Endpoint Tracking with XMC/XIQ-SE and VOSS

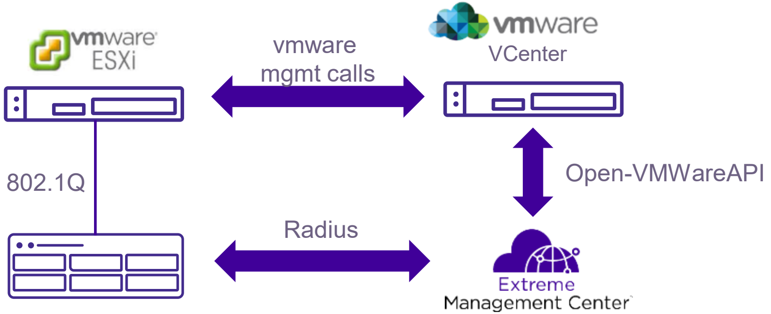
CTC Reading labs

Ludovico Stevens
Corporate Systems Engineering
March 2022

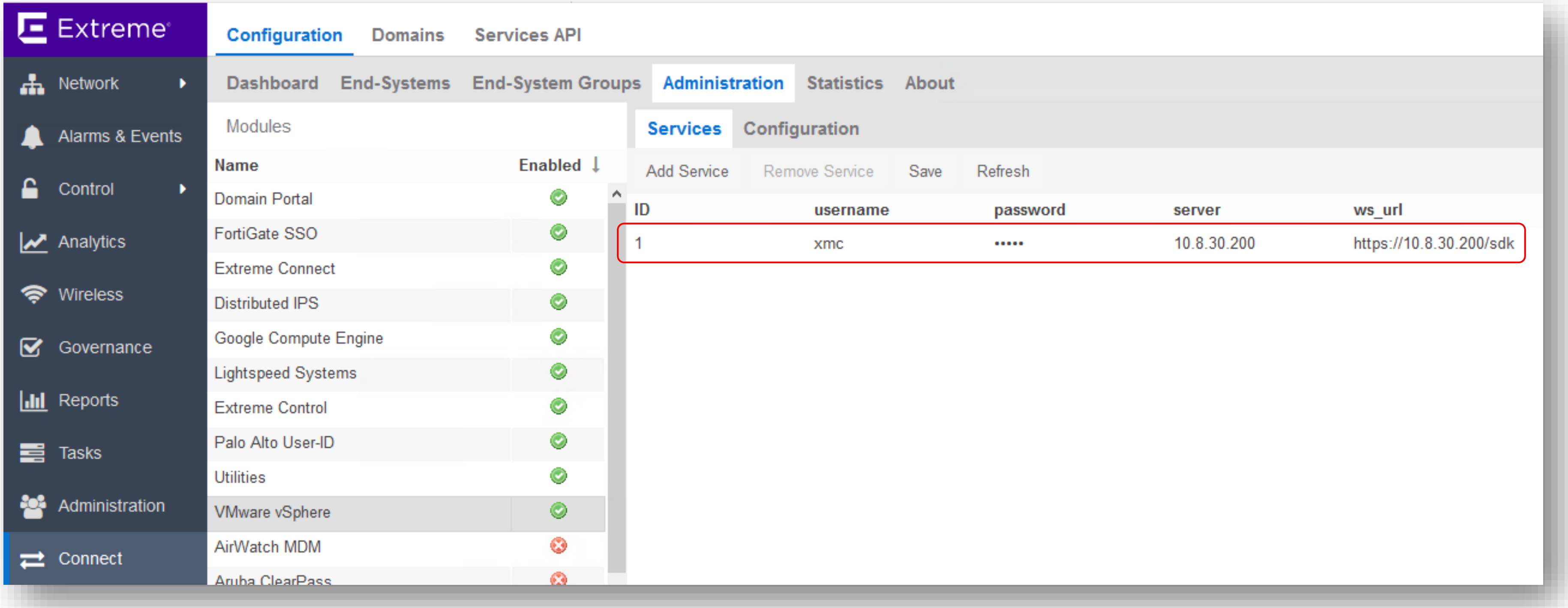
VM-Tracker/Automated End-point Tracking

Dynamic VM attachment Provisioning

- Capability to dynamically assign moving Virtual Machines (VMs) to correct IP Subnet (VLAN/ISID) at their destination location.
- ExtremeConnect API connector for VMWare ESXi and HyperV.
- Provisioning Flow:
  - VM “appears” on new switch port
  - Switch detects “new” VM and sends Radius Request to ExtremeControl/Connect.
  - ExtremeConnect checks with VCenter which PortGroup/VLAN/ISID device belongs to and sends Radius response back to switch with correct port configuration



XMC/XIQ-SE Connect – VCenter credentials

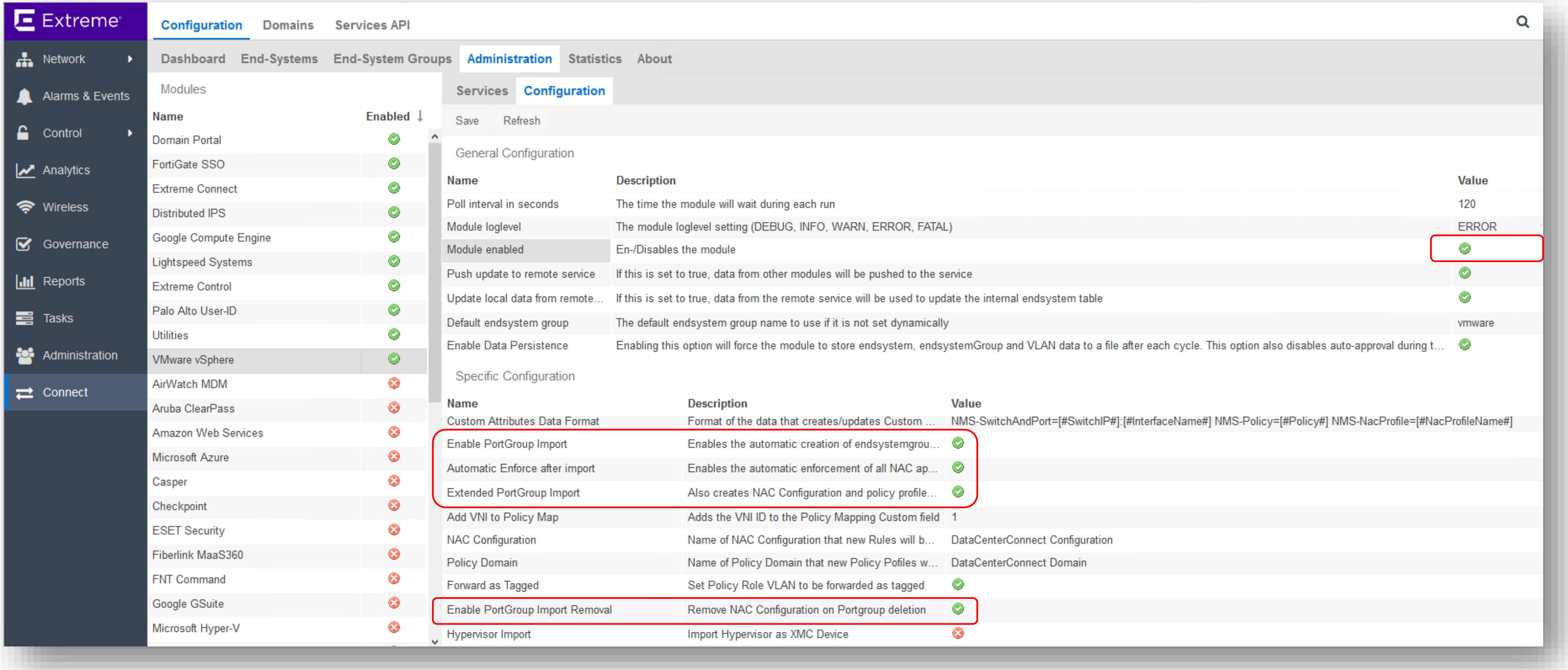


Name	Enabled
Domain Portal	✓
FortiGate SSO	✓
Extreme Connect	✓
Distributed IPS	✓
Google Compute Engine	✓
Lightspeed Systems	✓
Extreme Control	✓
Palo Alto User-ID	✓
Utilities	✓
VMware vSphere	✓
AirWatch MDM	✗
Aruba ClearPass	✗

ID	username	password	server	ws_url
1	xmc	•••••	10.8.30.200	https://10.8.30.200/sdk

- Provide credentials for XMC/XIQ-SE to connect to VCenter API

XMC/XIQ-SE Connect - Configuration



Modules

Name	Enabled
Domain Portal	✓
FortiGate SSO	✓
Extreme Connect	✓
Distributed IPS	✓
Google Compute Engine	✓
Lightspeed Systems	✓
Extreme Control	✓
Palo Alto User-ID	✓
Utilities	✓
VMware vSphere	✓
AirWatch MDM	✗
Aruba ClearPass	✗
Amazon Web Services	✗
Microsoft Azure	✗
Casper	✗
Checkpoint	✗
ESET Security	✗
Fiberlink MaaS360	✗
FNT Command	✗
Google GSuite	✗
Microsoft Hyper-V	✗

General Configuration

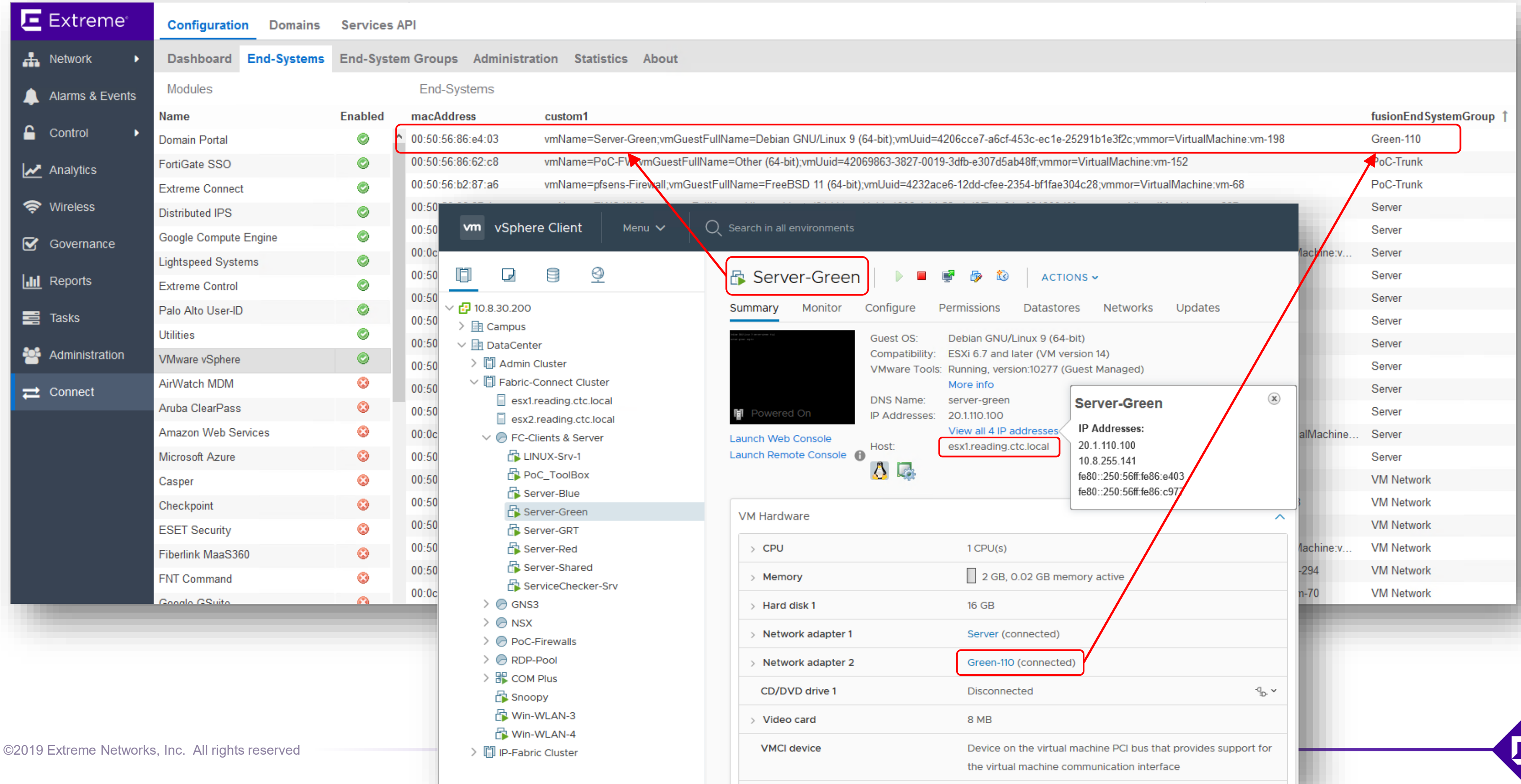
Name	Description	Value
Poll interval in seconds	The time the module will wait during each run	120
Module loglevel	The module loglevel setting (DEBUG, INFO, WARN, ERROR, FATAL)	ERROR
Module enabled	En-/Disables the module	✓
Push update to remote service	If this is set to true, data from other modules will be pushed to the service	✓
Update local data from remote…	If this is set to true, data from the remote service will be used to update the internal endsystem table	✓
Default endsystem group	The default endsystem group name to use if it is not set dynamically	vmware
Enable Data Persistence	Enabling this option will force the module to store endsystem, endsystemGroup and VLAN data to a file after each cycle. This option also disables auto-approval during t…	✓

Specific Configuration

Name	Description	Value
Custom Attributes Data Format	Format of the data that creates/updates Custom …	NMS-SwitchAndPort=[#SwitchIP#]:[#InterfaceName#] NMS-Policy=[#Policy#] NMS-NacProfile=[#NacProfileName#]
Enable PortGroup Import	Enables the automatic creation of endsystemgrou…	✓
Automatic Enforce after import	Enables the automatic enforcement of all NAC ap…	✓
Extended PortGroup Import	Also creates NAC Configuration and policy profile…	✓
Add VNI to Policy Map	Adds the VNI ID to the Policy Mapping Custom field	1
NAC Configuration	Name of NAC Configuration that new Rules will b…	DataCenterConnect Configuration
Policy Domain	Name of Policy Domain that new Policy Pofiles w…	DataCenterConnect Domain
Forward as Tagged	Set Policy Role VLAN to be forwarded as tagged	✓
Enable PortGroup Import Removal	Remove NAC Configuration on Portgroup deletion	✓
Hypervisor Import	Import Hypervisor as XMC Device	✗

- Enable the module, and required options (there are many, scroll window)

XMC/XIQ-SE Connect – VM MACs and info extracted from VCenter



Modules

Name	Enabled
Domain Portal	✓
FortiGate SSO	✓
Extreme Connect	✓
Distributed IPS	✓
Google Compute Engine	✓
Lightspeed Systems	✓
Extreme Control	✓
Palo Alto User-ID	✓
Utilities	✓
VMware vSphere	✓
AirWatch MDM	✗
Aruba ClearPass	✗
Amazon Web Services	✗
Microsoft Azure	✗
Casper	✗
Checkpoint	✗
ESET Security	✗
Fiberlink MaaS360	✗
FNT Command	✗
Google GSuite	✗

End-Systems

macAddress	custom1	fusionEndSystemGroup
00:50:56:86:e4:03	vmName=Server-Green;vmGuestFullName=Debian GNU/Linux 9 (64-bit);vmUuid=4206cce7-a6cf-453c-ec1e-25291b1e3f2c;vmmor=VirtualMachine:vm-198	Green-110
00:50:56:86:62:c8	vmName=PoC-FW;vmGuestFullName=Other (64-bit);vmUuid=42069863-3827-0019-3dfb-e307d5ab48ff;vmmor=VirtualMachine:vm-152	PoC-Trunk
00:50:56:b2:87:a6	vmName=pfsens-Firewall;vmGuestFullName=FreeBSD 11 (64-bit);vmUuid=4232ace6-12dd-cfee-2354-bf1fae304c28;vmmor=VirtualMachine:vm-68	PoC-Trunk
00:50		Server
00:50		Server
00:0c	lachine:v...	Server
00:50		Server
00:50		Server
00:50		Server
00:50		Server
00:50		Server
00:50		Server
00:50		Server
00:0c	alMachine...	Server
00:50		Server
00:50		VM Network
00:50	3	VM Network
00:50		VM Network
00:50	lachine:v...	VM Network
00:50	-294	VM Network
00:0c	n-70	VM Network

- 10.8.30.200
  - Campus
  - DataCenter
    - Admin Cluster
    - Fabric-Connect Cluster
      - esx1.reading.ctc.local
      - esx2.reading.ctc.local
      - FC-Clients & Server
        - LINUX-Srv-1
        - PoC_ToolBox
        - Server-Blue
        - Server-Green
        - Server-GRT
        - Server-Red
        - Server-Shared
        - ServiceChecker-Srv
      - GNS3
      - NSX
      - PoC-Firewalls
      - RDP-Pool
      - COM Plus
      - Snoopy
      - Win-WLAN-3
      - Win-WLAN-4
    - IP-Fabric Cluster

Server-Green

Guest OS: Debian GNU/Linux 9 (64-bit)
Compatibility: ESXi 6.7 and later (VM version 14)
VMware Tools: Running, version:10277 (Guest Managed)
More info
DNS Name: server-green
IP Addresses: 20.1.110.100
View all 4 IP addresses
Host: esx1.reading.ctc.local

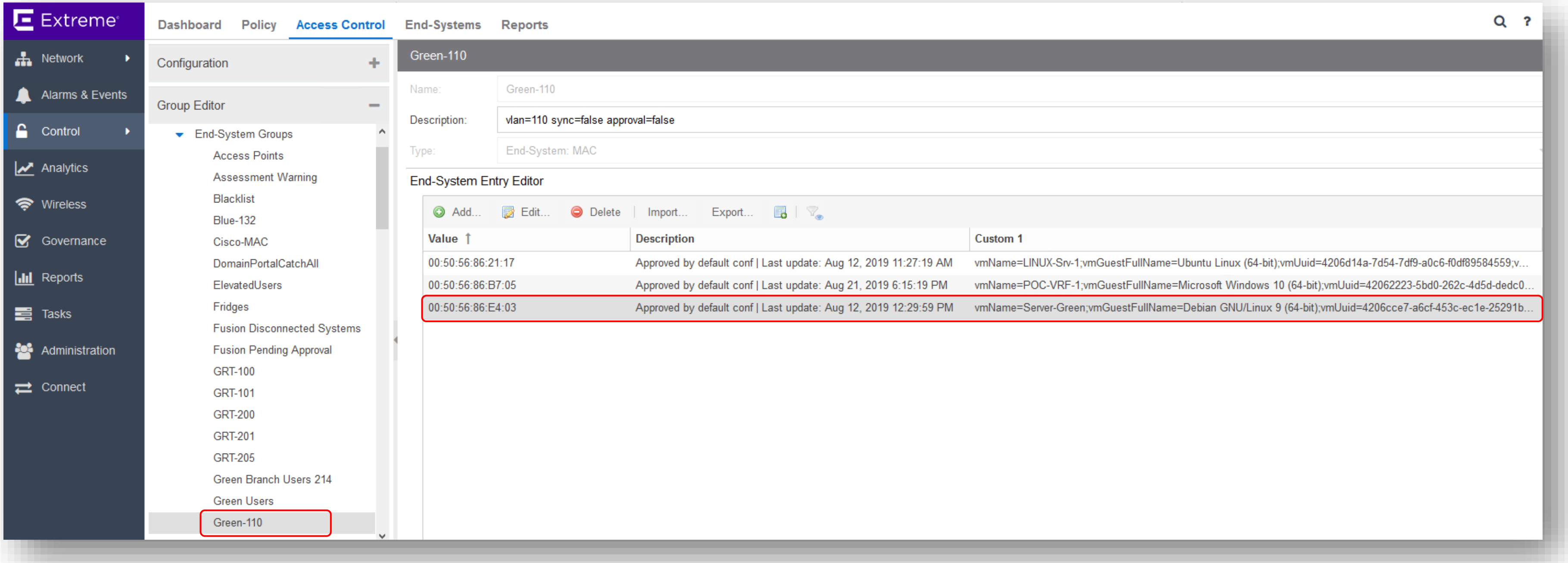
Server-Green

IP Addresses:
20.1.110.100
10.8.255.141
fe80::250:56ff:fe86:e403
fe80::250:56ff:fe86:c977

VM Hardware

CPU	1 CPU(s)
Memory	2 GB, 0.02 GB memory active
Hard disk 1	16 GB
Network adapter 1	Server (connected)
Network adapter 2	Green-110 (connected)
CD/DVD drive 1	Disconnected
Video card	8 MB
VMCI device	Device on the virtual machine PCI bus that provides support for the virtual machine communication interface

XMC/XIQ-SE Control – Automatically created End-System Group



Green-110

Name: Green-110

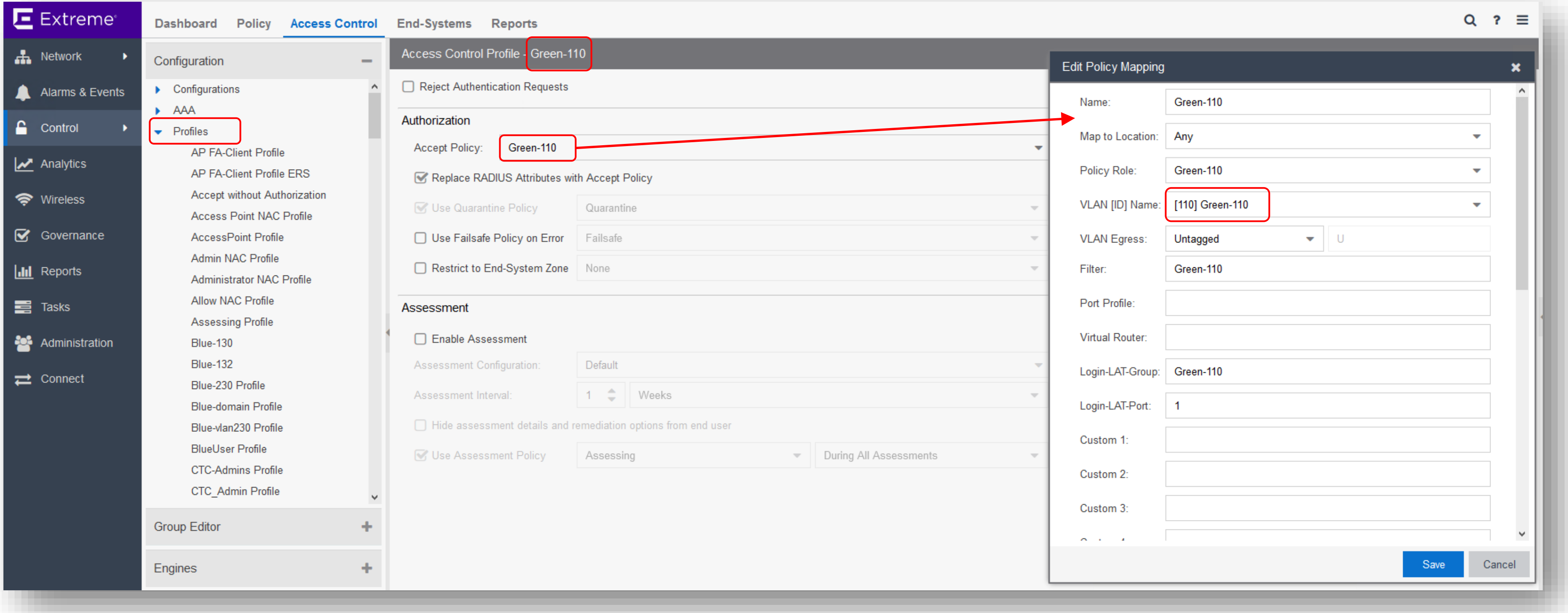
Description: vlan=110 sync=false approval=false

Type: End-System: MAC

Value	Description	Custom 1
00:50:56:86:21:17	Approved by default conf | Last update: Aug 12, 2019 11:27:19 AM	vmName=LINUX-Srv-1;vmGuestFullName=Ubuntu Linux (64-bit);vmUuid=4206d14a-7d54-7df9-a0c6-f0df89584559;v...
00:50:56:86:B7:05	Approved by default conf | Last update: Aug 21, 2019 6:15:19 PM	vmName=POC-VRF-1;vmGuestFullName=Microsoft Windows 10 (64-bit);vmUuid=42062223-5bd0-262c-4d5d-dedc0...
00:50:56:86:E4:03	Approved by default conf | Last update: Aug 12, 2019 12:29:59 PM	vmName=Server-Green;vmGuestFullName=Debian GNU/Linux 9 (64-bit);vmUuid=4206cce7-a6cf-453c-ec1e-25291b...

- End-System Groups are automatically created using the VmWare PortGroup Name and contain all the VM MACs which are connected to it
- Our Server-Green MAC is highlighted

XMC/XIQ-SE Control – Automatically created Access Control Profile



Access Control Profile - Green-110

☐ Reject Authentication Requests

Authorization

Accept Policy: Green-110

☑ Replace RADIUS Attributes with Accept Policy

☑ Use Quarantine Policy: Quarantine

☐ Use Failsafe Policy on Error: Failsafe

☐ Restrict to End-System Zone: None

Assessment

☐ Enable Assessment

Assessment Configuration: Default

Assessment Interval: 1 Weeks

☐ Hide assessment details and remediation options from end user

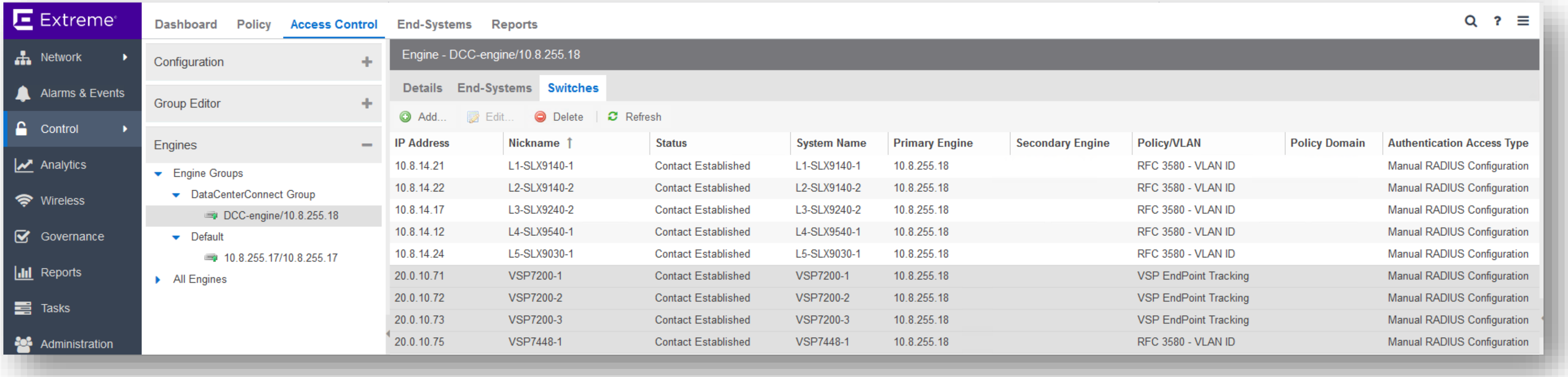
☑ Use Assessment Policy: Assessing, During All Assessments

Edit Policy Mapping

Name:	Green-110
Map to Location:	Any
Policy Role:	Green-110
VLAN [ID] Name:	[110] Green-110
VLAN Egress:	Untagged U
Filter:	Green-110
Port Profile:	
Virtual Router:	
Login-LAT-Group:	Green-110
Login-LAT-Port:	1
Custom 1:	
Custom 2:	
Custom 3:	

- Access Control Profiles are also automatically created using the VmWare PortGroup Name, and point to an equally named Accept Policy where the VLAN mapping is also automatically set by XMC/XIQ-SE Connect

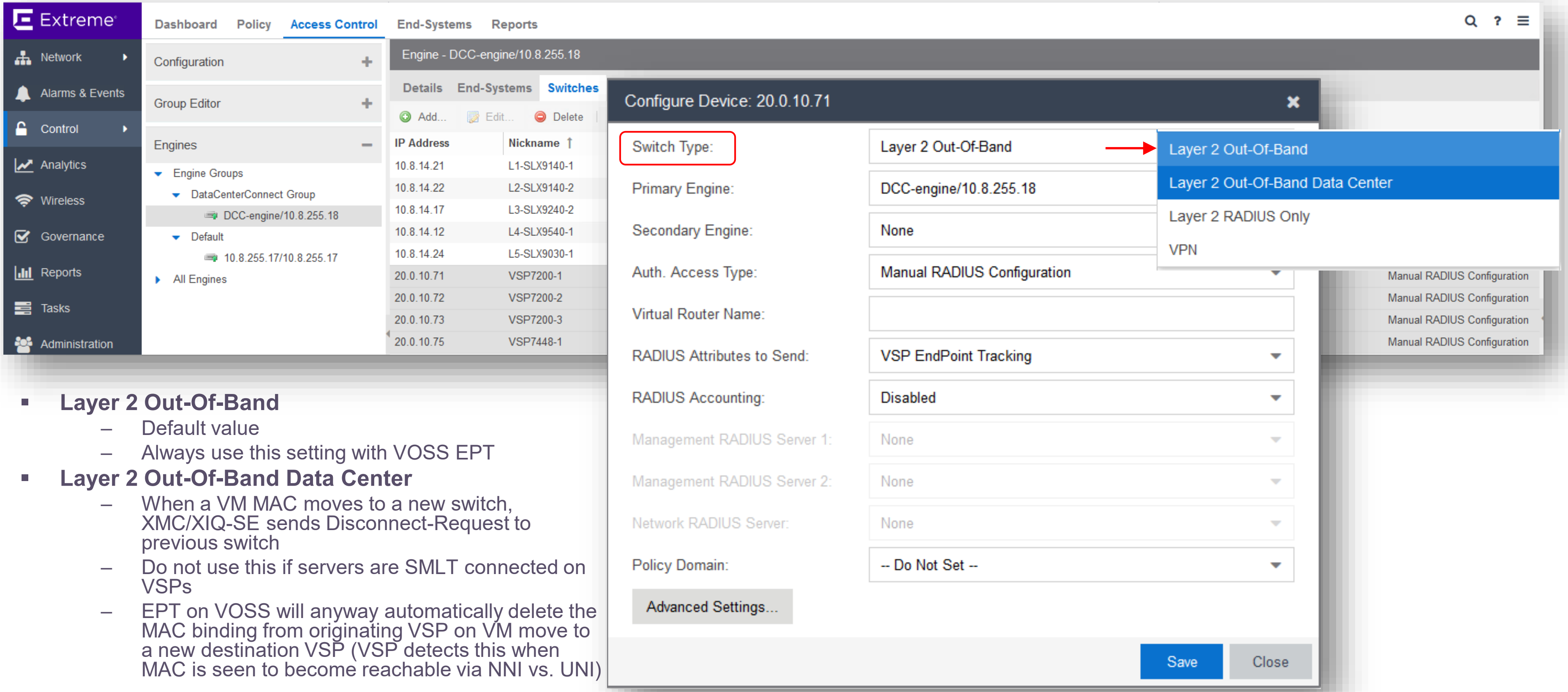
XMC/XIQ-SE Control – Add VSP switches to Access Control engine



IP Address	Nickname ↑	Status	System Name	Primary Engine	Secondary Engine	Policy/VLAN	Policy Domain	Authentication Access Type
10.8.14.21	L1-SLX9140-1	Contact Established	L1-SLX9140-1	10.8.255.18		RFC 3580 - VLAN ID		Manual RADIUS Configuration
10.8.14.22	L2-SLX9140-2	Contact Established	L2-SLX9140-2	10.8.255.18		RFC 3580 - VLAN ID		Manual RADIUS Configuration
10.8.14.17	L3-SLX9240-2	Contact Established	L3-SLX9240-2	10.8.255.18		RFC 3580 - VLAN ID		Manual RADIUS Configuration
10.8.14.12	L4-SLX9540-1	Contact Established	L4-SLX9540-1	10.8.255.18		RFC 3580 - VLAN ID		Manual RADIUS Configuration
10.8.14.24	L5-SLX9030-1	Contact Established	L5-SLX9030-1	10.8.255.18		RFC 3580 - VLAN ID		Manual RADIUS Configuration
20.0.10.71	VSP7200-1	Contact Established	VSP7200-1	10.8.255.18		VSP EndPoint Tracking		Manual RADIUS Configuration
20.0.10.72	VSP7200-2	Contact Established	VSP7200-2	10.8.255.18		VSP EndPoint Tracking		Manual RADIUS Configuration
20.0.10.73	VSP7200-3	Contact Established	VSP7200-3	10.8.255.18		VSP EndPoint Tracking		Manual RADIUS Configuration
20.0.10.75	VSP7448-1	Contact Established	VSP7448-1	10.8.255.18		RFC 3580 - VLAN ID		Manual RADIUS Configuration

- Add VSP switches to XMC/XIQ-SE Control engine
- In our CTC setup, XMC/XIQ-SE has two separate Control engines:
  - One for Campus Network Access Control
  - One for VM Endpoint-tracking in the Data Center

XMC/XIQ-SE Control – Add VSP switches to Access Control engine



Engine - DCC-engine/10.8.255.18

IP Address	Nickname
10.8.14.21	L1-SLX9140-1
10.8.14.22	L2-SLX9140-2
10.8.14.17	L3-SLX9240-2
10.8.14.12	L4-SLX9540-1
10.8.14.24	L5-SLX9030-1
20.0.10.71	VSP7200-1
20.0.10.72	VSP7200-2
20.0.10.73	VSP7200-3
20.0.10.75	VSP7448-1

Manual RADIUS Configuration
Manual RADIUS Configuration
Manual RADIUS Configuration
Manual RADIUS Configuration

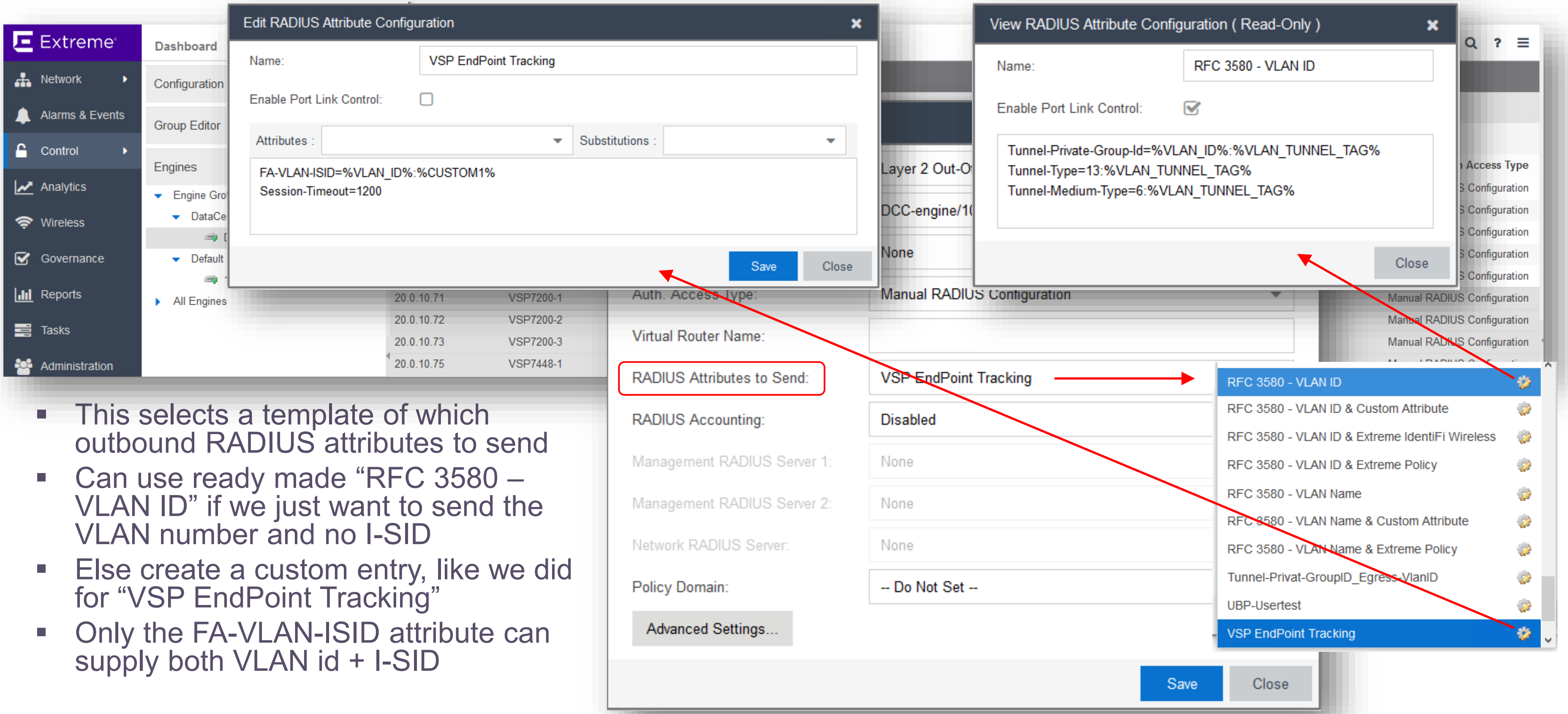
Configure Device: 20.0.10.71

Switch Type:	Layer 2 Out-Of-Band
Primary Engine:	DCC-engine/10.8.255.18
Secondary Engine:	None
Auth. Access Type:	Manual RADIUS Configuration
Virtual Router Name:	
RADIUS Attributes to Send:	VSP EndPoint Tracking
RADIUS Accounting:	Disabled
Management RADIUS Server 1:	None
Management RADIUS Server 2:	None
Network RADIUS Server:	None
Policy Domain:	-- Do Not Set --

Layer 2 Out-Of-Band
Layer 2 Out-Of-Band Data Center
Layer 2 RADIUS Only
VPN

- **Layer 2 Out-Of-Band**
  - Default value
  - Always use this setting with VOSS EPT
- **Layer 2 Out-Of-Band Data Center**
  - When a VM MAC moves to a new switch, XMC/XIQ-SE sends Disconnect-Request to previous switch
  - Do not use this if servers are SMLT connected on VSPs
  - EPT on VOSS will anyway automatically delete the MAC binding from originating VSP on VM move to a new destination VSP (VSP detects this when MAC is seen to become reachable via NNI vs. UNI)

XMC/XIQ-SE Control – Add VSP switches to Access Control engine



20.0.10.71	VSP7200-1
20.0.10.72	VSP7200-2
20.0.10.73	VSP7200-3
20.0.10.75	VSP7448-1

Edit RADIUS Attribute Configuration

Name: VSP EndPoint Tracking

Enable Port Link Control: ☐

Attributes : Substitutions :

```
FA-VLAN-ISID=%VLAN_ID%:%CUSTOM1%
Session-Timeout=1200
```

View RADIUS Attribute Configuration (Read-Only)

Name: RFC 3580 - VLAN ID

Enable Port Link Control: ☑

```
Tunnel-Private-Group-Id=%VLAN_ID%:%VLAN_TUNNEL_TAG%
Tunnel-Type=13:%VLAN_TUNNEL_TAG%
Tunnel-Medium-Type=6:%VLAN_TUNNEL_TAG%
```

Auth. Access Type: Manual RADIUS Configuration

Virtual Router Name:

RADIUS Attributes to Send: VSP EndPoint Tracking

RADIUS Accounting: Disabled

Management RADIUS Server 1: None

Management RADIUS Server 2: None

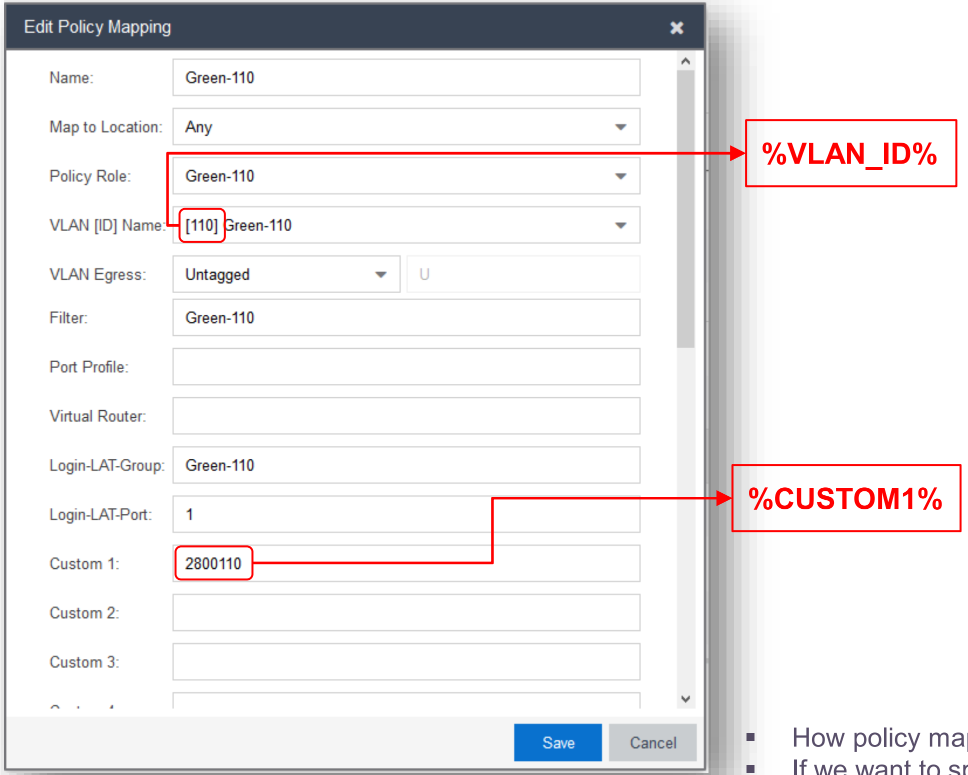
Network RADIUS Server: None

Policy Domain: -- Do Not Set --

Advanced Settings...
Save
Close
RFC 3580 - VLAN ID
RFC 3580 - VLAN ID & Custom Attribute
RFC 3580 - VLAN ID & Extreme IdentiFi Wireless
RFC 3580 - VLAN ID & Extreme Policy
RFC 3580 - VLAN Name
RFC 3580 - VLAN Name & Custom Attribute
RFC 3580 - VLAN Name & Extreme Policy
Tunnel-Privat-GroupID_Egress-VlanID
UBP-Usertest
VSP EndPoint Tracking

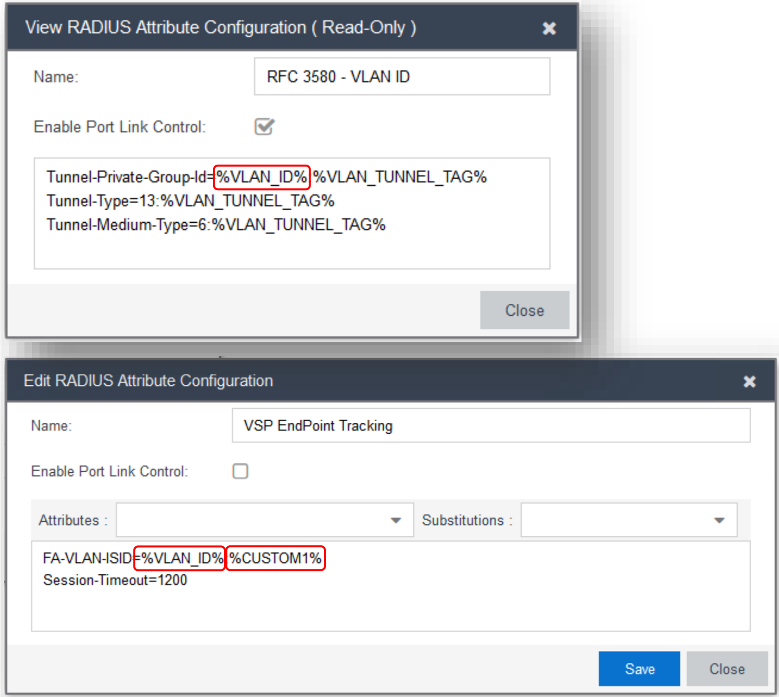
- This selects a template of which outbound RADIUS attributes to send
- Can use ready made “RFC 3580 – VLAN ID” if we just want to send the VLAN number and no I-SID
- Else create a custom entry, like we did for “VSP EndPoint Tracking”
- Only the FA-VLAN-ISID attribute can supply both VLAN id + I-SID

XMC/XIQ-SE Policy mappings to RADIUS templates



Edit Policy Mapping

Name:	Green-110
Map to Location:	Any
Policy Role:	Green-110
VLAN [ID] Name:	[110] Green-110
VLAN Egress:	Untagged
Filter:	Green-110
Port Profile:	
Virtual Router:	
Login-LAT-Group:	Green-110
Login-LAT-Port:	1
Custom 1:	2800110
Custom 2:	
Custom 3:	



View RADIUS Attribute Configuration (Read-Only)

Name: RFC 3580 - VLAN ID

Enable Port Link Control: ☑

```
Tunnel-Private-Group-Id=%VLAN_ID%:%VLAN_TUNNEL_TAG%
Tunnel-Type=13:%VLAN_TUNNEL_TAG%
Tunnel-Medium-Type=6:%VLAN_TUNNEL_TAG%
```

Edit RADIUS Attribute Configuration

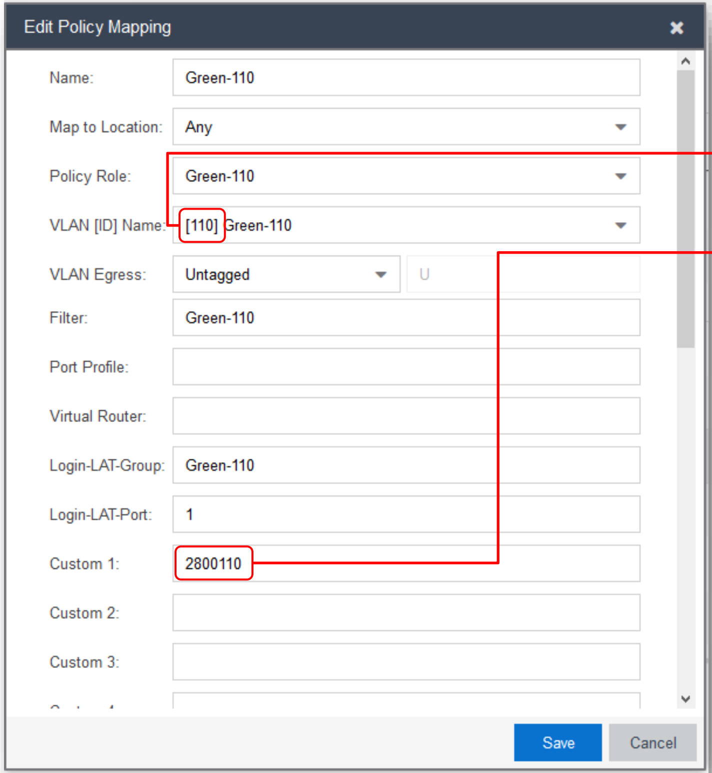
Name: VSP EndPoint Tracking

Enable Port Link Control: □

```
FA-VLAN-ISID=%VLAN_ID%:%CUSTOM1%
Session-Timeout=1200
```

- How policy mappings populated RADIUS attribute templates
- If we want to specify an I-SID we use the Custom1 field
- NOTE, to use FA-VLAN-ISID attribute with just VLAN-id, Custom1 field must be set to 0

XMC/XIQ-SE Policy mappings to RADIUS templates – cont.

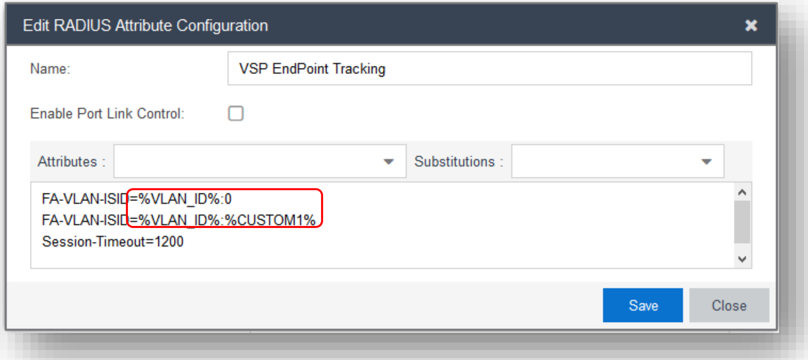


Edit Policy Mapping

Name:	Green-110
Map to Location:	Any
Policy Role:	Green-110
VLAN [ID] Name:	[110] Green-110
VLAN Egress:	Untagged U
Filter:	Green-110
Port Profile:	
Virtual Router:	
Login-LAT-Group:	Green-110
Login-LAT-Port:	1
Custom 1:	2800110
Custom 2:	
Custom 3:	

%VLAN_ID%

%CUSTOM1%



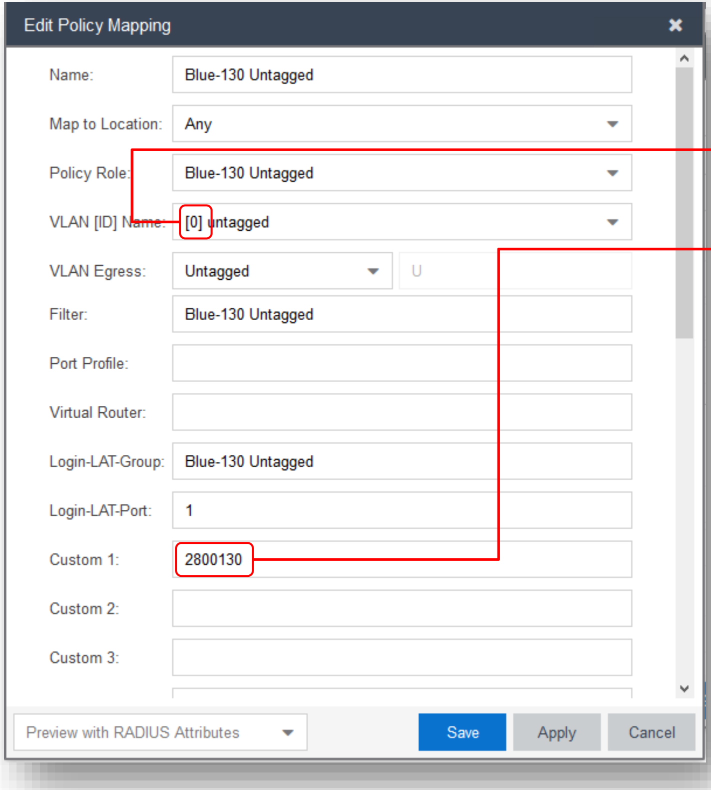
Edit RADIUS Attribute Configuration

Name:	VSP EndPoint Tracking
Enable Port Link Control:	☐
Attributes :	
Substitutions :	

```
FA-VLAN-ISID=%VLAN_ID%:0
FA-VLAN-ISID=%VLAN_ID%:%CUSTOM1%
Session-Timeout=1200
```

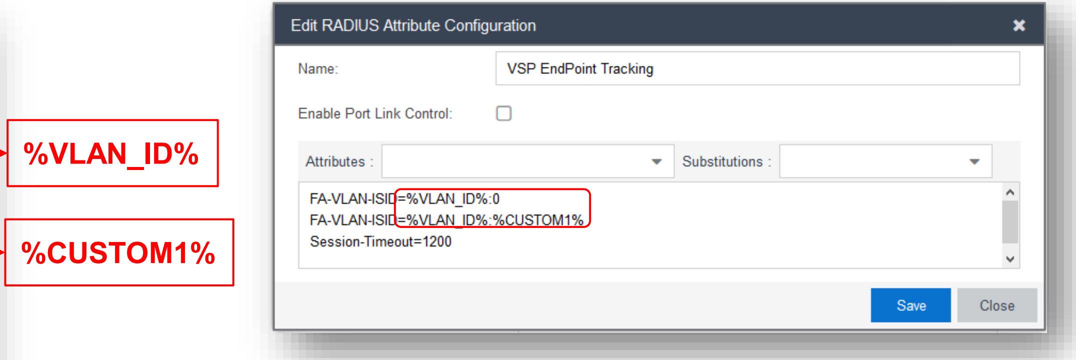
- Note that XMC/XIQ-SE Connect, when it auto generates the policies and policy mappings, the custom1 field remains by default empty
- If the custom1 field is empty, then %CUSTOM1% variable will be undefined and XMC/XIQ-SE will not return the FA-VLAN-ISID attribute at all
- Solution1: Edit the custom1 field of all policy mappings and set it to 0 (if using VSP auto-isid-offset) or set it to the desired I-SID otherwise; but this is painful if there are many server VLANs and we only want to set the I-SID for exceptions
- Solution2: Duplicate the FA-VLAN-ISID twice in the template, as shown above, the 1st timed with I-SID = 0 and the 2nd time with %CUSTOM1%. If the policy mapping has no value set in custom1 field, only the 1st FA-VLAN-ISID attribute will be sent (with a null I-SID) and the VSP auto-isid-offset will be used. If instead the policy mapping has a value, then both FA-VLAN-ISID attributes will be sent and the convention is that the device will only process the last occurrence of the attribute, which will include the I-SID custom1 value

XMC/XIQ-SE Policy mappings to RADIUS templates – Untagged binding



Edit Policy Mapping

Name:	Blue-130 Untagged
Map to Location:	Any
Policy Role:	Blue-130 Untagged
VLAN [ID] Name:	[0] untagged
VLAN Egress:	Untagged U
Filter:	Blue-130 Untagged
Port Profile:	
Virtual Router:	
Login-LAT-Group:	Blue-130 Untagged
Login-LAT-Port:	1
Custom 1:	2800130
Custom 2:	
Custom 3:	



%VLAN_ID%

%CUSTOM1%

Edit RADIUS Attribute Configuration

Name: VSP EndPoint Tracking

Enable Port Link Control: □

Attributes :

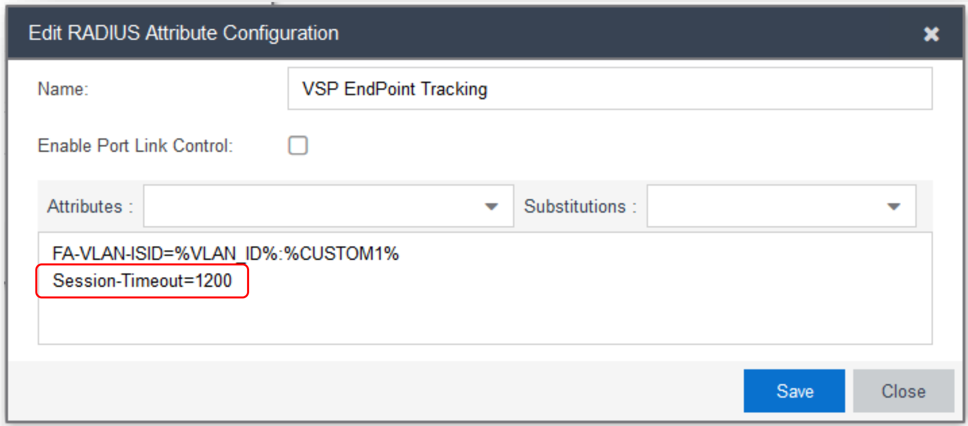
Substitutions :

```
FA-VLAN-ISID=%VLAN_ID%:0
FA-VLAN-ISID=%VLAN_ID%:%CUSTOM1%
Session-Timeout=1200
```

- To push an untagged binding for the MAC, we need to send the FA-VLAN-ISID attribute with a 0 VLAN-id and a valid I-SID
  - If you send 0:0 and auto-ISID-offset is enabled on the VSPs this will result in 0 being added to the ISID-offset which is probably not the I-SID you wanted for the untagged traffic
- Solution: Specify a VLAN ID of 0 in the Policy Mapping
  - Note that the VLAN Egress field is of no use here

RADIUS template – Session Timeout

- On VOSS EndPoint Tracking, when VM MACs age out from the FDB, a default 24 hours timer is used as timeout before removing the MAC from the endpoint bindings table.
- That 24 hours default timer is here overridden to 20 minutes



Edit RADIUS Attribute Configuration

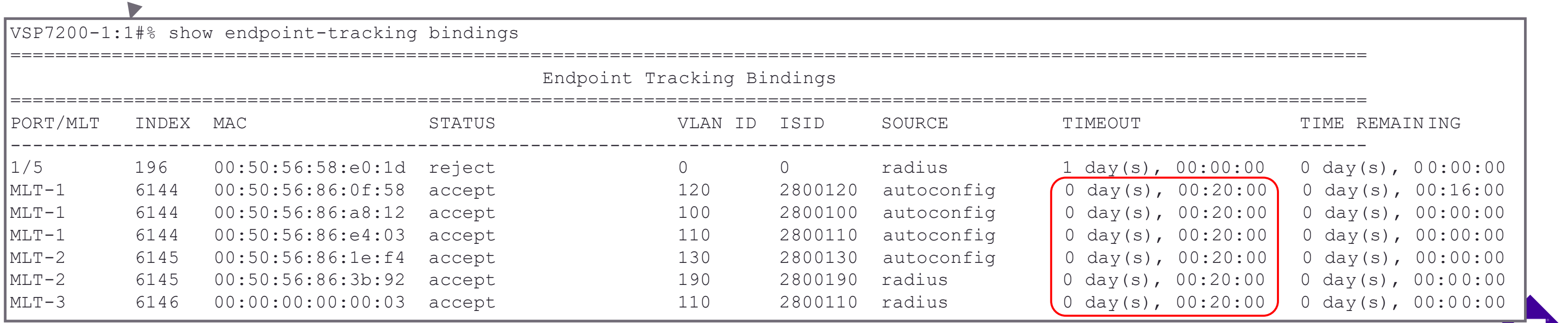
Name: VSP EndPoint Tracking

Enable Port Link Control: □

Attributes :

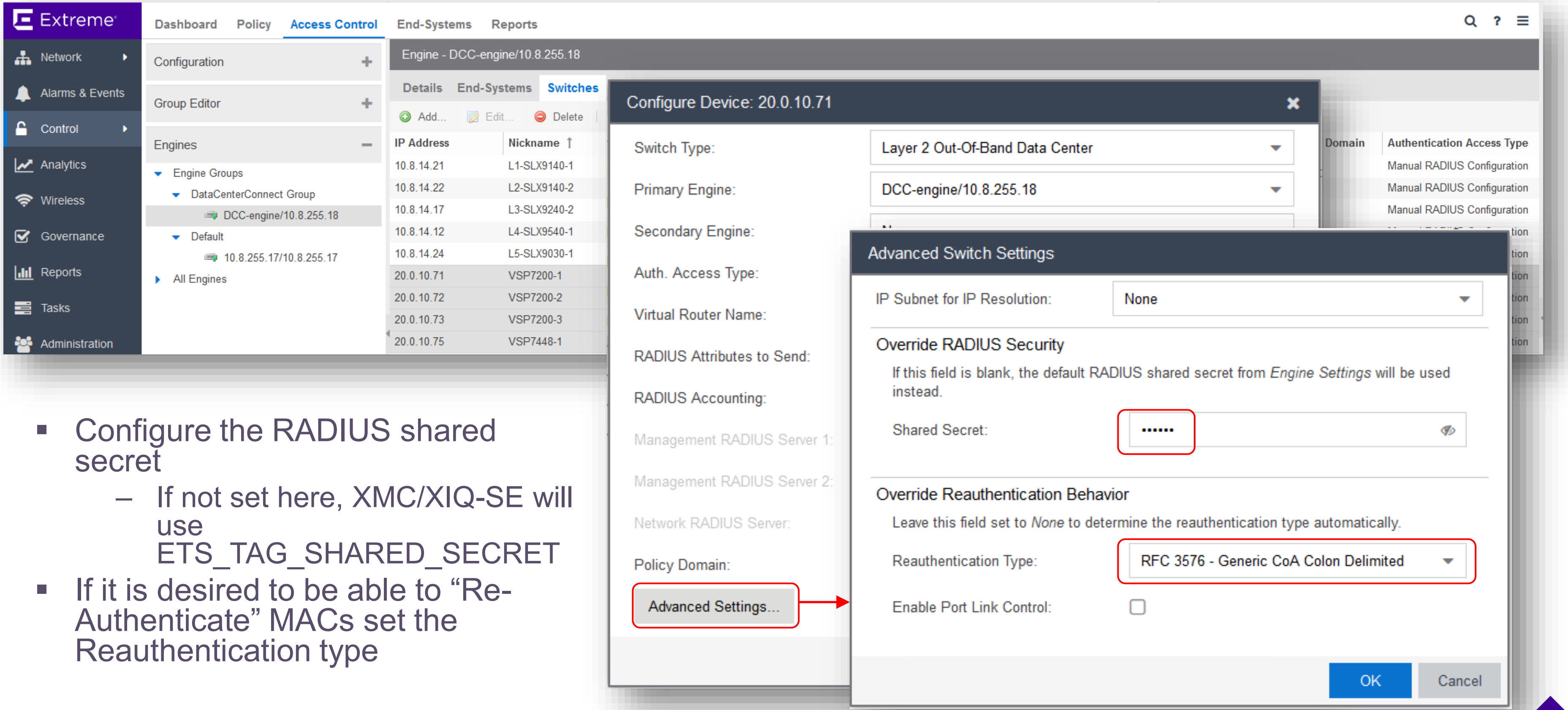
Substitutions :

FA-VLAN-ISID=%VLAN_ID%:%CUSTOM1%
Session-Timeout=1200



```
VSP7200-1:1#% show endpoint-tracking bindings
========================================================================================================================
                                              Endpoint Tracking Bindings
========================================================================================================================
PORT/MLT    INDEX  MAC                STATUS                VLAN ID  ISID      SOURCE           TIMEOUT                TIME REMAINING
------------------------------------------------------------------------------------------------------------------------
1/5         196    00:50:56:58:e0:1d  reject                0        0         radius           1 day(s), 00:00:00     0 day(s), 00:00:00
MLT-1       6144   00:50:56:86:0f:58  accept                120      2800120   autoconfig       0 day(s), 00:20:00     0 day(s), 00:16:00
MLT-1       6144   00:50:56:86:a8:12  accept                100      2800100   autoconfig       0 day(s), 00:20:00     0 day(s), 00:00:00
MLT-1       6144   00:50:56:86:e4:03  accept                110      2800110   autoconfig       0 day(s), 00:20:00     0 day(s), 00:00:00
MLT-2       6145   00:50:56:86:1e:f4  accept                130      2800130   autoconfig       0 day(s), 00:20:00     0 day(s), 00:00:00
MLT-2       6145   00:50:56:86:3b:92  accept                190      2800190   radius           0 day(s), 00:20:00     0 day(s), 00:00:00
MLT-3       6146   00:00:00:00:00:03  accept                110      2800110   radius           0 day(s), 00:20:00     0 day(s), 00:00:00
```

XMC/XIQ-SE Control – Add VSP switches to Access Control engine



Engine - DCC-engine/10.8.255.18

IP Address	Nickname
10.8.14.21	L1-SLX9140-1
10.8.14.22	L2-SLX9140-2
10.8.14.17	L3-SLX9240-2
10.8.14.12	L4-SLX9540-1
10.8.14.24	L5-SLX9030-1
20.0.10.71	VSP7200-1
20.0.10.72	VSP7200-2
20.0.10.73	VSP7200-3
20.0.10.75	VSP7448-1

Domain	Authentication Access Type
	Manual RADIUS Configuration
	Manual RADIUS Configuration
	Manual RADIUS Configuration

Configure Device: 20.0.10.71

Switch Type: Layer 2 Out-Of-Band Data Center

Primary Engine: DCC-engine/10.8.255.18

Secondary Engine:

Auth. Access Type:

Virtual Router Name:

RADIUS Attributes to Send:

RADIUS Accounting:

Management RADIUS Server 1:

Management RADIUS Server 2:

Network RADIUS Server:

Policy Domain:

Advanced Switch Settings

IP Subnet for IP Resolution: None

Override RADIUS Security

If this field is blank, the default RADIUS shared secret from *Engine Settings* will be used instead.

Shared Secret: ••••••

Override Reauthentication Behavior

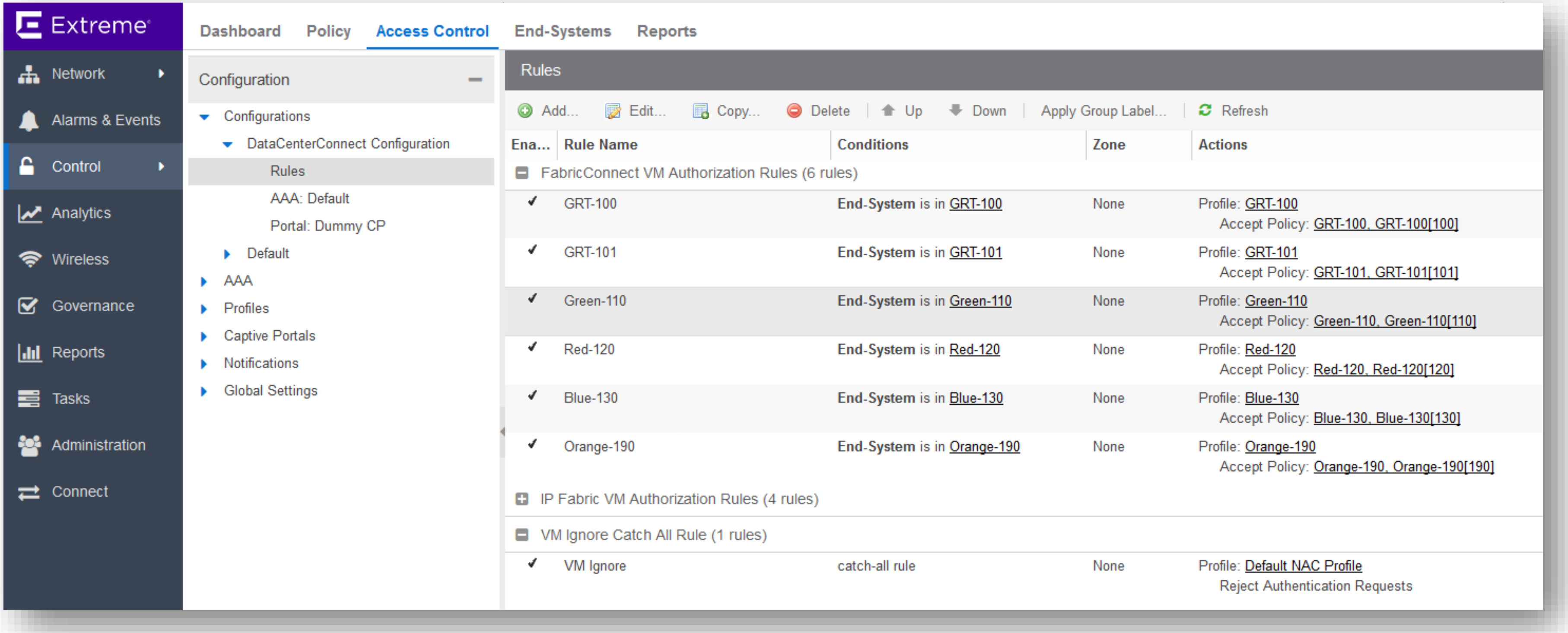
Leave this field set to *None* to determine the reauthentication type automatically.

Reauthentication Type: RFC 3576 - Generic CoA Colon Delimited

Enable Port Link Control: ☐

- Configure the RADIUS shared secret
  - If not set here, XMC/XIQ-SE will use ETS_TAG_SHARED_SECRET
- If it is desired to be able to “Re-Authenticate” MACs set the Reauthentication type

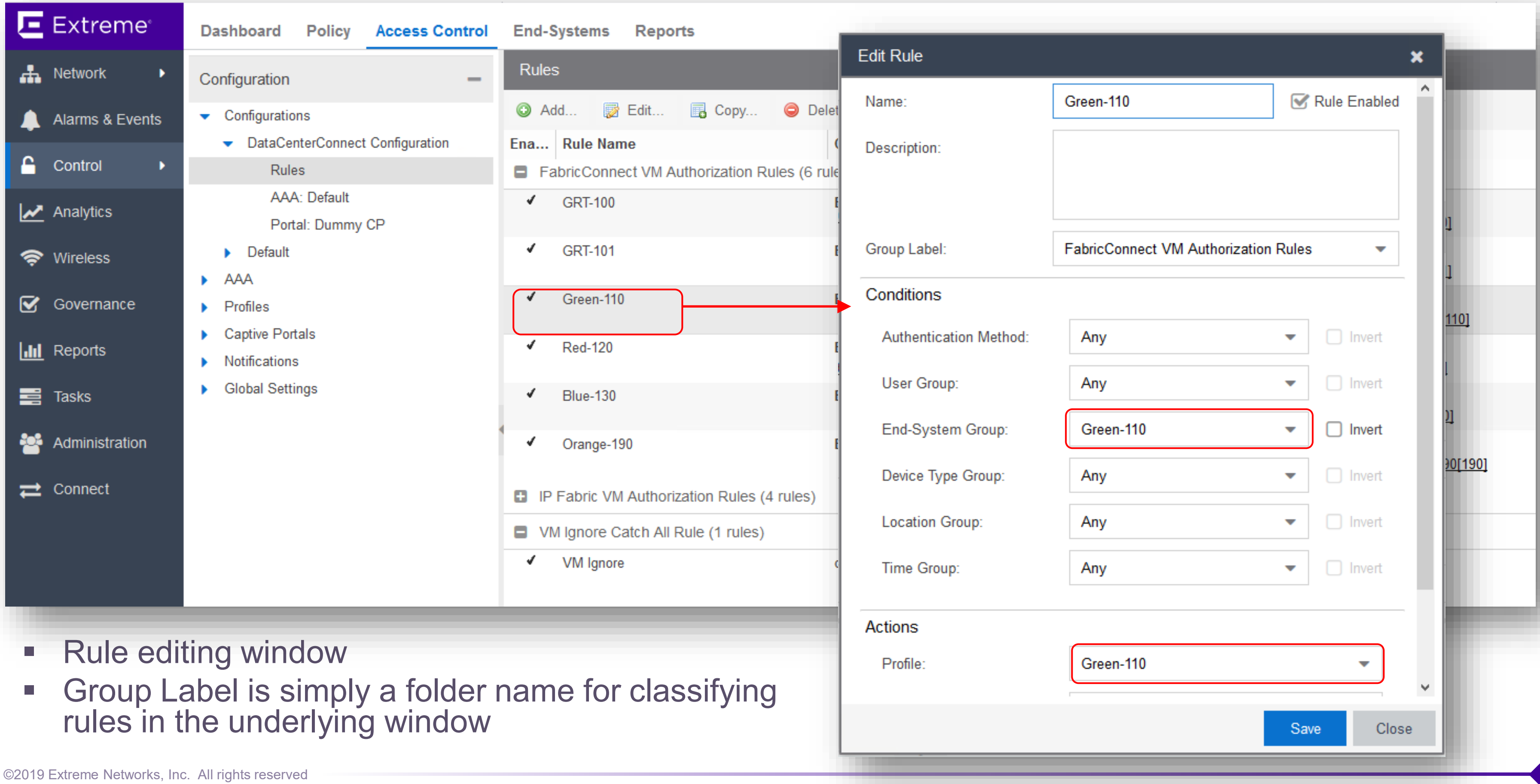
XMC/XIQ-SE Control – Endpoint-tracking rules



Ena...	Rule Name	Conditions	Zone	Actions
FabricConnect VM Authorization Rules (6 rules)				
✓	GRT-100	**End-System** is in GRT-100	None	Profile: GRT-100 Accept Policy: GRT-100, GRT-100[100]
✓	GRT-101	**End-System** is in GRT-101	None	Profile: GRT-101 Accept Policy: GRT-101, GRT-101[101]
✓	Green-110	**End-System** is in Green-110	None	Profile: Green-110 Accept Policy: Green-110, Green-110[110]
✓	Red-120	**End-System** is in Red-120	None	Profile: Red-120 Accept Policy: Red-120, Red-120[120]
✓	Blue-130	**End-System** is in Blue-130	None	Profile: Blue-130 Accept Policy: Blue-130, Blue-130[130]
✓	Orange-190	**End-System** is in Orange-190	None	Profile: Orange-190 Accept Policy: Orange-190, Orange-190[190]
IP Fabric VM Authorization Rules (4 rules)				
VM Ignore Catch All Rule (1 rules)				
✓	VM Ignore	catch-all rule	None	Profile: Default NAC Profile Reject Authentication Requests

- Rules are automatically created by XMC/XIQ-SE Connect (as unclassified)
- Administrator can simply edit these rules if desired (e.g. by introducing the I-SID configuration) and/or classify and re-order the rules (in above example rules were classified as “FC VM Authorization Rules”)

XMC/XIQ-SE Control – Add Endpoint-tracking rules



Ena...	Rule Name
FabricConnect VM Authorization Rules (6 rule	
✓	GRT-100
✓	GRT-101
✓	Green-110
✓	Red-120
✓	Blue-130
✓	Orange-190
IP Fabric VM Authorization Rules (4 rules)	
VM Ignore Catch All Rule (1 rules)	
✓	VM Ignore

Edit Rule

Name: Green-110 ☑ Rule Enabled

Description:

Group Label: FabricConnect VM Authorization Rules

Conditions

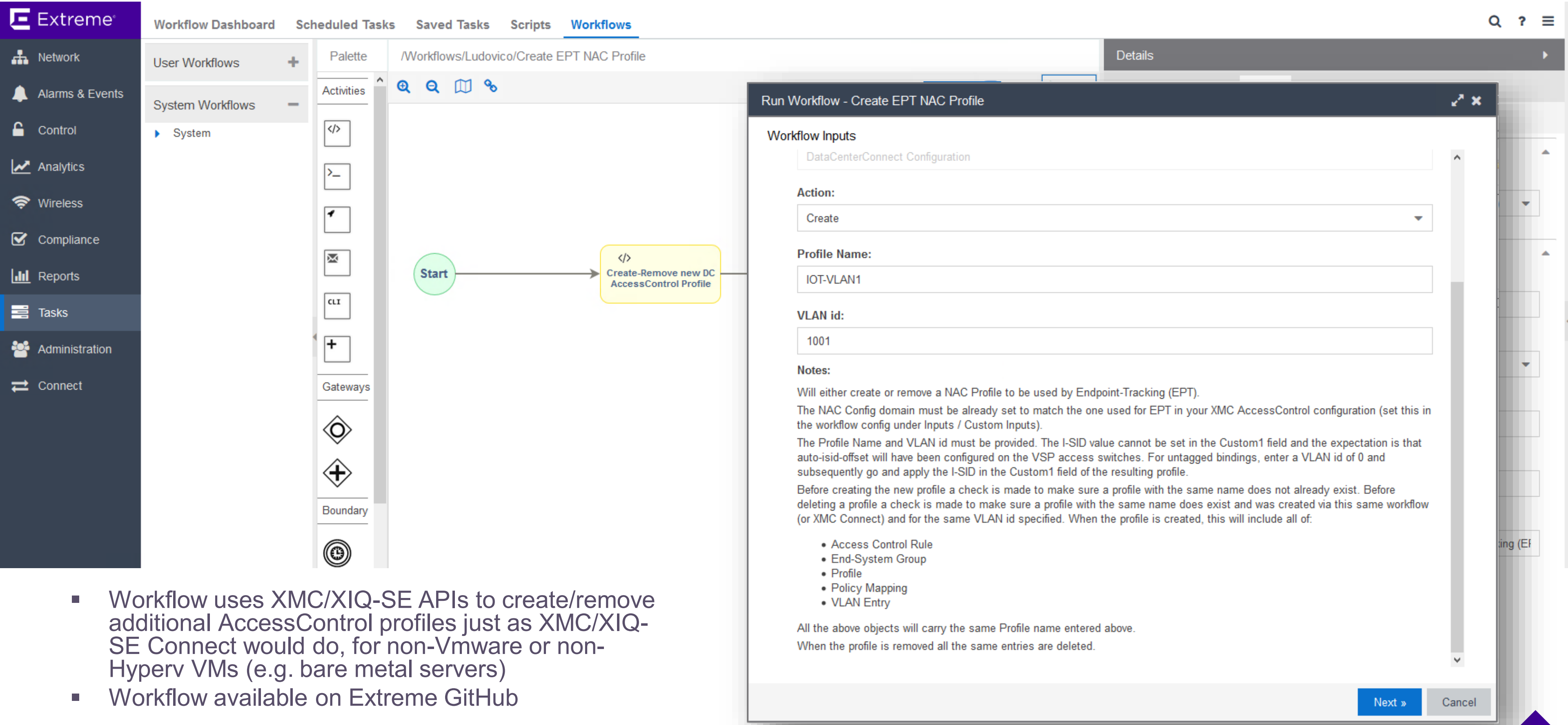
Authentication Method:	Any	□ Invert
User Group:	Any	□ Invert
End-System Group:	Green-110	□ Invert
Device Type Group:	Any	□ Invert
Location Group:	Any	□ Invert
Time Group:	Any	□ Invert

Actions

Profile: Green-110

- Rule editing window
- Group Label is simply a folder name for classifying rules in the underlying window

XMC/XIQ-SE Control – Add Endpoint-tracking rules



Run Workflow - Create EPT NAC Profile

Workflow Inputs

DataCenterConnect Configuration

Action: Create

Profile Name: IOT-VLAN1

VLAN id: 1001

Notes:

Will either create or remove a NAC Profile to be used by Endpoint-Tracking (EPT).

The NAC Config domain must be already set to match the one used for EPT in your XMC AccessControl configuration (set this in the workflow config under Inputs / Custom Inputs).

The Profile Name and VLAN id must be provided. The I-SID value cannot be set in the Custom1 field and the expectation is that auto-isid-offset will have been configured on the VSP access switches. For untagged bindings, enter a VLAN id of 0 and subsequently go and apply the I-SID in the Custom1 field of the resulting profile.

Before creating the new profile a check is made to make sure a profile with the same name does not already exist. Before deleting a profile a check is made to make sure a profile with the same name does exist and was created via this same workflow (or XMC Connect) and for the same VLAN id specified. When the profile is created, this will include all of:

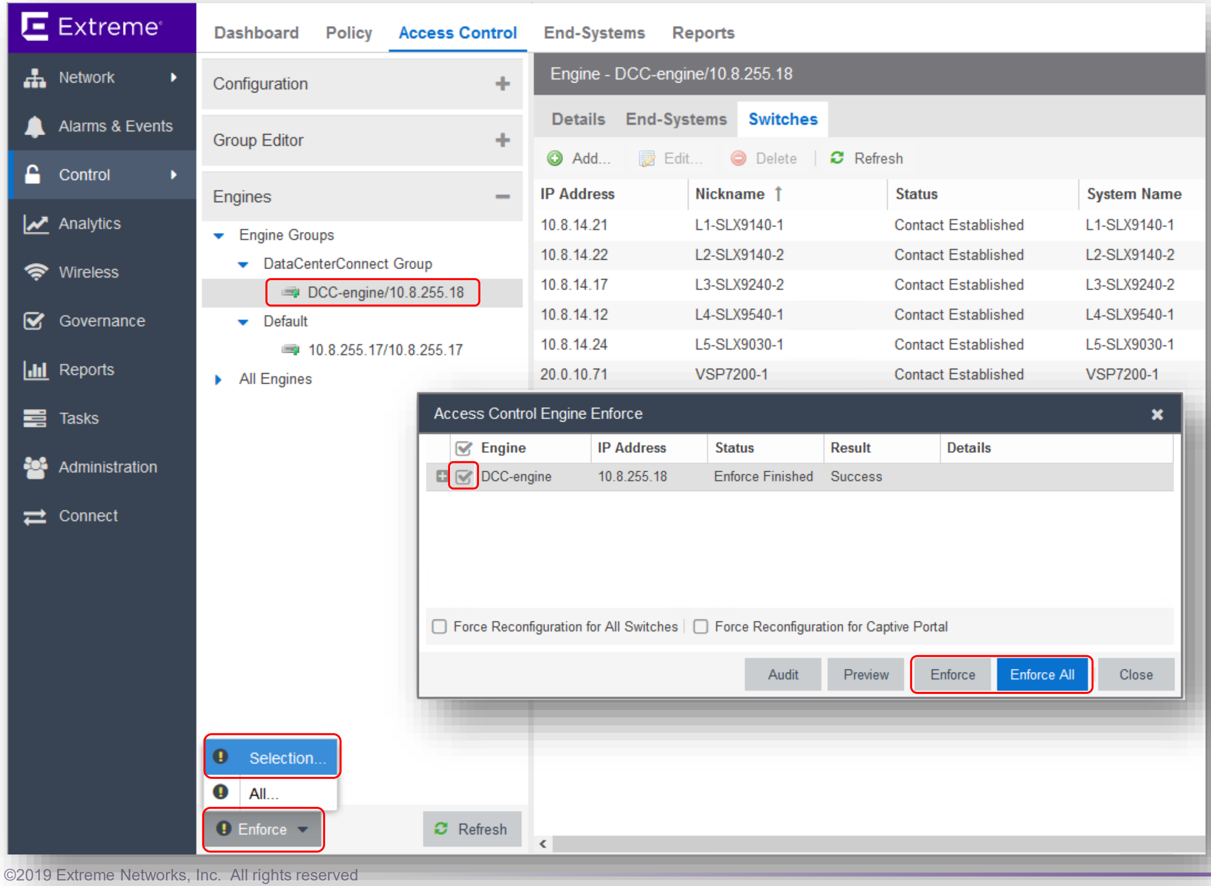
- Access Control Rule
- End-System Group
- Profile
- Policy Mapping
- VLAN Entry

All the above objects will carry the same Profile name entered above.

When the profile is removed all the same entries are deleted.

- Workflow uses XMC/XIQ-SE APIs to create/remove additional AccessControl profiles just as XMC/XIQ-SE Connect would do, for non-Vmware or non-Hyperv VMs (e.g. bare metal servers)
- Workflow available on Extreme GitHub

XMC/XIQ-SE Control – Enforce configuration to engines



Engine - DCC-engine/10.8.255.18

IP Address	Nickname ↑	Status	System Name
10.8.14.21	L1-SLX9140-1	Contact Established	L1-SLX9140-1
10.8.14.22	L2-SLX9140-2	Contact Established	L2-SLX9140-2
10.8.14.17	L3-SLX9240-2	Contact Established	L3-SLX9240-2
10.8.14.12	L4-SLX9540-1	Contact Established	L4-SLX9540-1
10.8.14.24	L5-SLX9030-1	Contact Established	L5-SLX9030-1
20.0.10.71	VSP7200-1	Contact Established	VSP7200-1

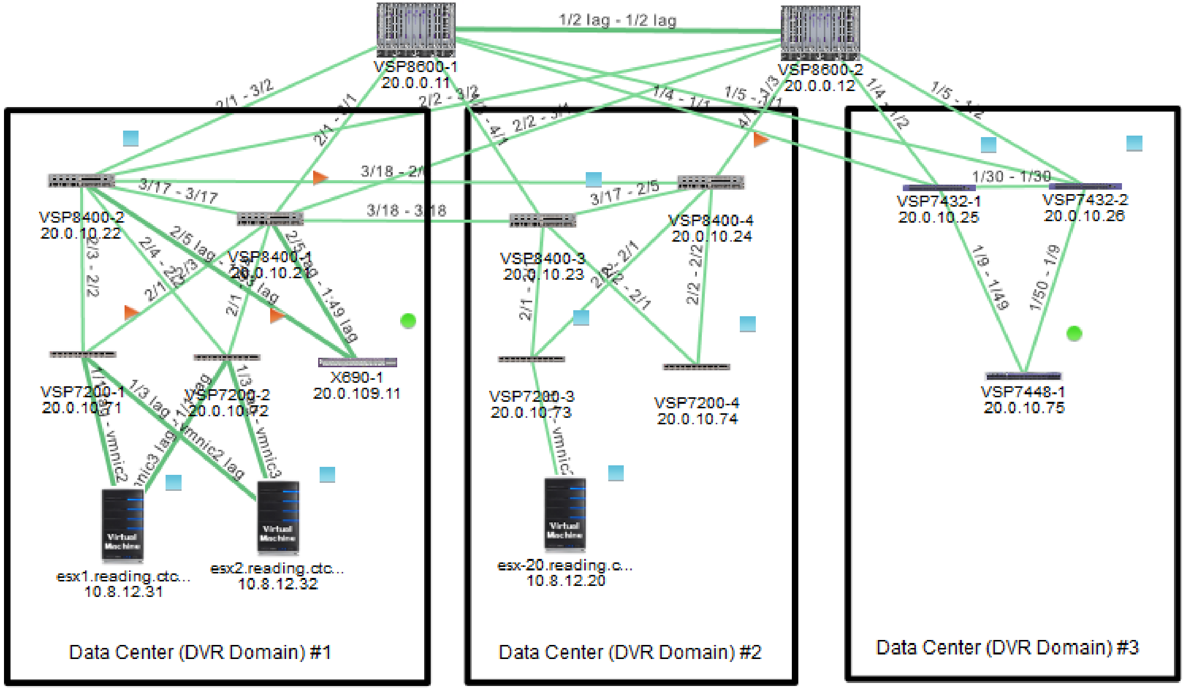
Access Control Engine Enforce

☑ Engine	IP Address	Status	Result	Details
☑ DCC-engine	10.8.255.18	Enforce Finished	Success	

☐ Force Reconfiguration for All Switches ☐ Force Reconfiguration for Captive Portal

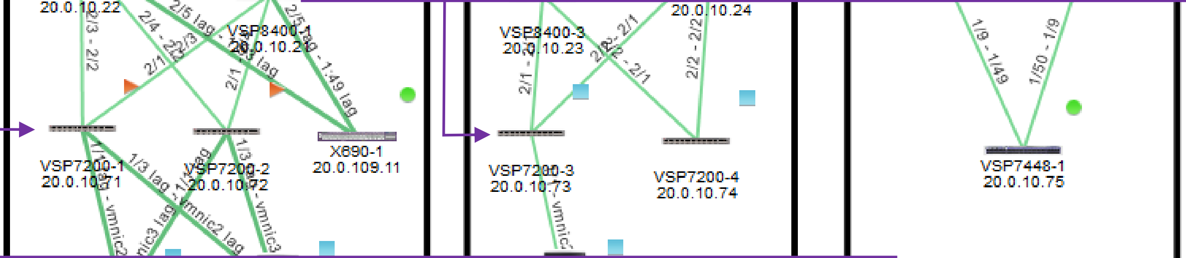
- After any configuration changes under XMC/XIQ-SE Control always remember to Enforce changes to the relevant engine(s)

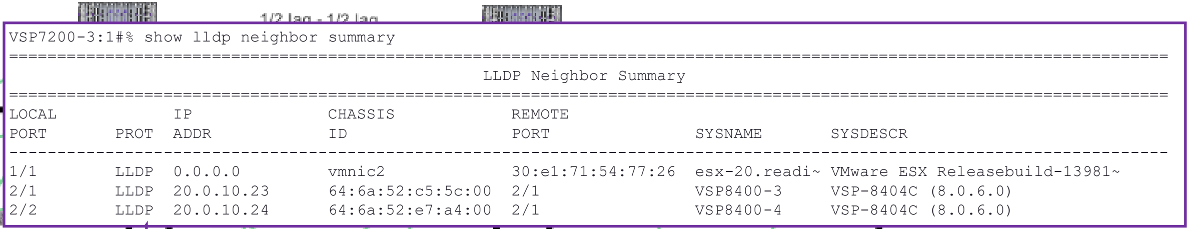
CTC Reading Fabric Connect Data Center



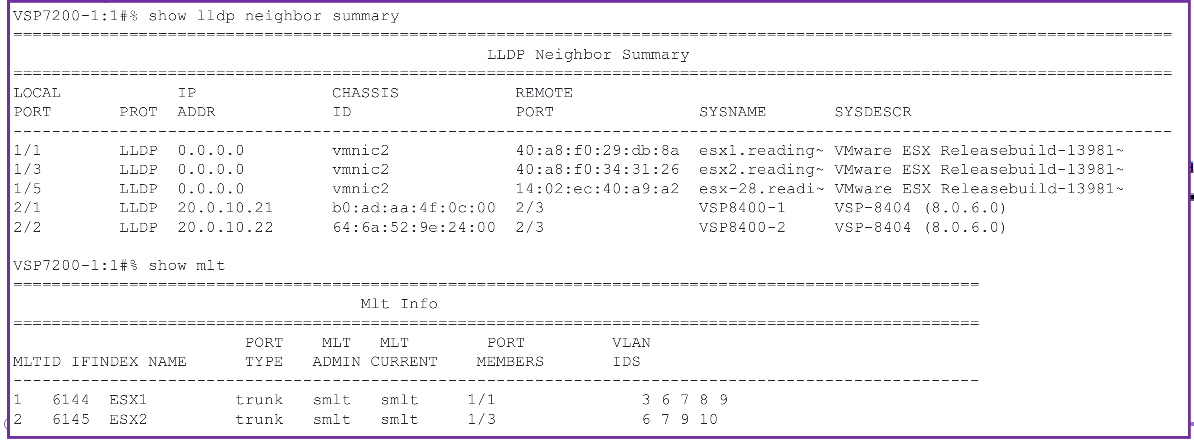
- Setup as mapped in XMC/XIQ-SE
- ESX hypervisors had SNMP enabled in order to be discovered

CTC Reading Fabric Connect Data Center





```
VSP7200-3:1#% show lldp neighbor summary
==================================================================================================================
                                          LLDP Neighbor Summary
==================================================================================================================
LOCAL              IP                CHASSIS            REMOTE
PORT      PROT    ADDR              ID                 PORT               SYSNAME       SYSDESCR
------------------------------------------------------------------------------------------------------------------
1/1       LLDP    0.0.0.0           vmnic2             30:e1:71:54:77:26  esx-20.readi~ VMware ESX Releasebuild-13981~
2/1       LLDP    20.0.10.23        64:6a:52:c5:5c:00  2/1                VSP8400-3     VSP-8404C (8.0.6.0)
2/2       LLDP    20.0.10.24        64:6a:52:e7:a4:00  2/1                VSP8400-4     VSP-8404C (8.0.6.0)
```

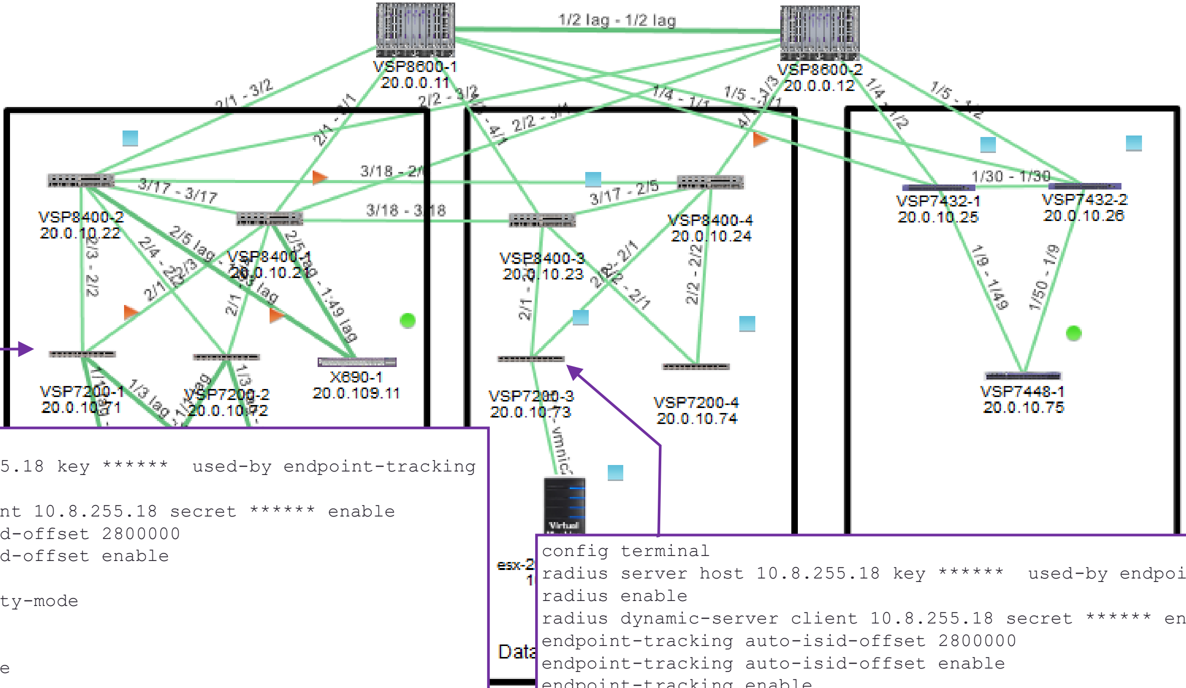


```
VSP7200-1:1#% show lldp neighbor summary
==================================================================================================================
                                          LLDP Neighbor Summary
==================================================================================================================
LOCAL              IP                CHASSIS            REMOTE
PORT      PROT    ADDR              ID                 PORT               SYSNAME       SYSDESCR
------------------------------------------------------------------------------------------------------------------
1/1       LLDP    0.0.0.0           vmnic2             40:a8:f0:29:db:8a  esx1.reading~ VMware ESX Releasebuild-13981~
1/3       LLDP    0.0.0.0           vmnic2             40:a8:f0:34:31:26  esx2.reading~ VMware ESX Releasebuild-13981~
1/5       LLDP    0.0.0.0           vmnic2             14:02:ec:40:a9:a2  esx-28.readi~ VMware ESX Releasebuild-13981~
2/1       LLDP    20.0.10.21        b0:ad:aa:4f:0c:00  2/3                VSP8400-1     VSP-8404 (8.0.6.0)
2/2       LLDP    20.0.10.22        64:6a:52:9e:24:00  2/3                VSP8400-2     VSP-8404 (8.0.6.0)

VSP7200-1:1#% show mlt
==================================================================================================
                                          Mlt Info
==================================================================================================
                        PORT     MLT    MLT          PORT          VLAN
MLTID IFINDEX NAME      TYPE    ADMIN  CURRENT      MEMBERS        IDS
--------------------------------------------------------------------------------------------------
1     6144   ESX1       trunk    smlt   smlt        1/1             3 6 7 8 9
2     6145   ESX2       trunk    smlt   smlt        1/3             6 7 9 10
```

- In this setup, SMLT links were used to ESX1 & ESX2 and simple links to ESX20, ESX28

VSP Endpoint-tracking Configuration - CLI



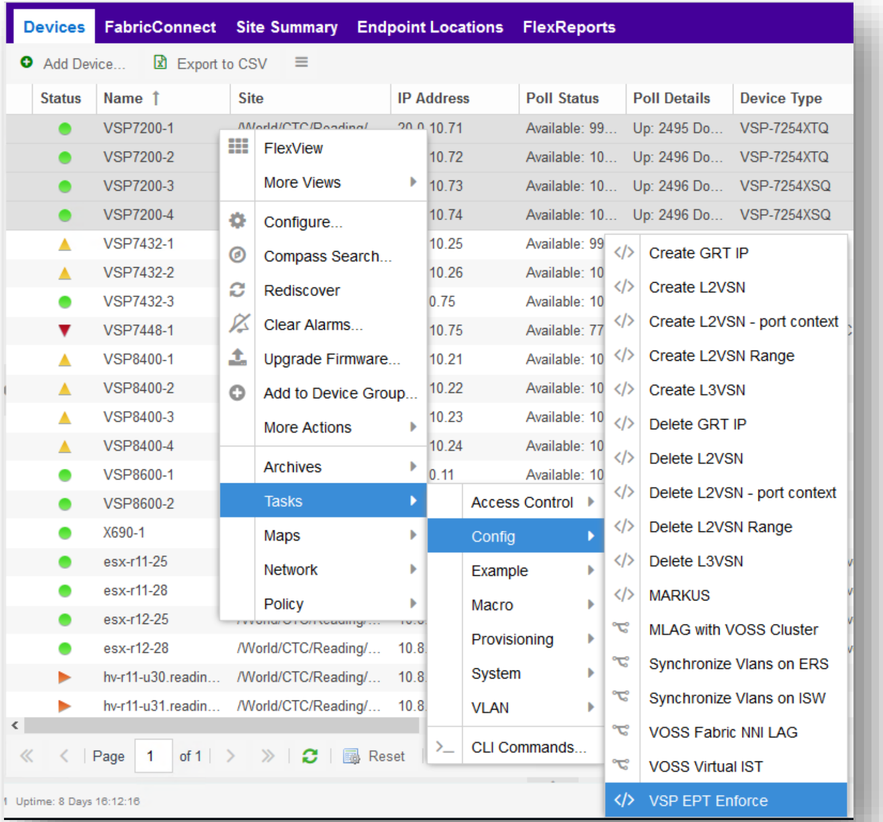
```
config terminal
radius server host 10.8.255.18 key ******  used-by endpoint-tracking
radius enable
radius dynamic-server client 10.8.255.18 secret ****** enable
endpoint-tracking auto-isid-offset 2800000
endpoint-tracking auto-isid-offset enable
endpoint-tracking enable
endpoint-tracking visibility-mode
interface mlt 1
   endpoint-tracking
   endpoint-tracking enable
exit
interface mlt 2
   endpoint-tracking
   endpoint-tracking enable
exit
interface GigabitEthernet 1/5
   endpoint-tracking
   endpoint-tracking enable
exit
end
```

```
config terminal
radius server host 10.8.255.18 key ******  used-by endpoint-tracking
radius enable
radius dynamic-server client 10.8.255.18 secret ****** enable
endpoint-tracking auto-isid-offset 2800000
endpoint-tracking auto-isid-offset enable
endpoint-tracking enable
interface GigabitEthernet 1/1
   endpoint-tracking
   endpoint-tracking enable
exit
end
```

- And make sure to delete any VLAN bindings on the EPT ports if we want those bindings to be dynamic

VSP Endpoint-tracking Configuration - XMC/XIQ-SE

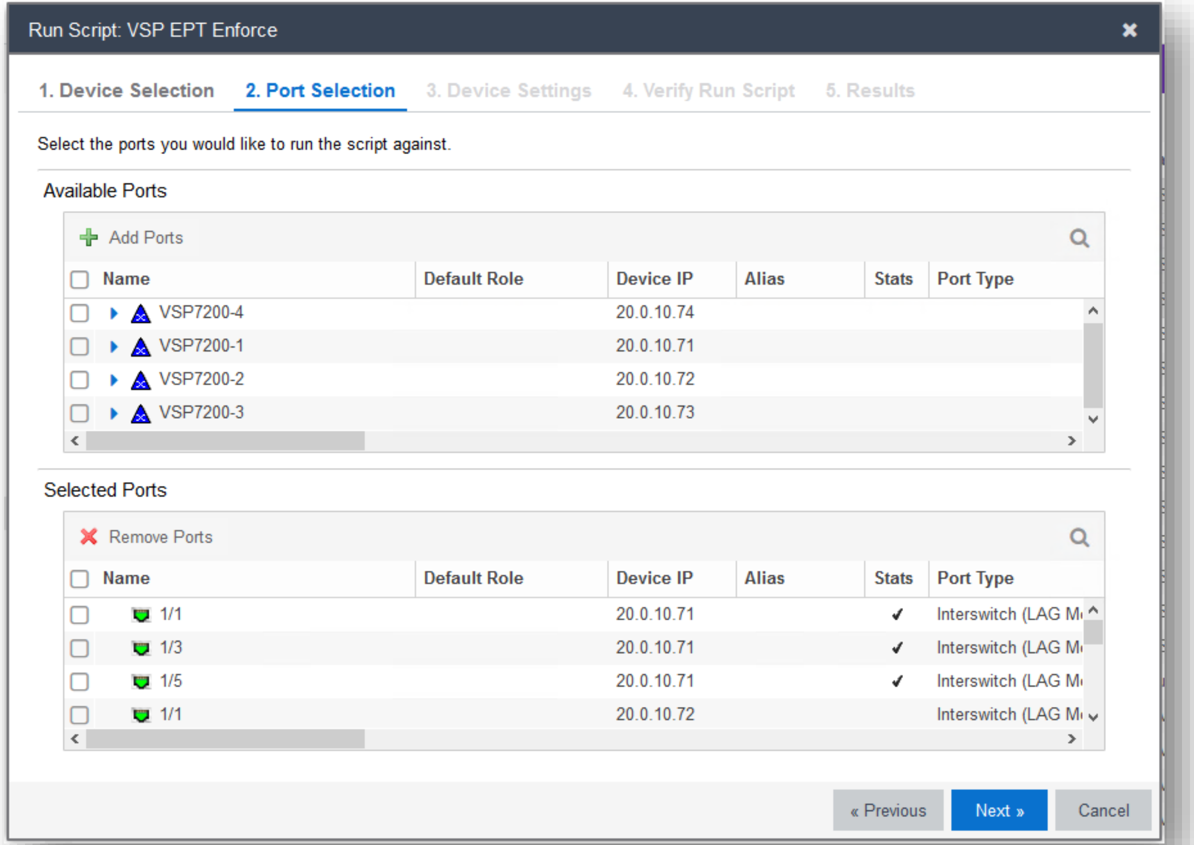
- Go to Extreme Github, XMC/XIQ-SE Scripts page: https://github.com/extremenetworks/ExtremeScripting/tree/master/Netsight/oneview_CLI_scripts
- Download the VSP EPT Enforce script as an XML file
- Then XMC/XIQ-SE Tasks / Scripts / Import
- Then run the script by selecting all VSP switches were to enable EPT, right-click Tasks / Config / VSP EPT Enforce



Status	Name	Site	IP Address	Poll Status	Poll Details	Device Type
●	VSP7200-1	/World/CTC/Reading/	20.0.10.71	Available: 99...	Up: 2495 Do...	VSP-7254XTQ
●	VSP7200-2		10.72	Available: 10...	Up: 2496 Do...	VSP-7254XTQ
●	VSP7200-3		10.73	Available: 10...	Up: 2496 Do...	VSP-7254XSQ
●	VSP7200-4		10.74	Available: 10...	Up: 2496 Do...	VSP-7254XSQ
▲	VSP7432-1		10.25	Available: 99		
▲	VSP7432-2		10.26	Available: 10		
●	VSP7432-3		0.75	Available: 10		
▼	VSP7448-1		10.75	Available: 77		
▲	VSP8400-1		10.21	Available: 10		
▲	VSP8400-2		10.22	Available: 10		
▲	VSP8400-3		10.23	Available: 10		
▲	VSP8400-4		10.24	Available: 10		
●	VSP8600-1		0.11	Available: 10		
●	VSP8600-2					
●	X690-1					
●	esx-r11-25					
●	esx-r11-28					
●	esx-r12-25	/World/CTC/Reading/...	10.8			
●	esx-r12-28	/World/CTC/Reading/...	10.8			
▶	hv-r11-u30.readin...	/World/CTC/Reading/...	10.8			
▶	hv-r11-u31.readin...	/World/CTC/Reading/...	10.8			

VSP Endpoint-tracking Configuration - XMC/XIQ-SE

- Select and Add ports where to enable EPT
- Ports which belong to LAG/MLTs can also be selected; script will work out whether to configure the individual port or the MLT bundle
- Or simply skip without selecting any ports if you only want to enforce global EPT and RADIUS config


Run Script: VSP EPT Enforce

Select the ports you would like to run the script against.

Available Ports

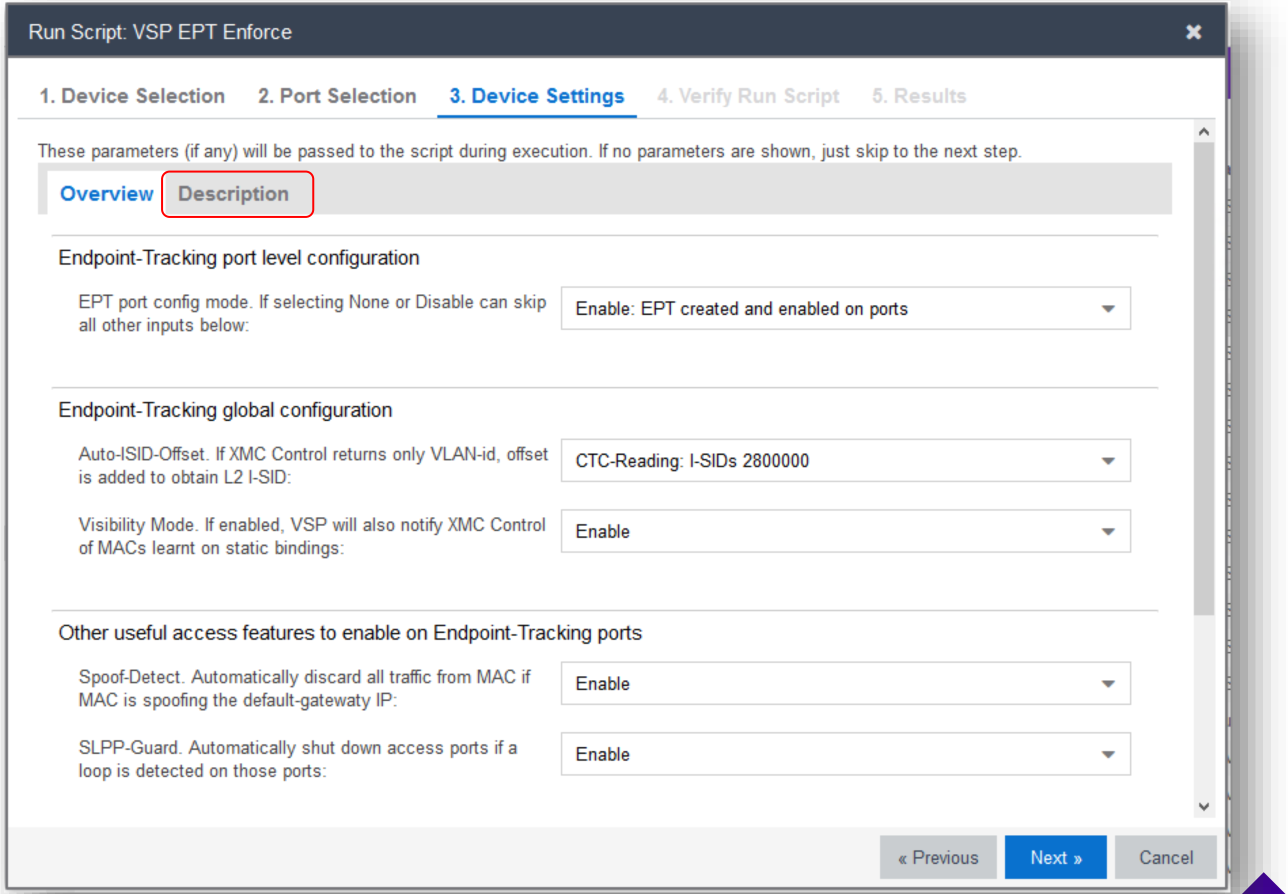
□	Name	Default Role	Device IP	Alias	Stats	Port Type
□	VSP7200-4		20.0.10.74			
□	VSP7200-1		20.0.10.71			
□	VSP7200-2		20.0.10.72			
□	VSP7200-3		20.0.10.73			

Selected Ports

□	Name	Default Role	Device IP	Alias	Stats	Port Type
□	1/1		20.0.10.71		✓	Interswitch (LAG M
□	1/3		20.0.10.71		✓	Interswitch (LAG M
□	1/5		20.0.10.71		✓	Interswitch (LAG M
□	1/1		20.0.10.72			Interswitch (LAG M

VSP Endpoint-tracking Configuration - XMC/XIQ-SE

- Set EPT configuration options
- The auto-ISID-offset pulldown values can be customized in the script itself
- Spoof-detect is a useful features to enable on any VSP DVR Leaf TOR
- SLPP-Guard is a useful features to enable on any VSP TOR switch
- Detailed description of what script does under the “Description” tab



These parameters (if any) will be passed to the script during execution. If no parameters are shown, just skip to the next step.

Endpoint-Tracking port level configuration

EPT port config mode. If selecting None or Disable can skip all other inputs below: Enable: EPT created and enabled on ports

Endpoint-Tracking global configuration

Auto-ISID-Offset. If XMC Control returns only VLAN-id, offset is added to obtain L2 I-SID: CTC-Reading: I-SIDs 2800000

Visibility Mode. If enabled, VSP will also notify XMC Control of MACs learnt on static bindings: Enable

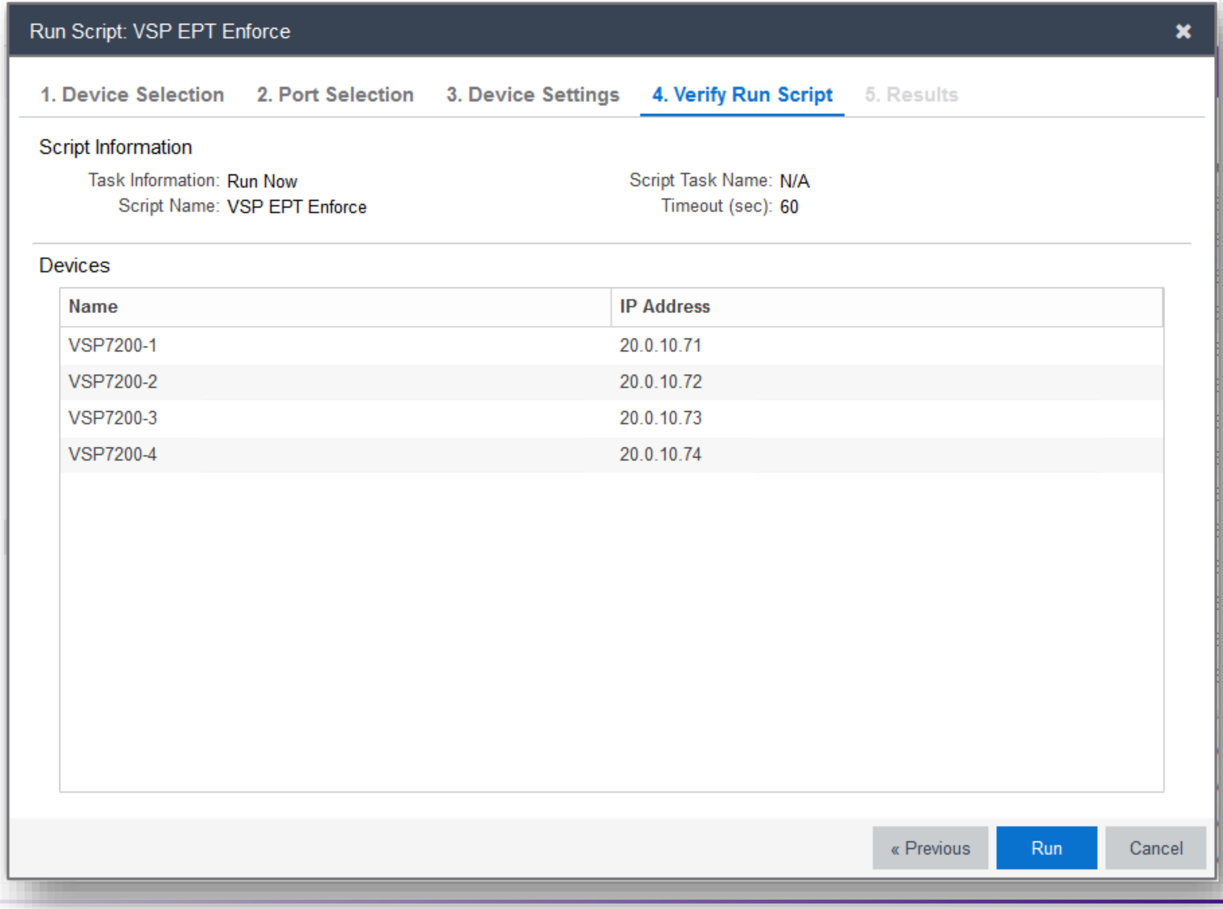
Other useful access features to enable on Endpoint-Tracking ports

Spoof-Detect. Automatically discard all traffic from MAC if MAC is spoofing the default-gatewaty IP: Enable

SLPP-Guard. Automatically shut down access ports if a loop is detected on those ports: Enable

VSP Endpoint-tracking Configuration - XMC/XIQ-SE

- Run the script



Script Information

Task Information: Run Now

Script Name: VSP EPT Enforce

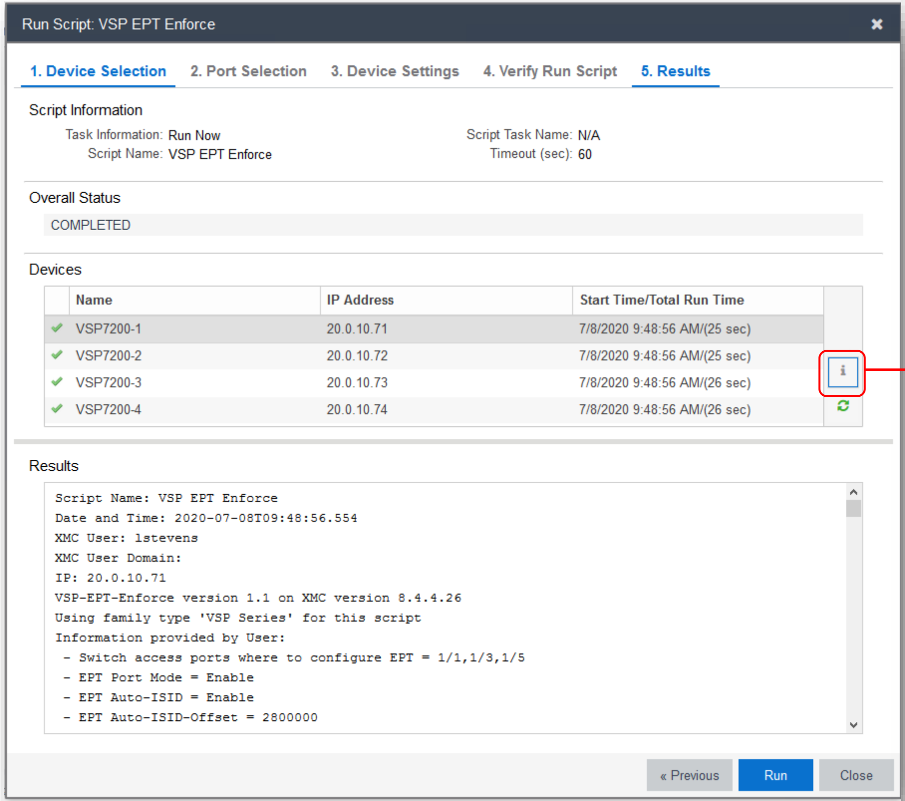
Script Task Name: N/A

Timeout (sec): 60

Devices

Name	IP Address
VSP7200-1	20.0.10.71
VSP7200-2	20.0.10.72
VSP7200-3	20.0.10.73
VSP7200-4	20.0.10.74

VSP Endpoint-tracking Configuration - XMC/XIQ-SE



Script Information

Task Information: Run Now
Script Name: VSP EPT Enforce
Script Task Name: N/A
Timeout (sec): 60

Overall Status

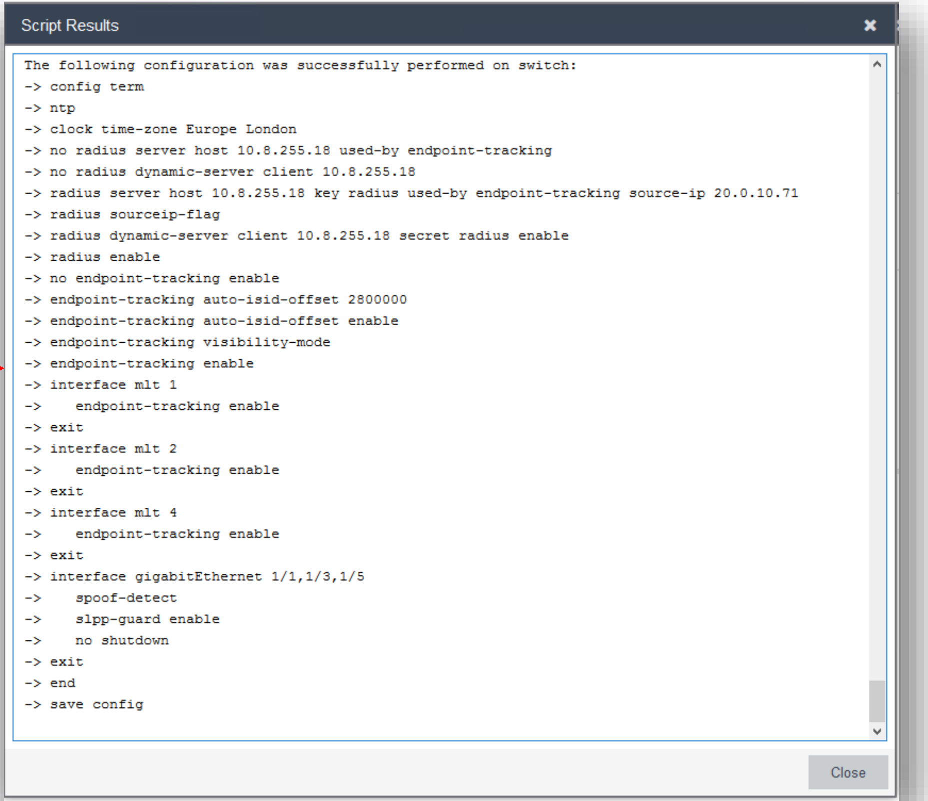
COMPLETED

Devices

	Name	IP Address	Start Time/Total Run Time
✓	VSP7200-1	20.0.10.71	7/8/2020 9:48:56 AM/(25 sec)
✓	VSP7200-2	20.0.10.72	7/8/2020 9:48:56 AM/(25 sec)
✓	VSP7200-3	20.0.10.73	7/8/2020 9:48:56 AM/(26 sec)
✓	VSP7200-4	20.0.10.74	7/8/2020 9:48:56 AM/(26 sec)

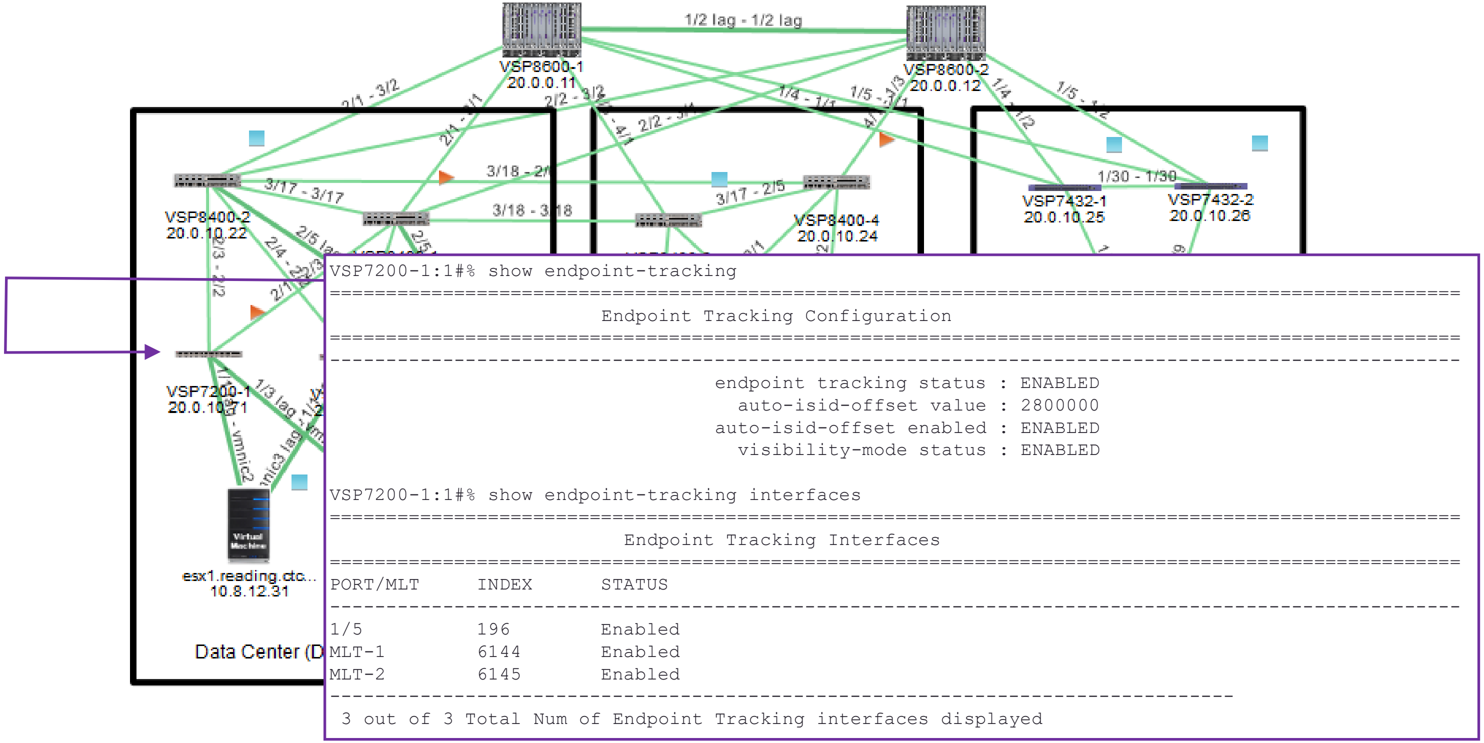
Results

```
Script Name: VSP EPT Enforce
Date and Time: 2020-07-08T09:48:56.554
XMC User: lstevens
XMC User Domain:
IP: 20.0.10.71
VSP-EPT-Enforce version 1.1 on XMC version 8.4.4.26
Using family type 'VSP Series' for this script
Information provided by User:
 - Switch access ports where to configure EPT = 1/1,1/3,1/5
 - EPT Port Mode = Enable
 - EPT Auto-ISID = Enable
 - EPT Auto-ISID-Offset = 2800000
```



```
The following configuration was successfully performed on switch:
-> config term
-> ntp
-> clock time-zone Europe London
-> no radius server host 10.8.255.18 used-by endpoint-tracking
-> no radius dynamic-server client 10.8.255.18
-> radius server host 10.8.255.18 key radius used-by endpoint-tracking source-ip 20.0.10.71
-> radius sourceip-flag
-> radius dynamic-server client 10.8.255.18 secret radius enable
-> radius enable
-> no endpoint-tracking enable
-> endpoint-tracking auto-isid-offset 2800000
-> endpoint-tracking auto-isid-offset enable
-> endpoint-tracking visibility-mode
-> endpoint-tracking enable
-> interface mlt 1
->    endpoint-tracking enable
-> exit
-> interface mlt 2
->    endpoint-tracking enable
-> exit
-> interface mlt 4
->    endpoint-tracking enable
-> exit
-> interface gigabitEthernet 1/1,1/3,1/5
->    spoof-detect
->    slpp-guard enable
->    no shutdown
-> exit
-> end
-> save config
```

VSP Endpoint-tracking Configuration



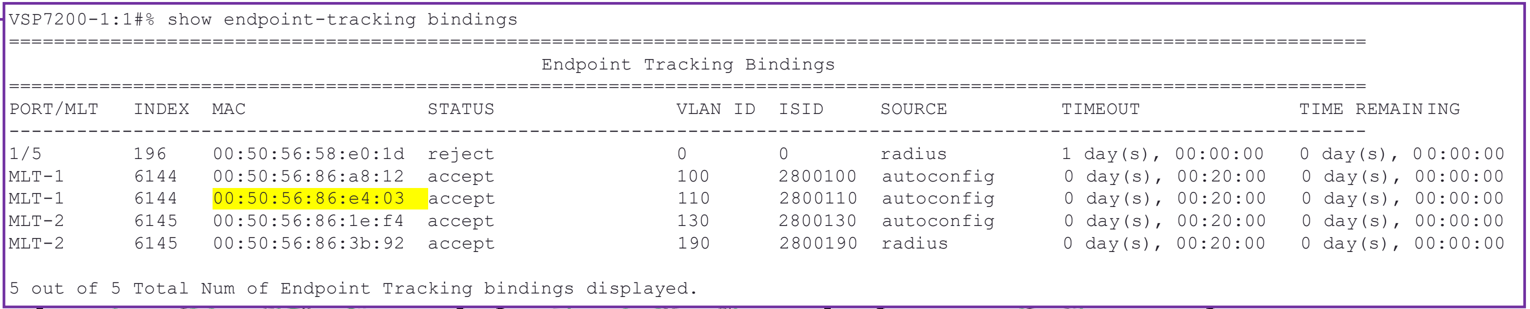
```
VSP7200-1:1#% show endpoint-tracking
====================================================================================================
                                  Endpoint Tracking Configuration
====================================================================================================
----------------------------------------------------------------------------------------------------
                                      endpoint tracking status : ENABLED
                                        auto-isid-offset value : 2800000
                                      auto-isid-offset enabled : ENABLED
                                        visibility-mode status : ENABLED

VSP7200-1:1#% show endpoint-tracking interfaces
====================================================================================================
                                    Endpoint Tracking Interfaces
====================================================================================================
PORT/MLT     INDEX      STATUS
----------------------------------------------------------------------------------------------------
1/5          196        Enabled
MLT-1        6144       Enabled
MLT-2        6145       Enabled
--------------------------------------------------------------------------------
 3 out of 3 Total Num of Endpoint Tracking interfaces displayed
```

Endpoint-tracking Visibility-mode

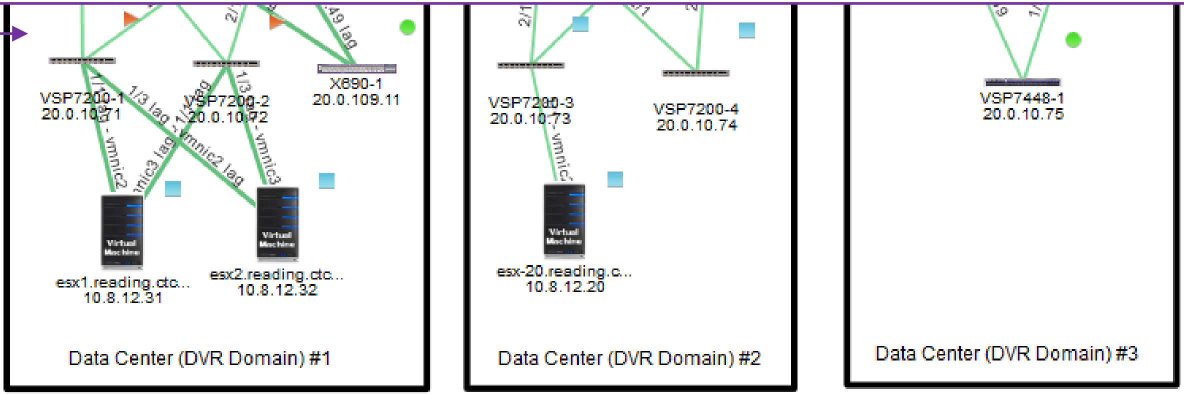
- Static Switched UNI VLAN/I-SID bindings can exist on ports which are enabled for Endpoint tracking
- By default, for MACs learned on static Switched UNIs configured on Endpoint Tracking enabled ports, no RADIUS request is sent (as there is no need to get a VLAN/I-SID binding from the RADIUS server)
- However, it can be interesting to generate a RADIUS request even for these MACs, in which case the Endpoint-tracking Visibility-mode can be enabled.
- This is useful for two reasons:
  1. It is useful to gain visibility of where exactly those server MACs are located in the Data Center; i.e. let these MACs also show up in XMC/XIQ-SE's end-stations and Multi-Cloud dashboards
  2. It can be useful as a way to migrate to Endpoint-tracking and gain confidence on the functionality before letting it manage all server VLAN/I-SID bindings
     a) Initially all VLAN/I-SID bindings are static on the TOR access ports and EPT is disabled
     b) Then EPT is enabled, globally and on all the TOR access ports
     c) EPT Visibility-mode is enabled, and all server MACs can be monitored and tracked from XMC/XIQ-SE. Once satisfied that EPT is performing correctly, the next step can be taken.
     d) The static Switched UNI VLAN/I-SID binding can be deleted, thus leaving EPT to assign VLAN/I-SID bindings dynamically

VSP Endpoint-tracking Configuration



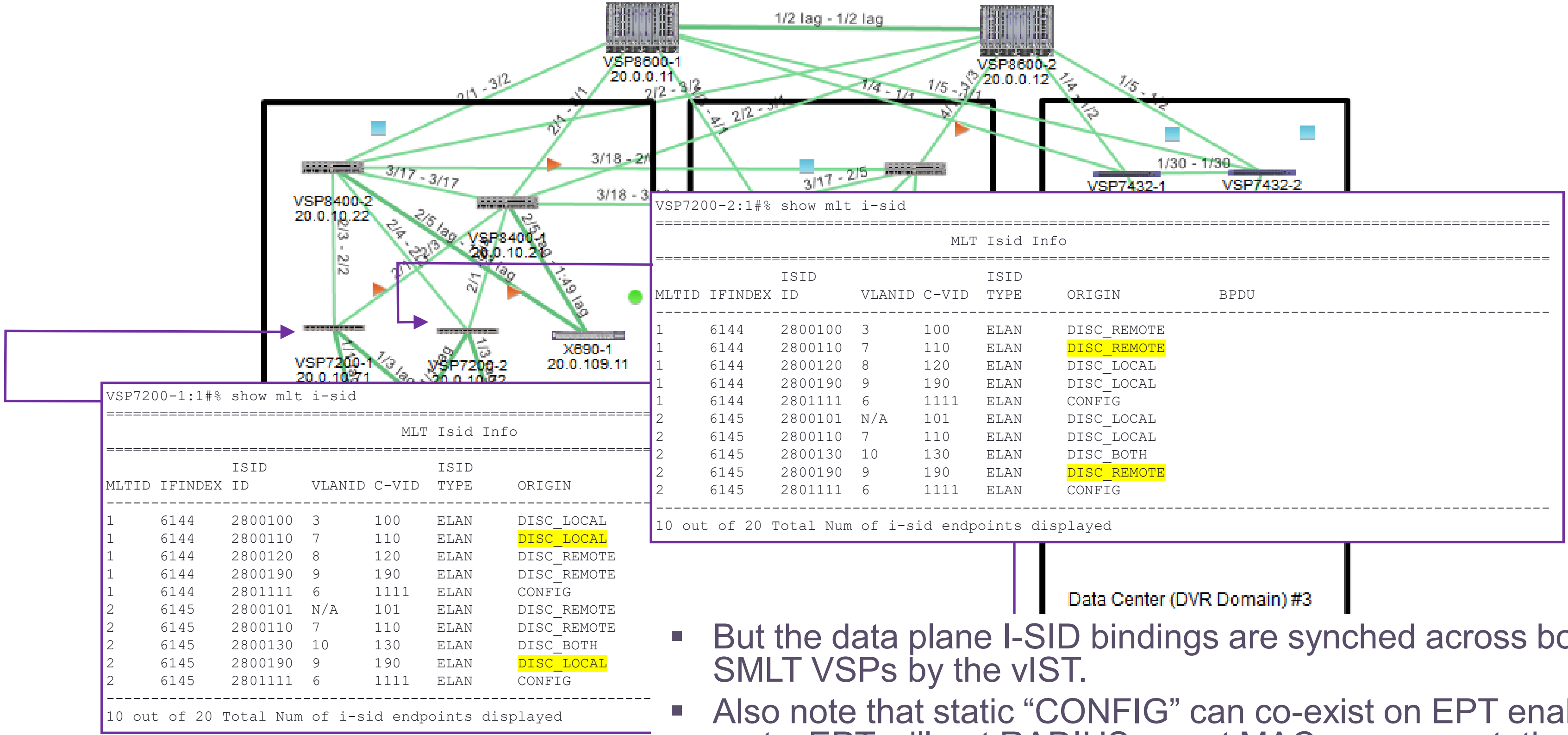
```
VSP7200-1:1#% show endpoint-tracking bindings
=========================================================================================================
                                           Endpoint Tracking Bindings
=========================================================================================================
PORT/MLT    INDEX  MAC                  STATUS                 VLAN ID  ISID      SOURCE           TIMEOUT                TIME REMAINING
---------------------------------------------------------------------------------------------------------
1/5         196    00:50:56:58:e0:1d    reject                 0        0         radius           1 day(s), 00:00:00     0 day(s), 00:00:00
MLT-1       6144   00:50:56:86:a8:12    accept                 100      2800100   autoconfig       0 day(s), 00:20:00     0 day(s), 00:00:00
MLT-1       6144   00:50:56:86:e4:03    accept                 110      2800110   autoconfig       0 day(s), 00:20:00     0 day(s), 00:00:00
MLT-2       6145   00:50:56:86:1e:f4    accept                 130      2800130   autoconfig       0 day(s), 00:20:00     0 day(s), 00:00:00
MLT-2       6145   00:50:56:86:3b:92    accept                 190      2800190   radius           0 day(s), 00:20:00     0 day(s), 00:00:00

5 out of 5 Total Num of Endpoint Tracking bindings displayed.
```



- Notice that our highlighted Server-Green MAC has been received RADIUS bindings with VLAN-id only, hence the I-SID was autoconfig-ured (offset 2800000 + VLAN-id)
- Whereas MAC 00:50:56:86:3b:92 received both VLAN 190 and I-SID 2800190 directly from RADIUS
- With SMLT links, a MAC can appear in the binding table of one VSP peer or both (binding tables are not synched by the vIST)

VSP Endpoint-tracking Configuration

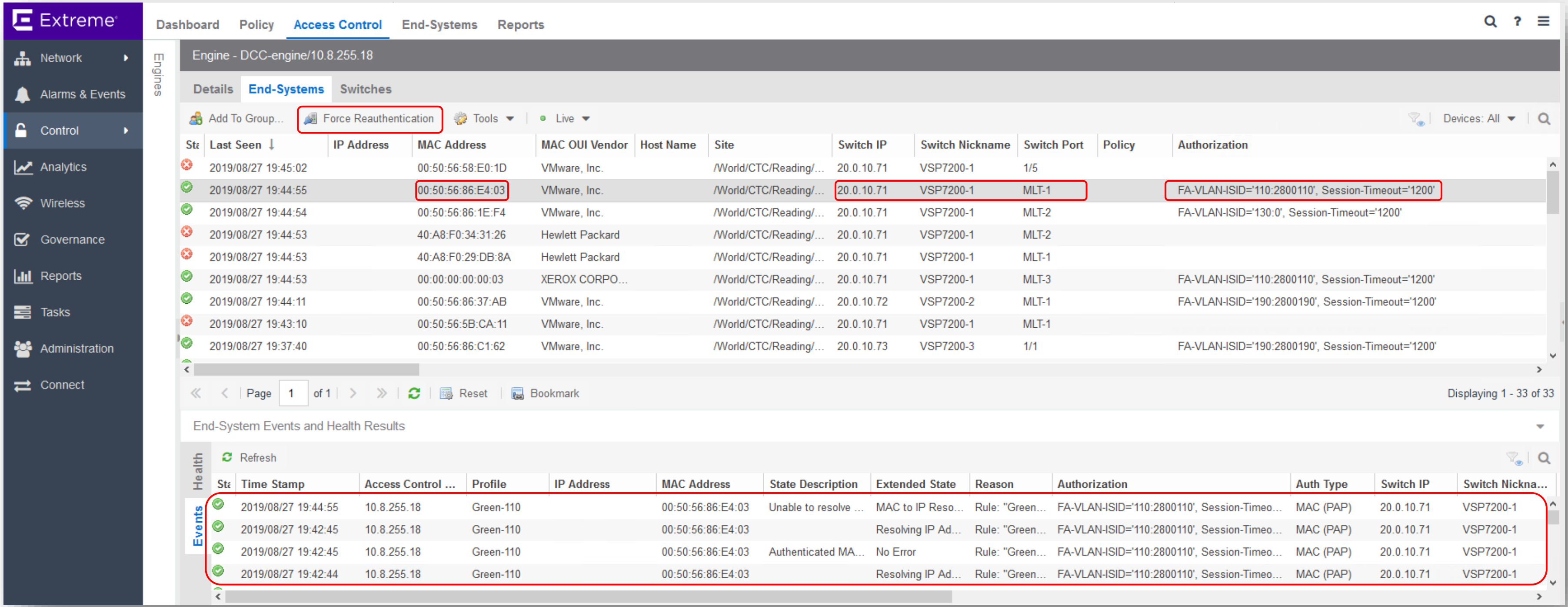


```
VSP7200-2:1#% show mlt i-sid
====================================================================================================
                                          MLT Isid Info
====================================================================================================
             ISID                        ISID
MLTID IFINDEX ID          VLANID C-VID   TYPE       ORIGIN           BPDU
----------------------------------------------------------------------------------------------------
1      6144    2800100   3       100     ELAN       DISC_REMOTE
1      6144    2800110   7       110     ELAN       DISC_REMOTE
1      6144    2800120   8       120     ELAN       DISC_LOCAL
1      6144    2800190   9       190     ELAN       DISC_LOCAL
1      6144    2801111   6       1111    ELAN       CONFIG
2      6145    2800101   N/A     101     ELAN       DISC_LOCAL
2      6145    2800110   7       110     ELAN       DISC_LOCAL
2      6145    2800130   10      130     ELAN       DISC_BOTH
2      6145    2800190   9       190     ELAN       DISC_REMOTE
2      6145    2801111   6       1111    ELAN       CONFIG
----------------------------------------------------------------------------------------------------
10 out of 20 Total Num of i-sid endpoints displayed
```

```
VSP7200-1:1#% show mlt i-sid
==============================================================
                          MLT Isid Info
==============================================================
             ISID                        ISID
MLTID IFINDEX ID          VLANID C-VID   TYPE       ORIGIN
--------------------------------------------------------------
1      6144    2800100   3       100     ELAN       DISC_LOCAL
1      6144    2800110   7       110     ELAN       DISC_LOCAL
1      6144    2800120   8       120     ELAN       DISC_REMOTE
1      6144    2800190   9       190     ELAN       DISC_REMOTE
1      6144    2801111   6       1111    ELAN       CONFIG
2      6145    2800101   N/A     101     ELAN       DISC_REMOTE
2      6145    2800110   7       110     ELAN       DISC_REMOTE
2      6145    2800130   10      130     ELAN       DISC_BOTH
2      6145    2800190   9       190     ELAN       DISC_LOCAL
2      6145    2801111   6       1111    ELAN       CONFIG
--------------------------------------------------------------
10 out of 20 Total Num of i-sid endpoints displayed
```

- But the data plane I-SID bindings are synched across both SMLT VSPs by the vIST.
- Also note that static “CONFIG” can co-exist on EPT enabled ports; EPT will not RADIUS report MACs seen on static bindings.

XMC/XIQ-SE – Viewing Data Center VM MACs



Engine - DCC-engine/10.8.255.18

Sta	Last Seen	IP Address	MAC Address	MAC OUI Vendor	Host Name	Site	Switch IP	Switch Nickname	Switch Port	Policy	Authorization
✗	2019/08/27 19:45:02		00:50:56:58:E0:1D	VMware, Inc.		/World/CTC/Reading/...	20.0.10.71	VSP7200-1	1/5		
✓	2019/08/27 19:44:55		00:50:56:86:E4:03	VMware, Inc.		/World/CTC/Reading/...	20.0.10.71	VSP7200-1	MLT-1		FA-VLAN-ISID='110:2800110', Session-Timeout='1200'
✓	2019/08/27 19:44:54		00:50:56:86:1E:F4	VMware, Inc.		/World/CTC/Reading/...	20.0.10.71	VSP7200-1	MLT-2		FA-VLAN-ISID='130:0', Session-Timeout='1200'
✗	2019/08/27 19:44:53		40:A8:F0:34:31:26	Hewlett Packard		/World/CTC/Reading/...	20.0.10.71	VSP7200-1	MLT-2		
✗	2019/08/27 19:44:53		40:A8:F0:29:DB:8A	Hewlett Packard		/World/CTC/Reading/...	20.0.10.71	VSP7200-1	MLT-1		
✓	2019/08/27 19:44:53		00:00:00:00:00:03	XEROX CORPO...		/World/CTC/Reading/...	20.0.10.71	VSP7200-1	MLT-3		FA-VLAN-ISID='110:2800110', Session-Timeout='1200'
✓	2019/08/27 19:44:11		00:50:56:86:37:AB	VMware, Inc.		/World/CTC/Reading/...	20.0.10.72	VSP7200-2	MLT-1		FA-VLAN-ISID='190:2800190', Session-Timeout='1200'
✗	2019/08/27 19:43:10		00:50:56:5B:CA:11	VMware, Inc.		/World/CTC/Reading/...	20.0.10.71	VSP7200-1	MLT-1		
✓	2019/08/27 19:37:40		00:50:56:86:C1:62	VMware, Inc.		/World/CTC/Reading/...	20.0.10.73	VSP7200-3	1/1		FA-VLAN-ISID='190:2800190', Session-Timeout='1200'

Page 1 of 1

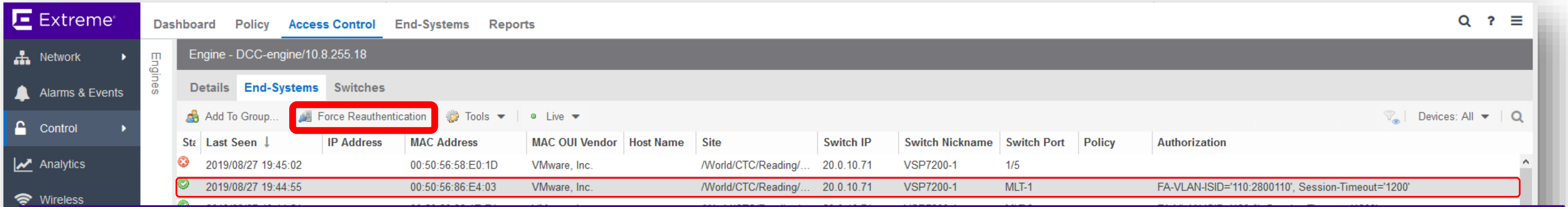
Displaying 1 - 33 of 33

End-System Events and Health Results

Sta	Time Stamp	Access Control ...	Profile	IP Address	MAC Address	State Description	Extended State	Reason	Authorization	Auth Type	Switch IP	Switch Nickna...
✓	2019/08/27 19:44:55	10.8.255.18	Green-110		00:50:56:86:E4:03	Unable to resolve ...	MAC to IP Reso...	Rule: "Green...	FA-VLAN-ISID='110:2800110', Session-Timeo...	MAC (PAP)	20.0.10.71	VSP7200-1
✓	2019/08/27 19:42:45	10.8.255.18	Green-110		00:50:56:86:E4:03		Resolving IP Ad...	Rule: "Green...	FA-VLAN-ISID='110:2800110', Session-Timeo...	MAC (PAP)	20.0.10.71	VSP7200-1
✓	2019/08/27 19:42:45	10.8.255.18	Green-110		00:50:56:86:E4:03	Authenticated MA...	No Error	Rule: "Green...	FA-VLAN-ISID='110:2800110', Session-Timeo...	MAC (PAP)	20.0.10.71	VSP7200-1
✓	2019/08/27 19:42:44	10.8.255.18	Green-110		00:50:56:86:E4:03		Resolving IP Ad...	Rule: "Green...	FA-VLAN-ISID='110:2800110', Session-Timeo...	MAC (PAP)	20.0.10.71	VSP7200-1

- MAC of our Server-Green VM as seen by XMC/XIQ-SE once RADIUS authenticated
- Notice the Authorization RADIUS attributes
- Lower window shows authentication recent history of selected MAC
- To re-authenticate the VM MAC, select the entry in the upper table and hit the “Force Reauthentication” button

XMC/XIQ-SE – Forcing Reauthentication



Sta	Last Seen	IP Address	MAC Address	MAC OUI Vendor	Host Name	Site	Switch IP	Switch Nickname	Switch Port	Policy	Authorization
✗	2019/08/27 19:45:02		00:50:56:58:E0:1D	VMware, Inc.		/World/CTC/Reading/...	20.0.10.71	VSP7200-1	1/5		
✓	2019/08/27 19:44:55		00:50:56:86:E4:03	VMware, Inc.		/World/CTC/Reading/...	20.0.10.71	VSP7200-1	MLT-1		FA-VLAN-ISID='110:2800110', Session-Timeout='1200'

XMC/XIQ-SE Reauthentication Type = Generic CoA Colon Delimited

```
15:45:22.096657 IP (tos 0x0, ttl 64, id 61185, offset 0, flags [DF], proto UDP (17), length 73)
    dcc-engine.reading.ctc.local.52547 > 20.0.10.71.3799: [bad udp cksum 0x27a8 -> 0x5aa4!] RADIUS, length: 45
        Disconnect-Request (40), id: 0x8b, Authenticator: 0e9d21453e51df7672113e878dbee91e
          Calling-Station-Id Attribute (31), length: 19, Value: 00:50:56:86:E4:03
            0x0000:  3030 3a35 303a 3536 3a38 363a 4534 3a30
            0x0010:  33
          Event-Timestamp Attribute (55), length: 6, Value: Fri Aug 30 15:45:22 2019
            0x0000:  5d69 3682

15:45:22.103668 IP (tos 0x0, ttl 61, id 40225, offset 0, flags [none], proto UDP (17), length 48)
    20.0.10.71.3799 > dcc-engine.reading.ctc.local.52547: [udp sum ok] RADIUS, length: 20
        Disconnect-ACK (41), id: 0x8b, Authenticator: bd90f46ce42e57b7b119df359c447e63
```

- What XMC/XIQ-SE sends if user hits the Force Reauthentication
- VSP will remove the MAC from its EPT binding table
- NOTE: for MACs on SMLT links, XMC/XIQ-SE will only send the Disconnect-Request to 1 VSP only
  - But a VSP will automatically trigger a disconnect for the same MAC on the vIST peer

Extreme™

Customer-Driven Networking

WWW.EXTREMENETWORKS.COM