



# **VSP Edge Deployment Guide with ExtremeCloud IQ - Site Engine/NAC Automation**

**Abstract:** This document describes the steps needed to deploy a VSP switch running VOSS 8.3 or later using a combination of VOSS fabric automation features and ExtremeCloud™ IQ - Site Engine (XIQ-SE) / Network Access Control (NAC) onboarding automation.

**Part Number:** 9037480-00 Rev AA

**Published:** July 2022

Extreme Networks, Inc.  
Phone +1 408.579.2800  
Toll-free +1 888.257.3000  
**[www.extremenetworks.com](http://www.extremenetworks.com)**

Copyright © 2022 Extreme Networks, Inc.

## Legal Notice

Extreme Networks, Inc. reserves the right to make changes in specifications and other information contained in this document and its website without prior notice. The reader should in all cases consult representatives of Extreme Networks to determine whether any such changes have been made.

The hardware, firmware, software or any specifications described or referred to in this document are subject to change without notice.

## Trademarks

Extreme Networks and the Extreme Networks logo are trademarks or registered trademarks of Extreme Networks, Inc. in the United States and/or other countries.

All other names (including any product names) mentioned in this document are the property of their respective owners and may be trademarks or registered trademarks of their respective companies/owners.

For additional information on Extreme Networks trademarks, see:

<https://www.extremenetworks.com/Company/legal/trademarks/>

## Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at:

<https://www.extremenetworks.com/support/policies/open-source-declaration/>

# Contents

---

Prerequisites .....	4
Overview .....	4
Objectives .....	4
Network Diagram .....	5
Preexisting Configuration Review .....	7
XIQ-SE Preexisting Configuration Review .....	7
XIQ-SE: Script and Workflow Review .....	15
Prepare VSP Core Switches for Automated VSP Edge .....	18
Site Selection for VSP Core Switches .....	18
Apply DVR Controller, VLAN, and IP Config .....	20
Apply Seed Config for Zero Touch Fabric .....	22
Prepare XIQ-SE for VSP Edge Deployment .....	24
ZTP+ Configuration .....	24
XIQ-SE Workflow Configuration for VSP Onboarding .....	28
Universal Edge Switch OS Conversion Using XIQ .....	34
Prepare OS Conversion Using XIQ .....	35
Zero Touch Onboarding of VSP Edge Switches .....	36
Switch Installation and Power Up .....	36
OS Conversion Using XIQ .....	36
Observe Progress Using the VSP Edge Console .....	36
Manual Steps Required if OS Conversion Was Done Using XIQ .....	39
Monitor XIQ-SE Onboarding Workflow Execution .....	41
Migrate VSP Edge to Dedicated Switch Management CLIP .....	43
Configure XIQ-SE Control Switch Reauthentication Type .....	47
Verify All End Devices Are Operational .....	51
Inspect the VSP Fabric .....	51
Inspect the Auto-Sense Ports on the VSP Edge Switches .....	53
Verify the WLAN AP Is Operational .....	54
Verify the IP Phone Is Operational .....	56
Verify Client PC Authentication .....	56
Appendix .....	59
XCC Preexisting Configuration Review .....	59
Terms & Conditions of Use .....	61

## Prerequisites

---

- An existing Fabric Connect core switch running VOSS 8.3 or later
- ExtremeCloud IQ – Site Engine (XIQ-SE) and Extreme Control version 22.3 or later
- DHCP/DNS server reachable on the existing Fabric Connect network
- An active Extreme Cloud IQ account for XIQ-SE, used for onboarding and changing switch persona from EXOS to VOSS/Fabric Engine

## Overview

---

### Objectives

This document describes the procedure to automate the deployment of a VSP switch using a combination VSP Fabric Connect automation features and XIQ-SE/Extreme Control automation features. In particular, the guide describes the following tasks.

- XIQ-SE preparation for a successful VSP switch automated, zero-touch deployment
- VSP ZTP+ provisioning automation
- UniversalHardware switch OS conversion from EXOS/Switch Engine to VOSS/Fabric Engine via XIQ or XIQ-SE
- VSP Zero-Touch-Fabric and port auto-sense functionality

#### Note

As of VOSS 8.6, the OS running on Universal Hardware switches has been re-branded to Fabric Engine and the switch is no longer referred to as a VSP switch, but as a Fabric Engine switch. This change only applies to Universal Hardware and Non-Universal Hardware running VOSS (VSP4900) will still be referred to as VSP switches.

Likewise, Universal Hardware running EXOS 31.6 or later has been rebranded to Switch Engine in place EXOS.

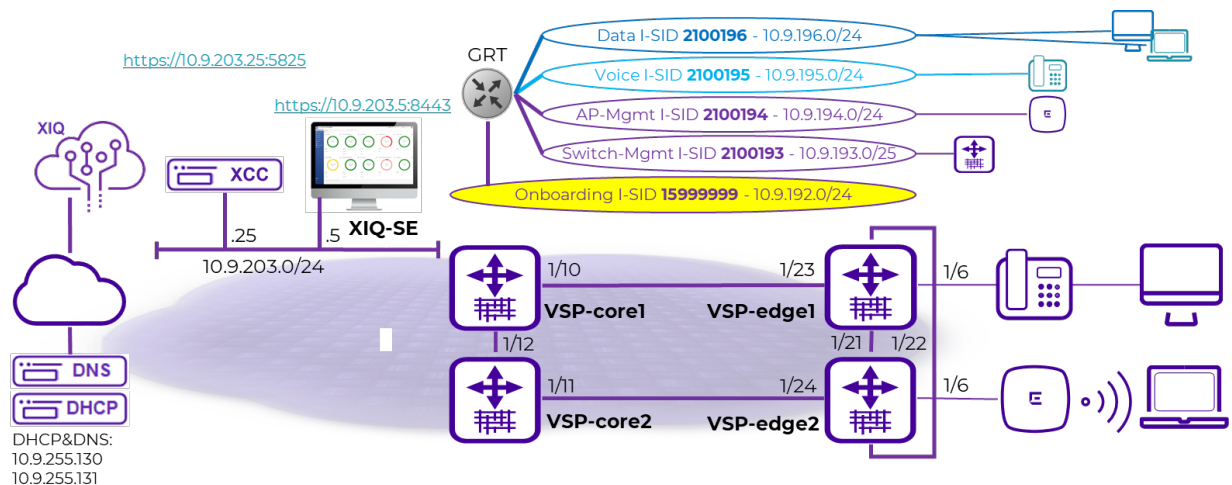
Throughout this guide the name VSP Edge and Fabric Engine Edge can be used interchangeably.



## Network Diagram

This guide uses the following network setup as an example of a typical VSP edge customer deployment. In particular it consists of the following devices:

- Two VSP core/distribution switches running VOSS 8.3 or later code. These switches represent an existing customer fabric connect deployment.
- Two Universal Edge 5520 VSP switches. In reality, any VSP switch will work as an edge switch as long as it supports VOSS 8.3 or later.
- One IP phone; Mitel 6920 model
- One Extreme Wireless AP; model AP505i
- One client VM acting as a wired client connected to the IP phone
- One XIQ-SE instance running 21.11 or later software, and one Extreme Control NAC appliance running the same version
- One Extreme Campus Controller (XCC) VM appliance
- ExtremeCloud IQ (XIQ) user account for onboarding the Universal Edge switches



It is assumed in this guide that the two VSP core switches have already been deployed and are part of an existing fabric network and reachable by XIQ-SE. This guide focuses on describing the additional configuration necessary to successfully onboard the VSP edge switches from a “factory default” condition where each edge switch does not have an existing configuration file present on the internal flash. The edge switches will use XIQ-SE ZTP+ and the VOSS Zero Touch Fabric functionality to achieve a typical VSP Edge deployment with the following characteristics:

- No SMLT Clustering (MLAG) of the core nodes
- Use of DVR Controller on the core nodes and DVR Leaf on the VSP edge

- Use of Zero Touch Fabric as an alternative to edge switch stacking
- Complete automation of VSP Edge deployment

The VSP edge switches have no Out of Band (OOB) management connection. All management of the edge switches will be via an inband IP address which is typical in campus VSP edge switch deployments.

At the end of the deployment, all connected endpoints (IP phone, AP, client) will be operational without any manual configuration on the VSP Edge switches including the access ports.

Some initial fabric “seed” configuration will be required on the VSP core, and this guide covers that configuration in detail. But the real gains of Zero Touch Fabric are reaped when deploying the large quantities of edge access switches in any fabric design.

The network diagram above shows both the physical fabric topology as well as the logical fabric topology. The logical topology consists of five L2VSNs and each is allocated a corresponding I-SID and IP subnet.

The onboarding I-SID 15999999 is a special I-SID and should be unique across the fabric network. The onboarding I-SID is the default I-SID that a newly unboxed VSP (with no configuration file) will always use when onboarding itself once it has joined the existing fabric.

All these L2VSNs will be IP routed in the base GRT (VRF-0) of the core VSPs and edge DVR-Leaf nodes. Use of VRFs and L3VSNs is of course possible but will not be covered in this guide because the deployment procedure is similar to the GRT scenario.

# Preexisting Configuration Review

## XIQ-SE Preexisting Configuration Review

The objective of this guide is to focus on the Fabric VSP Edge deployment and the steps required to achieve that. Therefore, it is assumed that any unrelated XIQ-SE configuration has already been done and this section simply explains what the customer will need to pre-configure on XIQ-SE.

As an example, the Building1 and Building2 sites have already been configured:

The screenshot shows the ExtremeCloud IQ Site Engine interface. The left sidebar has a 'Network' tab highlighted with a red box and the number '1'. The main area has a 'Devices' tab highlighted with a red box and the number '2'. Below the 'Devices' tab, there is a 'World' site selected, which contains two sub-sites: 'Building1' and 'Building2', both highlighted with a red box. To the right, a table lists the configured devices:

Device Status	Status	Name	Site	IP Address
●	●	Fabric	/World	10.9.203.7
●	●	NAC	/World	10.9.203.6
●	●	VSP-core1	/World	10.9.193.131
●	●	VSP-core2	/World	10.9.193.132

A map of the same name is already defined for each site and the corresponding map has already been set under the site Actions “add to Map” option.

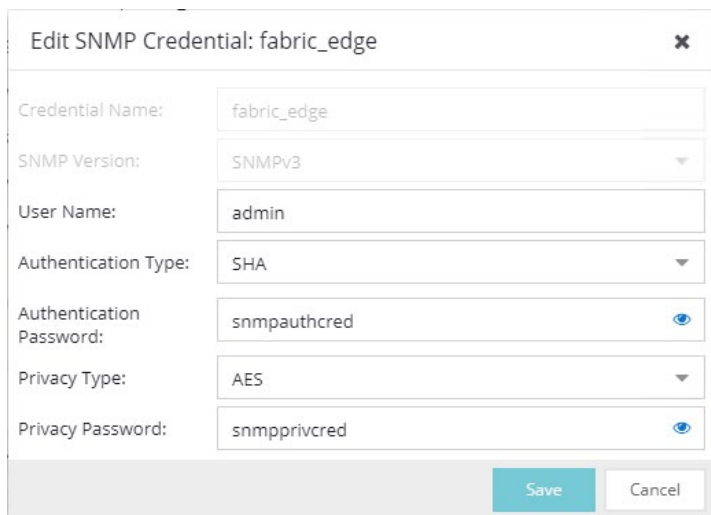
The VSP core switches will initially be found under the World Site.

Under Administration, the admin profile “Fabric Edge” has been defined to manage the switches, as shown here:

The screenshot shows the ExtremeCloud IQ Site Engine interface with the 'Administration' tab highlighted with a red box and the number '1'. The 'Profiles' tab is highlighted with a red box and the number '2'. Below the 'Profiles' tab, there is a table listing the configured profiles:

Name	SNMP Version	Read Credential	Write Credential	Max Access Credential	Read Security Level	Write Security Level	Max Access Security Level	CLI Credential
public_v2_Profile	SNMPv2	public_v2	public_v2	public_v2				Default
EXTR_v2_Profile	SNMPv2	public_v2	private_v2	private_v2				Default
snmp_v3_profile	SNMPv3	default_snmp_v3	default_snmp_v3	default_snmp_v3	AuthPriv	AuthPriv	AuthPriv	Default
VOSS_v1_Profile	SNMPv1	public_v1	private_v1	private_v1				Default RWA
BOSS_ESM_v1_Profile	SNMPv1	public_v1	private_v1	private_v1				Default BOSS ESM
BOSS_4800_v1_Profile	SNMPv1	public_v1	private_v1	private_v1				Default BOSS 48...
BOSS_v1_Profile	SNMPv1	public_v1	private_v1	private_v1				Default BOSS
VOSS_v2_Profile	SNMPv2	public_v2	private_v2	private_v2				Default RWA
BOSS_ESM_v2_Profile	SNMPv2	public_v2	private_v2	private_v2				Default BOSS ESM
BOSS_4800_v2_Profile	SNMPv2	public_v2	private_v2	private_v2				Default BOSS 48...
BOSS_v2_Profile	SNMPv2	public_v2	private_v2	private_v2				Default BOSS
san_security_profile	SNMPv1	public_v1	public_v1	public_v1				SAN Security
Servers	SNMPv3	default_snmp_v3	default_snmp_v3	default_snmp_v3	AuthPriv	AuthPriv	AuthPriv	Server
Fabric Edge	SNMPv3	fabric_edge	fabric_edge	< No Access >	AuthPriv	AuthPriv	NoAuthNoPriv	FabricEdge

This admin profile uses the following SNMP credentials:

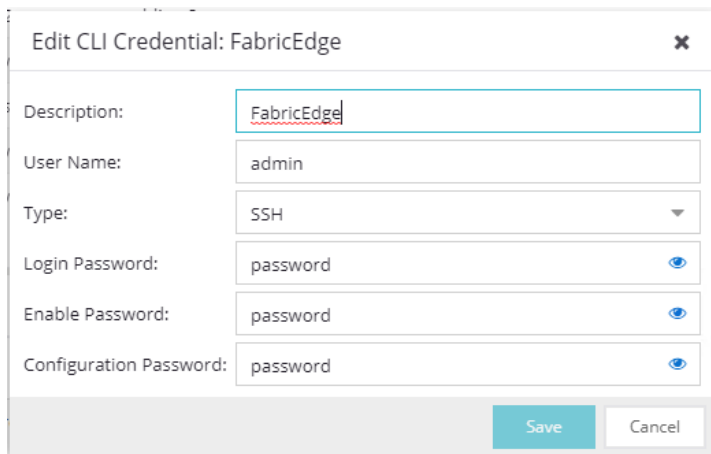


The dialog box titled "Edit SNMP Credential: fabric\_edge" contains the following fields:

Credential Name:	fabric_edge
SNMP Version:	SNMPv3
User Name:	admin
Authentication Type:	SHA
Authentication Password:	snmpauthcred
Privacy Type:	AES
Privacy Password:	snmpprivcred

At the bottom right are "Save" and "Cancel" buttons.

This admin profile uses the following CLI credentials:



The dialog box titled "Edit CLI Credential: FabricEdge" contains the following fields:

Description:	FabricEdge
User Name:	admin
Type:	SSH
Login Password:	password
Enable Password:	password
Configuration Password:	password

At the bottom right are "Save" and "Cancel" buttons.

These are non-default credentials, so ZTP+ will configure these credentials on the VSP edge switch when it is onboarded for the first time.

Under XIQ-SE Network, Topology definitions, the following Fabric Connect Topology settings are configured:

The screenshot shows the Network Configuration interface. On the left sidebar, the 'Network' tab is selected (1). The main panel shows the 'Fabric Connect' configuration. The 'Fabric Infrastructure Settings' section includes a table with the following values:

IS-IS Manual Area:	49.0000
Primary BVLAN:	4051
Secondary BVLAN:	4052

The 'DvR Domain Settings' section includes a table with the following values:

Name	Domain ID
Domain1	1

The 'Features' section includes checkboxes for Multicast, IP Shortcuts, and IPv6 Shortcuts.

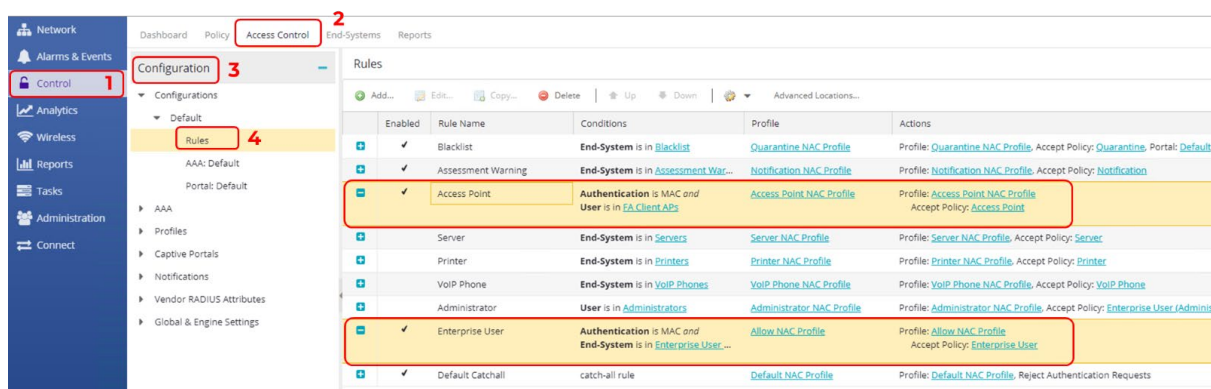
And the settings are assigned to both the Building1 and Building2 sites.

The screenshot shows the Network Configuration interface. On the left sidebar, the 'Network' tab is selected (1). The main panel shows the 'Building1' configuration (2). The 'Fabric' section includes a table with the following values:

Topology Definition:	Fabric Connect
DvR Domain ID:	Domain1

As mentioned, this guide assumes that both VSP core nodes are already configured for Fabric Connect. When onboarding the VSP edge switches, the “Onboard VSP” workflow will automatically convert the VSP edge switches to DVR Leaf nodes. However, for this to happen, the workflow must be able to read the DVR Domain ID from the site.

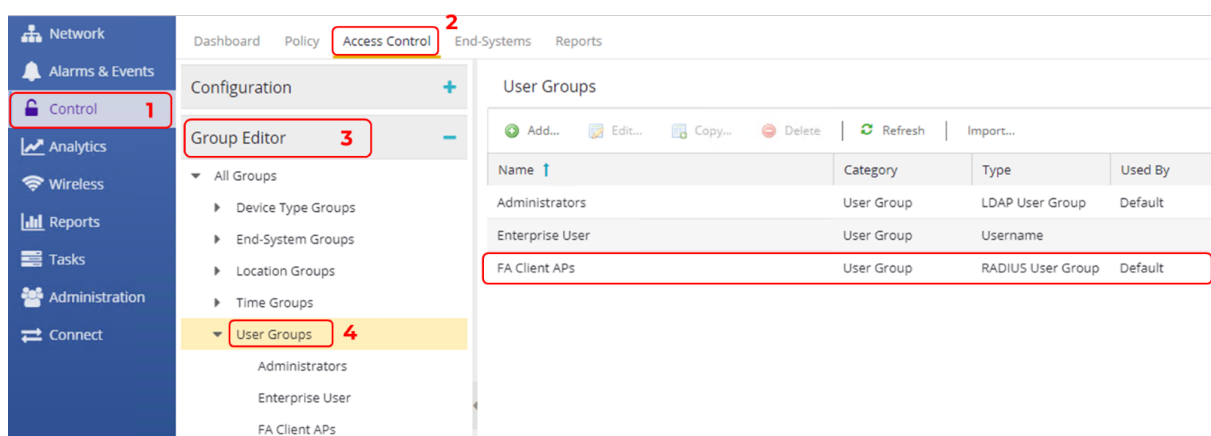
On the XIQ-SE Control, Access Control tab, in the Configuration section, the following rules will be used for authenticating the PC client and onboarding the Wireless AP:



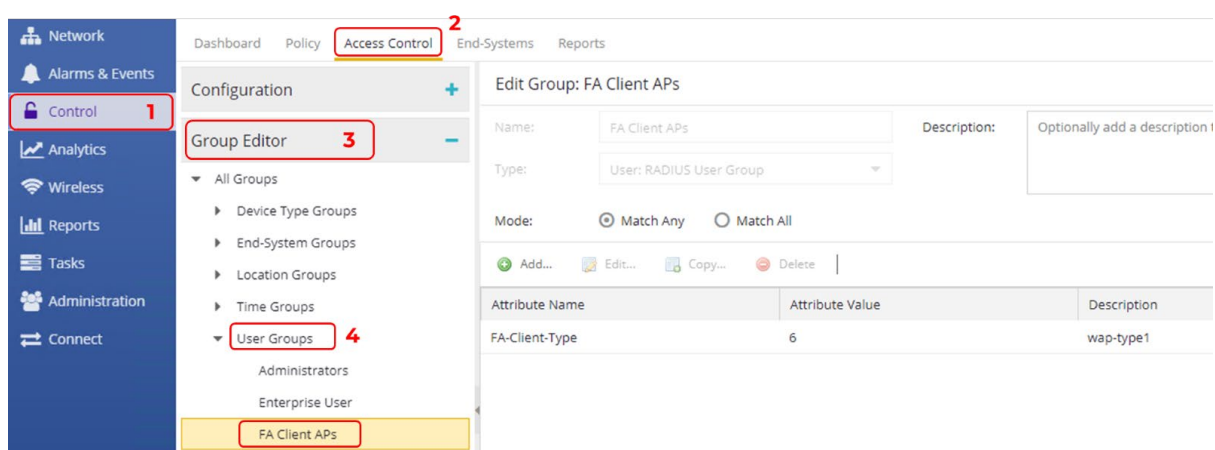
The Access Point rule will be used to MAC authenticate the WLAN APs using inbound RADIUS FA attributes.

Note that in this guide, MAC authentication is used for the Windows PC client. In reality, the Enterprise User rule would typically be an 802.1X authentication rule.

Under the Group Editor section, the user group “FA Client APs” has been defined:

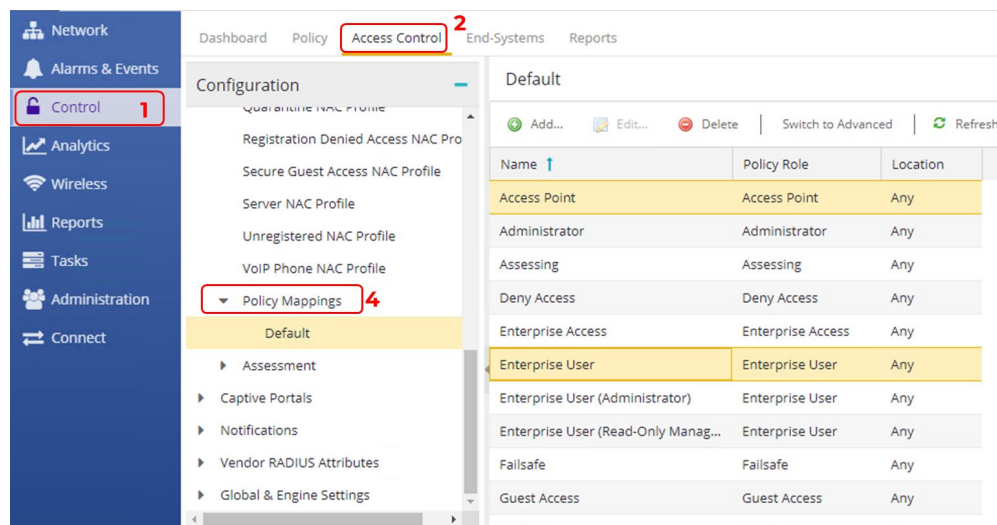


This user group has the following RADIUS attribute defined :



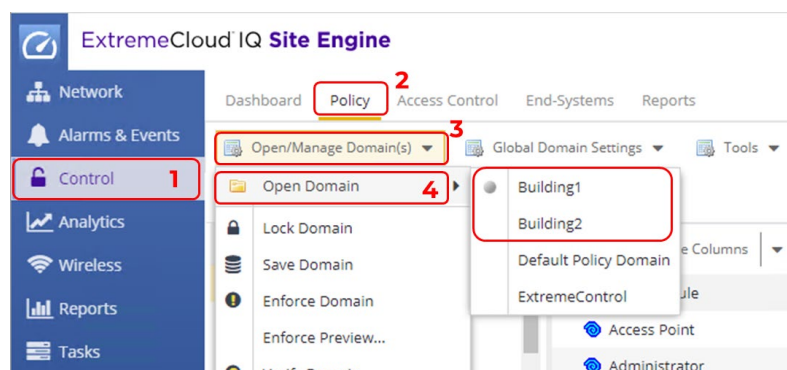
This user group will allow easier and more secure authentication of the AP based on its FA Client inbound RADIUS attributes (instead of having to base the authentication solely on the AP's MAC address).

The Access Point and Enterprise User rules contain the policy mappings shown below. The mappings can be found under the Configuration section, Profiles, Policy Mappings sub-folder:



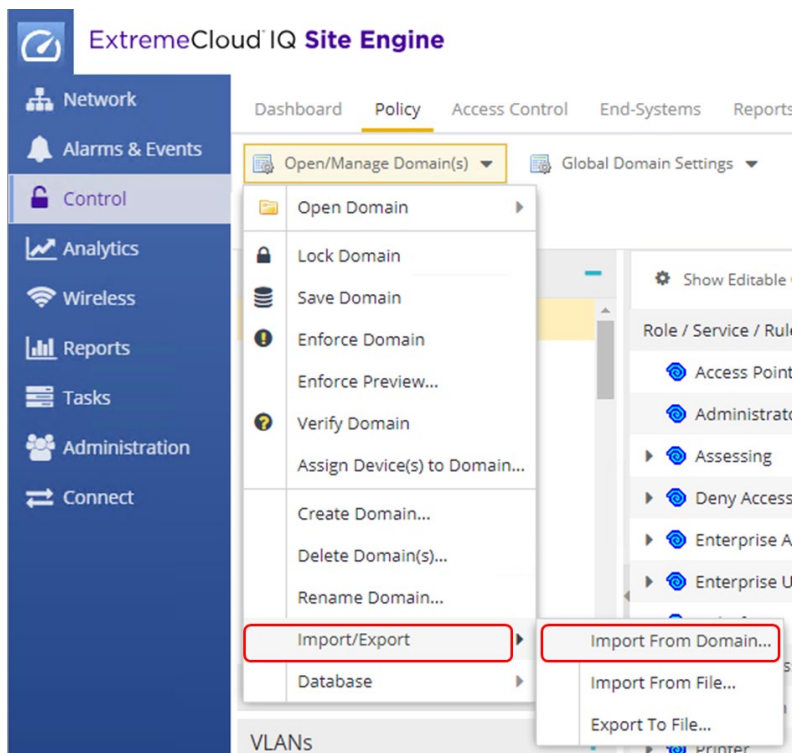
These policy mappings can be used to directly set the returned RADIUS attributes such as vlan/i-sid bindings, but the best practice is to use the Policy configuration tab to define the returned RADIUS attributes. Because Policy will be used in this guide, the above entries are simply mapping the Access Control rules to Policy roles configured within the XIQ-SE Policy framework.

The Policy framework is configured on the Policy tab. Two Policy domains are created: Building1 and Building2, as shown below.

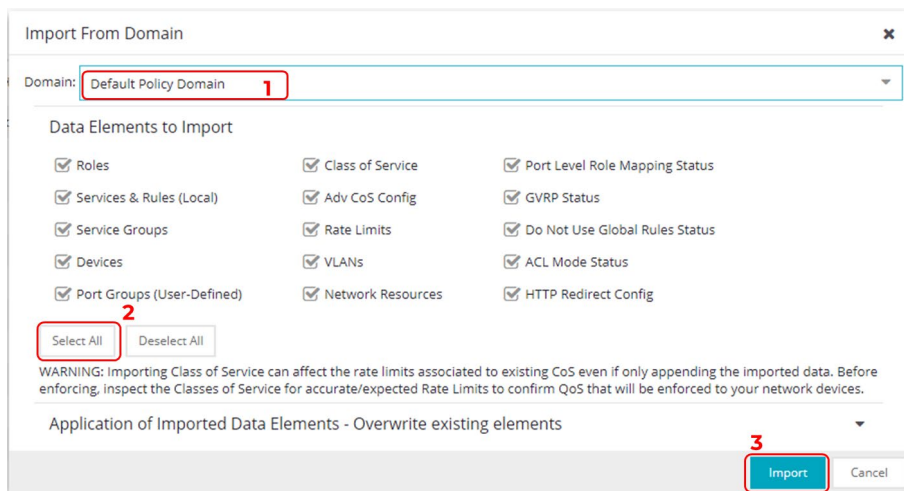


These Policy definitions, are cloned from the “Default Policy Domain” using the “Import/Export, Import from Domain” wizard.





All settings are imported from the “Default Policy Domain.”



As shown below, the following changes are made to the Building1 and Building2 policy domains.

For the Access Point policy role, only the I-SID value is changed, and the VLAN-id is the same for both locations. Also, the “AP Aware” parameter is left at the default value of “Enabled.” This setting will enable Extreme Control to send the necessary outbound attribute to enable MHSa (Multiple Host Single Authentication) on the switch access port where the AP is authenticated.



Domain: Building1

Roles/Services

- Roles
  - Access Point
  - Administrator
  - Assessing
  - Deny Access
  - Enterprise Access
  - Enterprise User
  - Failsafe
  - Guest Access
- Class of Service
- VLANs
- Network Resources

Role: Access Point

General

Name: Access Point

Description: The Access Point role is useful for B@AP topology. When this role

TCI Overwrite: Disabled

Default Actions

Access Control: Contain to VLAN

VLAN: 194[AP-Mgmt]

Service ID: 2100194

AP Aware: Enabled

Domain: Building2

Roles/Services

- Roles
  - Access Point
  - Administrator
  - Assessing
  - Deny Access
  - Enterprise Access
  - Enterprise User
  - Failsafe
  - Guest Access
- Class of Service
- VLANs
- Network Resources

Role: Access Point

General

Name: Access Point

Description: The Access Point role is useful for B@AP topology. When this role

TCI Overwrite: Disabled

Default Actions

Access Control: Contain to VLAN

VLAN: 194[AP-Mgmt]

Service ID: 2200194

AP Aware: Enabled

For the Enterprise User policy role, again note that only the I-SID value is changed, and the VLAN-id is the same for both locations.

Domain: Building1

Roles/Services

- Roles
  - Access Point
  - Administrator
  - Assessing
  - Deny Access
  - Enterprise Access
  - Enterprise User
  - Failsafe
  - Guest Access
- Class of Service
- VLANs
- Network Resources

Role: Enterprise User

General

Name: Enterprise User

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

TCI Overwrite: Disabled

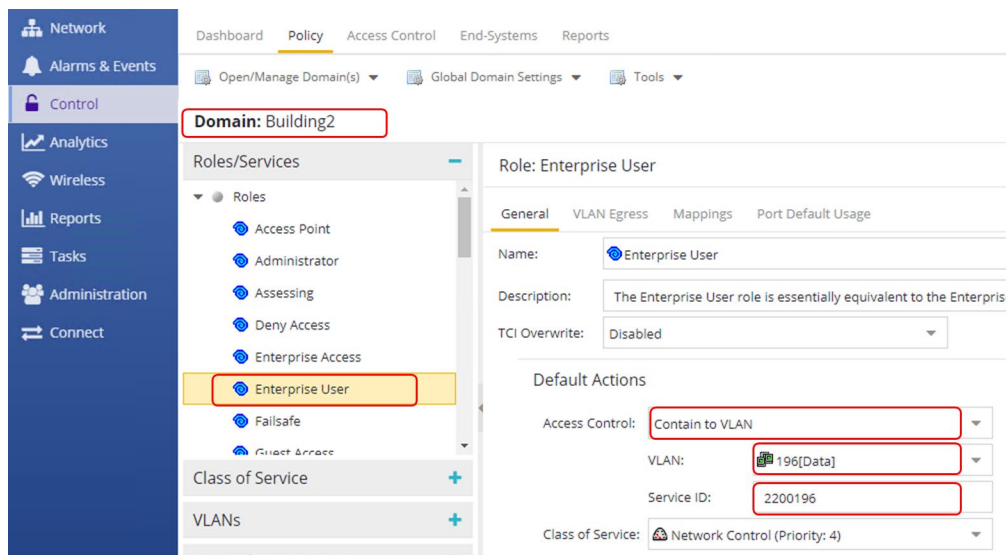
Default Actions

Access Control: Contain to VLAN

VLAN: 196[Data]

Service ID: 2100196

Class of Service: Network Control (Priority: 4)

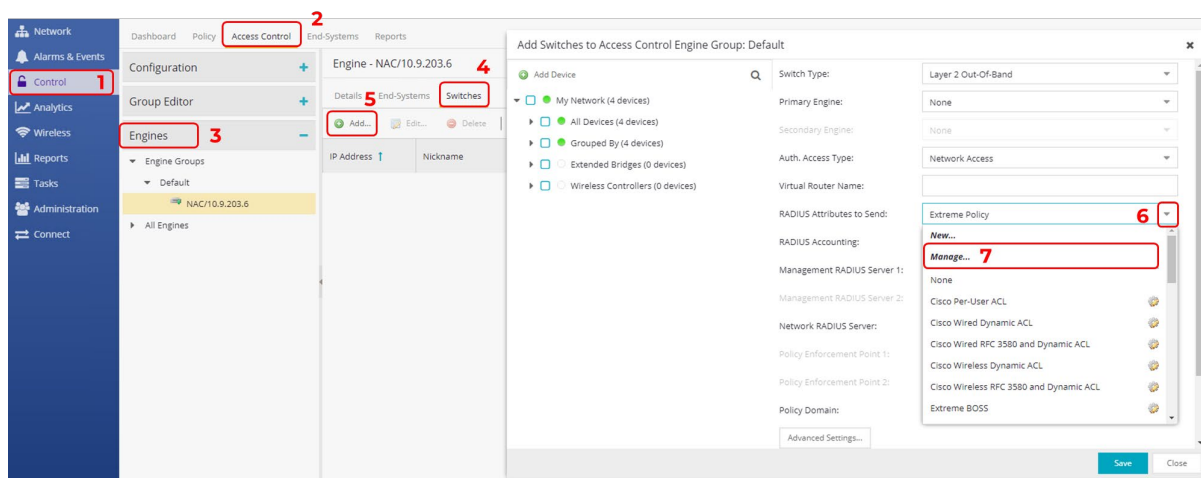


As of XIQ-SE 21.11 it is no longer necessary to configure a custom RADIUS attribute template. Default templates have been added for Policy and non-Policy NAC scenarios. As mentioned before, the best practice is to use Policy to configure Radius outbound attributes. In the default templates shown below, for Policy scenarios use the “Extreme VOSS-Per User ACL” template and for non-Policy scenarios use the “Extreme VOSS-Fabric Attach” template. Because this guide uses Policy, the “Extreme VOSS-Per User ACL” is used.

Name	Attributes
Extreme NetLogin - VLAN ID	Extreme-Netlogin-Extended-Vlan=%VLAN_EGRESS%%VLAN_ID%,Extreme-Security-Profile=%PORT_P...
Extreme NetLogin - VLAN Name	Extreme-Netlogin-Extended-Vlan=%VLAN_EGRESS%%VLAN_NAME%,Extreme-Security-Profile=%POR...
Extreme Policy	Filter-Id=Enterasys:version=1:%MANAGEMENT%policy=%POLICY_NAME%,Service-Type=%MGMT_SE...
Extreme Policy - Fabric Attach	Filter-Id=Enterasys:version=1:%MANAGEMENT%policy=%POLICY_NAME%,FA-VLAN-ISID=%VLAN_ID...
Extreme VOSS	Tunnel-Private-Group-Id=%VLAN_ID%%VLAN_TUNNEL_TAG%,Tunnel-Type=13:%VLAN_TUNNEL_TA...
Extreme VOSS - Fabric Attach	FA-VLAN-ISID=0:%CUSTOM1%,Passport-Access-Priority=%MGMT_SERV_TYPE%
Extreme VOSS - Fabric Attach - EPT	FA-VLAN-ISID=%VLAN_ID%:0,FA-VLAN-ISID=%VLAN_ID%:%CUSTOM1%,Passport-Access-Priority=%M...
Extreme VOSS - Per-User ACL	Filter-Id=%POLICY_NAME%,Passport-Access-Priority=%MGMT_SERV_TYPE%,%PER_USER_ACL_VOSS%
Extreme VOSS Per-User ACL	%PER_USER_ACL_VOSS%
Extreme XNV - VLAN ID	Extreme-VM-VLAN-ID=%VLAN_ID%,Extreme-VM-VPP-Name=%PORT_PROFILE%,Extreme-VM-VR-Nam...

These RADIUS templates can be viewed (or created) when a switch is added or edited under the Access Control tab, Engines section, Switches sub-tab.

If no switches exist, simply click Add as if to add a first switch. Then use the “RADIUS Attributes to Send” drop-down and select the “Manage...” option.



## XIQ-SE: Script and Workflow Review

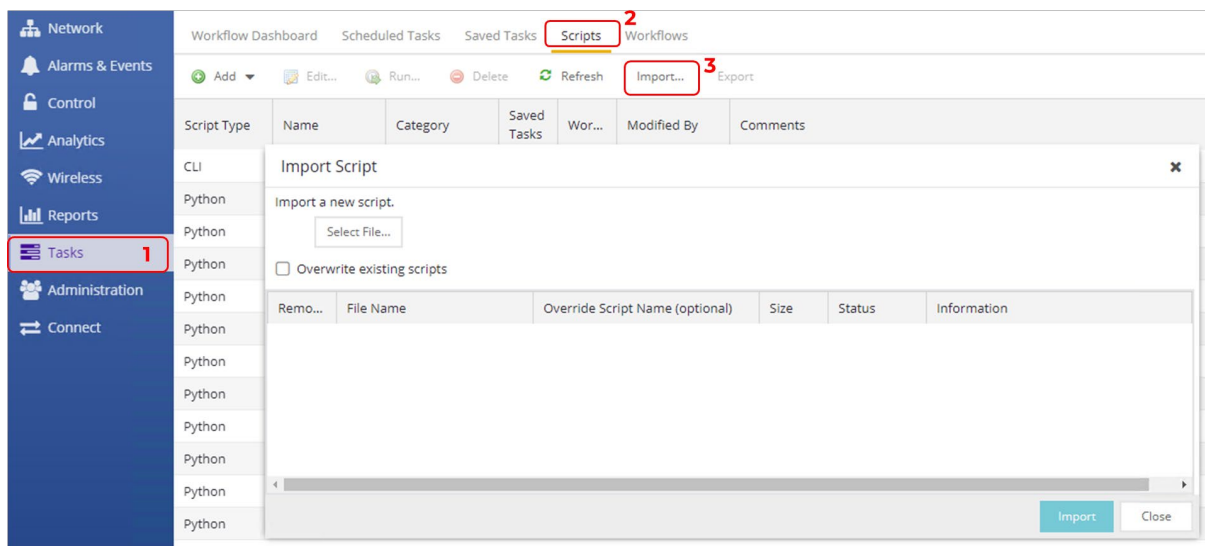
This deployment guide makes use of following scripts and workflows which do not ship with XIQ-SE but are provided on GitHub.

Name	Type	GitHub URL
Move to CLIP Mgmt IP	Script	<a href="https://github.com/extremenetworks/ExtremeScripting/tree/master/XMC_XIQ-SE/oneview_CLI_scripts">https://github.com/extremenetworks/ExtremeScripting/tree/master/XMC_XIQ-SE/oneview_CLI_scripts</a>
Change the persona to EXOS	Workflow	<a href="https://github.com/extremenetworks/ExtremeScripting/tree/master/XMC_XIQ-SE/oneview_workflows">https://github.com/extremenetworks/ExtremeScripting/tree/master/XMC_XIQ-SE/oneview_workflows</a>
Change the persona to VOSS	Workflow	<a href="https://github.com/extremenetworks/ExtremeScripting/tree/master/XMC_XIQ-SE/oneview_workflows">https://github.com/extremenetworks/ExtremeScripting/tree/master/XMC_XIQ-SE/oneview_workflows</a>
Onboard VSP	Workflow	<a href="https://github.com/extremenetworks/ExtremeScripting/tree/master/XMC_XIQ-SE/oneview_workflows">https://github.com/extremenetworks/ExtremeScripting/tree/master/XMC_XIQ-SE/oneview_workflows</a>

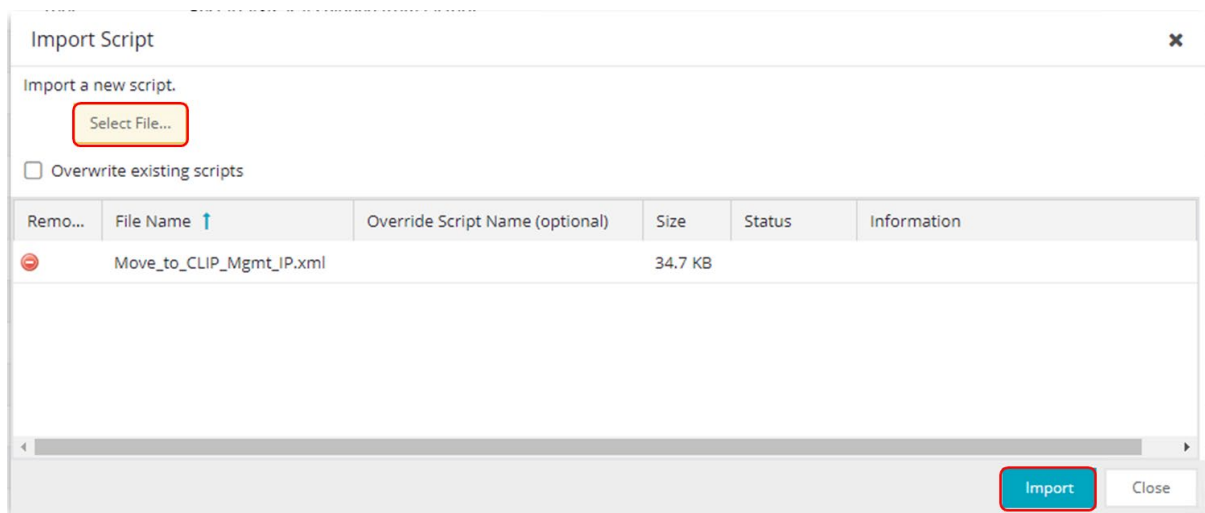
The following examples show how to download and install these scripts and workflows into XIQ-SE.

Download the script you want, for example “Move to CLIP Mgmt IP,” using right-click and then “Save link as...”

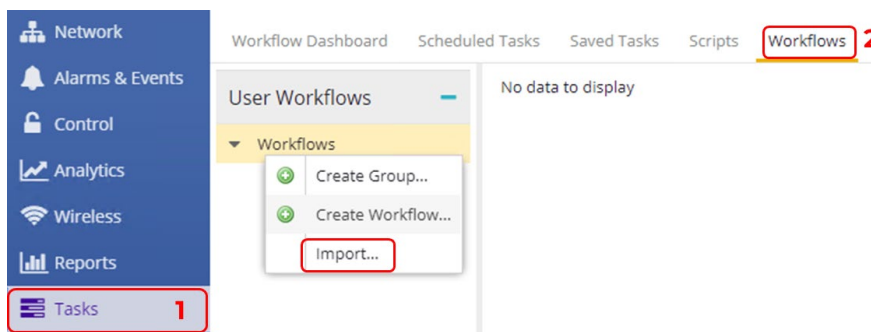
Then import the script into XIQ-SE using Tasks > Scripts > Import ...



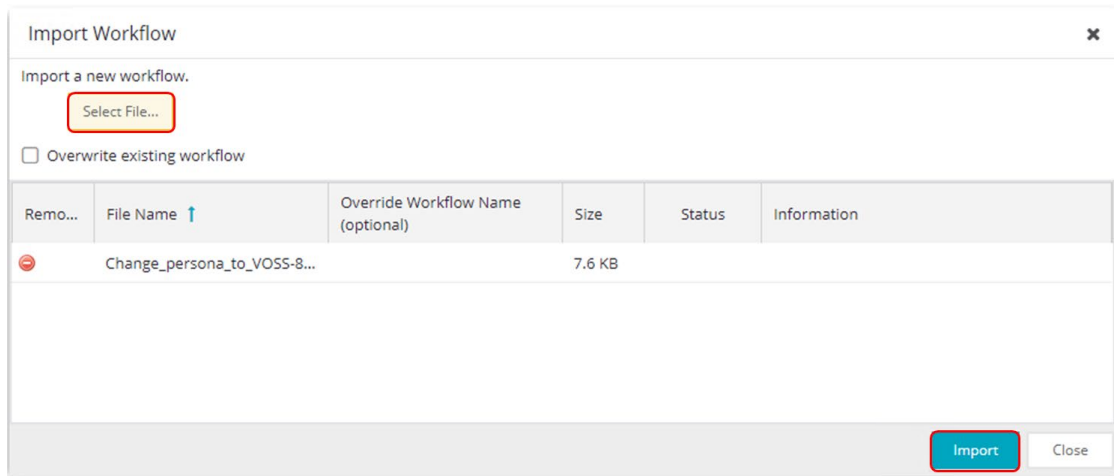
Then select the XML file downloaded from GitHub, click the Import button, then Close.



Similarly, you can download the workflow named “ZTP+ Change the persona to VOSS” and then import it under XIQ-SE > Tasks > Workflows.

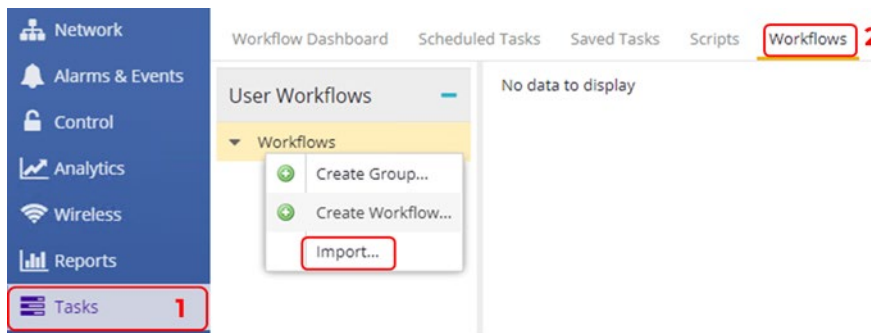


The file just downloaded is selected, followed by Import and then Close.

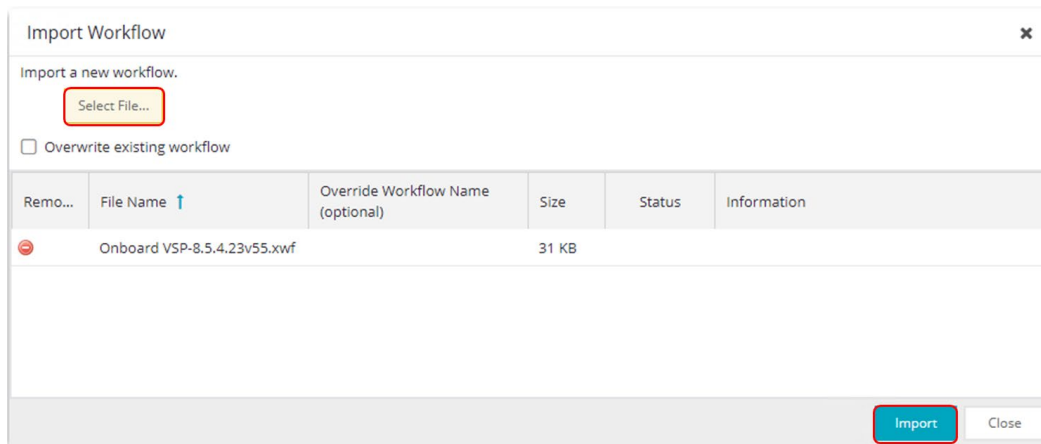


Similar steps are used to import the workflow “Change persona to EXOS.”

Finally, you can download the workflow “Onboard VSP” and then import it under XIQ-SE > Tasks > Workflows.



Select the downloaded file, click Import, and then click Close.

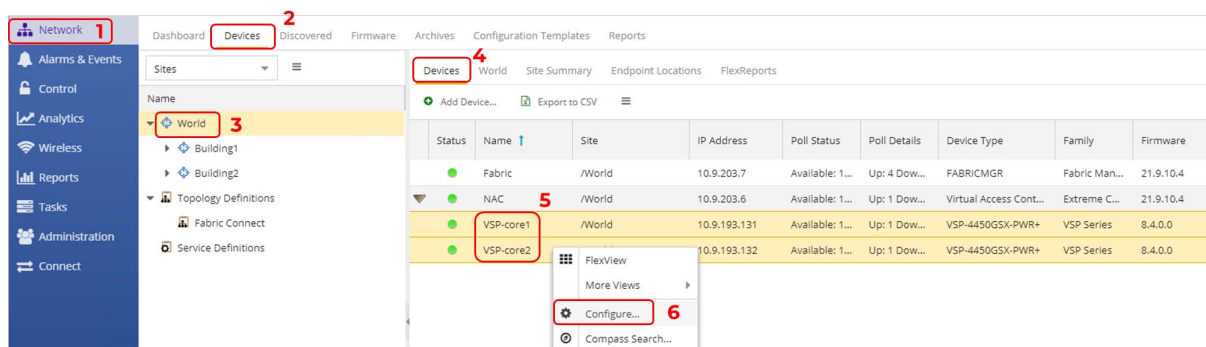


# Prepare VSP Core Switches for Automated VSP Edge

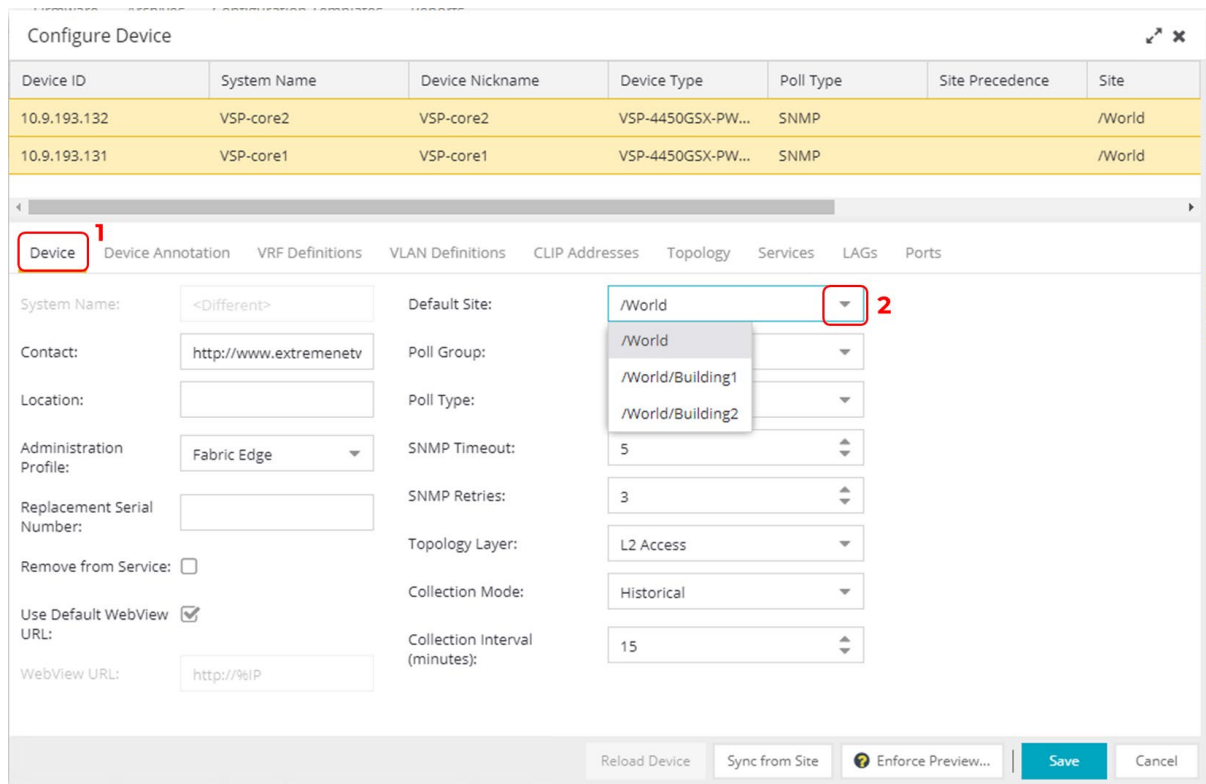
## Site Selection for VSP Core Switches

Even though we show two sites in XIQ-SE (Building1 and Building2), this guide illustrates how to deploy the core and edge switches in Building1 only. Building2 is shown as an example of a typical customer deployment where multiple sites exist.

Navigate to the Network, Devices tab, World site. Select both VSP core switches, right-click, and select Configure.

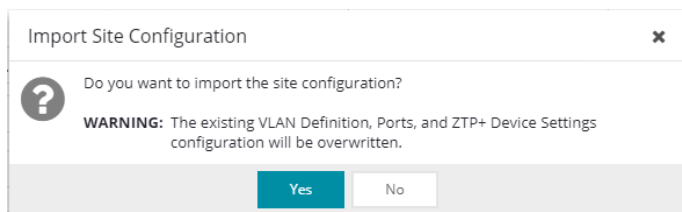


Assign both switches to the Building1 site.



In the confirmation pop-up, select Yes.





Then select Save to commit.

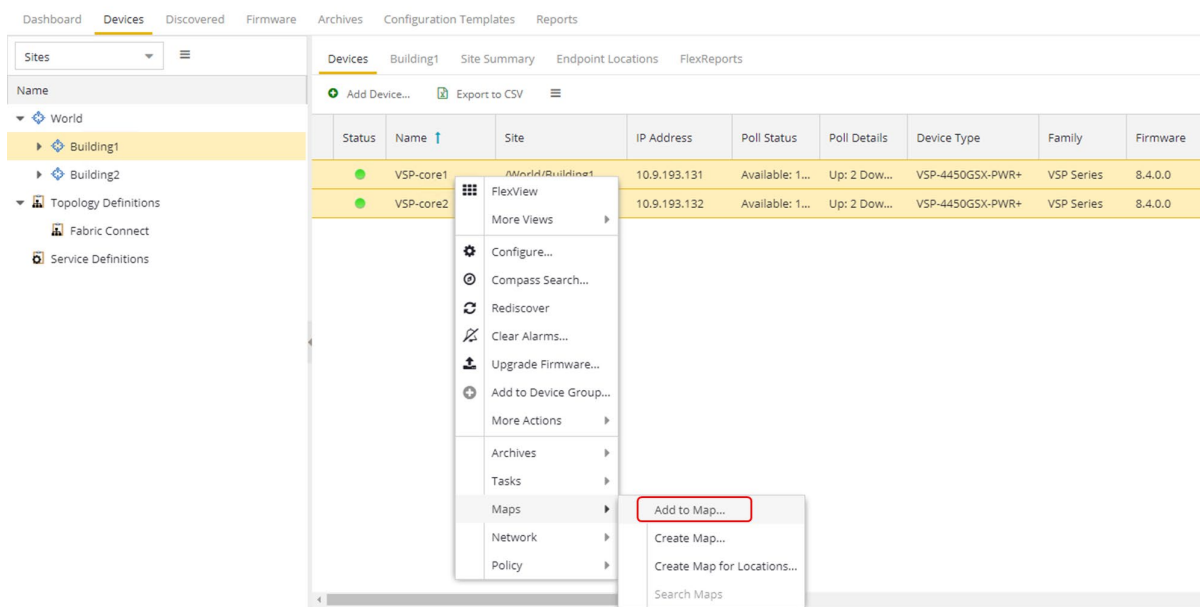
Now navigate to the Building1 site that was selected and make sure both VSP cores have been added.

Dashboard Devices Discovered Firmware Archives Configuration Templates Reports									
Sites									
Name									
World									
Building1									
Building2									
Topology Definitions									
Fabric Connect									
Service Definitions									

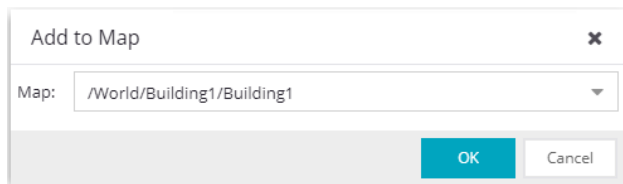
  

Dashboard Devices Discovered Firmware Archives Configuration Templates Reports									
Devices Building1 Site Summary Endpoint Locations FlexReports									
Add Device... Export to CSV									
Status	Name	Site	IP Address	Poll Status	Poll Details	Device Type	Family	Firmware	
●	VSP-core1	/World/Building1	10.9.193.131	Available: 1...	Up: 2 Dow...	VSP-4450GSX-PWR+	VSP Series	8.4.0.0	
●	VSP-core2	/World/Building1	10.9.193.132	Available: 1...	Up: 2 Dow...	VSP-4450GSX-PWR+	VSP Series	8.4.0.0	

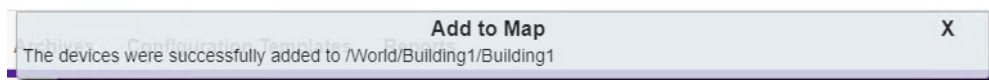
Next, right-click on both VSP cores again and select Maps > Add to Map...



Then enter the Building site that was chosen and select OK.



The VSP cores have now been added to the map.



## Apply DVR Controller, VLAN, and IP Config

The VSP cores will need to route IP traffic across a number of VLAN/L2VSNs. These VLANs do not exist on the VSP cores and need to be created.

Because the VSP edge switches will be onboarded as DVR Leaf nodes, the VSP cores will also need to be configured as DVR Controllers and a DVR-GW IP will be configured on the Voice and Data VLANs. VRRP will be used on the Switch-Mgmt and AP-Mgmt VLANs.

The above configuration will be performed using SSH CLI.

Open an SSH session to both VSP cores and paste the following commands.



## Building 1

## VSP-Core1

```

enable
config term
dvr controller 1

vlan create 193 name "Switch-Mgmt" type port-mstprstp 0
vlan i-sid 193 2100193
i-sid name 2100193 "Building1-Switch-Mgmt"
interface Vlan 193
    ip address 10.9.193.2/25
    ip vrrp version 3
    ip vrrp address 193 10.9.193.1
    ip vrrp 193 enable
exit
slpp vid 193

vlan create 194 name "AP-Mgmt" type port-mstprstp 0
vlan i-sid 194 2100194
i-sid name 2100194 "Building1-AP-Mgmt"
interface Vlan 194
    ip address 10.9.194.2/24
    ip vrrp version 3
    ip vrrp address 194 10.9.194.1
    ip vrrp 194 enable
    ip dhcp-relay
    ip dhcp-relay fwd-path 10.9.255.130
    ip dhcp-relay fwd-path 10.9.255.130 enable
    ip dhcp-relay fwd-path 10.9.255.131
    ip dhcp-relay fwd-path 10.9.255.131 enable
    ip dhcp-relay fwd-path 10.9.203.6
    ip dhcp-relay fwd-path 10.9.203.6 enable
exit
slpp vid 194

vlan create 195 name "Voice" type port-mstprstp 0
vlan i-sid 195 2100195
i-sid name 2100195 "Building1-Voice"
interface Vlan 195
    dvr gw-ipv4 10.9.195.1
    dvr enable
    ip address 10.9.195.2/24
    ip dhcp-relay
    ip dhcp-relay fwd-path 10.9.255.130
    ip dhcp-relay fwd-path 10.9.255.130 enable
    ip dhcp-relay fwd-path 10.9.255.131
    ip dhcp-relay fwd-path 10.9.255.131 enable
    ip dhcp-relay fwd-path 10.9.203.6
    ip dhcp-relay fwd-path 10.9.203.6 enable
exit
slpp vid 195

vlan create 196 name "Data" type port-mstprstp 0
vlan i-sid 196 2100196
i-sid name 2100196 "Building1-Data"
interface Vlan 196
    dvr gw-ipv4 10.9.196.1
    dvr enable
    ip address 10.9.196.2/24
    ip dhcp-relay
    ip dhcp-relay fwd-path 10.9.255.130
    ip dhcp-relay fwd-path 10.9.255.130 enable
    ip dhcp-relay fwd-path 10.9.255.131
    ip dhcp-relay fwd-path 10.9.255.131 enable
    ip dhcp-relay fwd-path 10.9.203.6
    ip dhcp-relay fwd-path 10.9.203.6 enable
exit
slpp vid 196
slpp enable
end

```

## VSP-Core2

```

enable
config term
dvr controller 1

vlan create 193 name "Switch-Mgmt" type port-mstprstp 0
vlan i-sid 193 2100193
i-sid name 2100193 "Building1-Switch-Mgmt"
interface Vlan 193
    ip address 10.9.193.3/25
    ip vrrp version 3
    ip vrrp address 193 10.9.193.1
    ip vrrp 193 enable
exit
slpp vid 193

vlan create 194 name "AP-Mgmt" type port-mstprstp 0
vlan i-sid 194 2100194
i-sid name 2100194 "Building1-AP-Mgmt"
interface Vlan 194
    ip address 10.9.194.3/24
    ip vrrp version 3
    ip vrrp address 194 10.9.194.1
    ip vrrp 194 enable
    ip dhcp-relay
    ip dhcp-relay fwd-path 10.9.255.130
    ip dhcp-relay fwd-path 10.9.255.130 enable
    ip dhcp-relay fwd-path 10.9.255.131
    ip dhcp-relay fwd-path 10.9.255.131 enable
    ip dhcp-relay fwd-path 10.9.203.6
    ip dhcp-relay fwd-path 10.9.203.6 enable
exit
slpp vid 194

vlan create 195 name "Voice" type port-mstprstp 0
vlan i-sid 195 2100195
i-sid name 2100195 "Building1-Voice"
interface Vlan 195
    dvr gw-ipv4 10.9.195.1
    dvr enable
    ip address 10.9.195.3/24
    ip dhcp-relay
    ip dhcp-relay fwd-path 10.9.255.130
    ip dhcp-relay fwd-path 10.9.255.130 enable
    ip dhcp-relay fwd-path 10.9.255.131
    ip dhcp-relay fwd-path 10.9.255.131 enable
    ip dhcp-relay fwd-path 10.9.203.6
    ip dhcp-relay fwd-path 10.9.203.6 enable
exit
slpp vid 195

vlan create 196 name "Data" type port-mstprstp 0
vlan i-sid 196 2100196
i-sid name 2100196 "Building1-Data"
interface Vlan 196
    dvr gw-ipv4 10.9.196.1
    dvr enable
    ip address 10.9.196.3/24
    ip dhcp-relay
    ip dhcp-relay fwd-path 10.9.255.130
    ip dhcp-relay fwd-path 10.9.255.130 enable
    ip dhcp-relay fwd-path 10.9.255.131
    ip dhcp-relay fwd-path 10.9.255.131 enable
    ip dhcp-relay fwd-path 10.9.203.6
    ip dhcp-relay fwd-path 10.9.203.6 enable
exit
slpp vid 196
slpp enable
end

```

Open XIQ-SE Device View against both core VSPs, and verify that the VLANs and L2VSNs have been configured.

The screenshot displays the configuration for VSP-core1. On the left, a sidebar shows the device details: Universal Platform Fabric Engine 5520-12MW-36W-FabricEngine (3 modules), Slot 1 5520-12MW-36W-FabricEngine, Slot 2 5520-VIM-4YE. The main content area is divided into two tabs: 'VLAN Table' and 'I-SID L2VSN'.

**VLAN Table**

IP Address	Instance	System Name	VLAN ID	VLAN Name	Status	VLAN Status	VLAN Spanning Tree MSTP ID	VLAN I-SID Mapping	VLAN Type	VLAN Color	Virtual Router	VLAN Po
10.9.193.1...	1	VSP-core1	1	Default	active	active	1	0	byPort	0	0	256-259
10.9.193.1...	193	VSP-core1	193	Switch-Mgmt	active	active	1	2100193	byPort	0	0	
10.9.193.1...	194	VSP-core1	194	AP-Mgmt	active	active	1	2100194	byPort	0	0	
10.9.193.1...	195	VSP-core1	195	Voice	active	active	1	2100195	byPort	0	0	
10.9.193.1...	196	VSP-core1	196	Data	active	active	1	2100196	byPort	0	0	
10.9.193.1...	4051	VSP-core1	4051	B-VLAN-1	active	active	63	0	spbm-bvlan	0	0	203
10.9.193.1...	4052	VSP-core1	4052	B-VLAN-2	active	active	63	0	spbm-bvlan	0	0	203

**I-SID L2VSN**

IP Address	I-SID	I-SID Name	Service Type	Row Status	Service Status	Service Max MAC Limit	Service MAC Limit Enable	Service Origin	Service Action
10.9.193.131	2100193	Building1-5w...	I2vsn	active	active	-	-	config	none
10.9.193.131	2100194	Building1-AP...	I2vsn	active	active	-	-	config	none
10.9.193.131	2100195	Building1-Vo...	I2vsn	active	active	-	-	config	none
10.9.193.131	2100196	Building1-Data	I2vsn	active	active	-	-	config	none
10.9.193.131	16777001	FAN-I-SID	elan	active	active	-	-	config	none

## Apply Seed Config for Zero Touch Fabric

In order for the VSP edge switches to automatically join the fabric when they are connected to the VSP core nodes, the VSP core nodes need the following items configured.

1. **Nickname server:** Assigns Shortest Path Bridging (SPB) nicknames to VSP edge switches as they join the fabric. An SPB node needs a nickname to create multicast I-SID trees, which are used to transmit BUM (Broadcast/Unknown-unicast/Multicast) traffic in fabric VSNs. Without a nickname, a VSP edge switch cannot transmit a DHCP Discovery on the onboarding I-SID to get an IP address.

The VSP cores (or any pair of core/distribution VSPs) need to be set up as nickname servers. It is sufficient to have two nickname servers per fabric (as of VOSS 8.4, with multi-area support, a pair of nickname servers will be required per ISIS area). Both nickname servers can be set up to assign nicknames in the same prefix range or different ranges. The mechanism used by the nickname server to assign nicknames is essentially identical to how a DHCP server works with the exception that nicknames are assigned instead of IP addresses.

To enable nickname server functionality on a VSP, the VSP needs to be already configured with a static nickname (the VSP core switches were already pre-configured with a static nickname).

2. The **onboarding I-SID 15999999** must be set up on the core VSPs so that it can service DHCP requests, from the edge switches and from other onboarding devices. There are two options for configuring the onboarding I-SID:
  - a. One of the core VSPs is configured to simply bridge the onboarding I-SID onto an existing segment where DHCP is available.

However, this can be done only on one core VSP or else a loop is created. This approach will be unlikely in a typical customer deployment

- b. The onboarding I-SID is created into a new dedicated IP subnet for which both fabric cores will act as default gateways and DHCP-relay agent. This is the approach that will be used in the sandbox, because it is a better design approach. If the fabric cores were originally built from VOSS 8.2 or later, the default onboarding Private-VLAN 4048 will already be present. If the fabric cores were originally built from VOSS 8.3 or later, the default onboarding Private-VLAN 4048 will also already be assigned to the onboarding I-SID 15999999 and the same I-SID will also already be defined as the auto-sense onboarding I-SID. It will therefore be sufficient to simply add an IP address and DHCP relay config to the existing onboarding Private-VLAN 4048.
3. If the VSP core was not originally built from VOSS 8.3 defaults (for example. it was upgraded from a pre-VOSS 8.3 release) it will also need to have auto-sense enabled on the interfaces connecting to the VSP edge.

In this guide, it is assumed the VSP core configs were built from pre-VOSS 8.2 defaults – and therefore, no onboarding I-SID is defined, all unused ports are disabled, autosense is disabled on all ports, and no nickname server is configured. Thus, these configuration items need to be configured on both VSP core nodes.

Apply the following config on both VSP core nodes:

VSP-core1	VSP-core2
<pre>enable config term interface gigabitEthernet 1/10   auto-sense enable   no shutdown exit vlan create 4048 name "onboarding-vlan" type pvlan-mstprstp 0 secondary 4049 vlan i-sid 4048 15999999 i-sid name 15999999 "Onboarding I-SID" auto-sense onboarding i-sid 15999999 interface Vlan 4048   ip address 10.9.192.2/24   ip vrrp version 3   ip vrrp address 1 10.9.192.1   ip vrrp 1 enable   ip dhcp-relay   ip dhcp-relay fwd-path 10.9.255.130   ip dhcp-relay fwd-path 10.9.255.130 mode dhcp   ip dhcp-relay fwd-path 10.9.255.130 enable   ip dhcp-relay fwd-path 10.9.255.131   ip dhcp-relay fwd-path 10.9.255.131 mode dhcp   ip dhcp-relay fwd-path 10.9.255.131 enable exit spbm nick-name server prefix a.10.00 spbm nick-name server end</pre>	<pre>enable config term interface gigabitEthernet 1/11   auto-sense enable   no shutdown exit vlan create 4048 name "onboarding-vlan" type pvlan-mstprstp 0 secondary 4049 vlan i-sid 4048 15999999 i-sid name 15999999 "Onboarding I-SID" auto-sense onboarding i-sid 15999999 interface Vlan 4048   ip address 10.9.192.3/24   ip vrrp version 3   ip vrrp address 1 10.9.192.1   ip vrrp 1 enable   ip dhcp-relay   ip dhcp-relay fwd-path 10.9.255.130   ip dhcp-relay fwd-path 10.9.255.130 mode dhcp   ip dhcp-relay fwd-path 10.9.255.130 enable   ip dhcp-relay fwd-path 10.9.255.131   ip dhcp-relay fwd-path 10.9.255.131 mode dhcp   ip dhcp-relay fwd-path 10.9.255.131 enable exit spbm nick-name server prefix a.10.00 spbm nick-name server end</pre>

Note that SLPP must not be enabled for the onboarding VLAN 4048, because this could result in the fabric edge switches cutting themselves off after they have SLPP-Guard enabled on their auto-sense ports in some scenarios.

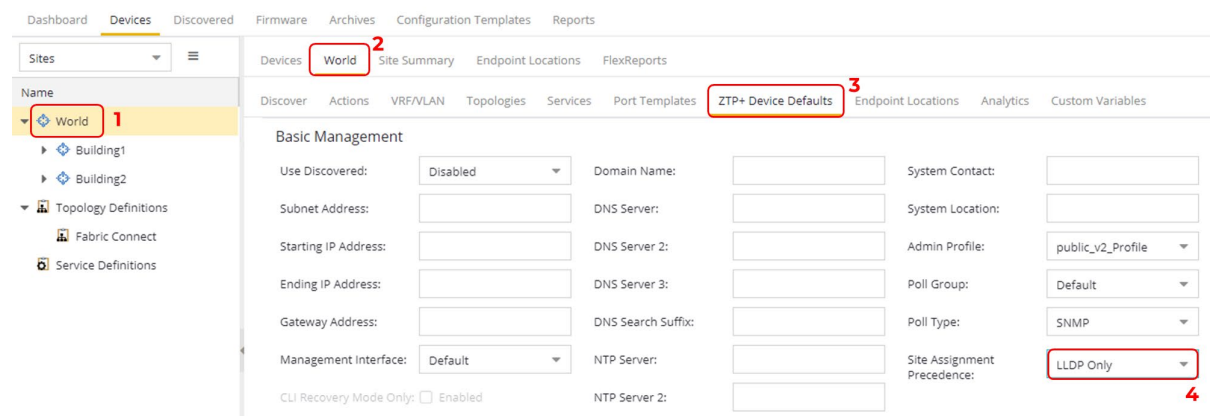
# Prepare XIQ-SE for VSP Edge Deployment

## ZTP+ Configuration

In a previous section, the two fabric core switches were manually added to the Building1 XIQ-SE site. However, the Universal Edge switches will be automatically assigned to the Building1 site during the onboarding process.

To automate the site assignment, locate XIQ-SE's global ZTP+ configuration located under the World site, and click the ZTP+ Device Defaults tab.

Locate the Site Assignment Precedence drop-down and set to "LLDP Only." Note that this drop-down is configurable only from the World site. With this setting, XIQ-SE will use the LLDP neighbor table of the VSP core switches to determine the correct site assignment for the Universal Edge switches. Because the VSP core switches are in Building1, the edge switches will be assigned to this site. Save the change.



Confirm that the ZTP+ config for the Building1 site is correct before onboarding the Universal Hardware edge switch into the site. Go to the selected Building1 site and click the ZTP+ Device Defaults tab.

Under Basic Management, set options as follows:

- Use Discovered: **IP and Management Interface**
- Admin Profile: **Fabric Edge**
- Poll Type: **SNMP**
- NTP Server: **10.9.255.155**

Devices **Building1** <sup>1</sup> Site Summary Endpoint Locations FlexReports

Discover Actions VRF/VLAN Topologies Services Port Templates **ZTP+ Device Defaults** <sup>2</sup> Endpoint Locations Analytics Custom Variables

### Basic Management

Use Discovered:	<b>IP and Management</b>	Domain Name:		System Contact:	
Subnet Address:		DNS Server:		System Location:	
Starting IP Address:		DNS Server 2:		Admin Profile:	<b>Fabric Edge</b>
Ending IP Address:		DNS Server 3:		Poll Group:	Default
Gateway Address:		DNS Search Suffix:		Poll Type:	<b>SNMP</b>
Management Interface:	Default	NTP Server:	<b>10.9.255.155</b>	Site Assignment Precedence:	None
CLI Recovery Mode Only:	<input type="checkbox"/> Enabled	NTP Server 2:			

With the “Use Discovered” parameter set at “IP and Management,” ZTP+ will use the same IP address and Management interface used during the onboarding process. Later in the guide, there will be steps to move the Management interface to a VLAN interface or CLIP interface.

Under Configuration/Upgrade, leave Configuration Updates set to Always (this setting does not apply in SNMP Poll Type). Set Firmware Upgrades to Never. Because this guide is using the Universal Hardware edge, the conversion from EXOS to VOSS will require download of a VOSS software image. By using this process, it will ensure that the VSP edge is upgraded to the desired software version.

### Configuration/Upgrade

Configuration Updates:	Always	Firmware Upgrades:	<b>Never</b>
Update Date:	6/23/2021	Upgrade Date:	6/23/2021
Update Time:	09:30 AM	Upgrade Time:	09:30 AM
Update UTC Offset:	UTC-04:00	Upgrade UTC Offset:	UTC-04:00

In the “Device Protocols” section, deselect (uncheck) MVRP. The rest can be left as is, and MSTP must remain enabled. Note that the Telnet, HTTP, and HTTPS protocol options only work as of VOSS 8.4. All protocol options work with EXOS and will apply when the Universal Edge switch is initially onboarded as EXOS.

### Device Protocols

Telnet: <input checked="" type="checkbox"/> Enabled	HTTP: <input checked="" type="checkbox"/> Enabled	LACP: <input type="checkbox"/> Enabled	<b>MSTP: <input checked="" type="checkbox"/> Enabled</b>
SSH: <input checked="" type="checkbox"/> Enabled	HTTPS: <input checked="" type="checkbox"/> Enabled	LLDP: <input checked="" type="checkbox"/> Enabled	POE: <input checked="" type="checkbox"/> Enabled
SNMP: <input checked="" type="checkbox"/> Enabled	FTP: <input checked="" type="checkbox"/> Enabled	<b>MVRP: <input type="checkbox"/> Enabled</b>	VXLAN: <input type="checkbox"/> Enabled

Select Save to commit changes to the site.

Ensure that MVRP is deselected, because ZTP+ will try to apply the default port templates during switch onboarding. These default port templates are listed under the Port Template tab as shown below.

Source	Configuration	PVID	Default Role	Span Guard	Loop Protect	MVRP	SLPP	SLPP Guard	SLPP Guard Timer	PoE Enable	PoE Priority
/World	AP	Default [1]	None		✓				60	✓	LOW
/World	Access	Default [1]	None	✓					60	✓	LOW
Global	AutoSense	0	None						60	✓	LOW
/World	Interswitch	Default [1]	None		✓	✓			60	✓	LOW
/World	IoT	Default [1]	None		✓				60	✓	LOW
/World	Management	Default [1]	None						60	✓	LOW
/World	Other	Default [1]	None		✓				60	✓	LOW
/World	Phone	Default [1]	None		✓				60	✓	LOW
/World	Printer	Default [1]	None		✓				60	✓	LOW
/World	Router	Default [1]	None		✓				60	✓	LOW
/World	Security	Default [1]	None		✓				60	✓	LOW
/World	vSwitch	Default [1]	None		✓				60	✓	LOW

ZTP+ will apply the default port templates based on the LLDP discovery process. If LLDP discovers an AP connected to the switch port, ZTP+ will apply the AP port template. Likewise, if LLDP discovers a switch/bridge neighbor then ZTP+ will apply the Interswitch port template to the switch port.

The problem is that some of the default parameters in the port templates can cause issues with a VSP edge deployment, in particular Span Guard and MVRP.

The MVRP setting will apply only when the Universal Hardware is onboarded in EXOS mode. In some topologies, this can cause a MAC learning issue because the EXOS switches generate MVRP PDUs with the switch's MAC out of Spanning Tree Blocked ports, causing the VSP cores to learn those MACs on the wrong ports, and resulting in intermittent connectivity to the EXOS DHCP IP address. By disabling the MVRP Protocol, we make sure that MVRP will not get activated by any port templates.

Span Guard is also a problem because it will result in BPDU-Guard getting enabled on VOSS auto-sense ports when the Universal Hardware is onboarded in VOSS mode. If those ports are then used to interconnect VSPs together, BPDU-Guard will conflict with some auto-sense states that generate self-generated BPDUs to prevent loops, resulting in auto-sense ports going offline. To avoid these issues, XIQ-SE 21.9 introduced a new Global "AutoSense" port template which is automatically applied to VOSS Universal Hardware devices via a ZTP+ Automated Template entry:

The screenshot shows the 'Port Templates' section in the VSP Edge Deployment interface. The 'Global' template is highlighted with a red box, showing 'AutoSense' configuration. Below it, the 'ZTP+ Automated Templates' section shows two entries: 'AutoSense VOSS' and 'AutoSense Fabric Engine', both with 'Universal Platform' families. The 'Port Mappings' section on the right shows a mapping for 'AutoSense' to a specific port.

The Auto-Sense ZTP+ Template entry will override the automatic application of the default port templates described above.

Note that the Auto-Sense ZTP+ Template entry will exist only for new sites created in XIQ-SE 21.9 or later. If an older version of XIQ-SE or XMC was used to create the site, the template entry will not exist and will need to be created manually (or the site deleted and re-created).

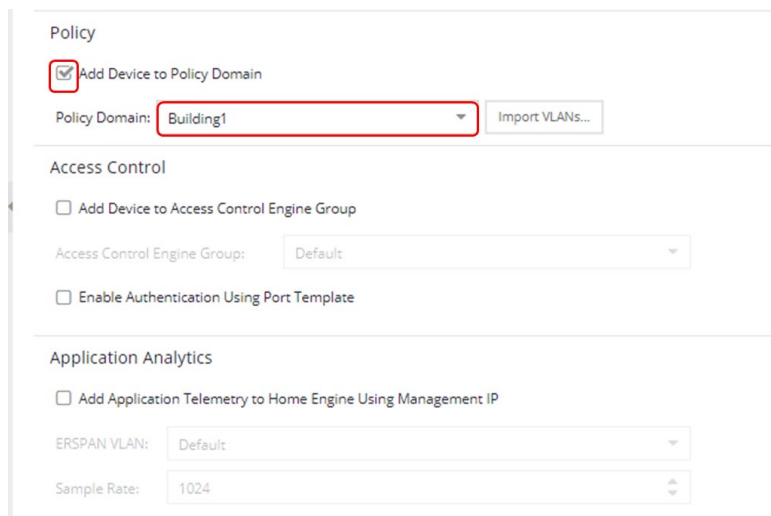
Also note that default template entries exist for VOSS and Fabric Engine Universal Hardware switches. If you are onboarding a VSP4900 or other VSP switch model, then create a similar entry and set the family to “VSP Series.”

To continue with the Building1 site configuration, navigate to the Actions tab, and verify that all these site actions are set:

- Automatically Add Devices
- Add Trap Receiver
- Add Syslog Receiver
- Add to Archive
- Add to Map (and that the correct Building1 map is selected)

The screenshot shows the 'Actions' tab for 'Building1' in the VSP Edge Deployment interface. The 'Actions' tab is highlighted with a red box and labeled '2'. The 'Automatically Add Devices' checkbox is checked and labeled '1'. The 'Collection Mode' is set to 'Historical'. The 'Collection Interval (minutes)' is set to '15'. The 'Map Name' is set to '/World/Building1/Building1'.

Farther down on the same page, there are additional parameters. Enable “Add Device to Policy Domain” and select “Building1” from the drop-down.



The screenshot shows a configuration interface with three main sections: Policy, Access Control, and Application Analytics. In the Policy section, the checkbox "Add Device to Policy Domain" is checked and highlighted with a red box. Below it, the "Policy Domain:" dropdown menu is set to "Building1" and is also highlighted with a red box. To the right of the dropdown is a button labeled "Import VLANs...". In the Access Control section, there are two unchecked checkboxes: "Add Device to Access Control Engine Group" and "Enable Authentication Using Port Template". Below these is a dropdown menu for "Access Control Engine Group:" set to "Default". In the Application Analytics section, there is an unchecked checkbox "Add Application Telemetry to Home Engine Using Management IP". Below this are two dropdown menus: "ERSPAN VLAN:" set to "Default" and "Sample Rate:" set to "1024".

Leave the other parameters disabled, and select Save to save the changes.

## XIQ-SE Workflow Configuration for VSP Onboarding

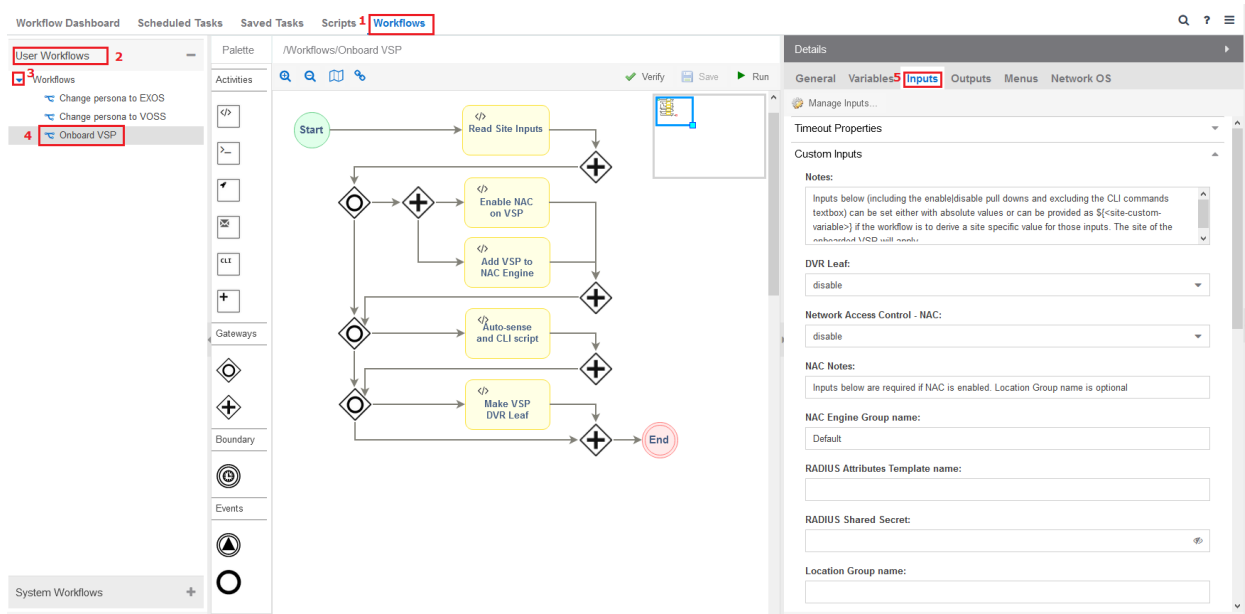
The following configurations need to be performed on XIQ-SE to fully automate the onboarding of the VSP edge switches:

1. Add the VSP to the NAC Engine group, using the correct RADIUS attributes template.
2. Add the switch to the correct Policy Domain.
3. Configure the RADIUS server and EAPoL on the VSP edge switch.
4. Configure the VSP edge switch auto-sense parameters, such as:
  - a. Voice I-SID
  - b. Data I-SID
  - c. ISIS Hello authentication (Optional)
  - d. FA Message authentication (Optional)
5. Convert the VSP edge switch into a DVR Leaf.

As of release 22.3, XIQ-SE cannot natively support some of the functions outlined above. Therefore, to fully automate the VSP edge onboarding process, the XIQ-SE workflow named “Onboard VSP” will be used. This workflow is available on GitHub and has already been imported into XIQ-SE in a previous section.

The workflow needs to be configured for use. Go to XIQ-SE Tasks. On the Workflows tab, select the “Onboard VSP” workflow. Under the workflow details, view the Inputs tab.





Provide the following inputs:

- DVR Leaf: **enable**
- Network Access Control (NAC): **enable**
- NAC Engine Group name: **Default**
- RADIUS Attributes Template name: **Extreme VOSS – Per-User ACL**
- RADIUS Shared Secret: **<choose the RADIUS secret to use; this workflow configures the shared secret for this switch, and on XIQ-SE Control engine>**
- Location Group name: **<leave empty, Building1/2 will use different Policy domains rather than different Access Control Location Groups>**
- Auto-sense Voice I-SID: **`\${voicelsid}`**
- Auto-sense Voice VLAN-id only if tagged: **195**
- Auto-sense Data I-SID: **<leave empty, will be using NAC for the client>**
- Auto-sense ISIS Authentication key: **<either leave empty, or set a key for ISIS auth>**
- Auto-sense FA Authentication key: **<leave empty or set an FA auth key>**
- Additional CLI commands:
  - **auto-sense eapol voice lldp-auth**
  - **clock time-zone US Eastern**

Note: NAC will not be used for the IP phone. Instead, EAP Voice LLDP detection bypass will be used.

Note: The **`\${voicelsid}`** variable is case-sensitive.

Palette /Workflows/Onboard VSP

Activities

Gateways

Boundary

Events

Start

Read Site Inputs

Enable NAC on VSP

Add VSP to NAC Engine

Auto-sense and CLI script

Make VSP DVR Leaf

End

Details

General Variables Inputs Outputs Menus Network OS

Manage Inputs...

DVR Leaf:

enable

Network Access Control - NAC:

enable

NAC Notes:

Inputs below are required if NAC is enabled. Location Group name is optional. To configure a given Engine, of the NAC Engine Group, as primary RADIUS server on the switch, add "primary" to any of userData1-4 for that Engine under its Device Annotation.

NAC Engine Group name:

Default

RADIUS Attributes Template name:

Extreme VOSS - Per-User ACL

RADIUS Shared Secret:

\*\*\*\*\*

On switch create RADIUS server for:

eapol

Location Group name:

Palette /Workflows/Onboard VSP

Activities

Gateways

Boundary

Events

Start

Read Site Inputs

Enable NAC on VSP

Add VSP to NAC Engine

Auto-sense and CLI script

Make VSP DVR Leaf

End

Details

General Variables Inputs Outputs Menus Network OS

Manage Inputs...

Auto-sense Voice I-SID:

\$(voicelsid)

Auto-sense Voice VLAN-id only if tagged:

195

Auto-sense Data I-SID:

Auto-sense Data platform VLAN-id:

Auto-sense WAP-Type1 I-SID:

Auto-sense WAP-Type1 platform VLAN-id:

Auto-sense ISIS Authentication key:

Auto-sense FA Authentication key:

Auto-sense Wait Interval:

45

Palette /Workflows/Onboard VSP

Activities

Gateways

Boundary

Events

Start

Read Site Inputs

Enable NAC on VSP

Add VSP to NAC Engine

Auto-sense and CLI script

Make VSP DVR Leaf

End

Details

General Variables Inputs Outputs Menus Network OS

Manage Inputs...

Auto-sense FA Authentication key:

Auto-sense Wait Interval:

45

Additional CLI commands:

auto-sense eapol voice lldp-auth  
clock time-zone US Eastern

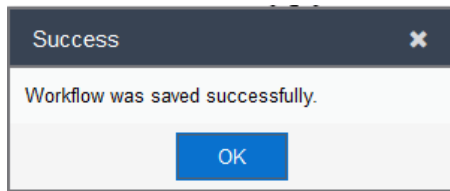
Sanity and Debug Notes:

Sanity: enable if you do not trust this workflow and wish to first see what it does. In sanity mode configuration changes are not actually made. Debug: enable if you need to report a problem to the script author.

Sanity:

Debug:

Save the modified workflow and click OK.

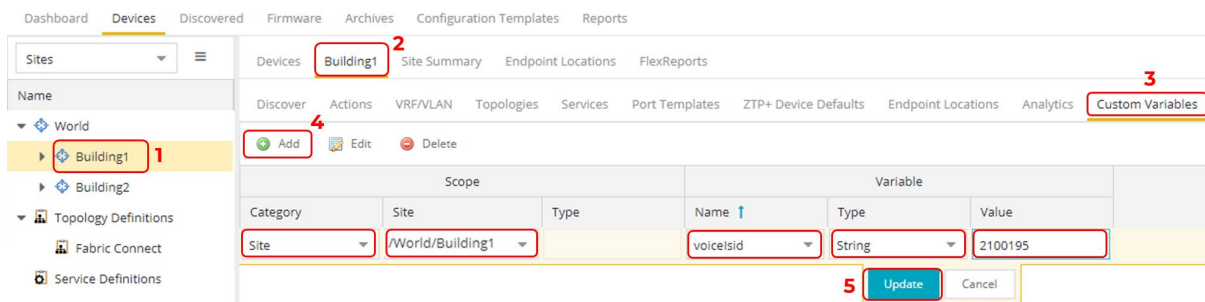


Note that for the Voice I-SID, the absolute value is not provided but is referenced as a variable in the format `{{<variable-name>}}`. This is because these inputs are site-specific and will vary based on the site where the edge switches are onboarded.

In this guide, the VSP edge switches are onboarded into the Building1 site, but a typical customer deployment will have multiple sites as shown below with different “voicelsid” values for each site.

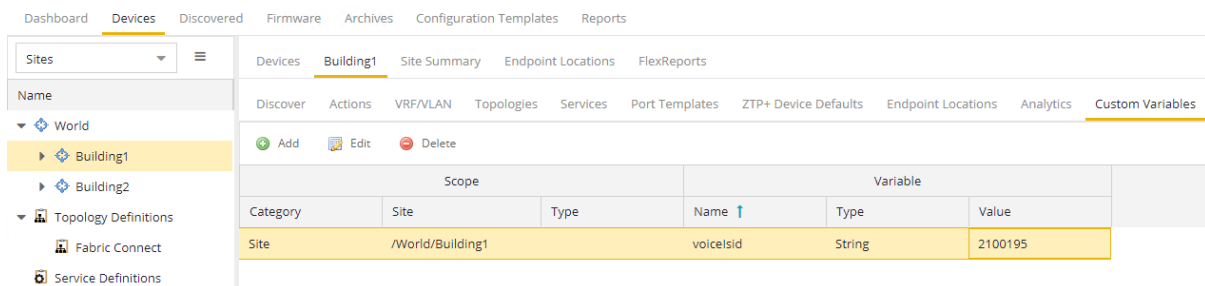
Site	voicelsid
Building1	2100195
Building2	2200195

Go to the XIQ-SE Site for Building1, Custom Variables tab, and add the “voicelsid” variable as shown below.



Note: The variable names are case-sensitive. Make sure to enter them correctly.

Note: The variables must be created as Category = Site and from the local site (not Global) and as Type = String. When completed, the variable settings should look as shown below:



Select Save to save the variables.

When you are done, the table will refresh to show both variables as well as a Global version holding the same value that was configured. This is normal, so that XIQ-SE can ensure that a fallback Global variable exists if a site-specific one was specified. Ignore the Global version of the same variable (or set it to an empty value). In any case, the “Onboard VSP” workflow will only look for the site-specific variable if it exists.

Dashboard | **Devices** | Discovered | Firmware | Archives | Configuration Templates | Reports

Sites ⌵ ☰

Name

- World
  - Building1**
  - Building2
- Topology Definitions
  - Fabric Connect
  - Service Definitions

Devices | **Building1** | Site Summary | Endpoint Locations | FlexReports

Discover | Actions | VRF/VLAN | Topologies | Services | Port Templates | ZTP+ Device Defaults | Endpoint Locations | Analytics | **Custom Variables**

➕ Add | ✎ Edit | 🗑 Delete

Scope			Variable		
Category	Site	Type	Name ↑	Type	Value
Site	Global		voicelsid	String	2100195
Site	/World/Building1		voicelsid	String	2100195

In a typical customer multi-site deployment, repeat the above steps for each site. The steps for the Building2 site are shown below.

Go to XIQ-SE Site for Building2, Custom Variables tab.

Dashboard | **Devices** | Discovered | Firmware | Archives | Configuration Templates | Reports

Sites ⌵ ☰

Name

- World
  - Building1
  - Building2** 1
- Topology Definitions
  - Fabric Connect
  - Service Definitions

Devices | **Building2** 2 | Site Summary | Endpoint Locations | FlexReports

Discover | Actions | VRF/VLAN | Topologies | Services | Port Templates | ZTP+ Device Defaults | Endpoint Locations | Analytics | **Custom Variables** 3

➕ Add | ✎ Edit | 🗑 Delete

Scope			Variable		
Category	Site	Type	Name ↑	Type	Value
Site	Global		voicelsid	String	2100195

The Global version of the defined variable for Building1 is already visible. Add the Building2 site-specific variable as shown below. Note that the variable name is already proposed in the Name field.

Dashboard | **Devices** | Discovered | Firmware | Archives | Configuration Templates | Reports

Sites ⌵ ☰

Name

- World
  - Building1
  - Building2**
- Topology Definitions
  - Fabric Connect
  - Service Definitions

Devices | **Building2** | Site Summary | Endpoint Locations | FlexReports

Discover | Actions | VRF/VLAN | Topologies | Services | Port Templates | ZTP+ Device Defaults | Endpoint Locations | Analytics | **Custom Variables**

➕ Add | ✎ Edit | 🗑 Delete

Scope			Variable		
Category	Site	Type	Name ↑	Type	Value
Site	/World/Building2		voicelsid	String	2200195
Site	Global		voicelsid	String	2100195

Select Save to save the variables for Building2.

Go to the XIQ-SE Building1 site. In the Actions tab, under Custom Configuration, add an additional entry with the following:

- Vendor: **Extreme**
- Family: **Universal Platform Fabric Engine**

- Topology: **Any**
- Task: **Provisioning/Onboard VSP**

If the Provisioning/Onboard VSP workflow is not listed, cancel out and refresh the XIQ-SE page.

Note: In earlier versions of XIQ-SE, the “Family” value for Universal Hardware switches was “Unified Switching VOSS” but this has changed to “Universal Platform VOSS.” If you are running a pre-8.6 version of VOSS, set the “Family” value to “Universal Platform VOSS.” If you are running VOSS 8.6 or later (also known as Fabric Engine) set the “Family” value to “Universal Platform Fabric Engine.” Make sure the entry points to the correct workflow “Onboard VSP” as shown below

Note: If you are using non-Universal Hardware VSP models, such as VSP4900 or VSP7400, an additional entry will need to be created with the “Family” set to : **“VSP Series”** and pointing to the workflow “Onboard VSP.”

The screenshot shows the XIQ-SE interface with the following configuration details:

- Building1** (highlighted with red box 1)
- Actions** (highlighted with red box 2)
- Custom Configuration** table:

Enabled	Vendor	Family	Topology	Task
<input checked="" type="checkbox"/>	<b>Extreme</b> (highlighted with red box 3)	<b>Universal Platform Fabric Engine</b> (highlighted with red box 4)	Any	<b>Provisioning/Onboard VSP</b> (highlighted with red box 5)
<input checked="" type="checkbox"/>	Extreme	Universal Platform Switch Engine	Any	Provisioning/Change persona to VOSS
<input checked="" type="checkbox"/>	Extreme	Universal Platform EXOS	Any	Provisioning/Change persona to VOSS

Select Save to commit changes.

## Universal Edge Switch OS Conversion Using XIQ

Because we are deploying a fabric with VSP fabric edge, the Universal Edge switches need to be converted to VOSS/Fabric Engine. (They are initially booted into EXOS/Switch Engine when powered up.) If you are using VSP switches and not Universal Edge switches, then they will boot directly into VOSS and the OS conversion is not needed. This guide assumes the use of Universal Edge switches and will use XIQ to perform the OS conversion.

Performing OS conversion via XIQ and ZTP+ onboarding will require the switch to restart two times after initial bootup:

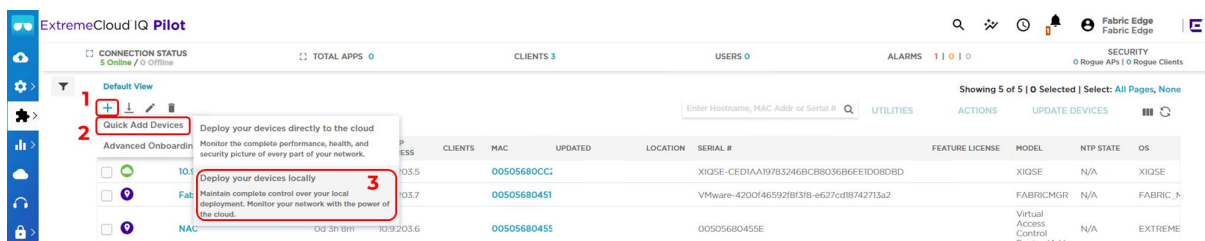
1. Initial boot as EXOS:
  - a. The switch onboards to XIQ.
  - b. In XIQ, the switch serial number is associated with the Fabric Engine OS.
  - c. XIQ converts the switch to the latest GA version of Fabric Engine.
2. The switch boots with latest Fabric Engine GA version in a factory ship state:
  - a. The switch has no configuration file and onboards to XIQ-SE via ZTP+.
  - b. The switch is added to the XIQ-SE Building1 site but in a read-only state.  
➔ Manual action is required:
    - On XIQ: delete the device from XIQ
    - On XIQ-SE: re-add the device to XIQ via XIQ-SE
  - c. The Onboard VSP workflow is triggered.
  - d. The XIQ-SE workflow sets the DVR Leaf config and reboots the switch a final time.
3. The switch boots as DVR Leaf with final configuration.

### Caution

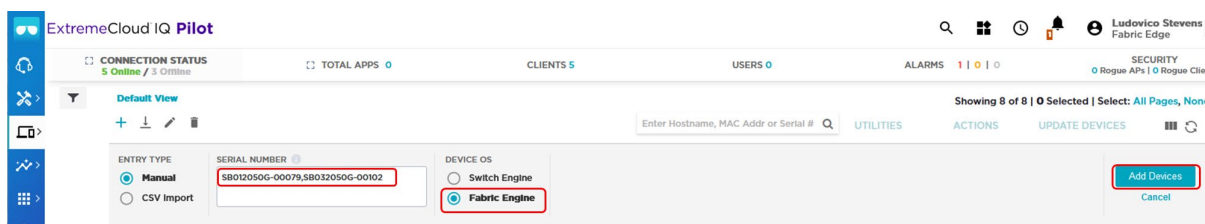
Currently, with XIQ-SE, the above step 2c (and 2d) will not happen automatically if the switch is already added to XIQ, because XIQ-SE is designed not to manage or configure a device that is already added to XIQ. Manual action is required to first delete the switch from XIQ and then force XIQ-SE to re-add the same switch to XIQ (details will follow). Then the above steps 2c (and 2d) will resume automatically.

## Prepare OS Conversion Using XIQ

Log in to XIQ, and add the new Universal Edge switch using the switch's serial number. Under Manage, Devices, click the + button, and then select Quick Add Devices.



Set the Entry Type to “Manual,” input the Universal Edge switch serial number in the box provided, set the Device OS to “Fabric Engine,” and click “Add Devices” as shown below.



For this deployment guide, two sample 5520 Universal Hardware models will be used for onboarding.

Switch	Hardware Model	Serial Number
VSP-edge1	5520-12MW-36W	SB012050G-00079
VSP-edge2	5520-24W	SB032050G-00102

Note: The desired OS for the Universal Edge switch is set to Fabric Engine. As a result, XIQ will convert the switch OS to Fabric Engine after it is initially onboarded

# Zero Touch Onboarding of VSP Edge Switches

## Switch Installation and Power Up

In the previous sections, XIQ-SE and XIQ were provisioned for the automated onboarding of the VSP edge switches. To kick off the Zero Touch Onboarding, install each of the edge switches, apply power, and connect at least one of the edge switches to an existing Fabric Connect core. As mentioned previously, each edge switch will be in a “factory ship” state, meaning it does not have an existing configuration file and will boot up into EXOS/Switch Engine. When the switch is booted, the ZTP+ process starts and the edge switch connects to XIQ where the OS conversion to VOSS/Fabric Engine will start.

The final stages of the VSP edge deployment are zero-touch, and there is no need for the technician to connect to the switch console port or pre-stage the switches.

## OS Conversion Using XIQ

In XIQ, to monitor the OS conversion to Fabric Engine, there is an activity bar located in the “Updated” column as shown below.

The screenshot shows the ExtremeCloud IQ Pilot interface. At the top, there are summary statistics: CONNECTION STATUS (7 Online / 0 Offline), TOTAL APPS (0), CLIENTS (6), USERS (0), and ALARMS (1 | 0 | 0). Below this is a table with columns: STATUS, HOST NAME, POLICY, UPTIME, HOST IP ADDRESS, CLIENTS, MAC, UPDATED, LOCATION, SERIAL #, FEATURE LICENSE, MODEL, NTP STATE, OS VERSION, IQAGENT, WIFID CHANNEL, and WIFID POWER. The table lists several devices, including '10.9.203.5', 'Fabric', 'HOSTNAME', 'NAC', 'VSP-core1', and 'VSP-core2'. The 'UPDATED' column shows progress bars and status like 'Assign Loc.' and 'Assign Policy'. The 'FEATURE LICENSE' column shows 'Not Supported' for most devices.

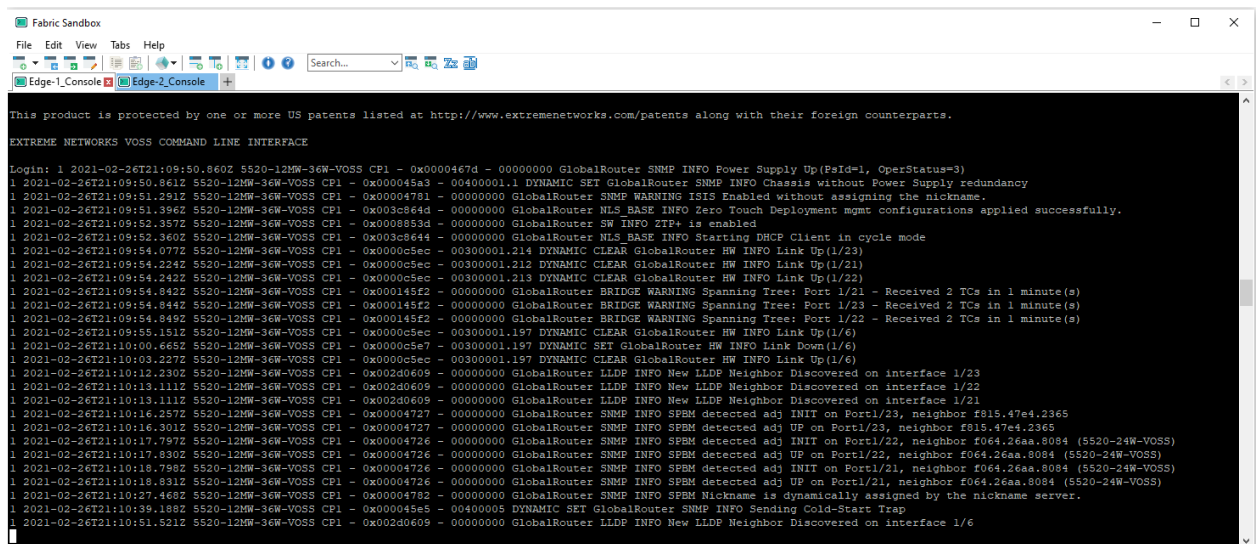
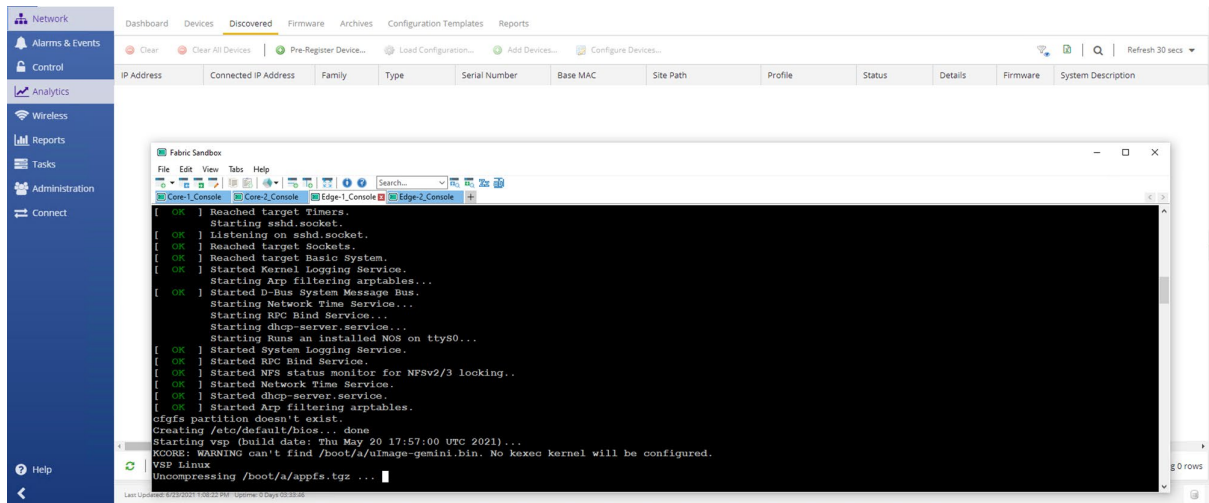
STATUS	HOST NAME	POLICY	UPTIME	HOST IP ADDRESS	CLIENTS	MAC	UPDATED	LOCATION	SERIAL #	FEATURE LICENSE	MODEL	NTP STATE	OS VERSION	IQAGENT	WIFID CHANNEL	WIFID POWER
Online	10.9.203.5		0d 3h 32m	10.9.203.5		00505680CC1			XIQSE-1AF39BD9CC24	Not Supported	XIQSE	N/A	21.9.10.4 (2...	N/A	N/A	N/A
Online	Fabric		0d 3h 33m	10.9.203.7		00505680451			VMware-420014609278f3	Not Supported	FABRICMGR	N/A	21.9.10.4 (2...	N/A	N/A	N/A
Online	HOSTNAME	Assign Policy	N/A	10.9.192.104	0	F06426ABE4C	80% IQ Engine Firmw...		58012050G-00079	Not Supported	EXOS-5520-12W-36W	N/A	3111.3	0.4.5	N/A	N/A
Online	HOSTNAME	Assign Policy	N/A	10.9.192.103	3	F06426AAB01	80% IQ Engine Firmw...		58012050G-00102	Not Supported	EXOS-5520-24W	N/A	3111.3	0.4.5	N/A	N/A
Online	NAC		0d 3h 30m	10.9.203.6		00505680455			00505680455E	Not Supported	Virtual Access Control Engine IA-V	N/A	21.9.10.4 (2...	N/A	N/A	N/A
Online	VSP-core1		0d 6h 20m	10.9.193.131		F81547E4230C			14JP335E50B1	Not Supported	VSP-4450GSX-PWR+	N/A	8.4.0.0 (8...	N/A	N/A	N/A
Online	VSP-core2		0d 6h 20m	10.9.193.132		14612FEE7B0C			17JP0230E58J	Not Supported	VSP-4450GSX-PWR+	N/A	8.4.0.0 (8...	N/A	N/A	N/A

## Observe Progress Using the VSP Edge Console

As the edge switches boot into VOSS/Fabric Engine, if possible, connect to the switches' serial consoles and observe the log messages as the switches go through the various phases of Zero-Touch-Fabric and ZTP+. Most VSP edge deployments will not have direct console access to the switches, but here we just show what the console output looks like.

In addition, monitor the XIQ-SE Discovery tab and set the Auto-Refresh rate to 30 seconds. This will provide a view of the ZTP+ progress from both XIQ-SE and the switch.





The screenshot shows the VSP Edge Deployment interface. At the top, there's a navigation bar with tabs: Dashboard, Devices, Discovered, Firmware, Archives, Configuration Templates, and Reports. Below this is a toolbar with various actions like Clear, Clear All Devices, Pre-Register Device..., Load Configuration..., Add Devices..., and Configure Devices... A search bar and a refresh button are also present.

The main table displays a list of discovered devices. The columns are: IP Address, Connected IP Address, Family, Type, Serial Number, Base MAC, Site Path, Profile, Status, Details, Firmware, and System Description. One device is listed with IP 10.9.192.102, Connected IP 10.9.192.102, Family Unified Switch, Type 5520-12MW-36..., Serial Number SB012050G-00079, Base MAC R0 64 26 a8 e4 00, Site Path /World, Profile public\_v2\_Profile, Status ZTP+ Pending E..., Firmware 8.3.0.0, and System Description 5520-12MW-36W-VOSS (8.3.0.0).

An inset window titled 'Fabric Sandbox' shows a console output with various network events. The events include:
 

- Dynamic Clear GlobalRouter HW INFO Link Up (1/23)
- Dynamic Clear GlobalRouter HW INFO Link Up (1/21)
- Dynamic Clear GlobalRouter HW INFO Link Up (1/22)
- Bridge Warning Spanning Tree: Port 1/21 - Received 2 TCs in 1 minute(s)
- Bridge Warning Spanning Tree: Port 1/23 - Received 2 TCs in 1 minute(s)
- Bridge Warning Spanning Tree: Port 1/22 - Received 2 TCs in 1 minute(s)
- Dynamic Clear GlobalRouter HW INFO Link Up (1/6)
- Dynamic Set GlobalRouter HW INFO Link Down (1/6)
- Dynamic Clear GlobalRouter HW INFO Link Up (1/6)
- LLDP New LLDP Neighbor Discovered on interface 1/23
- LLDP New LLDP Neighbor Discovered on interface 1/22
- LLDP New LLDP Neighbor Discovered on interface 1/21
- SNMP INFO SPM detected adj INIT on Port1/23, neighbor f815.47e4.2365
- SNMP INFO SPM detected adj UP on Port1/23, neighbor f815.47e4.2365
- SNMP INFO SPM detected adj INIT on Port1/22, neighbor f064.26aa.8084 (5520-24W-VOSS)
- SNMP INFO SPM detected adj UP on Port1/22, neighbor f064.26aa.8084 (5520-24W-VOSS)
- SNMP INFO SPM detected adj INIT on Port1/21, neighbor f064.26aa.8084 (5520-24W-VOSS)
- SNMP INFO SPM detected adj UP on Port1/21, neighbor f064.26aa.8084 (5520-24W-VOSS)
- SNMP INFO SPM Nickname is dynamically assigned by the nickname server.
- Dynamic Set GlobalRouter SNMP INFO Sending Cold-Start Trap
- LLDP New LLDP Neighbor Discovered on interface 1/6
- NLS BASE INFO DHCP Address 10.9.192.102 added to interface mgmt-vlan
- NLS BASE INFO DHCP Default route with nexthop 10.9.192.1 added to interface vlan.
- NLS BASE INFO Dynamic DNS domain-name FabricEdge-HW-CTC-Local added
- NLS BASE INFO Dynamic DNS Address 10.9.255.130 added
- NLS BASE INFO Dynamic DNS Address 10.9.255.131 added
- LLDP New LLDP Neighbor Discovered on interface 1/6
- LLDP New LLDP Neighbor Deleted on interface 1/6
- LLDP New LLDP Neighbor Deleted on interface 1/6
- LLDP New LLDP Neighbor Discovered on interface 1/6
- SW INFO Boot sequence successful
- SW INFO ZTP+ process started.

As the Fabric Engine switch boots, the order of onboarding events will occur based on two deployment scenarios.

Scenario 1: No ISIS Hello Authentication configured on the VSP cores' NNI links:

1. ISIS adjacency forms with neighboring VSP core switches.
2. A nickname is dynamically assigned by Nickname servers on VSP core switches.
3. DHCP obtains the IP address on onboarding I-SID 15999999.
4. DHCP provides default gateway, DNS servers, and Domain Name.
5. The switch performs a DNS lookup for **extremecontrol.<domain-name>** and discovers the XIQ-SE IP address.
6. The switch connects to XIQ-SE and appears in the Discovered tab.
7. If XIQ-SE can allocate the switch to a Site, then the site ZTP+ config is pushed; else the switch remains in the Discovered tab until an administrator manually configures or adds the switch to a Site.
8. When the switch is allocated to an XIQ-SE Site, the Site's actions are performed; and the "Onboard VSP" workflow is executed.
9. The "Onboard VSP" workflow applies NAC, Auto-sense, and DVR-Leaf configuration.

Scenario 2: ISIS Hello Authentication configured on the VSP cores NNI links:

1. ISIS adjacency does not form with neighboring VSP core switches because there is no ISIS authentication key on the booting edge switches.
2. The onboarding switch issues a DHCP request on the onboarding VLAN 4048 on the VSP cores.

3. The switch obtains IP address, default gateway, and DNS domain name.
4. The switch performs a DNS lookup for **extremecontrol.<domain-name>** and discovers the XIQ-SE IP address
5. The switch connects to XIQ-SE and appears in the Discovered tab.
6. If XIQ-SE can allocate the switch to a Site, then the site ZTP+ config is pushed; else the switch remains in the Discovered tab until an administrator manually configures or adds the switch to a site.
7. When the switch is allocated to an XIQ-SE Site, the Site's Actions are performed, and the "Onboard VSP" workflow is executed.
8. The "Onboard VSP" workflow applies the final NAC config, Auto-sense config, and DVR-Leaf config. In addition, the VSP edge switch is configured with the Auto-sense ISIS authentication key.
9. ISIS adjacency can now form with neighboring VSP core switches.
10. A nickname is dynamically assigned by Nickname servers on the VSP core switches.
11. There is a brief period of time where the onboarding switch is unreachable while its connectivity into the onboarding I-SID 15999999 transitions from a UNI connection to a fabric NNI connection.

When the onboarding process completes, the VSP edge switches are placed into the correct site (Building1) and topology map.

Devices Building1 Site Summary Endpoint Locations FlexReports								
<a href="#">Add Device...</a> <a href="#">Export to CSV</a>								
Status	Name ↑	Site	IP Address	Poll Status	Poll Details	Device Type	Family	Firmware
●	5520-12MW-36W-VO55	/World/Building1	10.9.192.104	Available: 1...	Up: 192 Do...	5520-12MW-36W-V...	Unified Swi...	8.4.0.0
●	5520-24W-VO55	/World/Building1	10.9.192.103	Available: 1...	Up: 2 Dow...	5520-24W-VO55	Unified Swi...	8.4.0.0
●	VSP-core1	/World/Building1	10.9.193.131	Available: 1...	Up: 193 Do...	VSP-4450GSX-PWR+	VSP Series	8.4.0.0
●	VSP-core2	/World/Building1	10.9.193.132	Available: 1...	Up: 193 Do...	VSP-4450GSX-PWR+	VSP Series	8.4.0.0

If you were to observe the edge switch console, you would see a number of SSH connections coming into the newly onboarded switch. Some of these will be XIQ-SE performing the site actions, such as adding XIQ-SE as Trap and Syslog receiver on the switch, and some will be the "Onboard VSP" workflow performing the switch configuration.

## Manual Steps Required if OS Conversion Was Done Using XIQ

In a previous section, this guide described the steps to onboard the Universal Edge switch into XIQ and set the desired OS type to Fabric Engine. However, this creates issues when ZTP+ is onboarding the universal switch into XIQ-SE. During the onboarding process, XIQ-SE detects that the universal switch is already managed by XIQ and adds the switch to the site in read-only mode. Once the switch is in this mode, the onboarding workflow will not execute and the onboarding process will not complete.

This can be verified by inspecting the XIQ “Onboarded” column, in XIQ-SE. If the check mark is missing, then the switch is onboarded to XIQ and is currently in a read-only state.

Devices											
Status	Name ↑	Site	IP Address	Poll Status	Poll Details	Device Type	Family	Firmware	Reference	Connector	XIQ Onboarded
●	5520-12MW-36...	/World/Building1	10.9.192.101	Available: 1...	Up: 18 Do...	5520-12MW-36W-V...	Unified Swi...	8.4.0.0			
●	5520-24W-VOSS	/World/Building1	10.9.192.103	Available: 1...	Up: 1 Dow...	5520-24W-VOSS	Unified Swi...	8.4.0.0			
●	VSP-core1	/World/Building1	10.9.193.131	Available: 1...	Up: 52 Do...	VSP-4450GSX-PWR+	VSP Series	8.4.0.0			✓
●	VSP-core2	/World/Building1	10.9.193.132	Available: 1...	Up: 52 Do...	VSP-4450GSX-PWR+	VSP Series	8.4.0.0			✓

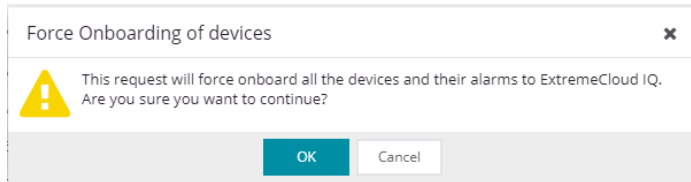
To allow XIQ-SE to fully manage these devices, two manual actions are required.

First, delete the devices from XIQ by selecting the device(s) in XIQ and clicking the Delete button.

Confirm the deletion by clicking Yes.

Second, XIQ-SE needs to re-synch its device database with XIQ. To re-synch the database, in XIQ-SE, navigate to Administration > Diagnostics, select Level Advanced, and then select the “ExtremeCloud IQ Device Message Details” folder under the System main folder.

Click the “Force Onboard to ExtremeCloud IQ,” button and select OK in the confirmation pop-up.



It might take a few seconds for XIQ-SE to re-sync all devices with XIQ. Verify that all devices are now onboarded to XIQ and have a check mark in the “XIQ Onboarded” column.

Devices Building1 Site Summary Endpoint Locations FlexReports												
Add Device... Export to CSV												
Status	Name ↑	Site	IP Address	Poll Status	Poll Details	Device Type	Family	Firmware	Reference	Connector	XIQ Onboarded	
●	5520-12MW-36...	/World/Building1	10.9.192.101	Available: 1...	Up: 22 Do...	5520-12MW-36W-V...	Unified Swi...	8.4.0.0			✓	
●	5520-24W-VOSS	/World/Building1	10.9.192.103	Available: 1...	Up: 4 Dow...	5520-24W-VOSS	Unified Swi...	8.4.0.0			✓	
▶	VSP-core1	/World/Building1	10.9.193.131	Available: 1...	Up: 56 Do...	VSP-4450GSX-PWR+	VSP Series	8.4.0.0			✓	
▶	VSP-core2	/World/Building1	10.9.193.132	Available: 1...	Up: 56 Do...	VSP-4450GSX-PWR+	VSP Series	8.4.0.0			✓	

XIQ now shows that the switches have been onboarded via XIQ-SE.

ExtremeCloud IQ Pilot																
CONNECTION STATUS 7 Online / 0 Offline TOTAL APPS 0 CLIENTS 4 USERS 0 ALARMS 0   0   0 SECURITY 0 Rogue APs / 0 Rogue Clients																
Default View + - Enter Hostname, MAC Addr or Serial # UTILITIES ACTIONS UPDATE DEVICES																
STATUS	HOST NAME	POLICY	UPTIME	MGT IP ADDRESS	CLIENTS	MAC	UPDATED	LOCATION	SERIAL #	FEATURE LICENSE	MODEL	NTP STATE	OS VERSION	IGAGENT	WIFI0 CHANNEL	WIFI0 POWER
●	10.9.203.5		0d 4h 44m	10.9.203.5		00505680CC			XIQSE-CEIDAA1978324	Not Supported	XIQSE	N/A	21.9.10.50	N/A	N/A	N/A
●	5520-12MW-36W-VOSS		0d 1h 54m	10.9.192.101		F06426A8E4C			S8012050G-00079	Not Supported	VSP 5520-12MW-36W	N/A	8.4.0.0	N/A	N/A	N/A
●	5520-24W-VOSS		N/A	10.9.192.103		F06426A80K			S8032050G-00102	Not Supported	VSP 5520-24W	N/A	8.4.0.0	N/A	N/A	N/A
●	Fabric		0d 4h 43m	10.9.203.7		00505680451			VMware-420014659218f2e627cd18742713	Not Supported	FABRICMGR	N/A	21.9.10.50	N/A	N/A	N/A
●	NAC		0d 4h 45m	10.9.203.6		00505680455			00505680455E	Not Supported	Virtual Access Control Engine IA-V	N/A	21.9.10.50	N/A	N/A	N/A
●	VSP-core1		0d 5h 0m	10.9.193.131		F81547E4230K			14JP335E5081	Not Supported	VSP-4450GSX-PWR+	N/A	8.4.0.0	N/A	N/A	N/A
●	VSP-core2		0d 5h 0m	10.9.193.132		14612FEE7B0K			17JP0230E58J	Not Supported	VSP-4450GSX-PWR+	N/A	8.4.0.0	N/A	N/A	N/A

When the VSP edge switches have been onboarded to XIQ-SE and XIQ, the XIQ-SE site actions will execute and the “Onboard VSP” workflow will start automatically to finish the switch onboarding process.

## Monitor XIQ-SE Onboarding Workflow Execution

To monitor workflow execution, go to XIQ-SE Tasks, Workflow Dashboard tab. Click the Active pie chart, and double click any “Onboarding VSP” workflow that is running.

Summary

Status	Start Date/Time	Name	Version	Source	# Devices	Started By	End Date/Time	Message
⚙️	8/24/2021 1:07:05 ...	Onboard VSP	79	Workflow Designer ...	1	root		

Graph View Table View

🔍 🔍 📖

■ Stop Workflow 📄 Show Output 📄 Show Variables

If no active workflows are running, set the drop-down to “Historical” and locate the most recently run “Onboard VSP” workflow. Double click on the workflow to view the execution details.

Workflow Dashboard Scheduled Tasks Saved Tasks Scripts Workflows **Onboard VSP (3)**

Summary

Status	Start Date/Time	Name	Version	Source	# Devices	Started By	End Date/Time	Message	Path
✓	8/24/2021 11:30:15...	Onboard VSP	79	Site Discover Action...	1	NetSight Server	8/24/2021 11:30:46...	VSP 10.9.192.101 applied auto-sense config ...	/Workflows/Onboard VSP

Graph View Table View

🔍 🔍 📖

■ Stop Workflow 📄 Show Output 📄 Show Variables

Devices Grid

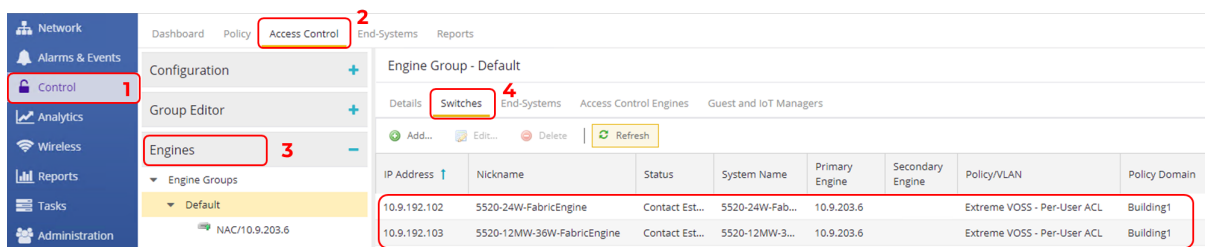
Status	Device IP	Output Path	Start Date/Time
No Data Av...			

Note that the last activity of the “Onboard VSP” workflow converts the VSP switch to a DVR Leaf and reboots the switch one last time.

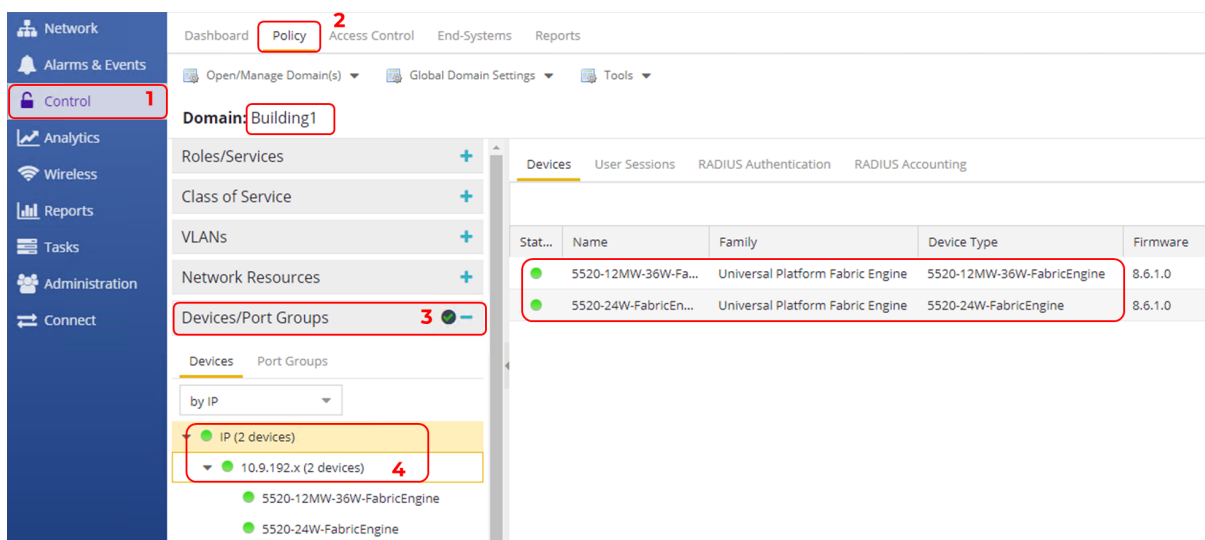
When the VSP edge switches finish booting, the onboard process is complete and the final configuration is saved to the switch flash memory. The switches are now deployed as VSP edge switches

Navigate to the XIQ-SE Control tab and verify that the VSP edge switches have been added to Extreme Control.

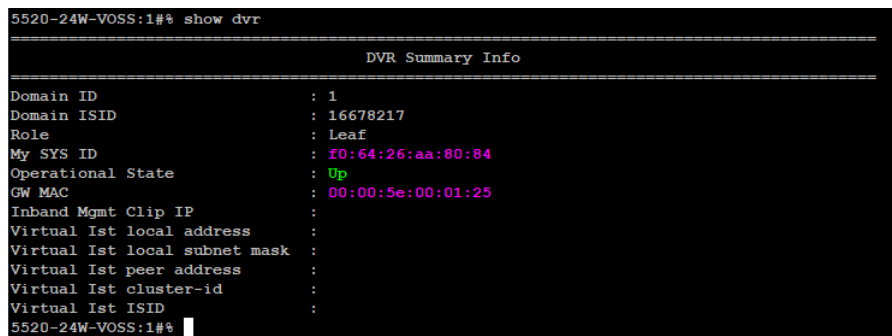




Verify that the VSP switches have been added to the Building1 Policy domain.



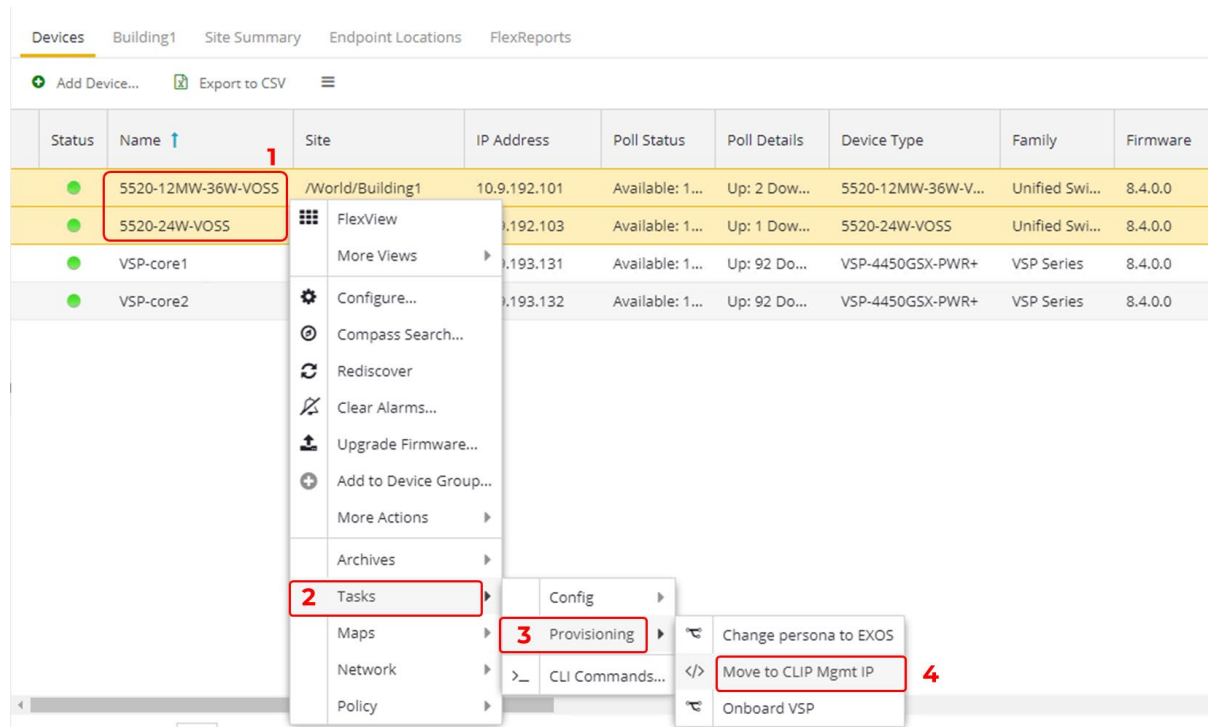
SSH into the VSP edge switches and use the CLI command `show dvr` and verify that the DVR Role is shown as “Leaf.”



## Migrate VSP Edge to Dedicated Switch Management CLIP

The VSP edge switches were onboarded using their DHCP-assigned IP addresses, which were converted to static addresses by ZTP+. However, these management IP addresses are configured on the onboarding VLAN/I-SID (4048/159999999). It is a best-practice to move the switch management IP address from the default onboarding VLAN/I-SID to a CLIP management IP address. The XIQ-SE script “Move to CLIP Mgmt” (available on GitHub) will be used to configure a CLIP management address.

To run the script, select both VSP edge switches, right-click, and select Tasks > Provisioning > Move to CLIP Mgmt IP.



In the script input window, provide the CLIP IP address for each VSP-edge switch. Use the following CLIP addresses.

- VSP-edge1 10.9.193.133
- VSP-edge2 10.9.193.134

Leave the associated VRF as GlobalRouter (this is the only VRF supported for mgmt CLIP on a DVR Leaf), and set the drop-down to delete the preexisting mgmt VLAN IP. Configure the new Mgmt CLIP IP for each VSP edge switch. Enter only the IP address and not the mask. Finally, because the script will remove and rediscover the switches back into XIQ-SE, set the desired System Name of the switches as shown below.



Run Script: Move to CLIP Mgmt IP

1. Device Selection 2. Device Settings 3. Verify Run Script 4. Results

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

Overview Description

New switch mgmt circuitless IP (mask will be 32bits)

Associated VRF name (default is GRT):

Existing mgmt VLAN IP:

Complete	Name	Device IP Address	Mgmt CLIP IP	System Name
✓	5520-12M...	10.9.192.101	10.9.193.133	VSP-edge1
✓	5520-24W...	10.9.192.103	10.9.193.134	VSP-edge2

Sanity / Debug

Sanity: enable if you do not trust this script and wish to first see what it does. In sanity mode config commands are not executed:

Debug: enable if you need to report a problem to the script author:

« Previous Next » Cancel

Click Next, then click Run.

Run Script: Move to CLIP Mgmt IP

1. Device Selection 2. Device Settings 3. Verify Run Script 4. Results

Script Information

Task Information: Run Now Script Name: Move to CLIP Mgmt IP Script Task Name: N/A Timeout (sec): 60

Overall Status

COMPLETED

Devices

Name	IP Address	Start Time/Total Run Time
✓ 5520-12MW-36W-VOSS	10.9.192.101	8/24/2021 2:41:20 PM/(24 sec)
✓ 5520-24W-VOSS	10.9.192.103	8/24/2021 2:41:20 PM/(24 sec)

Results

```

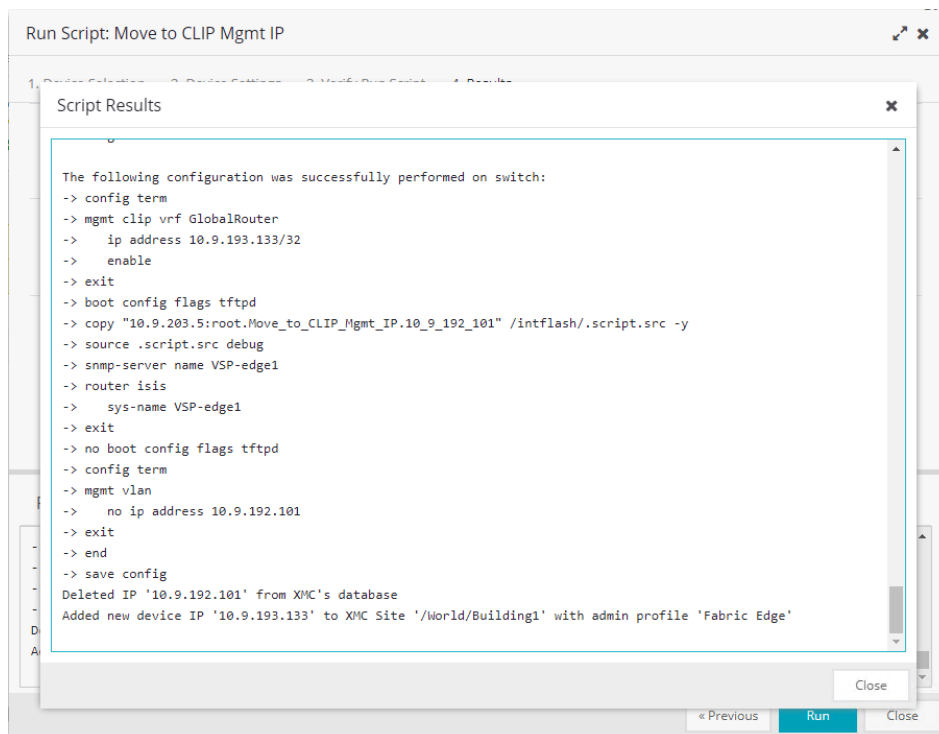
no ip address 10.9.192.101
exit
end
save config
Deleted IP '10.9.192.101' from XMC's database
Added new device IP '10.9.193.133' to XMC Site '/World/Building1' with admin profile 'Fabric Edge'

```

« Previous Run Close

The script creates the new mgmt CLIP, deletes the existing mgmt VLAN IP, deletes the switch from XIQ-SE, and re-adds it using the new CLIP IP and System Name.

When the script has completed, expand the Results window by clicking the “i” button.



Repeat these steps for the other VSP edge switch.

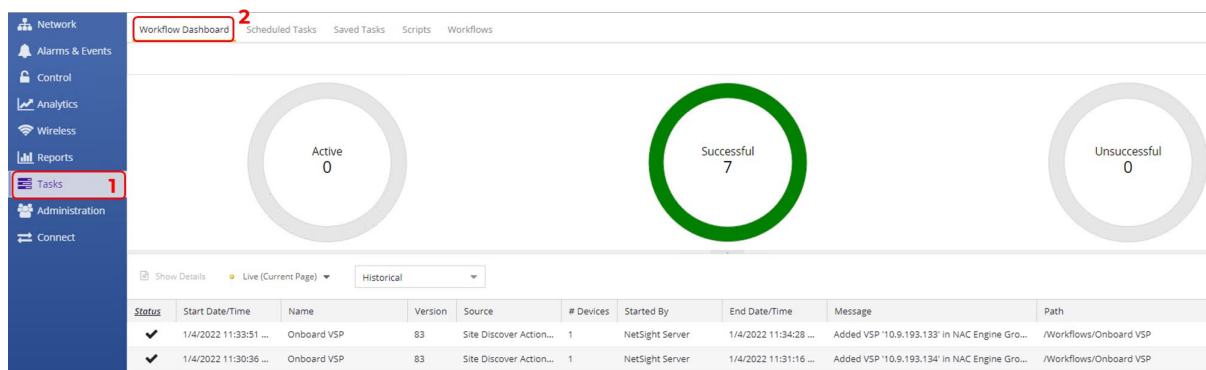
Confirm that all four VSPs have their correct management IP.

Click Refresh if necessary.

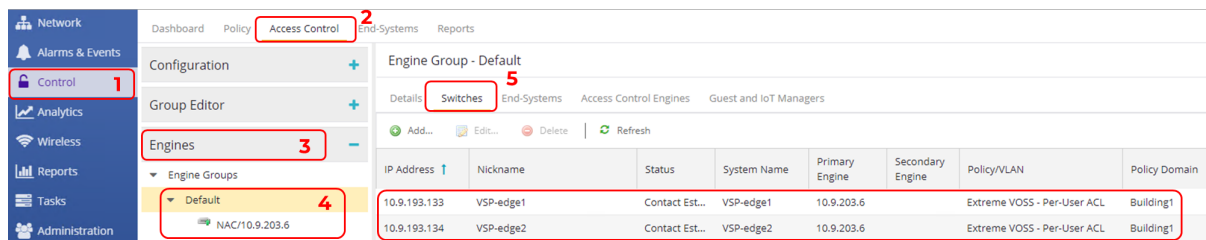
Dashboard <b>Devices</b> Discovered Firmware Archives Configuration Templates Reports									
Sites		Devices Building1 Site Summary Endpoint Locations FlexReports							
Name		Add Device... Export to CSV							
World									
Building1									
Building2									
Topology Definitions									
Fabric Connect									
Service Definitions									
Status	Name	Site	IP Address	Poll Status	Poll Details	Device Type	Family	Firmware	
●	VSP-core1	/World/Building1	10.9.193.131	Available: 1...	Up: 95 Do...	VSP-4450GSX-PWR+	VSP Series	8.4.0.0	
●	VSP-core2	/World/Building1	10.9.193.132	Available: 1...	Up: 95 Do...	VSP-4450GSX-PWR+	VSP Series	8.4.0.0	
●	VSP-edge1	/World/Building1	10.9.193.133	Available: 1...	Up: 1 Dow...	5520-12MW-36W-V...	Unified Swi...	8.4.0.0	
●	VSP-edge2	/World/Building1	10.9.193.134	Available: 1...	Up: 1 Dow...	5520-24W-VOSS	Unified Swi...	8.4.0.0	

Note: Running the “Move to CLIP Mgmt IP” script also executes the “Onboard VSP” workflow one more time. During the workflow execution, the new management CLIP IP address is added to XIQ-SE Control.

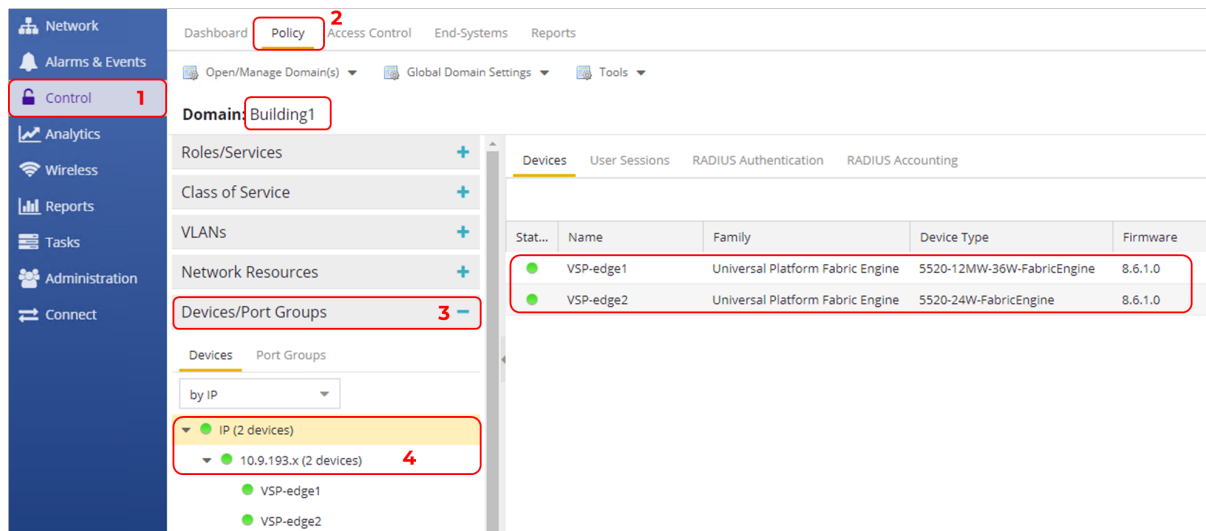
Verify the workflow execution for the new switch IPs under Tasks > Workflow Dashboard.



In XIQ-SE Control, verify that all switches have been added with the correct IP addresses as shown below.



Verify that VSP Edge switches have been added to the Building1 Policy domain.



## Configure XIQ-SE Control Switch Reauthentication Type

In XIQ-SE Control, configure the reauthentication type for each VSP edge switch so XIQ-SE can force device reauthentication. Note that as of XIQ-SE version 22.3, VSP switches are automatically configured with the correct reauthentication profile when added to Control, however the configuration is shown anyway in case you are using an earlier version than 22.3

To configure the reauthentication type, select XIQ-SE Control > Access Control > Engines > Default NAC engine. Select each switch entry and click Edit.

Access Control

Configuration

Group Editor

Engines

Engine Groups

Default

NAC/10.9.203.6

Switches

Engine Group - Default

Details Switches End-Systems Access Control Engines Guest and IoT Managers

Add... Edit... Delete Refresh

IP Address	Nickname	Status	System Name	Primary Engine
10.9.193.131	VSP-core1	Contact Established	VSP-core1	10.9.203.6
10.9.193.132	VSP-core2	Contact Established	VSP-core2	10.9.203.6
10.9.193.133	VSP-edge1	Contact Established	VSP-edge1	10.9.203.6
10.9.193.134	VSP-edge2	Contact Established	VSP-edge2	10.9.203.6

In the Configure Device window, click Advanced Settings.

Configure Device: 10.9.193.133

Switch Type: Layer 2 Out-Of-Band

Primary Engine: NAC/10.9.203.6

Secondary Engine: None

Auth. Access Type: Manual RADIUS Configuration

Virtual Router Name:

RADIUS Attributes to Send: VSP Fabric Attach

RADIUS Accounting: Enabled

Management RADIUS Server 1: None

Management RADIUS Server 2: None

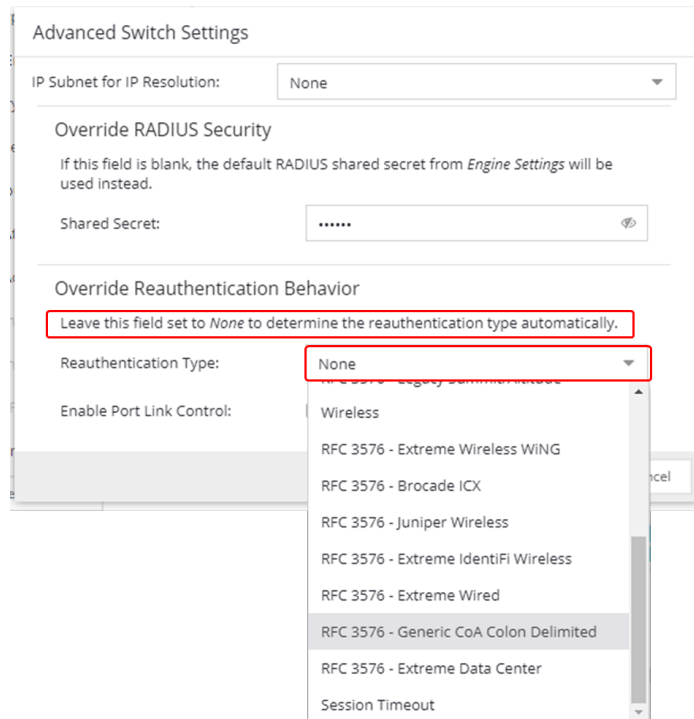
Network RADIUS Server: None

Policy Domain: -- Do Not Set --

Advanced Settings

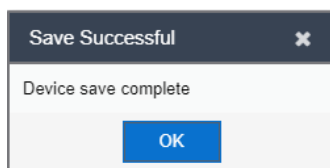
Save Close

In the Advanced Switch Settings window, set the Reauthentication Type drop-down to “None.” This will allow XIQ-Control to set the Reauthentication Type automatically. On the other hand, if you want to manually set the Reauthentication Type, set it to “RFC 3576 – Generic CoA Colon Delimited.”



The image shows a screenshot of the 'Advanced Switch Settings' dialog box. It contains several sections: 'IP Subnet for IP Resolution' with a dropdown set to 'None'; 'Override RADIUS Security' with a note about the default RADIUS shared secret and a 'Shared Secret' field; and 'Override Reauthentication Behavior' with a note and a 'Reauthentication Type' dropdown. The 'Reauthentication Type' dropdown is open, showing a list of options including 'None', 'Wireless', 'RFC 3576 - Extreme Wireless WING', 'RFC 3576 - Brocade ICX', 'RFC 3576 - Juniper Wireless', 'RFC 3576 - Extreme Identity Wireless', 'RFC 3576 - Extreme Wired', 'RFC 3576 - Generic CoA Colon Delimited', 'RFC 3576 - Extreme Data Center', and 'Session Timeout'. The 'None' option is highlighted. There is also an 'Enable Port Link Control' checkbox.

Click OK. Then Save out of both of the above windows. Then click OK in the Device Save pop-up.



Repeat the same steps for all VSP switches added to XIQ-SE Control engine.

When done, click Enforce to enforce changes to the Control Engine.

The screenshot shows the 'Access Control' tab in the VSP Edge Deployment with Automation interface. The left sidebar contains navigation options: Network, Alarms & Events, Control, Analytics, Wireless, Reports, Tasks, Administration, and Connect. The main content area displays the 'Engine Group - Default' configuration. The 'Switches' tab is selected, showing a table of switches with columns: IP Address, Nickname, Status, System Name, and Primary Engine. The table lists four switches: VSP-core1, VSP-core2, VSP-edge1, and VSP-edge2, all with a status of 'Contact Established'. Below the table, there are buttons for 'Add...', 'Edit...', 'Delete', and 'Refresh'. At the bottom of the interface, there is a 'Selection...' dropdown menu with options 'All...' (labeled 2) and 'Enforce' (labeled 1). A 'Refresh' button is also present.

IP Address	Nickname	Status	System Name	Primary Engine
10.9.193.131	VSP-core1	Contact Established	VSP-core1	10.9.203.6
10.9.193.132	VSP-core2	Contact Established	VSP-core2	10.9.203.6
10.9.193.133	VSP-edge1	Contact Established	VSP-edge1	10.9.203.6
10.9.193.134	VSP-edge2	Contact Established	VSP-edge2	10.9.203.6

Then click Enforce All.

The screenshot shows the 'Access Control Engine Enforce' dialog box. It contains a table with columns: Engine, IP Address, Status, Result, and Details. The table lists one entry: NAC, 10.9.203.6, Audit Completed, Pass. Below the table, there are checkboxes for 'Force Reconfiguration for All Switches' and 'Force Reconfiguration for Captive Portal'. At the bottom, there are buttons for 'Audit', 'Preview', 'Enforce', 'Enforce All' (highlighted with a red box), and 'Close'.

Engine	IP Address	Status	Result	Details
NAC	10.9.203.6	Audit Completed	Pass	

When the enforce has completed, close the window.

The screenshot shows the 'Access Control Engine Enforce' dialog box after the enforcement process has completed. The table now shows the status 'Enforce Finished' and 'Success'. The 'Enforce All' button remains highlighted with a red box.

Engine	IP Address	Status	Result	Details
NAC	10.9.203.6	Enforce Finished	Success	

Dashboard **Devices** Discovered Firmware Archives Configuration Templates Reports

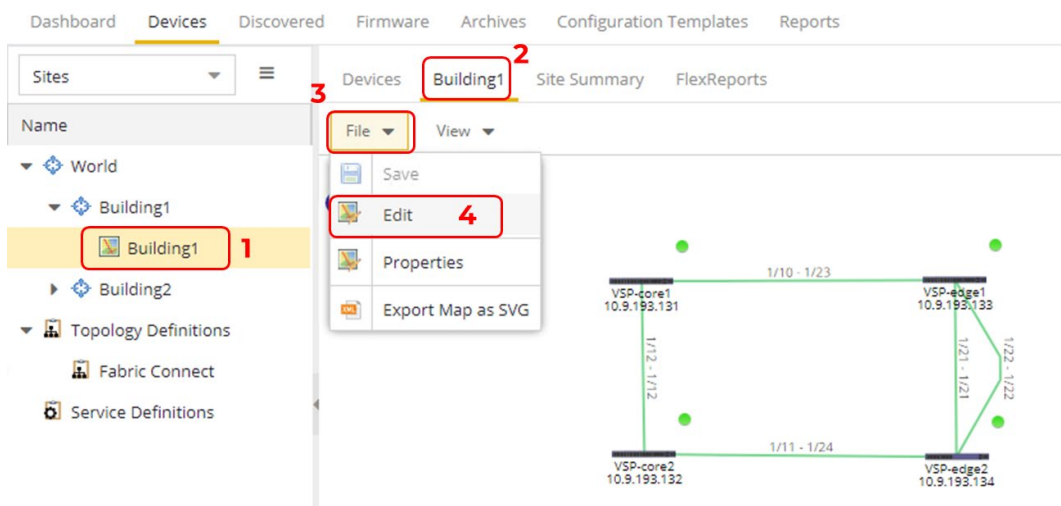
Sites **Devices** Building1 Site Summary Endpoint Locations FlexReports

Name Add Device... Export to CSV

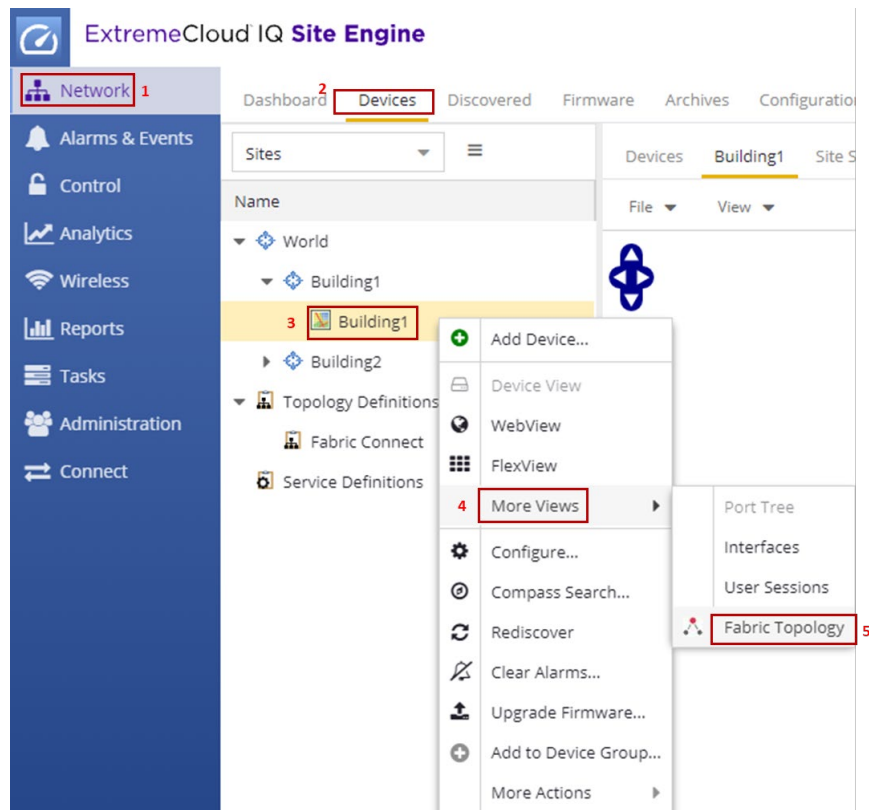
- World
  - Building1**
  - Building2
- Topology Definitions
- Fabric Connect
- Service Definitions

Status	Name ↑	Site	IP Address	Poll Status	Poll Details	Device Type	Family	Firmware
●	VSP-core1	/World/Building1	10.9.193.131	Available: 1...	Up: 263 Down: 0	5520-12MW-36W-FabricEngine	Universal P...	8.6.1.0
●	VSP-core2	/World/Building1	10.9.193.132	Available: 1...	Up: 263 Down: 0	5520-12MW-36W-FabricEngine	Universal P...	8.6.1.0
●	VSP-edge1	/World/Building1	10.9.193.133	Available: 1...	Up: 124 Down: 0	5520-12MW-36W-FabricEngine	Universal P...	8.6.1.0
●	VSP-edge2	/World/Building1	10.9.193.134	Available: 1...	Up: 124 Down: 0	5520-24W-FabricEngine	Universal P...	8.6.1.0

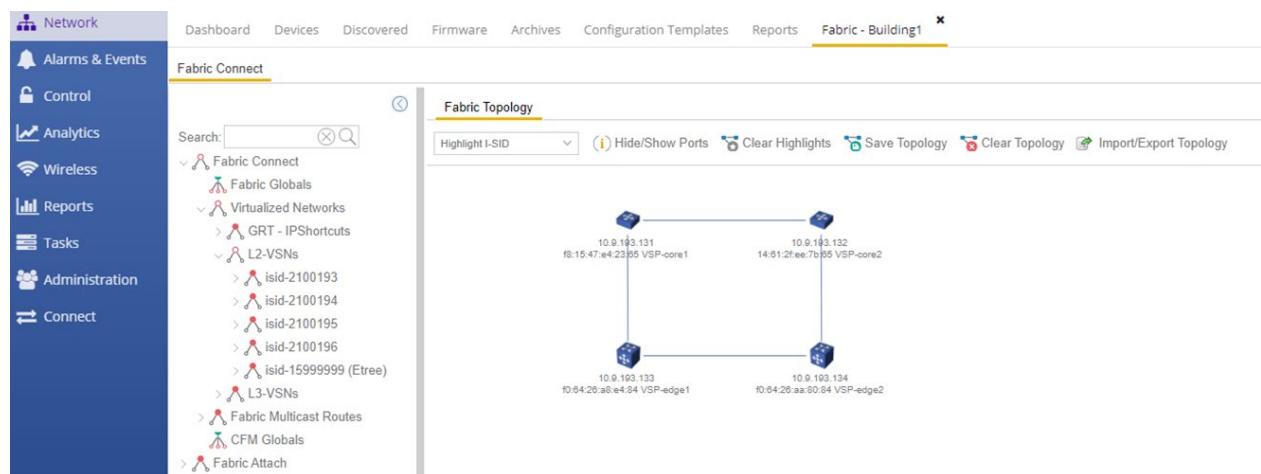
Go to the topology map and arrange the icons.



Right click on the Building1 site and select More Views > Fabric Topology. Note: This step is optional and assumes you have Fabric Manager installed. If that is not the case, then skip this step.



Arrange the map.



The fabric is up, and the fabric services are listed under L2VSN and can be highlighted on the map using the drop-down.

To verify that DVR is operational, SSH to one of the VSPs and run the CLI command `show dvr members`



```
VSP-core1:1# show dvr members
```

DVR Members (Domain ID: 1)				
System Name	Nick-Name	Nodal MAC	Role	SPB Cost
VSP-core1	0.00.01	f0:64:26:95:3c:84	Controller	-
VSP-core2	0.00.02	f0:64:26:a8:90:84	Controller	10
VSP-edge1	a.10.0a	f0:64:26:a8:e4:84	Leaf	10
VSP-edge2	a.10.0b	f0:64:26:aa:80:84	Leaf	20

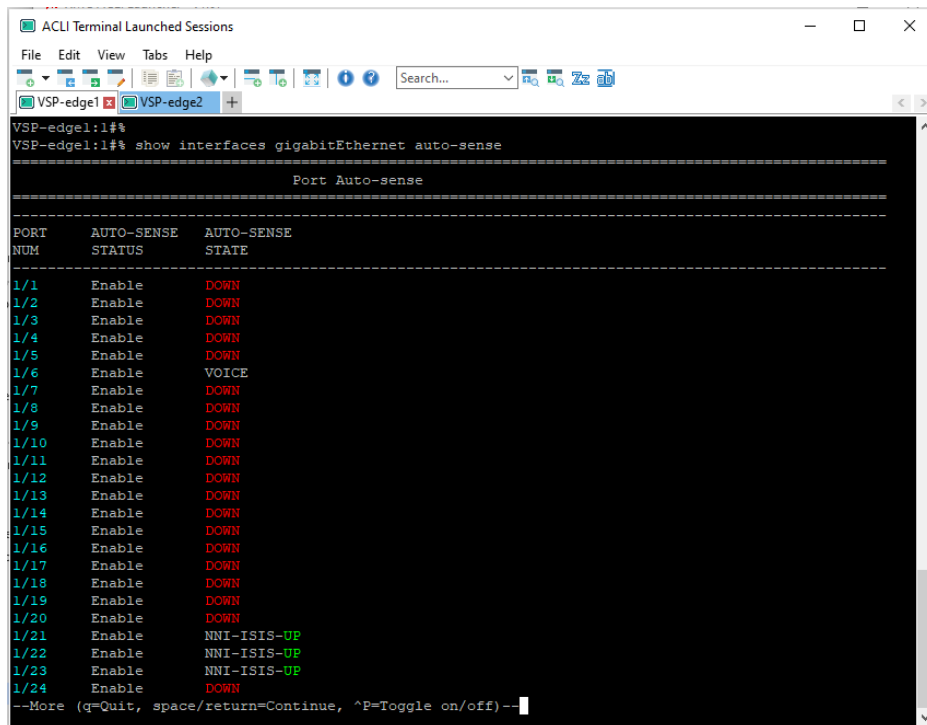
```

4 out of 4 Total Num of DVR Members displayed
accli.pl: Displayed Record Count = 4
VSP-core1:1#
```

The VSP cores are shown as DVR Controllers and the VSP Edge switches as DVR Leaf nodes.

## Inspect the Auto-Sense Ports on the VSP Edge Switches

Connect using SSH to both VSP edge switches. Run the CLI command `show interfaces gigabitEthernet auto-sense`



```
VSP-edge1:1# show interfaces gigabitEthernet auto-sense
```

Port Auto-sense		
PORT NUM	AUTO-SENSE STATUS	AUTO-SENSE STATE
1/1	Enable	DOWN
1/2	Enable	DOWN
1/3	Enable	DOWN
1/4	Enable	DOWN
1/5	Enable	DOWN
1/6	Enable	VOICE
1/7	Enable	DOWN
1/8	Enable	DOWN
1/9	Enable	DOWN
1/10	Enable	DOWN
1/11	Enable	DOWN
1/12	Enable	DOWN
1/13	Enable	DOWN
1/14	Enable	DOWN
1/15	Enable	DOWN
1/16	Enable	DOWN
1/17	Enable	DOWN
1/18	Enable	DOWN
1/19	Enable	DOWN
1/20	Enable	DOWN
1/21	Enable	NNI-ISIS-UP
1/22	Enable	NNI-ISIS-UP
1/23	Enable	NNI-ISIS-UP
1/24	Enable	DOWN

```
--More (q=Quit, space/return=Continue, ^P=Toggle on/off)--
```

Note that VSP-edge1 is in the auto-sense Voice state on port 1/6 where the Telephone is connected, and ports 1/21-1/23 are in the auto-sense NNI-ISIS-UP state. Ports 1/21-1/23 are the fabric interconnects that were automatically configured.

Similarly, VSP-edge2 port 1/6 is in the auto-sense FA-WAP state where the Extreme Access Point is connected, and fabric NNI links 1/21-1/22,1/24 are in the auto-sense NNI-ISIS-UP state.

```
VSP-edge2:1# show interfaces gigabitEthernet auto-sense
```

Port Auto-sense		
PORT NUM	AUTO-SENSE STATUS	AUTO-SENSE STATE
1/1	Enable	DOWN
1/2	Enable	DOWN
1/3	Enable	DOWN
1/4	Enable	DOWN
1/5	Enable	DOWN
1/6	Enable	FA-WAP
1/7	Enable	DOWN
1/8	Enable	DOWN
1/9	Enable	DOWN
1/10	Enable	DOWN
1/11	Enable	DOWN
1/12	Enable	DOWN
1/13	Enable	DOWN
1/14	Enable	DOWN
1/15	Enable	DOWN
1/16	Enable	DOWN
1/17	Enable	DOWN
1/18	Enable	DOWN
1/19	Enable	DOWN
1/20	Enable	DOWN
1/21	Enable	NNI-ISIS-UP
1/22	Enable	NNI-ISIS-UP
1/23	Enable	DOWN
1/24	Enable	NNI-ISIS-UP

```
VSP-edge2:1#
```

## Verify the WLAN AP Is Operational

Connect to Extreme Campus Controller (XCC) and go to Monitor > Devices > Access points. Make sure the AP is online and green. It should have an IP address on the AP-Mgmt I-SID 2100194 in subnet 10.9.194.0/24.

Status	Name	IP Address	Site	Version	Model	Radio 1	Radio 2	R1 Clients	R2 Clients
Online	Edge-WAP	10.9.194.100	Fabric Edge Sandbox	7.4.1.0-016R	AP505i-FCC	Off	Off	0	0

On VSP-edge2, inspect the I-SIDs configured on AP port 1/6 with the CLI command `show interface gigabitEthernet i-sid 1/6`

```
VSP-edge2:1# show interface gigabitEthernet i-sid 1/6
```

PORT Isid Info										
PORTNUM	IFINDEX	ISID ID	VLANID	C-VID	ISID TYPE	ORIGIN	ISID NAME	BPDU	MAC	SUNI
1/6	197	2100194	N/A	untag	ELAN	- - - - E1-	ISID-2100194	disabled	FALSE	
1/6	197	2100196	3	196	ELAN	- D1- - - -	ISID-2100196		FALSE	

```
2 out of 2 Total Num of i-sid endpoints displayed
acl1.pl: Displayed Record Count = 2
ORIGIN Legend:
C: manually configured; D: discovered by FA or EPT
M: FA management; E: discovered by EAP; A: auto-sense
l: discover by local switch r: discover by remote VIST switch
VSP-edge2:1#
```

Note: There are two bindings on the port where the AP is connected. The first binding was created by RADIUS authentication when the AP was first onboarded and corresponds to the AP-Mgmt I-SID. Confirm this by inspecting the MAC authentications on the switch by running the CLI command `show eapol multihost non-eap-mac status`

```
VSP-edge2:1#% show eapol multihost non-eap-mac status
```

Non-Eap Oper Status								
PORT NUM	MAC	STATE	VLAN ID	PRI	Flex-UNI Enable	I-SID SOURCE	NON-EAP AUTH	VLAN:I-SID
1/6	dc:b8:08:c2:80:79	authenticated	N/A	1	true	radius	radius	0:2100194

```
Total Number of NEAP Sessions: 1
VSP-edge2:1#%
```

Note that there is a MAC address authenticated on port 1/6 and the AP-Mgmt I-SID was assigned to the port using RADIUS.

Go to the XIQ-SE Control > End Systems tab.

Stk	Last Seen	MAC Address	MAC OUI Vendor	Device Family	Device Type	IP Address	Host Name	User Name	Authentication Type	Reason	Profile
1	2020/02/11 10:41:12 PM	DC:B8:08:C2:80:79	Extreme Networ...	Wireless Access Point	Extreme Wireless Access Point				MAC (RADIUS)	Rule: "Access Point"	Access Point MAC Profile

Inspect the port's EAPoL config by running the CLI command `show eapol port 1/6`

```
VSP-edge2:1#% show eapol port 1/6 ^mhsa
```

Eapol Configuration																					
PORT NUM	STATUS	OPER MODE	DYN	Flex-UNI ENABLE	MAX REQ	QUIET INTVL	REAUTH PERIOD	REAUTH ENABLE	NON-EAP ENABLE	LLDP-AUTH ENABLE	MAX MAC	MAX EAP	MAX NEAP	GST VLAN	GST I-SID	FAIL VLAN	FAIL I-SID	COA ENABLE	ADMIN TRAFFIC CONTROL	OPER TRAFFIC CONTROL	ORIGIN
1/6	Auto	MHSA	true	true	2	60	3600	false	true	false	2	2	2	N/A	15999999	N/A	N/A	false	in-out	in	AUTO-SENSE

```
VSP-edge2:1#%
```

Note that Dynamic MHSA is true. Port 1/6 is now open for all MACs behind the AP.

The second binding on the 1/6 port was discovered using Fabric Attach and is the Data I-SID binding for which the AP received the config from XCC.

**Edit VLAN**

Name: Data Building1

Mode: Fabric Attach

VLAN ID: 196 Tagged: ☒

I-SID: 2100196

ADVANCED

CANCEL Save

Confirm by inspecting the Fabric Attach assignments on the switch with the CLI command `show fa assignment`

As shown, the Data I-SID and VLAN are now configured on port 1/6.

```
VSP-edge2:1#% show fa assignment
```

Fabric Attach Assignment Map					
Interface	I-SID	Vlan	State	Origin	I-SID Name
1/6	2100196	196	active	client	ISID-2100196

The AP is fully operational and is ready to service wireless clients in Building1.

## Verify the IP Phone Is Operational

On VSP-edge1, view the I-SIDs that are configured on the phone port 1/6 using the CLI command `show interface gigabitEthernet i-sid 1/6`

```
VSP-edge1:1#% show interface gigabitEthernet i-sid 1/6
```

PORT Isid Info									
PORTNUM	IFINDEX	ISID ID	VLANID	C-VID	ISID TYPE	ORIGIN	ISID NAME	BPDU	MAC SUNI
1/6	197	2100195	2	195	ELAN	- - - - A	Auto-sense Voice		FALSE
1/6	197	2100196	3	untag	ELAN	- - - - El-	ISID-2100196	disabled	TRUE
1/6	197	15999999	4048	untag	ELAN	- - - - El-	Onboarding I-SID	disabled	FALSE

```

3 out of 3 Total Num of i-sid endpoints displayed
acl1.pl: Displayed Record Count = 3
ORIGIN Legend:
C: manually configured; D: discovered by FA or EPT
M: FA management; E: discovered by EAP; A: auto-sense
l: discover by local switch r: discover by remote VIST switch
VSP-edge1:1#%

```

Note that there are three bindings on the phone port. The first binding is the Voice I-SID 2100195, which was assigned by auto-sense when the telephone was detected via LLDP signaling. This is a tagged binding because it shows VLAN-id 195 in the C-VID column.

Inspect the LLDP neighbor details on the same port using the CLI command `show lldp neighbor port 1/6`

```
VSP-edge1:1#% show lldp neighbor port 1/6
```

LLDP Neighbor	
Port: 1/6	Index : 6977
	Protocol : LLDP
	ChassisId: Network Address 10.9.195.100
	PortId : MAC Address 00:08:5d:62:bf:f0
	SysName : regDN 4052,MINET_6920
	SysCap : BT / BT
	PortDescr: LAN port
	SysDescr : regDN 4052,MINET_6920,ver: 01.05.00.075,PxE: 6.5,01/01/1970 10:31:56 +0000
	Address : 10.9.195.100
	IPv6 Address : 0:0:0:0:0:0:0:0

```

Total Neighbors : 1

Capabilities Legend: (Supported/Enabled)
B= Bridge, D= DOCSIS, O= Other, R= Repeater,
S= Station, T= Telephone, W= WLAN, r= Router
VSP-edge1:1#%

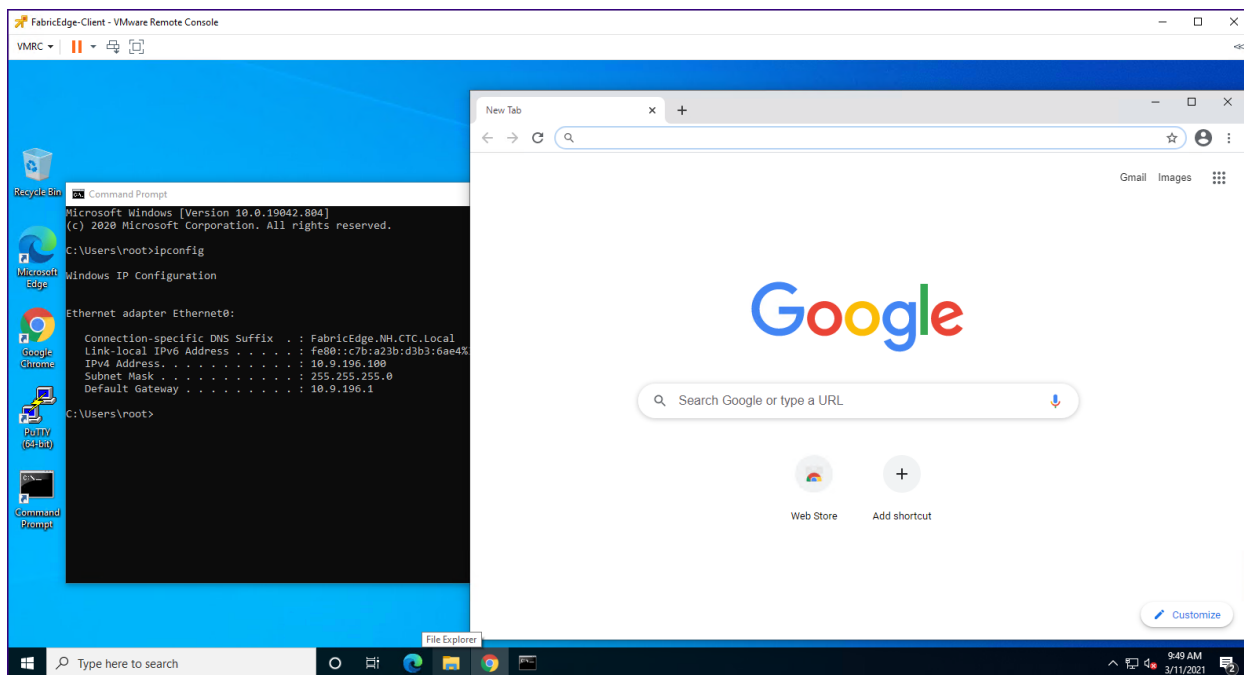
```

Note the neighbor system capabilities: B = Bridge and T = Telephone. Also note the IP address the phone obtained and in the Voice I-SID subnet. Ping the phone's IP address.

```
VSP-core1:1#% ping 10.9.195.100
Sending ping in context grt with source IP 10.9.193.129
10.9.195.100 is alive
VSP-core1:1#%
```

## Verify Client PC Authentication

Verify the client PC obtained an IP address on Data I-SID 2100196 and IP subnet 10.9.196.0/24. As shown below, the PC has obtained an IP address on the Data subnet.



On VSP-edge1 port 1/6, where the phone is connected, show the I-SID bindings.

```
VSP-edge1:1# show interface gigabitEthernet i-sid 1/6
```

PORT Isid Info										
PORTNUM	IFINDEX	ISID ID	VLANID	C-VID	ISID TYPE	ORIGIN	ISID NAME	BFDU	MAC	SUNI
1/6	197	2100195	2	195	ELAN	- - - - A	Auto-sense Voice			FALSE
1/6	197	2100196	3	untag	ELAN	- - - - E1-	ISID-2100196	disabled	TRUE	
1/6	197	15999999	4048	untag	ELAN	- - - - E1-	Onboarding I-SID	disabled	FALSE	

```

3 out of 3 Total Num of i-sid endpoints displayed
ac11.pl: Displayed Record Count = 3
ORIGIN Legend:
C: manually configured; D: discovered by FA or EPT
M: FA management; E: discovered by EAP; A: auto-sense
l: discover by local switch r: discover by remote VIST switch
VSP-edge1:1#

```

The first binding is the phone and will be covered in the next section. The second binding is untagged and is the PC that was RADIUS authenticated by Extreme Control. The third binding is the default Onboarding I-SID which is assigned to every auto-sense port.

Confirm both the first and second bindings by inspecting the MAC authentications on the switch, using the CLI command `show eapol sessions neap`

```
VSP-edge1:1# show eapol sessions neap
```

Non-Eap Oper Status									
PORT NUM	MAC	STATE	VLAN ID	PRI	Flex-UNI Enable	I-SID SOURCE	NON-EAP AUTH	VLAN: I-SID	
1/6	00:08:5d:62:bf:f0	authenticated	N/A	N/A	true	n/a	lldp	195:2100195	
1/6	00:50:56:80:5d:ca	authenticated	N/A	0	true	radius	radius	0:2100196	

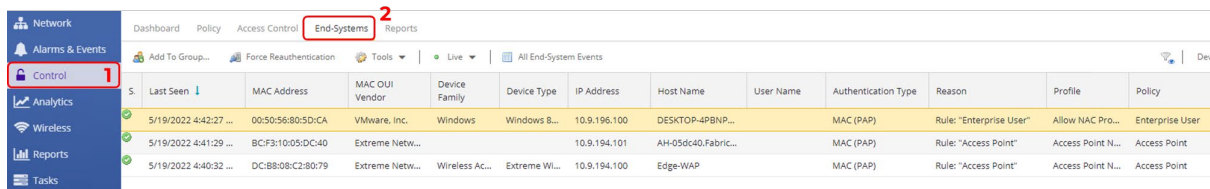
```

Total Number of NEAP Sessions: 2
VSP-edge1:1#

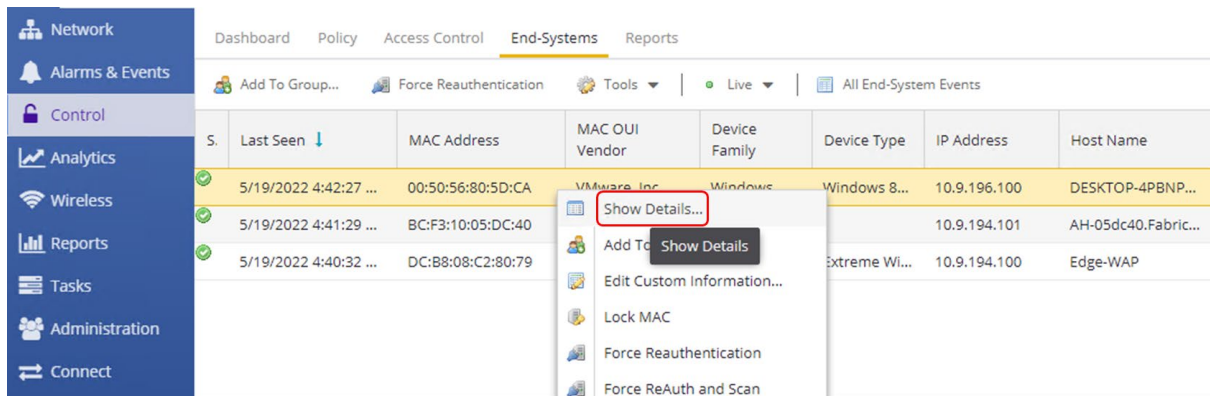
```

The first MAC is the phone. It was authenticated via LLDP. The second MAC is the client PC, and it was authenticated via RADIUS. Notice that the RADIUS attribute has a null VLAN-id which results in an untagged binding for the Data I-SID on the port.

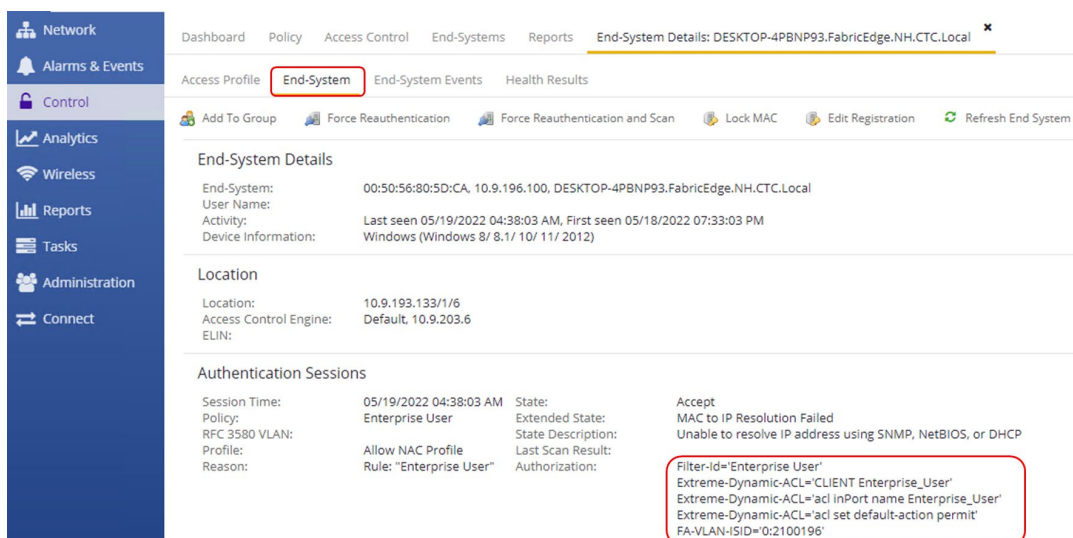
Go to the XIQ-SE Control > End Systems tab.



In XIQ-SE Control, only the client PC is shown. To see the RADIUS attributes sent to the switch, right click on the entry and select "Show Details."



Select the "End Systems" tab.

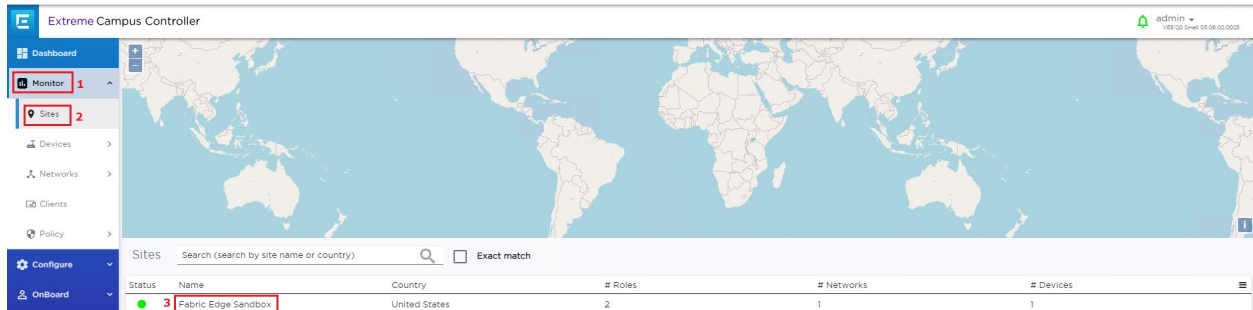


In Authentication Sessions, note the outbound RADIUS attributes which include a "permit all" dynamic ACL and the VLAN:ISID for the PC. (VLAN 0 denotes untagged access.)

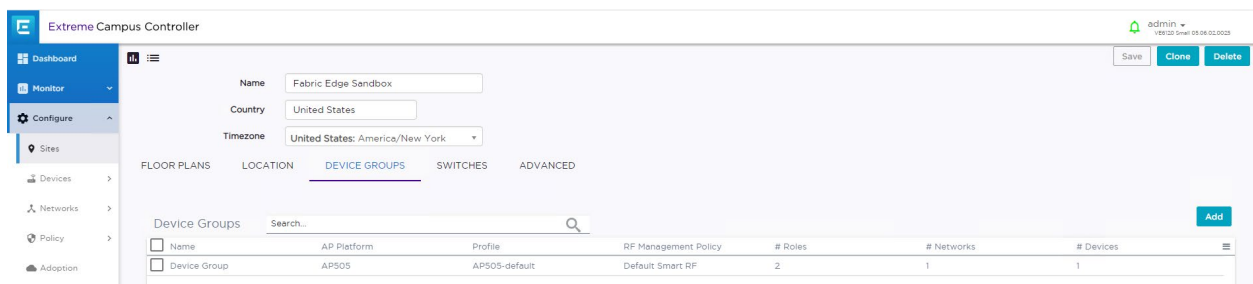
## Appendix

### XCC Preexisting Configuration Review

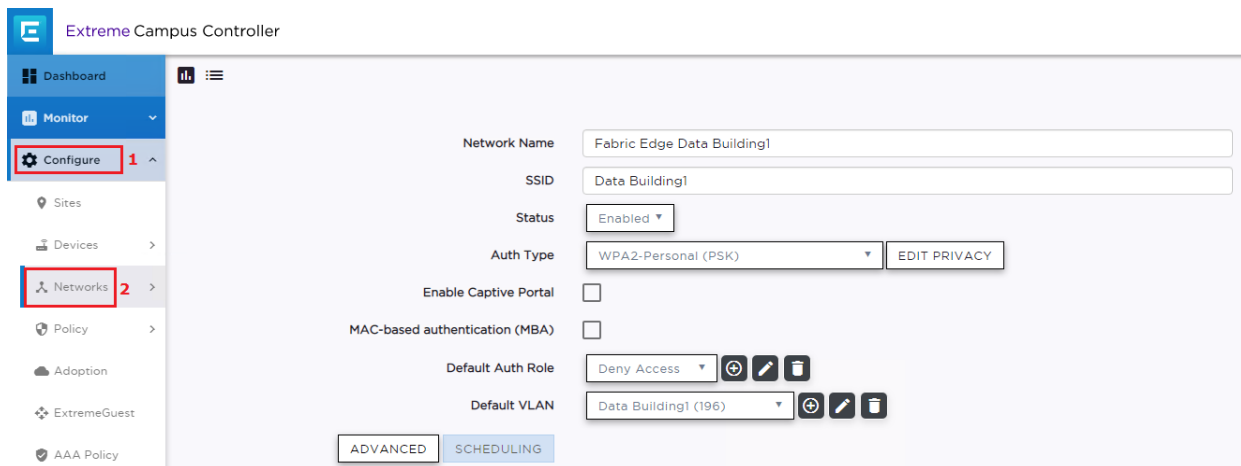
Use this XCC configuration to validate the WLAN AP autosense adoption.



There is a single Device Group for our AP505.



The following WLAN Network is defined and assigned to the above Device Group.



And the associated VLAN is in Fabric Attach mode with the VLAN & I-SID for Building1 only.

Edit VLAN

Name

Data Building1

Mode

Fabric Attach

VLAN ID

196

Tagged

☒

I-SID

2100196

ADVANCED

CANCEL

Save



## Terms & Conditions of Use

---

Extreme Networks, Inc. reserves all rights to its materials and the content of the materials. No material provided by Extreme Networks, Inc. to a Partner (or Customer, etc.) may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording, or by any information storage or retrieval system, or incorporated into any other published work, except for internal use by the Partner and except as may be expressly permitted in writing by Extreme Networks, Inc.

This document and the information contained herein are intended solely for informational use. Extreme Networks, Inc. makes no representations or warranties of any kind, whether expressed or implied, with respect to this information and assumes no responsibility for its accuracy or completeness. Extreme Networks, Inc. hereby disclaims all liability and warranty for any information contained herein and all the material and information herein exists to be used only on an "as is" basis. More specific information may be available on request. By your review and/or use of the information contained herein, you expressly release Extreme from any and all liability related in any way to this information. A copy of the text of this section is an uncontrolled copy, and may lack important information or contain factual errors. All information herein is Copyright ©Extreme Networks, Inc. All rights reserved. All information contain in this document is subject to change without notice.

For additional information refer to: <http://www.extremenetworks.com/company/legal/terms/>