



VSP Edge Deployment Guide without NAC

9037928-00 Rev AA
October 2023



Copyright © 2023 Extreme Networks, Inc. All rights reserved.

Legal Notice

, 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 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

and the logo are trademarks or registered trademarks of , 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 trademarks, see:

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/>



Table of Contents

Preface.....	5
Text Conventions.....	5
Documentation and Training.....	6
Open Source Declarations.....	7
Training.....	7
Help and Support.....	7
Subscribe to Product Announcements.....	8
Send Feedback.....	8
Overview.....	9
Prerequisites.....	9
Objectives.....	9
Network Diagram.....	10
Pre-Existing Configuration.....	12
ExtremeCloud IQ - Site Engine Preparation for VSP Edge	14
Site Creation.....	14
Admin Profile Creation.....	14
Fabric Topology Definitions.....	15
ExtremeCloud IQ - Site Engine Add-On Scripts and Workflows	16
VSP Core Preparation for Automated VSP Edge.....	20
Site Selection.....	20
Applying DVR Controller, VLAN and IP Configuration.....	22
Applying Seed Configuration for Zero Touch Fabric	24
Preparing ExtremeCloud IQ - Site Engine for Fully Automated Edge Deployment	26
Configuration of ZTP+.....	26
Preparing Universal Hardware Edge OS Conversion	29
Preparing via ExtremeCloud IQ	31
Preparing via ExtremeCloud IQ - Site Engine Workflow	31
Configuration of ExtremeCloud IQ - Site Engine workflow for VSP onboarding	33
Manual Run of ExtremeCloud IQ - Site Engine Workflow on VSP Core Nodes	36
Deployment of Edge Switches.....	41
Onboarding of VSP Edge Switches.....	42
OS Conversion via ExtremeCloud IQ	42
OS Conversion via ExtremeCloud IQ - Site Engine Workflow.....	42
VSP Edge Onboarding Steps	44
Manual Steps Required if OS Conversion Was Done via ExtremeCloud IQ	46
Observing ExtremeCloud IQ - Site Engine Onboarding Workflow Completion	48
Migrating VSP Edge to Dedicated Switch mgmt CLIP.....	49

Verification that All End-Devices Are Operational.....	54
Inspection of VSP Fabric	54
Inspection of Endpoint Auto-Sense.....	56
Verification that WLAN AP Is in Service	58
Verification that IP Phone Is in Service.....	59
Verification that Client PC Is on Data I-SID	60
Appendix – Final Configurations.....	62
VSP-core1	62
VSP -core2	72
VSP -edge1	83
VSP -edge2	92



Preface

Read the following topics to learn about:

- The meanings of text formats used in this document.
- Where you can find additional information and help.
- How to reach us with questions and comments.

Text Conventions

Unless otherwise noted, information in this document applies to all supported environments for the products in question. Exceptions, like command keywords associated with a specific software version, are identified in the text.

When a feature, function, or operation pertains to a specific hardware product, the product name is used. When features, functions, and operations are the same across an entire product family, such as ExtremeSwitching switches or SLX routers, the product is referred to as *the switch* or *the router*.

Table 1: Notes and warnings






Icon	Notice type	Alerts you to...
	Tip	Helpful tips and notices for using the product
	Note	Useful information or instructions
	Important	Important features or instructions
	Caution	Risk of personal injury, system damage, or loss of data
	Warning	Risk of severe personal injury

Table 2: Text

Convention	Description
screen displays	This typeface indicates command syntax, or represents information as it is displayed on the screen.
The words <i>enter</i> and <i>type</i>	When you see the word <i>enter</i> in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says <i>type</i> .
Key names	Key names are written in boldface, for example Ctrl or Esc . If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press Ctrl+Alt+Del
<i>Words in italicized type</i>	Italics emphasize a point or denote new terms at the place where they are defined in the text. Italics are also used when referring to publication titles.
NEW!	New information. In a PDF, this is searchable text.

Table 3: Command syntax

Convention	Description
bold text	Bold text indicates command names, keywords, and command options.
<i>italic text</i>	Italic text indicates variable content.
[]	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
{ x y z }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
x y	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, such as passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, <i>member[member...]</i> .
\	In command examples, the backslash indicates a “soft” line break. When a backslash separates two lines of a command input, enter the entire command at the prompt without the backslash.

Documentation and Training

Find Extreme Networks product information at the following locations:

[Current Product Documentation](#)

[Release Notes](#)

[Hardware and Software Compatibility](#) for Extreme Networks products
[Extreme Optics Compatibility](#)
[Other Resources](#) such as articles, white papers, and case studies

Open Source Declarations

Some software files have been licensed under certain open source licenses. Information is available on the [Open Source Declaration](#) page.

Training

Extreme Networks offers product training courses, both online and in person, as well as specialized certifications. For details, visit the [Extreme Networks Training](#) page.

Help and Support

If you require assistance, contact using one of the following methods:

Extreme Portal

Search the GTAC (Global Technical Assistance Center) knowledge base; manage support cases and service contracts; download software; and obtain product licensing, training, and certifications.

The Hub

A forum for customers to connect with one another, answer questions, and share ideas and feedback. This community is monitored by employees, but is not intended to replace specific guidance from GTAC.

Call GTAC

For immediate support: (800) 998 2408 (toll-free in U.S. and Canada) or 1 (408) 579 2800. For the support phone number in your country, visit www.extremenetworks.com/support/contact.

Before contacting for technical support, have the following information ready:

- Your service contract number, or serial numbers for all involved products
- A description of the failure
- A description of any actions already taken to resolve the problem
- A description of your network environment (such as layout, cable type, other relevant environmental information)
- Network load at the time of trouble (if known)
- The device history (for example, if you have returned the device before, or if this is a recurring problem)
- Any related RMA (Return Material Authorization) numbers

Subscribe to Product Announcements

You can subscribe to email notifications for product and software release announcements, Field Notices, and Vulnerability Notices.

1. Go to [The Hub](#).
2. In the list of categories, expand the **Product Announcements** list.
3. Select a product for which you would like to receive notifications.
4. Select **Subscribe**.
5. To select additional products, return to the **Product Announcements** list and repeat steps 3 and 4.

You can modify your product selections or unsubscribe at any time.

Send Feedback

The User Enablement team at has made every effort to ensure that this document is accurate, complete, and easy to use. We strive to improve our documentation to help you in your work, so we want to hear from you. We welcome all feedback, but we especially want to know about:

- Content errors, or confusing or conflicting information.
- Improvements that would help you find relevant information.
- Broken links or usability issues.

To send feedback, email us at .

Provide as much detail as possible including the publication title, topic heading, and page number (if applicable), along with your comments and suggestions for improvement.



Overview

[Prerequisites](#) on page 9

[Objectives](#) on page 9

[Network Diagram](#) on page 10

This guide describes the steps needed to automate the deployment of a VSP switch running VSP Operating System Software (VOSS) 8.3 or later in environments where Network Access Control (NAC) is not used. The process uses a combination of automation features in VOSS Fabric Connect and in ExtremeCloud™ IQ - Site Engine onboarding.

Prerequisites

- An existing Fabric Connect core switch running VSP Operating System Software (VOSS) 8.3 or later
- Extreme Management Center (XMC) 8.5 or later, or ExtremeCloud IQ - Site Engine version 21.9 or later (this guide uses ExtremeCloud IQ - Site Engine)
- A DHCP/DNS server reachable on the existing Fabric Connect network
- An active ExtremeCloud IQ account for running ExtremeCloud IQ - Site Engine and for changing the switch persona from ExtremeXOS (EXOS) to VOSS

Objectives

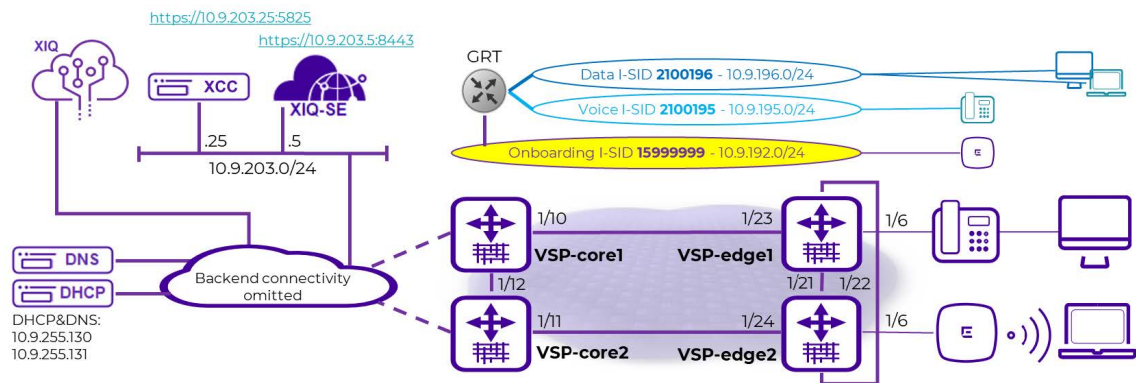
This guide describes the steps needed to automate the deployment of a VSP switch using a combination VSP Fabric Connect automation features and ExtremeCloud IQ - Site Engine, without the use of Network Access Control (NAC). In particular, this guide describes the following:

- Preparing ExtremeCloud IQ - Site Engine for a successful automated, zero-touch deployment of a VSP switch
- Automating VSP ZTP+ provisioning
- Converting a universal hardware switch from EXOS to VOSS using ExtremeCloud IQ or ExtremeCloud IQ - Site Engine
- Using VSP Zero Touch Fabric and port auto-sense functionality

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. These represent an existing customer Fabric Connect deployment.
- Two universal-hardware switches as edge/access switches. Any VSP switch will work as an edge switch if it supports VOSS 8.3 or later.
- One IP phone; Mitel 6920 model.
- One Extreme Wireless AP, model AP505i.
- One client VM acting as the wired client connected behind the phone.
- One ExtremeCloud IQ - Site Engine instance.
- One Extreme Campus Controller (XCC) instance.
- ExtremeCloud IQ profile for onboarding the universal hardware 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 ExtremeCloud IQ - Site Engine. 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 use ExtremeCloud IQ - Site Engine ZTP+ and the VOSS Zero Touch Fabric functionality to achieve a typical VSP edge deployment with the following characteristics:

- No more 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 edge VSPs have no connection at all on their OOB Ethernet management ports, which is customary in campus access deployments. All management of these switches is inband and shows how VOSS 8.3 Zero Touch Fabric solves the chicken-and-egg problem of past times: cannot manage the switch inband until Fabric is deployed; cannot deploy Fabric without having management access to switch.

At the end of the deployment, all connected endpoints (IP phone, AP, client) must be operational without any need to have performed any manual configuration on the VSP edge switches and in particular on any of the access ports.

It should be noted that some fabric *seed* configuration is initially be required on the VSP core, and this guide covers that configuration in detail. But the real gains of Zero Touch Fabric are realized when deploying the large quantities of edge access switches in any Fabric design.

The same network diagram tries to depict both the physical topology of the setup as well as the logical Fabric topology when deployed. The latter comprises 3 L2 VSNs where each is allocated an I-SID and an IP subnet.

The onboarding I-SID 15999999 is a special I-SID which is always unique across the whole Fabric (or area, if SPB multi-area is in use). This is because it is the default I-SID that a newly unboxed VSP, with no configuration, always uses when onboarding itself after it has joined the existing fabric.

The other two L2 VSNs are the Voice I-SID for the IP phones and the Data I-SID for client connectivity. Currently, if Network Access Control (NAC) is not in use, only one global Data I-SID can be set on the VSP edge. As of VOSS 8.4.2, it is possible to set a different Data ISID per port, and in a future version of ExtremeCloud IQ - Site Engine it will be possible to set these via ZTP+ port templates. This guide will be updated when these enhancements become available.

All these L2 VSNs are IP routed in the base GRT (VRF-0) of the core VSPs and edge DVRLeaf nodes. Use of VRF and L3VSNs is of course possible but is not be covered in this guide as it changes nothing from the VSP to the edge model.



Pre-Existing Configuration

A review of the Extreme Campus Controller pre-existing configuration. Extreme Campus Controller has already been configured with one site for the VSP edge Deployment.

Status	Name	Country	# Roles	# Networks	# Devices
●	Fabric Edge Sandbox	United States	2	1	1

With a single device group for our AP505.

Name	AP Platform	Profile	RF Management Policy	# Roles	# Networks	# Devices
Device Group	AP505	AP505-default	Default Smart RF	2	1	1

The following WLAN network is defined and assigned to the above device group.

Network Name: Fabric Edge Data Building1
SSID: Data Building1
Status: Enabled
Auth Type: WPA2-Personal (PSK) [EDIT PRIVACY]
Enable Captive Portal:
MAC-based authentication (MBA):
Default Auth Role: Deny Access
Default VLAN: Data Building1 (196)

And the associated VLAN is in fabric attach mode with the VLAN and I-SID.

Edit VLAN

Name Data Building1

Mode Fabric Attach

VLAN ID 196 **Tagged**

I-SID 2100196

ADVANCED

CANCEL Save



ExtremeCloud IQ - Site Engine Preparation for VSP Edge

Site Creation

Under ExtremeCloud IQ - Site Engine Network, the following sites are created:

The screenshot shows the ExtremeCloud IQ Site Engine interface. The 'Network' menu is highlighted with a red box and the number '1'. The 'Devices' tab is selected with a red box and the number '2'. The interface displays a tree view on the left with 'World' expanded to show 'Building1' and 'Building2'. A table on the right lists the 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.

In this deployment guide the VSP edge switches are onboarded into the Building1 site

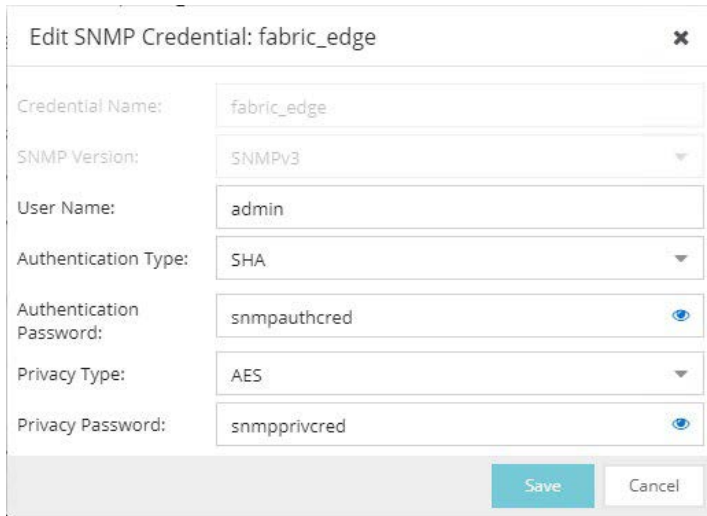
Admin Profile Creation

Under Administration, the following admin profile is created to manage the switches:

The screenshot shows the ExtremeCloud IQ Administration interface. The 'Administration' menu is highlighted with a red box and the number '1'. The 'Profiles' tab is selected with a red box and the number '2'. A table lists the admin 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

Which uses these SNMP credentials:

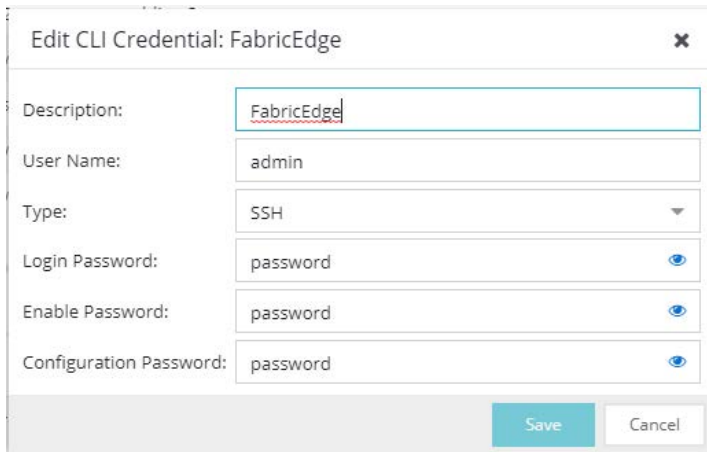


The screenshot shows a dialog box titled "Edit SNMP Credential: fabric_edge". It contains the following fields:

- 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, there are "Save" and "Cancel" buttons.

And these CLI credentials:



The screenshot shows a dialog box titled "Edit CLI Credential: FabricEdge". It contains the following fields:

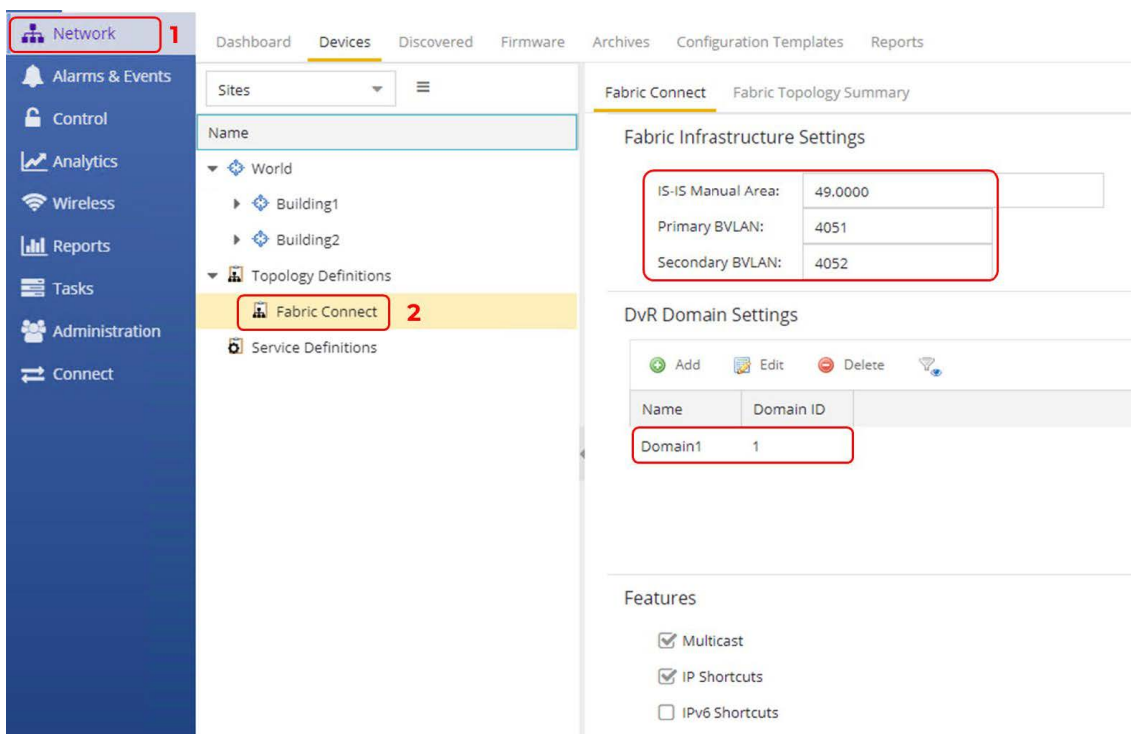
- Description: FabricEdge
- User Name: admin
- Type: SSH
- Login Password: password
- Enable Password: password
- Configuration Password: password

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

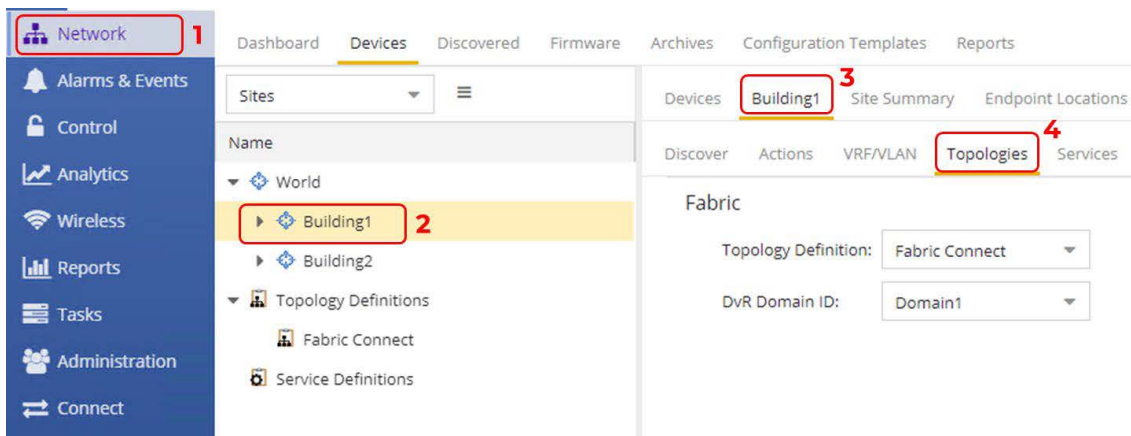
These are non-default credentials, so they illustrate how ZTP+ is able to configure these credentials on the switch when it is onboarded for the first time.

Fabric Topology Definitions

Under **ExtremeCloud IQ - Site Engine Network > Topology** definitions, the following **Fabric Connect** topology settings are configured.



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



The VSP cores are already fabric configured. But when onboarding the VSP edge, the *Onboard VSP* workflow automatically converts the VSP edge into DVR Leaf nodes, and for this to happen the workflow must be able to read the DVR Domain ID from the site.

ExtremeCloud IQ - Site Engine Add-On Scripts and Workflows

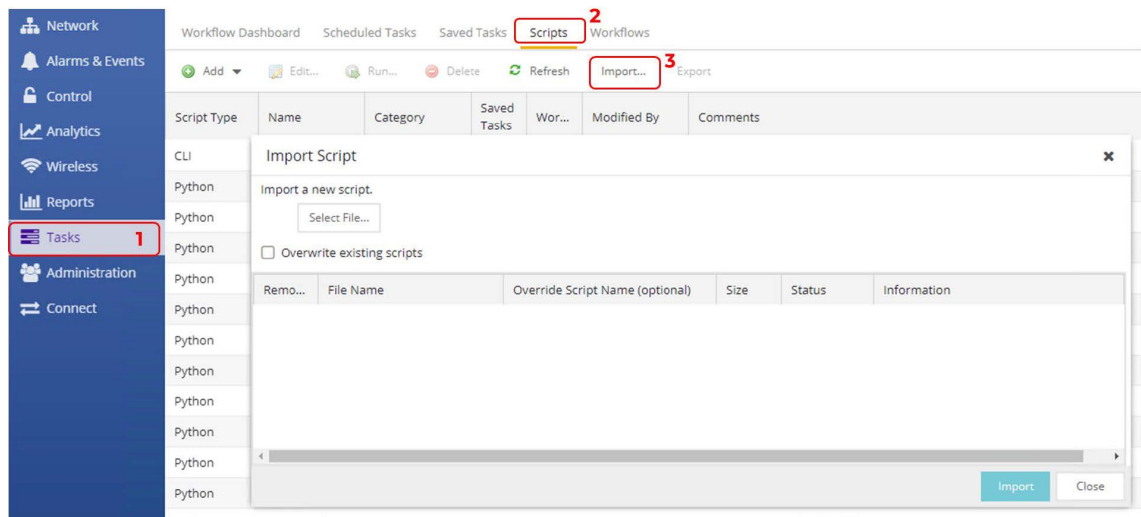
The following ExtremeCloud IQ - Site Engine scripts and workflows from GitHub are used for automating the deployment of VSP edge.

Name	Type	GitHub URL
Move to CLIP Mgmt IP	Script	https://github.com/extremenetworks/

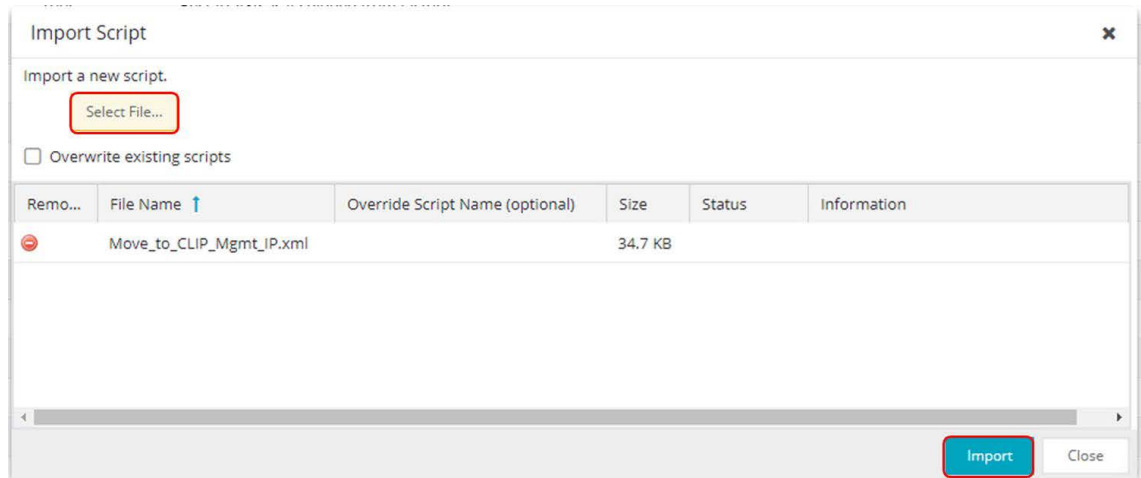
Name	Type	GitHub URL
		ExtremeScripting/tree/master/Netsight/oneview_CLI_scripts
Change persona to VOSS	Workflow	https://github.com/extremenetworks/ExtremeScripting/tree/master/Netsight/oneview_workflows
Onboard VSP	Workflow	https://github.com/extremenetworks/ExtremeScripting/tree/master/Netsight/oneview_workflows

The script named **Move to CLIP Mgmt IP** is downloaded using right-click and **Save link as....**

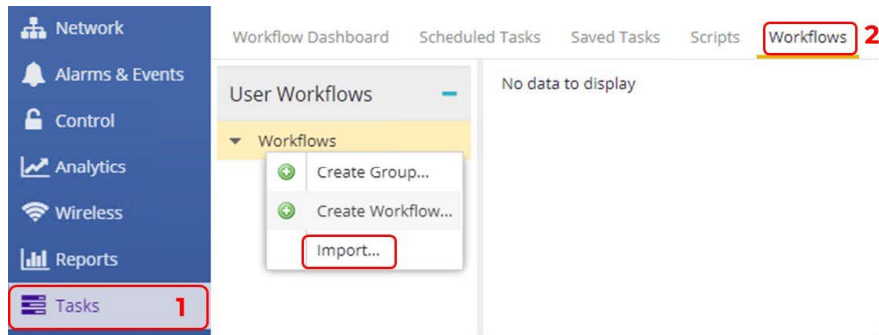
Then the script is imported into ExtremeCloud IQ - Site Engine by selecting **Tasks > Scripts > Import....**



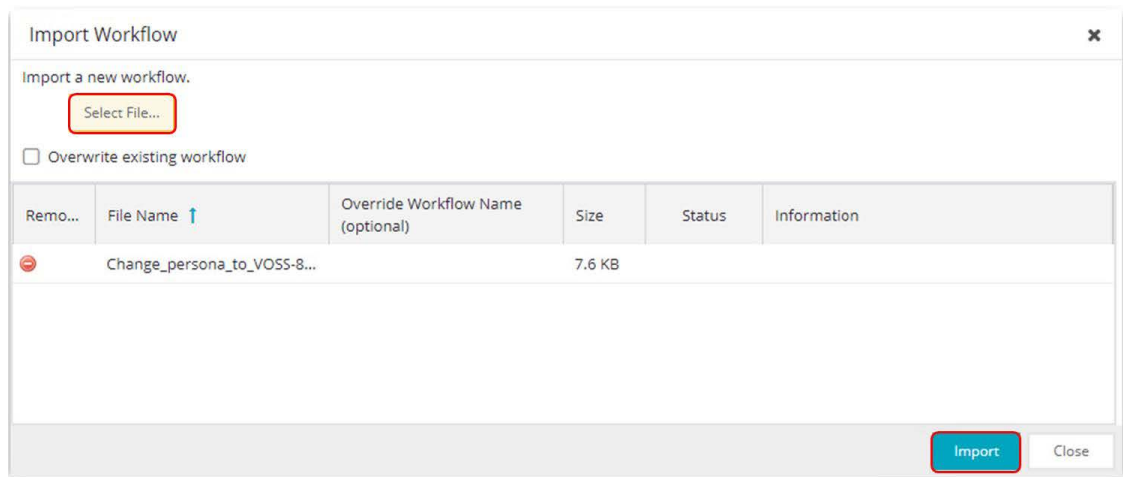
Then by selecting the XML file downloaded from GitHub, selecting the **Import** button, and selecting **Close**.



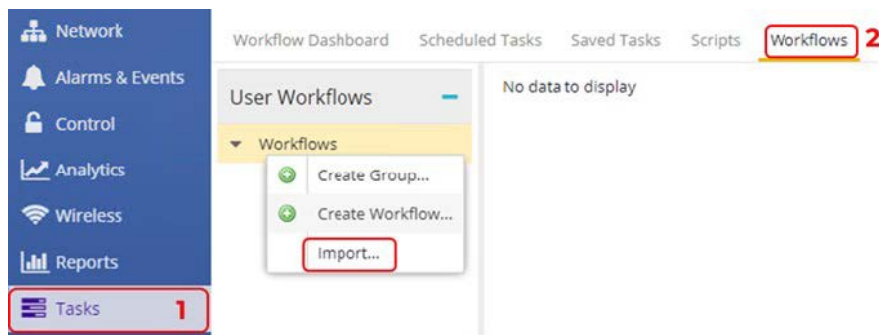
The workflow named *ZTP+ Change the persona to VOSS* is downloaded and then imported under ExtremeCloud IQ - Site Engine **Tasks > Workflows**.



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



Finally, the workflow named *Onboard VSP* is downloaded and then imported under ExtremeCloud IQ - Site Engine **Tasks > Workflows**.



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

Import Workflow ✕

Import a new workflow.

Select File...

Overwrite existing workflow

Remo...	File Name ↑	Override Workflow Name (optional)	Size	Status	Information
⊖	Onboard VSP-8.5.4.23v55.xwf		31 KB		

Import Close



VSP Core Preparation for Automated VSP Edge

Site Selection

When deploying VSP edge across multiple buildings, the goal is to have the switches automatically added to the correct ExtremeCloud IQ - Site Engine Site without any operator action.

To achieve this, it is sufficient to position the VSP core switches into the correct ExtremeCloud IQ - Site Engine Site and then let ZTP+ auto allocate VSP edge switches based on their LLDP neighbors to the core/distribution VSPs. How to configure ZTP+ to achieve this is covered in the ZTP+ configuration topic.

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

Status	Name	Site	IP Address	Poll Status	Poll Details	Device Type	Family	Firmware
●	Fabric	/World	10.9.203.7	Available: 1...	Up: 4 Dow...	FABRICMGR	Fabric Man...	21.9.10.4
●	NAC	/World	10.9.203.6	Available: 1...	Up: 1 Dow...	Virtual Access Cont...	Extreme C...	21.9.10.4
●	VSP-core1	/World	10.9.193.131	Available: 1...	Up: 1 Dow...	VSP-4450GSX-PWR+	VSP Series	8.4.0.0
●	VSP-core2	/World	10.9.193.132	Available: 1...	Up: 1 Dow...	VSP-4450GSX-PWR+	VSP Series	8.4.0.0

Assign both switches to the Building1 site.

Configure Device

Device ID	System Name	Device Nickname	Device Type	Poll Type	Site Precedence	Site
10.9.193.132	VSP-core2	VSP-core2	VSP-4450GSX-PW...	SNMP		/World
10.9.193.131	VSP-core1	VSP-core1	VSP-4450GSX-PW...	SNMP		/World

Device Annotation VRF Definitions VLAN Definitions CLIP Addresses Topology Services LAGs Ports

System Name: <Different> Default Site: /World

Contact: http://www.extremenetv Poll Group: /World

Location: Poll Type: /World/Building1

Administration Profile: Fabric Edge SNMP Timeout: 5

Replacement Serial Number: SNMP Retries: 3

Remove from Service: Topology Layer: L2 Access

Use Default WebView Collection Mode: Historical

URL: WebView URL: http://%IP Collection Interval (minutes): 15

Reload Device Sync from Site Enforce Preview... Save Cancel

Select **Yes** in the confirmation popup.

Import Site Configuration

Do you want to import the site configuration?

WARNING: The existing VLAN Definition, Ports, and ZTP+ Device Settings configuration will be overwritten.

Yes No

Then select **Save** to commit.

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

Dashboard Devices Discovered Firmware Archives Configuration Templates Reports

Sites

World

Building1

Building2

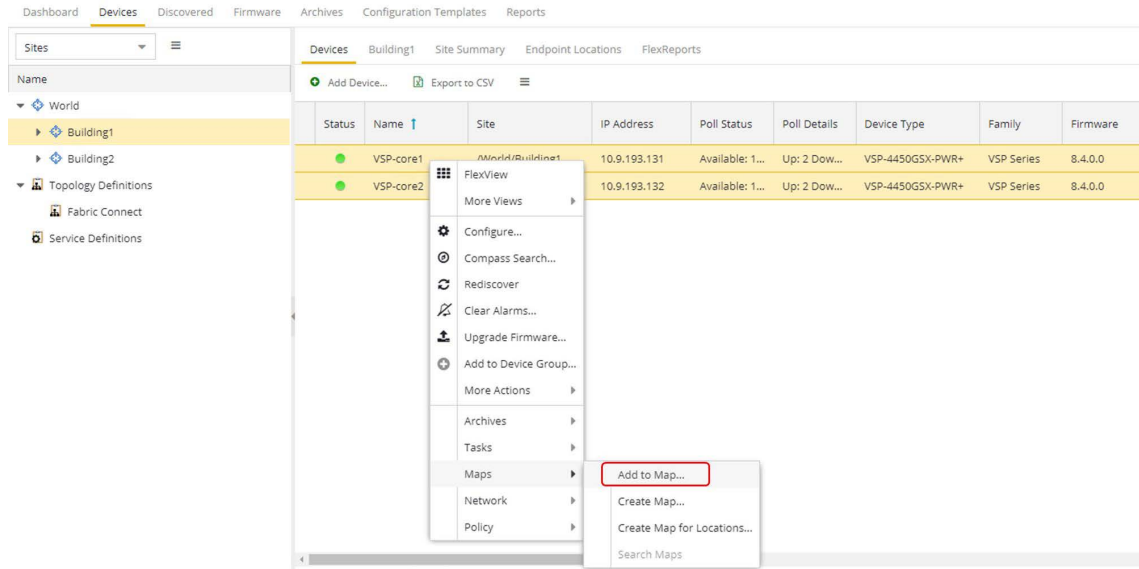
Topology Definitions

Devices Building1 Site Summary Endpoint Locations FlexReports

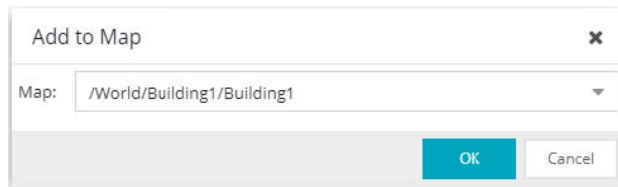
Add Device... Export to CSV

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

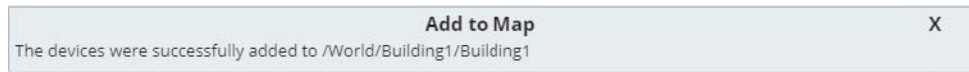
Next, right-click on both VSP cores again and select **Maps > Add to Map...**



Then enter the Building site that was chosen. Select **OK**.



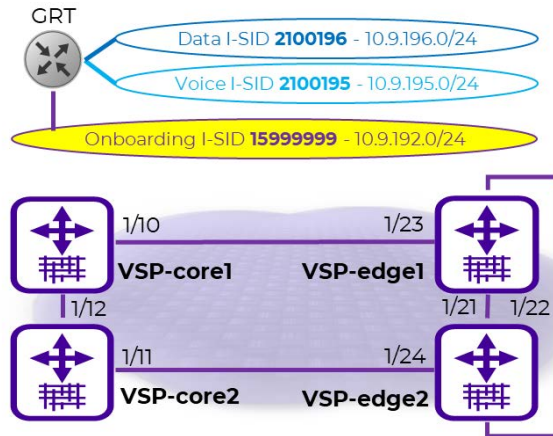
The VSP cores have now been added to the map.



Applying DVR Controller, VLAN and IP Configuration

The VSP cores need to route IP traffic across a number of VLANs/L2 VSNs. These VLANs do not exist on the VSP cores and must be created.

Because the VSP edge is onboarded as DVR Leaf nodes, the VSP cores also need to be configured as DVR Controllers and a DVR-GW IP is configured on the voice and data VLANs.



The above configuration is accomplished via SSH CLI.

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

VSP-core1	VSP-core2
<pre>enable config term dvr controller 1 vlan create 195 name "Voice" type port-mstprstp 0 vlan i-sid 195 2100195 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 10.9.255.130 mode bootp_dhcp ip dhcp-relay fwd-path 10.9.255.131 ip dhcp-relay fwd-path 10.9.255.131 enable ip dhcp-relay fwd-path 10.9.255.131 mode bootp_dhcp exit vlan create 196 name "Data" type port-mstprstp 0 vlan i-sid 196 2100196 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 10.9.255.130 mode bootp_dhcp ip dhcp-relay fwd-path 10.9.255.131 ip dhcp-relay fwd-path 10.9.255.131 enable ip dhcp-relay fwd-path 10.9.255.131 mode bootp_dhcp exit end</pre>	<pre>enable config term dvr controller 1 vlan create 195 name "Voice" type port-mstprstp 0 vlan i-sid 195 2100195 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 10.9.255.130 mode bootp_dhcp ip dhcp-relay fwd-path 10.9.255.131 ip dhcp-relay fwd-path 10.9.255.131 enable ip dhcp-relay fwd-path 10.9.255.131 mode bootp_dhcp exit vlan create 196 name "Data" type port-mstprstp 0 vlan i-sid 196 2100196 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 10.9.255.130 mode bootp_dhcp ip dhcp-relay fwd-path 10.9.255.131 ip dhcp-relay fwd-path 10.9.255.131 enable ip dhcp-relay fwd-path 10.9.255.131 mode bootp_dhcp exit end</pre>

Open ExtremeCloud IQ - Site Engine Device View against both core VSPs and verify that the VLANs and L2 VSNs have been configured.

The screenshot displays two configuration views for a VSP device (VSP-core1) with IP address 10.9.193.131. The top view shows the VLAN configuration table, and the bottom view shows the I-SID L2VSN configuration table.

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
10.9.193.131	1	VSP-core1	1	Default	active	active	1	0	byPort	0	0
10.9.193.131	195	VSP-core1	195	Voice	active	active	1	2100195	byPort	0	0
10.9.193.131	196	VSP-core1	196	Data	active	active	1	2100196	byPort	0	0
10.9.193.131	4051	VSP-core1	4051	B-VLAN-1	active	active	63	0	spbm-bvlan	0	0
10.9.193.131	4052	VSP-core1	4052	B-VLAN-2	active	active	63	0	spbm-bvlan	0	0

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
10.9.193.131	2100195	Auto-sense V...	elan	active	active	32000	false	config
10.9.193.131	2100196	ISID-2100196	l2vsn	active	active	32000	false	config
10.9.193.131	15999999	Onboarding ...	elan	active	active	32000	false	config
10.9.193.131	16777001	FAN-ISID	elan	active	active	32000	false	config

Applying Seed Configuration for Zero Touch Fabric

Before the VSP edge can automatically join the fabric further down, the VSP core first needs to be configured in these areas:

1. **Nickname server:** This is so that unique SPB nicknames can be assigned to VSP edge switches as they join the fabric. An SBP node needs a nickname to create multicast I-SID trees, which in turn are needed for transmitting BUM (Broadcast/Unknownunicast/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) must be set up as nickname servers. It is sufficient to have two nickname servers per fabric (and in VOSS 8.4, with multi-area support, a pair of nickname servers is required for each ISIS area). Both nickname servers can be set up to assign nicknames in the same prefix range or in 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 must already be 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 handle DHCP requests, from the universal-hardware edge and from other onboarding devices. Two approaches are possible:
 - a. The VSP cores are configured simply to bridge the onboarding I-SID onto an existing segment where DHCP is available.

Redundantly bridging a segment out of two VSP cores requires that those VSPs are configured as a Virtual-IST cluster and also require the use of SMLT links. That approach is not covered here.
 - b. The onboarding I-SID is created into a new dedicated IP subnet for which both VSP cores act as default gateways and DHCP-relay agent. This is the approach used here, as it is a better design approach.

If the VSP cores were originally built from VOSS 8.2 (or later) default values, the default onboarding private-VLAN 4048 is already present and needs to be deleted and re-created as a regular port-based VLAN (because VOSS currently does not support IP configuration on PVLANS [this will become possible in VOSS8.5]). In this case, the VSP cores do not have private-VLAN 4048, so a regular port-based VLAN needs to be created with a DHCP relay configuration and then assigned to the onboarding I-SID.

3. If the VSP core was not originally built from VOSS 8.3 default values (for example, it was upgraded from a pre-VOSS 8.3 release), it also needs to have auto-sense enabled on the interfaces connecting to the VSP edge.

The VSP core configurations were built from pre-VOSS 8.2 default values. As a result, they have no onboarding I-SID defined, all unused ports are disabled, no ports are auto-sense enabled, and there is no nickname server. Thus, the three configuration areas enumerated above need to be applied to these VSP Cores.

Apply the following configuration to both core VSPs:

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 port-mstprstp 0 vlan i-sid 4048 15999999 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 port-mstprstp 0 vlan i-sid 4048 15999999 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>



Preparing ExtremeCloud IQ - Site Engine for Fully Automated Edge Deployment

Configuration of ZTP+

Confirm the ZTP+ configuration for these sites is correct before onboarding the universalhardware edge into either Building1 or Building2. Go to the selected site and select 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**

The screenshot shows the configuration page for 'Building1' in the 'ZTP+ Device Defaults' tab. The 'Basic Management' section includes the following fields:

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

Initiate the onboarding of the VSP edge switches by using the same DHCP IP address that they initially acquired on the onboarding I-SID. To do this, set **Use Discovered** to **IP and Management Interface**. After the switches are onboarded, there are steps on how to move them to their final Mgmt CLIPs.

Under **Configuration/Upgrade**, **Configuration Updates** can be left to **Always** (this setting is not applicable in SNMP Poll Type).

The value for **Firmware Upgrades** depends on how the universal-hardware OS conversion is performed (next topic). If you are using the ExtremeCloud IQ - Site

Engine workflow *Change persona to VOSS*, set **Firmware Upgrades** to **None** because the workflow is configured with the desired VOSS software version from the start. On the other hand, if you are using ExtremeCloud IQ for the OS conversion, **Firmware Upgrades** can be left enabled if the desired VOSS image to use is not the same version of the VOSS image that ExtremeCloud IQ will use for the OS conversion (currently 8.4.0.0).

Configuration/Upgrade

Configuration Updates:	Always	Firmware Upgrades:	Never
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, clear the **MVRP** check box because ZTP+ attempts to apply the default port templates during switch onboarding. (The templates can be inspected on the Port Template tab.)

Note that SSH is automatically enabled on the VSP – not because of the setting below but because the IQAgent running on the switch always attempts to activate it.

Device Protocols

Telnet:	<input checked="" type="checkbox"/> Enabled	HTTP:	<input checked="" type="checkbox"/> Enabled	LACP:	<input type="checkbox"/> Enabled	MSTP:	<input checked="" type="checkbox"/> Enabled
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	MVRP:	<input type="checkbox"/> Enabled	VXLAN:	<input type="checkbox"/> Enabled

Select **Save** to commit changes to the site.

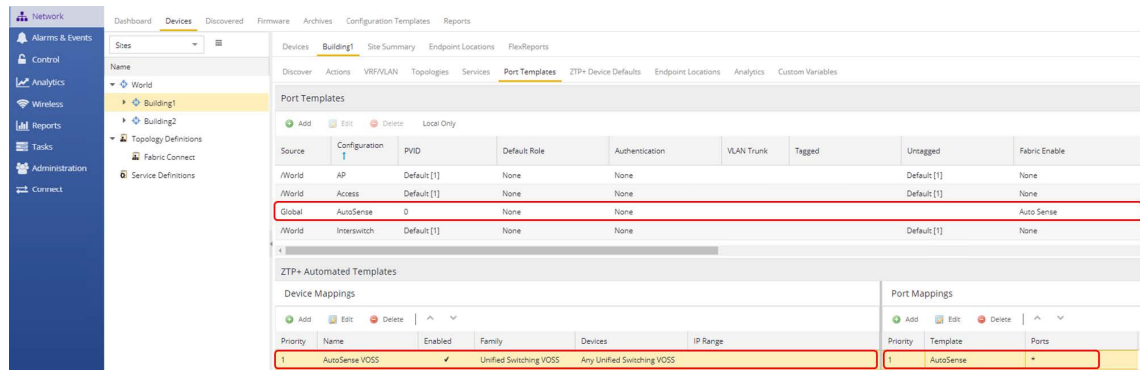
Source	Configuration	PVID	Default Role	Span Guard	Loop Protect	MVRP	SLPP	SLPP Guard	SLPP Guard Timer	PoE Enable	PoE Priority
/World	AP	Default [1]	None		✓				60	✓	LOW
/World	Access	Default [1]	None	✓					60	✓	LOW
Global	AutoSense	0	None						60	✓	LOW
/World	Interswitch	Default [1]	None		✓	✓			60	✓	LOW
/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

The default AP, Access, Interswitch, and Phone port templates are automatically applied by ZTP+ when onboarding a new switch. The logic is that the AP and Phone port templates are applied on ports where an AP or Phone was LLDP discovered. Likewise, the Interswitch port template is applied on ports where a Bridge/Switch neighbor was LLDP discovered, and the Access port template is applied to all other ports.

Some of the port-based features enabled by the default port templates can be detrimental to the successful deployment of universal hardware VSP edge. Two such features are Span Guard and MVRP.

MVRP has effect only when the universal hardware is onboarded in EXOS mode. In some topologies, it can cause a MAC learning issue because the EXOS switches generate MVRP PDUs with the switch’s MAC out of Spanning Tree Blocked ports, which cause the VSP cores to learn those MACs on the wrong ports, causing intermittent connectivity to the EXOS DHCP IP address. Disabling the MVRP Protocol ensures that MVRP does not get activated by any port templates.

Span Guard is also a problem because it results in BPDU-Guard being enabled on VOSS autosense ports when the universal hardware is onboarded in VOSS mode. If those ports are then used to interconnect VSPs together, BPDU-Guard conflicts with some auto-sense states which trigger self-generated BPDUs to prevent loops and also result in auto-sense ports going offline. To avoid these issues, ExtremeCloud IQ - Site Engine 21.9 introduces a new Global AutoSense port template which is automatically applied to VOSS universal hardware devices via a ZTP+ Automated Templates entry:



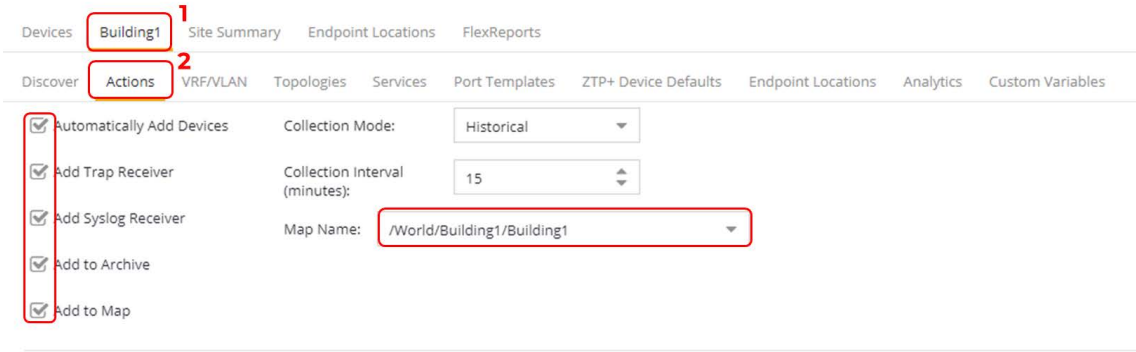
The ZTP+ Automated Templates entries allow for overriding the automatic application of the default port templates described above.

Note that the ZTP+ Automated Templates entry exist only on new sites created in ExtremeCloud IQ - Site Engine. If an older version of ExtremeCloud IQ - Site Engine or XMC is upgraded to ExtremeCloud IQ - Site Engine 21.9 or later, then that entry does not exist and needs to be created (or the Site deleted and re-created).

Also note that the default entry only covers VOSS universal hardware switches. If you onboard a VSP4900 or other VSP switch model, it is necessary to create a similar entry with Family set to **VSP Series**.

Now move to the **Actions** tab, and verify that all of these actions are set:

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

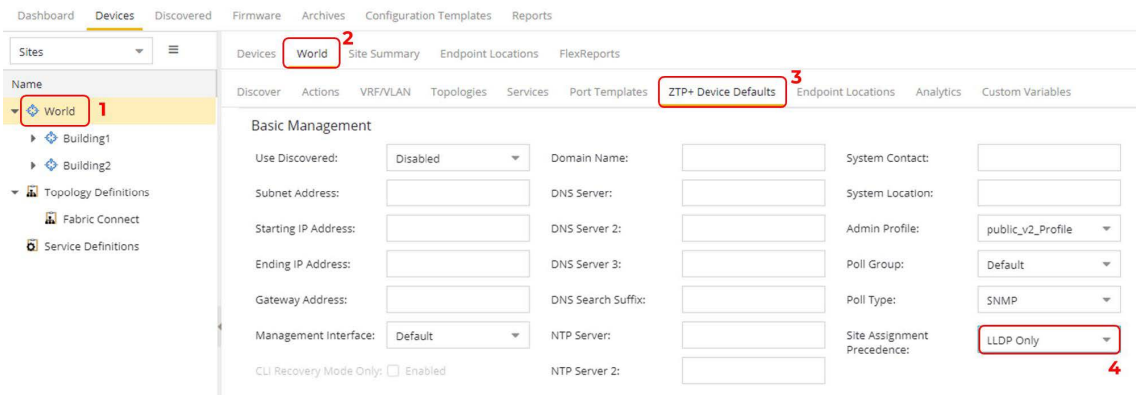


Now configure ExtremeCloud IQ - Site Engine so that it can automatically onboard the universal-hardware edge to the correct site Building1/2 and thus perform all of that site's ZTP+ configuration as well as the Site Actions setup mentioned above.

The VSP cores have been manually added to the Building1 ExtremeCloud IQ - Site Engine site. For the universal-hardware edge this is not a manual process but is automated by ExtremeCloud IQ - Site Engine.

To do this, access ExtremeCloud IQ - Site Engine's global ZTP+ configuration located under the root world site, and select the **ZTP+ Device Defaults** tab.

Locate the **Site Assignment Precedence** dropdown and set its value to **LLDP Only**. Note that this dropdown is configurable only from the root site World.



Now, when ExtremeCloud IQ - Site Engine discovers the universal-hardware edge switches, it examines their LLDP neighbor tables, and when it finds one of the VSP core switches, it assumes that this access switch must automatically be onboarded into the same ExtremeCloud IQ - Site Engine Site as the VSP cores.

Save the change.

Preparing Universal Hardware Edge OS Conversion

Because you are deploying a fabric with VSP edge, the universal-hardware switches need to be converted into running VOSS. Two approaches are possible here: using ExtremeCloud IQ or using an ExtremeCloud IQ - Site Engine workflow. In each case, the process involves three switch restarts.

Doing the OS conversion via ExtremeCloud IQ:

1. Initial boot as EXOS
 - a. Switch onboards ExtremeCloud IQ
 - b. In ExtremeCloud IQ, the switch serial number is associated with VOSS OS
 - c. ExtremeCloud IQ converts the switch to VOSS
 - d. Currently, ExtremeCloud IQ converts the switch to VOSS using 8.4.0.0
2. Switch boots as VOSS with 8.4.0.0
 - a. Switch onboards ExtremeCloud IQ - Site Engine via ZTP+
 - b. Switch is added to ExtremeCloud IQ - Site Engine Site, but in read-only state

Manual action required:

- On ExtremeCloud IQ: delete the device from ExtremeCloud IQ
 - On ExtremeCloud IQ - Site Engine: re-add the device to ExtremeCloud IQ via ExtremeCloud IQ - Site Engine
- c. *Onboard VSP* workflow is triggered
 - d. ExtremeCloud IQ - Site Engine workflow sets the DVR Leaf configuration and reboots the switch a final time
3. Switch boots as DVR Leaf with final configuration



Caution

Currently, with ExtremeCloud IQ - Site Engine, the above steps 2c and 2d do not happen automatically if the switch is already added to ExtremeCloud IQ, because ExtremeCloud IQ - Site Engine is designed not to manage or configure a device already added to ExtremeCloud IQ. Manual action is required to first delete the switch from ExtremeCloud IQ and then force ExtremeCloud IQ - Site Engine to re-add the same switch to ExtremeCloud IQ (details follow). Then, the above steps 2c and 2d resume automatically. This manual action is somewhat impractical and is no longer required after a `monitoronly` profile is added to ExtremeCloud IQ in a future release.

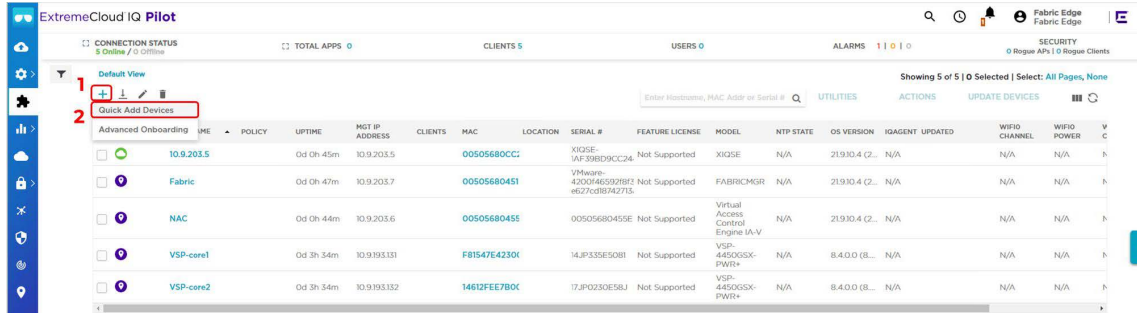
Doing the OS conversion via ExtremeCloud IQ - Site Engine workflow:

1. Initial boot as EXOS
 - a. Switch onboards ExtremeCloud IQ - Site Engine via ZTP+
 - b. Switch is added to ExtremeCloud IQ - Site Engine Site and the “Convert Persona to VOSS” workflow is executed
 - c. The VOSS image configured on the workflow (8.3 or later) is downloaded to the switch as part of OS conversion to VOSS.
2. Switch boots as VOSS
 - a. Switch re-onboards ExtremeCloud IQ - Site Engine via ZTP+
 - b. Switch is added to ExtremeCloud IQ - Site Engine site and “Onboard VSP” workflow is triggered
 - c. ExtremeCloud IQ - Site Engine workflow sets the DVR Leaf configuration and reboots the switch a final time
3. Switch boots as DVR Leaf with final configuration.

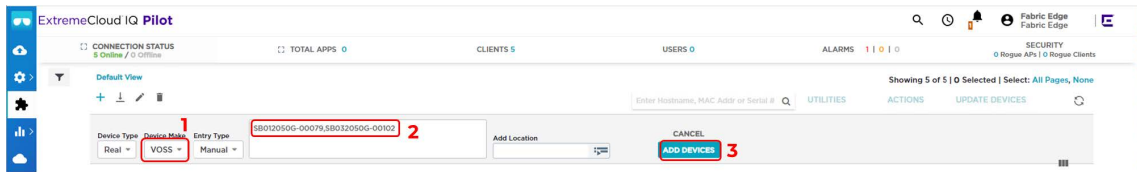
To proceed, decide which approach to use by following the relevant sections below.

Preparing via ExtremeCloud IQ

Log in to ExtremeCloud IQ and add a new switch using the serial number of the relevant universal-hardware switch. **Under Manage, Devices**, select **+** (add), then select **Quick Add Devices**.



In the **Device Add** banner that is revealed, set the **Device Make** to **VOSS**, paste the universalhardware edge serial number into the serial number text box, and select the appropriate location.



Note

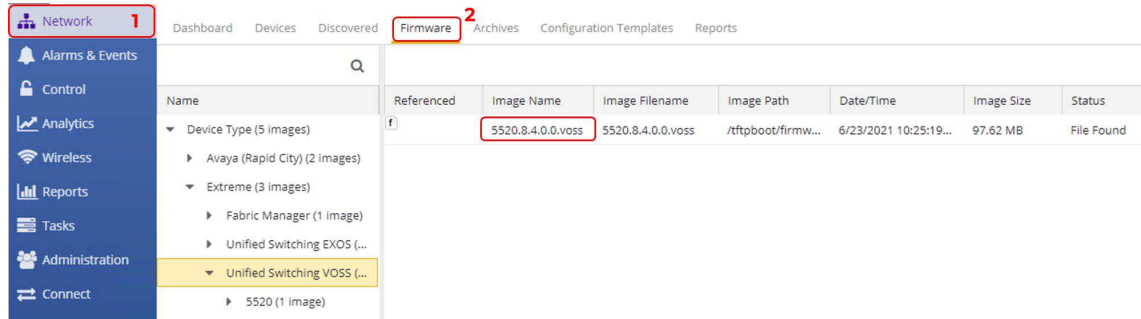
The desired OS for the universal hardware edge is specified to be VOSS. When the universal hardware onboards to ExtremeCloud IQ, if it is found to be in EXOS mode (which it is out of the box) then ExtremeCloud IQ immediately converts it to VOSS.

Preparing via ExtremeCloud IQ - Site Engine Workflow

To use ExtremeCloud IQ - Site Engine to convert a universal-hardware switch from EXOS to VOSS, the **Change Persona to VOSS** workflow will be used. This workflow is available on GitHub.

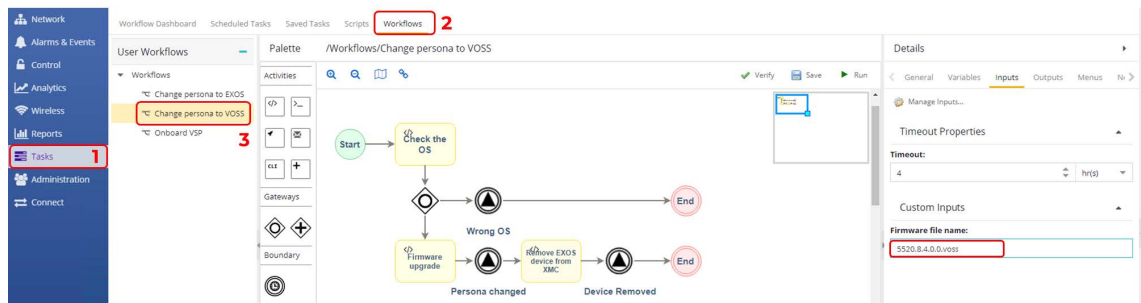
This workflow has already been imported into ExtremeCloud IQ - Site Engine, but it needs to be configured to use the desired VOSS image for the OS conversion.

Under ExtremeCloud IQ - Site Engine Network, go to the **Firmware** tab and locate the universalhardware VOSS image to use. Use VOSS 8.4.0.0 or later.

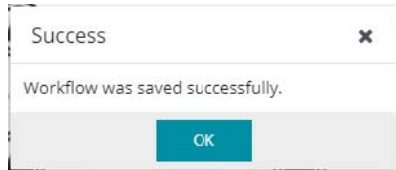


Copy and paste the desired image name. Note that the workflow uses FTP to transfer the image, and so the image must be located in `/tftpboot/firmware/images`.

Then navigate to the **ExtremeCloud IQ - Site Engine Tasks > Workflows** tab, select the **Change persona to VOSS** workflow, and under the workflow details, view the **Inputs** tab.



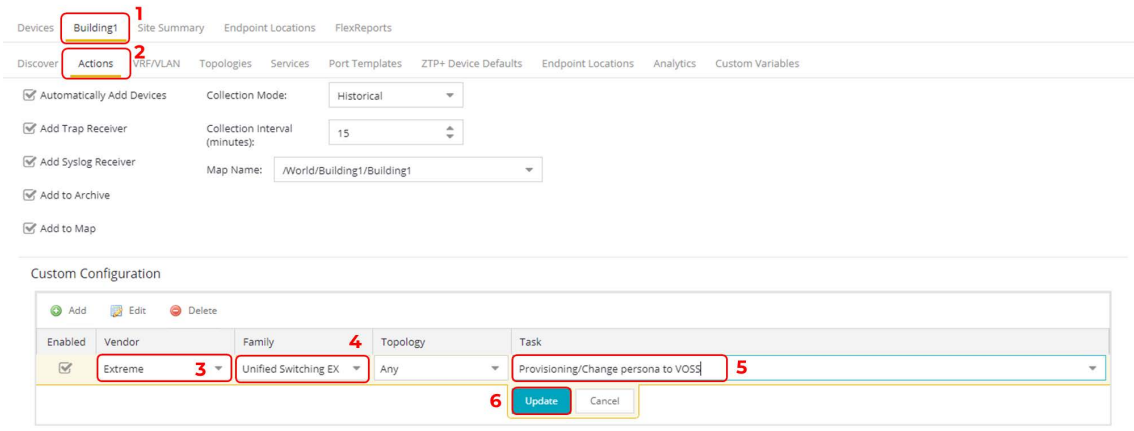
In the **Firmware file name** field, paste the 5520 VOSS image name to use. Then select **Save** and **OK** the confirmation popup.



Now go to the selected Building1/2 Site, **Actions Tab**, and under **Custom Configuration** add an entry pointing to the workflow:

- Vendor: **Extreme**
- Family: **Unified Switching EXOS**
- Topology: **Any**
- Task: **Provisioning/Change persona to VOSS**

Select **Update** and then select **Save**.



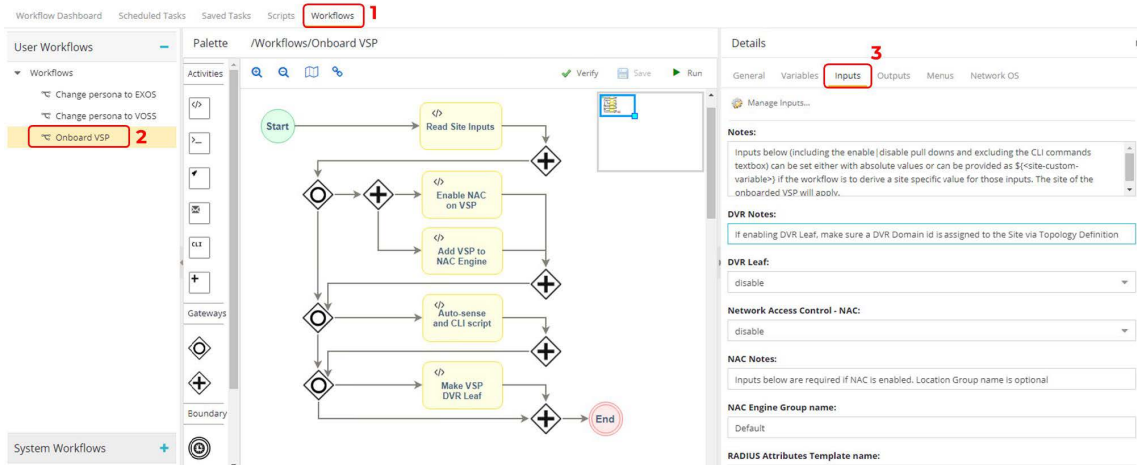
The onboarding section describes how this workflow kicks in after the universal-hardware switch initially booting as EXOS gets added to the site in the following sections.

Configuration of ExtremeCloud IQ - Site Engine workflow for VSP onboarding

The following configurations need to be performed on ExtremeCloud IQ - Site Engine in order to fully automate the onboarding of the VSP edge switches and deploy a set of network infrastructure and service parameter as a starter configuration:

1. Configure any of the VSP auto-sense parameters, such as:
 - a. Voice I-SID
 - b. Data I-SID
 - c. ISIS Hello authentication
 - d. FA Message authentication
2. Convert the VSP into a DVR Leaf

With the current release 21.4.11.3, ExtremeCloud IQ - Site Engine cannot natively perform the above, so to fully automate the VSP edge onboarding process the ExtremeCloud IQ - Site Engine Workflow named *Onboard VSP* is used. This workflow is available on GitHub and needs to be configured for use. Go to ExtremeCloud IQ - Site Engine **Tasks** then the **Workflow** tab and select the **Onboard VSP** workflow. Under the workflow details, view the **Input** tab.



Provide the following inputs:

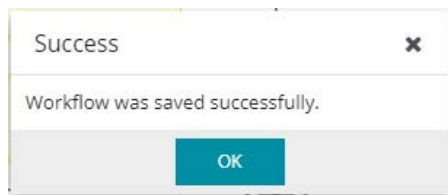
- DVR Leaf: enable
- Network Access Control (NAC): disable
- NAC Engine Group name:
- RADIUS Attributes Template name:
- RADIUS Shared Secret:
- On switch create RADIUS for:
- Location Group name:
- Auto-sense Voice I-SID: 2100195
- Auto-sense Voice VLAN-ID only if tagged: 195
- Auto-sense Data I-SID: 2100196
- Auto-sense Data platform VLAN-ID:
- Auto-sense ISIS Authentication key:
- Auto-sense FA Authentication key:
- Additional CLI commands:
 - clock time-zone US Eastern



Note

NAC is not used in this deployment guide, so the **NAC** dropdown is set to disable and all the workflow NAC related inputs can be ignored and left empty.

Save the modified workflow, and select **OK** the confirmation popup.



Now go to the ExtremeCloud IQ - Site Engine site where the core VSPs have been onboarded, under the **Actions** tab. Under **Custom Configuration**, add an additional entry with the following:

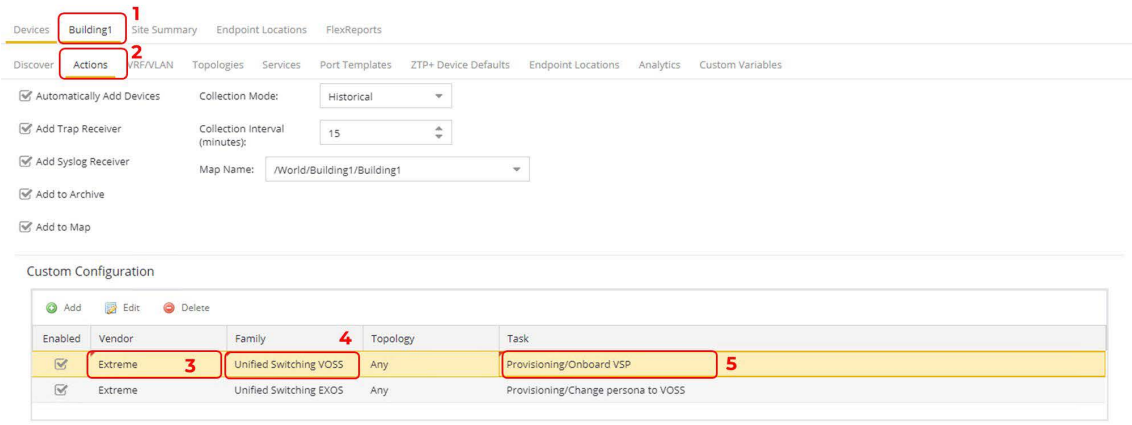
- Vendor: **Extreme**
- Family: **Unified Switching VOSS**
- Topology: **Any**
- Task: **Provisioning/Onboard VSP**

If the **Provisioning/Onboard VSP** workflow is not listed, cancel out and refresh the ExtremeCloud IQ - Site Engine page.



Note

If you are using a recent non-universal VSP hardware model (such as VSP 4900 or VSP 7400), an additional entry for: Extreme / VSP Series needs to be set. Older VSP models require creating an entry for: Avaya / VSP Series. A good way to determine a family type is by configuring the device in ExtremeCloud IQ - Site Engine and inspecting the **Vendor Profile** tab.



Select **Save** to commit changes.

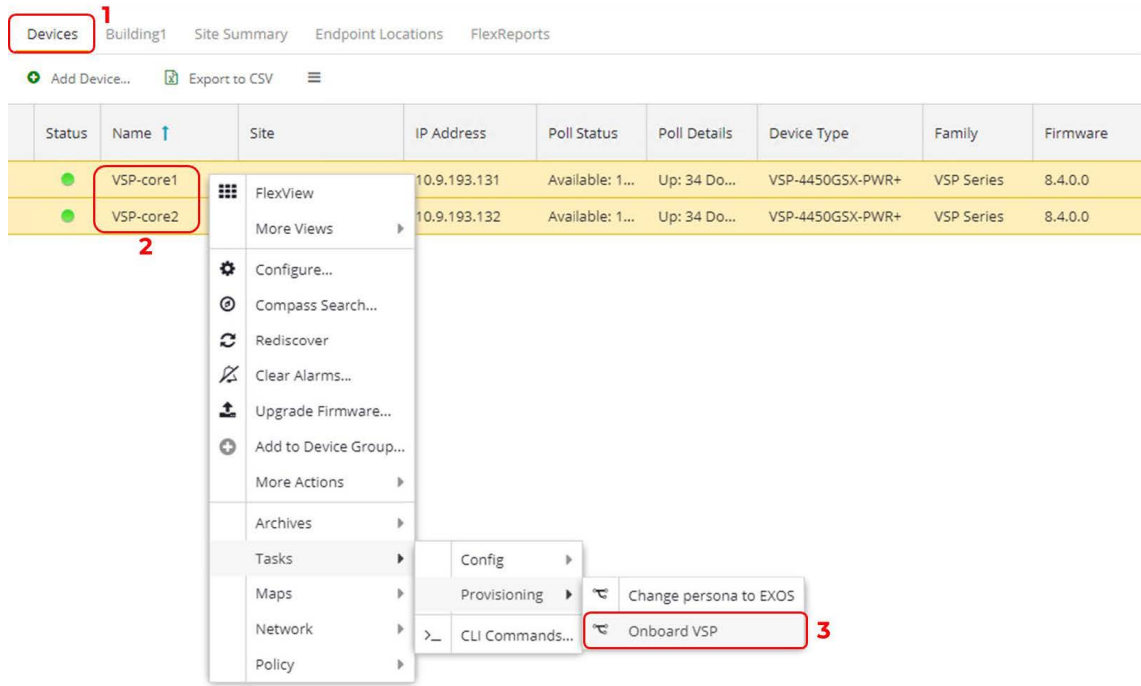
Manual Run of ExtremeCloud IQ - Site Engine Workflow on VSP Core Nodes

This step is not necessarily required, but it might be needed if any of the settings performed by the workflow on the VSP edge switches are also required on the VSP core nodes.

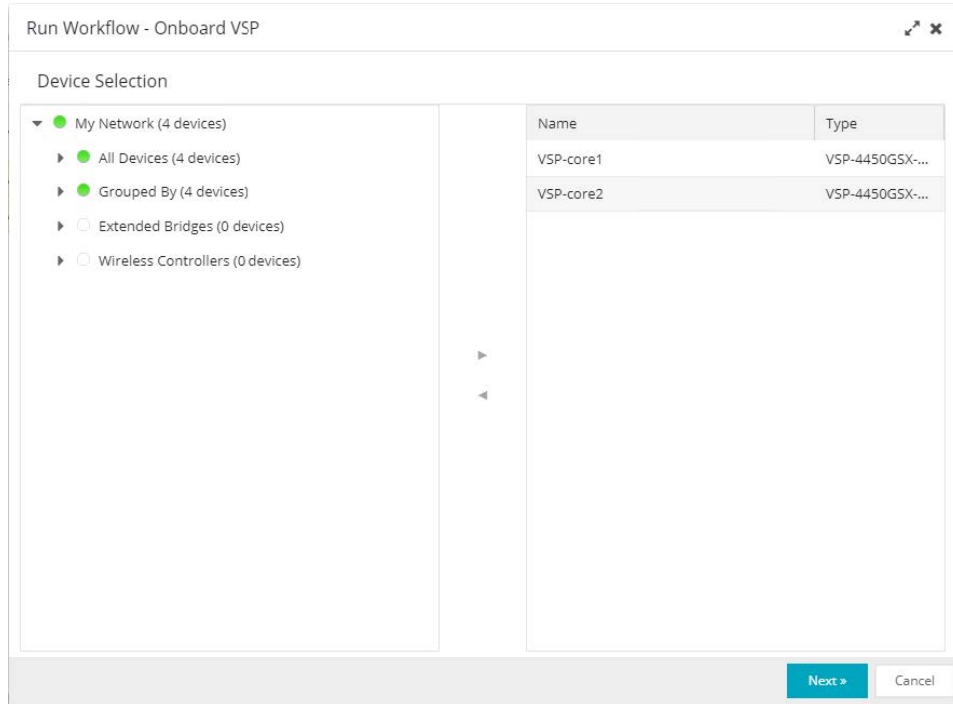
For example, are auto-sense Voice/Data I-SID settings required on them? That depends on whether phones and end-stations are going to be directly connected on the VSP core nodes

The VSP core nodes will never need to be made DVR Leaf nodes, but there might be a need to set the auto-sense ISIS Hello authentication key if ISIS authentication is required before new edge VSPs are allowed to perform Zero-Touch-Fabric. For example, in this use case, the autosense ISIS Authentication key is required, so the *Onboard VSP* workflow must be executed manually to configure the VSP Cores with this parameter. Here are the steps to do this.

Navigate to the ExtremeCloud IQ - Site Engine Site where the VSP cores were onboarded. Select both VSP cores and select **Tasks > Provisioning > Onboard VSP**.



Accept the switch selection of both VSP cores. Then select **Next**.

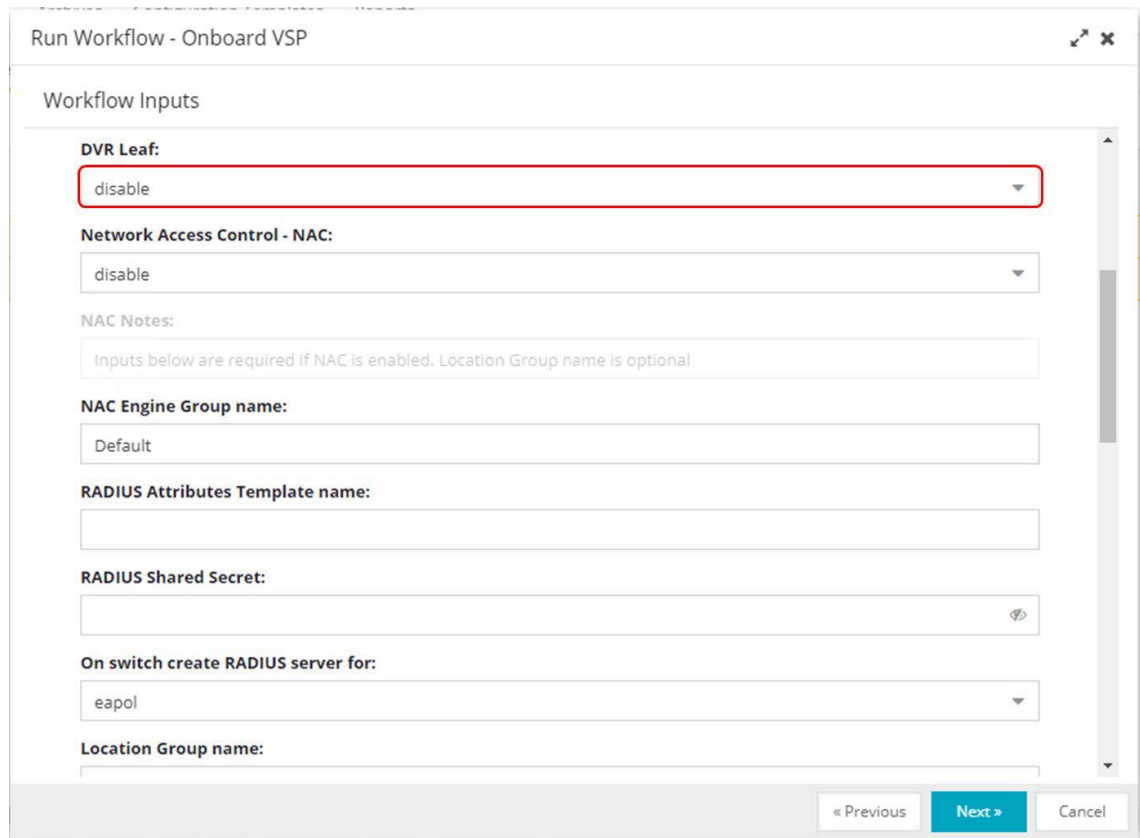


The same workflow inputs is shown, but this time any change made for those inputs do not persist beyond this run of the workflow. That is, if any changes are made here, those changes do not override the workflow input settings that have been set on the workflow.

This time set the inputs to:

- DVR Leaf: disable
- Network Access Control (NAC): disable
- NAC Engine Group name: <ignore>
- RADIUS Attributes Template name: <leave empty>
- RADIUS Shared Secret: <leave empty>
- On switch create RADIUS for: <ignore>
- Location Group name: <leave empty>
- Auto-sense Voice I-SID: 2100195
- Auto-sense Voice VLAN-ID only if tagged: 195
- Auto-sense Data I-SID: 2100196
- Auto-sense Data platform VLAN-ID: <leave empty, will be auto-allocated>
- Auto-sense ISIS Authentication key: <leave empty, or set a key for ISIS auth>
- Auto-sense FA Authentication key: <leave empty for this sandbox>
- Additional CLI commands:
 - clock time-zone US Eastern

Basically, this means you will only change the **DVR Leaf** dropdown to disable. The rest is left the same—though the **DVR Leaf** could have been left untouched as well, because the workflow does not try to convert the switch into a DVR leaf if it detects that the VSP is already configured as a DVR Controller.

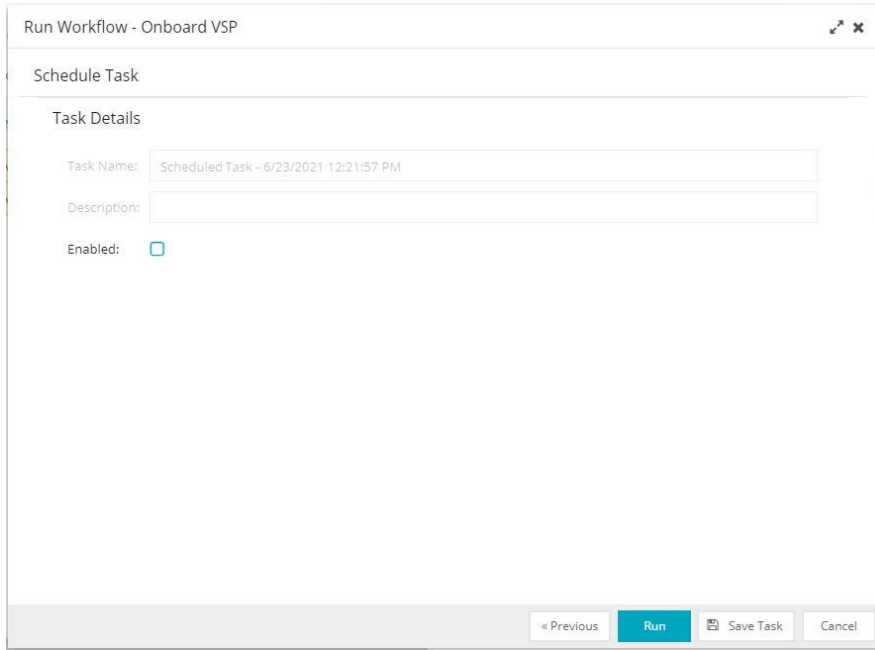


The screenshot shows a dialog box titled "Run Workflow - Onboard VSP". The "Workflow Inputs" section contains the following fields:

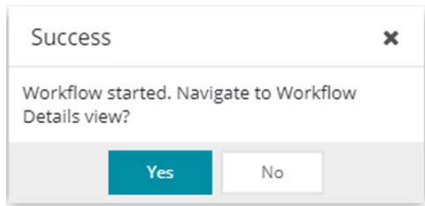
- DVR Leaf:** A dropdown menu with "disable" selected. This field is highlighted with a red border.
- Network Access Control - NAC:** A dropdown menu with "disable" selected.
- NAC Notes:** A text area containing the message: "Inputs below are required if NAC is enabled. Location Group name is optional".
- NAC Engine Group name:** A text input field with "Default" entered.
- RADIUS Attributes Template name:** An empty text input field.
- RADIUS Shared Secret:** An empty text input field with a visibility icon on the right.
- On switch create RADIUS server for:** A dropdown menu with "eapol" selected.
- Location Group name:** An empty text input field.

At the bottom right of the dialog, there are three buttons: "« Previous", "Next >" (highlighted in blue), and "Cancel".

Select **Next**.



Then select **Run** and **Yes** to view the workflow as it runs.

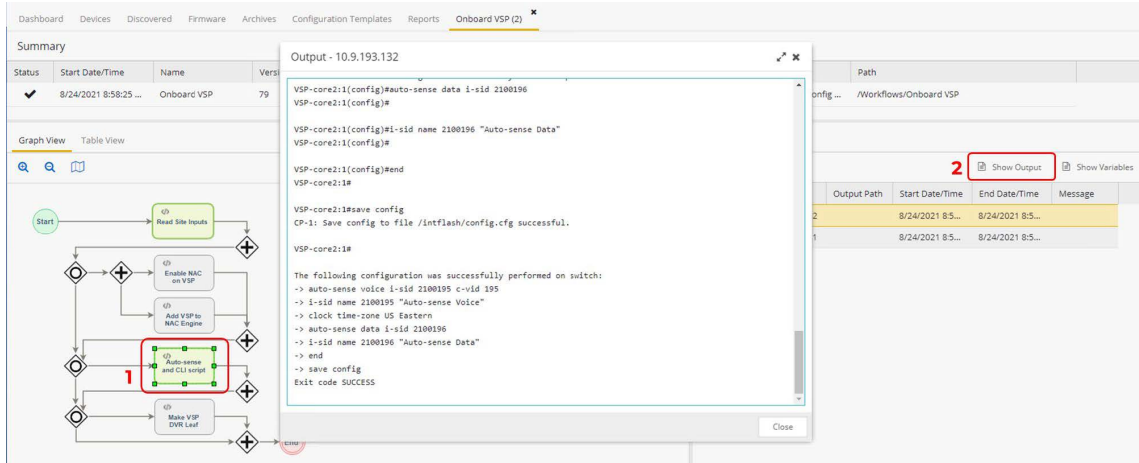


Wait for the workflow to complete. On completion, the status rotating cog changes to a checkmark if the workflow is completed successfully and to an exclamation mark otherwise.

Status	Start Date/Time	Name	Version	Source	# Devices	Started By	End Date/Time	Message	Path
✓	8/24/2021 8:58:25 ...	Onboard VSP	79	Workflow Designer ...	2	root	8/24/2021 8:58:42 ...	VSP 10.9.193.131 applied auto-sense config ...	/Workflows/Onboard VSP

When the workflow has completed, inspect the various workflow activity boxes by selecting them and then selecting **Show Output** to see the detail of the actions performed.

The auto-sense configuration was applied.



Notice that the activity blocks named *Enable NAC on VSP*, *Add VSP to NAC Engine*, and *Make VSP DVR Leaf* did not run.



Deployment of Edge Switches

Everything is now ready to accept the automated deployment of universal-hardware switches as VSP edge.

It will be sufficient for a technician to unbox the switches, rack the switches into their wiring closet rack, connect the fabric uplinks into the VSP core, connect any fabric side links into adjacent units in the same wiring closet rack, and power on the switches.

The rest the deployment is zero-touch, and there is no need for the technician to connect via the serial console of the switch. Nor is there any need to pre-stage the switches before deploying them in their final wiring closet rack.



Caution

The exception is non universal hardware that ships with a VOSS version earlier than 8.3.0.0. This is currently the case for the VSP 4900. Going forward, the VSP 4900 will ship with VOSS 8.3.1.0, but there is always a chance that the units were shipped from a distributor, in which case the shipped software might not be 8.3.1.0.



Onboarding of VSP Edge Switches

OS Conversion via ExtremeCloud IQ

If the universal-hardware serial numbers have been added to ExtremeCloud IQ in the previous section, then as soon as the switches come online as EXOS switches they are able to join ExtremeCloud IQ.

An activity bar in the **UPDATED** column displays the switch's firmware update status.

STATUS	HOST NAME	POLICY	UPTIME	MGT IP ADDRESS	CLIENTS	MAC	UPDATED	LOCATION	SERIAL #	FEATURE LICENSE	MODEL	NTP STATE	OS VERSION	IGAGENT	WFIO CHANNEL	WFIO POWER
<input type="checkbox"/>	10.9.203.5		0d 3h 33m	10.9.203.5		00505680CC			XIGSE-1AF39BD9CC24	Not Supported	XIGSE	N/A	21.9.10.4 (2...	N/A	N/A	N/A
<input type="checkbox"/>	Fabrie		0d 3h 33m	10.9.203.7		00505680451			Vmware-4200f4659278f2	Not Supported	FABRICHGR	N/A	21.9.10.4 (2...	N/A	N/A	N/A
<input type="checkbox"/>	HOSTNAME	Assign Policy	N/A	10.9.192.104	0	F06426A8E4c	IQ Engine Firmw... 80%	Assign Loc	S802050G-00079	Not Supported	EXOS-5520-12MW-36W	N/A	311.3	0.4.5	N/A	N/A
<input type="checkbox"/>	HOSTNAME	Assign Policy	N/A	10.9.192.103	3	F06426A8A0c	IQ Engine Firmw... 47%	Assign Loc	S8032050G-00082	Not Supported	EXOS-5520-24W	N/A	311.3	0.4.5	N/A	N/A
<input type="checkbox"/>	NAC		0d 3h 30m	10.9.203.6		00505680455E			00505680455E	Not Supported	Virtual Access Control Engine IA-V	N/A	21.9.10.4 (2...	N/A	N/A	N/A
<input type="checkbox"/>	VSP-core1		0d 6h 20m	10.9.193.131		F81547E4230f			14JP335E508f	Not Supported	VSP-4450GSX-PWR+	N/A	8.4.0.0 (8...	N/A	N/A	N/A
<input type="checkbox"/>	VSP-core2		0d 6h 20m	10.9.193.132		14612FEE780c			17JP0230E58J	Not Supported	VSP-4450GSX-PWR+	N/A	8.4.0.0 (8...	N/A	N/A	N/A

ExtremeCloud IQ currently does the OS conversion using VOSS 8.4.0.0.

The switch is rebooted and comes back as a VOSS switch.

The conversion to VOSS takes about 8 minutes and it takes VOSS a further 3 minutes to join the Fabric, obtain a nickname, obtain a DHCP address, and call into ExtremeCloud IQ - Site Engine for the first time as a VOSS switch.

OS Conversion via ExtremeCloud IQ - Site Engine Workflow

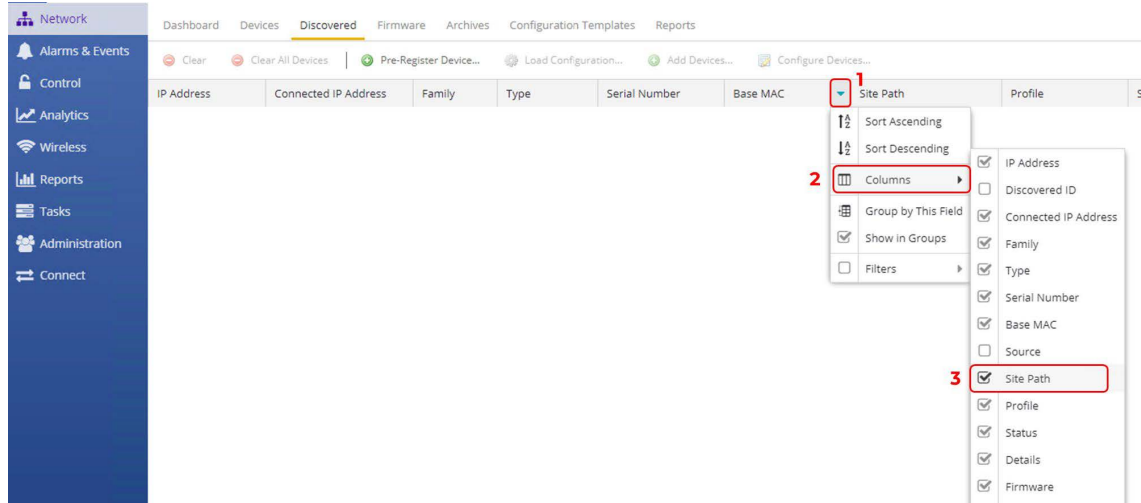
Another method is to automate the universal-hardware OS conversion via ExtremeCloud IQ - Site Engine. This process begins as soon as the universal-hardware edge onboards to ExtremeCloud IQ - Site Engine using ZTP+ as an EXOS switch.

Monitor the ExtremeCloud IQ - Site Engine **Discovered** tab.

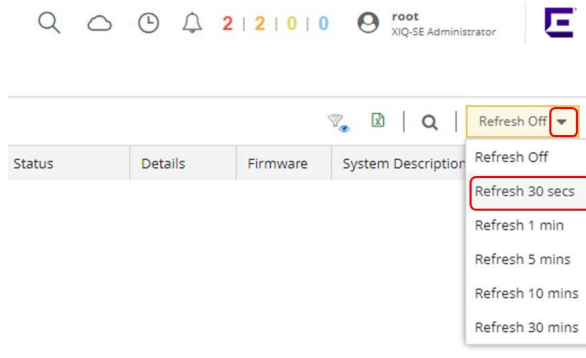
IP Address	Connected IP Address	Family	Type	Serial Number	Base MAC	Profile	Status	Details	Firmware	System Description
------------	----------------------	--------	------	---------------	----------	---------	--------	---------	----------	--------------------

While waiting, tune the **Discovery** tab to show the site path, which is useful information to see.

Select any of the columns, select the dropdown triangle, then select **Columns** and enable (check) **Site Path**.



Then, in the top right-hand corner, set auto refresh to 30 seconds



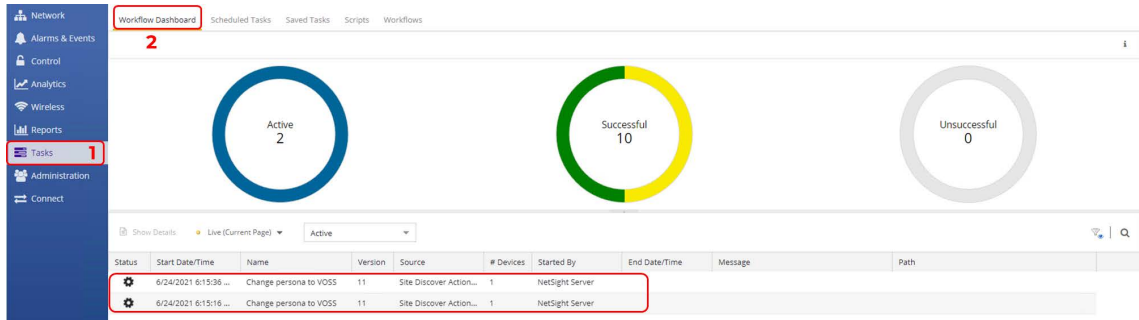
When the universal-hardware switches finally register with ExtremeCloud IQ - Site Engine, the switches appear in the **Discovered** tab.

IP Address	Connected IP Address	Family	Type	Serial Number	Base MAC	Site Path	Profile	Status	Details	Firmware	System Description
Discovered ID: SB012050G-00079											
N/A	10.9.192.104	Unified Swl...	5520-12MW-3...	SB012050G-00079	F0:64:26:A8:E4:00	/World	public_v2_Profile	ZTP+ Pending ...		31.1.1.3	ExtremeXOS (5520-12MW-38W-EXOS) v...
Discovered ID: SB032050G-00102											
N/A	10.9.192.103	Unified Swl...	5520-24W-EXOS	SB032050G-00102	F0:64:26:AA:80:00	/World	public_v2_Profile	ZTP+ Pending ...		31.1.1.3	ExtremeXOS (5520-24W-EXOS) version

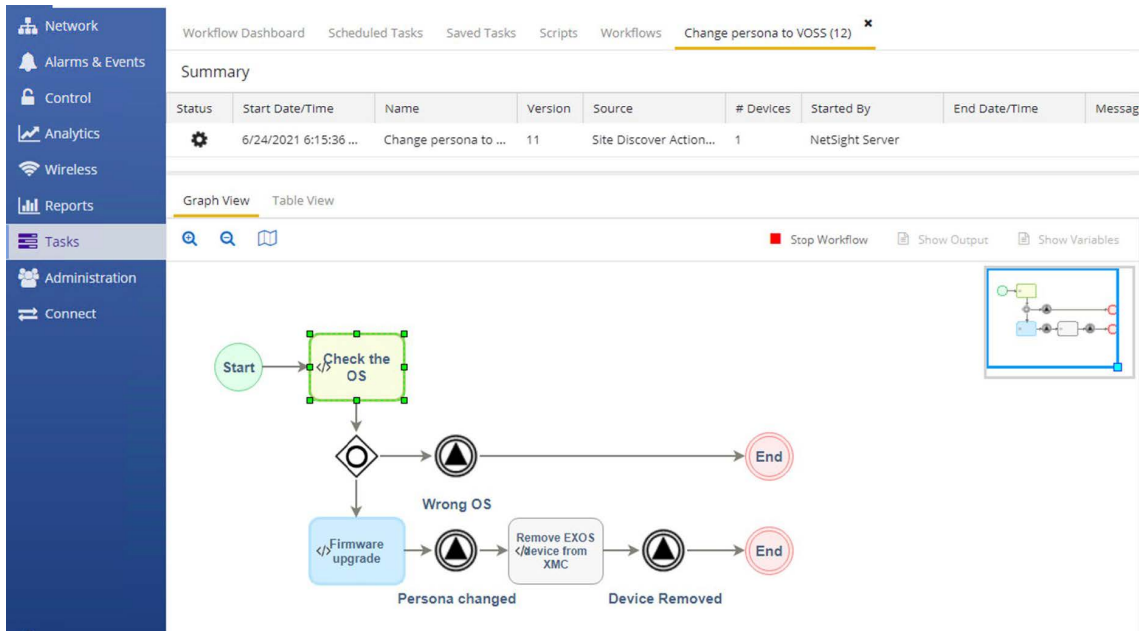
And it takes about 3 minutes before the ZTP+ onboarding stages the configuration and adds the EXOS switch into the ExtremeCloud IQ - Site Engine site.

IP Address	Connected IP Address	Family	Type	Serial Number	Base MAC	Site Path	Profile	Status	Details	Firmware	System Description
Discovered ID: SB032050G-00102											
10.9.192.103	10.9.192.103	Unified Swl...	5520-24W-EXOS	SB032050G-00102	F0:64:26:AA:80:00	/World/Building1	Fabric Edge	ZTP+ Staged	Configurati...	31.1.1.3	ExtremeXOS (5520-24W-EXOS) version

As soon as the switches are deleted from the **Discovered** tab, they are added and can be found on the onboarded site. At the same time, the site's actions are performed. Quickly go to ExtremeCloud IQ - Site Engine **Tasks > Workflow Dashboard**. There is a chance the workflows are still running (they run for a couple of minutes).



If a non-zero count is displayed in the Active chart, click on the chart to list the currently active workflows. Double-click on the workflow entry to reveal the workflow details as it is running.



Green activity boxes have run and have completed successfully; red activity boxes have run and failed; blue activity boxes are still running.

When the workflow has completed successfully, the EXOS universal-hardware switches reboot into VOSS and are deleted from ExtremeCloud IQ - Site Engine.

The conversion to VOSS takes about 8 minutes, and it takes VOSS a further 3 minutes to join the Fabric, obtain a Nickname, obtain a DHCP address, and call into ExtremeCloud IQ - Site Engine again as a VOSS switch.

VSP Edge Onboarding Steps

The order of events should be as follows. There are two possibilities.

If the Auto-sense ISIS Hello Authentication key was not specified on the VSP cores:

1. ISIS adjacency form with neighboring VOSS switches
2. Nickname is dynamically assigned by nickname servers (VSP core)
3. DHCP obtains IP address on onboarding I-SID 15999999
4. DHCP provides default gateway, DNS servers, domain name
5. Switch does a DNS lookup for *extremecontrol*.
6. DNS lookup must return ExtremeCloud IQ - Site Engine's IP address
7. Switch calls in to ExtremeCloud IQ - Site Engine, and now appears in the **Discovered** tab (provided it does not already exist in ExtremeCloud IQ - Site Engine's database)
8. If ExtremeCloud IQ - Site Engine can allocate the switch to a site, then the site's ZTP+ configuration is pushed. If not, the switch remains in the **Discovered** tab until an administrator manually configures or adds the switch to a site.
9. When the switch is allocated to an ExtremeCloud IQ - Site Engine site, the site's actions are performed; this is when the *Onboard VSP* workflow is executed
10. *Onboard VSP* applies final Auto-sense configuration as well as DVR-Leaf conversion

If the Auto-sense ISIS Hello Authentication key was specified on the VSP cores:

1. ISIS adjacency does not form with neighboring VSP core switches because there is no ISIS authentication key on the booting edge switches
2. But the auto-sense ports get untagged connectivity into the onboarding VLAN 4048 on the VSP cores
3. DHCP obtains IP address on untagged UNI management onboarding VLAN4048
4. DHCP provides default gateway, DNS servers, domain name
5. Switch does a DNS lookup for *extremecontrol*.
6. DNS lookup must return ExtremeCloud IQ - Site Engine's IP address
7. Switch calls in to ExtremeCloud IQ - Site Engine, and now appears in the **Discovered** tab (provided it does not already exist in ExtremeCloud IQ - Site Engine's database)
8. If ExtremeCloud IQ - Site Engine can allocate the switch to a site, then the site's ZTP+ configuration is pushed. If not, the switch remains in the **Discovered** tab until an administrator manually configures or adds the switch to a site.
9. When the switch is allocated to an ExtremeCloud IQ - Site Engine site, the site's Actions are performed; this is when the *Onboard VSP* workflow will be executed
10. *Onboard VSP* applies final Auto-sense configuration as well as DVR-Leaf conversion. Only now the onboarded VSP edge switch gets the Auto-sense ISIS Hello authentication key
11. ISIS adjacency can now form with neighboring VSP core switches
12. Nickname is dynamically assigned by nickname servers (VSP core)
13. There is a brief period where the onboarding switch is unreachable as its connectivity into the onboarding I-SID 15999999 transitions from a UNI connection to a fabric NNI connection

When the configuration is saved, the switch disappears from ExtremeCloud IQ - Site Engine **Discovered** tab. It is added to the final site and to the corresponding site map.

Status	Name ↑	Site	IP Address	Poll Status	Poll Details	Device Type	Family	Firmware
●	5520-12MW-36W-VOSS	/World/Building1	10.9.192.104	Available: 1...	Up: 192 Do...	5520-12MW-36W-V...	Unified Swi...	8.4.0.0
●	5520-24W-VOSS	/World/Building1	10.9.192.103	Available: 1...	Up: 2 Dow...	5520-24W-VOSS	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

Manual Steps Required if OS Conversion Was Done via ExtremeCloud IQ

If the OS conversion of the universal-hardware was performed by the ExtremeCloud IQ - Site Engine workflow, this section can be skipped.

If, on the other hand, ExtremeCloud IQ made the OS conversion, the universal hardware is added to ExtremeCloud IQ - Site Engine by ZTP+. But ExtremeCloud IQ - Site Engine detects that these devices are already present in ExtremeCloud IQ and does not attempt to manage the devices. The devices are in a read-only mode where they cannot be configured, and no ExtremeCloud IQ - Site Engine script or workflow can be executed against them. As a result, the *Onboard VSP* workflow does not execute.

This can be seen by inspecting the **ExtremeCloud IQ Onboarded** device column, which has a missing check mark.

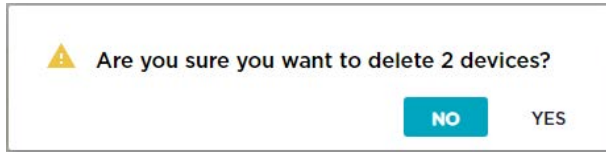
Status	Name ↑	Site	IP Address	Poll Status	Poll Details	Device Type	Family	Firmware	Reference	Connector	XIQ Onboarded
●	5520-12MW-36...	/World/Building1	10.9.192.101	Available: 1...	Up: 18 Do...	5520-12MW-36W-V...	Unified Swi...	8.4.0.0			
●	5520-24W-VOSS	/World/Building1	10.9.192.103	Available: 1...	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 ExtremeCloud IQ - Site Engine to fully manage these devices, two manual actions are required.

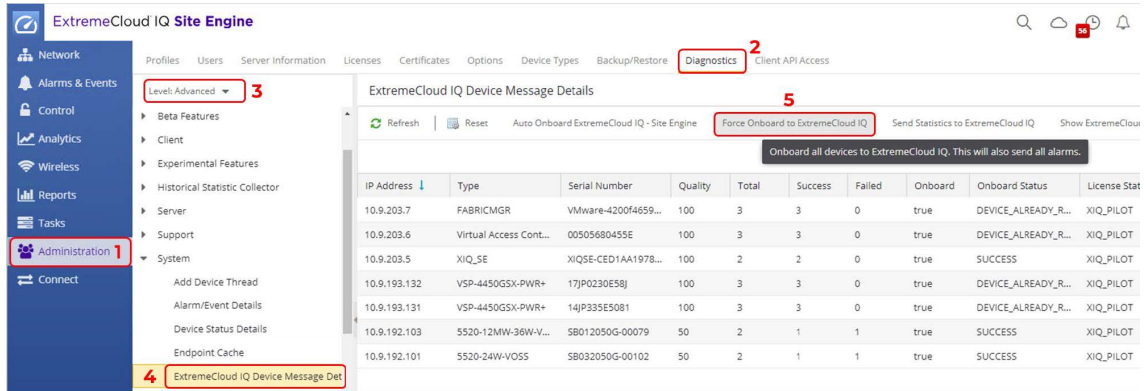
First, the devices must be deleted from ExtremeCloud IQ. Select the universal hardware switches in ExtremeCloud IQ (these should now be seen as VOSS devices), and select **Delete**.

STATUS	HOST NAME	POLICY	UPTIME	MGT IP ADDRESS	CLIENTS	MAC	UPDATED	LOCATION	SERIAL #	FEATURE LICENSE	MODEL	NTP STATE	OS VERSION	IGAGENT	WFO CHANNEL	WFO POWER
●	10.9.203.5		0d 4h 15m	10.9.203.5		00505680CC	2021-08-24 09:42:29		XIGSE-CEDFA11078324	Not Supported	XIGSE	N/A	219.10.50	N/A	N/A	N/A
●	5520-12MW-36W-VOSS	Assign Policy	0d 1h 30m	10.9.192.101	3	F06426A8E4C	2021-08-24 09:42:29		S8032050G-00079	None	VSP 5520-12MW-36W	N/A	8.4.0.0	0.4.13	N/A	N/A
●	5520-24W-VOSS	Assign Policy	0d 0h 39m	10.9.192.103	3	F06426A801	2021-08-24 10:33:10		S8032050G-00102	None	VSP 5520-24W	N/A	8.4.0.0	0.4.13	N/A	N/A

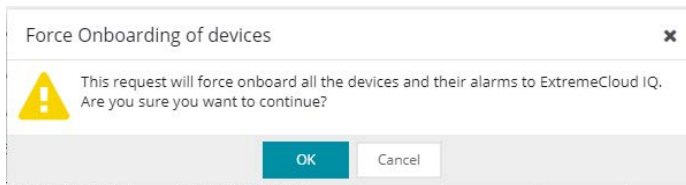
Confirm the deletion by selecting **Yes**.



Second, ExtremeCloud IQ - Site Engine needs to be instructed to re-synch its devices with ExtremeCloud IQ. Navigate ExtremeCloud IQ - Site Engine to **Administration** > **Diagnostics**, select level **Advanced** then select the **ExtremeCloud IQ Device Message Details** folder under the **System** main folder.



Select the **Force Onboard to ExtremeCloud IQ** button. Then select **OK** in the confirmation popup.



Allow a few seconds for ExtremeCloud IQ - Site Engine to re-submit all devices to ExtremeCloud IQ. Then inspect the devices. They should now have a check mark in the **XIQ Onboarded** column.

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			✓

Inspection of ExtremeCloud IQ also shows the same switches are re-added to ExtremeCloud IQ, but this time by ExtremeCloud IQ - Site Engine.

STATUS	HOST NAME	POLICY	UPTIME	MGT IP ADDRESS	CLIENTS	MAC	UPDATED	LOCATION	SERIAL #	FEATURE LICENSE	MODEL	NTP STATE	OS VERSION	IDAGENT	WF10 CHANNEL	WF10 POWER
✓	10.9.203.5		0d 4h 44m	10.9.203.5		00505680CC			XIGSE-CE01A1078324	Not Supported	XIGGE	N/A	21.9.10.50	N/A	N/A	N/A
✓	5520-12MW-36W-V05S		0d 1h 54m	10.9.192.101		F06426A8E4C			SB012050G-03029	Not Supported	VSP 5520-12MW-36W	N/A	8.4.0.0	N/A	N/A	N/A
✓	5520-24W-V05S		N/A	10.9.192.103		F06426A8B0X			SB032050G-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-6620274603028B2	Not Supported	FABRICMSR	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 L4-V	N/A	21.9.10.50	N/A	N/A	N/A
✓	VSP-core1		0d 5h 0m	10.9.193.131		F81547E4230C			14.P335E5081	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		14612FE780C			17.IP0230E58J	Not Supported	VSP-4450GSX-PWR+	N/A	8.4.0.0	N/A	N/A	N/A

A few moments later, the ExtremeCloud IQ - Site Engine site actions, which had been defined to start the *Onboard VSP* workflow execute automatically without any need for further manual intervention. Follow through into the next section.

Observing ExtremeCloud IQ - Site Engine Onboarding Workflow Completion

If you are quick, you can view the progress of the *Onboard VSP* workflow as it is being executed. Go to ExtremeCloud IQ - Site Engine Tasks and display the **Workflow Dashboard** tab. See if any workflows are actively running; select the **Active** pie chart, then double-click any *Onboard VSP* workflow seen running in the list below.

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

```

graph TD
    Start((Start)) --> Read[Read Site Inputs]
    Read --> Merge1{+}
    Merge1 --> Enable[Enable NAC on VSP]
    Merge1 --> Add[Add VSP to NAC Engine]
    Enable --> Merge2{+}
    Add --> Merge2
    Merge2 --> Auto[Auto-sense and CLI script]
    Auto --> Merge3{+}
    Merge3 --> Make[Make VSP DVR Leaf]
    Make --> End((End))
    
```

If there are no active workflows, the *Onboard VSP* workflow has probably completed. If this is the case, set the dropdown to **Historical** and find the most recently run workflows. There should be some for *Onboard VSP*, you can double-click on them to inspect their 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

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 into a DVR leaf, and to do so the switch is automatically rebooted one last time.

Now the VSP edge onboarding process is complete, and the configuration is saved and final. When the switches come back online, there is no more ZTP+ for them and no more site actions. They are fully deployed as VSP edge.

When the switches have come back online, SSH into them and verify that indeed they were made DVR leaf nodes, with the CLI command `show dvr`.

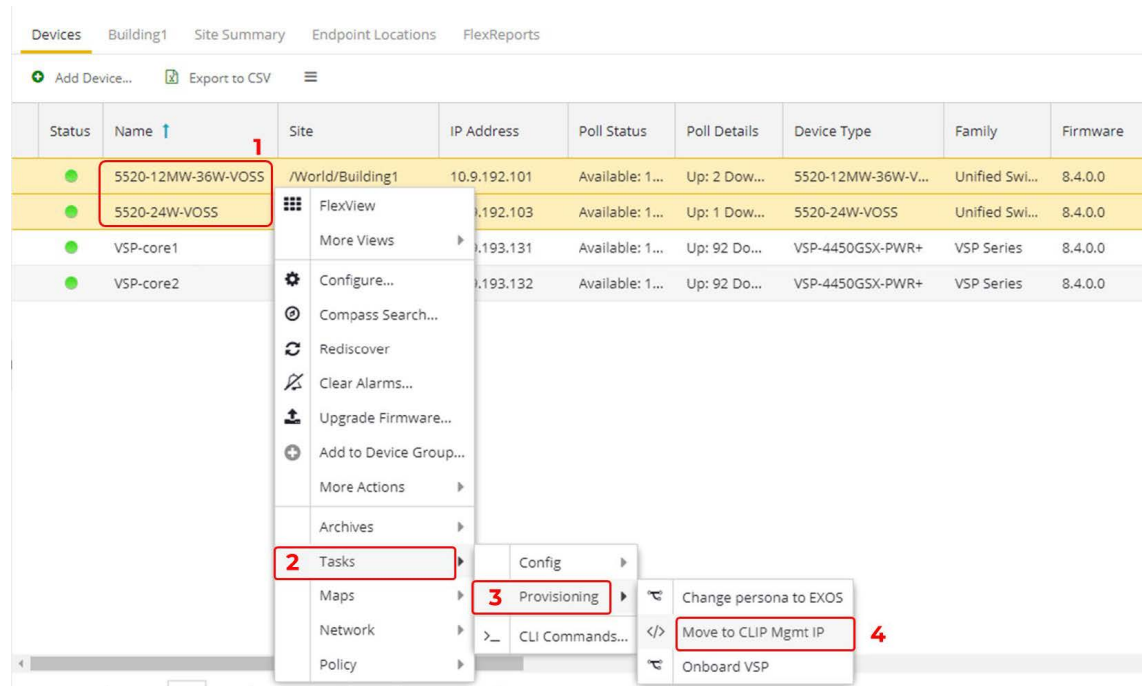
```
5520-24W-VOSS:1# show dvr
=====
DVR Summary Info
=====
Domain ID           : 1
Domain ISID         : 16678217
Role                 : Leaf
My SYS ID           : f0:64:26:aa:80:84
Operational State   : Up
GW MAC              : 00:00:5e:00:01:25
Inband Mgmt Clip IP :
Virtual Ist local address :
Virtual Ist local subnet mask :
Virtual Ist peer address :
Virtual Ist cluster-id :
Virtual Ist ISID    :
5520-24W-VOSS:1#
```

Migrating VSP Edge to Dedicated Switch mgmt CLIP

Both VSP edge switches were onboarded using their DHCP assigned IP addresses (which were made static IPs by ZTP+) and are still using the onboarding VLAN 4048 I-SID 15999999.

We want to transition the management of these VSP edge switches to a mgmt CLIP. To perform this task, the ExtremeCloud IQ - Site Engine Script named *Move to CLIP Mgmt IP* (available from GitHub) will be used.

Select both VSP edge switches, right-click, and select **Task > Provisioning > Move to CLIP Mgmt IP**.

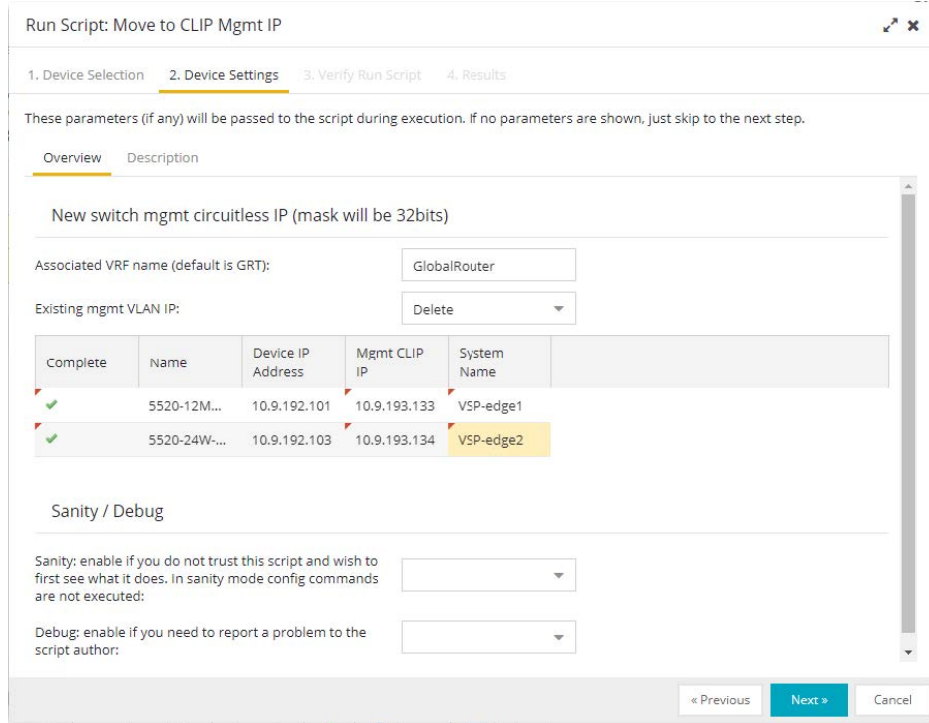


In the script input window, we provide the CLIP IP for the VSP edge switches. We allocate a couple of extra CLIPs from the 10.9.193.128/25 subnet that is available.

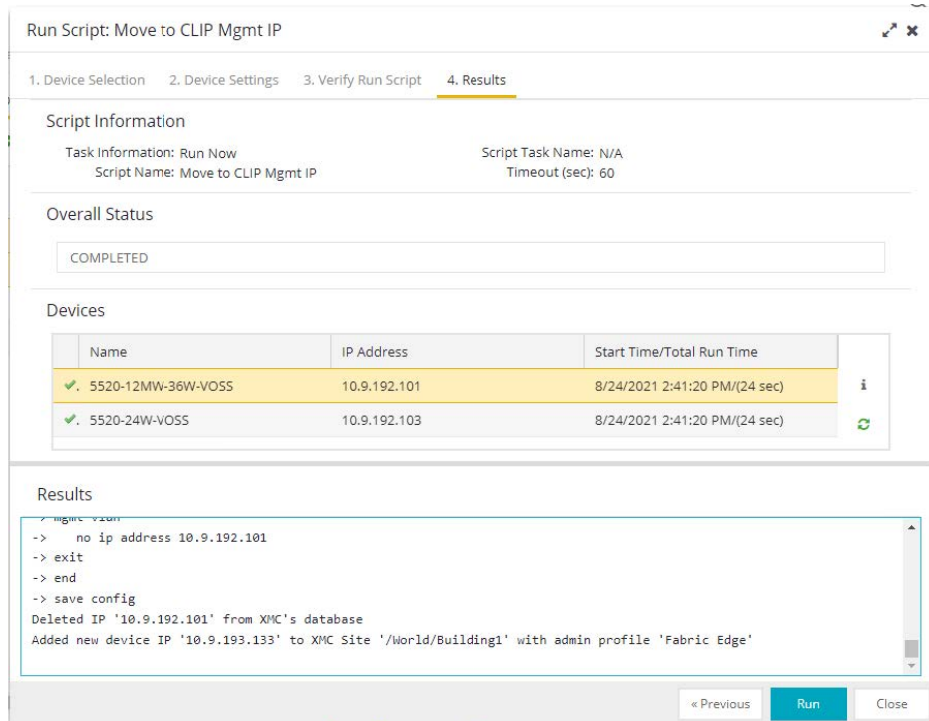
- VSP-edge1 10.9.193.133/32
- VSP-edge2 10.9.193.134/32

In the script inputs, leave the associated VRF as GlobalRouter (this is the only VRF supported for mgmt CLIP on a DVR Leaf), and set the dropdown to delete the pre-existing mgmt VLAN IP. Then provide the new CLIP IP for each VSP edge switch in the table below. Enter only the IP address (not the mask).

Because the script effectively removes and re-adds the same switch to ExtremeCloud IQ - Site Engine, it makes sense to rename the VSP edge switches as part of the same process. To do this, provide the desired switch names in the **System Name** column.



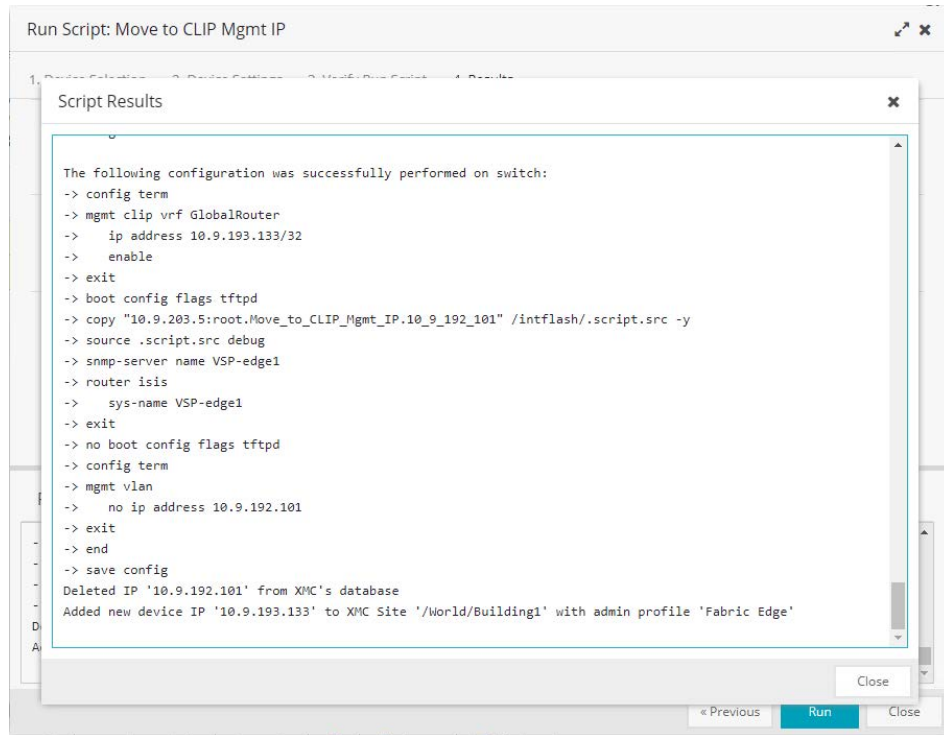
Select **Next**. Then select **Run**.



The script creates the new mgmt CLIP while at the same time deleting any preexisting mgmt CLIP or any pre-existing mgmt VLAN IP. Then it deletes the switch from ExtremeCloud IQ - Site Engine and re-adds it using the new CLIP IP. As part of the

same process, the switch is renamed. The new switch system name is assigned to both SNMP (CLI prompt) and ISIS.

When the script has completed, expand the **Results** window by selecting the **i** button.



The script essentially packs up the necessary CLI commands into a text file, which is then positioned on ExtremeCloud IQ - Site Engine's TFTP root directory. The switch then fetches the file via TFTP and executes it locally. Finally, the script deletes and re-adds the switch to ExtremeCloud IQ - Site Engine with the new CLIP IP (In a future VOSS release, single-command management IP conversion options will be made available).

Close the script window

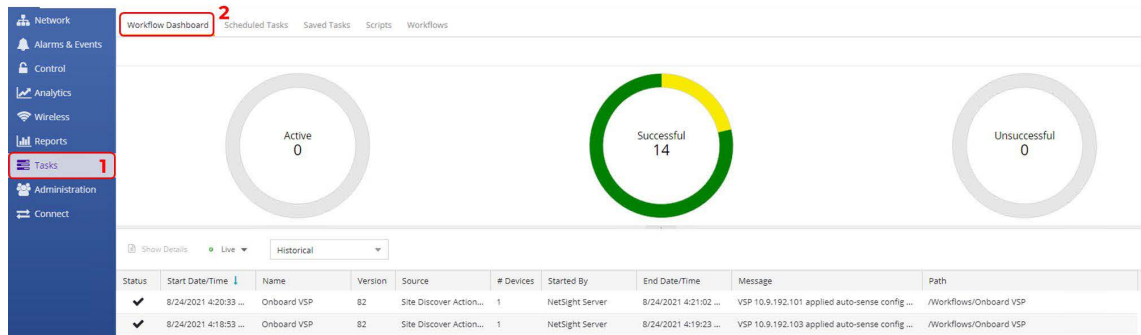
Now confirm that all four VSPs have their final management IP.

Select **Refresh** if necessary.

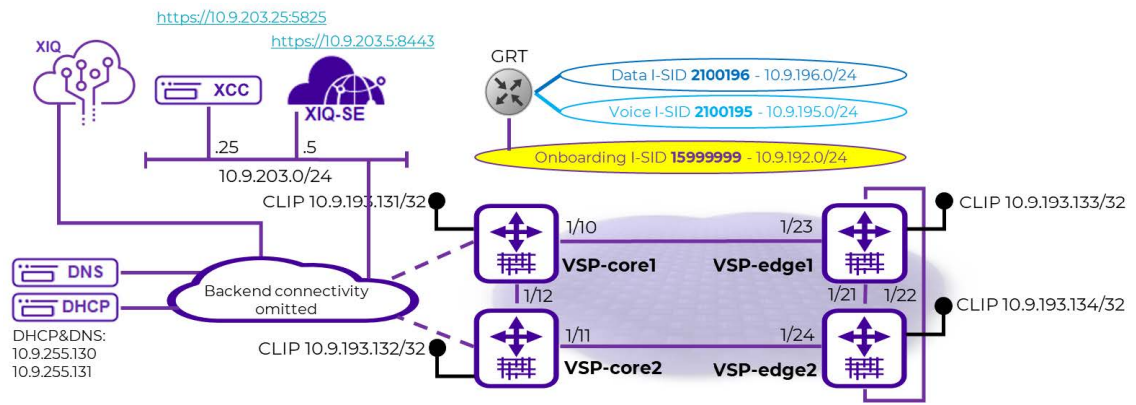
Status	Name ↑	Site	IP Address	Poll Status	Poll Details	Device Type	Family	Firmware
●	VSP-core1	/World/Building1	10.9.193.131	Available: 1...	Up: 55 Do...	VSP-4450GSX-PWR+	VSP Series	8.4.0.0
●	VSP-core2	/World/Building1	10.9.193.132	Available: 1...	Up: 55 Do...	VSP-4450GSX-PWR+	VSP Series	8.4.0.0
●	VSP-edge1	/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 that the *Move to CLIP Mgmt IP* script will have caused the *Onboard VSP* workflow to execute again. Verify the workflow execution for the new switch IP under **Tasks, Workflow Dashboard**.

Verify the workflow execution for the new switch IP under **Tasks, Workflow Dashboard**.



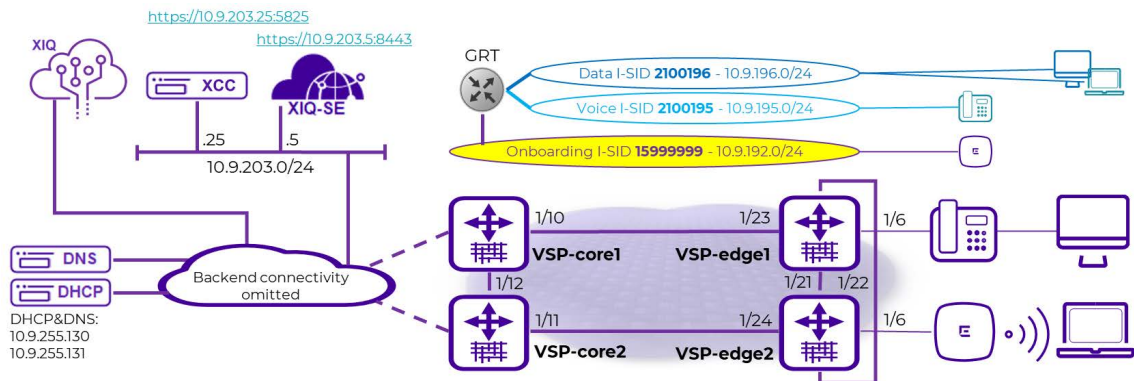
The following diagram shows what has been configured so far.





Verification that All End-Devices Are Operational

To verify that the process has worked, here is the same diagram with end stations added.



Inspection of VSP Fabric

Refresh the **Site Device** view.

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

Sites

World Building2 Topology Definitions Fabric Connect Service Definitions

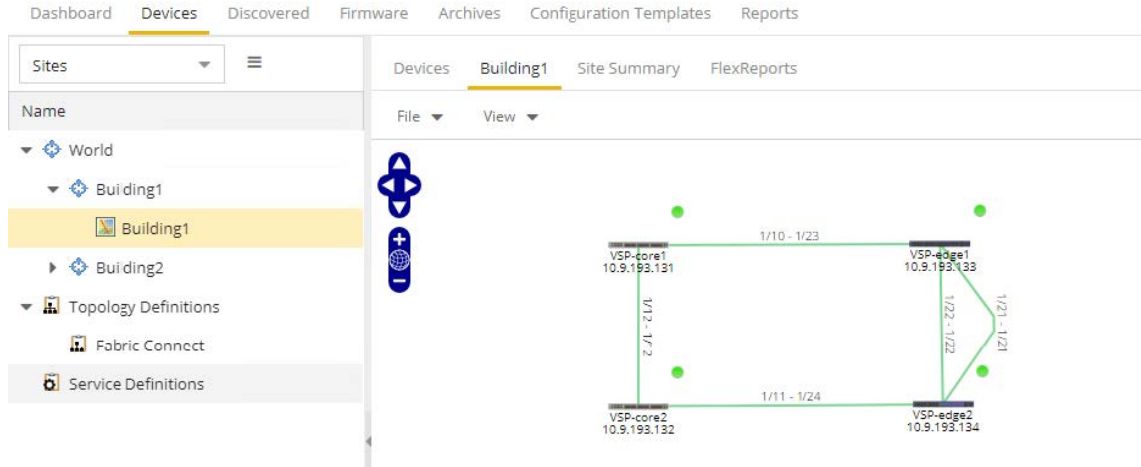
Devices Building1 Site Summary Endpoint Locations FlexReports

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: 65 Do...	VSP-4450GSX-PWR+	VSP Series	8.4.0.0
●	VSP-core2	/World/Building1	10.9.193.132	Available: 1...	Up: 65 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

The Fabric Edge is now deployed.

Visit the map and arrange the icons.



Right-click on the site or map and select **More Views > Fabric Topology**.

1

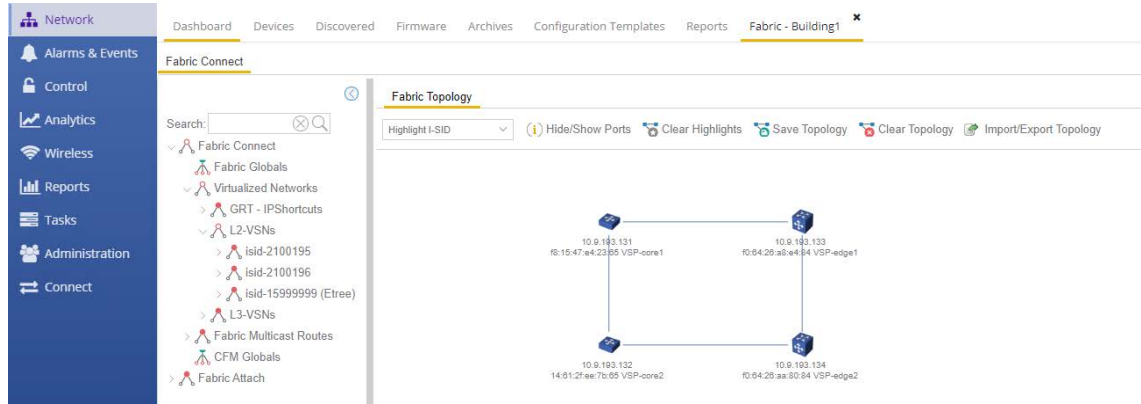
2

3

4

5

Then arrange the map.



The fabric is up. The fabric services are listed under **L2 VSN** and can be highlighted on the map using the dropdown.

To verify that DVR is operational, SSH to one of the VSPs and execute `show dvr members`.

```
VSP-core1:1#% show dvr members
-----
DVR Members (Domain ID: 1)
-----
System Name           Nick-Name           Nodal MAC           Role           SPB Cost
-----
VSP-core2             0.00.02            14:61:2f:ee:7b:65   Controller     10
VSP-edge1             a.10.0b           f0:64:26:a9:e4:84   Leaf           0
VSP-edge2             a.10.0a           f0:64:26:aa:80:84   Leaf           0
VSP-core1             0.00.01            f8:15:47:e4:23:65   Controller     -

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

The VSP cores are set up as controllers and the edge VSPs as DVR leaf.

Inspection of Endpoint Auto-Sense

Connect via SSH to both VSP edge switches. Run the CLI command

```
show interfaces gigabitEthernet auto-sense
```



```

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

-----
Port Auto-sense
-----
PORT      AUTO-SENSE  AUTO-SENSE
NUM      STATUS      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 has transitioned to voice state on the port where the telephone is connected. Also notice that ports 1/21-1/23 are auto-sense transitioned into NNI-ISIS state. These are the fabric interconnects that are automatically configured.

```

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

-----
Port Auto-sense
-----
PORT      AUTO-SENSE  AUTO-SENSE
NUM      STATUS      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#%

```

On VSP-edge2, notice that auto-sense transitioned into FA-WAP state where the access point is connected.

Verification that WLAN AP Is in Service

Connect to Extreme Campus Controller, and go to **Monitor > Devices > Access Points**. Make sure the AP is online and green. It must have an IP address on the AP-Mgmt I-SID 2X00194 in the onboarding subnet 10.9.192.0/24.

Status	Name	IP Address	Site	Version	Model	Radio 1	Radio 2	R1 Clients	R2 Clients
●	Edge-WAP	10.9.192.100	Fabric Edge Sandbox	7.4.1.0-016R	AP505i-FCC	Off	Off	0	0

On VSP-edge2, inspect what I-SIDs are configured on the AP port 1/6 using 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	2100196	2	196	ELAN	- D1-	Auto-sense Data		FALSE
1/6	197	15999999	4048	untag	ELAN	- - - - A -	Onboarding I-SID	disabled	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; R: multi-area redist
 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 is the onboarding I-SID, which is where the AP performs DHCP initially.

The second binding on the 1/6 port is discovered via fabric attach and is the Data I-SID binding for which the AP received the configuration from Extreme Campus Controller.

Edit VLAN [?] [X]

Name: Data Building1

Mode: Fabric Attach

VLAN ID: 106 Tagged

I-SID: 2100196

[ADVANCED]

[CANCEL] [Save]

Confirm by inspecting the fabric attach assignments on the switch using the CLI command

```
show fa assignment
```

```
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    Auto-sense Data

1 out of 1 Total Num of fabric attach assignment mappings displayed
acli.pl: Displayed Record Count = 1
=====
VSP-edge2:1#% █
```

The AP is fully operational, and a wireless client is able to associate onto the Data I-SID.

Verification that IP Phone Is in Service

On VSP-edge1, inspect what I-SIDs are configured on 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      VLANID C-VID  ISID  ORIGIN  ISID  NAME  BPDU  MAC
-----
1/6     197     2100195  3      195   ELAN  - - - - A -   Auto-sense Voice  FALSE
1/6     197     2100196  2      untag ELAN  - - - - A -   Auto-sense Data  disabled FALSE

2 out of 2 Total Num of i-sid endpoints displayed
acli.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; R: multi-area redist
l: discover by local switch  r: discover by remote VIST switch
VSP-edge1:1#% █
```

Note there are two bindings on the port where the phone is connected. The first binding is the Voice I-SID 2100195, which was assigned by auto-sense because a telephone was detected via LLDP. This is a tagged binding because it shows a VLAN-ID 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,PxB: 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#>
```

Notice the neighbor system capabilities: B = Bridge and T = Telephone. Also notice the IP address, which the phone obtained, is in the expected Voice I-SID subnet.

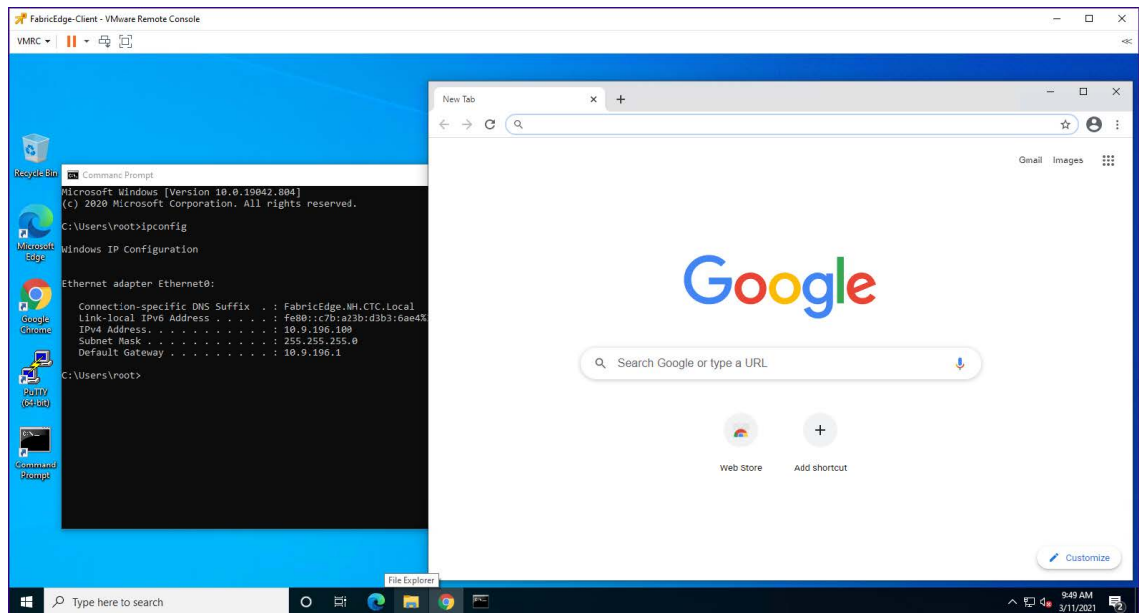
Verify that the phone can be pinged from either of the VSP cores. The phone must be able to connect to its call server.

```
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#>
```

Verification that Client PC Is on Data I-SID

On the PC client, run the browser and verify that it has connectivity to the Internet (hence, over the VSP Fabric).

Verify also that the client VM obtained an IP address in the Data I-SID 2X00196 IP subnet 10.9.196.0/24.



On the same VSP-edge1 port 1/6 where the phone is connected, confirm these 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	BPDU	MAC SUNI			
1/6	197	2100195	3	195	ELAN	-	---	-	---	A	-	Auto-sense Voice	disabled	FALSE
1/6	197	2100196	2	untag	ELAN	-	---	-	---	A	-	Auto-sense Data	disabled	FALSE

```

2 out of 2 Total Num of i-sid endpoints displayed
acli.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; R: multi-area redist
l: discover by local switch  r: discover by remote VIST switch
VSP-edge1:1#%

```

The second binding is untagged and is the auto-sense Data I-SID which automatically replaces the Onboarding I-SID on auto-sense ports that are in the state UNIONBOARDING and VOICE.

Deployment of Fabric VSP edge is now complete.



Appendix – Final Configurations

Here are the final configurations of all four VSPs.

VSP-core1

```
#
# Wed Aug 25 20:05:01 2021 EDT
# box type           : VSP-4450GSX-PWR+
# software version   : 8.4.0.0
# cli mode           : ECLI
#
#Card Info :
#   Slot 1 :
#
#               CardType : 4450GSX-PWR+
#               CardDescription : 4450GSX-PWR+
#               CardSerial# : 14JP335E5081
#               CardPart# :
#               CardAssemblyDate : 20140814
#               CardHWRevision : 01
#               CardHWConfig : none
#               OperStatus : up
#
#!end
#
config terminal
#
# BOOT CONFIGURATION
#
boot config flags sshd
#boot config sio console baud 9600 1
# end boot flags
#
# SPBM CONFIGURATION
#
spbm
spbm ethertype 0x8100
spbm nick-name server prefix A.10.00
spbm nick-name server
#
# CLI CONFIGURATION
#
prompt "VSP-core1"
password password-history 3
#
# CLOCK TIME-ZONE CONFIGURATION
#
clock time-zone US Eastern
#
# SYSTEM CONFIGURATION
#
ip domain-name "FabricEdge.NH.CTC.Local"
ip name-server primary 10.9.255.130
```

```

ip name-server secondary 10.9.255.131
syslog host 1
syslog host 1 address 10.9.203.5
syslog host 1 enable
#
# LOG CONFIGURATION
#
# LINK-FLAP-DETECT CONFIGURATION
#
# IEEE VLAN AGING CONFIGURATION
#
# ACCESS-POLICY CONFIGURATION
#
# SSH CONFIGURATION
#
ssh
#
# MCAST SOFTWARE FORWARDING CONFIGURATION
#
# SNMP V3 GLOBAL CONFIGURATION
#
# SNMP V3 GROUP MEMBERSHIP CONFIGURATION
#
snmp-server user admin group "initial"
snmp-server user snmpuser group "snmpuser"
snmp-server user snmpuser group "snmpuser"
#
# SNMP V3 NOTIFY FILTER CONFIGURATION
#
# SNMP V3 MIB VIEW CONFIGURATION
#
# SNMP V3 GROUP CONFIGURATION
#
snmp-server group "snmpuser" "" auth-priv notify-view root
#
# SNMP V3 TARGET ADDRESS CONFIGURATION #
snmp -server host 10.9.203.5 v3 authPriv snmpuser inform
#
# DDI CONFIGURATION #
# SLOT CONFIGURATION #
# MAC AGING CONFIGURATION #
# SMTP CONFIGURATION #
# WEB CONFIGURATION #
web-server enable
no web-server secure-only
#
# GLOBAL FDB FILTER CONFIGURATION
#
# QOS CONFIGURATION- PHASE I
#
# LACP CONFIGURATION
#
# VRF CONFIGURATION
#
# MAINTENANCE-DOMAIN CONFIGURATION
#
# MAINTENANCE-ASSOCIATION CONFIGURATION
#
# MAINTENANCE-ENDPOINT CONFIGURATION
#
# POE GLOBAL CONFIGURATION
#
# PORT CONFIGURATION- PHASE I
#

```

```
interface GigabitEthernet 1/12
encapsulation dot1q

exit

#
# ISIS SPBM CONFIGURATION
#
router isis
spbm 1
spbm 1 nick-name 0.00.01
spbm 1 b-vid 4051-4052 primary 4051
spbm 1 multicast enable
spbm 1 ip enable
exit

#
# SPB-PIM-GW CONFIGURATION
#
# MLT CONFIGURATION
#
# IP PREFIX LIST CONFIGURATION- GlobalRouter
#
# IP PREFIX LIST CONFIGURATION- VRF
#
# IPv6 PREFIX LIST CONFIGURATION- GlobalRouter
#
# IPv6 PREFIX LIST CONFIGURATION- VRF
#
# RMON CONFIGURATION
#
# DVR CONFIGURATION
#
dvr controller 1

#
# VLAN CONFIGURATION
#
vlan members remove 1 1/1-1/50 portmember
vlan create 195 name "Voice" type port-mstprstp 0
vlan i-sid 195 2100195
interface Vlan 195
dvr gw-ipv4 10.9.195.1
dvr enable
ip address 10.9.195.2 255.255.255.0 1
ip dhcp-relay
exit
vlan create 196 name "Data" type port-mstprstp 0
vlan i-sid 196 2100196
interface Vlan 196
dvr gw-ipv4 10.9.196.1
dvr enable
ip address 10.9.196.2 255.255.255.0 1
ip dhcp-relay
exit
vlan create 4048 name "onboarding-vlan" type port-mstprstp 0
vlan i-sid 4048 15999999
interface Vlan 4048
ip address 10.9.192.2 255.255.255.0 2
ip dhcp-relay
ip vrrp version 3
ip vrrp address 1 10.9.192.1
ip vrrp 1 enable
exit
```



```
vlan create 4051 name "B-VLAN-1" type spbm-bvlan
vlan create 4052 name "B-VLAN-2" type spbm-bvlan

#
# MSTP CONFIGURATION
#
# NLS CONFIGURATION
#
mgmt clip vrf GlobalRouter
ip address 10.9.193.131/32
enable
exit
#
# FHS CONFIGURATION
#
# MAC ACL CONFIGURATION
#
# IPv6 FHS ACL CONFIGURATION
#
# RA-GUARD CONFIGURATION
#
# DHCP-GUARD CONFIGURATION
#
# FHS SNOOPING CONFIGURATION
#
# SFLOW CONFIGURATION
#
# DHCP SNOOPING CONFIGURATION
#
# DHCP SNOOPING BINDING CONFIGURATION
#
# VIRTUAL IST CONFIGURATION
#
# MLT INTERFACE CONFIGURATION
#
# PORT CONFIGURATION - PHASE II
#
interface GigabitEthernet 1/2
no shutdown
brouter port 1/2 vlan 4000 subnet 10.9.223.2/255.255.255.252 mac-offset 0
ip bfd enable
no spanning-tree mstp force-port-state enable
exit
interface GigabitEthernet 1/10
default-vlan-id 0
auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/12
default-vlan-id 0
no shutdown
isis
isis spbm 1
isis enable
no spanning-tree mstp force-port-state enable
no spanning-tree mstp msti 62 force-port-state enable
exit
interface GigabitEthernet 1/13
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/14
no lldp tx-tlv med extendedPSE
```

```
exit
interface GigabitEthernet 1/15
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/16
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/17
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/18
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/19
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/20
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/21
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/22
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/23
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/24
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/25
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/26
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/27
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/28
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/29
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/30
no lldp tx-tlv med extendedPSE
```

```
exit
interface GigabitEthernet 1/31
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/32
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/33
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/34
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/35
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/36
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/37
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/38
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/39
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/40
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/41
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/42
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/43
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/44
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/45
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/46
no lldp tx-tlv med extendedPSE
```

```
exit
interface GigabitEthernet 1/47
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/48
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/49
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/50
no lldp tx-tlv med extendedPSE

exit

#
# LINK-STATE TRACKING
#
# IP CONFIGURATION
#
# IP AS LIST CONFIGURATION - GlobalRouter
#
# IP COMMUNITY LIST CONFIGURATION - GlobalRouter
#
# IP EXTENDED COMMUNITY LIST CONFIGURATION - GlobalRouter
#
# IP ROUTE MAP CONFIGURATION - GlobalRouter
#
# IP CONFIGURATION - GlobalRouter
#
ip route 0.0.0.0 0.0.0.0 10.9.223.1 weight 10

#
# BFD CONFIGURATION - GlobalRouter
#
router bfd enable
ip route bfd 10.9.223.1

#
# CIRCUITLESS IP INTERFACE CONFIGURATION - GlobalRouter
#
interface loopback 1
ip address 1 10.9.193.129/255.255.255.255
exit

#
# TOPOLOGY-CLIP-IP
#
# MSDP CONFIGURATION - GlobalRouter
#
# CIRCUITLESS IPV6 INTERFACE CONFIGURATION - GlobalRouter
#
# VRRP CONFIGURATION - GlobalRouter
#
# UDP FORWARDING CONFIGURATION - GlobalRouter
#
# UDP FORWARDING CONFIGURATION - VRF
#
# UDP FORWARDING PORT CONFIGURATION
#
# UDP FORWARDING VLAN CONFIGURATION
```

```
#
# DHCP CONFIGURATION - GlobalRouter
#
ip dhcp-relay fwd-path 10.9.192.2 10.9.255.130
ip dhcp-relay fwd-path 10.9.192.2 10.9.255.130 enable
ip dhcp-relay fwd-path 10.9.192.2 10.9.255.130 mode dhcp
ip dhcp-relay fwd-path 10.9.192.2 10.9.255.131
ip dhcp-relay fwd-path 10.9.192.2 10.9.255.131 enable
ip dhcp-relay fwd-path 10.9.192.2 10.9.255.131 mode dhcp
ip dhcp-relay fwd-path 10.9.195.2 10.9.255.130
ip dhcp-relay fwd-path 10.9.195.2 10.9.255.130 enable
ip dhcp-relay fwd-path 10.9.195.2 10.9.255.130 mode bootp_dhcp
ip dhcp-relay fwd-path 10.9.195.2 10.9.255.131
ip dhcp-relay fwd-path 10.9.195.2 10.9.255.131 enable
ip dhcp-relay fwd-path 10.9.195.2 10.9.255.131 mode bootp_dhcp
ip dhcp-relay fwd-path 10.9.196.2 10.9.255.130
ip dhcp-relay fwd-path 10.9.196.2 10.9.255.130 enable
ip dhcp-relay fwd-path 10.9.196.2 10.9.255.130 mode bootp_dhcp
ip dhcp-relay fwd-path 10.9.196.2 10.9.255.131
ip dhcp-relay fwd-path 10.9.196.2 10.9.255.131 enable
ip dhcp-relay fwd-path 10.9.196.2 10.9.255.131 mode bootp_dhcp

#
# RIP CONFIGURATION - GlobalRouter
#
# RIP VLAN CONFIGURATION
#
# IGMP CONFIGURATION - GlobalRouter
#
# MCAST RESOURCE USAGE CONFIGURATION
#
# TIMED PRUNE CONFIGURATION - GlobalRouter
#
# RSMLT CONFIGURATION
#
# IPV6 CONFIGURATION - GlobalRouter
#
# MLD CONFIGURATION - GlobalRouter
#
# ISIS CONFIGURATION
#
router isis
sys-name "VSP-core1"
ip-source-address 10.9.193.129
is-type l1
manual-area 49.0000
exit
router isis enable
#
# LOGICAL ISIS CONFIGURATION
#
# VTEP CONFIGURATION
#
# REMOTE VTEP CONFIGURATIONS
#
# VLAN NODAL MEP/MIP CONFIGURATION
#
# QOS CONFIGURATION - PHASE II
#
qos queue-profile 1 member add 1/1-1/50
#
# CFM CONFIGURATION - PHASE II
#
cfm spbm enable
```

```
#
# DIAG CONFIGURATION
#
# NTP CONFIGURATION
#
no ntp

#
# ES CONFIGURATION
#
# OSPF CONFIGURATION - GlobalRouter
#
router ospf
exit

#
# OSPF CONFIGURATION - VRF
#
# OSPF ACCEPT CONFIGURATION - GlobalRouter
#
# OSPF ACCEPT CONFIGURATION - VRF
#
# BGP CONFIGURATION - GlobalRouter
#
# BGP CONFIGURATION - VRF
#
# ISIS SPBM IPVPN CONFIGURATION
#
# IP ISID LIST CONFIGURATION - GlobalRouter
#
# IP ISID LIST CONFIGURATION - VRF
#
# ISIS ACCEPT CONFIGURATION - GlobalRouter
#
# ISIS ACCEPT CONFIGURATION - VRF
#
# ISIS IPv6 ACCEPT CONFIGURATION - GlobalRouter
#
# ISIS IPv6 ACCEPT CONFIGURATION - VRF
#
# IP REDISTRIBUTION CONFIGURATION - GlobalRouter
#
router isis
redistribute static
redistribute static enable
redistribute direct
redistribute direct enable
exit

#
# IP REDISTRIBUTION CONFIGURATION - VRF
#
# OSPF VLAN CONFIGURATION
#
# OSPF PORT CONFIGURATION
#
# OSPF LOOPBACK CONFIGURATION
#
# RIP PORT CONFIGURATION
#
# IPVPN CONFIGURATION
#
# SLPP CONFIGURATION
```

```
#
# FILTER CONFIGURATION
#
# APPLICATION TELEMETRY CONFIGURATION
#
# IPV6 TUNNEL CONFIGURATION
#
# IPV6 OSPFV3 CONFIGURATION - GlobalRouter
#
# IPV6 RIPng CONFIGURATION
#
router rip
exit

#
# IPV6 STATIC ROUTE CONFIGURATION - GlobalRouter
#
# IPV6 OSPF VLAN CONFIGURATION
#
# IPV6 OSPF PORT CONFIGURATION
#
# IPV6 RIP VLAN CONFIGURATION
#
# IPV6 RIP PORT CONFIGURATION
#
# IPV6 VRRP VLAN CONFIGURATION
#
# IPV6 VRRP PORT CONFIGURATION
#
# IPV6 NEIGHBOR CONFIGURATION - GlobalRouter
#
# IPV6 STATIC ROUTE BFD CONFIGURATION - GlobalRouter
#
# IPV6 DHCP CONFIGURATION - GlobalRouter
#
# IPV6 DHCP CONFIGURATION - VRF
#
# I-SID NAME CONFIGURATION
#
i-sid name 2100195 "Auto-sense Voice"
i-sid name 2100196 "Auto-sense Data"
i-sid name 15999999 "Onboarding I-SID"
#
# I-SID CONFIGURATION
#
i-sid 2100195 elan
exit i-sid 15999999 elan
exit

#
# GLOBAL AUTO-SENSE CONFIGURATION
#
auto-sense voice i-sid 2100195 c-vid 195
auto-sense eapol voice lldp-auth
auto-sense data i-sid 2100196
auto-sense onboarding i-sid 15999999

#
# RADIUS CONFIGURATION
#
radius server host 10.9.203.6 key ***** used-by eapol
radius enable
radius dynamic-server client 10.9.203.6 secret ***** enable
```

```

#
# TACACS CONFIGURATION
#
# LLDP CONFIGURATION
#
# EAP CONFIGURATION
#
eapol enable

#
# MACSEC CONFIGURATION
#
# GLOBAL MACSec CA Configured
#
# FABRIC ATTACH CONFIGURATION
#
# DVR IP REDISTRIBUTION CONFIGURATION - GlobalRouter
#
# DVR IP REDISTRIBUTION CONFIGURATION - VRF
#
# SPB -PIM-GW CONFIGURATION
#
# SOFTWARE CONFIGURATION
#
# APPLICATION CONFIGURATION
#
# IPSEC CONFIGURATION
#
# IPSEC POLICY TABLE CONFIGURATION
#
# IPSEC SA TABLE CONFIGURATION
#
# IPSEC SA POLICY LINK TABLE CONFIGURATION
#
# IPV6 OSPFV3 IPSEC CONFIGURATION
#
# IPV6 IPSEC INTERFACE CONFIGURATION
#
# IP IPSEC INTERFACE CONFIGURATION
#
# IKE CONFIGURATION
#
# SYSTEM CONFIGURATION Phase 2
#
end

#
# IP REDISTRIBUTE APPLY CONFIGURATIONS
#
isis apply redistribute static
isis apply redistribute direct
#
# IP ECMP APPLY CONFIGURATIONS

```

VSP -core2

```

#
# Wed Aug 25 22:32:22 2021 EDT
# box type : VSP-4450GSX-PWR+
# software version : 8.4.0.0
# cli mode : ECLI
#

```



```
#Card Info :
# Slot 1 :
#
#           CardType : 4450GSX-PWR+
#           CardDescription : 4450GSX-PWR+
#           CardSerial# : 17JP0230E58J
#           CardPart# : EC4400A05-E6
#           CardAssemblyDate : 20170110
#           CardHWRevision : 03
#           CardHWConfig : none
#           OperStatus : up
#!end
#
config terminal
#
# BOOT CONFIGURATION
#
boot config flags sshd
#boot config sio console baud 9600 1
# end boot flags
#
# SPBM CONFIGURATION
#
spbm
spbm ethertype 0x8100
spbm nick-name server prefix A.10.00 spbm nick-name server
#
# CLI CONFIGURATION
#
prompt "VSP-core2"
password password-history 3
#
# CLOCK TIME-ZONE CONFIGURATION
#
clock time-zone US Eastern
#
# SYSTEM CONFIGURATION
#
ip domain-name "FabricEdge.NH.CTC.Local" ip name-server primary 10.9.255.130
ip name-server secondary 10.9.255.131 syslog host 1
syslog host 1 address 10.9.203.5
syslog host 1 enable
#
# LOG CONFIGURATION
#
# LINK-FLAP-DETECT CONFIGURATION
#
# IEEE VLAN AGING CONFIGURATION
#
# ACCESS-POLICY CONFIGURATION
#
# SSH CONFIGURATION
#
ssh
#
# MCAST SOFTWARE FORWARDING CONFIGURATION
#
# SNMP V3 GLOBAL CONFIGURATION
#
# SNMP V3 GROUP MEMBERSHIP CONFIGURATION
#
snmp-server user admin group "initial" snmp-server user snmpuser group "snmpuser" snmp-
server user snmpuser group "snmpuser"
#
# SNMP V3 NOTIFY FILTER CONFIGURATION
```

```
#
# SNMP V3 MIB VIEW CONFIGURATION
#
# SNMP V3 GROUP CONFIGURATION
#
snmp-server group "snmpuser" "" auth-priv notify-view root
#
# SNMP V3 TARGET ADDRESS CONFIGURATION
#
snmp-server host 10.9.203.5 v3 authPriv snmpuser inform
#
# DDI CONFIGURATION
#
# SLOT CONFIGURATION
#
# MAC AGING CONFIGURATION
#
# SMTP CONFIGURATION
#
# WEB CONFIGURATION
#
web-server enable
no web-server secure-only
#
# GLOBAL FDB FILTER CONFIGURATION
#
# QOS CONFIGURATION - PHASE I
#
# LACP CONFIGURATION
#
# VRF CONFIGURATION
#
# MAINTENANCE-DOMAIN CONFIGURATION
#
# MAINTENANCE-ASSOCIATION CONFIGURATION
#
# MAINTENANCE-ENDPOINT CONFIGURATION
#
# POE GLOBAL CONFIGURATION
#
# PORT CONFIGURATION - PHASE I
#
interface GigabitEthernet 1/12
encapsulation dot1q
exit
#
# ISIS SPBM CONFIGURATION
#
router isis
spbm 1
spbm 1 nick-name 0.00.02
spbm 1 b-vid 4051-4052 primary 4051
spbm 1 multicast enable
spbm 1 ip enable
exit
#
# SPB-PIM-GW CONFIGURATION
#
# MLT CONFIGURATION
#
# IP PREFIX LIST CONFIGURATION - GlobalRouter
#
# IP PREFIX LIST CONFIGURATION - VRF
#
```

```
# IPv6 PREFIX LIST CONFIGURATION - GlobalRouter
#
# IPv6 PREFIX LIST CONFIGURATION - VRF
#
# RMON CONFIGURATION
#
# DVR CONFIGURATION
#
dvr controller 1
#
# VLAN CONFIGURATION
#
vlan members remove 1 1/1-1/50 portmember
vlan create 195 name "Voice" type port-mstprstp 0
vlan i-sid 195 2100195
interface Vlan 195
dvr gw-ipv4 10.9.195.1
dvr enable
ip address 10.9.195.3 255.255.255.0 1
ip dhcp-relay
exit
vlan create 196 name "Data" type port-mstprstp 0
vlan i-sid 196 2100196
interface Vlan 196
dvr gw-ipv4 10.9.196.1
dvr enable
ip address 10.9.196.3 255.255.255.0 1
ip dhcp-relay
exit
vlan create 4048 name "onboarding-vlan" type port-mstprstp 0 vlan i-sid 4048 15999999
interface Vlan 4048
ip address 10.9.192.3 255.255.255.0 2
ip dhcp-relay
ip vrrp version 3
ip vrrp address 1 10.9.192.1
ip vrrp 1 enable
exit
vlan create 4051 name "B-VLAN-1" type spbm-bvlan
vlan create 4052 name "B-VLAN-2" type spbm-bvlan
#
# MSTP CONFIGURATION
#
# NLS CONFIGURATION
#
mgmt clip vrf GlobalRouter
ip address 10.9.193.132/32
enable
exit
#
# FHS CONFIGURATION
#
# MAC ACL CONFIGURATION
#
# IPv6 FHS ACL CONFIGURATION
#
# RA-GUARD CONFIGURATION
#
# DHCP-GUARD CONFIGURATION
#
# FHS SNOOPING CONFIGURATION
#
# SFLOW CONFIGURATION
#
# DHCP SNOOPING CONFIGURATION
```

```
#
# DHCP SNOOPING BINDING CONFIGURATION
#
# VIRTUAL IST CONFIGURATION
#
# MLT INTERFACE CONFIGURATION
#
# PORT CONFIGURATION - PHASE II
#
interface GigabitEthernet 1/2
no shutdown
brouter port 1/2 vlan 4000 subnet 10.9.223.6/255.255.255.252 mac-offset 0 ip bfd enable
no spanning-tree mstp force-port-state enable
exit
interface GigabitEthernet 1/11
default-vlan-id 0
auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/12
default-vlan-id 0
no shutdown
isis
isis spbm 1
isis enable
no spanning-tree mstp force-port-state enable
no spanning-tree mstp msti 62 force-port-state enable

exit
interface GigabitEthernet 1/13
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/14
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/15
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/16
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/17
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/18
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/19
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/20
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/21
no lldp tx-tlv med extendedPSE
```

```
exit
interface GigabitEthernet 1/22
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/23
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/24
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/25
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/26
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/27
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/28
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/29
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/30
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/31
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/32
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/33
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/34
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/35
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/36
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/37
no lldp tx-tlv med extendedPSE
```

```
exit
interface GigabitEthernet 1/38
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/39
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/40
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/41
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/42
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/43
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/44
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/45
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/46
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/47
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/48
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/49
no lldp tx-tlv med extendedPSE

exit
interface GigabitEthernet 1/50
no lldp tx-tlv med extendedPSE

exit
#
# LINK-STATE TRACKING
#
# IP CONFIGURATION
#
# IP AS LIST CONFIGURATION - GlobalRouter
#
# IP COMMUNITY LIST CONFIGURATION - GlobalRouter
#
# IP EXTENDED COMMUNITY LIST CONFIGURATION - GlobalRouter
#
```

```

# IP ROUTE MAP CONFIGURATION - GlobalRouter
#
# IP CONFIGURATION - GlobalRouter
#
ip route 0.0.0.0 0.0.0.0 10.9.223.5 weight 10
#
# BFD CONFIGURATION - GlobalRouter
#
router bfd enable
ip route bfd 10.9.223.5
#
# CIRCUITLESS IP INTERFACE CONFIGURATION - GlobalRouter
#
interface loopback 1
ip address 1 10.9.193.130/255.255.255.255
exit
#
# TOPOLOGY-CLIP-IP
#
# MSDP CONFIGURATION - GlobalRouter
#
# CIRCUITLESS IPV6 INTERFACE CONFIGURATION - GlobalRouter
#
# VRRP CONFIGURATION - GlobalRouter
#
# UDP FORWARDING CONFIGURATION - GlobalRouter
#
# UDP FORWARDING CONFIGURATION - VRF
#
# UDP FORWARDING PORT CONFIGURATION
#
# UDP FORWARDING VLAN CONFIGURATION
#
# DHCP CONFIGURATION - GlobalRouter
#
ip dhcp-relay fwd-path 10.9.192.3 10.9.255.130
ip dhcp-relay fwd-path 10.9.192.3 10.9.255.130 enable
ip dhcp-relay fwd-path 10.9.192.3 10.9.255.130 mode dhcp
ip dhcp-relay fwd-path 10.9.192.3 10.9.255.131
ip dhcp-relay fwd-path 10.9.192.3 10.9.255.131 enable
ip dhcp-relay fwd-path 10.9.192.3 10.9.255.131 mode dhcp
ip dhcp-relay fwd-path 10.9.195.3 10.9.255.130
ip dhcp-relay fwd-path 10.9.195.3 10.9.255.130 enable
ip dhcp-relay fwd-path 10.9.195.3 10.9.255.130 mode bootp_dhcp ip dhcp-relay fwd-path
10.9.195.3 10.9.255.131
ip dhcp-relay fwd-path 10.9.195.3 10.9.255.131 enable
ip dhcp-relay fwd-path 10.9.195.3 10.9.255.131 mode bootp_dhcp ip dhcp-relay fwd-path
10.9.196.3 10.9.255.130
ip dhcp-relay fwd-path 10.9.196.3 10.9.255.130 enable
ip dhcp-relay fwd-path 10.9.196.3 10.9.255.130 mode bootp_dhcp ip dhcp-relay fwd-path
10.9.196.3 10.9.255.131
ip dhcp-relay fwd-path 10.9.196.3 10.9.255.131 enable
ip dhcp-relay fwd-path 10.9.196.3 10.9.255.131 mode bootp_dhcp
#
# RIP CONFIGURATION - GlobalRouter
#
# RIP VLAN CONFIGURATION
#
# IGMP CONFIGURATION - GlobalRouter
#
# MCAST RESOURCE USAGE CONFIGURATION
#
# TIMED PRUNE CONFIGURATION - GlobalRouter
#

```

```
# RSMLT CONFIGURATION
#
# IPV6 CONFIGURATION - GlobalRouter
#
# MLD CONFIGURATION - GlobalRouter
#
# ISIS CONFIGURATION
#
router isis
sys-name "VSP-core2"
ip-source-address 10.9.193.130
is-type l1
manual-area 49.0000
exit
router isis enable
#
# LOGICAL ISIS CONFIGURATION
#
# VTEP CONFIGURATION
#
# REMOTE VTEP CONFIGURATIONS
#
# VLAN NODAL MEP/MIP CONFIGURATION
#
# QOS CONFIGURATION - PHASE II
#
qos queue-profile 1 member add 1/1-1/50
#
# CFM CONFIGURATION - PHASE II
#
cfm spbm enable
#
# DIAG CONFIGURATION
#
# NTP CONFIGURATION
#
no ntp
#
# ES CONFIGURATION
#
# OSPF CONFIGURATION - GlobalRouter
#
router ospf
exit
#
# OSPF CONFIGURATION - VRF
#
# OSPF ACCEPT CONFIGURATION - GlobalRouter
#
# OSPF ACCEPT CONFIGURATION - VRF
#
# BGP CONFIGURATION - GlobalRouter
#
# BGP CONFIGURATION - VRF
#
# ISIS SPBM IPVPN CONFIGURATION
#
# IP ISID LIST CONFIGURATION - GlobalRouter
#
# IP ISID LIST CONFIGURATION - VRF
#
# ISIS ACCEPT CONFIGURATION - GlobalRouter
#
# ISIS ACCEPT CONFIGURATION - VRF
```



```
#
# ISIS IPv6 ACCEPT CONFIGURATION - GlobalRouter
#
# ISIS IPv6 ACCEPT CONFIGURATION - VRF
#
# IP REDISTRIBUTION CONFIGURATION - GlobalRouter
#
router isis
redistribute static
redistribute static enable
redistribute direct
redistribute direct enable
exit
#
# IP REDISTRIBUTION CONFIGURATION - VRF
#
# OSPF VLAN CONFIGURATION
#
# OSPF PORT CONFIGURATION
#
# OSPF LOOPBACK CONFIGURATION
#
# RIP PORT CONFIGURATION
#
# IPVPN CONFIGURATION
#
# SLPP CONFIGURATION
#
# FILTER CONFIGURATION
#
# APPLICATION TELEMETRY CONFIGURATION
#
# IPV6 TUNNEL CONFIGURATION
#
# IPV6 OSPFV3 CONFIGURATION - GlobalRouter
#
# IPV6 RIPng CONFIGURATION
#
router rip
exit
#
# IPV6 STATIC ROUTE CONFIGURATION - GlobalRouter
#
# IPV6 OSPF VLAN CONFIGURATION
#
# IPV6 OSPF PORT CONFIGURATION
#
# IPV6 RIP VLAN CONFIGURATION
#
# IPV6 RIP PORT CONFIGURATION
#
# IPV6 VRRP VLAN CONFIGURATION
#
# IPV6 VRRP PORT CONFIGURATION
#
# IPV6 NEIGHBOR CONFIGURATION - GlobalRouter
#
# IPV6 STATIC ROUTE BFD CONFIGURATION - GlobalRouter
#
# IPV6 DHCP CONFIGURATION - GlobalRouter
#
# IPV6 DHCP CONFIGURATION - VRF
#
# I-SID NAME CONFIGURATION
```

```
#
i-sid name 2100195 "Auto-sense Voice"
i-sid name 2100196 "Auto-sense Data"
i-sid name 15999999 "Onboarding I-SID"
#
# I-SID CONFIGURATION
#
i-sid 2100195 elan
exit
i-sid 15999999 elan
exit
#
# GLOBAL AUTO-SENSE CONFIGURATION
#
auto-sense voice i-sid 2100195 c-vid 195
auto-sense eapol voice lldp-auth
auto-sense data i-sid 2100196
auto-sense onboarding i-sid 15999999
#
# RADIUS CONFIGURATION
#
radius server host 10.9.203.6 key ***** used-by eapol radius enable
radius dynamic-server client 10.9.203.6 secret ***** enable
#
# TACACS CONFIGURATION
#
# LLDP CONFIGURATION
#
# EAP CONFIGURATION
#
eapol enable
#
# MACSEC CONFIGURATION
#
# GLOBAL MACSec CA Configured
#
# FABRIC ATTACH CONFIGURATION
#
# DVR IP REDISTRIBUTION CONFIGURATION - GlobalRouter
#
# DVR IP REDISTRIBUTION CONFIGURATION - VRF
#
# SPB-PIM-GW CONFIGURATION
#
# SOFTWARE CONFIGURATION
#
# APPLICATION CONFIGURATION
#
# IPSEC CONFIGURATION
#
# IPSEC POLICY TABLE CONFIGURATION
#
# IPSEC SA TABLE CONFIGURATION
#
# IPSEC SA POLICY LINK TABLE CONFIGURATION
#
# IPV6 OSPFV3 IPSEC CONFIGURATION
#
# IPV6 IPSEC INTERFACE CONFIGURATION
#
# IP IPSEC INTERFACE CONFIGURATION
#
# IKE CONFIGURATION
#
```

```

# SYSTEM CONFIGURATION Phase 2
#
end
#
# IP REDISTRIBUTE APPLY CONFIGURATIONS
isis apply redistribute static isis apply redistribute direct
#
# IP ECMP APPLY CONFIGURATIONS

```

VSP -edge1

```

#
# Thu Aug 26 03:01:28 2021 EDT
# box type : 5520-12MW-36W-VOSS
# software version           : 8.4.0.0
# cli mode                   : ECLI #
#Card Info :
# Slot 1 :
#
#                               CardType : 5520-12MW-36W-VOSS
#                               CardDescription : 5520-12MW-36W-VOSS
#                               CardSerial# : SB012050G-00079
#                               CardPart# : 800990-00-AB
#                               CardAssemblyDate : 20201216
#                               CardHWRevision : AB
#                               CardHWConfig :
#                               AdminStatus : up
#                               OperStatus : up
#
#!end
#
config terminal

#
# BOOT CONFIGURATION
#
boot config flags dvr-leaf-mode
boot config flags ftpd
boot config flags sshd
boot config flags telnetd
#boot config sio console baud 115200 1
# end boot flags
#
# SPBM CONFIGURATION
#
spbm
spbm ethertype 0x8100
#
# CLI CONFIGURATION
#
prompt "VSP-edge1"
password password-history 3
#
# CLOCK TIME-ZONE CONFIGURATION
#
clock time-zone US Eastern
#
# SYSTEM CONFIGURATION
#
ip domain-name "FabricEdge.NH.CTC.Local" ip name-server primary 10.9.255.130
ip name-server secondary 10.9.255.131 syslog host 1
syslog host 1 address 10.9.203.5
syslog host 1 enable
#

```

```

# LOG CONFIGURATION
#
# LINK-FLAP-DETECT CONFIGURATION
#
# IEEE VLAN AGING CONFIGURATION
#
# ACCESS-POLICY CONFIGURATION
#
# SSH CONFIGURATION
#
ssh
#
# MCAST SOFTWARE FORWARDING CONFIGURATION
#
# SNMP V3 GLOBAL CONFIGURATION
#
# SNMP V3 GROUP MEMBERSHIP CONFIGURATION
#
snmp-server user admin group "initial" snmp-server user snmpuser group "snmpuser" snmp-
server user snmpuser group "snmpuser"
#
# SNMP V3 NOTIFY FILTER CONFIGURATION
#
# SNMP V3 MIB VIEW CONFIGURATION
#
# SNMP V3 GROUP CONFIGURATION
#
snmp-server group "snmpuser" "" auth-priv notify-view root
#
# SNMP V3 TARGET ADDRESS CONFIGURATION
#
snmp-server host 10.9.203.5 v3 authPriv snmpuser inform
#
# DDI CONFIGURATION
#
# SLOT CONFIGURATION
#
# MAC AGING CONFIGURATION
#
# SMTP CONFIGURATION
#
# WEB CONFIGURATION
#
web-server enable
no web-server secure-only
#
# GLOBAL FDB FILTER CONFIGURATION
#
# QOS CONFIGURATION - PHASE I
#
# LACP CONFIGURATION
#
# VRF CONFIGURATION
#
# MAINTENANCE-DOMAIN CONFIGURATION
#
# MAINTENANCE-ASSOCIATION CONFIGURATION
#
# MAINTENANCE-ENDPOINT CONFIGURATION
#
# POE GLOBAL CONFIGURATION
#
# PORT CHANNELIZE CONFIGURATION
#

```

```
# PORT CONFIGURATION - PHASE I
#
# ISIS SPBM CONFIGURATION
#
router isis
exit
#
# SPB-PIM-GW CONFIGURATION
#
# MLT CONFIGURATION
#
# IP PREFIX LIST CONFIGURATION - GlobalRouter
#
# IP PREFIX LIST CONFIGURATION - VRF
#
# IPv6 PREFIX LIST CONFIGURATION - GlobalRouter
#
# IPv6 PREFIX LIST CONFIGURATION - VRF
#
# RMON CONFIGURATION
#
# VLAN CONFIGURATION
#
vlan members remove 1 1/1-1/48 portmember
vlan create 4048 name "onboarding-vlan" type pvlan-mstprstp 0 secondary 4049 vlan i-sid
4048 15999999
vlan create 4051 type spbm-bvlan
vlan create 4052 type spbm-bvlan
#
# MSTP CONFIGURATION
#
# NLS CONFIGURATION
#
mgmt oob
exit
mgmt clip vrf GlobalRouter
ip address 10.9.193.133/32
enable
exit
mgmt vlan 4048
mac-offset 0
ip route 0.0.0.0/0 next-hop 10.9.192.1 weight 200
enable
exit

#
# FHS CONFIGURATION
#
# MAC ACL CONFIGURATION
#
# IPv6 FHS ACL CONFIGURATION
#
# RA-GUARD CONFIGURATION
#
# DHCP-GUARD CONFIGURATION
#
# FHS SNOOPING CONFIGURATION
#
# SFLOW CONFIGURATION
#
# DHCP SNOOPING CONFIGURATION
#
# DHCP SNOOPING BINDING CONFIGURATION #
# VIRTUAL IST CONFIGURATION
```

```
#
# MLT INTERFACE CONFIGURATION
#
# DVR CONFIGURATION
#
dvr leaf 1
#
# PORT CONFIGURATION - PHASE II
#
interface GigabitEthernet 1/1
auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/2
auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/3
auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/4
auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/5
auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/6 default-vlan-id 0
auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/7
auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/8
auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/9
auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/10 auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/11 auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/12 auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/13 auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/14 auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/15 auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/16 auto-sense enable
```

```
no shutdown
exit
interface GigabitEthernet 1/17 auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/18 auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/19 auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/20
auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/21 default-vlan-id 0
auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/22 default-vlan-id 0
auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/23 default-vlan-id 0
auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/24 auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/25 auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/26 auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/27 auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/28 auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/29 auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/30 auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/31 auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/32 auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/33 auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/34 auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/35 auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/36 auto-sense enable
```

```
no shutdown
exit
interface GigabitEthernet 1/37 auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/38 auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/39 auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/40 auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/41 auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/42 auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/43 auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/44 auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/45
auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/46
auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/47
auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/48
auto-sense enable
no shutdown
exit
#
# LINK-STATE TRACKING
#
# IP CONFIGURATION
#
# IP AS LIST CONFIGURATION - GlobalRouter
#
# IP AS LIST CONFIGURATION - VRF
#
# IP COMMUNITY LIST CONFIGURATION - GlobalRouter
#
# IP COMMUNITY LIST CONFIGURATION - VRF
#
# IP EXTENDED COMMUNITY LIST CONFIGURATION - GlobalRouter
#
# IP EXTENDED COMMUNITY LIST CONFIGURATION - VRF
#
# IP ROUTE MAP CONFIGURATION - GlobalRouter
#
# IP ROUTE MAP CONFIGURATION - VRF
#
# IP CONFIGURATION - GlobalRouter
```



```
#
# IP CONFIGURATION - VRF
#
# BFD CONFIGURATION - GlobalRouter
#
# BFD CONFIGURATION - VRF
#
# CIRCUITLESS IP INTERFACE CONFIGURATION - GlobalRouter
#
# CIRCUITLESS IP INTERFACE CONFIGURATION - VRF
#
# TOPOLOGY-CLIP-IP
#
# MSDP CONFIGURATION - GlobalRouter
#
# VRRP CONFIGURATION - GlobalRouter
#
# VRRP CONFIGURATION - VRF
#
# UDP FORWARDING CONFIGURATION - GlobalRouter
#
# UDP FORWARDING CONFIGURATION - VRF
#
# UDP FORWARDING VLAN CONFIGURATION
#
# DHCP CONFIGURATION - GlobalRouter
#
# DHCP CONFIGURATION - VRF
#
# RIP CONFIGURATION - GlobalRouter
#
# RIP CONFIGURATION - VRF
#
# RIP VLAN CONFIGURATION
#
# IGMP CONFIGURATION - GlobalRouter
#
# IGMP CONFIGURATION - VRF
#
# MROUTE CONFIGURATION
#
# MCAST RESOURCE USAGE CONFIGURATION
#
# MCAST RESOURCE USAGE CONFIGURATION
#
# TIMED PRUNE CONFIGURATION - GlobalRouter
#
# TIMED PRUNE CONFIGURATION - VRF
#
# IPFIX CONFIGURATION
#
# RSMLT CONFIGURATION
#
# MLD CONFIGURATION - GlobalRouter
#
# MROUTE6 CONFIGURATION
#
# ISIS CONFIGURATION
#
router isis
sys-name "VSP-edge1"
is-type ll
exit
router isis enable
```

```
#
# LOGICAL ISIS CONFIGURATION
#
# VLAN NODAL MEP/MIP CONFIGURATION
#
# QOS CONFIGURATION - PHASE II
#
qos queue-profile 1 member add 1/1-1/48
#
# CFM CONFIGURATION - PHASE II
#
cfm spbm enable
#
# DIAG CONFIGURATION
#
# NTP CONFIGURATION
#
no ntp
ntp server 10.9.255.155
#
# ES CONFIGURATION
#
# OSPF CONFIGURATION - GlobalRouter
#
# OSPF CONFIGURATION - VRF
#
# OSPF ACCEPT CONFIGURATION - GlobalRouter
#
# OSPF ACCEPT CONFIGURATION - VRF
#
# BGP CONFIGURATION - GlobalRouter
#
# BGP CONFIGURATION - VRF
#
# ISIS SPBM IPVPN CONFIGURATION
#
# IP ISID LIST CONFIGURATION - GlobalRouter
#
# IP ISID LIST CONFIGURATION - VRF
#
# ISIS ACCEPT CONFIGURATION - GlobalRouter
#
# ISIS ACCEPT CONFIGURATION - VRF
#
# ISIS IPv6 ACCEPT CONFIGURATION - GlobalRouter
#
# ISIS IPv6 ACCEPT CONFIGURATION - VRF
#
# IP REDISTRIBUTION CONFIGURATION - GlobalRouter
#
router isis
exit
#
# IP REDISTRIBUTION CONFIGURATION - VRF
#
# OSPF VLAN CONFIGURATION
#
# OSPF PORT CONFIGURATION
#
# OSPF LOOPBACK CONFIGURATION
#
# RIP PORT CONFIGURATION
#
# IPVPN CONFIGURATION
```

```
#
# SLPP CONFIGURATION
#
# FILTER CONFIGURATION
#
# APPLICATION TELEMETRY CONFIGURATION
#
# IPV6 TUNNEL CONFIGURATION
#
# IPV6 OSPFV3 CONFIGURATION - GlobalRouter
#
# IPV6 RIPng CONFIGURATION
#
# IPV6 MGMT INTERFACE CONFIGURATION
#
# IPV6 STATIC ROUTE CONFIGURATION - GlobalRouter
#
# IPV6 MGMT INTERFACE CONFIGURATION
#
# IPV6 OSPF VLAN CONFIGURATION
#
# IPV6 OSPF PORT CONFIGURATION
#
# IPV6 RIP VLAN CONFIGURATION
#
# IPV6 RIP PORT CONFIGURATION
#
# IPV6 VRRP VLAN CONFIGURATION
#
# IPV6 VRRP PORT CONFIGURATION
#
# I-SID NAME CONFIGURATION
#
i-sid name 2100195 "Auto-sense Voice"
i-sid name 2100196 "Auto-sense Data"
i-sid name 15999999 "Onboarding I-SID"
#
# I-SID CONFIGURATION
#
# GLOBAL AUTO-SENSE CONFIGURATION
#
auto-sense voice i-sid 2100195 c-vid 195 auto-sense data i-sid 2100196
auto-sense onboarding i-sid 15999999
#
# VNID CONFIGURATION
#
# RADIUS CONFIGURATION
#
# TACACS CONFIGURATION
#
# LLDP CONFIGURATION
#
# EAP CONFIGURATION
#
# MACSEC CONFIGURATION
#
# GLOBAL MACSec CA Configured
#
# FABRIC ATTACH CONFIGURATION
#
# ENDPOINT TRACKING CONFIGURATION
#
# SPB-PIM-GW CONFIGURATION
#
```

```

# SOFTWARE CONFIGURATION
#
# APPLICATION CONFIGURATION
#
# IPSEC CONFIGURATION
#
# IPSEC POLICY TABLE CONFIGURATION
#
# IPSEC SA TABLE CONFIGURATION
#
# IPSEC SA POLICY LINK TABLE CONFIGURATION
#
# IPV6 OSPFV3 IPSEC CONFIGURATION
#
# IPV6 IPSEC INTERFACE CONFIGURATION
#
# IP IPSEC INTERFACE CONFIGURATION
#
# IKE CONFIGURATION
#
# SYSTEM CONFIGURATION Phase 2
#
end
#
# IP REDISTRIBUTE APPLY CONFIGURATIONS
#
# IP ECMP APPLY CONFIGURATIONS

```

VSP -edge2

```

#
# Thu Aug 26 03:01:28 2021 EDT
# box type : 5520-24W-VOSS
# software version : 8.4.0.0
# cli mode : ECLI #
#Card Info :
# Slot 1 :
#
# CardType : 5520-24W-VOSS
# CardDescription : 5520-24W-VOSS
# CardSerial# : SB032050G-00102
# CardPart# : 800992-00-AB
# CardAssemblyDate : 20201215
# CardHWRevision : AB
# CardHWConfig :
# AdminStatus : up
# OperStatus : up
#
#!end
#
config terminal
#
# BOOT CONFIGURATION
#
boot config flags dvr-leaf-mode
boot config flags ftpd
boot config flags sshd
boot config flags telnetd
#boot config sio console baud 115200 1
# end boot flags
#
# SPBM CONFIGURATION
#
spbm

```

```
spbm ethertype 0x8100
#
# CLI CONFIGURATION
#
prompt "VSP-edge2"
password password-history 3
#
# CLOCK TIME-ZONE CONFIGURATION
#
clock time-zone US Eastern
#
# SYSTEM CONFIGURATION
#
ip domain-name "FabricEdge.NH.CTC.Local"
ip name-server primary 10.9.255.130
ip name-server secondary 10.9.255.131
syslog host 1
syslog host 1 address 10.9.203.5
syslog host 1 enable
#
# LOG CONFIGURATION
#
# LINK-FLAP-DETECT CONFIGURATION
#
# IEEE VLAN AGING CONFIGURATION
#
# ACCESS-POLICY CONFIGURATION
#
# SSH CONFIGURATION
#
ssh
#
# MCAST SOFTWARE FORWARDING CONFIGURATION
#
# SNMP V3 GLOBAL CONFIGURATION
#
# SNMP V3 GROUP MEMBERSHIP CONFIGURATION
#
snmp-server user admin group "initial"
snmp-server user snmpuser group "snmpuser"
snmp-server user snmpuser group "snmpuser"
#
# SNMP V3 NOTIFY FILTER CONFIGURATION
#
# SNMP V3 MIB VIEW CONFIGURATION
#
# SNMP V3 GROUP CONFIGURATION
#
snmp-server group "snmpuser" "" auth-priv notify-view root
#
# SNMP V3 TARGET ADDRESS CONFIGURATION
#
snmp-server host 10.9.203.5 v3 authPriv snmpuser inform
#
# DDI CONFIGURATION
#
# SLOT CONFIGURATION
#
# MAC AGING CONFIGURATION
#
# SMTP CONFIGURATION
#
# WEB CONFIGURATION
#
```

```

web-server enable
no web-server secure-only

#
# GLOBAL FDB FILTER CONFIGURATION
#
# QOS CONFIGURATION - PHASE I
#
# LACP CONFIGURATION
#
# VRF CONFIGURATION
#
# MAINTENANCE-DOMAIN CONFIGURATION
#
# MAINTENANCE-ASSOCIATION CONFIGURATION
#
# MAINTENANCE-ENDPOINT CONFIGURATION
#
# POE GLOBAL CONFIGURATION
#
# PORT CHANNELIZE CONFIGURATION
#
# PORT CONFIGURATION - PHASE I
#
# ISIS SPBM CONFIGURATION
#
router isis
exit
#
# SPB-PIM-GW CONFIGURATION
#
# MLT CONFIGURATION
#
# IP PREFIX LIST CONFIGURATION - GlobalRouter
#
# IP PREFIX LIST CONFIGURATION - VRF
#
# IPv6 PREFIX LIST CONFIGURATION - GlobalRouter
#
# IPv6 PREFIX LIST CONFIGURATION - VRF
#
# RMON CONFIGURATION
#
# VLAN CONFIGURATION
#
vlan members remove 1 1/1-1/24 portmember
vlan create 4048 name "onboarding-vlan" type pvlan-mstprstp 0 secondary 4049 vlan i-sid
4048 15999999
vlan create 4051 type spbm-bvlan
vlan create 4052 type spbm-bvlan
#
# MSTP CONFIGURATION
#
# NLS CONFIGURATION
#
mgmt oob
exit
mgmt clip vrf GlobalRouter
ip address 10.9.193.134/32
enable
exit
mgmt vlan 4048
mac-offset 0
ip route 0.0.0.0/0 next-hop 10.9.192.1 weight 200

```

```
enable
exit
#
# FHS CONFIGURATION
#
# MAC ACL CONFIGURATION
#
# IPv6 FHS ACL CONFIGURATION
#
# RA-GUARD CONFIGURATION
#
# DHCP-GUARD CONFIGURATION
#
# FHS SNOOPING CONFIGURATION
#
# SFLOW CONFIGURATION
#
# DHCP SNOOPING CONFIGURATION
#
# DHCP SNOOPING BINDING CONFIGURATION
#
# VIRTUAL IST CONFIGURATION
#
# MLT INTERFACE CONFIGURATION
#
# DVR CONFIGURATION
#
dvr leaf 1
#
# PORT CONFIGURATION - PHASE II
#
interface GigabitEthernet 1/1
auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/2
auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/3
auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/4
auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/5
auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/6
default-vlan-id 0
auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/7
auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/8
auto-sense enable
no shutdown
exit
```

```
interface GigabitEthernet 1/9
auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/10
auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/11
auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/12
auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/13
auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/14
auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/15
auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/16
auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/17
auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/18
auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/19
auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/20
auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/21
default-vlan-id 0
auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/22
default-vlan-id 0
auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/23
auto-sense enable
no shutdown
exit
interface GigabitEthernet 1/24
default-vlan-id 0
```



```
auto-sense enable
no shutdown
exit
#
# LINK-STATE TRACKING
#
# IP CONFIGURATION
#
# IP AS LIST CONFIGURATION - GlobalRouter
#
# IP AS LIST CONFIGURATION - VRF
#
# IP COMMUNITY LIST CONFIGURATION - GlobalRouter
#
# IP COMMUNITY LIST CONFIGURATION - VRF
#
# IP EXTENDED COMMUNITY LIST CONFIGURATION - GlobalRouter
#
# IP EXTENDED COMMUNITY LIST CONFIGURATION - VRF
#
# IP ROUTE MAP CONFIGURATION - GlobalRouter
#
# IP ROUTE MAP CONFIGURATION - VRF
#
# IP CONFIGURATION - GlobalRouter
#
# IP CONFIGURATION - VRF
#
# BFD CONFIGURATION - GlobalRouter
#
# BFD CONFIGURATION - VRF
#
# CIRCUITLESS IP INTERFACE CONFIGURATION - GlobalRouter
#
# CIRCUITLESS IP INTERFACE CONFIGURATION - VRF
#
# TOPOLOGY-CLIP-IP
#
# MSDP CONFIGURATION - GlobalRouter
#
# VRRP CONFIGURATION - GlobalRouter
#
# VRRP CONFIGURATION - VRF
#
# UDP FORWARDING CONFIGURATION - GlobalRouter
#
# UDP FORWARDING CONFIGURATION - VRF
#
# UDP FORWARDING VLAN CONFIGURATION
#
# DHCP CONFIGURATION - GlobalRouter
#
# DHCP CONFIGURATION - VRF
#
# RIP CONFIGURATION - GlobalRouter
#
# RIP CONFIGURATION - VRF
#
# RIP VLAN CONFIGURATION
#
# IGMP CONFIGURATION - GlobalRouter
#
# IGMP CONFIGURATION - VRF
#
```

```
# MROUTE CONFIGURATION
#
# MCAST RESOURCE USAGE CONFIGURATION
#
# MCAST RESOURCE USAGE CONFIGURATION
#
# TIMED PRUNE CONFIGURATION - GlobalRouter
#
# TIMED PRUNE CONFIGURATION - VRF
#
# IPFIX CONFIGURATION
#
# RSMLT CONFIGURATION
#
# MLD CONFIGURATION - GlobalRouter
#
# MROUTE6 CONFIGURATION
#
# ISIS CONFIGURATION
#
router isis
sys-name "VSP-edge2"
is-type ll
exit
router isis enable
#
# LOGICAL ISIS CONFIGURATION
#
# VLAN NODAL MEP/MIP CONFIGURATION
#
# QOS CONFIGURATION - PHASE II
#
qos queue-profile 1 member add 1/1-1/24
#
# CFM CONFIGURATION - PHASE II
#
cfm spbm enable
#
# DIAG CONFIGURATION
#
# NTP CONFIGURATION
#
no ntp
ntp server 10.9.255.155
#
# ES CONFIGURATION
#
# OSPF CONFIGURATION - GlobalRouter
#
# OSPF CONFIGURATION - VRF
#
# OSPF ACCEPT CONFIGURATION - GlobalRouter
#
# OSPF ACCEPT CONFIGURATION - VRF
#
# BGP CONFIGURATION - GlobalRouter
# BGP CONFIGURATION - VRF
#
# ISIS SPBM IPVPN CONFIGURATION
#
# IP ISID LIST CONFIGURATION - GlobalRouter
#
# IP ISID LIST CONFIGURATION - VRF
#
```

```

# ISIS ACCEPT CONFIGURATION - GlobalRouter
#
# ISIS ACCEPT CONFIGURATION - VRF
#
# ISIS IPv6 ACCEPT CONFIGURATION - GlobalRouter
#
# ISIS IPv6 ACCEPT CONFIGURATION - VRF
#
# IP REDISTRIBUTION CONFIGURATION - GlobalRouter
#
router isis
exit
#
# IP REDISTRIBUTION CONFIGURATION - VRF
#
# OSPF VLAN CONFIGURATION
#
# OSPF PORT CONFIGURATION
#
# OSPF LOOPBACK CONFIGURATION
#
# RIP PORT CONFIGURATION
#
# IPVPN CONFIGURATION
#
# SLPP CONFIGURATION
#
# FILTER CONFIGURATION
#
# APPLICATION TELEMETRY CONFIGURATION
#
# IPV6 TUNNEL CONFIGURATION
#
# IPV6 OSPFV3 CONFIGURATION - GlobalRouter
#
# IPV6 RIPng CONFIGURATION
#
# IPV6 MGMT INTERFACE CONFIGURATION
#
# IPV6 STATIC ROUTE CONFIGURATION - GlobalRouter
#
# IPV6 MGMT INTERFACE CONFIGURATION
#
# IPV6 OSPF VLAN CONFIGURATION
#
# IPV6 OSPF PORT CONFIGURATION
#
# IPV6 RIP VLAN CONFIGURATION
#
# IPV6 RIP PORT CONFIGURATION
#
# IPV6 VRRP VLAN CONFIGURATION
#
# IPV6 VRRP PORT CONFIGURATION
#
# I-SID NAME CONFIGURATION
#
i-sid name 2100195 "Auto-sense Voice"
i-sid name 2100196 "Auto-sense Data"
i-sid name 15999999 "Onboarding I-SID"
#
# I-SID CONFIGURATION
#
# GLOBAL AUTO-SENSE CONFIGURATION

```

```
#
auto-sense voice i-sid 2100195 c-vid 195
auto-sense data i-sid 2100196
auto-sense onboarding i-sid 15999999
#
# VNID CONFIGURATION
#
# RADIUS CONFIGURATION
#
# TACACS CONFIGURATION
#
# LLDP CONFIGURATION
#
# EAP CONFIGURATION
#
# MACSEC CONFIGURATION
#
# GLOBAL MACSec CA Configured
#
# FABRIC ATTACH CONFIGURATION
#
# ENDPOINT TRACKING CONFIGURATION
#
# SPB-PIM-GW CONFIGURATION
#
# SOFTWARE CONFIGURATION
#
# APPLICATION CONFIGURATION
#
# IPSEC CONFIGURATION
#
# IPSEC POLICY TABLE CONFIGURATION
#
# IPSEC SA TABLE CONFIGURATION
#
# IPSEC SA POLICY LINK TABLE CONFIGURATION
#
# IPV6 OSPFV3 IPSEC CONFIGURATION
#
# IPV6 IPSEC INTERFACE CONFIGURATION
#
# IP IPSEC INTERFACE CONFIGURATION
#
# IKE CONFIGURATION
#
# SYSTEM CONFIGURATION Phase 2
#
end
#
# IP REDISTRIBUTE APPLY CONFIGURATIONS
#
# IP ECMP APPLY CONFIGURATIONS
```