port:

Custom 1:

Custom 2:

Custom 3:

Custom 4:

Preview with RADIUS Attributes Save Apply Cancel

- 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

ExtremeCloud IQ Controller

Name: TestLudo

Bandwidth Limit: ☒ Unlimited Class of Service: No CoS

Default Action: Allow VLAN ID: Use default VLAN of Network

Associated Profiles: Role is not associated with any Profiles

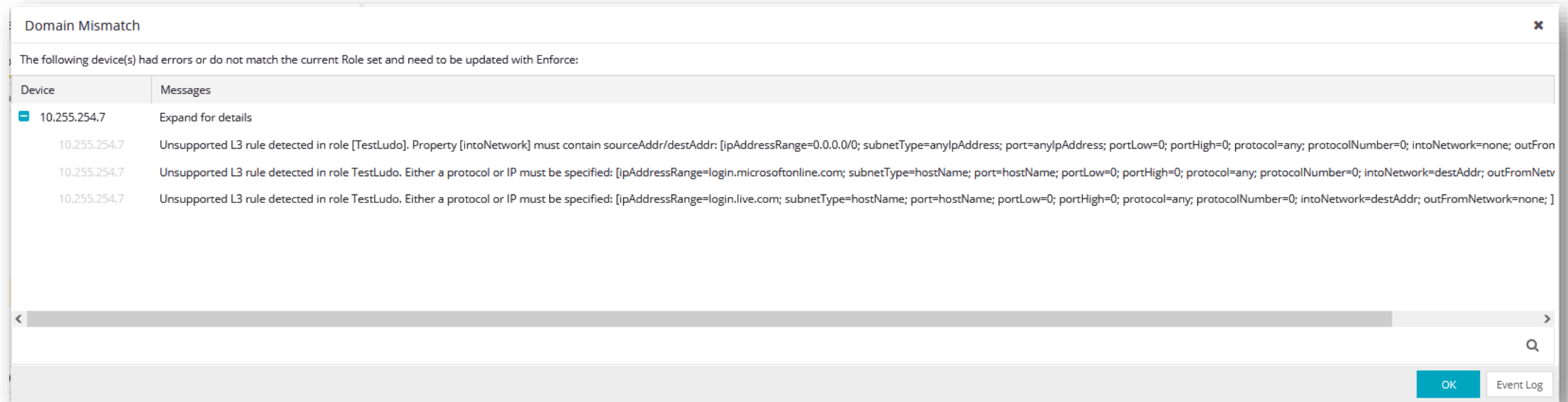
L2 (Mac Address) Rules (0 Rules)

L3,L4 Rules (IP and Port) Rules (8 Rules)

| Order | Name           | Action  |
|-------|----------------|---|
| 1     | Allow_DHCP     | Allow traffic, Class of Service No CoS, to any subnet, protocol UDP, port 67              |
| 2     | Allow_DNS      | Allow traffic, Class of Service No CoS, to any subnet, protocol UDP, port 53              |
| 3     | Allow_NAC      | Allow traffic, Class of Service No CoS, to subnet 10.255.254.2/32, any protocol, any port |
| 4     | Allow Src      | Allow traffic, to any subnet, any protocol, any port                                      |
| 5     | Allow FQDN 1   | Allow traffic, to FQDN login.microsoftonline.com, any protocol, any port                  |
| 6     | Allow FQDN 2   | Allow traffic, to FQDN login.live.com, any protocol, any port                             |
| 7     | Redirect HTTP  | Redirect traffic to the Redirect URL, to any subnet, protocol TCP, port 80                |
| 8     | Redirect HTTPS | Redirect traffic to the Redirect URL, to any subnet, protocol TCP, port 443               |

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

