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

9037480-00 Rev AB
October 2023

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/

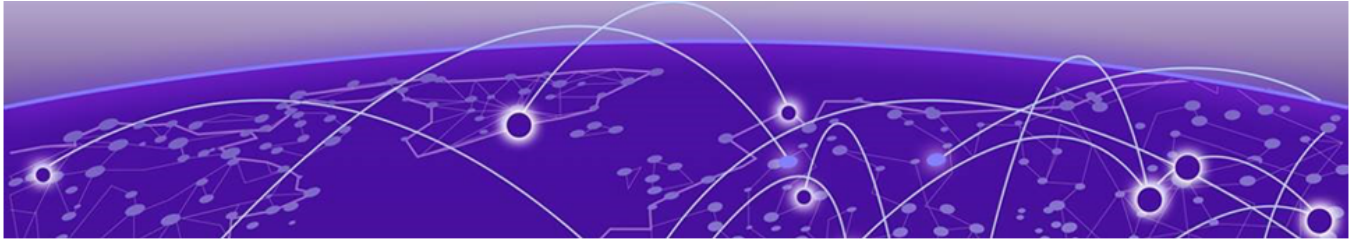


Table of Contents

Preface

Read the following topics to learn about:

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

Text Conventions

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

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

Table 1: Notes and warnings

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

Table 2: Text

Convention	Description
`screen displays`	This typeface indicates command syntax, or represents information as it is displayed on the screen.
The words *enter* and *type*	When you see the word *enter* 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 *type*.
Key names	Key names are written in boldface, for example **Ctrl** or **Esc**. If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press **Ctrl**+**Alt**+**Del**
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 3: Command syntax

Convention	Description
bold text	Bold text indicates command names, keywords, and command options.
italic text	Italic text indicates variable content.
`[ ]`	Syntax components displayed within square brackets are optional. Default responses to system prompts are enclosed in square brackets.
`{ x | y | z }`	A choice of required parameters is enclosed in curly brackets separated by vertical bars. You must select one of the options.
`x | y`	A vertical bar separates mutually exclusive elements.
`< >`	Nonprinting characters, such as passwords, are enclosed in angle brackets.
...	Repeat the previous element, for example, *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.

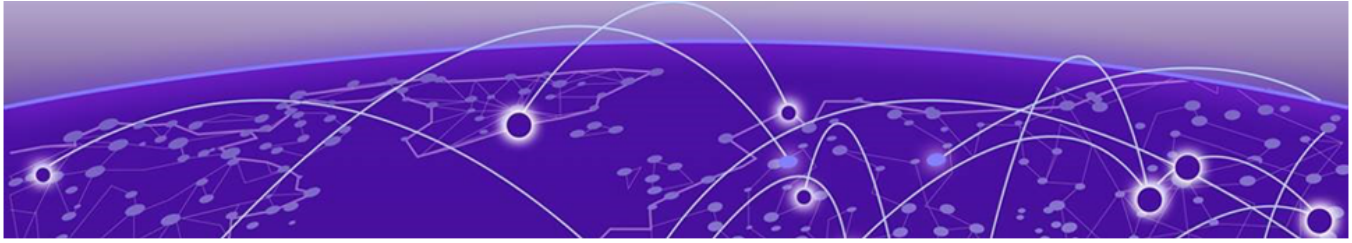
Send Feedback

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

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™ 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

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

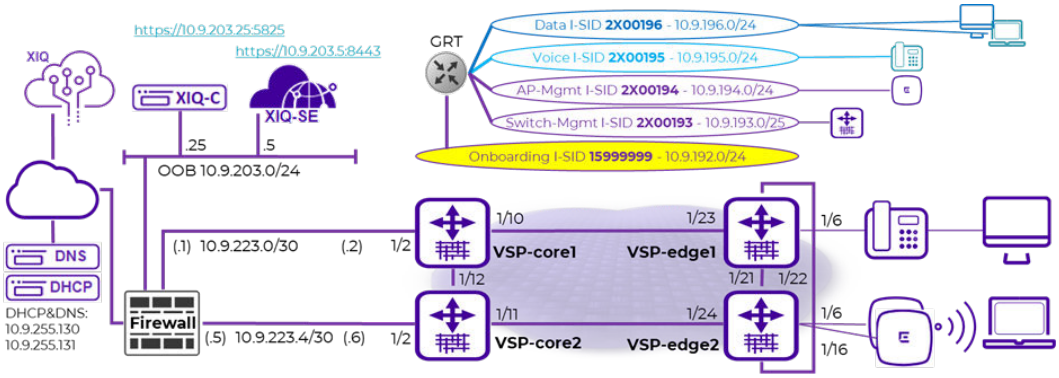
Network Diagram

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.

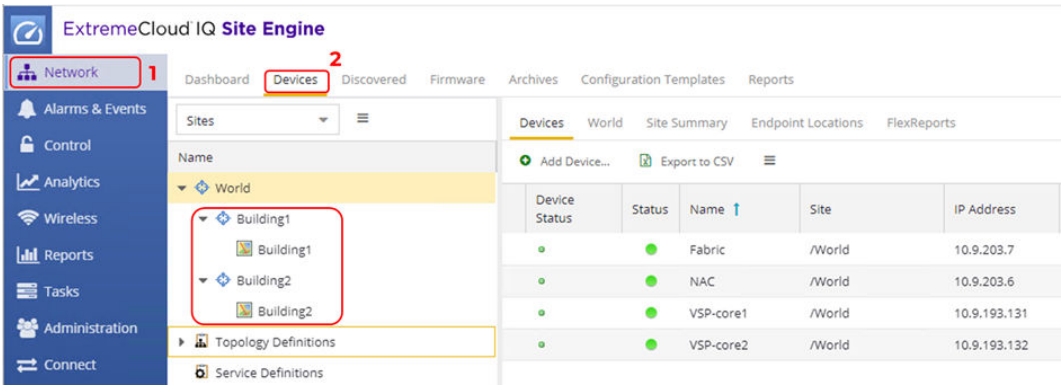
All the L2VSNs are IP routed in the base GRT (VRF-0) of the core nodes and edge DVR-Leaf nodes. Use of VRFs and L3VSNs is possible but will not be covered in this guide since the deployment procedure is similar to the GRT scenario.

Preexisting Configuration Review

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

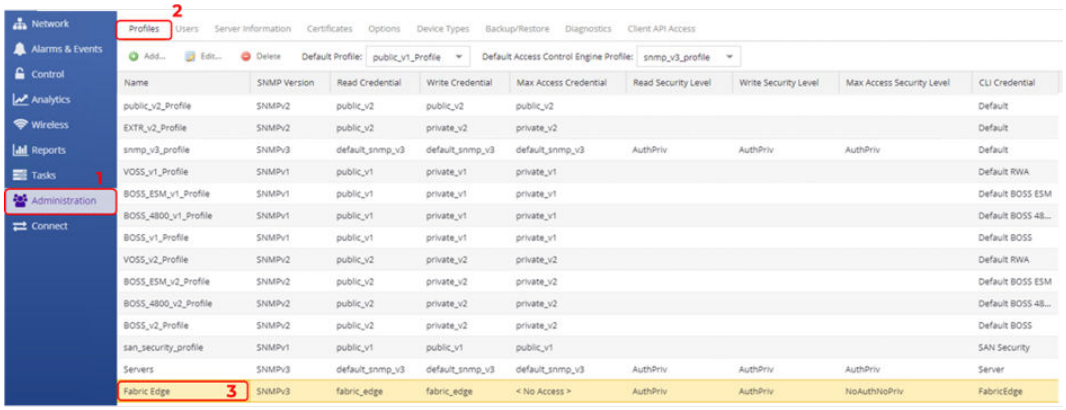
As an example, the Building1 and Building2 sites have already been configured:



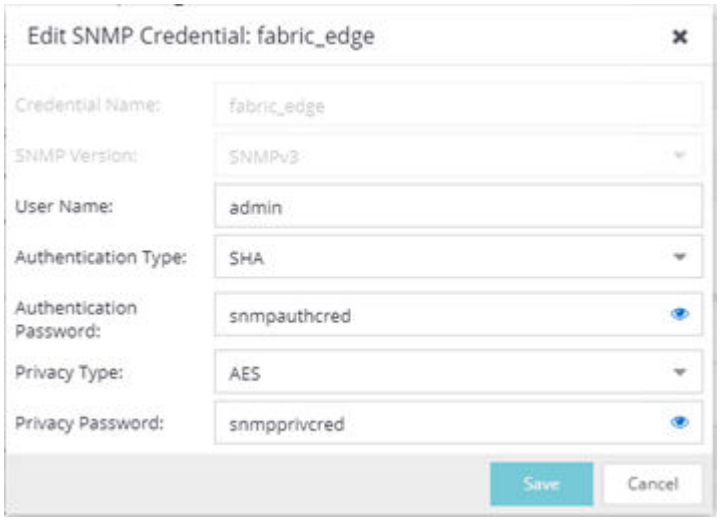
A map of the same name is defined for each site.

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

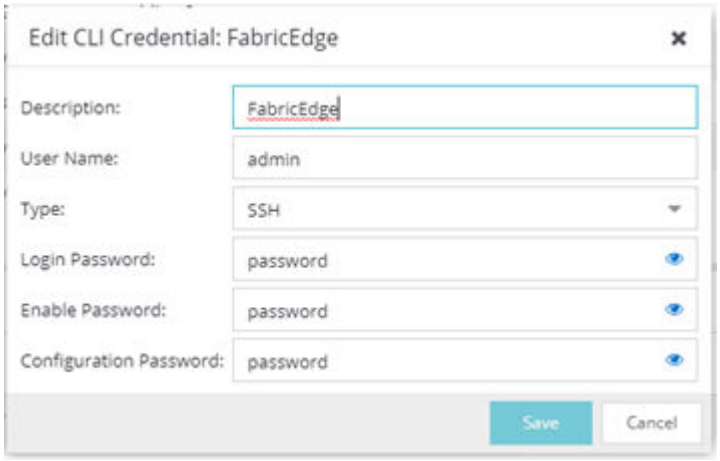
Under **Administration**, the admin profile **Fabric Edge** is defined to manage the switches, as shown here:



This admin profile uses the following SNMP credentials:

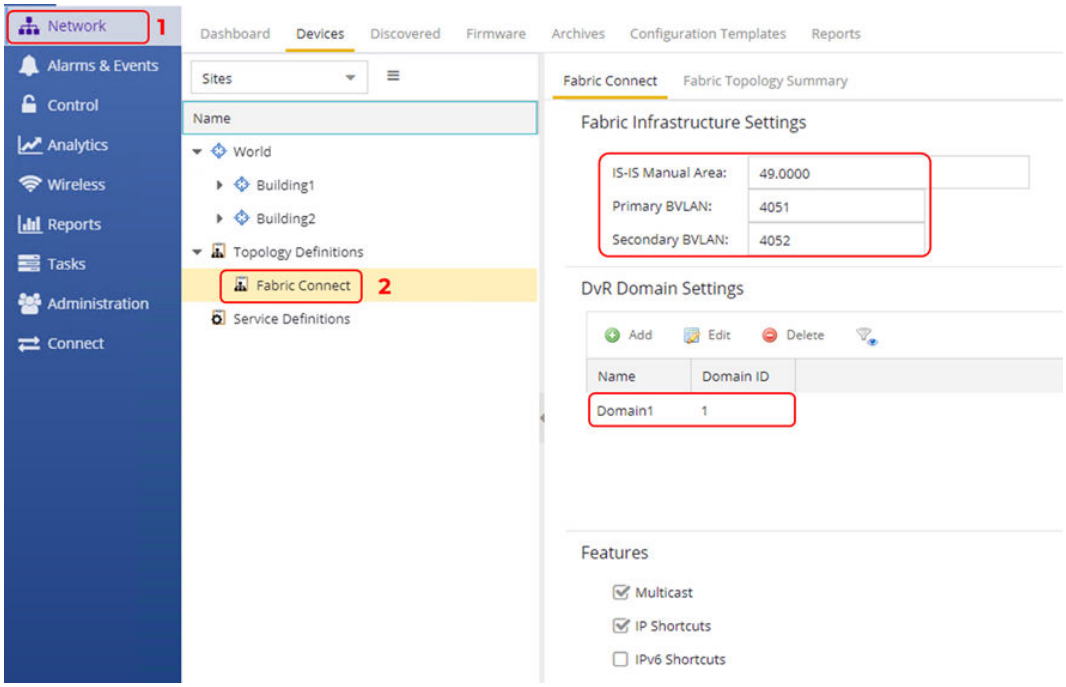


This admin profile uses the following CLI credentials:

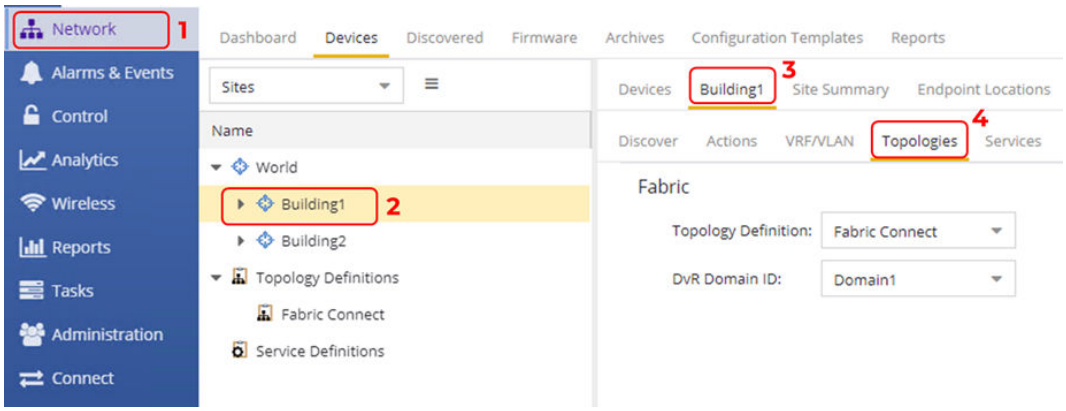


These are non-default credentials, so ZTP+ configures these credentials on the VSP/ Fabric Engine edge switch when it is onboarded for the first time.

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

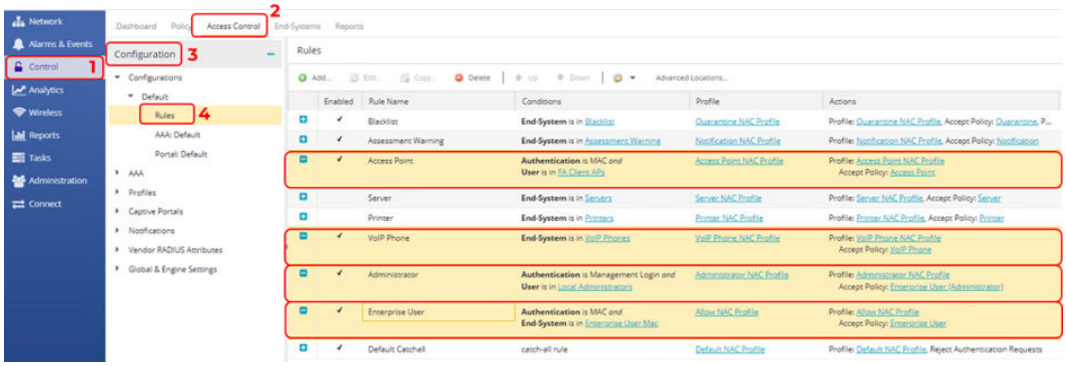


The same settings are assigned to both the Building1 and Building2 sites.



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.



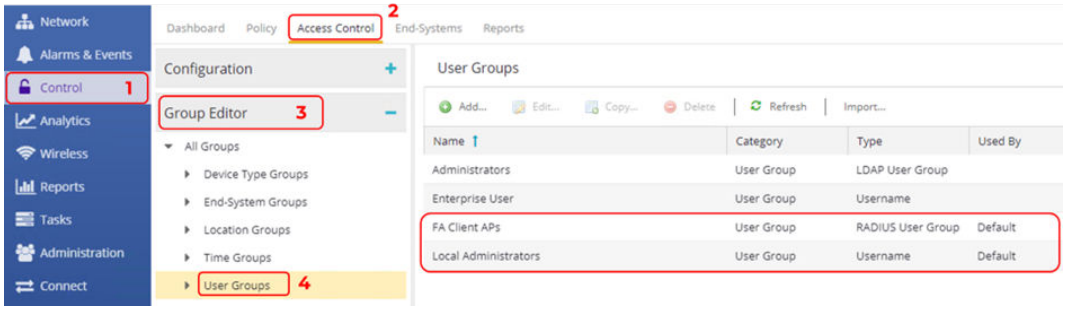
The **Access Point** rule is used to MAC authenticate the WLAN APs using inbound RADIUS FA attributes.

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.

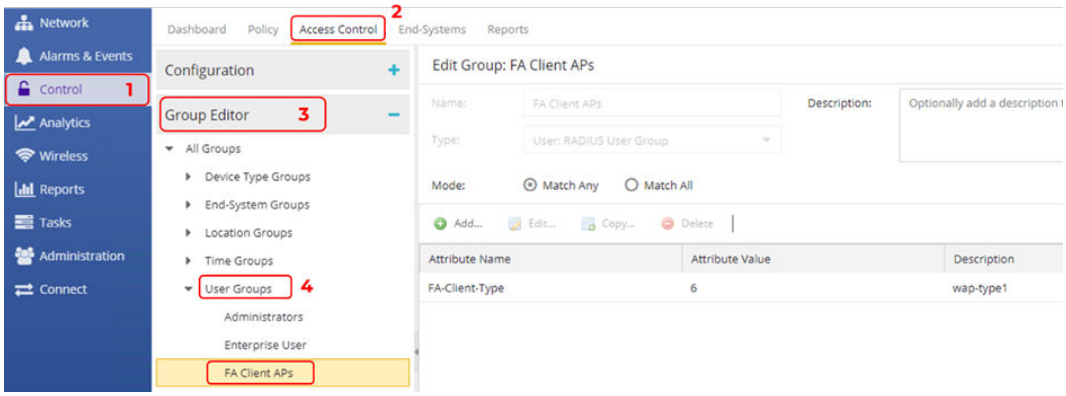
The **Administrator** rule is only used to authenticate CLI and WEB (EDM) access on the switches if these RADIUS authentications are activated during the switch onboarding.

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:



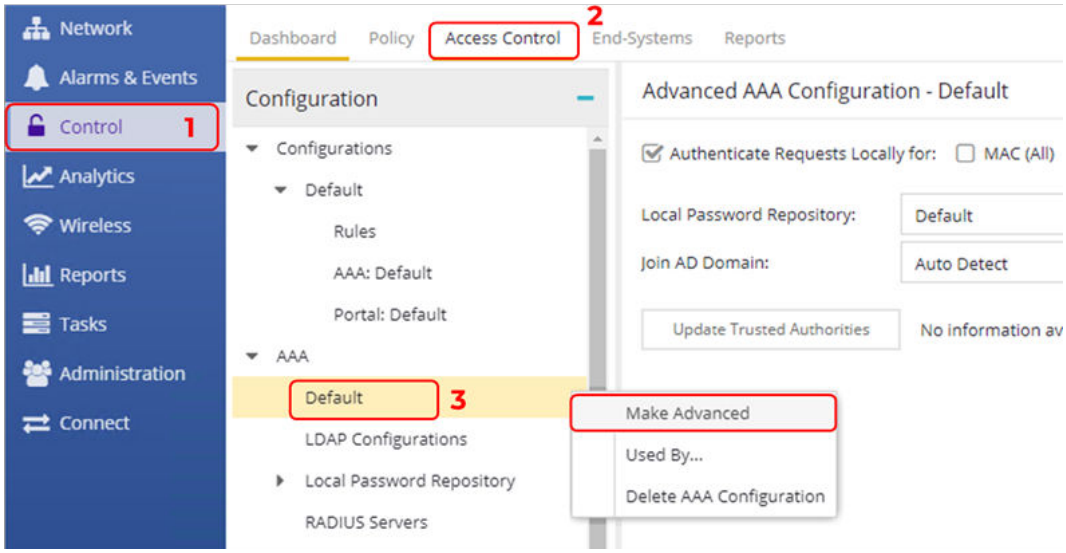
The **FA Client APs** group contains the following:



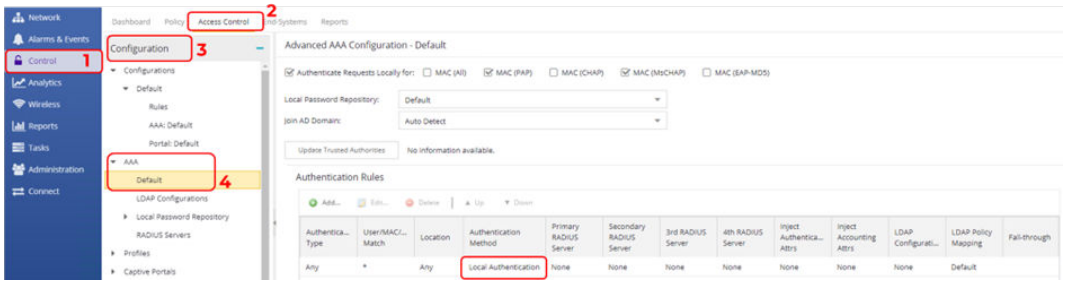
This user group enables easier and more secure authentication of the AP based on its FA Client inbound RADIUS attributes, instead of having to base the authentication solely on the AP's MAC address.

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

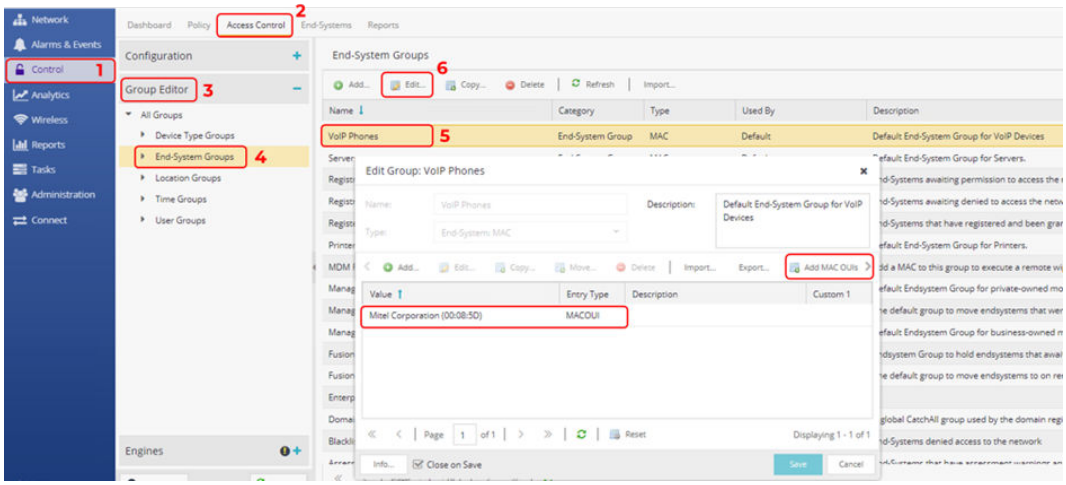
To set up the local password repository, right click the **Default** AAA group and set the mode to **Make Advanced**.



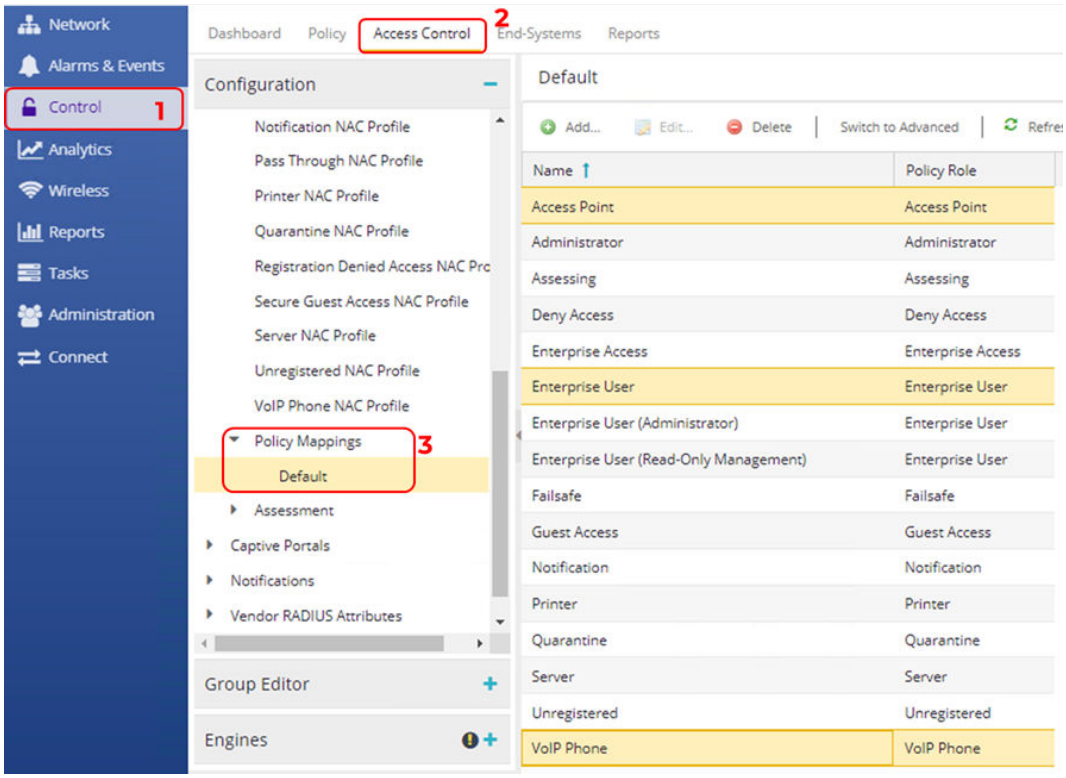
Set the **Authentication Method** to **Local Authentication**. This step is optional and is only used if the user configured `cli` and `web` radius authentication during the fabric edge switch onboarding.



Select **Control** > **Access Control** > **Group Editor** > **End-System Groups**. Edit the **VoIP 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.

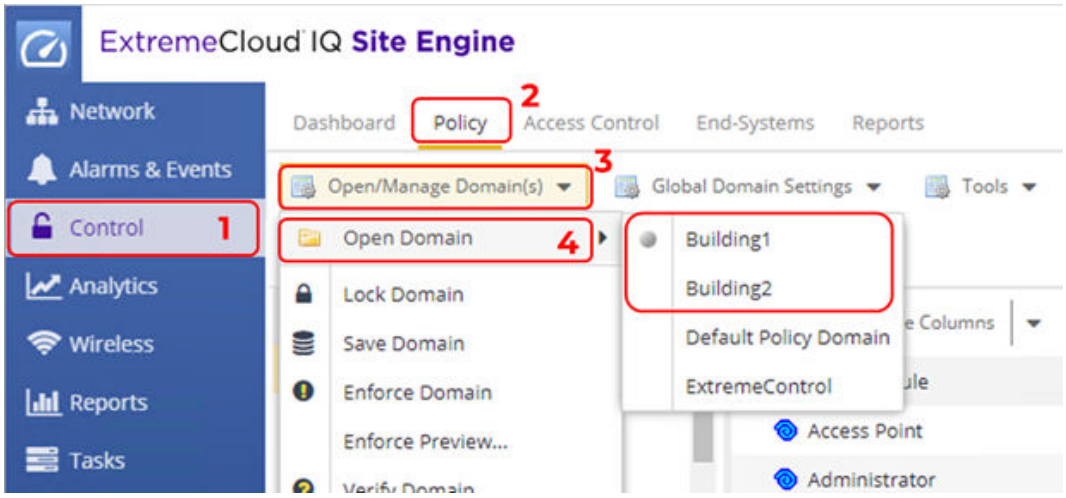


The **Access Point**, **Enterprise User,** and **VoIP Phone** rules contain the policy mappings shown below. The mappings are found in **Control** > **Access Control** > **Policy Mappings** > **Default**.

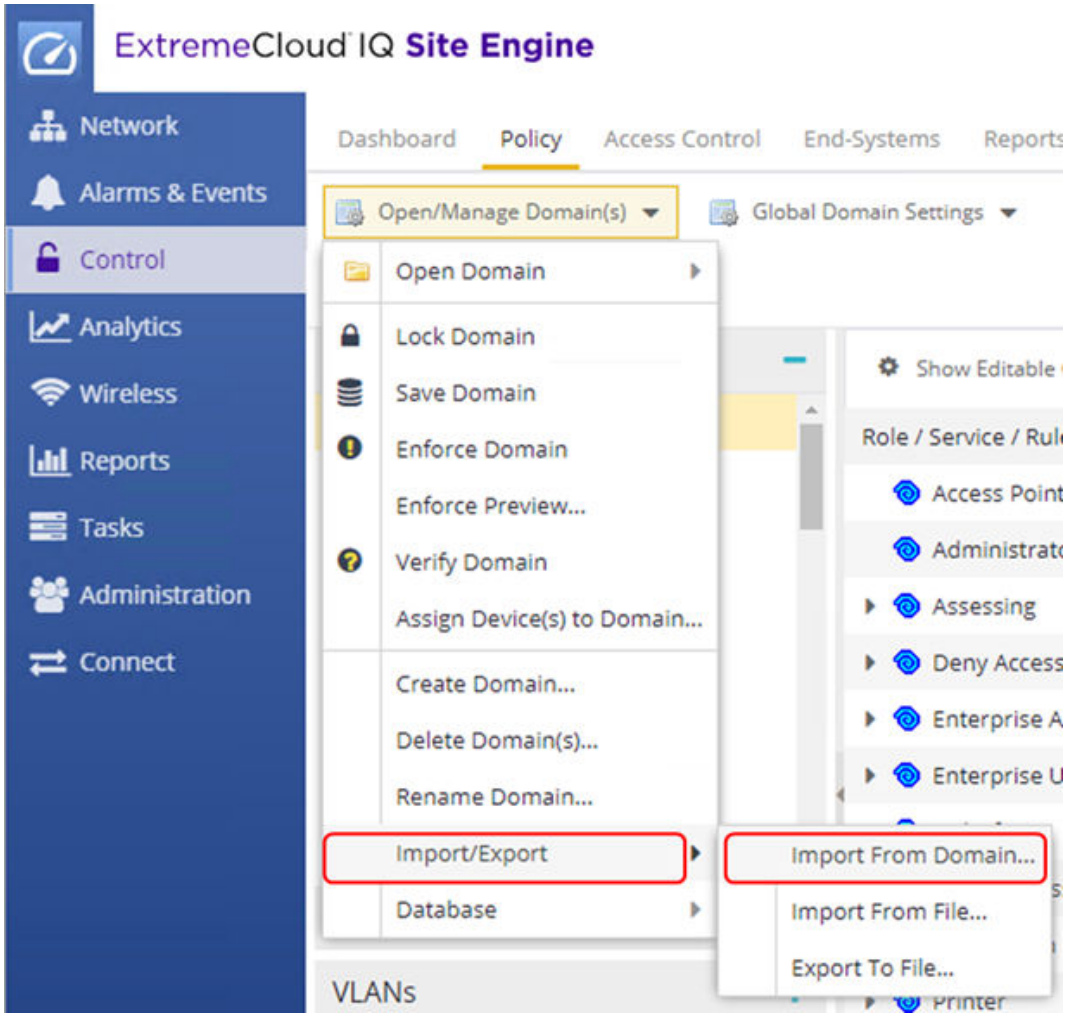


These policy mappings can be used to directly set the returned RADIUS attributes such as `vlan/i-sid bindings`, but the best practice is to use the **Policy** configuration tab to define the returned RADIUS attributes. Because policy is used in this guide, the above entries are mapping the Access Control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

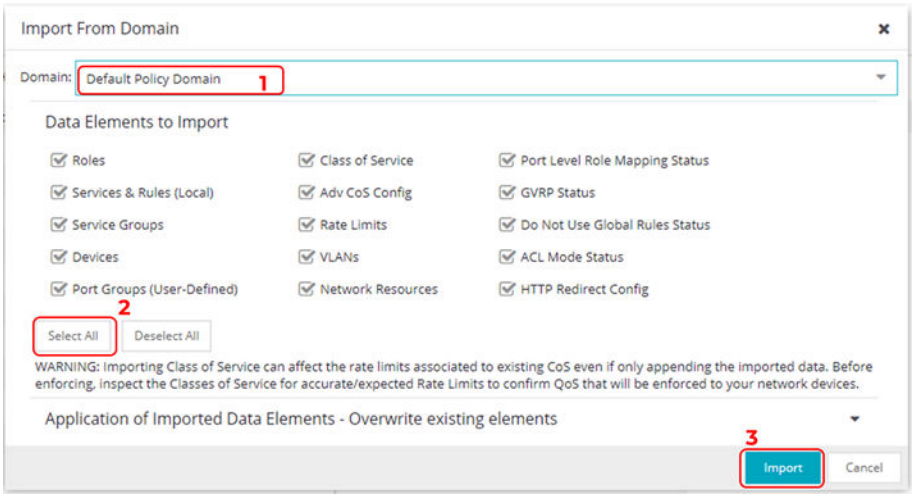
The policy framework is configured on the **Policy** tab. Two policy domains are created: Building1 and Building2, as shown below.



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

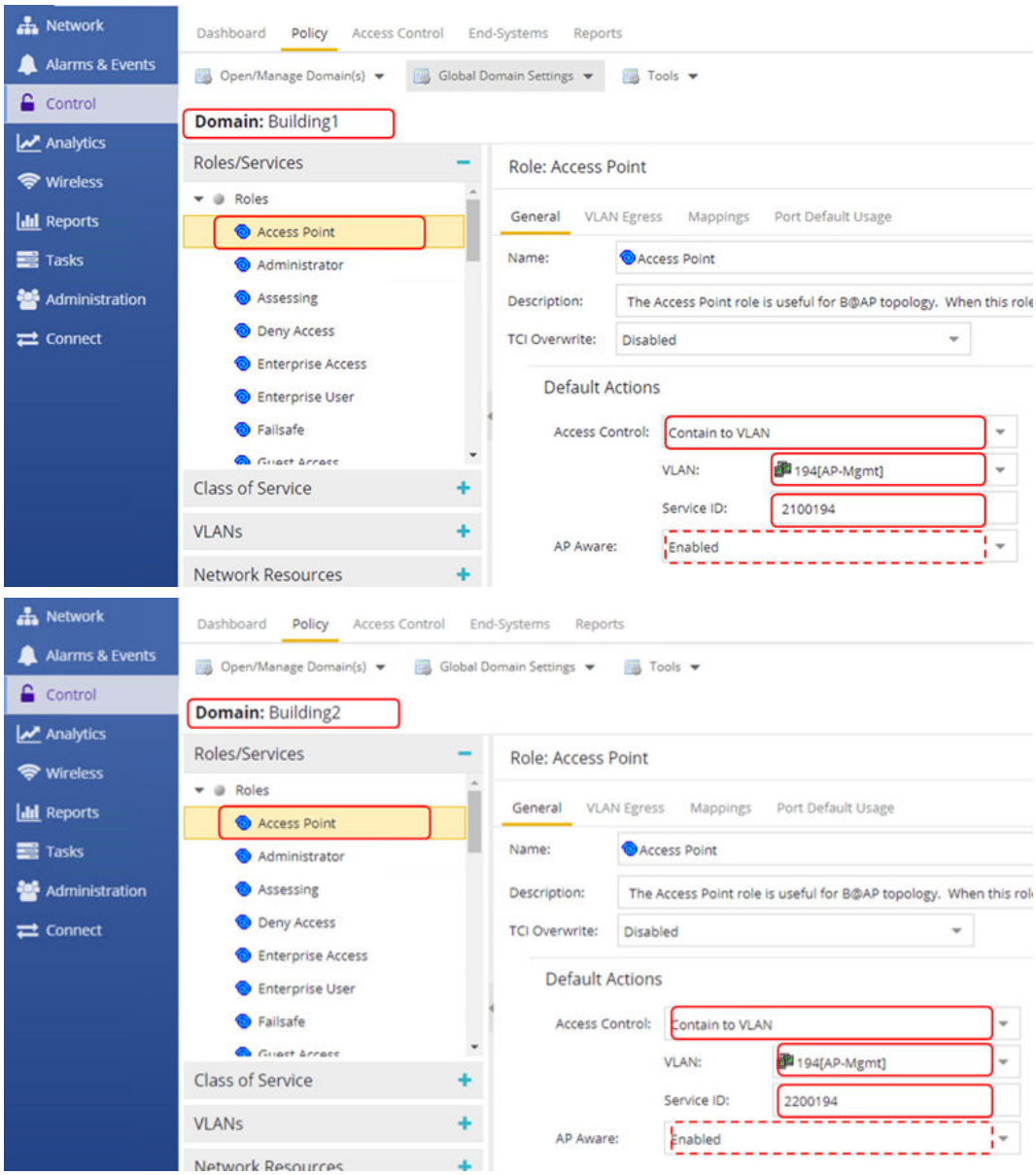


All settings are imported from the **Default Policy Domain**.

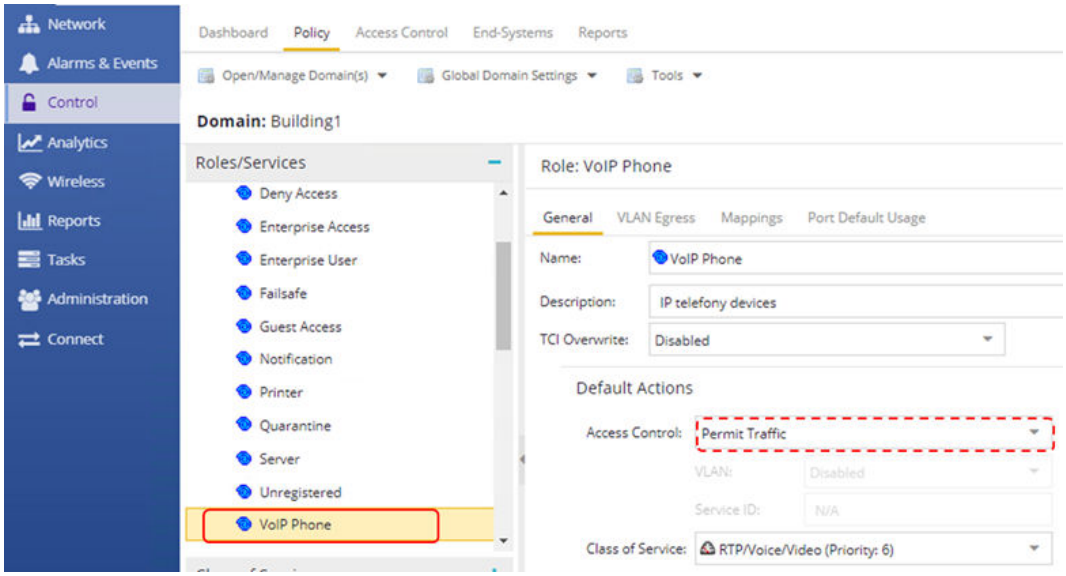


As shown below, the following changes are made to the Building1 and Building2 policy domains.

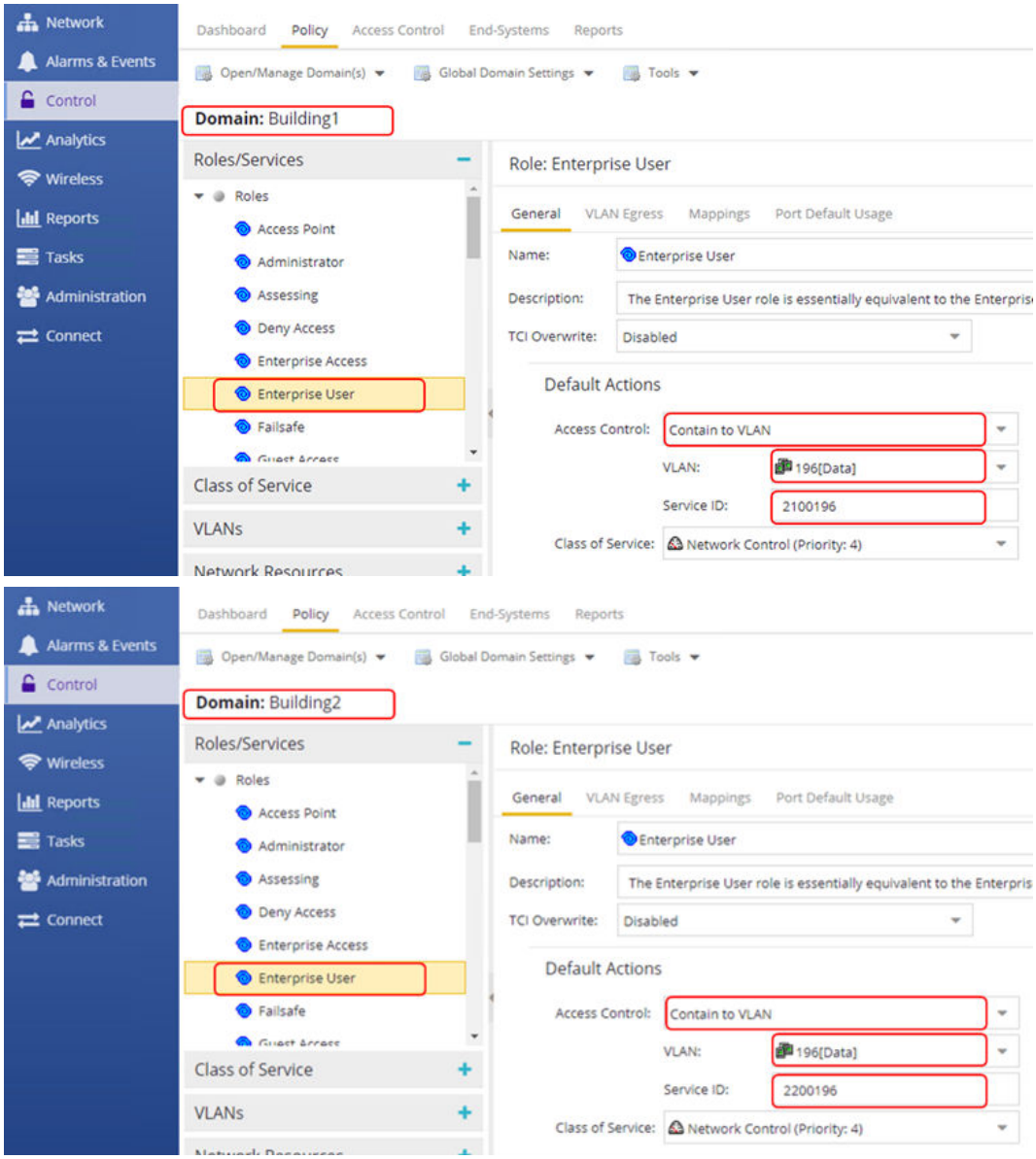
For the **Access Point** policy role, only the I-SID value is changed, and the VLAN-id is the same for both locations. Also, the **AP Aware** parameter is left at the default value of **Enabled**. This setting enables Extreme Control to send the necessary outbound attribute to enable MHSA (Multiple Host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



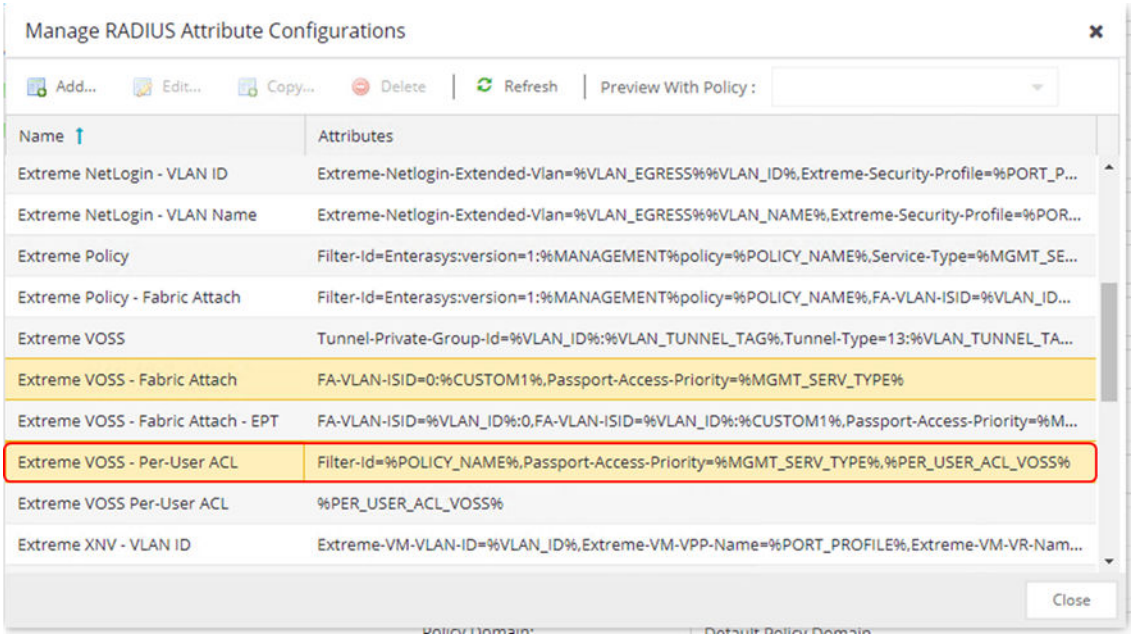
As shown below, the **VoIP Phone** policy role uses the same settings for both the Building1 and Building2 policy domains. Note, when RADIUS authenticating the phone, it is not necessary to provide the I-SID or VLAN values since these are signaled to the phone via LLDP and the auto-sense voice function.



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

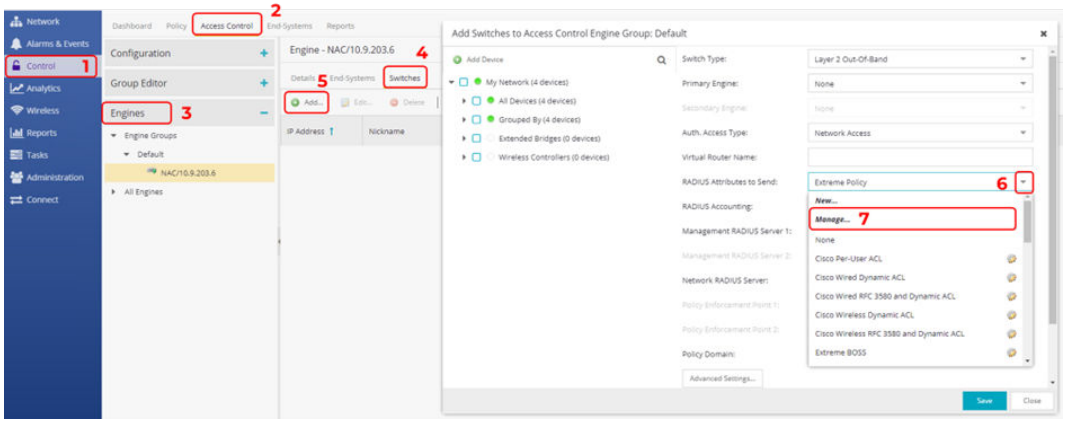


As of XIQ-SE 21.11 it is no longer necessary to configure a custom RADIUS attribute template. Default templates have been added for Policy and non-Policy NAC scenarios. The best practice is to use Policy to configure Radius outbound attributes. In the default templates shown below, for policy scenarios 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.



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.



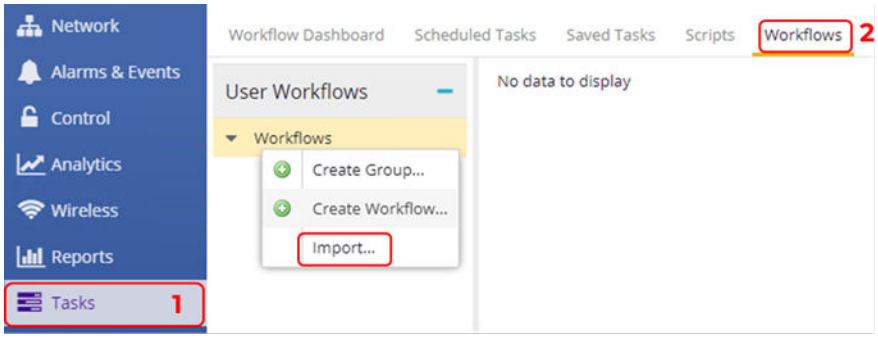
XIQ-SE: Script and Workflow Review

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

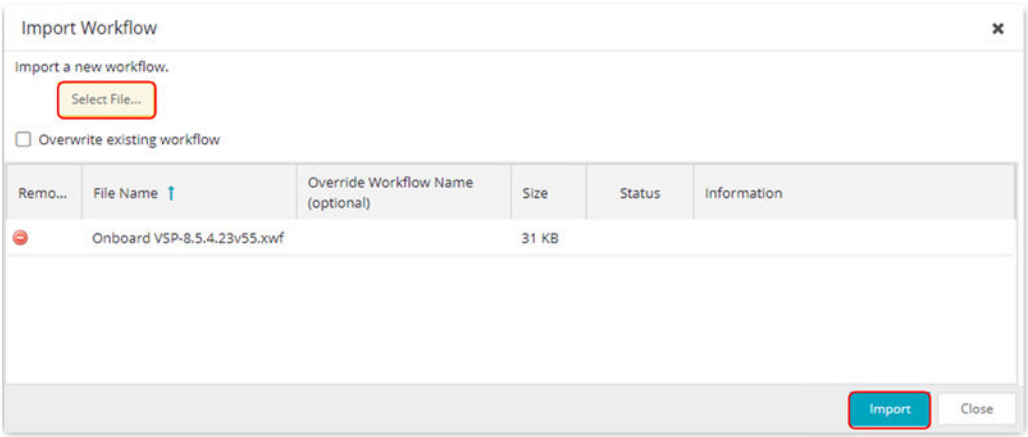
Name	Type	GitHub URL
Onboard Mgmt VLAN	Script	https://github.com/extremenetworks/ExtremeScripting/tree/master/XMC_XIQ-SE/oneview_workflows
Onboard Mgmt CLIP	Workflow	https://github.com/extremenetworks/ExtremeScripting/tree/master/XMC_XIQ-SE/oneview_workflows

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**.



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

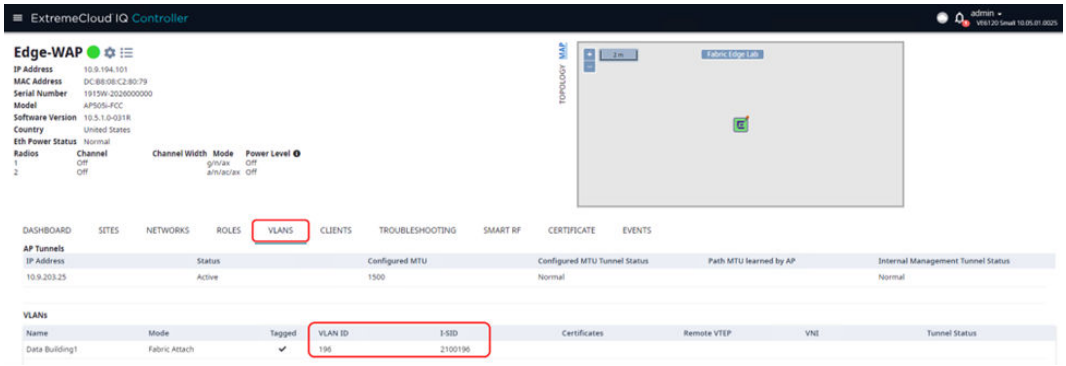


XIQ-C pre-existing configuration review

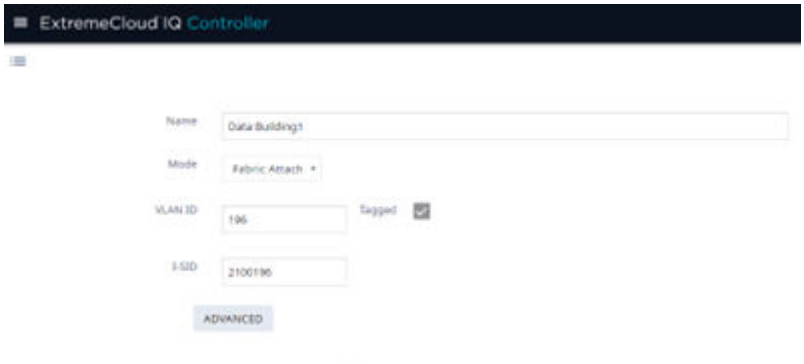
As an example, XIQ-C has already been configured with one site as shown below

With a single AP505.

With the following VLAN and Fabric Attach configuration.



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

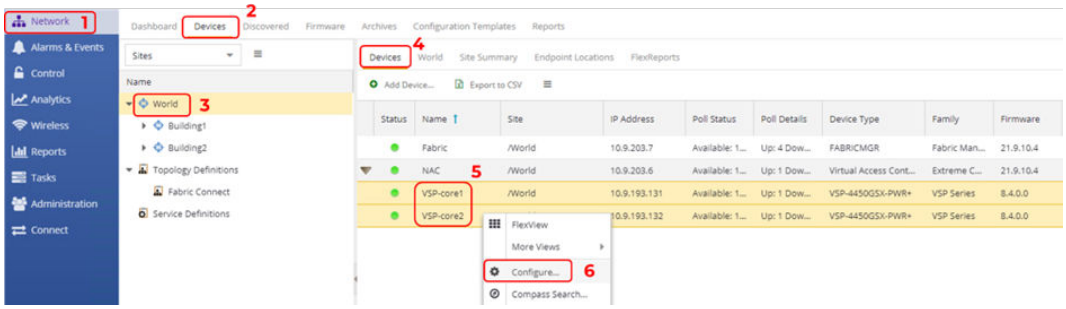


Prepare VSP/Fabric Engine Core Switches for Fabric Edge Deployment

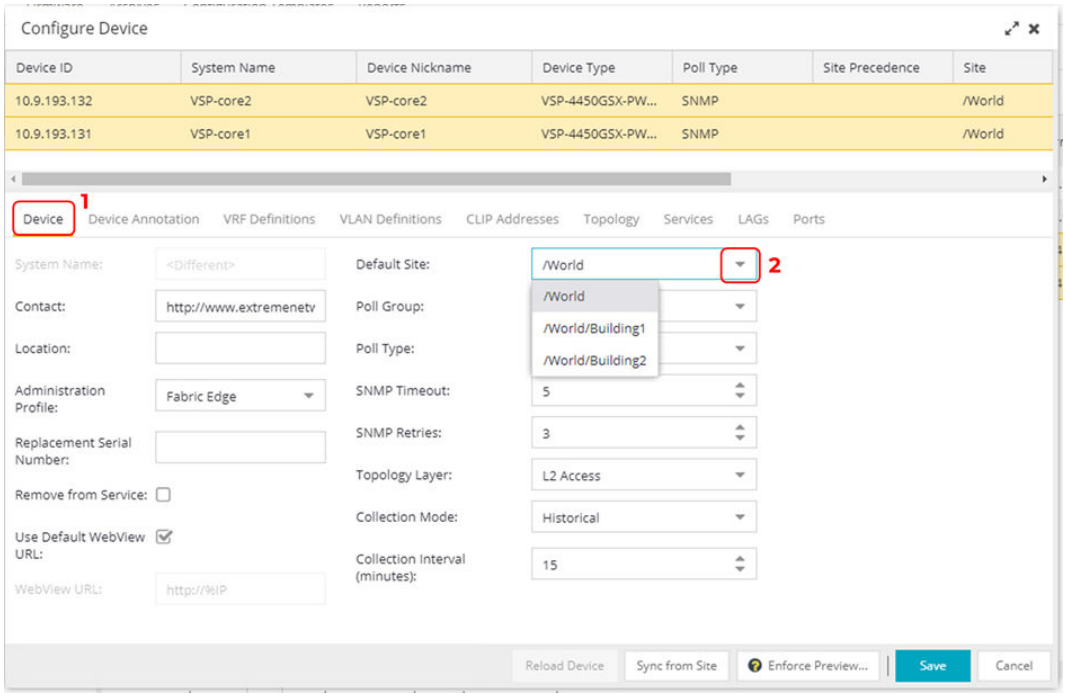
Site Selection for VSP Core Switches

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.

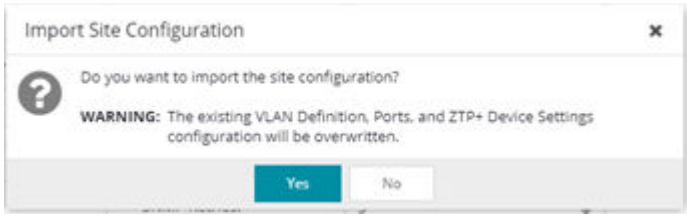
To add both core switches to Building1, select **Network** > **Devices** > **World** > **Devices**. Highlight both core switches, right click and select **Configure**.



Assign both switches to the World/Building1 site.

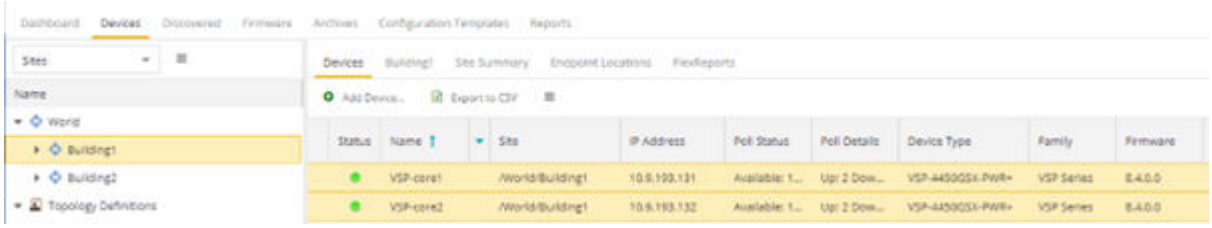


In the confirmation pop-up, select **Yes**.

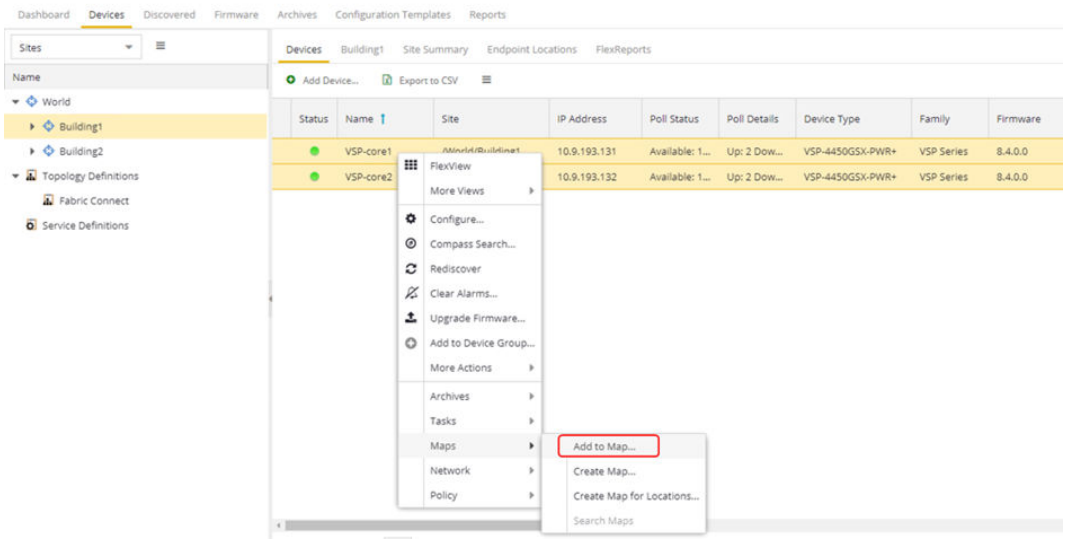


Then select **Save** to commit.

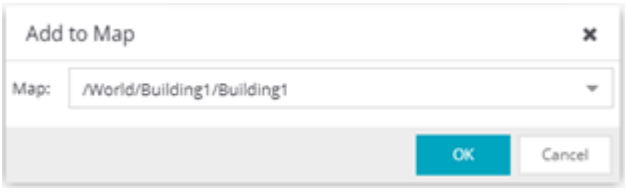
Now navigate to the Building1 site and make sure both core switches have been added.



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



Select the Building1 site map and then **OK**.



Both core switches have now been added to the map.

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

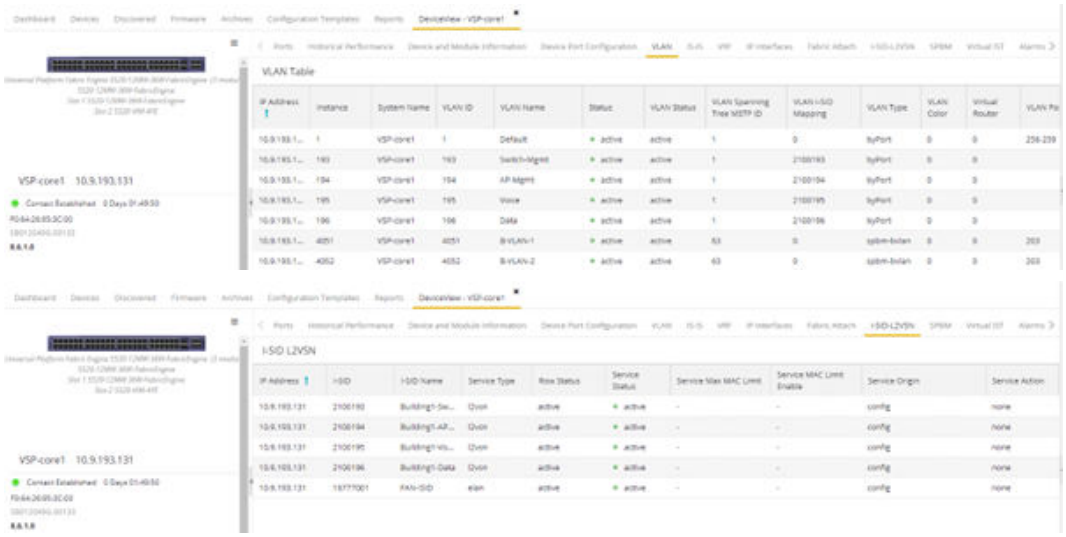
VSP-core1

```
enable
config term
dvr isolated controller 1

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

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

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

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

dvr controller vrrp-on-dvr-isids enable
slpp enable
end
```

VSP-core2

```
enable
config term
dvr isolated controller 1

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

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

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

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

dvr controller vrrp-on-dvr-isids enable
slpp enable
end
```

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



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.

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

   The VSP/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

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

VSP-core2

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

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.

Optionally, on both VSP-core1 & VSP-core2

```
enable
config term
auto-sense isis hello-auth type hmac-sha-256 key <user-defined-key>
end
```

Prepare XIQ-SE for VSP/Fabric Engine Edge Deployment

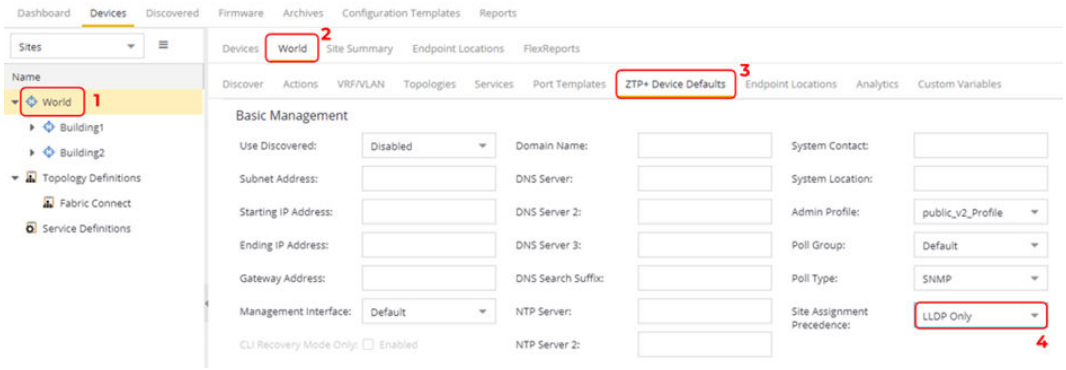
ZTP+ Configuration on page 32
XIQ-SE Workflow Configuration for VSP Onboarding on page 36

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**.

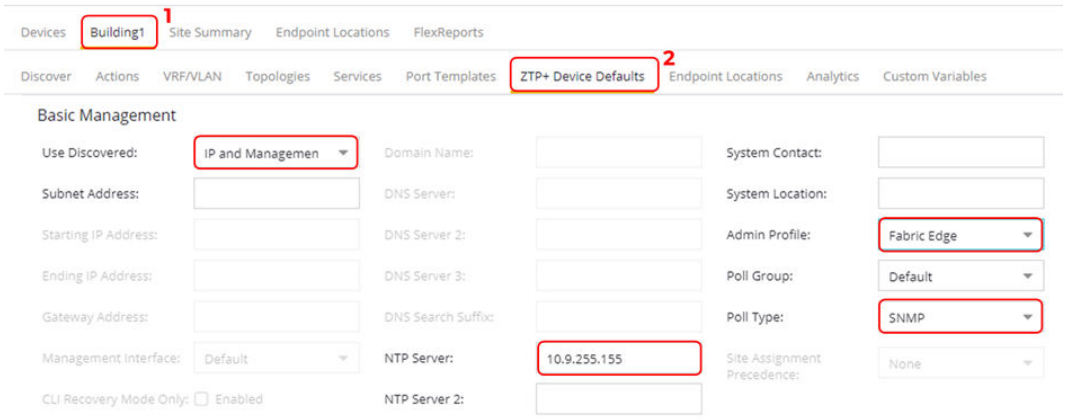
Set the **Site Assignment Precedence** drop-down to **LLDP Only** and then click **Save**. With this setting, XIQ-SE assigns the edge switches to a site based on the LLDP neighbor table found on the switches being onboarded. Because the VSP core switches are in Building1, the edge switches are assigned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



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.

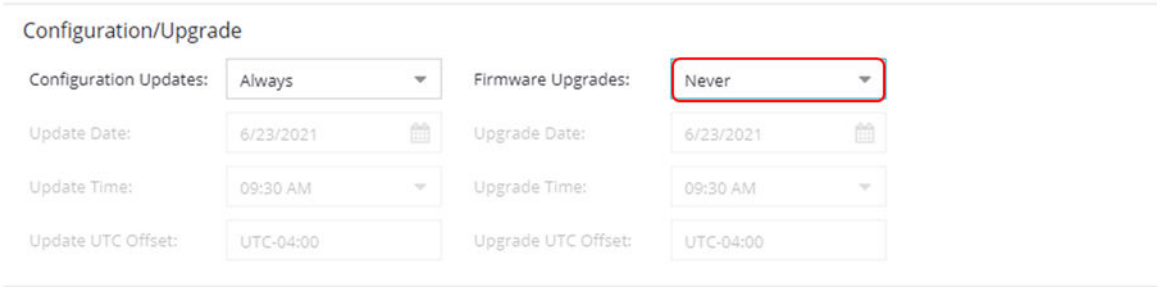
Under **Basic Management**, set options as follows:

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

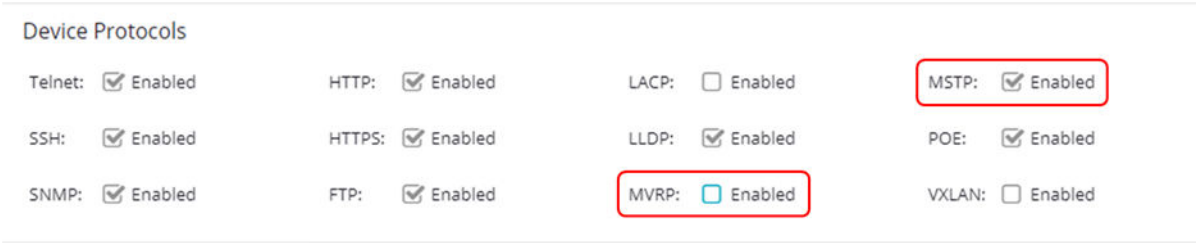


With the **Use Discovered** parameter set at **IP and Management**, ZTP+ uses the same IP address and Management interface used during the onboarding process. Later in the guide, there are steps to move the Management interface to a VLAN interface or CLIP interface.

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 **Never.** 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.

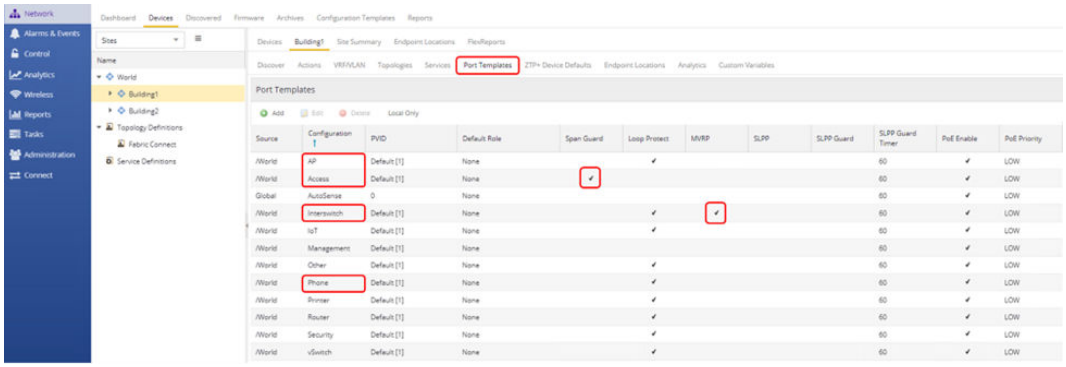


Scroll down to the **Device Protocols** section and uncheck **MVRP**. The rest can be left as is, and MSTP must remain enabled. Note that the Telnet, HTTP, and HTTPS protocol options only work as of VOSS 8.4. All protocol options work with EXOS/Switch Engine and are applied when the Universal Edge switch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



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

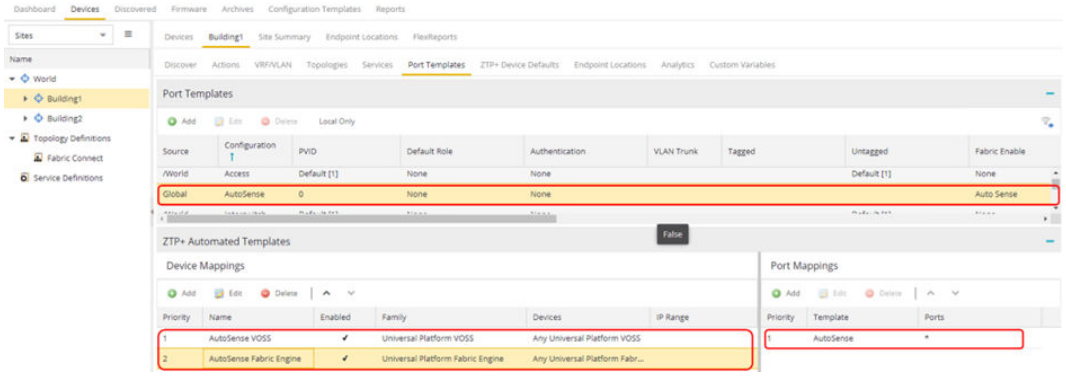
Disable MVRP because ZTP+ tries to apply the default port templates during switch onboarding. These default port templates are listed under the **Port Template** tab as shown below.



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:

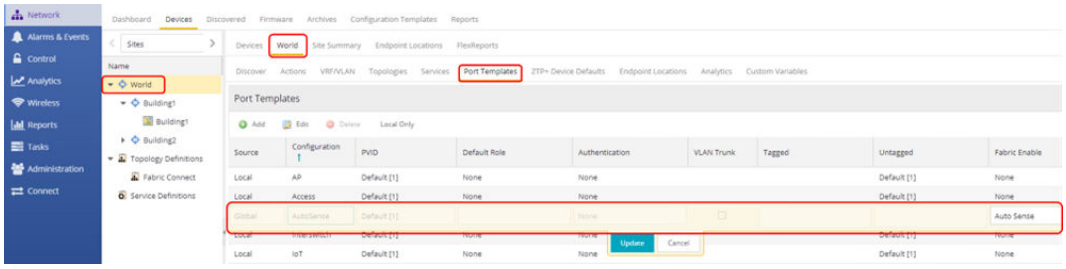


The Auto-Sense ZTP+ Template entry overrides the automatic application of the default port templates described above.

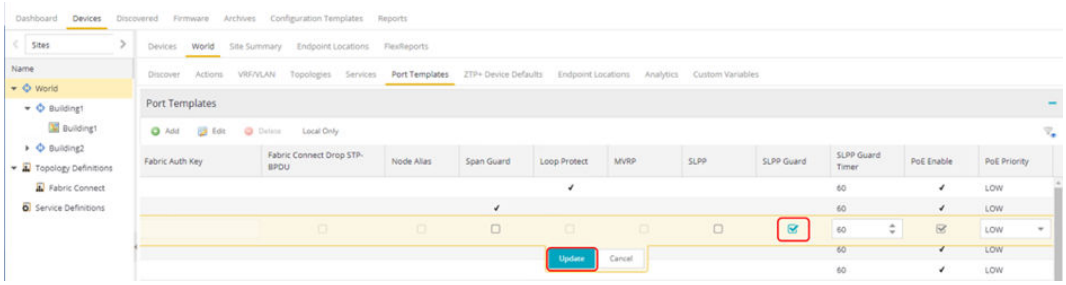
Note that the Auto-Sense ZTP+ Template entry exists only for new sites created in XIQ-SE 21.9 or later. If an older version of XIQ-SE or XMC was used to create the site, the template entry does not exist and needs to be created manually (or the site deleted and re-created).

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.



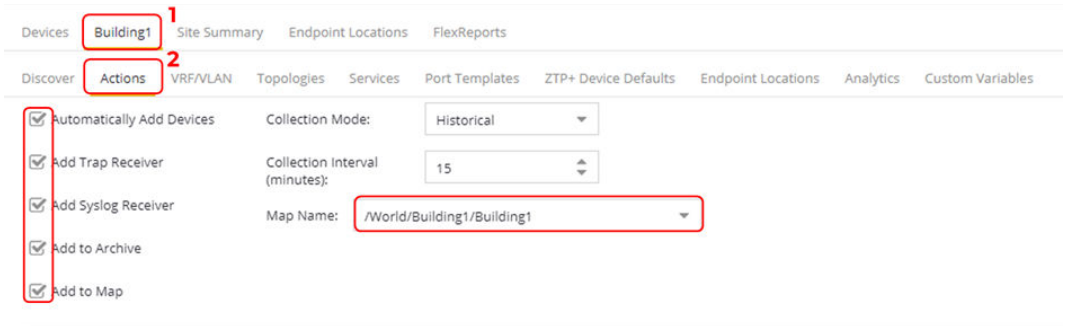
Scroll right, until the **SLPP-Guard** option is visible. Click the box, click **Update** and click **Save**.



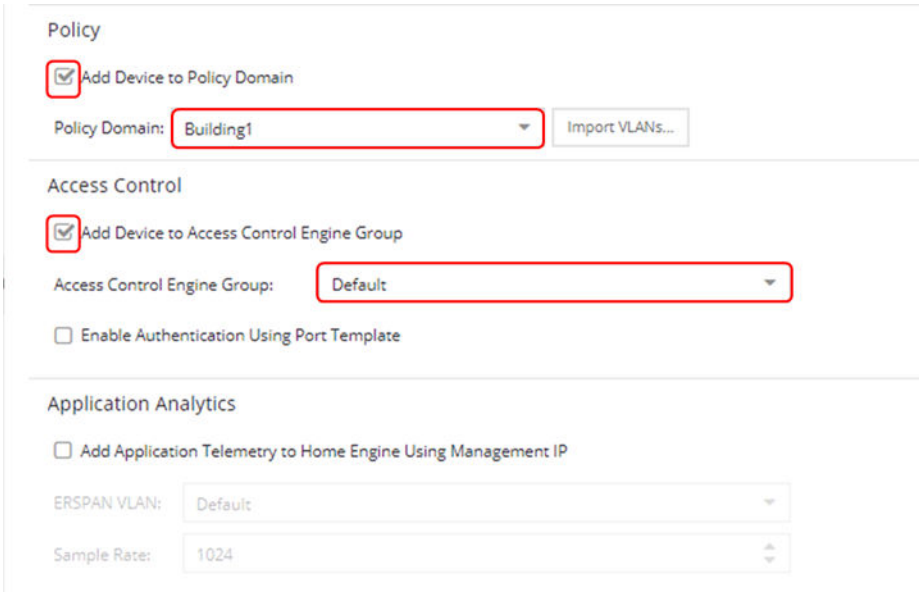
Configuration of Site Actions

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)



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.



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.

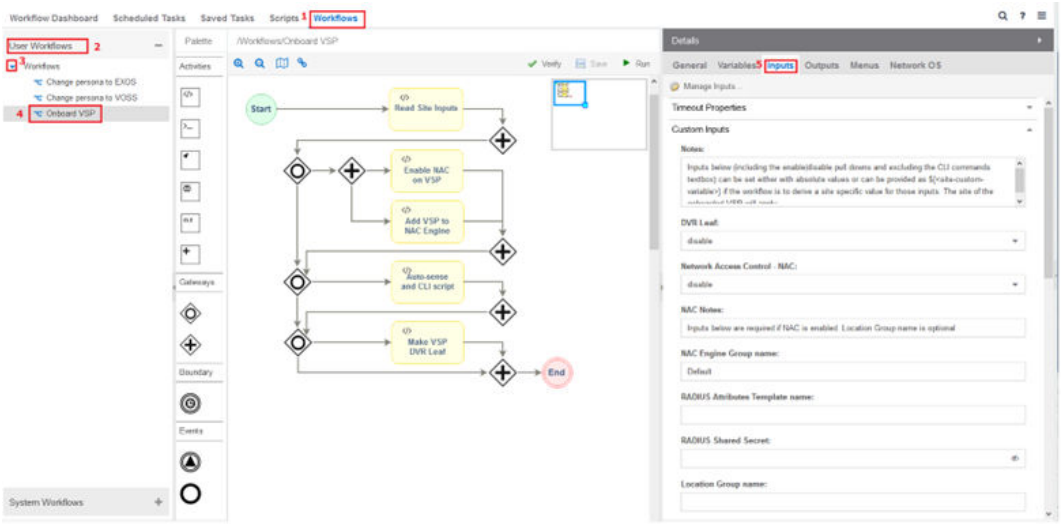
Step 1 is possible as of XIQ-SE 22.3 under **Site Actions**, and should always use either the *Extreme VOSS - Fabric Attach* or *Extreme VOSS - Per-User ACL* RADIUS attribute templates, depending on whether the switch is also being added to a Policy domain or not. This however only works properly as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



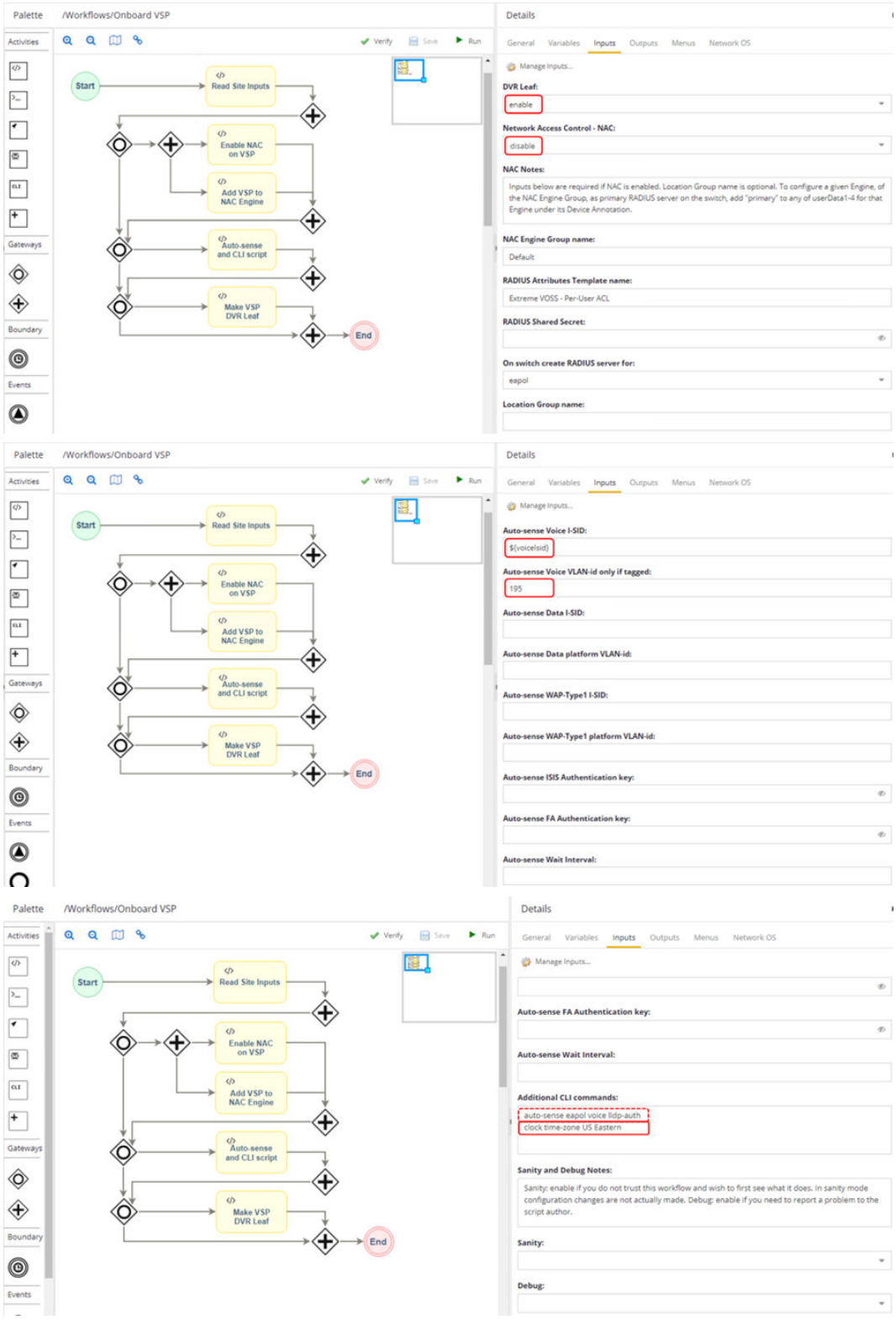
Provide the following inputs:

- 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: **${voiceIsid}**
- 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

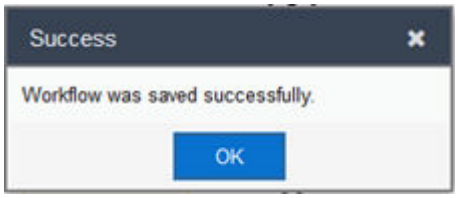
- clock time-zone US Eastern

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

Note
The ${voiceIsid} variable is case-sensitive.



Save the modified workflow and click **OK**.

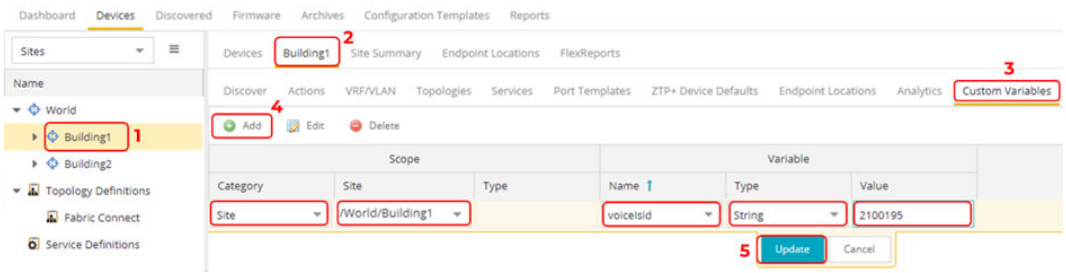


Note that for the Voice I-SID, the absolute value is not provided but is referenced as a variable in the format ${<variable-name>}. This is because these inputs are site-specific and vary based on the site where the edge switches are onboarded.

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 *voiceIsid* values for each site.

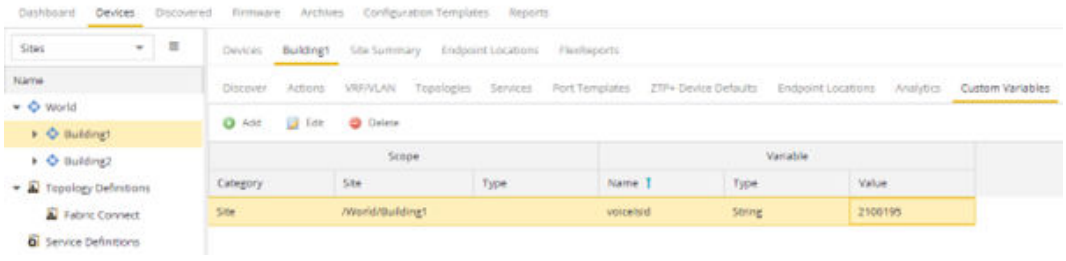
Site	*voiceIsid*
Building1	2100195
Building2	2200195

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



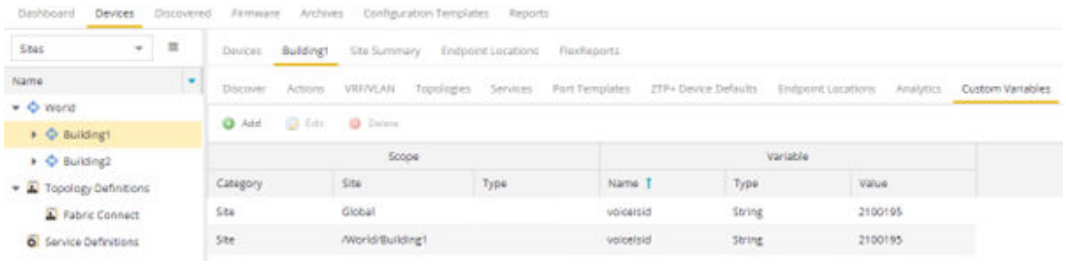
Note
The variable name is case-sensitive. Make sure to enter it correctly.

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



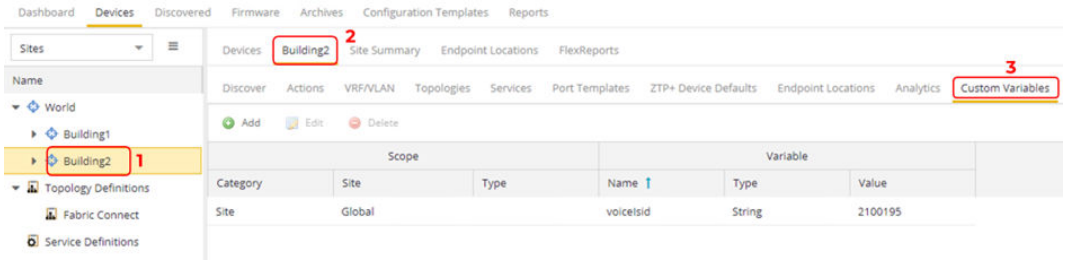
Select **Save** to save the variables.

When you are done, the table 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.

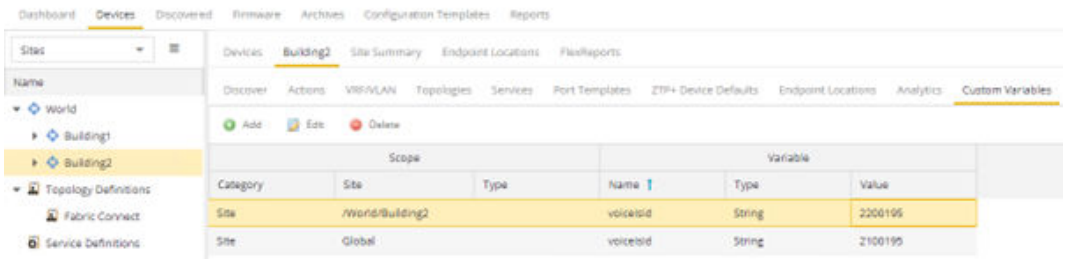


In a typical customer multi-site deployment, repeat the above steps for each site. The steps for the Building2 site are shown below.

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



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.



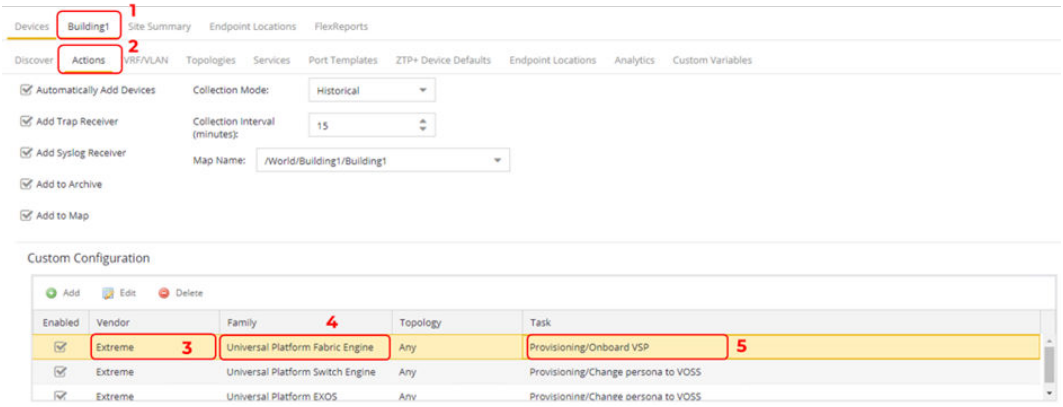
Select **Save** to save the variables for Building2.

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.



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

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

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+

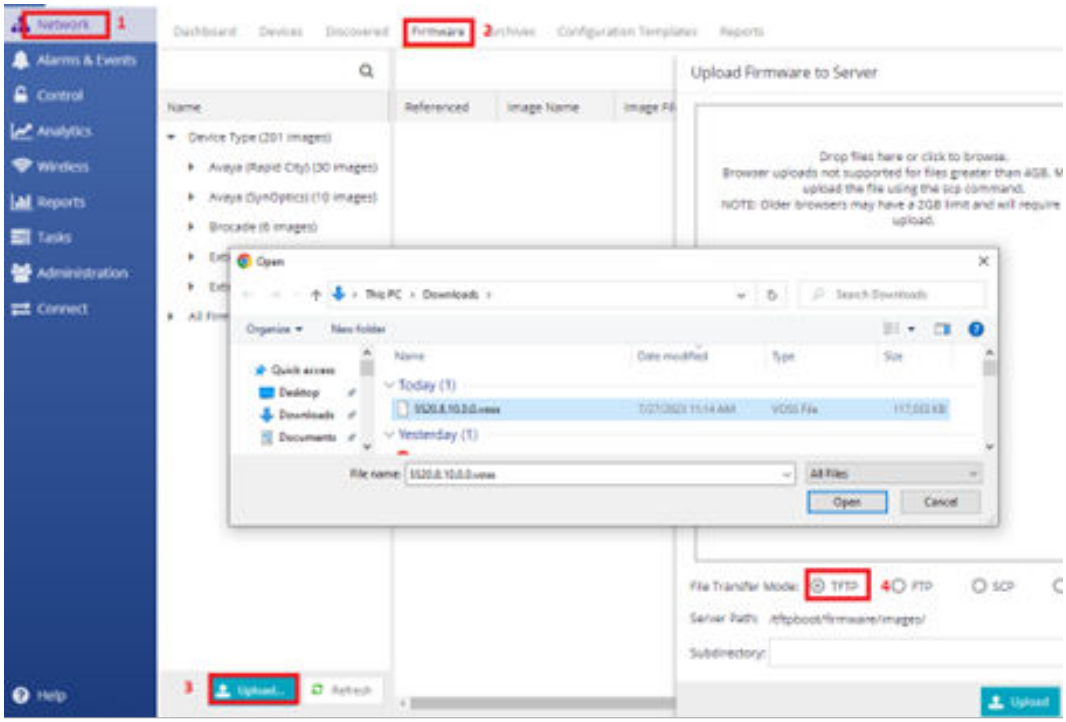
Note
If using 25G or 100G uplink ports to the existing Fabric core, the default Forward Error Correction (FEC) settings are different between Switch Engine and VSP/Fabric Engine. Therefore, before the Switch Engine switch can be onboarded, the

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

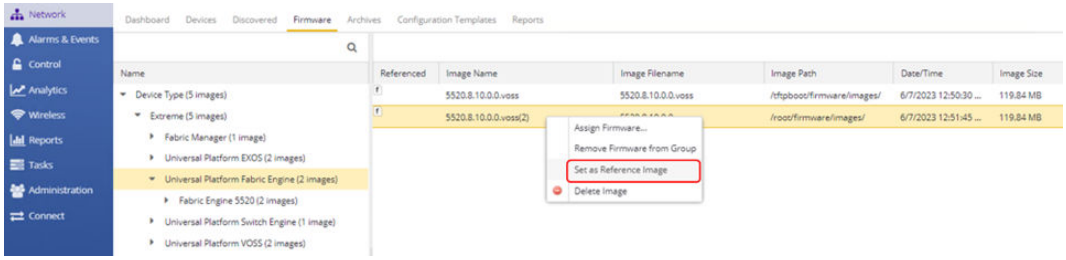
The Fabric Engine image must be uploaded to XIQ-SE twice; the first time using the TFTP transfer mode, and the second time using the SFTP transfer mode.

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.

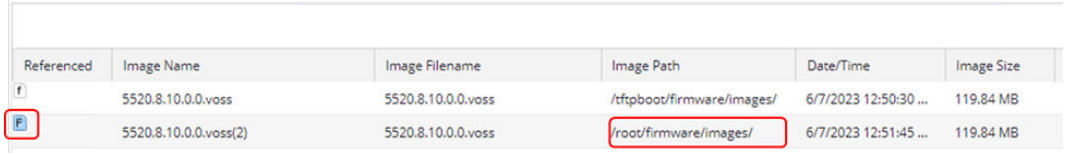
To upload the Fabric Engine image using SFTP, repeat the previous step, but select SFTP as the **File Transfer Mode**. The image is uploaded to the `/root/firmware/images` directory.



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.



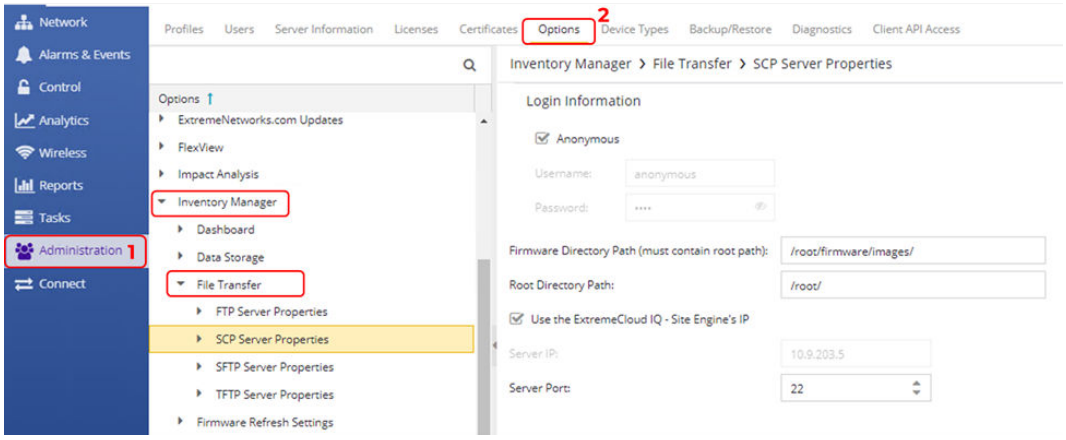
The referenced icon turns blue.



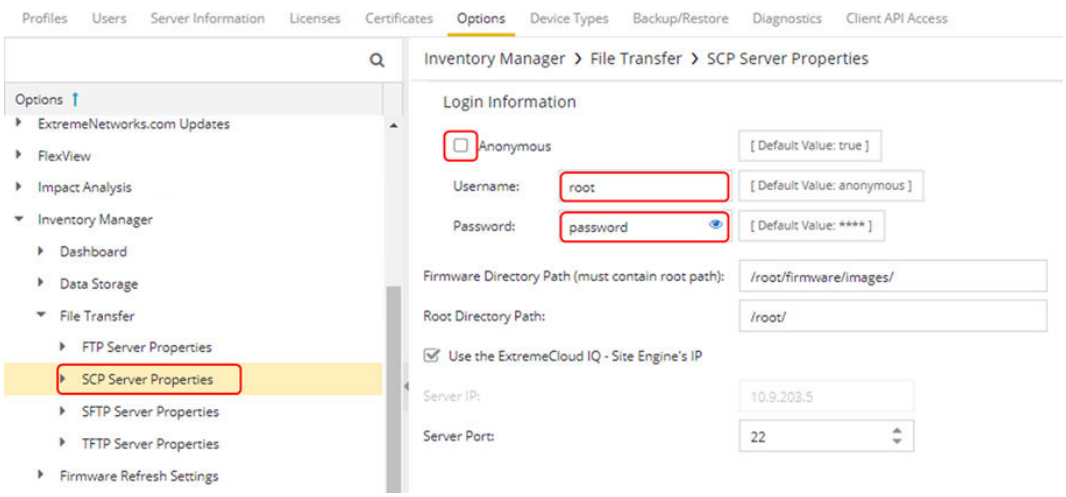
Referenced	Image Name	Image Filename	Image Path	Date/Time	Image Size
f	5520.8.10.0.0.voss	5520.8.10.0.0.voss	/tftpboot/firmware/images/	6/7/2023 12:50:30 ...	119.84 MB
F	5520.8.10.0.0.voss(2)	5520.8.10.0.0.voss	/root/firmware/images/	6/7/2023 12:51:45 ...	119.84 MB

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.

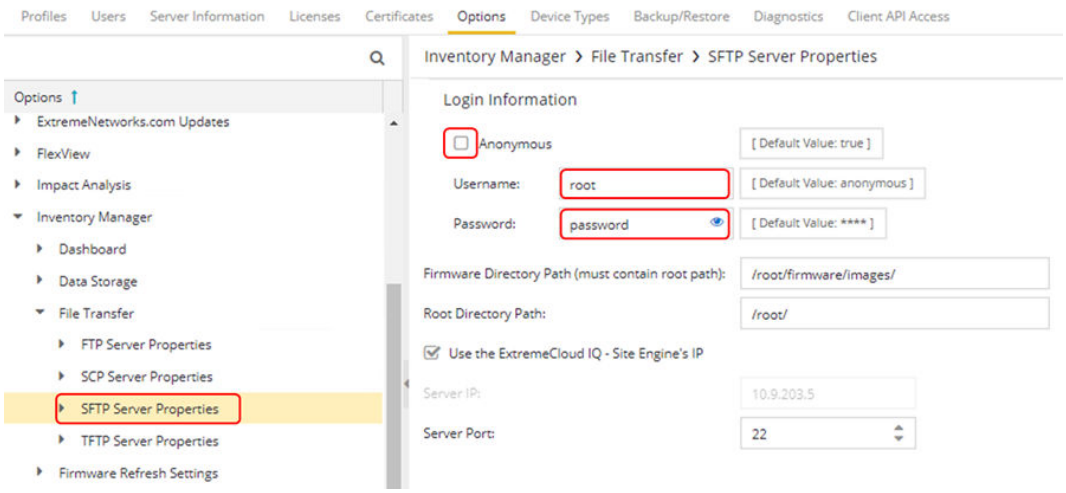
Select **Administration** > **Options** > **Inventory Manager** > **File Transfer** > **SCP Server Properties**.



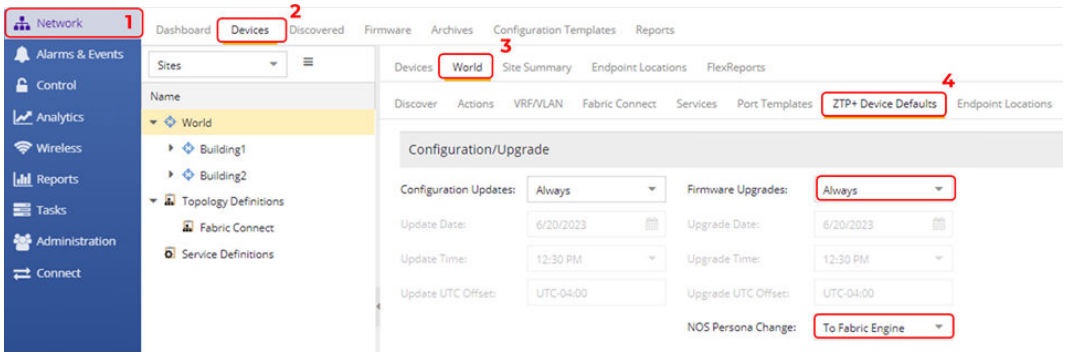
Disable Anonymous and specify the username and password for the SCP/SFTP server. You must set the username to `root` and then set a password. Here we set it to `password`. Click **Save**.



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



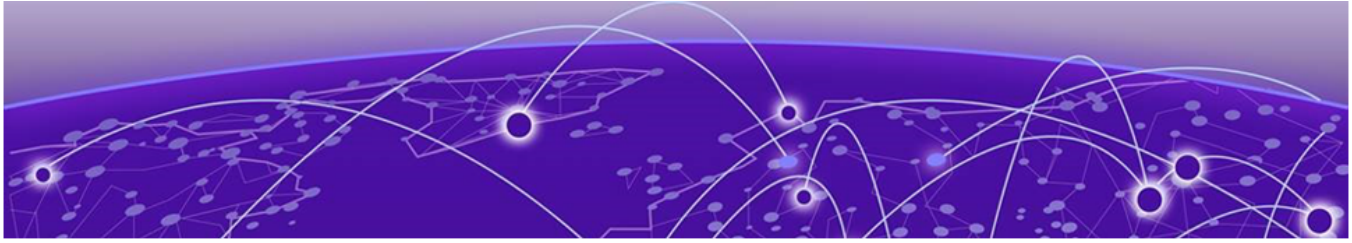
To Enable the ZTP+ OS conversion in XIQ-SE. Select **Network** > **Devices** > **World** > **ZTP+ Device Defaults**'



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

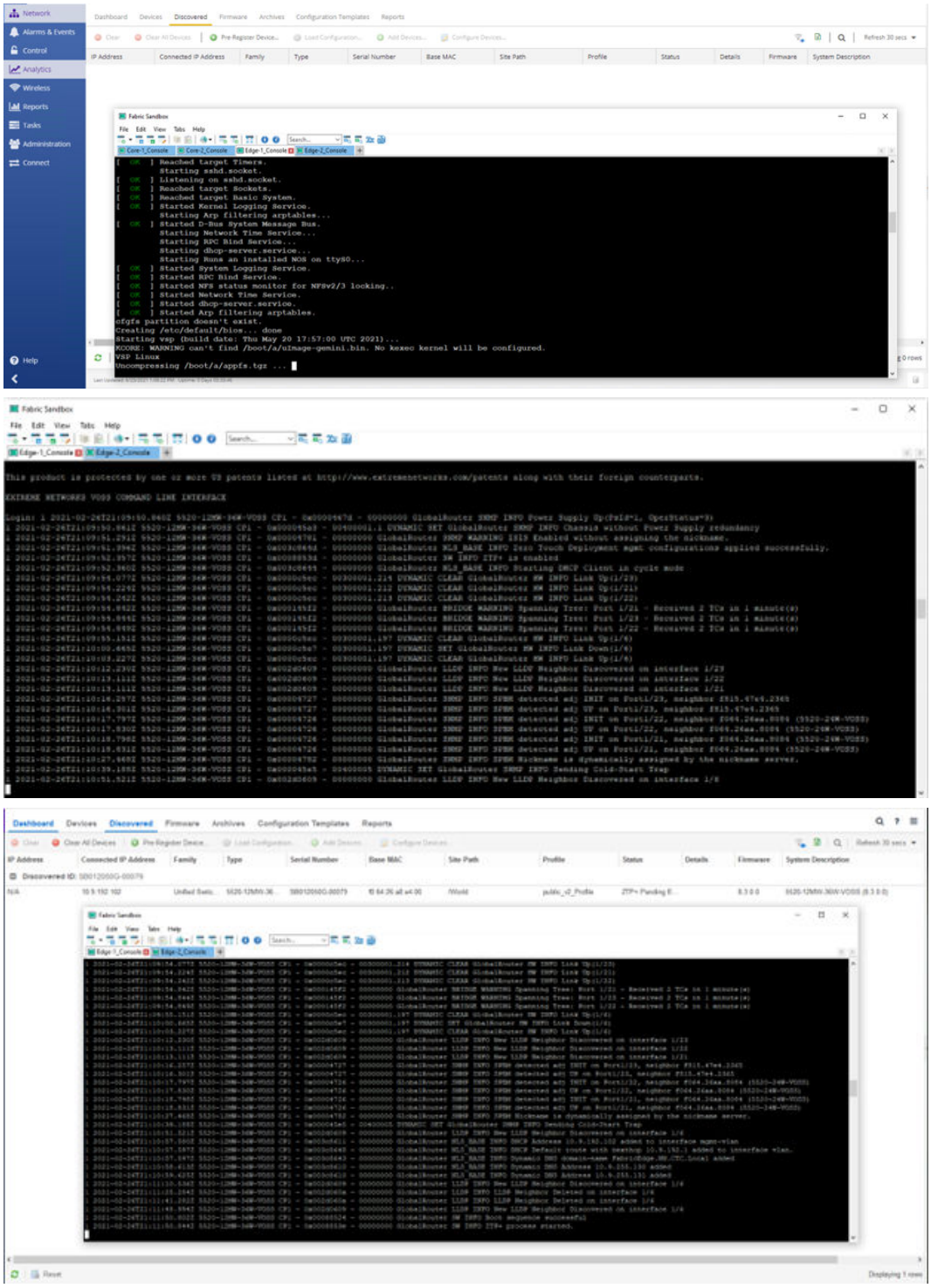
In previous topics, XIQ-SE was provisioned for the automated onboarding of the Fabric Engine edge switches. To initiate the onnboarding process, install each of the edge switches, apply power, and connect at least one edge switch to an existing Fabric Connect core. As mentioned previously, each edge 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:

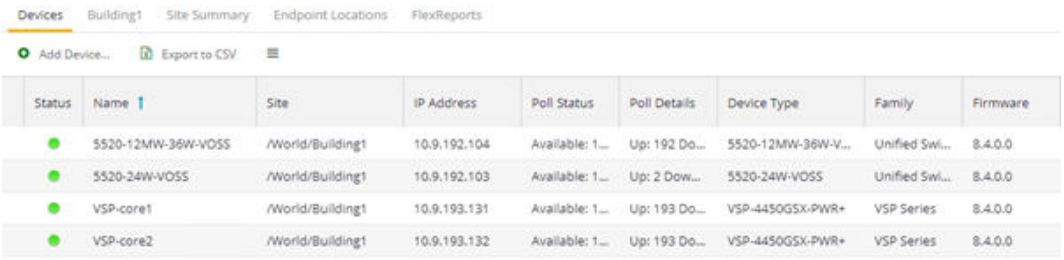
1. ISIS adjacency forms with neighboring core switches.
2. A nickname is dynamically assigned by Nickname servers on the core switches.

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.

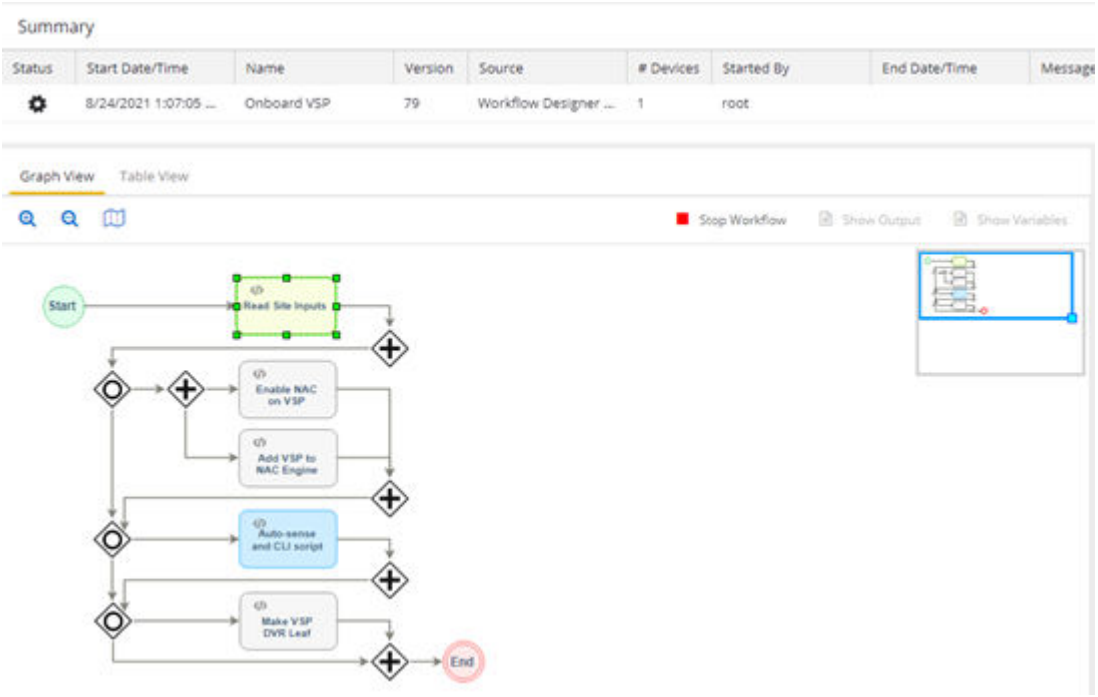
When the onboarding process completes, the VSP edge switches are placed into the correct site (Building1) and topology map.



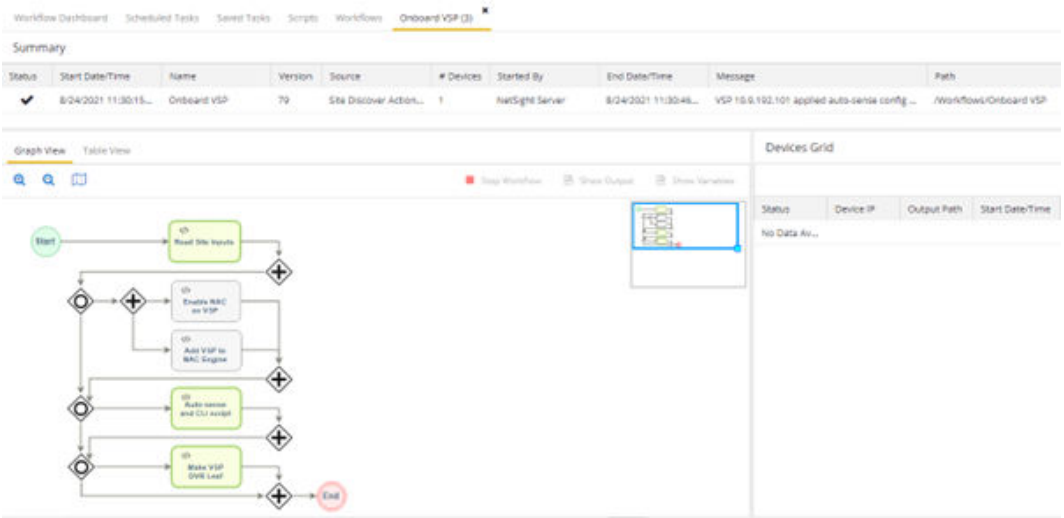
If you were to observe the edge switch console, you would see a number of SSH connections coming into the newly onboarded switch. Some of these are XIQ-SE performing the site actions, such as adding XIQ-SE as Trap and Syslog receiver on the switch, and some are the *Onboard VSP* workflow performing the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



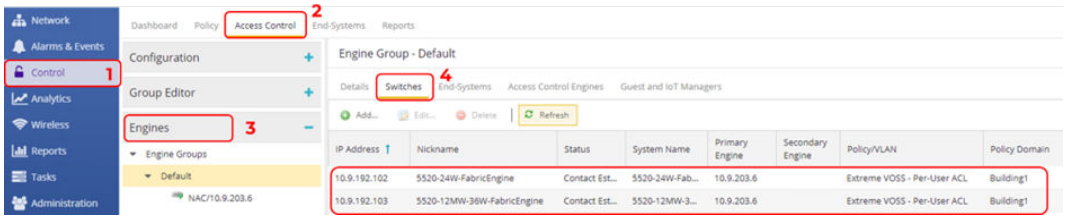
If no active workflows are running, set the drop-down to **Historical** and locate the most recently run of the *Onboarding VSP* workflow. Double click on the workflow to view the execution details.



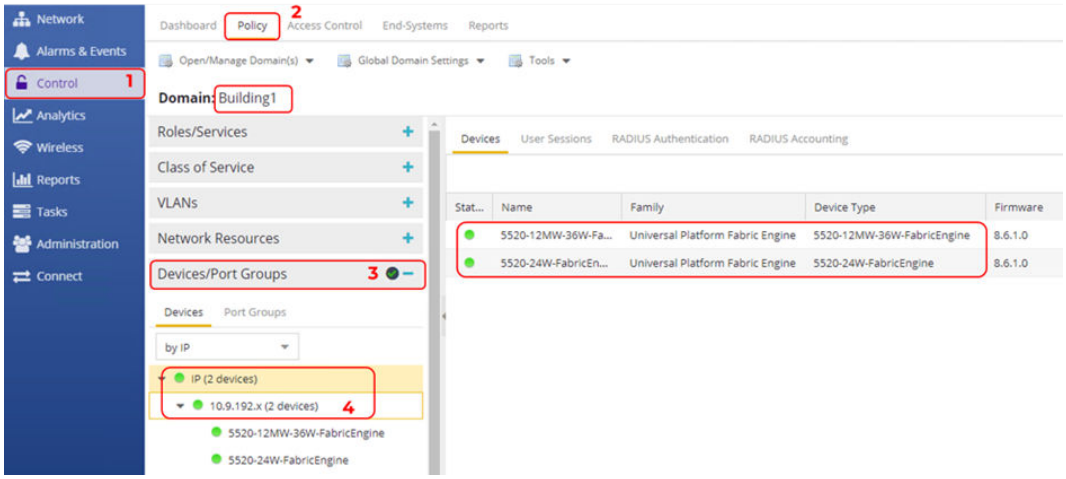
Note that the last activity of the *Onboarding VSP* workflow converts the VSP switch to a DVR Leaf and reboots the switch one last time.

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.



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

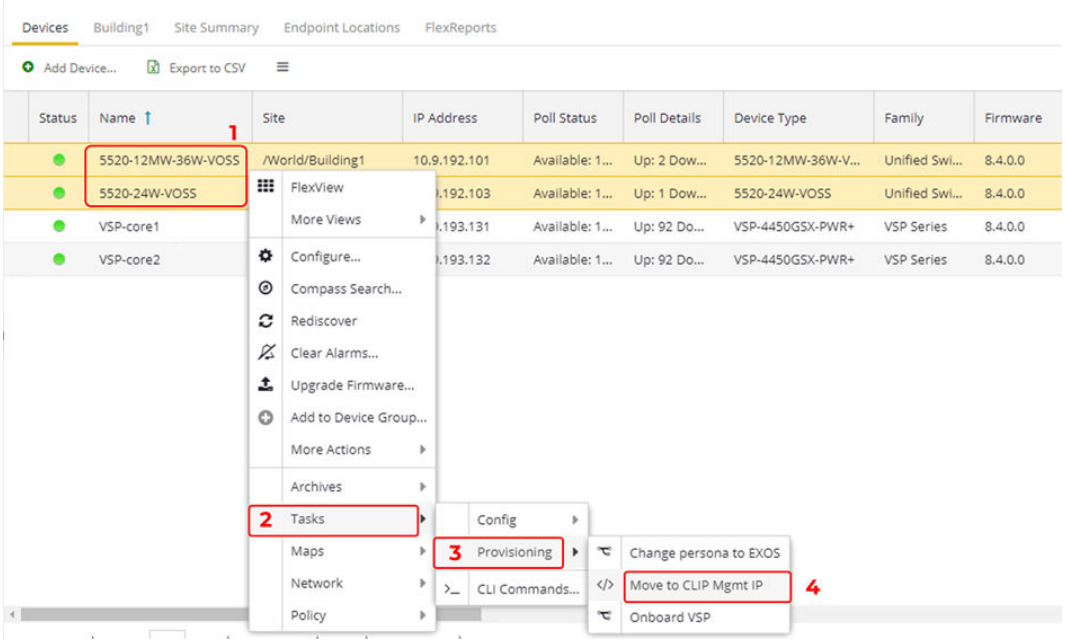


SSH into the VSP edge switches and use the CLI command `show dvr` and verify that the DVR Role is shown as *Leaf*.

Migrate VSP Edge to Dedicated Switch Management CLIP

The VSP edge switches 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.

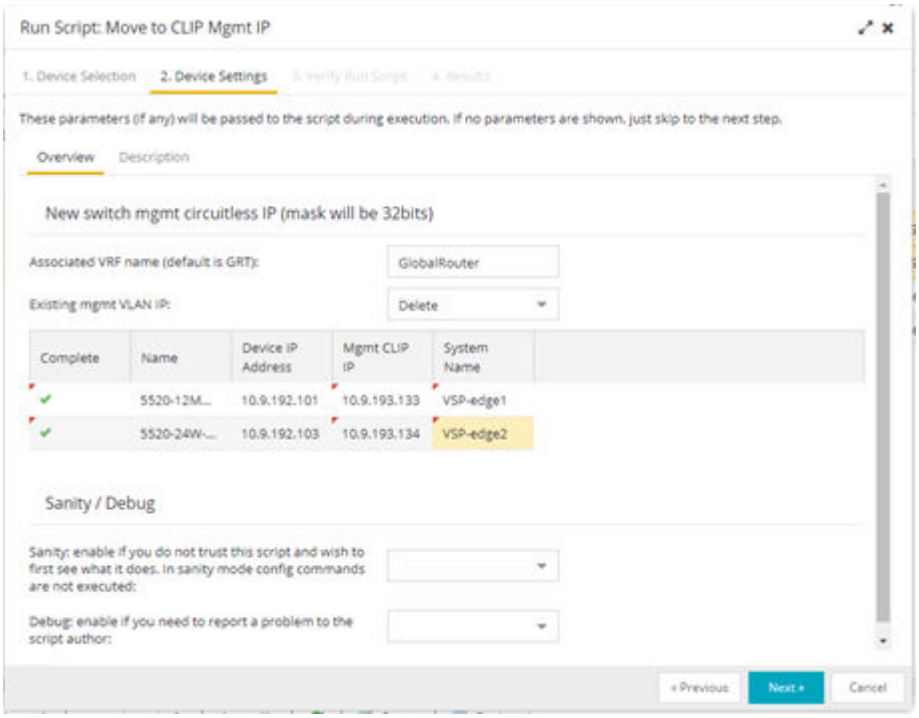
To run the script, select both VSP edge switches, right-click, and select **Tasks** > **Provisioning** > **Move to CLIP Mgmt IP**.



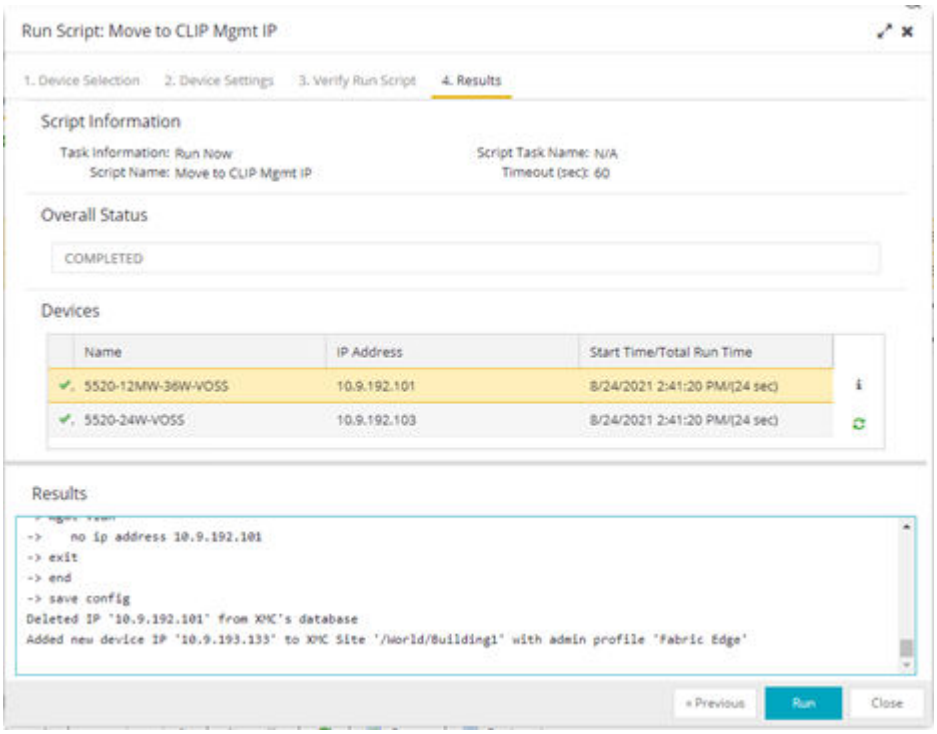
In the script input window, provide the CLIP IP address for each VSP-edge switch. Use the following CLIP addresses.

- VSP-edge1 **10.9.193.133**
- VSP-edge2 **10.9.193.134**

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

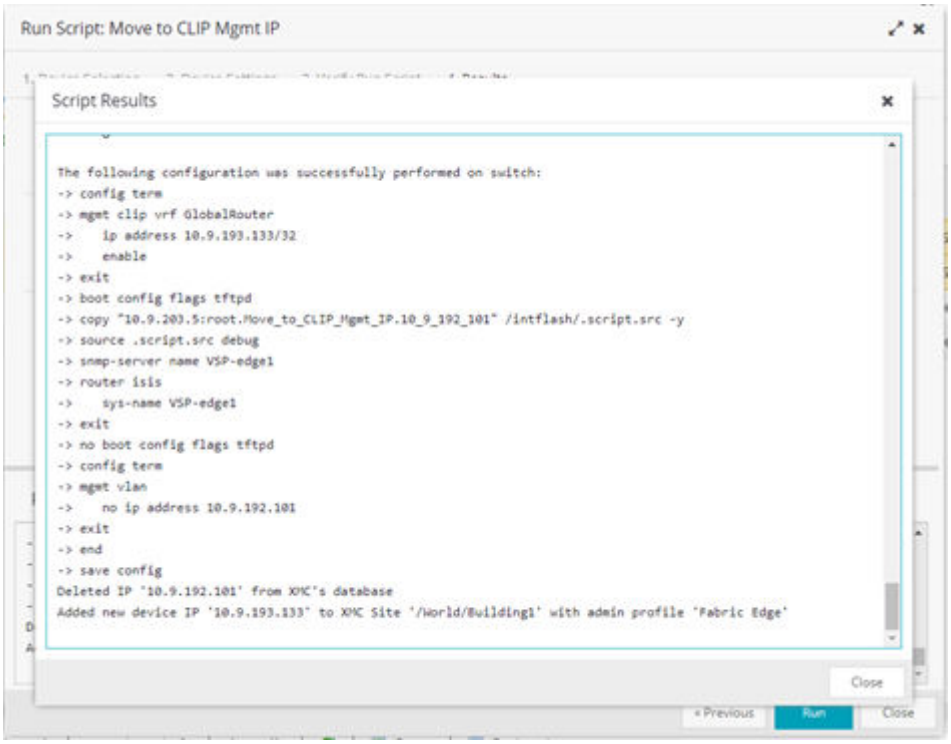


Click **Next**, then click **Run**.



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.

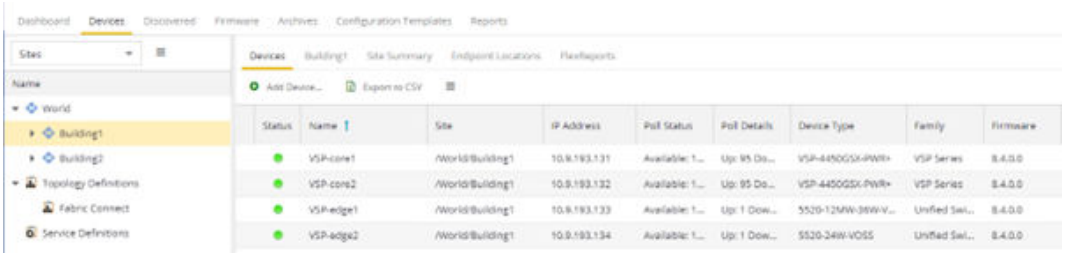
When the script has completed, expand the **Results** window by clicking the **i** button.



Repeat these steps for the other VSP edge switch.

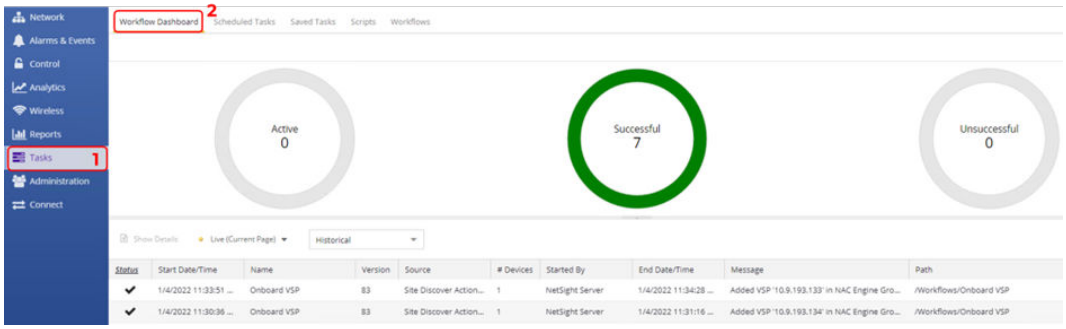
Confirm that all four VSPs have their correct management IP.

Click **Refresh** if necessary.

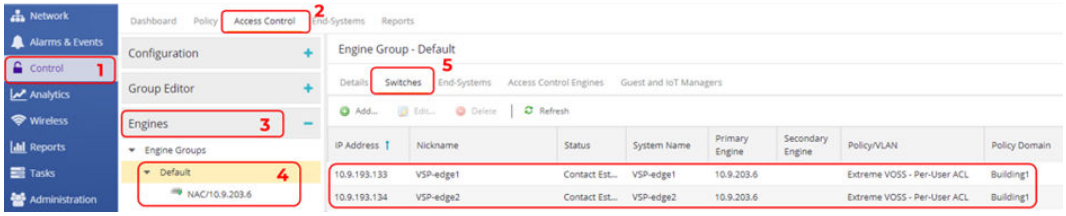


Note
Running the *Move to CLIP Mgmt IP* script also executes the *Onboard VSP* workflow one more time. During the worlflow execution, the new management CLIP IP address is added to XIQ-SE Control.

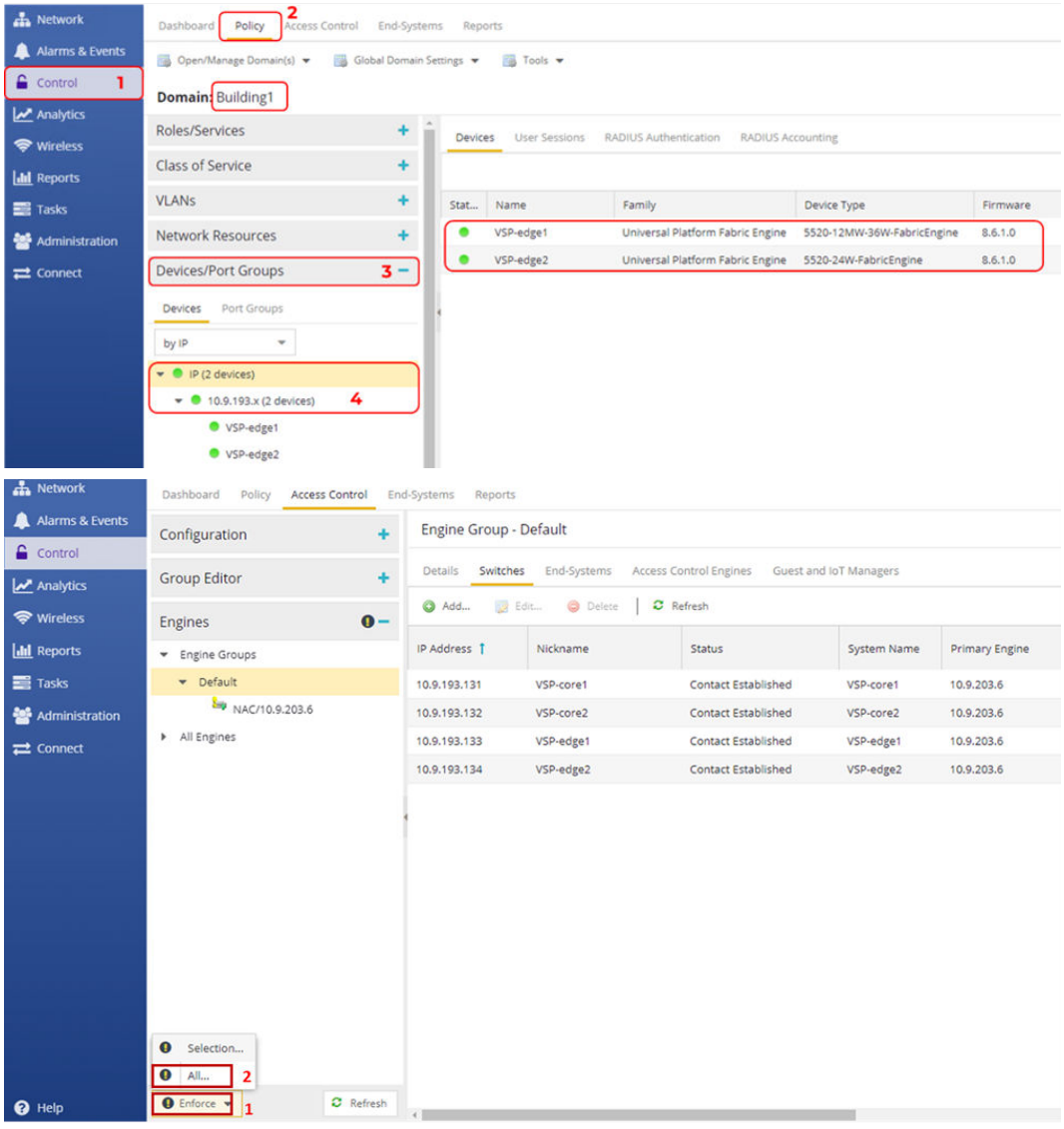
Verify the workflow execution for the new switch IPs under **Tasks** > **Workflow Dashboard**.



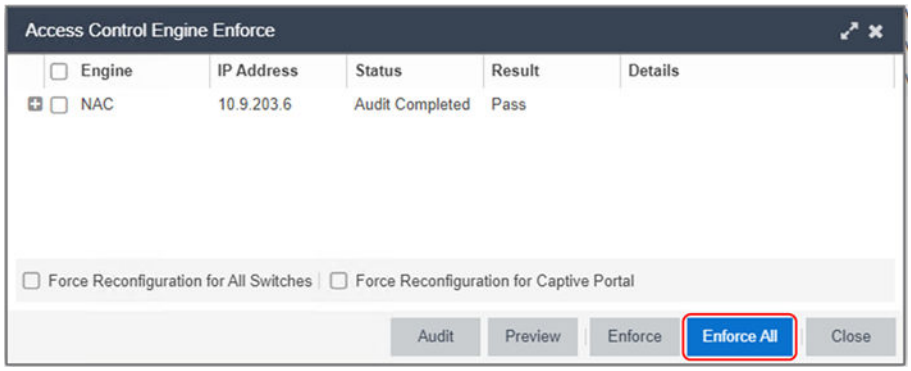
In XIQ-SE Control, verify that all switches have been added with the correct IP addresses as shown below.



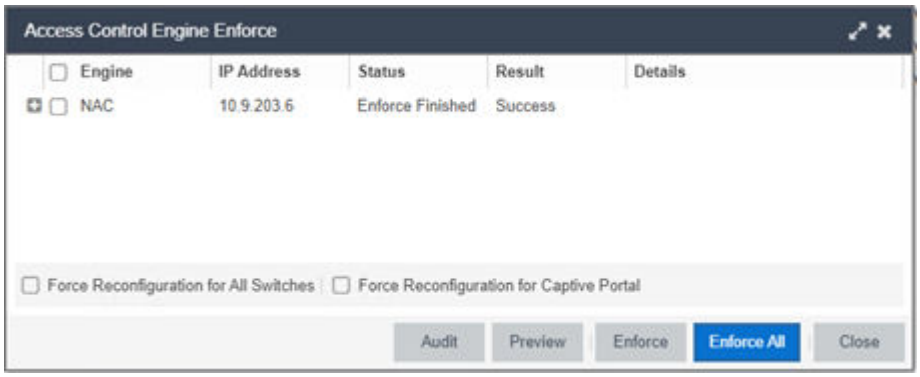
Verify that VSP Edge switches have been added to the **Building1 Policy** domain.



Then click **Enforce All**.

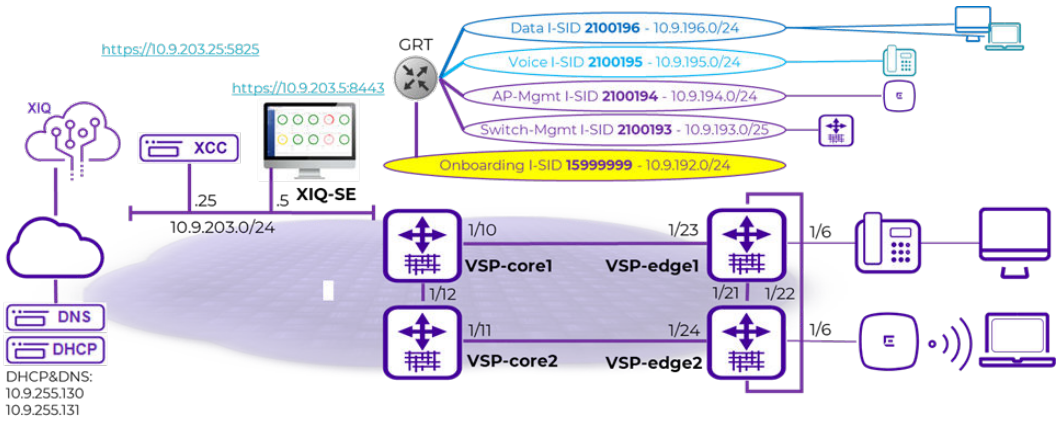


When the enforce has completed, close the window.

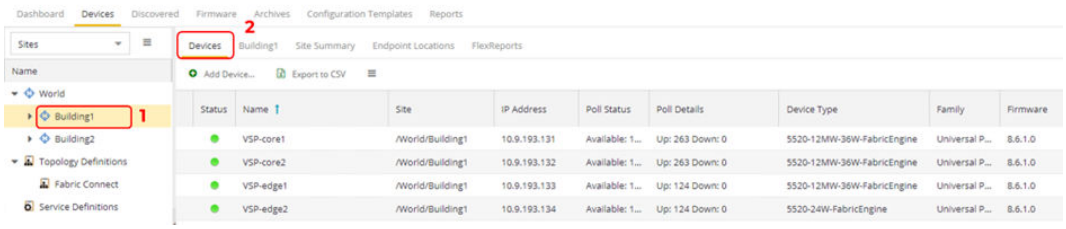

Access Control Engine Enforce
Engine
IP Address
Status
Result
Details
NAC
10.9.203.6
Enforce Finished
Success
Force Reconfiguration for All Switches
Force Reconfiguration for Captive Portal
Audit
Preview
Enforce
Enforce All
Close

Verify All End Devices Are Operational

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.)

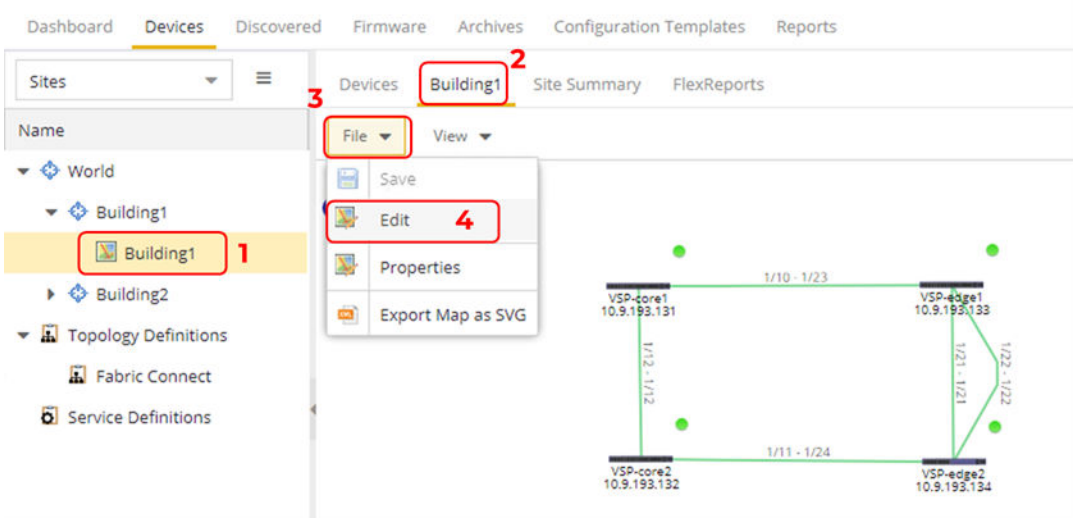


Inspect the VSP Fabric

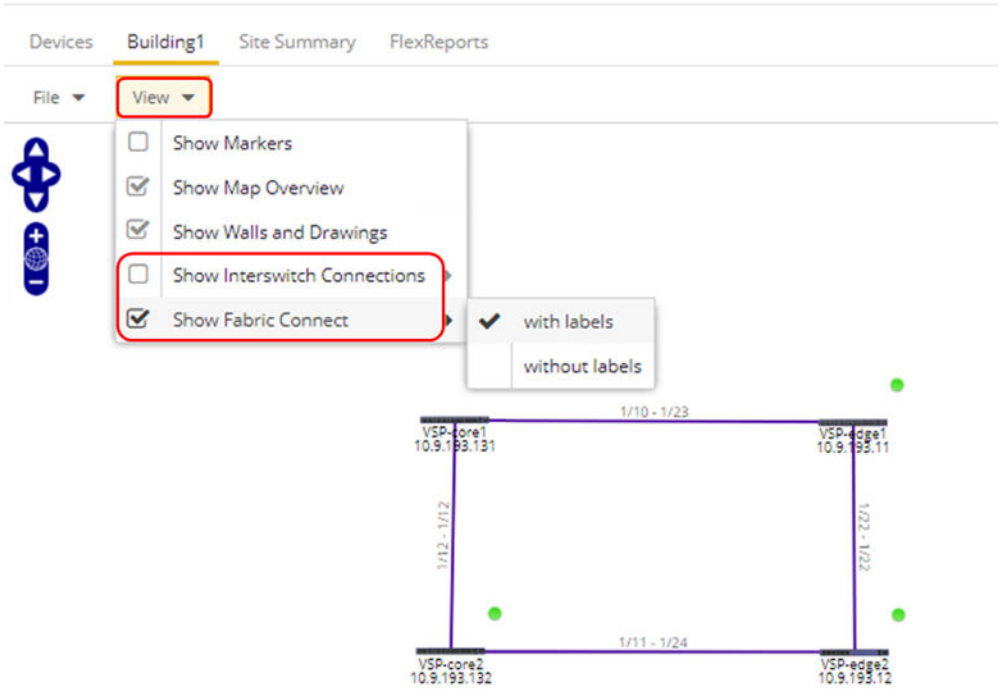


The Fabric Edge is now deployed.

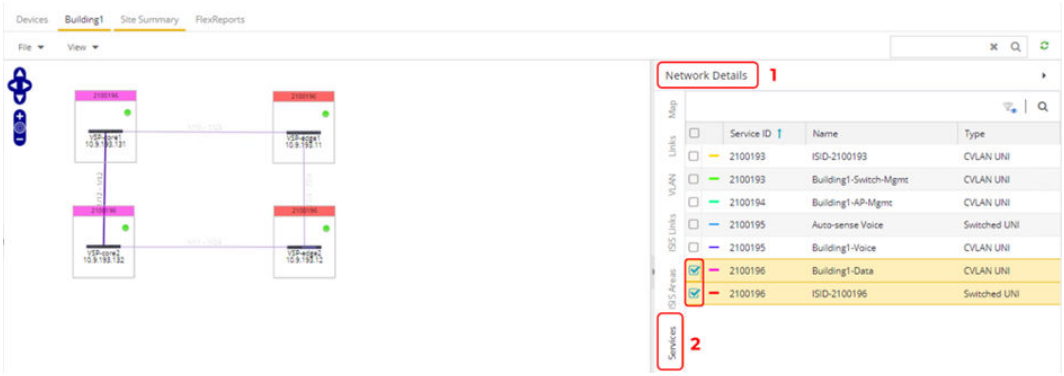
Go to the topology map and arrange the icons.



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.



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

```
show dvr members
```

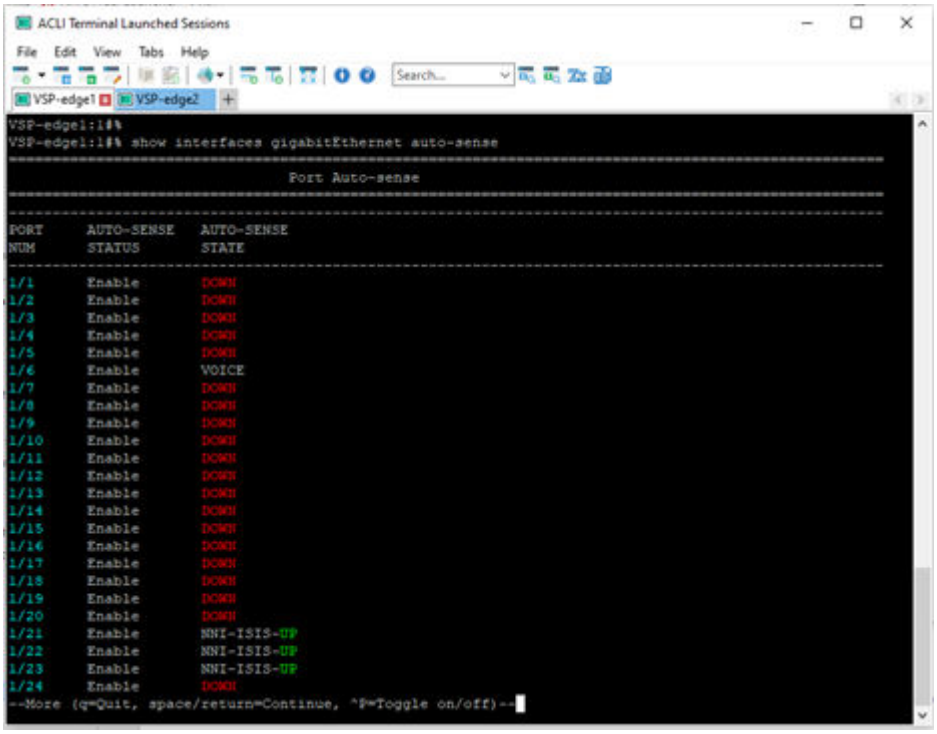
```
VSP-core1:1#% show dvr members
--------------------------------------------------------------------------------
                              DVR Members (Domain ID: 1)
--------------------------------------------------------------------------------
System Name                     Nick-Name     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

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

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

Inspect the Auto-Sense Ports on the VSP Edge Switches

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

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



Note that VSP-edge1 is in the auto-sense Voice state on port 1/6 where the Telephone is connected, and ports 1/21-1/23 are in the auto-sense NNI-ISIS-UP state. Ports 1/21-1/23 are the fabric interconnects that 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-edge2:1#% show interfaces gigabitEthernet auto-sense
                                Port Auto-sense
PORT     AUTO-SENSE   AUTO-SENSE          AUTO-SENSE
NUM      STATUS       STATE               PORT-DATA-ISID
1/1      Enable       DOWN                --
1/2      Enable       DOWN                --
1/3      Enable       DOWN                --
1/4      Enable       DOWN                --
1/5      Enable       DOWN                --
1/6      Enable       FA                  --
1/7      Enable       DOWN                --
1/8      Enable       DOWN                --
1/9      Enable       DOWN                --
1/10     Enable       DOWN                --
1/11     Enable       DOWN                --
1/12     Enable       DOWN                --
1/13     Enable       DOWN                --
1/14     Enable       DOWN                --
1/15     Enable       DOWN                --
1/16     Enable       FA                  --
1/17     Enable       DOWN                --
1/18     Enable       DOWN                --
1/19     Enable       DOWN                --
1/20     Enable       DOWN                --
1/21     Enable       NNI-ISIS-UP         --
1/22     Enable       NNI-ISIS-UP         --
1/23     Enable       DOWN                --
1/24     Enable       NNI-ISIS-UP         --
--More (q=Quit, space/return=Continue, ^P=Toggle on/off)--
```

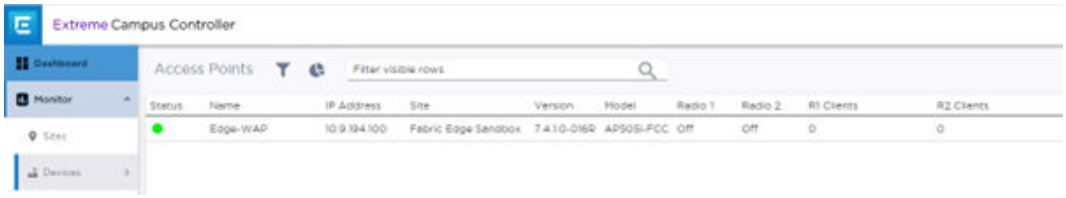
Check that SLPP-Guard is enabled on all auto-sense ports using the command

```
show slpp-guard
```

```
VSP-edge2:1#% show slpp-guard
================================================================================
                                SLPP Guard
================================================================================
                                Port Interface
================================================================================
Port       Link       Oper       SLPP-guard State      Timeout    TimerCount     Origin
--------------------------------------------------------------------------------
1/1        Up         Down       Enabled    N/A        60         N/A            CONFIG
1/2        Up         Down       Enabled    N/A        60         N/A            CONFIG
1/3        Up         Down       Enabled    N/A        60         N/A            CONFIG
1/4        Up         Down       Enabled    N/A        60         N/A            CONFIG
1/5        Up         Down       Enabled    N/A        60         N/A            CONFIG
1/6        Up         Up         Enabled    Monitoring 60         N/A            CONFIG
1/7        Up         Down       Enabled    N/A        60         N/A            CONFIG
1/8        Up         Down       Enabled    N/A        60         N/A            CONFIG
1/9        Up         Down       Enabled    N/A        60         N/A            CONFIG
1/10       Up         Down       Enabled    N/A        60         N/A            CONFIG
1/11       Up         Down       Enabled    N/A        60         N/A            CONFIG
1/12       Up         Down       Enabled    N/A        60         N/A            CONFIG
1/13       Up         Down       Enabled    N/A        60         N/A            CONFIG
1/14       Up         Down       Enabled    N/A        60         N/A            CONFIG
1/15       Up         Down       Enabled    N/A        60         N/A            CONFIG
1/16       Up         Up         Enabled    Monitoring 60         N/A            CONFIG
1/17       Up         Down       Enabled    N/A        60         N/A            CONFIG
1/18       Up         Down       Enabled    N/A        60         N/A            CONFIG
1/19       Up         Down       Enabled    N/A        60         N/A            CONFIG
1/20       Up         Down       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         Down       Enabled    N/A        60         N/A            CONFIG
1/24       Up         Up         Enabled    Monitoring 60         N/A            CONFIG
1/25       Up         Down       Enabled    N/A        60         N/A            CONFIG
1/26       Up         Down       Enabled    N/A        60         N/A            CONFIG
VSP-edge2:1#%
```

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.



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

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

```
VSP-edge2:1#% show interface gigabitEthernet i-sid 1/6
                                        PORT Isid Info
                ISID                    ISID                                                    MAC
PORTNUM IFINDEX ID      VLANID C-VID    TYPE    ORIGIN          ISID NAME               BPDU    SUNI
1/6     197     2100194 N/A    untag    ELAN    -  ---  -  El-  -  ISID-2100194         disabled FALSE
1/6     197     2100196 3      196      ELAN    -  Dl-  -  ---  -  ISID-2100196                  FALSE
2 out of 2 Total Num of i-sid endpoints displayed
acli.pl: Displayed Record Count = 2
ORIGIN Legend:
C: manually configured; D: discovered by FA or EPT
M: FA management; E: discovered by EAP; A: auto-sense
l: discover by local switch  r: discover by remote VIST switch
VSP-edge2:1#%
```

Note

There are two bindings on the port where the AP is connected. The first binding is 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`.

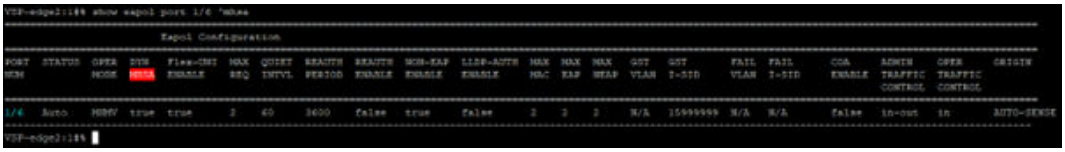
```
                                        Non-Eap Oper Status
PORT  MAC               STATE           VLAN  PRI  Flex-UNI  I-SID       NON-EAP  VLAN:I-SID
NUM                                     ID          Enable    SOURCE      AUTH
1/6   dc:b8:08:c2:80:79 authenticated   N/A   1    true      radius      radius   0:2100194
Total Number of NEAP Sessions: 1
VSP-edge2:1#%
```

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

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

`show eapol port 1/6`



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.

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

```
show fa assignment
```

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

```
VSP-edge2:1#% show fa assignment
=============================================================================
                        Fabric Attach Assignment Map
=============================================================================
Interface  I-SID      Vlan       State      Origin          I-SID Name
-----------------------------------------------------------------------------
1/6        2100196    196        active     client          ISID-2100196
```

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

Verify the IP Phone Is Operational

On VSP-edge1, view the I-SIDs that are configured on the phone port 1/6 using the CLI command

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

```
VSP-edge1:1#% show interface gigabitEthernet i-sid 1/6
=============================================================================
                                PORT Isid Info
=============================================================================
                ISID                    ISID                                MAC
PORTNUM IFINDEX ID       VLANID C-VID   TYPE     ORIGIN        ISID NAME     BPDU      SUNI
-----------------------------------------------------------------------------
1/6     197     2100195  2      195     ELAN     -  ---  -  ---  A  Auto-sense Voice          FALSE
1/6     197     2100196  3      untag   ELAN     -  ---  -  El-  -  ISID-2100196      disabled  TRUE
1/6     197     15999999 4048   untag   ELAN     -  ---  -  El-  -  Onboarding I-SID  disabled  FALSE
-----------------------------------------------------------------------------
3 out of 3 Total Num of i-sid endpoints displayed
acli.pl: Displayed Record Count = 3
ORIGIN Legend:
C: manually configured; D: discovered by FA or EPT
M: FA management; E: discovered by EAP; A: auto-sense
l: discover by local switch  r: discover by remote VIST switch
VSP-edge1:1#%
```

Note that there are three bindings on the phone port. The first binding is the Voice I-SID 2100195, which 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-edge1:1#% show lldp neighbor port 1/6
================================================================================
                                LLDP Neighbor
================================================================================
Port: 1/6       Index     : 6977
                Protocol  : LLDP
                ChassisId: Network Address    10.9.195.100
                PortId    : MAC Address       00:08:5d:62:bf:f0
                SysName   : regDN 4052,MINET_6920
                SysCap    : BT / BT
                PortDescr: LAN port
                SysDescr  : regDN 4052,MINET_6920,ver: 01.05.00.075,PxE: 6.5,01/01/1970 10:31:56 +0000
                Address   : 10.9.195.100
          IPv6 Address    : 0:0:0:0:0:0:0:0
--------------------------------------------------------------------------------
Total Neighbors : 1
--------------------------------------------------------------------------------
Capabilities Legend: (Supported/Enabled)
B= Bridge,    D= DOCSIS,    O= Other,     R= Repeater,
S= Station,   T= Telephone, W= WLAN,      r= Router
VSP-edge1:1#%
```

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

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

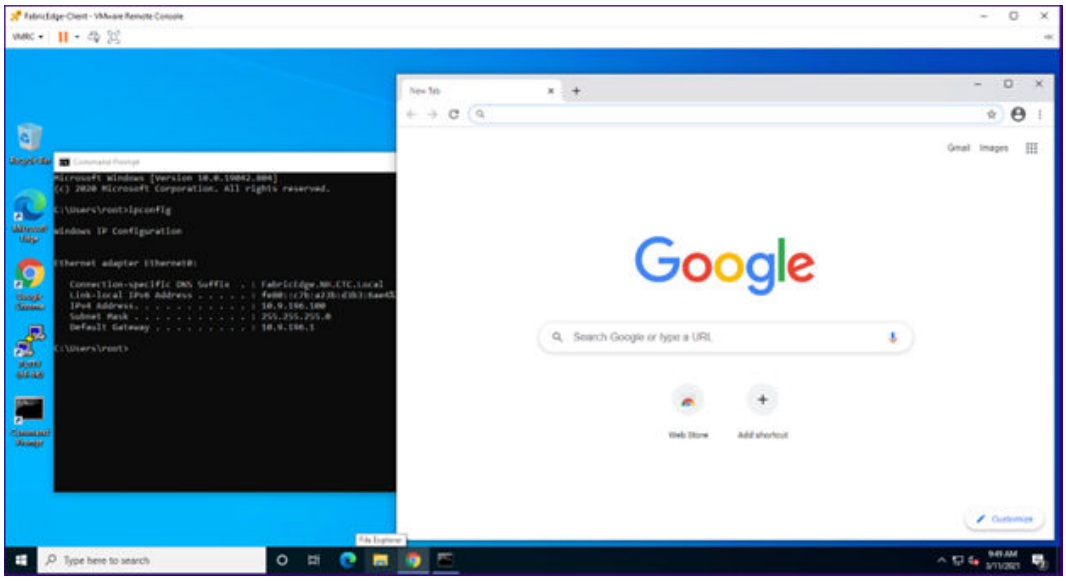
View the Network Access Control (NAC) sessions on port 1/6. If LLDP bypass authentication is used for the phone, then the *NON-EAP AUTH* type shows as `lldp`. If LLDP bypass is not used, then the *NON-EAP AUTH* type shows as `radius`.

```
VSP-edge1:1#% show eapol sessions neap
================================================================================
                                Non-Eap Oper Status
================================================================================
PORT  MAC               STATE          VLAN  PRI  Flex-UNI  I-SID      NON-EAP  VLAN:I-SID
NUM                                    ID         Enable    SOURCE     AUTH
--------------------------------------------------------------------------------
1/6   00:08:5d:62:bf:f0 authenticated  N/A   N/A  true      n/a        lldp     195:2100195
1/6   00:50:56:80:5d:ca authenticated  N/A   0    true      radius     radius   0:2100196
--------------------------------------------------------------------------------
Total Number of NEAP Sessions: 2

VSP-edge1:1#%
```

```
VSP-edge1:1#% show eapol sessions neap
================================================================================
                                Non-Eap Oper Status
================================================================================
PORT  MAC               STATE          VLAN  PRI  Flex-UNI  I-SID      NON-EAP  VLAN:I-SID
NUM                                    ID         Enable    SOURCE     AUTH
--------------------------------------------------------------------------------
1/6   00:08:5d:62:bf:f0 authenticated  N/A   0    true      n/a        radius
1/6   00:50:56:80:5d:ca authenticated  N/A   0    true      radius     radius   0:2100196
--------------------------------------------------------------------------------
Total Number of NEAP Sessions: 2

VSP-edge1:1#%
```

Verify Client PC Authentication

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



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

```
VSP-edge1:1#% show interface gigabitEthernet i-sid 1/6
                                        PORT Isid Info
                ISID                    ISID                                ISID                                    MAC
PORTNUM IFINDEX ID       VLANID C-VID   TYPE     ORIGIN                     NAME                          BPDU      SUNI
1/6     197     2100195  2      195     ELAN     - --- - --- A              Auto-sense Voice                        FALSE
1/6     197     2100196  3      untag   ELAN     - --- - El- -              ISID-2100196                  disabled  TRUE
1/6     197     15999999 4048   untag   ELAN     - --- - El- -              Onboarding I-SID              disabled  FALSE
3 out of 3 Total Num of i-sid endpoints displayed
acli.pl: Displayed Record Count = 3
ORIGIN Legend:
C: manually configured; D: discovered by FA or EPT
M: FA management; E: discovered by EAP; A: auto-sense
l: discover by local switch  r: discover by remote VIST switch
VSP-edge1:1#%
```

The first binding is the phone and 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.

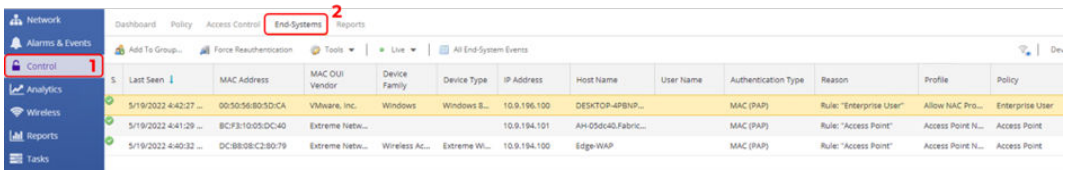
Confirm both the first and second bindings by inspecting the MAC authentications on the switch, using the CLI command

```
show eapol sessions neap
```

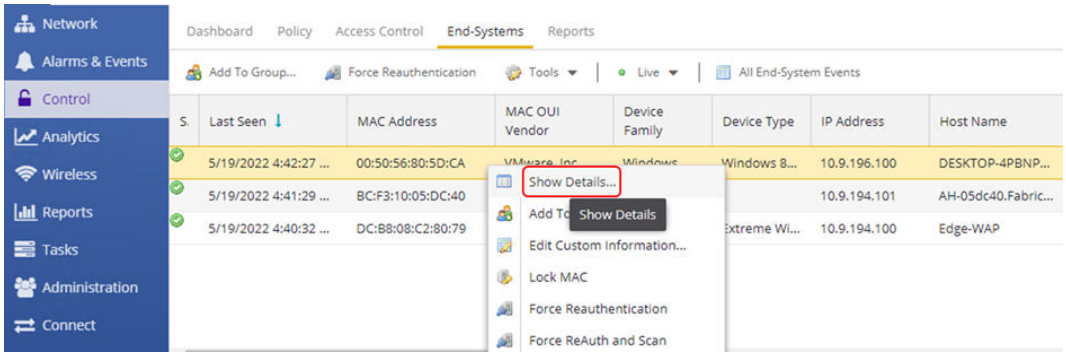
```
VSP-edge1:1#% show eapol sessions neap
                                        Non-Eap Oper Status
PORT  MAC               STATE          VLAN  PRI  Flex-UNI  I-SID       NON-EAP  VLAN:I-SID
NUM                                    ID          Enable    SOURCE      AUTH
1/6   00:08:5d:62:bf:f0 authenticated   N/A   N/A  true      n/a         lldp     195:2100195
1/6   00:50:56:80:5d:ca authenticated   N/A   0    true      radius      radius   0:2100196
Total Number of NEAP Sessions: 2
VSP-edge1:1#%
```

The first MAC is the phone. It 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.

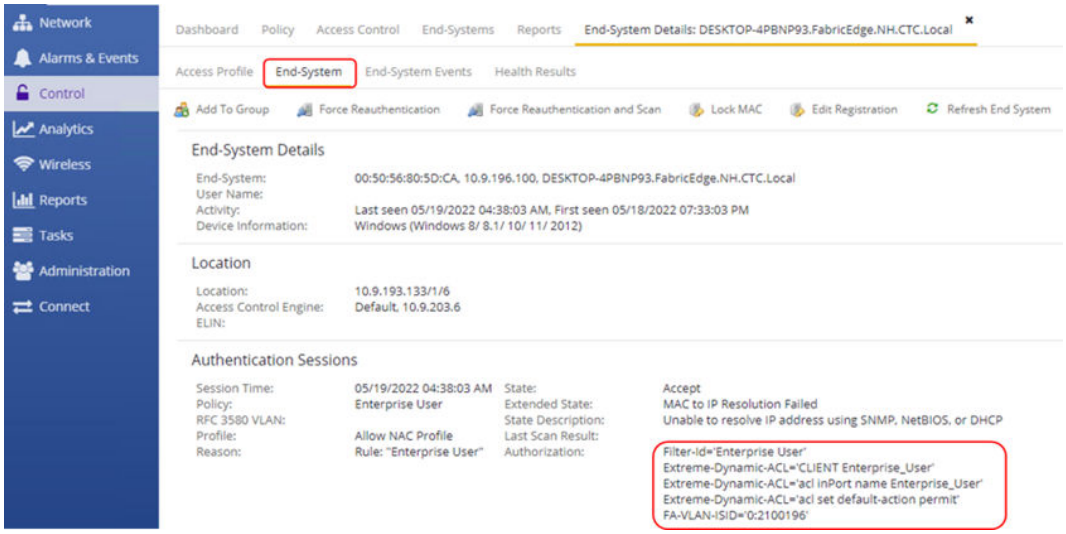
Go to the **XIQ-SE Control** > **End Systems** tab.



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



Select the **End Systems** tab.



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