

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



Copyright © 2024 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
Preexisting Configuration Review	12
XIQ-SE Preexisting Configuration Review	12
XIQ-SE: Script and Workflow Review	23
XIQ-C pre-existing configuration review	24
Prepare VSP/Fabric Engine Core Switches for Fabric Edge Deployment	26
	0
Site Selection for VSP Core Switches	
Apply DVR Controller, VLAN, and IP Config	28
Apply Seed Config for Zero Touch Fabric	
Prepare XIQ-SE for VSP/Fabric Engine Edge Deployment	
ZTP+ Configuration	
Configuration of Site Actions	35
XIQ-SE Workflow Configuration for VSP Onboarding	
Universal Edge Switch OS Conversion Using XIO	
Upload the Fabric Engine Image to XIQ-SE and Set the Reference Image	
	0
Switch Installation and Power Up	47
Observe Progress Using the VSP Edge Console	47
Monitor XIQ-SE Onboarding Workflow Execution	50
Migrate VSP Edge to Dedicated Switch Management CLIP	
Verify All End Devices Are Operational	58
Inspect the VSP Fabric	
Inspect the Auto Sansa Darts on the VSD Edge Switches	60
Inspect the Auto-sense Ports on the VSP Lage switches	
Verify the WLAN AP Is Operational	

Verify Client PC Authentication	55
---------------------------------	----



## 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*.

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

#### Table 1: Notes and warnings

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> .
<b>Key</b> names	Key names are written in boldface, for example <b>Ctrl</b> or <b>Esc</b> . If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press <b>Ctrl+Alt+Del</b>
Words in italicized type	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 2: Text

#### Table 3: Command syntax

Convention	Description
bold text	Bold text indicates command names, keywords, and command options.
<i>italic</i> text	Italic text indicates variable content.
[]	Syntax components displayed within square brackets are optional.
	Default responses to system prompts are enclosed in square brackets.
{ <b>x</b>   <b>y</b>   <b>z</b> }	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
х у	A vertical bar separates mutually exclusive elements.
< >	Nonprinting characters, such as passwords, are enclosed in angle brackets.
	Repeat the previous element, for example, member[member].
\	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 deploy a VSP switch running VSP Operating System Software (VOSS) 8.10.1.0 or later using a combination of VOSS fabric automation features and ExtremeCloud<sup>™</sup> IQ - Site Engine (XIQ-SE) / Network Access Control (NAC) onboarding automation.

## Prerequisites

- An existing Fabric Connect core switch running Fabric Engine 8.10.0.0 or later
- A universal hardware switch running Switch Engine firmware
- ExtremeCloud IQ Site Engine (XIQ-SE) and Extreme Control version 23.4.12.3 or later
- A DHCP/DNS server reachable on the existing Fabric Connect network

### Objectives

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

- XIQ-SE preparation for a successful Fabric Engine switch automated, zero-touch deployment
- Fabric Engine ZTP+ provisioning automation

- Universal Hardware switch OS conversion from EXOS/Switch Engine to VOSS/Fabric Engine using XIQ-SE
- VSP Zero Touch Fabric and port auto-sense functionality

#### Mote

- As of VOSS 8.6, the OS running on Universal Hardware switches has been re-branded to Fabric Engine and the switch is no longer referred to as a VSP switch, but as a Fabric Engine switch. This change only applies to Universal Hardware, and Non-Universal Hardware running VOSS (VSP4900) are still referred to as VSP switches.
- Likewise, Universal Hardware running EXOS 31.6 or later has been re-branded to Switch Engine in place of EXOS.
- Throughout this guide the name VSP Edge and Fabric Engine Edge are used interchangeably.

## Network Diagram

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

- Two VSP/Fabric Engine core/distribution running VOSS 8.10.0.0 or later, which an existing customer fabric connect deployment.
- Two Universal Edge 5520 Fabric Engine switches.



#### Note

Any VSP/Fabric Engine switch works as an edge switch as long as it supports VOSS 8.10.0.0 or later.

- One IP phone; Mitel 6920 model.
- One Extreme Wireless AP, model AP505i.
- One client VM acting as a wired client connected to the IP phone.
- One XIQ-SE instance running 23.4.12.3 or later software, and one Extreme Control NAC appliance running the same version.
- One XIQ-C VM appliance
- ExtremeCloud IQ (XIQ) user account for onboarding the Universal Edge switches.



It is assumed in this guide that the two VSP/Fabric Engine core switches have already been deployed and are part of an existing fabric network and are reachable by XIQ - SE. This guide focuses on describing the additional configuration necessary to successfully onboard the Fabric Engine 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 XIQ-SE ZTP+ and the Zero Touch Fabric functionality to achieve a typical VSP/Fabric Engine 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 Fabric Engine edge switches have no Out-of-Band (OOB) management connection. All management of the edge switches are via an inband IP address which is typical in campus Fabric edge switch deployments.



#### Note

DVR is not mandatory for fabric edge deployments. In this guide, DVR is enabled only on some access VLANs, and VRRP is enabled on other VLANs. This procedure is to illustrates the steps necessary to convert the fabric edge switch into DVR Leaf mode during the onboarding phase.

At the end of the deployment, all connected endpoints (IP phone, AP, PC client) must be operational without any manual configuration on the Fabric Engine switches, including the access ports.

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

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

The onboarding I-SID 15999999 is a special I-SID and must be unique across the fabric network. The onboarding I-SID is the default I-SID that a new VSP/Fabric Engine switch (with no configuration file) always uses when onboarding itself once it has joined the existing fabric.

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



## **Preexisting Configuration Review**

XIQ-SE Preexisting Configuration Review on page 12 XIQ-SE: Script and Workflow Review on page 23 XIQ-C pre-existing configuration review on page 24

The objective of this guide is to focus on the Fabric VSP Edge deployment and the steps required to achieve that. It is assumed that any unrelated XIQ-SE configuration has already been done. This topic explains what the customer needs to pre-configure on XIQ-SE.

## **XIQ-SE Preexisting Configuration Review**

ExtremeClo	ud IQ Site Engine					
Network 1	2 Dashboard Devices Discovered Firmware	Archives Config	uration Te	mplates Report	5	
🔔 Alarms & Events	Sites 👻 🗏	Devices World	Site S	ummary Endpo	int Locations FlexR	eports
Gontrol	Name	• Add Device	Exp	port to CSV 🔳		
Analytics	🕶 🔷 World	Device				
奈 Wireless	🔻 💠 Building1	Status	Status	Name 1	Site	IP Address
Lill Reports	Building1	0	٠	Fabric	/World	10.9.203.7
🧱 Tasks		•	٠	NAC	/World	10.9.203.6
Administration	Building2	0	٠	VSP-core1	/World	10.9.193.131
	Topology Definitions		٠	VSP-core2	/World	10.9.193.132
nt Connect	Service Definitions					

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

A map of the same name is defined for each site.

The VSP/Fabric Engine core switches are initially located under the world site.

Under **Administration**, the admin profile **Fabric Edge** is defined to manage the switches, as shown here:

A Network	2 Profiles Users Server II	nformation Certi	ficates Options	Device Types Back	up/Restore Diagnostics	Client API Access			
🔔 Alarms & Events	🗿 Add 🍃 Edt 🧔	Delete Defaul	It Profile: public_v1_I	Profile + Defau	It Access Control Engine Profile	t: snmp_v3_profile ~			
	Name	SNMP Version	Read Credential	Write Credential	Max Access Credential	Read Security Level	Write Security Level	Max Access Security Level	CLI Credential
Analytics	public_v2_Profile	SNMPv2	public_v2	public_v2	public_v2				Default
🗢 Wireless	EXTR_v2_Profile	SNMPv2	public_v2	private_v2	private_v2				Default
and Reports	snmp_v3_profile	SNMPv3	default_snmp_v3	default_snmp_v3	default_snmp_v3	AuthPriv	AuthPriv	AuthPriv	Default
📰 Tasks 📘	VOSS_v1_Profile	SNMPv1	public_v1	private_v1	private_v1				Default RWA
Main Administration	BOSS_ESM_v1_Profile	SNMPv1	public_v1	private_v1	private_v1				Default BOSS ESM
= Connect	BOSS_4800_v1_Profile	SNMPv1	public_v1	private_v1	private_v1				Default BOSS 48
	BOSS_vt_Profile	SNMPv1	public_v1	private_vt	private_v1				Default BOSS
	V055_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 3	SNMPv3	fabric_edge	fabric_edge	< No Access >	AuthPriv	AuthPriv	NoAuthNoPriv	FabricEdge

This admin profile uses the following SNMP credentials:

Edit SNMP Creder	ntial: fabric_edge		×
Credential Name:	fabric_edge		
SNMP Version:	SNMPv3		
User Name:	admin		
Authentication Type:	SHA		~
Authentication Password:	snmpauthcred		۲
Privacy Type:	AES		*
Privacy Password:	snmpprivcred		۲
		Save	Cancel

This admin profile uses the following CLI credentials:

Edit CLI Credential: F		×	
Description:	FabricEdge		
User Name:	admin		
Type:	SSH		*
Login Password:	password		۲
Enable Password:	password		۲
Configuration Password:	password		۲
		Save	Cancel

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

A Network	Dashboard Devices Discovered Firmware	Archives Configuration Templates Reports
🔔 Alarms & Events	Sites 👻 🗮	Fabric Connect Fabric Topology Summary
Control	Name	Fabric Infrastructure Settings
Analytics	🕶 💠 World	
🗢 Wireless	Building1	IS-IS Manual Area: 49.0000
land Reports	Building2	Primary BVLAN: 4051
Tasks	▼ 🚡 Topology Definitions	Secondary BYLANY: 4052
🐸 Administration	Fabric Connect 2	DvR Domain Settings
Z Connect	O Service Definitions	🔕 Add 🔯 Edit 🤤 Delete 🛛 🐾
		Name Domain ID
		Domain1 1
		Features
		✓ Multicast
		IP Shortcuts
		IPv6 Shortcuts

In XIQ-SE, select **Network > Topology Definitions**. The following **Fabric Connect Topology** settings are configured:

The same settings are assigned to both the Building1 and Building2 sites.



This guide assumes both VSP/Fabric Engine core nodes are already configured for Fabric Connect. When onboarding the Fabric edge switches, the **Onboard VSP** workflow automatically converts them to DVR Leaf nodes. However, for this to happen, the workflow must be able to read the DVR Domain ID from the site.

In XIQ-SE, select **Control** > **Access Control** > **Configuration** > **Rules**. The following rules are used to authenticate the AP, VoIP phone and PC client.

👍 Network	Dashboard Policy Access Control End	d-System	s Report				
Alarms & Events	Configuration 3 -	Rule	5				
Control	Configurations	0 4	85. D	Filt. 👩 Copy. 🙂 Delete	± Up ∓ Down   @ + Advance	d Locations	
Mayors	* Default		Enabled	Rule Name	Conditions	Profile	Actions
Wireless	Rules 4	0	*	Blacklist	End-System is in Stackling	Quarantine NAC Profile	Profile: <u>Quarantine NAC Profile</u> , Accept Policy: <u>Quarantine</u> , P.,.
Land Reports	AAA: Default	0	*	Assessment Warning	End-System is in <u>Assessment Warning</u>	Notification NAC Profile	Profile: Notification NAC Profile, Accept Policy: Notification
Tasks	Portal: Default AAA	•	1	Access Point	Authentication is MAC and User is in <u>FA Client APs</u>	Access Point NAC Profile	Profile: <u>Access Point NAC Profile</u> Accept Policy: <u>Access Point</u>
= Connect	Profiles	0		Server	End-System is in <u>Servers</u>	Server NAC Profile	Profile: Server NAC Profile, Accept Policy: Server
	<ul> <li>Captive Portals</li> </ul>	۰		Printer	End-System is in Printers	Printer NAC Profile	Profile: Printer NAC Profile, Accept Policy: Printer
	Notifications     Vendor RADIUS Attributes	-	1	VolP Phone	End-System is in <u>VolP Phones</u>	VolP.Phone.NAC.Profile	Profile: <u>ValP Phone NAC Profile</u> Accept Policy: <u>ValP Phone</u>
	<ul> <li>Global &amp; Engine Settings</li> </ul>	•	*	Administrator	Authentication is Management Login and User is in Local Administrators	Administrator, NAC Profile	Profile: <u>Administrator NAC Profile</u> Accept Policy: <u>Enterprise User (Edministrator</u> )
		-	1	Enterprise User	Authentication is MAC and End-System is in <u>Enterprise User Mac</u>	Alan,NAC.Profile	Profiler <u>Allow NAC Profile</u> Accept Policy: <u>Enterprise</u> User
		0	1	Default Catchall	catch-all rule	Refevit.NAC.Profile	Profile: Default NAC Profile. Reject Authentication Requests

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

The **VoIP Phone** rule is used to RADIUS authenticate the IP phone. The user can decide whether to use RADIUS to authenticate the IP phone or use LLDP bypass authentication, which is a feature of VOSS auto-sense.

The **Administrator** rule is only used to authenticate CLI and WEB (EDM) access on the switches if these RADIUS authentications are activated during the switch onboarding.

The **Enterprise User** rule is used to MAC authenticate the client VM. In a typical customer deployment, the Enterprise User rule uses an 802.1X authentication rule.

Under the Group Editor section, the following user groups are defined:

A Network	Dashboard Policy Access (	Control End-	-Systems Reports			
🜲 Alarms & Events	Configuration	+	User Groups			
Control 1	Group Editor 3	_	🗿 Add 🤰 Edit 📑 Copy 🥥 Delete	C Refresh	Import	
S Wireless	✓ All Groups		Name 🕇	Category	Туре	Used By
III Reports	Device Type Groups		Administrators	User Group	LDAP User Group	
🖹 Tasks	End-System Groups     Location Groups		FA Client APs	User Group	RADIUS User Group	Default
Administration	Time Groups		Local Administrators	User Group	Username	Default
럳 Connect	User Groups 4					

A Network Dashboard Policy Access Control End-Systems Reports 🔔 Alarms & Events Edit Group: FA Client APs Configuration G Control 1 Description: Optionally add a description Group Editor 3 Analytics All Groups S Wireless Device Type Groups Mode: Match Any
 O Match All III Reports End-System Groups Tasks 🔇 Add... 🛃 Edit... 🔣 Copy... 🤤 Delete Location Groups 警 Administration Time Groups Attribute Name Attribute Value Description ▼ User Groups 4 FA-Client-Type 6 wap-type1 Administrators Enterprise User FA Client APs

The **FA Client APs** group contains the following:

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

The **Administrators** user group holds only the admin user which is defined in the local password repository.

To set up the local password repository, right click the **Default** AAA group and set the mode to **Make Advanced**.



Set the **Authentication Method** to **Local Authentication**. This step is optional and is only used if the user configured cli and web radius authentication during the fabric edge switch onboarding.

di Network	Dashboard Policy Access Control Inc	s Systems Reports											
Alarms & Events	Configuration 3 -	Advanced AAA Configuration	n - Default										
Analytics	Configurations     Default	C Authenticate Requests Locally	for: 🗆 MAC (	ul) 🕑 MAC (PAP)	MAC (CH	P)	MISCHAP)	MAC (EAP-MD5)					
The Windess	Rules	Local Password Repository:	Default				*						
Line Reports	AAA: Default	join AD Domain:	Auto Detect				*						
Tasks	Portal: Default	Update Trusted Authorities	No information	avalable.									
Mainistration	* AAA	Authentication Bular											
n Connect	LDAP Configurations	Add_ I in.	O Deleter	a Up 🛛 🕈 Door									
	RADIUS Servers	Authentica User/MAC/ Type Match	- Location	Authentication Method	Primary RADIUS Server	Secondary RADIUS Server	ard RADIUS Server	4th RADIUS Server	inject Authentica Attrs	Inject Accounting Attrs	LDAP Configurati	LDAP Policy Mapping	Fall-through
	Captive Portals	Any *	Any	Local Authentication	None	None	None	None	None	None	None	Default	

Select **Control > Access Control > Group Editor > End-System Groups**. Edit the **VolP Phones** group with the MAC OUI of the phone vendor used in your network. This allows the phone to be MAC authenticated using the first three bytes of the MAC address. The example shown below, uses a Mitel phone OUI.

A Network	Dashboard Policy Access Control End	5-Systems Reports					
Alarms & Events	Configuration +	End-System Grou	ips				
Control	Group Editor 3 -	🗿 Add 🚺 Ed	it Copy 🕥 Delete	O Refresh	Import		
Se Wireless	✓ All Groups	Name 1		Category	Туре	Used By	Description
Las Reports	Device Type Groups	VolP Phones	5	End-System Group	MAC	Default	Default End-System Group for VolP Devices
	End-System Groups 4	Server			1117	A. C. 1	efault End-System Group for Servers.
145KS	Location Groups	Registr	o: VolP Phones			,	d-Systems awaiting permission to access the i
Marninistration	Time Groups	Registr			Description	Default End-System Group for VolP	d-Systems awaiting denied to access the netw
≓ Connect	User Groups	Registe				Devices	nd-Systems that have registered and been gran
		Printer					efault End-System Group for Printers.
			💭 Edt 🛐 Copy	To Nove_ O C	velete   Import.	. Export 📷 Add MAC OUIs	dd a MAC to this group to execute a remote wi
		Manag Value 1		Entry Type	Description	Custom 1	efault Endsystem Group for private-owned mo
		Manag Mitel Corpo	ration (00:08:5D)	MACOUI			e default group to move endsystems that wer
		Manag					efault Endsystem Group for business-owned m
		Fusion					dsystem Group to hold endsystems that awai
		Fusion					re default group to move endsystems to on re-
		Enterp					
		Domai					global CatchAll group used by the domain regi
		Blackle « <	Page 1 of 1 > >	🗧 🗌 🛄 Re	set	Displaying 1 - 1 of	1 nd-Systems denied access to the network
	Engines 🔮 🕈	Arrer Info., (	Close on Save			Save Cancel	vel.Currame that have according to service an

The Access Point, Enterprise User, and VoIP Phone rules contain the policy mappings shown below. The mappings are found in Control > Access Control > Policy Mappings > Default.

A Network	Dashboard Policy Access Control End	d-Systems Reports	
🔔 Alarms & Events	Configuration –	Default	
Control 1	Notification NAC Profile	Add      Edit     Delete Switch	n to Advanced C Refree
奈 Wireless	Printer NAC Profile	Access Point	Access Point
Land Reports	Quarantine NAC Profile	Administrator	Administrator
📑 Tasks	Registration Denied Access NAC Pro	Assessing	Assessing
🐸 Administration	Secure Guest Access NAC Profile	Deny Access	Deny Access
≓ Connect	Server NAC Profile	Enterprise Access	Enterprise Access
	Unregistered NAC Profile	Enterprise User	Enterprise User
	VoIP Phone NAC Profile	Enterprise User (Administrator)	Enterprise User
	Policy Mappings 3	Enterprise User (Read-Only Management)	Enterprise User
		Failsafe	Failsafe
	Captive Portals	Guest Access	Guest Access
	<ul> <li>Notifications</li> </ul>	Notification	Notification
	Vendor RADIUS Attributes	Printer	Printer
	< >	Quarantine	Quarantine
	Group Editor +	Server	Server
		Unregistered	Unregistered
	Engines 🚯 🕇	VolP Phone	VolP Phone

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

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



These Policy definitions, are cloned from the **Default Policy Domain** using the **Import/Export**, **Import from Domain** wizard shown below.

ExtremeClo	ud IQ Site Engine	
A Network	Dashboard Policy Access Contr	ol End-Systems Reports
Alarms & Events	📑 Open/Manage Domain(s) 🔻 🐻	Global Domain Settings 👻
Control	🔄 Open Domain 🕨	
Analytics	Lock Domain     Save Domain	- Show Editable
Lill Reports	Enforce Domain	Role / Service / Rule
Tasks Administration	Verify Domain     Assign Device(s) to Domain	<ul><li>Administrate</li><li>Assessing</li></ul>
<b>≓</b> Connect	Create Domain Delete Domain(s) Rename Domain	<ul> <li>Oeny Access</li> <li>Enterprise A</li> <li>Enterprise U</li> </ul>
	Import/Export	Import From Domain
	Database 🕨	Import From File
	VLANs	Export To File

Import From Domain × Domain: Default Policy Domain 1 -Data Elements to Import Roles Class of Service Port Level Role Mapping Status Services & Rules (Local) Adv CoS Config GVRP Status Service Groups Rate Limits 🕑 Do Not Use Global Rules Status C Devices VLANS ACL Mode Status Port Groups (User-Defined) S Network Resources HTTP Redirect Config Select All Deselect All WARNING: Importing Class of Service can affect the rate limits associated to existing CoS even if only appending the imported data. Before enforcing, inspect the Classes of Service for accurate/expected Rate Limits to confirm QoS that will be enforced to your network devices. Application of Imported Data Elements - Overwrite existing elements Cancel

All settings are imported from the **Default Policy Domain**.

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

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

A Network	Dashboard Policy Access C	ontrol End	-Systems Repor	ts				
🔔 Alarms & Events	Open/Manage Domain(s)	Global Do	omain Settings 👻	т.	ools 🔻			
Control	Domain: Building1							
Analytics	Domain. Domaing							
🗢 Wireless	Roles/Services	_	Role: Access F	Point				
I.III Reports	Roles		General VLA	N Egres	s Mappings	Port Default Usage		
Tasks	Access Point		Name:	(a) Acc	ess Point			
	Administrator			-	ess rome			
Sector Administration	Assessing		Description:	The /	Access Point role	is useful for B@AP topology.	When t	his role
<b>₽</b> Connect	Deny Access		TCI Overwrite:	Disab	led		¥	
	Enterprise Access		Default A	Actions	;			
	Eallsafe		have C	at at	C			
	Guest Access	-	Access Co	ontrol:	Contain to VLA	N	$\dashv$	<u> </u>
	Class of Service	+			VLAN:	194[AP-Mgmt]		*
	VIANC				Service ID:	2100194		
	VLAINS		AP Aware	8	Enabled			-
	Network Resources	+						
A Network	Dashboard Policy Access C	Control End	I-Systems Repor	rts				
🔔 Alarms & Events	Open/Manage Domain(s)	Global D	omain Settings 💌	IS T	ools 💌			
Gontrol	Democratics Devil-dimed							
Analytics	Domain: Building2							
🗢 Wireless	Roles/Services		Role: Access	Point				
Lud Reports	▼ @ Roles	<u> </u>	General VLA	N Egres	s Mappings	Port Default Usage		
	Access Point		Name		Delet			
	Administrator	- 1	ivarite.	ACI	Less Point			
Administration	Assessing		Description:	The	Access Point role	is useful for B@AP topology	When	this role
≓ Connect	Deny Access		TCI Overwrite:	Disab	led		*	
	Enterprise Access		Default /	Actions	s			
	Enterprise User							
	Cuest torong		Access C	ontrol:	Contain to VLA	N C		Ŧ
	Class of Service	+			VLAN:	194[AP-Mgmt]		-
	MAN-				Service ID:	2200194		
	VLANS	+	AP Aware	e:	Enabled			-
	Network Resources	+						

As shown below, the **VoIP Phone** policy role uses the same settings for both the Building1 and Building2 policy domains. Note, when RADIUS authenticating the phone, it is not necessary to provide the I-SID or VLAN values since these are signaled to the phone via LLDP and the auto-sense voice function.

A Network	Dashboard Policy Access Control End-Syst	tems Reports				
<ul> <li>Alarms &amp; Events</li> <li>Control</li> </ul>	Open/Manage Domain(s)   Global Domain Domain: Building1	n Settings 💌 📑	Tools	•		
Analytics	Roles/Services - Deny Access	Role: VoIP Pho	ne			
🖬 Reports	Enterprise Access     Enterprise User	General VLAN Name:	Seress Volf	Mappings Phone	Port Default Usage	
★ Administration ★ Connect	Failsafe     Guest Access     Notification	Description: TCI Overwrite:	IP tele	efony devices ed		*
	<ul> <li>Printer</li> <li>Quarantine</li> </ul>	Default Ac	tions	Permit Traffic		
	Server     Unregistered     Voll Phone			VLAN: Service ID:	Disabled N/A	~
		Class of Se	rvice:	A RTP/Voice/	Video (Priority: 6)	٣

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

A Network Dashboard Policy Access Control End-Systems Reports	
Alarms & Events	
Control	
Analytics	
Roles/Services Role: Enterprise User	
General VLAN Egress Mappings Port Default Usage	
Tasks O Administrator Name: O Enterprise User	
Administration Assessing Description: The Enterprise User role is essentially equivale	ent to the Enterprise
Connect O Deny Access TCI Overwrite: Disabled	¥
Enterprise Access	
Enterprise User     Default Actions	
Failsafe     Access Control:     Contain to VLAN	*
Class of Service + VLAN:	-
Service ID: 2100196	
Class of Service: A Network Control (Priority: 4)	•
Network Resources	
A Network Dashboard Policy Access Control End-Systems Reports	
Alarms & Events 📴 Open/Manage Domain(s) 👻 📑 Global Domain Settings 💌 📑 Tools 💌	
Control Domain: Building2	
Analytics Roles/Services Role: Enterprise User	
General VLAN Egress Mappings Port Default Usage	
Tasks O Administrator Name: O Enterprise User	
Administration Assessing Description: The Enterprise User role is essentially equivale	ent to the Enterpris
Connect Oreny Access TCI Overwrite: Disabled	*
Default Actions	
Enterprise User	
Failsafe     Access Control: Contain to VLAN	
Class of Service + VLAN:	
VLANS +	

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

Manage RADIUS Attribute Co	nfigurations	×
🛃 Add 🎲 Edit 📆 Cop	y 😂 Delete 🛛 😂 Refresh 🔹 Preview With Policy :	· ·
Name 🕇	Attributes	
Extreme NetLogin - VLAN ID	Extreme-Netlogin-Extended-Vlan=%VLAN_EGRESS%%VLAN_ID%,Extreme	e-Security-Profile=%PORT_P
Extreme NetLogin - VLAN Name	Extreme-Netlogin-Extended-Vlan=%VLAN_EGRESS%%VLAN_NAME%,Ext	reme-Security-Profile=%POR
Extreme Policy	Filter-Id=Enterasys:version=1:%MANAGEMENT%policy=%POLICY_NAME	%,Service-Type=%MGMT_SE
Extreme Policy - Fabric Attach	Filter-Id=Enterasys:version=1:%MANAGEMENT%policy=%POLICY_NAME	%,FA-VLAN-ISID=%VLAN_ID
Extreme VOSS	Tunnel-Private-Group-Id=%VLAN_ID%:%VLAN_TUNNEL_TAG%,Tunnel-Ty	/pe=13:%VLAN_TUNNEL_TA
Extreme VOSS - Fabric Attach	FA-VLAN-ISID=0:%CUSTOM1%,Passport-Access-Priority=%MGMT_SERV_	TYPE%
Extreme VOSS - Fabric Attach - EPT	FA-VLAN-ISID=%VLAN_ID%:0,FA-VLAN-ISID=%VLAN_ID%:%CUSTOM1%,P	assport-Access-Priority=%M
Extreme VOSS - Per-User ACL	Filter-Id=%POLICY_NAME%,Passport-Access-Priority=%MGMT_SERV_TYP	E%,%PER_USER_ACL_VOSS%
Extreme VOSS Per-User ACL	%PER_USER_ACL_VOSS%	
Extreme XNV - VLAN ID	Extreme-VM-VLAN-ID=%VLAN_ID%,Extreme-VM-VPP-Name=%PORT_PR	DFILE%,Extreme-VM-VR-Nam
		Close
	Kolio/ Domain: Dotault Policy Doma	in

To configure or view Radius templates, select **Control > Access Control > Engines > Switches**.

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



## XIQ-SE: Script and Workflow Review

This deployment guide uses the following workflows which are available on GitHub.

Name	Туре	GitHub URL
Onboard Mgmt VLAN	Script	https://github.com/extremenetworks/ ExtremeScripting/tree/master/XMC_XIQ-SE/ oneview_workflows
Onboard Mgmt CLIP	Workflow	https://github.com/extremenetworks/ ExtremeScripting/tree/master/XMC_XIQ-SE/ oneview_workflows

Onboard VSP	Workflow	https://github.com/extremenetworks/ ExtremeScripting/tree/master/XMC_XIQ-SE/ oneview_workflows
Change persona to VOSS	Workflow	https://github.com/extremenetworks/ ExtremeScripting/tree/master/XMC_XIQ-SE/ oneview_workflows
Change persona to EXOS	Workflow	https://github.com/extremenetworks/ ExtremeScripting/tree/master/XMC_XIQ-SE/ oneview_workflows

#### To import the workflows into XIQ-SE, select **Tasks** > **Workflows** > **Import**.

🚠 Network	Workflow Dashboard Schedul	ed Tasks Saved Tasks Scripts Workflows 2
Alarms & Events	User Workflows 🗕	No data to display
Analytics	Workflows     Create Group	
奈 Wireless	Create Workflow	
LIII Reports	Import	
📰 Tasks 📘		

#### Select the file followed by Import and then Close.

Select File				
Overwrite existing workflow Remo File Name  Override Workflow I (optional)	lame Size	Status	Information	
Onboard VSP-8.5.4.23v55.xwf	31 KB			

## XIQ-C pre-existing configuration review

As an example, XIQ-C has already been configured with one site as shown below

Ext	tremeCloud	IQ Controller									•	4 vest20 Small 10.05.01.0
De	eshboard	55				÷		SK -	145			0.7
8 M	onitor	*					ANA	Nº YA				
St	tes	2					AND THE					
							1251		and the second			
es	Search (search b	y site name or country)		Q Deact m	atch							
us	Name	Country	Roles	Network	is Switches	APs	Adoption Prima	ry Adoption Backup	Active APs	Non Active APs	Clients	Campus
		the second states of state										

#### With a single AP505.

Dashboard Monitor	2^										
Sites     Devices     Networks	Access	s Points <b>3</b> nes									
ExtremeCloud IG	Controller										Agadmin - ves120 Small 10.05.01.0025
Access Points											Auto Bafresh OFF +
Filter visible rows		9									т е а
Status Name	IP Address 5	lite	Version	Model	Radie 1	Radio 2	R1 Clients	R2 Clients	Radio 3	R3 Clients	=
<ul> <li>Edge-WAP</li> </ul>	10.9.194.101 F	Fabric Edge Sandbox	10.5.1.0-03	AP505i-FCC	Off	Off	0	0			

With the following VLAN and Fabric Attach configuration.

ExtremeCloud IQ Controller				Age admin - Ves120 Small 10.05.01.0025
Edge-WAP ● ☆ := IP Address MAC Address Serial Number 9 19/9/ 202000000			Tabric Edge 138	
Model AP305-FCC Software Version 10.5.16-031R Country United States Eth Power Status Normal Radios Channel Channel Width Mode Power Level O			đ	
1 Off Sinvax Off 2 Off anvacax Off				
DASHBOARD SETES NETWORKS ROLES VLANS	CLIENTS TROUBLESHOOTING SMART RF	CERTIFICATE EVENTS		
AP Tunnels				
IP Address Status	Configured MTU	Configured MTU Tunnel Status	Path MTU learned by AP Int	ernal Management Tunnel Status
10.9.203.25 Active	1500	Normal	No	renal
VLANS				
Name Mode Tagged	VLAN ID I-SID	Certificates	Remote VTEP VNE	Tunnel Status
Data Building1 Fabric Attach 🗸	196 2100196			

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

ExtremeCloud IQ Co	ntroller	
Name	Outar Buildingh	
Mode	Fabric Attach +	
WLAN ID	196	tagged
1-510	2100196	
	DWANCED	



## Prepare VSP/Fabric Engine Core Switches for Fabric Edge Deployment

Site Selection for VSP Core Switches on page 26 Apply DVR Controller, VLAN, and IP Config on page 28 Apply Seed Config for Zero Touch Fabric on page 30

## Site Selection for VSP Core Switches

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

To add both core switches to Building1, select **Network > Devices > World > Devices**. Highlight both core switches, right click and select **Configure**.

A Network	Dashboard Devices Discovered Firmware	Ard	hives	Configuration T	empla	tes Reports								
🌲 Alarms & Events	Sites 👻 🗏	0	Devices World Site Summary Endpoint Locations FlexReports											
Control	Name	0	Add Dev	ice_ 🗋 E	ports	scsv ≡								
Analytics	v world 3													
🗢 Wireless	A Building1     A		Status	Name 1		Site	IP Address	Poli Status	Poll Details	Device Type	Family	Firmware		
Labl Reports	Building2		•	Fabric		/World	10.9.203.7	Available: 1	Up: 4 Dow	FABRICMGR	Fabric Man	21.9.10.4		
📰 Tasks	<ul> <li>Topology Definitions</li> </ul>	Ŧ	•	NAC	5	/World	10.9.203.6	Available: 1	Up: 1 Dow	Virtual Access Cont	Extreme C	21.9.10.4		
Market Ma	Fabric Connect		•	VSP-core1		/World	10.9.193.131	Available: 1	Up: 1 Dow	VSP-4450GSX-PWR+	VSP Series	8.4.0.0		
Z Connect	Q: Service Definitions		•	VSP-core2	=	FlexView	10.9.193.132	Available: 1	Up: 1 Dow	VSP-4450GSX-PWR+	VSP Series	8.4.0.0		
						More Views 🕨								
		Ļ.			0	Configure_ 6								
					0	Compass Search								

Assign both switches to the World/Building1 site.

.onngure Device						*
evice ID	System Name	Device Nickname	Device Type	Poll Type	Site Precedence	Site
0.9.193.132	VSP-core2	VSP-core2	VSP-4450GSX-PW	SNMP		/World
).9.193.131	VSP-core1	VSP-core1	VSP-4450GSX-PW	SNMP		/World
1			-		-	
Device An	notation VRF Definitions	VLAN Definitions CLIP A	ddresses Topology	Services LAGS	Ports	
stem Name:		Default Site:	/World	~ 2		
ontact:	http://www.extremenetv	Poll Group:	/World	*		
			/World/Building1			
cation:		Poll Type:	/World/Building2	v		
ministration	Fabric Edge 🛛 👻	SNMP Timeout:	5	\$		
one.		SNMP Retries:	3			
placement Serial imber:						
move from Service:		Topology Layer:	L2 Access	*		
o Dofault MohView	-	Collection Mode:	Historical			
RL:		Collection Interval	15	ţ.		
ebView URL:	http://%IP	(minutes):				

#### In the confirmation pop-up, select Yes.

Impo	ort Site Configuration			×					
0	Do you want to import the site configuration?								
0	WARNING: The existing VLAN Definition, Ports, and ZTP+ Device Settings configuration will be overwritten.								
	1	Yes	No						

#### Then select **Save** to commit.

Now navigate to the Building1 site and make sure both core switches have been added.

Dathboard Devices Discovered Ferr	ware Archives C	ortiguistion Ten	plates Reports							
Stes + III	Devices	Devices Building! Site Summary Encodent Locations Revileponts								
Name	O Add Dev	. R 6-p)	etto Civ 🔳							
+ 🔷 Ward		CHARLE .				augeres.		1		
+ 🗘 Buildingt	Statut	Name I	<ul> <li>Sto</li> </ul>	IP Address	Poli Status	Pell Details	Device Type	Family	Fernivard	
<ul> <li>Ø Building2</li> </ul>		VSP-core1	/world/Building1	10.9.193.131	Available: 1.,	Up: 2 Dow	VSP-#450G5X-PWR+	VSP Series	E.4.0.0	
+ 📓 Topology Definitions		VSP-core2	Averid/Building1	10.9.193.132	Austable: 1_	Up! 2 Dom	15P-445003X-PWE+	VSP Series	8.4.0.0	

To add the core switches to the topology map, highlight both core switches, right-click and select **Add to Map**.

	Devices	Building1	Site	Summary Endpoint Lo	cations FlexRep	orts				
lame	O Add De	vice 🗋	Ехро	rt to CSV 🔳						
💠 World										
Suilding1	Status	Name 1		Site	IP Address Poll Status Poll Details Device 1		Device Type	Family	Firmware	
Building2		VSP-core1		AModd/Ruilding1	10.9.193.131	Available: 1	Up: 2 Dow	VSP-4450GSX-PWR+	VSP Series	8.4.0.0
Topology Definitions	•	VSP-core2		FlexView	10.9.193.132	Available: 1	Up: 2 Dow	VSP-4450GSX-PWR+	VSP Series	8.4.0.0
Fabric Connect			_	More views P						
Service Definitions			۰	Configure						
			0	Compass Search						
			C	Rediscover						
			12	Clear Alarms						
			1	Upgrade Firmware						
			0	Add to Device Group						
				Mara Articar h						
				More Actions P						
				Archives						
				Archives Tasks						
				Archives  Tasks  Maps	Add to Map					
				Archives > Tasks > Maps > Network >	Add to Map Create Map					

Select the Building] site map and then OK.

Add	to Map		×
Map:	/World/Building1/Building1		٣
		ОК	Cancel

Both core switches have now been added to the map.

Add to Map	Х
The devices were successfully added to /World/Building1/Building1	

## Apply DVR Controller, VLAN, and IP Config

The VSP/Fabric Engine core switches route IP traffic across a number of VLANs/L2VSNs. These VLANs do not exist on the VSP cores and must be created.

Because the VSP edge switches are 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. VRRP is used on the Switch-Mgmt and AP-Mgmt VLANs.



Note

The DVR controllers are configured in "isolated" mode, which means they will not redistribute host routes to the DVR backbone and possibly interefere with DVR routes in the Data Center. DVR-VRRP functionality is enabled for customer scenarios where VSP Edge switches are not deployed as DVR leaf nodes. SLPP is enabled on the VLANs and enabled globally. When the Fabric edge switches are onboarded, SLPP-Guard is enabled on all auto-sense access ports.

The VSP core configuration uses the CLI.

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

Building1	
VSP-core1	VSP-core2
enable config term dvr isolated controller 1	enable config term dvr isolated controller 1
<pre>vlan create 193 name "Switch-Mgmt" type port-mstprstp 0 vlan i-sid 103 2100193 i-sid name 2100193 "Building1-Switch-Mgmt" interface Vlan 193 ip address 10.9.193.2/25 ip vrrp version 3 ip vrrp address 193 10.9.193.1 ip vrrp 193 enable exit slpp vid 193</pre>	<pre>vlan create 193 name "Switch-Mgmt" type port-mstprstp 0 vlan i-sid 193 2100193 i-sid name 2100193 "Building1-Switch-Mgmt" interface Vlan 193     ip address 10.9.193.3/25     ip vrrp version 3     ip vrrp address 193 10.9.193.1     ip vrrp 193 enable exit slpp vid 193</pre>
<pre>vlan create 194 name "AP-Mgmt" type port-mstprstp 0 vlan i-sid 194 2100194 i-sid name 2100194 "Building1-AP-Mgmt" interface Vlan 194 ip address 10.9.194.2/24 ip vrrp version 3 ip vrrp address 194 10.9.194.1 ip vrrp 194 enable ip dhcp-relay fwd-path 10.9.255.130 ip dhcp-relay fwd-path 10.9.255.131 ip dhcp-relay fwd-path 10.9.255.131 ip dhcp-relay fwd-path 10.9.255.131 ip dhcp-relay fwd-path 10.9.255.131 ip dhcp-relay fwd-path 10.9.253.13 ip dhcp-relay fwd-path 10.9.253.131 ip dhcp-relay fwd-path 10.9.263.6 ip dhcp-relay fwd-path 10.9.203.6 exit slpp vid 194</pre>	<pre>vlan create 194 name "AP-Mgmt" type port-mstprstp 0 vlan i-sid 194 2100194 i-sid name 2100194 "Building1-AP-Mgmt" interface Vlan 194     ip address 10.9.194.3/24     ip vrrp version 3     ip vrrp address 194 10.9.194.1     ip vrrp 194 enable     ip dhcp-relay fwd-path 10.9.255.130     ip dhcp-relay fwd-path 10.9.255.131     ip dhcp-relay fwd-path 10.9.255.131     ip dhcp-relay fwd-path 10.9.255.131     ip dhcp-relay fwd-path 10.9.253.131     ip dhcp-relay fwd-path 10.9.253.131     ip dhcp-relay fwd-path 10.9.203.6     ip dhcp-relay fwd-path 10.9.203.6 enable exit slpp vid 194</pre>
<pre>vlan create 195 name "Voice" type port-mstprstp 0 vlan i-sid 195 2100195 i-sid name 2100195 "Building1-Voice" interface Vlan 195     dvr gw-ipv4 10.9.195.1     dvr enable     ip address 10.9.195.2/24     ip dhcp-relay fwd-path 10.9.255.130     ip dhcp-relay fwd-path 10.9.255.131 enable     ip dhcp-relay fwd-path 10.9.253.6     ip dhcp-relay fwd-path 10.9.283.6     ip dhcp-relay fwd-path 10.9.283.6     ip dhcp-relay fwd-path 10.9.283.6     ip dhcp-relay fwd-path 10.9.283.6     ip vid 195</pre>	<pre>vlan create 195 name "Voice" type port-mstprstp 0 vlan i-sid 195 2100195 i-sid name 2100195 "Building1-Voice" interface Vlan 195 dvr gw-ipv4 10.9.195.1 dvr enable ip address 10.9.195.3/24 ip dhcp-relay fwd-path 10.9.255.130 ip dhcp-relay fwd-path 10.9.255.131 ip dhcp-relay fwd-path 10.9.255.131 ip dhcp-relay fwd-path 10.9.255.131 ip dhcp-relay fwd-path 10.9.255.131 ip dhcp-relay fwd-path 10.9.203.6 ip dhcp-relay fwd-path 10.9.203.6 enable exit slpp vid 195</pre>
<pre>vlan create 196 name "Data" type port-mstprstp 0 vlan i-sid 196 2100196 i-sid name 2100196 "Building1-Data" interface Vlan 196 dvr gw-ipv4 10.9.196.1 dvr enable ip address 10.9.196.2/24 dvr vrrp-election ip dhcp-relay fwd-path 10.9.255.130 ip dhcp-relay fwd-path 10.9.255.131 enable ip dhcp-relay fwd-path 10.9.255.131 enable ip dhcp-relay fwd-path 10.9.253.131 enable ip dhcp-relay fwd-path 10.9.253.6 ip dhcp-relay fwd-path 10.9.283.6 ip dhc</pre>	<pre>vlan create 196 name "Data" type port-mstprstp 0 vlan i-sid 196 2100196 i-sid name 2100196 "Building1-Data" interface Vlan 196     dvr gw-ipv4 10.9.196.1     dvr enable     ip address 10.9.196.3/24     dvr vrrp-election     ip dhcp-relay     ip dhcp-relay fwd-path 10.9.255.130     ip dhcp-relay fwd-path 10.9.255.131     ip dhcp-relay fwd-path 10.9.263.6     ip dhcp-relay fwd-path 10.9.203.6     i</pre>

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

	( Jun	any a behav	teres (Inch.	end Minibula	policies and the second	Janua Port	Configuration.	<b>VLAN</b>	5.6. 10	informer Tablic Adult	- +10-L2V54	1204	what 51	Alleren 3
The second secon	VLAN Table	-												
1020 '2000' 2010 faite faite faite Size C1020 (2000 1900 faite faite Size 2.1020 with any	PADWL 1	instance	System Name	VLAN (D	yi,mina		10% c	1641 200	ut VLAN Spanning Tree MSTP (D	VLASI-SID Mapping	VLAN TIDE	ulan Color	Vriue Router	10.000
	1581881	£	VSP-cove1	£	Default		* 2014	40114	8	0	8,491			256-219
	15.81851	149	15P-cowt	162	3483-3	210	1.000	40.4	+	2100168	spirat			
VSP-core1 10.9.193.131	1681881-	194	VSP-core1	794	AP Mgm		+ 2014	10714		2100104	9yPert	0		
· Consentingent O Days 01-4850	+ 16.8.183.1.	195	viPoret	195	1000		* alter	attie	8	2100799	2/841			
404428453C00	16.818k1	196	VSP-caret	104	Data		* 10718	942119	1	2100156	NyPort			
8414	1681831-	451	VSP-ore1	4051	BVEAU-	6	a some	attie	43		spin-bolan			203
	1081951-	-4052	VSP-core1	4552	BYSAN		* 3054	30514	43	85	uproblan			368
Deriver Deen Dissert filmere en	Contention	n Templaten Improvi Perform	Naporta Device	By Harden	internation	Deute Part	(selgenere	95,480 I	55 147 1710	rlam fahruntar	1901249	5444	Veniel 10	Narry 3
Internal Referen Ratio (Expos 2500 (2000) 1000 Annothesis (Expose 1520 (2000) 2000 Anti-Antonitypes Ster (2520 (2000) 2000 (2000) Antonitypes Inter 25220 (2000) 2000 (2000) Anti- time 25220 (2000) 400 (2000)	Philippens 1	-90	Honixer	e le	ven Type	Res Status	Service Tratus	54	nine Max MAC Lines	Service MAC Limit Drubbe	Service Orga	1	Serv	ta Autor
	12.8.182.131	2106193	Buildingh	Sw. Qv	pit.	10.0	+ 47.4	÷			sortig		nore	
	104,101.131	2100104	BuildingS	AR. 04	04	104	* 40.4	÷			config		none	
	154183.331	2100195	Buildingh	va. De	ye .	4214	+ 42.4	1.1			xonte		none	
VSP-core1 10.9(193/131	154,161,131	2100106	autors	Data Dv		1014	1.000				unte		1004	
Contain Enderstand - Citings (2)-40.00     Provide 2012-2012     Contain Enderstand	15-8,193,131	18777001	(Ni-SD		• 1	101-4	* #25.4	1			ordg		none	

## Apply Seed Config for Zero Touch Fabric

In order for the VSP/Fabric Engine edge switches to join the fabric when they are connected to the fabric core nodes (core nodes), the following items must be configured in the core nodes.

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

The VSP/Fabric Engine core nodes (or any pair of core/distribution nodes) need to be set up as nickname servers. A best practice it to have two nickname servers per ISIS area. Both nickname servers can be set up to assign nicknames in the same prefix range or different ranges. The mechanism used by the nickname server to assign nicknames is essentially identical to how a DHCP server works, with the exception that nicknames are assigned instead of IP addresses.

To enable nickname server functionality on a VSP/Fabric Engine switch, it needs to be configured with a static nickname (the two core switches were already configured with a static nickname in a previous section).

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

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

b. The onboarding I-SID is created into a new dedicated IP subnet for which both core nodes act as the default gateway and DHCP-relay agent. The guide uses this option, as it is a best-practice design.

If the core nodes were originally built from VOSS 8.2 or later, the default onboarding Private-VLAN 4048 is already present. If the fabric cores were originally built from VOSS 8.3 or later, the default onboarding Private-VLAN 4048 is also already assigned to the onboarding I-SID 15999999 and the same I-SID is also already defined as the auto-sense onboarding I-SID. It will therefore be sufficient to simply add an IP address and DHCP relay config to the existing onboarding Private-VLAN 4048.

3. If the core nodes were not built from VOSS 8.3 defaults (for example. they were upgraded from a pre-VOSS 8.3 release) they also need to have auto-sense enabled on the interfaces connecting to the VSP edge.

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



#### Note

If the VSP cores configs were built from VOSS 8.3 defaults or later then only configure the nickname server on both VSP core.

Apply the following config on both core nodes:

VSP-core1	VSP-core2
<pre>enable config term interface gigabitEthernet 1/10 auto-sense enable no shutdown exit vlan create 4048 name "onboarding-vlan" type pvlan-mstprstp 0 secondary 4049 vlan 1-sid 4048 1599999 'onboarding I-SID' auto-sense onboarding 1-sid 1599999 'onboarding I-SID' auto-sense onboarding 1-sid 1599999 'onboarding I-SID' auto-sense onboarding 1-sid 15999999 interface Vlan 4048 ip address 10.9, 92.2/24 ip vrrp vddress 110.9, 192.1 ip vrrp 1 enable ip dhcp-relay fwd-path 10.9.255.130 ip dhcp-relay fwd-path 10.9.255.130 ip dhcp-relay fwd-path 10.9.255.131 ip dhcp-relay</pre>	<pre>enable config term interface gigabitEthernet 1/11 auto-sense enable no shutdown exit vlan create 4040 name "onboarding-vlan" type pvlan-mstprstp 0 secondary 4049 vlan 1-sid 4048 15090999 interface Vlan 4048 ip address 10.9.192.3/24 ip address 10.9.192.3/24 ip vrrp 1 enables 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 10.9.255.131 mode dhcp ip dhcp-relay fwd-path 10.9.</pre>

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

As a deployment option, set an auto-sense ISIS hello authentication key as shown below.





## Prepare XIQ-SE for VSP/Fabric Engine Edge Deployment

ZTP+ Configuration on page 32 XIQ-SE Workflow Configuration for VSP Onboarding on page 36

In a previous topic, the two fabric core switches were manually added to the Building1 XIQ-SE site. However, the Fabric Edge switches are automatically assigned to the Building1 site during the onboarding process.

### **ZTP+** Configuration

To automate the site assignment, in XIQ-SE select World > ZTP+ Device Defaults.

Set the **Site Assignment Precedence** drop-down to **LLDP Only** and then click **Save**. With this setting, XIQ-SE assigns the edge switches to a site based on the LLDP neighbor table found on the switches being onboarded. Because the VSP core switches are in Building1, the edge switches are assigned to this site.

ites 👻	=	Devices World Site Su	mmary Endpoint Locat	ions FlexReports				
world 1		Discover Actions VRF/	VLAN Topologies Se	rvices Port Templates	ZTP+ Device Defaults	3 Endpoint Locations Analytics	Custom Variables	
<ul> <li>Building1</li> <li>Building2</li> </ul>		Basic Management	Disabled *	Domain Name:		System Contact:		
Topology Definition:	6	Subnet Address:		DNS Server:		System Location:		
Fabric Connect		Starting IP Address:		DNS Server 2:		Admin Profile:	public_v2_Profile	*
Service Definitions		Ending IP Address:		DNS Server 3:		Poll Group:	Default	*
		Gateway Address:		DNS Search Suffix:		Poll Type:	SNMP	
		Management Interface:	Default	NTP Server:		Site Assignment Precedence:	LLDP Only	*
		CU Recovery Mode Only:	Enabled	NTP Server 2:				4

Confirm that the ZTP+ config for the Building1 site is correct before onboarding the edge switches into the site. Select **Building1** site under the **World** site. Click the **ZTP+ Device Defaults** tab.

Under Basic Management, set options as follows:

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

Discover Actions VRF/	VLAN Topologies Ser	vices Port Templates	ZTP+ Device Defaults En	dpoint Locations Analytic	s Custom Variables	i.
Basic Management						
Use Discovered:	IP and Managemen 💌	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	Ŧ
Gateway Address:		DNS Search Suffix:		Poll Type:	SNMP	~
Management Interface:	Default 👻	NTP Server:	10.9.255.155	Site Assignment	None	v

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

Scroll down the screen, in **Configuration/Upgrade**, leave **Configuration Updates** set to **Always** (this setting does not apply in SNMP Poll Type). Set **Firmware Upgrades** to **Always.** Because this guide is using the Universal Hardware edge switches, the switch image must be converted from Switch Engine to Fabric Engine. This conversion is addressed in a later topic of the guide.

Configuration/Upg	rade				
Configuration Updates:	Always	•	Firmware Upgrades:	Always	-
Update Date:	6/7/2024		Upgrade Date:	6/7/2024	
Update Time:	05:30 PM		Upgrade Time:	05:30 PM	-
Update UTC Offset:	UTC+01:00		Upgrade UTC Offset:	UTC+01:00	
			NOS Persona Change:	To Fabric Engine	•

Scroll down to the **Device Protocols** section and uncheck **MVRP**. The rest can be left as is, and MSTP must remain enabled. Note that the Telnet, HTTP, and HTTPS protocol options only work as of VOSS 8.4. All protocol options work with EXOS/Switch Engine and are applied when the Universal Edge switch is initially onboarded as Switch Engine.

Device	Protocols						
Telnet:	🕑 Enabled	HTTP:	🕑 Enabled	LACP:	Enabled	MSTP:	🕑 Enabled
SSH:	🕑 Enabled	HTTPS:	🕑 Enabled	LLDP:	🕑 Enabled	POE:	🕑 Enabled
SNMP:	S Enabled	FTP:	🕑 Enabled	MVRP:	Enabled	VXLAN:	Enabled

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

Disable MVRP because ZTP+ tries to apply the default port templates during switch onboarding. These default port templates are listed under the **Port Template** tab as shown below.

A Network	Dashboard Devices Discovered Fit	mware Archives	Configuration	Templates Reports									
Alarms & Events	Stes v ≡	Devices Bu	odings Site Sun	mary Endpoint Location	s FlexReports								
Control	Name	Duran A	State States	. Facilitation discussion	These Tempelaner TTTT: Co	in Party Res		And the Control					
Analytics	* 🔷 World	Lancolds .	unaria interiore	t raposges perios	Port reimpores	and Derabatic stra	grore coursers	respire como	in the sector				
💎 Wireless	+ 🔷 Building1	Port Templa	tes										
Las Reports	A Building2	O Add	ini 🔘 Oo	tis Local Only									
Tarks	Topology Definitions     Febric Connect	Source .	Configuration	PVID	Default Role	Span Guard	Loop Protect	MVRP	51,59	SLPP Guard	SLPP Guard Timer	PoE Enable	PoE Priority
Administration	Service Definitions	/World	AP.	Default [1]	None						60		LOW
E Connect		/World	Access	Default [1]	None						60		LOW
		Global	AutoSense	0	None	100		_			60		LOW
		/World	Interswitch	Default [1]	None			1			60		LOW
		World	Tol	Default [1]	None			1.1.1			60		LOW
		/World	Management	Default [1]	None						60		LOW
		/World	Other	Default [1]	None						60		LOW
		/World	Phone	Default [1]	None		*				60	1	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	1	LOW

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

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

To avoid these issues, XIQ-SE 21.9 introduced a new Global AutoSense port template which is automatically applied to VOSS/Fabric Engine Universal Hardware devices via a ZTP+ Automated Template entry:

Sites * 🗉	Devices	Building1 Site Sum	mary Endpoint Los	ations FlexReports								
Name	Discover	Actions VRF/VLAN	Topologies Ser	vices Port Templates ZTP+ Dev	ce Defaults Endpoint Location	Analytics (	Custom Variables					
• 💠 World												
A Buildingt	Port Ter	nplates										
Ø Building2	O Add	📴 Emi 🧿 Dele	- Local Only									1
Topology Definitions     Fabric Connect	Source	Configuration	PVID	Default Role	Authentication	VLAN Trunk	Tagged		Untagged		Fabric Enable	
Service Definitions	/World	Access	Default [1]	None	None				Default [1]		None	
	Global	AutoSense	0	None	None						Auto Sense	
	anna da a	And a set of the set	Ph. 2	Algues.	N++++				n.e. n.e.		A12.00	
	ZTP+ AL	itomated Templates				False						
	Device	Mappings					Po	rt Mappings				
	O Add	🛃 Edit 🥥 Delet	=   <b>^</b> ~				0	Add 🧾 Ea	It 🥥 Deleta	^ V		
	Priority	Name	Enabled	Family	Devices	IP Range	Prior	ity Templa	te	Ports		
	1	AutoSense VOSS	1	Universal Platform VOSS	Any Universal Platform VOSS			AutoSe	nse			
	2	AutoSense Fabric Engl	ne 🖌	Universal Platform Fabric Engine	Any Universal Platform Fabr							

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

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

Also note that default template entries exist for VOSS and Fabric Engine Universal Hardware switches. If you are onboarding a VSP4900 or other VSP switch model, then create a similar entry and set the family to **VSP Series**. Finally, enable SLPP-Guard on the auto-sense port template. Select **World > Port Templates** and double click on the **AutoSense Fabric Engine** template.

Network	Dashboard Devices Disc	overed Firms	rare Archives 0	Configuration Templates	Reports					
🌲 Alarms & Events	< Sites >	Devices	World Site Summa	ry Endpoint Locations	ResReports					
Gentrol	Name									
Analytics	👻 🔷 World	Discover	Actions VRF/VLAN	i Topologies Services	Port Templates 21P	Device Defaults Endpoint Locato	ons Analytics o	Custom Variables		
🗢 Wireless	🕶 💠 Building1	Port Temp	lates							
Lill Reports	🔯 Building1	O Add	📴 Eder 🔕 Deis	to Local Only						
Tasks	🕨 💠 Building2	-	Configuration		Parlanda Darla	1. the strates	10 ANT TALLEY	Turned	Hatsand	Palacia Parabila
and Administration	<ul> <li>Topology Definitions</li> </ul>	SOURCE	1	Prid	Devent hore	Autoenciación	VLACE ITURIE	raggeo	OursElen	Paoric Endore
	Fabric Connect	LOCAL	AP	Default [1]	None	None			Default [1]	None
Connect	Service Definitions	Local	Access	Default [1]	None	None			Default [1]	None
		Global								Auto Sense
		LOCAT	the smeet	Default [1]	teone	Hotes C			Default [1]	None
		Local	IoT	Default [1]	None	None	nite.		Default [1]	None

Scroll right, until the **SLPP-Guard** option is visible. Click the box, click **Update** and click **Save**.

C Sites >	Devices World Site S	iummary Endpoint Locations	FlexReports									
iame	Discover Actions VR	FALAN Topologies Services	Port Templates	ZTP+ Device Def	aults Endpoint L	ocations Analyt	ics Custom Vari	ables				
🔹 🔷 World												
+ 🔷 Buildingt	Port Templates											
🔛 Building1	🔾 Add 🔯 Edit 😋	Delate Local Only										3
<ul> <li>O Building2</li> <li>Topology Definitions</li> </ul>	Fabric Auth Key	Fabric Connect Drop STP- BPDU	Node Allas	Span Guard	Loop Protect	MVRP	SLPP	SLPP Guard	SLPP Guard Timer	PoE Enable	PoE Priorit	ty
Fabric Connect									60		LOW	
Service Definitions									60	1	LOW	
				0			D	8	60 \$	. 8	LOW	*
	1				( Index	Canad			60		LOW	
						Pracetain.			60		LOW	

### Configuration of Site Actions

Site Actions are triggered whenever a new device is added to a site. Configure the Building1 site actions by selecting **Building1** > **Actions**. Make sure the following items are enabled:

- Automatically Add Devices
- Add Trap Receiver
- Add Syslog Receiver
- Add to Archive
- Add to Site Map (Building1)

Devices Building1 Site Sum	mary Endpoint Locations	FlexReports				
Discover Actions 2 VRF/VLAN	Topologies Services	Port Templates	ZTP+ Device Defaults	Endpoint Locations	Analytics	Custom Variables
Automatically Add Devices	Collection Mode:	Historical	×			
🐨 Add Trap Receiver	Collection Interval (minutes):	15	<b>‡</b>			
🗹 Add Syslog Receiver	Map Name: /World	/Building1/Building1		· )		
🗹 Add to Archive						
Add to Map						

Farther down on the same page, there are additional parameters. Enable Add Device to Policy Domain and select Building1 from the drop-down. Enable Add Device to Access Control Engine Group and leave the engine group set to Default in the pull down.

Add Device to	to Policy Domain	
Policy Domain:	Building1	
ccess Contro	1	
Add Device to	to Access Control Engine Group	
Access Control E	ingine Group: Default *	
Access Control E	Engine Group: Default -	
Access Control E Enable Authe	Engine Group: Default -	
Access Control E Enable Authe Application An	Engine Group: Default   entication Using Port Template nalytics ion Telemetry to Home Engine Using Management IP	
Access Control E Enable Auther Application An Add Applicati	Engine Group: Default   entication Using Port Template  halytics  tion Telemetry to Home Engine Using Management IP  Default	

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

## XIQ-SE Workflow Configuration for VSP Onboarding

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

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

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

Step 1 is possible as of XIQ-SE 22.3 under **Site Actions**, and should always use either the *Extreme VOSS - Fabric Attach* or *Extreme VOSS - Per-User ACL* RADIUS attribute templates, depending on whether the switch is also being added to a Policy domain or not. This however only works properly as of XIQ-SE 22.6. In prior versions the *Onboard VSP* workflow was used.

Step 2 is possible for **Policy Domain**, under **Site Actions**, and this was also already configured earlier. However if the policy framework is not in use, and there was a

requirement to add the switch to an Access Control Location Group, then the *Onboard VSP* is required.

Step 3 is automatically taken care of by XIQ-SE since the 22.3 release, in conjunction with Action 1. This action is actually performed by the XIQ-SE Control Engine(s). Again, this works properly as of XIQ-SE 22.6. However XIQ-SE will only create configure RADIUS for *eapol* on the switch. To activate other RADIUS uses (like *cli* and *web*) in addition to *eapol* the *Onboard VSP* workflow can be used.

The workflow must be configured for use. In XIQ-SE, select **Tasks** > **Workflows**. In the **Workflows** tab, select the *Onboard VSP* workflow. Under the workflow details, view the **Inputs** tab.



Provide the following inputs:

- DVR Leaf: enable
- Network Access Control (NAC): disable
- NAC Engine Group name: <ignore if NAC is disabled>
- RADIUS Attributes Template name: <ignore if NAC is disabled>
- RADIUS Shared Secret: <ignore if NAC is disabled>
- Location Group name: <ignore if NAC is disabled>
- Auto-sense Voice I-SID: **\${voicelsid}**
- Auto-sense Voice VLAN-id only if tagged: **195**
- Auto-sense Data I-SID: <leave empty, will be using NAC for the client>
- Auto-sense ISIS Authentication key: <either leave empty, or set a key for ISIS auth>
- Auto-sense FA Authentication key: <leave empty or set an FA auth key>
- Auto-sense Wait Interval: <leave empty>
  - A 45 second wait interval was required in VOSS versions prior to 8.7 to ensure Cloud APs were placed in the correct VLAN
- Additional CLI commands
  - **auto-sense eapol voice lldp-auth**lldp-auth is optional, add this command to bypass NAC authentication for IP Phones

#### • clock time-zone US Eastern



#### Note

NAC is not used for the IP phone. Instead, EAP Voice LLDP detection bypass is used.

#### 

The **\${voiceIsid}** variable is case-sensitive.



Save the modified workflow and click OK.



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

In this guide, the VSP edge switches are onboarded into the Building1 site, but a typical customer deployment will have multiple sites as shown below with different *voice1sid* values for each site.

Site	voiceIsid
Building1	2100195
Building2	2200195

In XIQ-SE, select **Building1** > **Custom Variables**, and add the *voiceIsid* variable as shown below. Click **Update** to save the changes.





-0-0-0

#### Note

The variable name is case-sensitive. Make sure to enter it correctly.



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

Dashboard	Devices	Docovere	d Firmage	e Archiv	es Configuration Te	emplates Repor	rts.					
Sites	-		Devices	Building1	Site Summary 1	indpoint Locations	Hertop	orts				
Name			Discover	Actions	VRF/VLAN Topol	ogles Services	Port Tem	plates Z	ttP+ Device Defaults	Endpoint Locations	Analytics	Custom Variables
• 🔷 World												
+ 🔷 Buld	fingt		0 605	1 Ide	g Gelete							
+ O Build	ting2				Scope					Variable		
- A Tepolog	Defentions		Category		Site	Type		Name 1	Type	Value		
Telar	ne Conviect		51te		/World/Building1			voiceisid	String	2100	195	
6 Service (	Definitions											

Select **Save** to save the variables.

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

Dashboard Devices	Discovere	d Farrison	ne Archive	<ul> <li>Configuration Tempi</li> </ul>	utes Report	3				
Stas +	=	Devices	Buildingt	Site Summary Endp	oint Locations	RexRep	110			
Name	٠	Docover	Actions	VRENLAN Topologie	s Services	Part Term	plates ZTP-	+ Device Defaults	Endpoint Locations	Analytics Custom Variables
				A.A. 1921.2						
🕨 💠 Buildingt		O Add	1990 B	O Cartera						
🕨 💠 Building2				Scope				1	rariable	
+ 📓 Topology Definitions		Catagory		Site	Туре		Name 1	Туре	Value	i
Fabric Connect		Sta		Global			voicersid	String	2100	:95
Service Definitions		Ste		/World/Building1			voloetsid	String	2100	195

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

In XIQ-SE, select **Building2** > **Custom Variables**.

Sites 👻 🗄	Devices Build	ding2 Site Summary	Endpoint Locations FI	exReports			<u></u>
Name	Discover Acti	ons VRF/VLAN Topo	logies Services Por	t Templates ZTP+ De	vice Defaults Endpo	int Locations Analytics	S Custom Variable
<ul> <li>World</li> <li>Building1</li> </ul>	🔘 Add	Edit 🤤 Delete					
Building2		Scope			Variable		
<ul> <li>Topology Definitions</li> </ul>	Category	Site	Туре	Name 🕇	Туре	Value	
	Cito	Global		voicetsid	String	2100195	

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

Dushboard Devices D	Pocipular	nd firmware	Archives Con	figuration Templ	etes Repor	15					
Sites •	=	Devices But	iking2 Site Su	mmary Endp	ant Locations	Fluctupe	ens.				
Name		Discover Ad	tens VIRALA	N Topologies	Services	Port Temp	lates ZTP+ De	vice Defaults	Endpoint Locations	Malytics	Custom Variables
<ul> <li>World</li> <li>Buildingt</li> </ul>		O Add	Ecte 🥥 Owl	ata							
🖡 💠 Building2				Scope					Variable		
• 🔊 Topology Definitions		Category	Ste		Туре		Name 1	Type	Valu	e .	
D Fabric Connect		Site	/World/S	luleing2			volcetoid	String	2200	195	
Service Definitions		Site	Global				voicebid	String	2100	195	

Select **Save** to save the variables for Building2.

In XIQ-SE, select **Building1** > **Actions**. In the **Custom Configuration** section, add an entry with the following parameters:

- Vendor: Extreme
- Family: Universal Platform Fabric Engine
- Topology: Any
- Task: Provisioning/Onboard VSP

Select Save to commit changes.

This custom configuration entry links the *Onboard VSP* workflow to the Building1 site and the workflow executes when the onboarding switch is placed in the site.

Devices Buil	ding1 Site Sumr	mary Endpoint Location	s FlexReports				
Discover Act	ions 2 VRF/VLAN	Topologies Services	Port Templates	ZTP+ Device Defaults	Endpoint Locations Analytics Cust	om Variables	
Automatica	illy Add Devices	Collection Mode:	Historical	*			
🗹 Add Trap R	eceiver	Collection Interval (minutes):	15	\$			
😪 Add Syslog	Receiver	Map Name: /Work	/Building1/Building1	*			
Add to Arch	hive						
Add to Map	5						
Custom Co	onfiguration						
O Add	🗊 Edit 😄	Delete					
Enabled	Vendor	Family	4	Topology	Task		
S	Extreme	3 Universal Platf	orm Fabric Engine	Any	Provisioning/Onboard VSP	5	
S.	Extreme	Universal Platf	orm Switch Engine	Any	Provisioning/Change persona to VOS	is	
	Extreme	Howertal Platf	orm EXOS	Anv	Provisioning/Change persona to VOS	is.	



#### Note

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

000	
_	
_	
_	
_	

#### Note

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



## Universal Edge Switch OS Conversion Using XIQ

Upload the Fabric Engine Image to XIQ-SE and Set the Reference Image on page 43

Before the VSP fabric edge switch is onboarded, XIQ-SE needs to convert the OS of the Universal Edge switch to Fabric Engine. (It is initially booted into Switch Engine when powered up.)

Performing OS conversion via XIQ-SE and ZTP+ onboarding requires the switch to restart after intial bootup. The boot sequence is as follows:

- 1. Initial boot as Switch engine
  - a. Switch onboards XIQ-SE via ZTP+
  - b. NOS conversion is performed by XIQ-SE via ZTP+ upgrade
- 2. Switch boots as Fabric Engine with the referenced version installed in XIQ-SE
  - a. Switch onboards to XIQ-SE via ZTP+

## Note

If using 25G or 100G uplink ports to the existing Fabric core, the default Forward Error Correction (FEC) settings are different between Switch Engine and VSP/Fabric Engine. Therefore, before the Switch Engine switch can be onboarded, the

## Upload the Fabric Engine Image to XIQ-SE and Set the Reference Image

The Fabric Engine image must be uploaded to XIQ-SE twice; the first time using the TFTP transfer mode, and the second time using the SFTP transfer mode.

To upload the Fabric Engine image to XIQ-SE in TFTP mode, select **Network** > **Firmware** > **Upload**. For the **File Transfer Mode**, select **TFTP**, choose the image to upload and click **Upload**. The image is uploaded to the /tftpboot/firmware/images directory.

To upload the Fabric Engine image using SFTP, repeat the previous step, but select SFTP as the **File Transfer Mode**. The image is uploaded to the /root/firmware/images directory.

A Network 1	Dathbard Devise Discovered	Frenars 2/	Nine Configu	idan Terpla	wi Reporti		
Control	٩				Upload Firmware to	Server	
₩ Analytics ♥ Winders ↓ Reports ■ Tasks	Name	Referenced	image Nome	image FA	Dr Browser uploads no uploa NOTE Older browse	op files here or click to t supported for files gr d the file using the sc trs may here a 208 lim upliced.	browse. eater than AGE. 9 command. 6 and will require
Administration Connect	<ul> <li>De Cyan</li> <li>Al Free</li> <li>Organia          <ul> <li>Quick access</li> <li>Destroate</li> <lidestroate< li=""> <li>Destroate</li>             &lt;</lidestroate<></ul></li></ul>	Norme - Today (1) - MOULENDED-men - MOULENDED-men - MOULENDED-men - MOULENDED-men		Date mo	<ul> <li>D</li> <li>P</li> <li>Afer</li> <li>Trostant</li> <li>VCSC/Ve</li> <li>ARR</li> </ul>	Insuch Eportmach III - III Site HELGERIKE BE Open Cancel	•
<b>О</b> нер	1 1 tydar. O fated	4			File Transfer Model 💿 Server Refti Inflabooth Subdirectory:	40 rts maane/mages/	0 502 C

The Fabric Engine image in the /root/firmware/images/ folder must be made the reference image. Right click on the image and set it as a reference image.

A Network	Dashboard Devices Discovered Firmware Arch	ives Configura	tion Templates Reports	s					
🔔 Alarms & Events	9								
Control	Name	Referenced	Image Name			Image Filename	Image Path	Date/Time	Image Size
Analytics	<ul> <li>Device Type (5 images)</li> </ul>	1	5520.8.10.0.0.voss			5520.8.10.0.0.voss	/tftpboot/firmware/images/	6/7/2023 12:50:30	119.84 MB
💎 Wireless	<ul> <li>Extreme (5 images)</li> </ul>	0	5520.8.10.0.0.voss(2)	-	Austral D		/root/firmware/images/	6/7/2023 12:51:45	119.84 MB
Lini Reports	<ul> <li>Fabric Manager (1 image)</li> </ul>			1	Remove	rrmare			
Tasks	<ul> <li>Universal Platform EXOS (2 images)</li> </ul>				Set as Re	ference Image			
Administration	<ul> <li>Universal Platform Fabric Engine (2 images)</li> </ul>				Delete In	ace			
	<ul> <li>Fabric Engine 5520 (2 images)</li> </ul>			1		- • •			
Connect	<ul> <li>Universal Platform Switch Engine (1 image)</li> </ul>								
	<ul> <li>Universal Platform VOSS (2 images)</li> </ul>								

The referenced icon turns blue.

Referenced	Image Name	Image Filename	Image Path	Date/Time	Image Size	
T	5520.8.10.0.0.voss	5520.8.10.0.0.voss	/tftpboot/firmware/images/	6/7/2023 12:50:30	119.84 MB	
E	5520.8.10.0.0.voss(2)	5520.8.10.0.0.voss	/root/firmware/images/	6/7/2023 12:51:45	119.84 MB	

ZTP+ uses SFTP to upgrade Fabric Engine firmware and XIQ-SE uses SCP to upgrade Fabric Engine firmware. In both cases, the default SCP and SFTP credentials must be changed.

Select Administration > Options > Inventory Manager > File Transfer > SCP Server Properties.

	Q	Inventory Manag	ger > File Transfer > SCP	Server Properties
Options 1		Login Informa	tion	
ExtremeNetworks.com Updates				
▶ FlexView		🗹 Anonymou	s	
Impact Analysis		Username:	anonymous	
<ul> <li>Inventory Manager</li> </ul>		Password:	Ø	
<ul> <li>Dashboard</li> </ul>				
Data Storage		Firmware Directory	Path (must contain root path):	/root/firmware/images/
▼ File Transfer		Root Directory Path:		/root/
FTP Server Properties		🕑 Use the Extreme	Cloud IQ - Site Engine's IP	
<ul> <li>SCP Server Properties</li> </ul>				Concerne 1
SFTP Server Properties		Server IP:		
		Server Port:		22 🏛

Disable Anonymous and specify the username and password for the SCP/SFTP server. You must set the username to root and then set a password. Here we set it to password. Click **Save**.

Profiles Users Server Information License	Certificates	Options De	evice Types	Backup/Re	estore D	liagnostics	Client API	Access
	Q In	ventory Manag	ger 🕻 File 1	Transfer	SCP Ser	rver Prope	erties	
ntions 🕇		Login Informa	ation					
ExtremeNetworks.com Updates FlexView	^	Anonymou	IS		[	Default Value	true ]	
Impact Analysis		Username:	root		[]	Default Value	anonymous	1
Inventory Manager		Password:	password	ł	•	Default Value	****]	
<ul> <li>Dashboard</li> <li>Data Storage</li> </ul>	Fir	mware Directory	Path (must co	ontain root p	oath): /r	oot/firmwar	e/images/	
<ul> <li>File Transfer</li> </ul>	Ro	ot Directory Path			11	oot/		
FTP Server Properties     SCP Server Properties	V	Use the Extreme	eCloud IQ - Si	te Engine's I	P			
SETP Server Properties	Se	rver IP:				0.9.203.5		
TFTP Server Properties	Se	rver Port:			2	2	\$	
<ul> <li>Firmware Refresh Settings</li> </ul>								

Click on the SFTP Server Properties folder, and repeat the previous steps. Click Save.

	Q Inventory Mana	iger > File Transfer > SF	TP Server Properties	
ptions 🕇	Login Inform	ation		
ExtremeNetworks.com Updates	<b>^</b>			
FlexView	Anonymo	us	[Default Value: true]	
Impact Analysis	Username:	root	[ Default Value: anonymous ]	
Inventory Manager	Password:	password	[ Default Value: **** ]	
<ul> <li>Dashboard</li> </ul>		<b>~</b>		
Data Storage	Firmware Directory	Path (must contain root path)	: /root/firmware/images/	
<ul> <li>File Transfer</li> </ul>	Root Directory Path	1:	/root/	
FTP Server Properties	Use the Extrem	eCloud IQ - Site Engine's IP		
<ul> <li>SCP Server Properties</li> </ul>	4			
SFTP Server Properties	Server IP:		10.9.203.5	
TETP Server Properties	Server Port:		22 🇘	

To Enable the ZTP+ OS conversion in XIQ-SE. Select **Network** > **Devices** > **World** > **ZTP+ Device Defaults**'

🛔 Network 💦 🚹	Dashboard Devices Discovered	Firmware Archives Config	uration Templates	Report	5		
🔔 Alarms & Events	Sites - E	Devices World Site	Summary Endp	oint Locati	ons FlexReports		
Control	Name	Discover Actions Vi	RF/VLAN Fabric	Connect	Services Port Template	S ZTP+ Device D	4 Endpoint Locations
Analytics	👻 💠 World					<u> </u>	
🛜 Wireless	Building1	Configuration/Upg	rade				
III Reports	Building2	Configuration Updates:	Always	*	Firmware Upgrades:	Always	-
🧱 Tasks	<ul> <li>Topology Definitions</li> </ul>	Undate Date:	40000000		Liegende Dates	4/20/2022	
Mainistration	Fabric Connect						
➡ ≓ Connect	Service Definitions	Update Time:		*	Upgrade Time:		·*
		Update UTC Offset:			Upgrade UTC Offset:		
					NOS Persona Change:	To Fabric Engine	~

Set Firmware Upgrades to Always and set NOS Persona Change to To Fabric Engine.. Click Save.



Note

Both settings only work if configured under the world site.

XIQ-SE/ZTP+ is now configured to perform the OS conversion to Fabric Engine.



Switch Installation and Power Up on page 47 Observe Progress Using the VSP Edge Console on page 47 Monitor XIQ-SE Onboarding Workflow Execution on page 50 Migrate VSP Edge to Dedicated Switch Management CLIP on page 52

## Switch Installation and Power Up

In previous topics, XIQ-SE was provisioned for the automated onboarding of the Fabric Engine edge switches. To initiate the onnboarding process, install each of the edge switches, apply power, and connect at least one edge switch to an existing Fabric Connect core. As mentioned previously, each edge switch is in a *factory ship* state without an existing configuration file and boots into Switch Engine. When the switch is booted, the ZTP+ process starts and the edge switch connects to XIQ-SE where the OS conversion to Fabric Engine starts.

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

## Observe Progress Using the VSP Edge Console

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

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



The boot up sequence of the Fabric Engine switch is based on two possible deployment scenarios.

Scenario 1: ISIS Hello Authentication disabled on the VSP/Fabric Engine core NNI links:

- 1. ISIS adjacency forms with neighboring core switches.
- 2. A nickname is dynamically assigned by Nickname servers on the core switches.

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

Scenario 2: ISIS Hello Authentication enabled on the VSP/Fabric Engine cores NNI links:

- 1. ISIS adjacency does not form with neighboring core switches because there is no ISIS authentication key on the booting edge switches.
- 2. The onboarding switch issues a DHCP request on the onboarding VLAN 4048 on the core switches.
- 3. The switch obtains an IP address, default gateway, and DNS domain name.
- 4. The switch performs a DNS lookup for *extremecontrol.<domain-name>* and discovers the XIQ-SE IP address
- 5. The switch connects to XIQ-SE and appears in the **Discovered** tab.
- 6. If XIQ-SE can allocate the switch to a site, then the site ZTP+ config is pushed; else the switch remains in the **Discovered** tab until an administrator manually configures or adds the switch to a site.
- 7. When the switch is allocated to an XIQ-SE Site, the Site's Actions are performed, and the *Onboard VSP* workflow is executed.
- 8. The *Onboard VSP* workflow applies the final NAC config, Auto-sense config, and DVR-Leaf config. In addition, the VSP edge switch is configured with the Auto-sense ISIS authentication key.
- 9. ISIS adjacency can now form with neighboring VSP core switches.
- 10. A nickname is dynamically assigned by Nickname servers on the VSP core switches.
- 11. There is a brief period of time where the onboarding switch is unreachable while its connectivity into the onboarding I-SID 15999999 transitions from a UNI connection to a fabric NNI connection.

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

Devices	Building1 Site Summary	Endpoint Locations	FlexReports					
• Add De	vice 🚺 Export to CSV	=						
Status	Name 1	Site	IP Address	Poll Status	Poll Details	Device Type	Family	Firmware
•	5520-12MW-36W-VO55	/World/Building1	10.9.192.104	Available: 1	Up: 192 Do	5520-12MW-36W-V	Unified Swi	8.4.0.0
•	5520-24W-VO55	/World/Building1	10.9.192.103	Available: 1_	Up: 2 Dow	5520-24W-VOSS	Unified Swi	8.4.0.0
•	VSP-core1	/World/Building1	10.9.193.131	Available: 1_	Up: 193 Do	VSP-4450G5X-PWR+	VSP Series	8.4.0.0
•	VSP-core2	/World/Building1	10.9.193.132	Available: 1	Up: 193 Do	VSP-4450GSX-PWR+	VSP Series	8.4.0.0

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

## Monitor XIQ-SE Onboarding Workflow Execution

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



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



Note that the last activity of the *Onboarding VSP* workflow converts the VSP switch to a DVR Leaf and reboots the switch one last time.

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

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

A Network	Dashboard Policy Access Control	Dashboard Policy Access Control End-Systems Reports											
Alarms & Events	Configuration	Engine Group - Default											
Control 1	Group Editor	Details Swi	Details Switches 4. Systems Access Control Engines Guest and IoT Managers										
Analytics		O Add	📴 Edit., 😂 Delete 🛛 🕄 Re	fresh									
★ Wireless	Engines 3	ID Address 1	Nickeame	Chabur	Furthern Minama	Primary	Secondary	Dolinu/M AN	Dello, Demain				
an Reports	Engine Groups     Definit	(in more st	The second secon	518103	System Harris	Engine	Engine	Forty Fort	Policy Domain				
	NAC/10.9.203.6	10.9.192.102	5520-24W-FabricEngine	Contact Est	5520-24W-Fab	10.9.203.6		Extreme VOSS - Per-User ACL	Building1				
Marks	<ul> <li>Default</li> <li>NAC/10.9.203.6</li> </ul>	10.9.192.102	5520-24W-FabricEngine 5520-12MW-36W-FabricEngine	Contact Est	5520-24W-Fab 5520-12MW-3	10.9.203.6		Extreme VOSS - Per-User ACL Extreme VOSS - Per-User ACL	Building1 Building1				

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



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

5520-24W-VOSS:1#% show dvr										
DVR Summary Info										
Domain ID Domain ISID Role My SYS ID Operational State GW MAC Inband Momt Clip IP Virtual Ist local address Virtual Ist local subnet mask Virtual Ist peer address Virtual Ist peer address Virtual Ist oluster-id Virtual Ist ISID 5520-24M-VOSS:184	: 1 : 16678217 : Leaf : f0:64:26:aa:80:84 : Up : 00:00:5e:00:01:23 : :									

## Migrate VSP Edge to Dedicated Switch Management CLIP

The VSP edge switches are onboarded using their DHCP-assigned IP addresses, which are converted to static addresses by ZTP+. However, these management IP addresses are configured on the onboarding VLAN/I-SID (4048/15999999). It is a best-practice to move the switch management IP address from the default onboarding VLAN/I-SID to a CLIP management IP address. The XIQ-SE script *Move to CLIP Mgmt* (available on GitHub) is used to configure a CLIP management address.

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

Status	Name 1	Sit	e 1	P Addr	ess	Poll Statu	s	Poll Details	Device Ty	pe	Family	Firmwar
•	5520-12MW-36W-VOSS	/W	orld/Building1 1	0.9.19	2.101	Available	: 1	Up: 2 Dow	5520-12M	W-36W-V	Unified Swi	8.4.0.0
•	5520-24W-VOSS		FlexView	.19	2.103	Available	:1	Up: 1 Dow	5520-24W	-VOSS	Unified Swi	8.4.0.0
٠	VSP-core1		More Views	1.19	3.131	Available	: 1	Up: 92 Do	VSP-4450	GSX-PWR+	VSP Series	8.4.0.0
•	VSP-core2	۰	Configure	1.19	3.132	Available	:1	Up: 92 Do	VSP-4450	GSX-PWR+	VSP Series	8.4.0.0
		© ≈ 4 0	Compass Search Rediscover Clear Alarms Upgrade Firmware Add to Device Group More Actions Archives	 >								
		2	Tasks	•	Config	Þ						
			Maps	• 3	Provisi	oning 🕨	Ψ	Change person	a to EXOS			
			Network	* >_	CLI Cor	mmands		Move to CLIP N	Igmt IP	4		
		1	Policy	> 100		-	T	Onboard VSP				

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

- VSP-edgel 10.9.193.133
- VSP-edge2 10.9.193.134

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

Run Script: M	love to CLIP Mg	gmt IP							1	×
1. Device Select	ion 2. Device S	ettings 1. inv								
These paramete	rs (if any) will be p Description	assed to the scr	ot during	execut	ion, if no param	ieters	are shown, just si	up to the nex	t step.	
New swite	ch mgmt circuit	tless IP (mask	will be	32bits	)					Ì
Associated VRF	F name (default is	GRT):		Glob	alRouter					
Existing mgmt	VLAN IP:			Delet	te	٠				
Complete	Name	Device IP Address	Mgmt IP	CUP	System Name					L
14	5520-12M	10.9.192.101	10.9.15	93.133	VSP-edge1					
	5520-24W	10.9.192.103	10.9.19	93.134	VSP-edge2					
Sanity / D	ebug									
Sanity: enable first see what i are not execut	if you do not trust t does. In sanity m ed:	this script and v ode config com	vish to mands			*				
Debug: enable script author:	if you need to rep	oort a problem to	o the			÷				
								« Previous	Next # Cance	el .

#### Click Next, then click Run.

un Script: Move to CLIP Mgmt IP			1
Device Selection 2. Device Settings	3. Verify Run Script 4. Re	suits	
Script Information			
Task Information: Run Now Script Name: Move to CLIP M	gmt IP	Script Task Name: N/A Timeout (sec): 60	
Overall Status			
COMPLETED			
Devices			
Name	IP Address	Start Time/Total Run Time	
✓, 5520-12MW-36W-VOSS	10.9.192.101	8/24/2021 2:41:20 PM/(24 sec)	4
✓. 5520-24W-VOSS	10.9.192.103	8/24/2021 2:41:20 PM/(24 sec)	ø
lesults.			
<pre>- no ip address 10.9.192.101 - exit - end</pre>			
<ul> <li>save config</li> <li>eleted IP '10.9.192.101' from XMX</li> <li>ded new device IP '10.9.193.133'</li> </ul>	's database 'to XMC Site '/World/Build	ingl' with admin profile 'Fabric Edge'	

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

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



Repeat these steps for the other VSP edge switch.

Confirm that all four VSPs have their correct management IP.

Click Refresh	if	necessary.
---------------	----	------------

Dashboard Devices Discovered	feminiet Anth	ives Configuration Ter	nplates Reports						
Stes + II	Devices	Buildingt Site Summ	ary Endpoint Locatio	rs. Hadaports					
Name	O Ant De	ere_ Deporto CS							
+ 🔷 world		The second s							
🔹 💠 Building1	Status	Name	50+	IP Address	Pal Solus	Pol Details	Device Type	Family	Firmaire .
+ 🗢 Building2	•	VSP-core1	(World/Building1	10.8.193.131	Available: 1_	Up: R5 Do-	V5P-4450G5X-PWIN	VSP Serves	R.4.0.0
+ 🔊 Topology Definitions		VSP-core2	/World/Building1	10.9.193.132	Available:1_	Up: 95 Do	VSP-4450GSX-PWR+	VSP Series	840.0
Fabric Connect		VSP-edge1	/World/Building1	10.8.193.133	Available: 1_	Up: 1 Dow	5520-125/W-36W-V-	Unified Sal.,	840.0
Service Definitions		VSP-adge2	/World/Building1	10.0.193.134	Available: 1_	Up:1 Dow.,	5520-24W-VOS5	Unified Sel.,	8.4.0.0

#### Note

000

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

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

A Network	Workflo	w Dashboard	ied Tasks Saved Tasks	Scripts V	veridiows					
Alarma & Events Control  Analytics Wireless Analytics Tables Tab			Active O				(	uccessful 7		Unsuccessful O
	B See	a Details	rent Page) 💌 Historia	Version	* Source	# Devices	Started By	End Date/Time	Message	Path
	~	1/4/2022 11:33:51	Onboard VSP	83	Site Discover Action	1	NetSight Server	1/4/2022 11:34:28	Added VSP '10.9.193.133' in NAC Engine Gro	/Workflows/Onboard VSP
	~	1/4/2022 11:30:36	Onboard VSP	83	Site Discover Action	1	NetSight Server	1/4/2022 11:31:16	Added VSP '10.9.193.134' in NAC Engine Gro-	/Workflows/Onboard VSP

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

A Network	Dashboard Policy Access Control	2 End-Systems Repo	rts						
🔔 Alarms & Events	Configuration	+ Engine Group	p - Default						
Control 1		Details Swite	ches End-Systems Access Co.	ntrol Engines	Guest and IoT Mana	agers			
Analytics	Group Editor	• 0 Add	Edit O Delete D Re	fresh					
P Wireless	Engines 3	-	· · · · · · · · · · · ·			Brimany	Secondary		
Land Reports	<ul> <li>Engine Groups</li> </ul>	IP Address	Nickname	Status	System Name	Engine	Engine	Policy/VLAN	Policy Domain
Tasks 📰	✓ Default 4	10.9.193.133	VSP-edge1	Contact Est	VSP-edge1	10.9.203.6		Extreme VOSS - Per-User ACL	Building1
Administration	NAC/10.9.203.6	10.9.193.134	VSP-edge2	Contact Est	VSP-edge2	10.9.203.6		Extreme VOSS - Per-User ACL	Building1

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

A Network	2		2.				
Alarms & Events	Dashboard Policy Access Control End	Systems ke	ports				
	📑 Open/Manage Domain(s) 🔻 📑 Global Do	main Settings 🔻	Tools 🔻				
Let Analytics	Domain: Building1						
Analytics	Roles/Services	+ î Devi	ces User Sessions	RADIUS Authentication	RADIUS Accourt	nting	
♥ Wireless	Class of Service	•					
Lili Reports	VLANs	+ Ctut	Name	family	0	autra Tuna	Eirmunen
Tasks	Notwork Posources	stat	VSP-edge1	Universal Platform Fa	abric Engine 55	520-12MW-36W-FabricEngin	e 8.6.1.0
Administration	Network Resources	-	VSP-edge2	Universal Platform Fa	abric Engine 55	520-24W-FabricEngine	8.6.1.0
Connect	Devices/Port Groups 3						
	Devices Port Groups						
	by IP 👻						
	👻 🌒 IP (2 devices)						
	👻 🔍 10.9.193.x (2 devices) 🛛 🕹						
	VSP-edge1						
	VSP-edge2						
A Network	Dashboard Policy Access Control En	d-Systems I	Reports				
🔔 Alarms & Events	Configuration +	Engine G	roup - Default				
Control			-				
Analytics	Group Editor +	Details	Switches End-Sys	tems Access Control Eng	gines Guest a	nd loT Managers	
奈 Wireless	Engines O-	Add	😡 Edit 🤤	Delete C Refresh			
III Reports	✓ Engine Groups	IP Address	1 Nicknam	e Status		System Name	Primary Engine
🧱 Tasks	▼ Default	10.9.193.13	VSP-core	Contact	t Established	VSP-core1	10.9.203.6
Market Ma	http://www.wac/10.9.203.6	10.9.193.13	2 VSP-core	2 Contact	t Established	VSP-core2	10.9.203.6
➡ Connect	<ul> <li>All Engines</li> </ul>	10.9.193.13	3 VSP-edge	1 Contact	t Established	VSP-edge1	10.9.203.6
		10.9.193.13	4 VSP-edge	2 Contact	t Established	VSP-edge2	10.9.203.6
		1					
	Selection						
	Aller 2						
A Help	C Refresh						
- Help		4					

#### Then click Enforce All.

Access Control Eng	jine Enforce				2 ×
Engine	IP Address	Status	Result	Details	
D NAC	10.9.203.6	Audit Completed	Pass		
Force Reconfigurat	ion for All Switches	Force Reconfigura	ation for Captive	e Portal	
		Audit	Preview	Enforce Enforce A	Close

When the enforce has completed, close the window.

Acces	s Control En	gine Enforce				2 ×
	Engine	IP Address	Status	Result	Details	
	NAC	10.9.203.6	Enforce Finished	Success		
) For	ce Reconfigura	tion for All Switches	Force Reconfigura	ition for Captive	Portal	



# **Verify All End Devices Are Operational**

Inspect the VSP Fabric on page 58 Inspect the Auto-Sense Ports on the VSP Edge Switches on page 60 Verify the WLAN AP Is Operational on page 62 Verify the IP Phone Is Operational on page 64 Verify Client PC Authentication on page 65

Confirm that the fabric network is deployed and the end devices are operational. In this example, an IP Phone and a PC are connected to port 1/6 on VSP-edge1 and an Extreme AP is connected to port 1/6 on VSP-edge2. Auto-sense is enabled on both ports (it is enabled on all ports.)



## Inspect the VSP Fabric

Sites 💌 🗉	Devices	Building1 Site Summary	Endpoint Locations Fle	orReports					
iame	O Add Dev	vice D Export to CSV	=						
r 💠 World									
Building1	Status	Name 1	Site	1P Address	Poll Status	Poll Details	Device Type	Family	Firmware
Building2	•	VSP-core1	/World/Building1	10.9.193.131	Available: 1	Up: 263 Down: 0	5520-12MW-36W-FabricEngine	Universal P	8.6.1.0
Topology Definitions	•	VSP-core2	/World/Building1	10.9.193.132	Available: 1	Up: 263 Down: 0	5520-12MW-36W-FabricEngine	Universal P	8.6.1.0
Fabric Connect		VSP-edge1	/World/Building1	10.9.193.133	Available: 1	Up: 124 Down: 0	5520-12MW-36W-FabricEngine	Universal P	8.6.1.0
Service Definitions		VSP-edge2	/World/Building1	10.9.193.134	Available: 1	Up: 124 Down: 0	5520-24W-FabricEngine	Liniversal P.	8.6.1.0

The Fabric Edge is now deployed.

Go to the topology map and arrange the icons.



To view the fabric connect links. Select **View** > **Show Fabric Connect** and click the checkbox. The fabric connect links are displayed in purple as shown below.



The fabric is up, and the fabric services are listed in the **Network Details** tab and can be highlighted on the map as show below. The Data I-SID is highlighted and notice the same I-SID is shown separately for CVLAN-UNI and Switched-UNI. The VSP cores have CVLAN UNIs and IP routing enabled for the L2VSNs and the edge switches use Switched UNIs on the access auto-sense ports.

		Net	twor	k D	etails 1			
2100196	2102194	day	Γ				Ψ.	1 (
	VSP-ecget	2	0		Service ID	Name	Type	
10.8.101.01	10.9.193.11	CP.		-	2100193	ISID-2100193	CVLAN UNI	
04		NV		-	2100193	Building1-Switch-Mgmt	CVLAN UNI	
3		5		-	2100194	Building1-AP-Mgmt	CVLAN UNI	
•	•	Unks		-	2100195	Auto-sense Voice	Switched UNI	1
VSP-core2	VSP+siget	8		-	2100195	Building1-Voice	CVLAN UNI	
10.9.193.132	10 9.193.12	· · ·	<b>S</b>	-	2100196	Building1-Data	CVLAN UNI	
		Shee	8	-	2100196	ISID-2100196	Switched UNI	l.

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

show dvr members

	DVR Members	DVR Members (Domain ID: 1)						
System Name	Nick-Name	Nodal MAC	Role	SPB Cost				
VSP-corel	0.00.01	£0:64:26:95:3c:84	Controller					
VSP-core2	0.00.02		Controller	10				
VSP-edge1	a.10.0a		Leaf	10				
VSP-edge2	a.10.0b		Leaf	20				
4 out of 4 Total Num of DVR M acli.pl: Displayed Record Cou	where displayed $nt = 4$							

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

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

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

show interfaces gigabitEthernet auto-sense

10 - 1	117   単窓		7: 🗃	
VSP-	edge1 🔲 💓 VSP-edg	2 +		1610
VSP-ed	pel:14%			-
VSP-ed/	gel:1#% show 1	terfaces gigabitEthernet auto-sense		
		Port Auto-sense		
PORT	AUTO-SENSE	AUTO-SENSE		
NUM	STATUS	STATE		
	Pashla			
1/2	Faable			
1/3	Enable			
1/4	Enable			
1/5	Enable			
1/6	Enable	VOICE		
1/7	Enable			
1/8	Enable			
1/9	Enable			
1/10	Enable			
1/11	Enable			
1/12	Enable			
1/13	Enable			
1/14	Enable			
1/15	Enable			
1/16	Enable			
1/17	Enable			
1/18	Enable			
1/19	Enable			
1/20	Enable			
1/21	Enable	SNI-ISIS-UP		
1/22	Enable	NNI-ISIS-UP		
1/23	Enable	NNI-ISIS-UP		

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

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

VSP-edg	ge2:1∰% sho	ow interfaces gigabitE	thernet auto-sense
		Port A	uto-sense
PORT NUM	AUTO-SEN STATUS	NSE AUTO-SENSE STATE	AUTO-SENSE PORT-DATA-ISID
1/1	Enable		
1/2	Enable		
1/3	Enable		
1/4	Enable		
1/5	Enable		
1/6	Enable	FA	
1/7	Enable		
1/8	Enable		
1/9	Enable		
1/10	Enable		
1/11	Enable		
1/12	Enable		
1/13	Enable		
1/14	Enable		
1/15	Enable		
1/16	Enable	FA	
1/17	Enable		
1/18	Enable		
1/19	Enable		
1/20	Enable		
1/21	Enable	NNI-ISIS-UP	
1/22	Enable	NNI-ISIS-UP	
1/23	Enable		
1/24	Enable	NNI-ISIS-UP	
More	(q-Quit, s	space/return=Continue,	^P=Toggle on/off)

Check that SLPP-Guard is enabled on all auto-sense ports using the command

show	slpp-	quard
		-)

			SLPP Gua	rd			
			Port Inter	face			
Port	Link	Oper	SLPP-guard	State	Timeout	TimerCount	Origin
1/1	Up	Down	Enabled	N/A	60	N/A	CONFIG
1/2	Up		Enabled	N/A	60	N/A	CONFIG
1/3	Up		Enabled	N/A	60	N/A	CONFIG
1/4	Up		Enabled	N/A	60	N/A	CONFIG
1/5	Up		Enabled	N/A	60	N/A	CONFIG
1/6	Up	Up	Enabled	Monitoring	60	N/A	CONFIG
1/7	Up		Enabled	N/A	60	N/A	CONFIG
1/8	Up		Enabled	N/A	60	N/A	CONFIG
1/9	Up		Enabled	N/A	60	N/A	CONFIG
1/10	Up		Enabled	N/A	60	N/A	CONFIG
1/11	Up		Enabled	N/A	60	N/A	CONFIG
1/12	Up		Enabled	N/A	60	N/A	CONFIG
1/13	Up		Enabled	N/A	60	N/A	CONFIG
1/14	Up		Enabled	N/A	60	N/A	CONFIG
1/15	Up		Enabled	N/A	60	N/A	CONFIG
1/16	Up	Up	Enabled	Monitoring	60	N/A	CONFIG
1/17	Up		Enabled	N/A	60	N/A	CONFIG
1/18	Up		Enabled	N/A	60	N/A	CONFIG
1/19	Up		Enabled	N/A	60	N/A	CONFIG
1/20	Up		Enabled	N/A	60	N/A	CONFIG
1/21	Up	Up	Enabled	Monitoring	60	N/A	CONFIG
1/22	Up	Up	Enabled	Monitoring	60	N/A	CONFIG
1/23	Up		Enabled	N/A	60	N/A	CONFIG
1/24	Up	Up	Enabled	Monitoring	60	N/A	CONFIG
1/25	Up		Enabled	N/A	60	N/A	CONFIG
1/26	Up		Enabled	N/A	60	N/A	CONFIG
VSP-edge	e2:1#8						

## Verify the WLAN AP Is Operational

Connect to XIQ-C (formerly Extreme Campus Controller) and go to **Monitor**, **Devices**, **Access Points**. Make sure the AP is online and green and it should have an IP address on the AP-Mgmt I-SID 2X00194 in subnet 10.9.194.0/24.

Davidsoard	Acc	ess Poin	ts 🝸	e	Fitter vis	ible rows		Q				
Monitor	Staty	Norte		IP.	Address	Site	Version	Model	Redio 1	Redio 2	RI Clerita	R2 Clients
Q 5cm	٠	Eoge	WAP	10	9 194 100	Fabric Edge Sandbox	7.4.1.0-0169	APS05I-FCC	017	0/7	0	0

On VSP-edge2, inspect the I-SIDs configured on AP port 1/6 with the CLI command

show interface gigabitEthernet i-sid 1/6

									PORT	Isid In	nfo		
PORTNUM	IFINDEX	ISID ID	VLANID	C-VID	ISID TYPE	OF	IGIN				ISID NAME	BPDO	MAC
1/6 1/6	197 197	2100194 2100196	N/A 3	untag 196	ELAN ELAN		D1-	-	E1-		ISID-2100194 ISID-2100196	disabled	PALSE PALSE
2 out of acli.pl: ORIGIN 1 C: manua M: FA ma 1: disco VSP-edge	2 Total Display egend: ally cons magement over by 2 12:100	l Num of yed Recor figured: t: E: dis local swi	i-sid e d Count D: disc covered tob r:	overed by EAP discov	by PA o ; A: au er by r	r EPT to-se smote	mse VIST	t an	itch				

#### Note

There are two bindings on the port where the AP is connected. The first binding is created by RADIUS authentication when the AP is first onboarded and corresponds to the AP-Mgmt I-SID. Confirm this by inspecting the MAC authentications on the switch by running the CLI command show eapol sessions neap.

				Non	-Eap Oper	Status		
PORT	MAC	STATE	VLAN ID	PRI	Flex-UNI Enable	I-SID SOURCE	NON-EAP AUTH	VLAN:I-SID
1/6	dc:b8:08:c2:80:79	authenticated	N/A		true	radius	radius	0:2100194
Total	Number of NEAP Ses	sions: 1						
VSP-e	dge2:10%							

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

Go to the **XIQ-SE Control** > **End Systems** tab. Scroll to the right to see the **Authorization** attributes.

Ð	without Policy	Antess Control 6	nd-Systems Ro	ports							Q 1
4	Atthone 🛋	forta Roadhertication	@ Tath + - +	Les • 🛛 🖬 Al Enity	dant Dants						😧 Denne Al +
54	Last Seen 1	MAC Address	MAC OUT thendur	Device Family	Denton Type	9" Address	First Name	Over Name	Automitation Type	freeze	Pulle
0	2010/2521 16 41 (62 PM	DC 89 89 C2 88 79	Estore lates:	Western Access Part	Externe Workes Access Paint				MAC (FMP)	Byle "Access Pare"	Access Park NAC Polle

Inspect the port's EAPoL config by running the CLI command

show eapol port 1/6

Vitil - e	dge2:184	altered	expol.	pors 1/6 '	10.44																
				Espol Cost	-	61.55															
1017	STATUS	OPER NORE	britis Mental	Flee-CHI FIG.51 F	100X \$100	COTEL DELAL	READER PERSON	ARAITS TRACE	NON-EAP FOLMLE	LLDD-ADTH WALSIE	10.X 10.C	10.X 7.1.7	HAX HEAD	GST VLAN	457 7-518	FAIL VLAN	FA31. 7-510	COA EXAMINE	ADMIN TRAFFIC CONTROL	COFER TRAFFIC CONTROL	CRIGIN
1/4	Auto: Spelii#9	HINK	tise	true	4	65	3600	false	true	false	-	2	3	34/34	15999999	34/74	11/2.	false	in-out	in	MITO-SERSE

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

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

Edit VLA	N		0 ×
Name	Data Building!	1	
VLAN ID	Fabric Attach*	Tagged	
I-SID	2100196		
	ADVANCED		
			CANCEL

Confirm by inspecting the Fabric Attach assignments on the switch with the CLI command

show fa assignment

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

VSP-edge2:	1#8 show f	a assignmen	t			
		Fabri	c Attach A	ssignment Map		
Interface	I-SID	Vlan	State	Origin	I-SID Name	
1/6	2100196	196	active	client	ISID-2100196	

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

### Verify the IP Phone Is Operational

On VSP-edgel, view the I-SIDs that are configured on the phone port 1/6 using the CLI command

show	interface	gigabitEthernet	i-sid	1/	6
------	-----------	-----------------	-------	----	---

								PORT	Isid In	fo		
IFINDEX	ISID ID	VLANID	C-VID	ISID TYPE	OR	IGIN				ISID NAME	<b>B</b> 2D0	MAC
197	2100195		195	ELAN						Auto-sense Voice		FALSE
1.97	2100196		untag	ELAN				E1-		ISID-2100196	disabled	TRUE
197	15999999	4048	untag	ELAN				E1-		Onboarding I-SID	disabled	FALSE
	197 197	ISID IFINDEX ID 197 2100195 197 2100196 197 1599999	ISID IFINDEX ID VLANID 197 2100195 2 197 2100196 3 197 15999999 4048	ISID IPINDEX ID VLANID C-VID 197 2100195 2 195 197 2100196 3 untag 197 1599999 4048 untag	ISID ISID ISID IFINDEX ID VLANID C-VID TYPE 197 2100195 2 195 ELAN 197 2100196 3 untag ELAN 197 1599999 4048 untag ELAN	ISID VLANID C-VID TYPE OR 191NDEX ID VLANID C-VID TYPE OR 197 2100195 2 195 ELAN - 197 2100196 3 untag ELAN - 197 1599999 4048 untag ELAN -	ISID ISID ISID IPINDEX ID VLANID C-VID TYPE ORIGIN 197 2100195 2 195 ELAN 197 2199999 4048 untag ELAN	ISID ISID ISID IPINDEX ID VLANID C-VID TYPE ORIGIN 197 2100195 2 195 ELAN 197 2199999 4048 untag ELAN	ISID ISID IPINDEX ID VLANID C-VID TYPE ORIGIN 197 2100195 2 195 ELAN E1- 197 2100196 3 untag ELAN E1- 197 1599999 4048 untag ELAN E1-	ISID ISID IPINDEX ID VLANID C-VID TYPE ORIGIN 197 2100195 2 195 ELAN A 197 2100196 3 untag ELAN E1 197 1599999 4048 untag ELAN E1-	ISID         ISID         ISID         ISID           IPINDEX ID         VLANID         C-VID         TYPE         ORIGIN         NAME           197         2100195         2         195         ELAN          A         Auto-sense Voice           197         2100196         3         untag         ELAN          EL         -         ISID-2100196           197         15999999         4048         untag         ELAN          EL         -         ISID-2100196	ISID         ISID         ISID         ISID           IPINDEX ID         VLAND C-VID         TYPE         ORIGIN         NAME         DFDU           197         2100195         2         195         ELAN          A         Auto-sense Voice           197         2100196         3         untag         ELAN          BL-         ISID-2100196         disabled           197         1599999         4048         untag         ELAN          BL-         ISID-2100196         disabled

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

Show the LLDP neighbor details on the same port using the CLI command

```
show lldp neighbor port 1/6
```

VSP-edgel:1#% show lldp neighbor port 1/6	
LLDP Neighbor	
Port: 1/6 Index : 6977 Protocol : LLDP ChassisId: Network Address 10.9.195.100 PortId : MAC Address 00:08:5d:62:bf:f0 SysName : regDN 4052,MINET_6920 SysCap : BT / BT PortDescr: LAN port SysDescr : regDN 4052,MINET_6920,ver: 01.05.00.075,PxE: 6.5,01/01/1970 10:31:56 +000 Address : 10.9.195.100 IPv6 Address : 0:0:0:0:0:00	0
Total Neighbors : 1	
Capabilities Legend: (Supported/Enabled) B= Bridge, D= DOCSIS, O= Other, R= Repeater, S= Station, T= Telephone, W= WLAN, r= Router VSP-edge1:1#%	

Note the neighbor system capabilities: B = Bridge and T = Telephone. Also note the IP address the phone obtained and in the Voice I-SID subnet. Ping the phone's IP address from Core1



View the Network Access Control (NAC) sessions on port 1/6. If LLDP bypass authentication is used for the phone, then the *NON-EAP AUTH* type shows as lldp. If LLDP bypass is not used, then the *NON-EAP AUTH* type shows as radius.

VSP-e	dge1:1#% show eapol	sessions neap						
				Non	-Eap Oper	Status		
PORT NUM	MAC	STATE	VLAN ID	PRI	Flex-UNI Enable	I-SID SOURCE	NON-EAP AUTH	VLAN: I-SID
1/6 1/6	00:08:5d:62:bf:f0 00:50:56:80:5d:ca	authenticated authenticated	N/A N/A	N/A 0	true true	n/a radius	11dp radius	195:2100195 0:2100196
Total	Number of NEAP Ses	sions: 2						
VSP-e	dge1:1#%							
VSP-e	dge1:1#% show eapol	sessions neap						
				Non	-Eap Oper	Status		
PORT NUM	MAC	STATE	VLAN ID	PRI	Flex-UNI Enable	I-SID SOURCE	NON-EAP AUTH	VLAN: I-SID
1/6 1/6	00:08:5d:62:bf:f0 00:50:56:80:5d:ca	authenticated authenticated	N/A N/A	0 0	true true	n/a radius	radius radius	0:2100196
Total	Number of NEAP Ses	sions: 2						
VSP-e	dge1:1#%							

## Verify Client PC Authentication

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

📌 FabricEdge-Chent - VM-use Renote Consile		~ 0 ×
vivec + Ⅲ + db [0]		-
See Se	* *	- 0 X
F 4 0 (4		8 <b>O</b> :
Connection-specific OK Suffle ,   fabricige.Ms.Ctt.iscal Identity () Statement ()   fabricige.ms.Ctt.iscal Connection-specific OK Suffle ,   fabricige.Ms.Ctt.iscal Likeiner ()   fabricige.ms.Ctt.iscal Connection-specific OK Suffle ,   fabricige.Ms.Ctt.iscal Likeiner ()   fabricige.Ms.Ctt.iscal Connection-specific OK Suffle ,   fabricige.Ms.Ctt.iscal Likeiner ()   fabricige.Ms.Ctt.iscal	Google	Gnat Inages III
Control Contro	Q. Search Google or type a URL	•
Pik Lipson		( Catalogue
🟥 🔎 Type here to search 🛛 O Eli 💽 🚍 🌖 📼		^ 🖓 🖕 MIAM

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

								PORT	Isid In	fo		
PORTNUM	IPINDEX	ISID ID	VLANID	C-VID	ISID TYPE	OR	IGIN			ISID NAME	8500	MAC SUNI
1/6	197	2100195	2	195	ELAN				A	Anto-sense Voice	·····	PALSE
1/6	197	2100196		untag	ELAN			E1-		ISID-2100196	disabled	TRUE
16	197	15999999	4048	untag	ELAN			81-		Onboarding I-SID	disabled	PALSE

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

Confirm both the first and second bindings by inspecting the MAC authentications on the switch, using the CLI command

show eapol sessions neap

Non-Eap Oper Status									
TUM	MAC	STATE	VLAN ID	PRI	Flex-UNI Enable	I-SID SOURCE	NON-EAP AUTH	VLAN:I-SID	
/6	00:00:5d:62:bf:f0 00:50:56:80:5d:oa	authenticated authenticated	N/A N/A	N/A 0	true true	n/a radius	lldp radius	195:2100195 0:2100196	
lotal	Number of NEAP Ses	sions: 2							

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

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

A Network	Burbbaard Policy Access Cantrol End-Systems Reports												
🔔 Alarms & Events	🚓 Add To Group 🔊 Force Resubservation 🥥 Tools 💌 🔹 Lite 👻 🔄 All End System Events									🤹   De			
Control 1	5	Last Seen 1	MAC Address	MAC OUI Vendor	Device Family	Device Type	IP Address	Host Name	User Name	Authentication Type	Reason	Profile	Policy
♥ wireless	0	5/19/2022 4:42:27	00:50:56:80:5D:CA	VMware, Inc.	Windows	Windows 8	10.9.196.100	DESKTOP-4PBNP		MAC (PAP)	Rule: "Enterprise User"	Allow NAC Pro	Enterprise User
Las Dervets	0	5/19/2022 4:41:29	BC/F3:10:05:DC:40	Extreme Netw			10.9.194.101	AH-05dc40.Fabric		MAC (PAP)	Rule: "Access Point"	Access Point N	Access Point
Tasks	°	5/19/2022 4:40:32	DC:88:08:C2:80:79	Extreme Netw	Wireless Ac	Extreme WI	10.9.194.100	Edge-WAP		MAC (PAP)	Rule: "Access Point"	Access Point N	Access Point

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

A Network	D	ashboard Policy A	ccess Control End-S	ystem	s Reports				
🔔 Alarms & Events	đ	Add To Group 🔏	Force Reauthentication	0	Tools 💌	• Live 🕶	All End-Syste	m Events	
Control				MAC OUI Dev Vendor Fam		Device	Device Type	IP Address	Host Name
Analytics	S.	Last Seen 🖡	MAC Address			Family			
🗢 Wireless	0	5/19/2022 4:42:27	00:50:56:80:5D:CA	VA		Windows	Windows 8	10.9.196.100	DESKTOP-4PBNP
I M Descete	0	5/19/2022 4:41:29	BC:F3:10:05:DC:40 DC:B8:08:C2:80:79		Show Details.			10.9.194.101	AH-05dc40.Fabric
(iiiii Reports		5/19/2022 4:40:32		Add To Show Details		v Details	Extreme Wi	10.9.194.100	Edge-WAP
Tasks				2	Edit Custom I	nformation			
🐸 Administration				1	Lock MAC				
- Connect				1	Force Reauth	entication			
Connect					Force ReAuth	and Scan			

#### Select the End Systems tab.

A Network	Dashboard Policy Acce	ss Control End-Systems	Reports End-Syst	tem Details: DESKTOP-4PBNP93.FabricEdge.NH.C	TC.Local						
🔔 Alarms & Events	Access Profile End-System	End-System Events	Health Results								
Control	Add To Group All Ford	e Resurbentication	orce Reauthentication and	I Sran 🚳 Lock MAC 🚿 Edit Registration	C Refresh End Sustem						
Analytics				san a contrarte a contragonation							
🗢 Wireless	End-System Details End-System:	00:50:56:80:5D:CA, 10.9.1	96.100, DESKTOP-4PBN	P93.FabricEdge.NH.CTC.Local							
Lall Reports	User Name: Activity: Last seen 05/19/2022 04:38:03 AM, First seen 05/18/2022 07:33:03 PM										
Tasks	Device Information: Windows (Windows 8/ 8.1/10/11/2012)										
🚰 Administration	Location										
≓ Connect	Location: 10.9.193.132/1/6 Access Control Engine: Default, 10.9.203.6 ELIN:										
	Authentication Sessions										
	Session Time: Policy: RFC 3580 VLAN: Profile: Reason:	05/19/2022 04:38:03 AM Enterprise User Allow NAC Profile Rule: "Enterprise User"	State: Extended State: State Description: Last Scan Result: Authorization:	Accept MAC to IP Resolution Failed Unable to resolve IP address using SNMP, NetBIOS, or DHCP Filter-Id="Enterprise User" Extreme-Dynamic-ACL=*CLIENT Enterprise User"							
				Extreme-Dynamic-ACL='acl inPort name En Extreme-Dynamic-ACL='acl set default-action FA-VLAN-ISID='0:2100196'	iterprise_User' on permit'						

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