

ExtremeCloud IQ - Site Engine and ExtremeControl -VOSS/Fabric Engine Downloadable ACL Guide

Abstract: This document details the utilization of a VOSS or Fabric Engine switch as an edge enforcement point in ExtremeControl using Downloadable ACLs (also known as Per-User ACLs) as an enforcement method.

Part Number: 9037358-00 Rev AB

Published: March 2022

Extreme Networks, Inc. 6480 Via Del Oro San Jose, California 95119 Phone / +1 408.579.2800 Toll-free / +1 888.257.3000 **www.extremenetworks.com** Copyright © 2022 Extreme Networks, Inc.

Legal Notice

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

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

Trademarks

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

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

For additional information on Extreme Networks trademarks, see: https://www.extremenetworks.com/Company/legal/trademarks/

Open Source Declarations

Some software files have been licensed under certain open source or third-party licenses. End-user license agreements and open source declarations can be found at: https://www.extremenetworks.com/support/policies/open-source-declaration/

Contents

Acronyms4	1
Test Environment	ŧ
Topology	1
Overview	5
Objective5	5
Policy and Downloadable ACLs5	;
Rule Ordering	,
Policy Support	3
Supported Platforms	•
ExtremeCloud IQ - Site Engine Preparation for VOSS/Fabric Engine Downloadable ACL Metho	od 10
Policy Domain Preparation	0
Step 1: Create a Policy Domain	0
Step 2: Set up Roles	0
Step 3: Create Services	3
Step 4: Create Rules15	5
Step 5: Assign Services to Roles17	7
VOSS/Fabric Engine Switch Discovery19	9
Option 1: Manual Discovery	9
Option 2: Automated Discovery through ZTP+2	2
Access Control Preparation	28
Step 1: AAA Configuration	8
Step 2: Create Rules	2
VOSS/Fabric Engine Switch Configuration3	57
SNMP Configuration	57
RADIUS Configuration	57
Verification – Client Testing	38
Appendix – Troubleshooting	10
ZTP+ Troubleshooting	10
Downloadable ACL Troubleshooting4	10
802.1X Supplicant Configuration for Windows Clients4	12
Terms and Conditions of Use4	13

Acronyms

Term or Acronym	Definition
ААА	Authentication, Authorization, Accounting
ACL	Access Control List
NAC	Network Access Control
NAS	Network Access Server
OOB	Out of Band
VOSS	VSP Operating System
VSA	Vendor Specific Attribute
ZTP+	Zero Touch Provisioning Plus

Test Environment

Testing was performed on the following software and hardware models and versions.

- ExtremeCloud IQ Site Engine (Site Engine) version 21.11.10.57
- ExtremeControl for ExtremeCloud IQ Site Engine version 21.11.10.57
- 5520-48T (VOSS) version 8.4.2.0

Topology

The testing topology can be found below.



Overview

Objective

This guide describes how to deploy a VOSS/Fabric Engine switch as an edge enforcement point in ExtremeControl using Downloadable ACLs (also referred as Per-User ACLs). In particular, the guide focuses on the following tasks:

- How to prepare and construct a policy domain for VOSS/Fabric Engine switches
- How to prepare Access Control settings for the VOSS/Fabric Engine Downloadable ACL method
- How to add a VOSS/Fabric Engine switch to the ExtremeCloud IQ Site Engine database via Zero Touch Provisioning Plus (ZTP+)
- Verification and troubleshooting

When a VOSS/Fabric Engine switch is deployed at the access layer of the network, it is most commonly done using a Fabric to the Edge topology. The steps needed to deploy a VOSS/Fabric Engine switch in a Fabric to the Edge scenario using Zero Touch Fabric and ExtremeCloud IQ - Site Engine onboarding automation are outside the scope of this guide.

Policy and Downloadable ACLs

A Downloadable ACL is an Access Control List that is created and stored in the RADIUS Server, which in this scenario is ExtremeControl. The Network Access Server device (NAS), which in this case is the VOSS/Fabric Engine switch, does not save any preconfigured ACLs in the running configuration. Downloadable ACLs are dynamically installed on the switch upon successful authentication as part of the RADIUS Access-Accept message. A Downloadable ACL action can assign different ACLs for each user session.

The Policy tab in ExtremeControl provides a single pane of glass to configure access permissions for roles that can be assigned via Access Control. A feature enhancement starting with ExtremeCloud IQ - Site Engine version 21.9.10.90 extends this functionality to VOSS/Fabric Engine switches through the use of Downloadable ACLs.

The new feature takes advantage of the ability to write ACLs as part of the RADIUS Accept message that is returned to the switch during client authentication. The traditional method of policy enforcement with Extreme wireless and EXOS based switches is to write the policy rules and roles via SNMP or REST API calls so that they exist locally on the device. This new method does not write the ACLs to switch itself; rather, the ACLs are saved in the local database on the Access Control Engine. Therefore, when an enforce is done, a VOSS/Fabric Engine switch will have the policy converted automatically to a Downloadable ACL that is saved in the database.



VOSS 8.3 and above

Figure 1 - Policy enforcement with VOSS/Fabric Engine switches

Upon enforcement of the policy domain, the exact ACLs to be assigned can be reviewed in the Enforce Preview screen as shown in Figure 2.



Figure 2 - How to visualize VOSS/Fabric Engine Downloadable ACLs during Policy Enforce



When a device authenticates to Access Control and Downloadable ACLs are configured to be returned to the authenticated session, the appropriate RADIUS attributes are included. These RADIUS attributes specify the ACLs to assign to the authenticated session.

Rule Ordering

When converting policy rules to Downloadable ACLs, ExtremeCloud IQ - Site Engine makes some intelligent decisions to set a precedence of the ordering. However, the ordering that is derived might not be the outcome you would like. In this case, the ordering of the Downloadable ACLs can be re-arranged during assignment. This is accomplished by following the steps shown in Figure 3, using the "Move Up" or "Move Down" options to arrange the rules as desired.

NOTE

The Rule Ordering view appears in the UI only after a VOSS/Fabric Engine switch has been added to the policy domain.



Figure 3 - How to order ACL rules within a policy domain

Policy Support

Because Extreme Policy has many features in addition to traditional ACL support, certain feature sets within Policy cannot be converted to Downloadable ACLs. The following policy match conditions are supported and work properly with VOSS/Fabric Engine.

- Ethertype
- IP Address Source and Destination
- IP Protocol Type
- IP Type of Service
- IP Fragment
- TCP Source and Destination
- UDP Source and Destination
- ICMP
- IP Socket Destination
- IP Socket Source
- Destination MAC Address

CAUTION

- Socket (IPSOCKETDEST, IPSOCKETSOURCE) are translated into two rules, one for UDP and one for TCP.
- Range (IPUDPPORTDESTRANGE, IPTCPPORTDESTRANGE, IPTCPPORTSOURCERANGE, IPUDPPORTSOURCERANGE) are translated to more rules with MASK.
- Hierarchical (Filtering Rules) and ACL mode (Access Control Entries) are supported.
- Bilateral (IPTCPPORTBILAT, IPUDPPORTBILAT, IPADDRESSBILAT) are not supported in the tested release of ExtremeCloud IQ Site Engine.

Supported Platforms

The following hardware platforms support Downloadable ACLs that work in conjunction with ExtremeCloud IQ - Site Engine Policy. All Fabric Engine versions support Downloadable ACL. The minimum VOSS version to support Downloadable ACLs is 8.3.

- Universal Switching (VOSS and Fabric Engine)
- VSP 4450 Series (VOSS only)
- VSP 4900 Series (VOSS only)
- VSP 7200 Series (VOSS only)
- VSP 7400 Series (VOSS only)
- VSP 8000 Series (VOSS only)

ExtremeCloud IQ - Site Engine Preparation for VOSS/Fabric Engine Downloadable ACL Method

Policy Domain Preparation

Step 1: Create a Policy Domain

Navigate to **Control** and then **Policy** and follow the steps illustrated in Figure 4 to create a new policy domain and give the domain a name when prompted.



Figure 4 - How to create a new policy domain

Step 2: Set up Roles

The hierarchical Policy Framework consists of three main components: roles, services and rules. Below are the functions of each component within the Policy Framework:

- Roles are at the Business / Network level and define the job responsibility and function of individual employees or groups of employees for example, engineering, finance, and sales.
- Services are policy containers for groups of similar rules. Grouping rules allows the network administrator to apply rules in groups rather than as individual components.
- Rules are the individual granular policies that are enforced at the port level. When a VOSS/Fabric Engine switch is used, these rules translate into Downloadable ACL entries that can be stored in Access Control and are ready to be included in the RADIUS Access-Accept messages after a successful authentication.

After you create the policy domain, either a Top-Down or a Bottom-Up approach can be followed when setting up the Policy Framework. A Top-Down approach would include creating roles which are in most

scenarios in parallel with Organizational Units in Active Directory, followed by adding services and finally rules. This guide will follow the Top-Down approach, which is illustrated in Figure 5.



Figure 5 - Policy Framework with roles, services, and rules

Right click on **Roles** and create the following roles:

- Operator
- Contractor
- Guest
- Access Point

When you have created these roles, the policy domain will look like Figure 6.



Figure 6 - Creating the roles in a policy domain

After you create each role, select the role, and expand the Default Actions on the right pane by selecting **Show All**. Figure 7 shows the supported Default Action fields for VOSS/Fabric Engine switches, which are also listed below.

- 1. Access Control: There are 3 options under Access Control
 - i. Permit Traffic
 - ii. Deny Traffic
 - iii. Contain to VLAN

In order to assign a Service Identifier (I-SID) value in the context of the Fabric to the Edge architecture, **Contain to VLAN** must be selected and the Service ID field needs to be populated accordingly. If a Service ID is defined, the following VSA is sent: *"FA-VLAN-ISID=0:ServiceID"*

CAUTION

VLAN assignment is not supported in the tested version of ExtremeCloud IQ - Site Engine.

CAUTION

VSP 4450 does not support the following EAP enhancements: EAP on Flex UNI ports, Auto-sense ports, auto-isid-offset.

NOTE

When a VOSS/Fabric Engine switch is used as an access switch in Fabric to the Edge topology, the most common scenario is when the switch acts as a DvR Leaf which does not allow Platform VLANs to be created. Therefore Flex-UNI is required for L2VSNs, which is more powerful and flexible and which does not require VLAN ID information for untagged bindings because it directly assigns I-SID to ports.

 AP Aware: When AP Aware is enabled as a Default Action on a role, only the access point itself will be authenticated on that particular port and all subsequent traffic through the port will not need authentication. This setting is very useful when you want a uniform port configuration regardless of the connected end-system type. If AP Aware is enabled, the following VSA is sent: "Extreme-Dynamic-MHSA=1".

C ExtremeClo	oud IQ Site Engine											
A Network	Dashboard Policy * Access Control End-Systems	Reports										
🔔 Alarms & Events	🐻 Open/Manage Domain(s) 💌 📑 Global Domain Settin	ngs 💌 📑 Taols 💌										
Control	Domain: VOSS Domain (Modified Locally) - Und	der edit by root										
Analytics	Roles/Services Role: Operator											
🗢 Wireless	▼	Role. Operator										
Lill Reports	Operator	General VLAN Egres	s Mappings Port Default Usage									
Tasks	▼ ● Service Repository	Name: Op	erator									
曫 Administration	▼	Description:										
≓ Connect	Service Groups	TCI Overwrite: Disab	TCI Overwrite: Disabled *									
	Services Global Capitors (All Domains)	Default Actions										
		Access Control:	Contain to VLAN	-)1								
			VLAN: 1[DEFAULT VLAN]	Ť								
			Service ID: 10010	2								
		Class of Service:	None	*								
		System Log:	Disabled	v								
		Audit Trap:	Disabled	w.								
		Disable Port:	Disabled	v								
		AP Aware:	Disabled	- 3								
		HTTP Redirect:	Disabled	Ψ.								
		Traffic Mirror:	Disabled	✓ Mirror First 15 Packets								

Figure 7- Supported Default Action fields for VOSS/Fabric Engine switches

After adding the Service-IDs to each role and enabling the AP-Aware feature on the "Access Point" role, the Roles Summary looks like Figure 8.

C ExtremeClo	oud IQ Site Engine		
A Network	Dashboard Policy * Access Co	ntrol End-Systems Reports	
🔔 Alarms & Events	🐻 Open/Manage Domain(s) 👻 📷	Global Domain Settings 👻 📷 Tools 👻	
Control	Domain: VOSS Domain (Modi	ied Locally) - Under edit by root	
Analytics	Deles (Censiers	ied cocary, onder ear by root	
SWireless	Roles/Services	Show Editable Columns Collapse	All
Peports	👻 🥥 Roles	Role / Service / Rule	Summary
reports	Access Point	Access Point	[1 [DEFAULT VLAN] (SVC ID:2800200)/AP Aware]
Tasks	Contractor	Contractor	[1 [DEFAULT VLAN] (SVC ID:2800210)]
Administration	🔞 Guest	log Guest	[Deny Traffic]
2 Connect	Operator	Operator	[1 [DEFAULT VLAN] (SVC ID:2800220)]

Figure 8 – Roles Summary

Step 3: Create Services

After you set up the roles, the next step is to create services. Services are containers for similar types of rules. To create a new service, expand the **Service Repository** and right click on **Services** as depicted in Figure 9. Give the service a meaningful name. The name will represent a group of rules that will be created in Step 4.

In this guide, the policy structure depicted in Figure 5 will be used; therefore the names of the services are as follows:

- Deny Internal Apps
- Deny Administrative Protocols
- Permit Internet Only

C ExtremeClo	oud IQ Site Engine		
A Network	Dashboard Policy * Access Control End-Syste	ms Reports	
🔔 Alarms & Events	📑 Open/Manage Domain(s) 👻 📑 Global Domain Se	ttings 👻 🎆 Tools 👻	
Control	Domain: VOSS_Domain (Modified Locally) - U	nder edit by root	
Analytics	Roles/Services –	Show Editable Columns	IL
Reports	✓	Service / Rule	Summary
Tasks	Contractor		
🕍 Administration	Suest		
₽ Connect	 Operator Service Repository Local Services Service Groups 		
	Service Create Service Global Ser Create Automated Service Export All Services to File Paste		

After all the services are created, the Services Summary will look like Figure 10, with no rules in them yet. Continue with Step 4 to create rules within each service.

C ExtremeClo	ud IQ Site Engine		
A Network	Dashboard Policy * Access Control End-System	ns Reports	
🔔 Alarms & Events	🎆 Open/Manage Domain(s) 💌 📑 Global Domain Sett	ings 💌 📷 Tools 💌	
Control	Domain: VOSS_Domain (Modified Locally)		
Analytics	Roles/Services		
🗢 Wireless	Roles	Collapse All	
Lill Reports	Service Repository	Service / Rule	Summary
📑 Tasks	 Decal Services 	Deny Administrative Protocols	Rules: 0
🐸 Administration	Service Groups	A Permit Internet Only	Rules: 0
≓ Connect	🔻 🥥 Services		10.048.40.2000
	Deny Administrative Protocols		
	🕨 🛃 Deny Internal Apps		
	🕨 👶 Permit Internet Only		
	 Global Services (All Domains) 		

Step 4: Create Rules

Each of the services created in Step 3 needs to be populated with rules. These rules will then be translated into Downloadable ACL entries for VOSS/Fabric Engine switches. Right click on a service and select **Create Rule** as shown in Figure 11.

ExtremeClo	ud IQ Site Engine	
A Network	Dashboard Policy* Access Control End-Systems	Reports
Alarms & Events Control Analytics	 Open/Manage Domain(s) Global Domain Settings Domain: VOSS_Domain (Modified Locally) 	s 🕶 📖 Tools 🕶
Adaptics Adaptics Wireless Adoption Tasks Administration Connect	Roles/Services	 Show Editable Columns Collapse All Rule Create Rule 2 Add to Role(s) Enable Rule(s) Disable Rule(s) Rename Delete Show Role Usage Export Service(s) to File Copy Paste

After the rule is created, two actions need to be performed for VOSS/Fabric Engine switches:

- 1. Edit Traffic Description: L2, L3 and L4 Traffic Classification Layers
- 2. Access Control: Permit or Deny

Supported traffic description types for VOSS/Fabric Engine switches can be found in the **Policy Support** section under **Overview**. As an example, Figure 12 shows a rule description that denies Telnet protocol.

	Dashboard Policy * Access Control End-Sy	stems Reports						
Alarms & Events	B Open/Manage Domain(s) Global Domain Domain: VOSS_Domain (Modified Locally)	Settings 🔻 🔝 Tools						
 ✓ Analytics ♥ Wareless ▲ Reports Tasks ▲ Administration ➡ Connect 	Roles/Services	 Rule: Deny T Service Name: Descripton: Rule Status: Rule Status: Rule Type: Traffic Dest Traffic Dest Type: Value: Actions Access Control: Class of Service System Log: Audit Trap: Ditable Fort: TTP Bedrect: Quarantine Ruie: 	ADeny Administrative P Enabled Al Devices Disabled None None Deny Traffic Service D: None Disabled Disabled Disabled Disabled Disabled Disabled	Traffic Classification Traffic Classification Traffic Classification Traffic Classification O single value: O Range: Traffic Classification Value: Maintenne Value: Traffic Classification Value: Maintenne Value: Value: Maintenne Value: Val	escription In Layer: Layer 4 - Application Transport on Type: IP TCP Port Destination iffication Value Value: Tenet (23) 4 23 Start Value: end value iffication Optional Value	Ve S Cancel	Ren	tdr
😧 Help	Enforce	Traffic Mirror:	Disabled		Mirror First 15 Packets			

After you create all the rules for the services, the Services Summary will look like Figure 13. Rule details are listed under each respective service.



Step 5: Assign Services to Roles

The final step in policy domain preparation is to assign the services to their respective roles. To achieve this, select **Roles** and then **Add/Remove** under **Services** to add the desired services to the role. See Figure 14 for reference.

etwork	Dashboard Policy Arress Control Ford-Sys	terns Reports				XXQ-sit Administrator
larms & Events ontrol nalytics	Open/Manage Domain(s) Global Domai Omain: VOSS_Domain	n Settings 👻 📑 Tools	•			
/ireless	Roles/Services	Role: Opera	ator			
eports	Access Point	General V	LAN Egress Mappings Port Default	Jsage		
asks	Contractor	Name:	Operator	Add/Remove Services	*	
dministration	Guest	Description:		Additioned Services	~	
onnect	Operator 2	TCI Overwrite	: Disabled	All Services & Service Groups	Selected Services & Service Groups	
	 Service Repository Local Services Services Services	Defaul	t Actions - AC:1[DEFAULT VLAN](N) es Add/Remove Name 1	Create Service Q Deny Administrative Protocols Deny Internal Apps Permit Internet Only	4 4 4 Carcel	Q
	Class of Service	+				
	VLANs	+				
	Network Resources	+				
	Devices/Port Groups	+				

After all the services are assigned according to the Policy Framework in Figure 5, save the domain to the database as shown in Figure 15. The domain enforce will be done automatically after a VOSS/Fabric Engine switch is discovered, onboarded, and added to the policy domain using ZTP+. This process is detailed in the following section.



VOSS/Fabric Engine Switch Discovery

In order to manage a VOSS/Fabric Engine switch in ExtremeCloud IQ - Site Engine, the switch needs to be discovered and added to the ExtremeCloud IQ - Site Engine database. There are two ways a VOSS/Fabric Engine switch can be added to the ExtremeCloud IQ - Site Engine database. These are as follows:

Option 1: Manual Discovery

Any Extreme Networks or third-party device can be added manually to the ExtremeCloud IQ - Site Engine database. For this purpose, SNMP and CLI credentials should be created and added to a Device Profile which will then be used during the discovery process.

As depicted in Figure 16, navigate to **Administration** and follow the steps to create SNMP and CLI credentials for the VOSS/Fabric Engine switch. Be sure to configure the same SNMP user name, authentication and privacy types, and passwords that are configured on the switch.

ExtremeClo	oud IQ Site Engine										Q	
A Network	Profiles Users Server I	nformation Licer	nses Certificates Op	tions	Device Types Ba	ckup/Restore Di	agnostics	Client API Access				
Alarms & Events	🗿 Add 🝺 Edit 🌾	Delete Defau	It Profile: public_v1_Prof	file 🔻	Default Access C	ontrol Engine Profil	e: snmp	_v3_profile 🔻				
Control	Name	SNMP Version	Read Credential		Write Credential	Max Access Crede	ntial	Read Security Level	Write Sec	urity Level	Max Access Secu	irity Level
Analytics	VOSS_v2_Profile	SNMPv2	public_v2		private_v2	private_v2						
🗢 Wireless	BOSS_ESM_v2_Profile	SNMPv2	public_v2		private_v2	private_v2						
III Reports	BOSS_4800_v2_Profile	SNMPv2	public_v2		private_v2	private_v2						
Tasks 1	BOSS_v2_Profile	SNMPv2	public_v2		private_v2	private_v2						
🔮 Administration	san_security_profile	SNMPv1	public_v1		public_v1	public_v1						
≓ Connect	VOSS_v3_Profile	SNMPv3	default_snmp_v3		default_snmp_v3	default_snmp_v3		AuthPriv	AuthPriv		AuthPriv	
	XCC_v3	SNMPv3	XCC_v3_authnopriv		XCC_v3_authnop	XCC_v3_authnopri	v	AuthNoPriv	AuthNoPr	riv	AuthNoPriv	
	Cisco	SNMPv2	public_v2		Pr Add SNIMD Cr	Add SNMP Credential						
	Cisco_v3_Profile	SNMPv3	Cisco_SNMP_v3	c Add SNMP Credential					1		AuthPriv	
	PoC SNMPv2 Profile	SNMPv2	public_v2		P Credential Name: V		VOSS_snmp_v3					
	≪ < Page 1 c	Page 1 of 1 > > 📿 🔜 Reset			SNMP Version: SNMPv3			~				
		dontials - Dovico M	User Name: snmpuser									
		Series Series	ind bhing		Authentication Ty	pe: MD5	MD5		- 4			
	Add	Delete			Authentication				Ð			
	Name	SNMP Version	Community Name	User N	Password:				_	Privacy Passy	vord 🕇	
	public_v1	SNMPv1	*****		Privacy Type:	DES						
	default_snmp_v3	SNMPv3		snmpu	IS Privacy Password:				<u></u>	*******	*	
	private_v1	SNMPv1	*****					Save	Cancel			
	Cisco_SNMP_v3	SNMPv3		snmpu	iser MD5	,	*******	DES		********	×	
	public_v2	SNMPv2	*****									
	private_v2	SNMPv2	*****									
	XCC_v3_authnopriv	SNMPv3		snmpu	iser MD5	,	******	***				
	XCC_v3_authpriv_AES	SNMPv3		snmpu	iser MD5	,	*******	*** AES		*******	*****	

A CLI credential is needed to access the CLI terminal of the device directly from ExtremeCloud IQ - Site Engine and to run scripts or workflows that will interact with the device through the CLI. Note that the CLI credential is also needed for RADIUS configuration on VOSS/Fabric Engine devices starting from ExtremeCloud IQ - Site Engine version 21.11.

Network	Profiles Users Serve	er Information Lice	enses Certifica	ates Options	Device Types Bac	kup/Restore Diagnosti	cs Client API Access			
Narms & Events	🗿 Add 🔯 Edit	Delete Defa	ult Profile: pub	lic v1 Profile	▼ Default Access C	ontrol Engine Profile: sn	mp v3 profile 🔻			
	Name	SNMP Version	Read Creden	itial	Write Credential	Max Access Credential	Read Security Level	Write Security Level	Max Access Security Level	CLI Credential
knalytics	VOSS v2 Brafia	SNMD-2	public v2		oriusta 1/2	oriusta v2				Default PIA/A
Wireless	POSS_ESM_v2_Profile	SNMP V2	public v2		private_v2	private_v2				Default DOSS SSA
eports	BOSS 4800 v2 Profile	SNMPv2	public v2		private_v2	private v2				Default BOSS 48
asks	BOSS v2 Profile	SNMPv2	public v2		private v2	private v2				Default BOSS
dministration	san security profile	SNMPv1	public_v1		public_v1	public_v1				SAN Security
	VOSS_v3_Profile	SNMPv3	default_snm	p_v3	default_snmp_v3	default_snmp_v3	AuthPriv	AuthPriv	AuthPriv	XMC
onnect	XCC_V3	SNMPv3	XCC_v3_auth	nopriv	XCC_v3_authnop	XCC_v3_authnopriv	AuthNoPriv	AuthNoPriv	AuthNoPriv	XCC
	Cisco	SNMPv2	public_v2		Add CLI Credentia	1		×		Default
	Cisco_v3_Profile	5NMPv3	Cisco_SNMP	v3				Priv	AuthPriv	Cisco_CLI
	PoC SNMPv2 Profile	SNMPv2	public_v2		Description:	VOS5_CLI				PoC CLI Credent.
	« < Page 1	of 1 > >>	0	leset	User Name:	nwa				
		2			Type:	Telnet		- 4		
	SNMP Credentials	redentials Device	Mapping		Login Password:			Φ		
	Add) ³ 🗊 Edit	Oelete			Enable Password:			Ø		
	Description	User Name	Туре	Login Passv	Configuration Password	d:				
	Default	admin	Telnet				Same	anal		
	< No Access >									
	Default RWA	rwa	Teinet	***						
	Default BOSS ESM	admin	SSH	*******						
	Default BOSS 4800	RW	Telnet	******	**					
	Default BOSS	RW	Teinet	*****						
	SAN Security	root	Teinet							
	022000									

When both SNMP and CLI credentials have been set up, add a new Device Profile and bind the credentials to the profile as shown in Figure 18.

ExtremeClo	oud IQ Site Engine								9 0 4	D A 3101110
A Network	Profiles 2 Users Server	Information Lice	nses Certificates C	Options Device Typ	es Backup/Restore	Diagnostics Client A	PI Access			5 4 5 6 1 1 6
🌲 Alarms & Events	Add 3 Edg	Belete Defai	ult Profile: oublic vd. Dr	ofile T Default	Access Control Engine	Profile: como v2 profile				
	Name	ShiMD Vertice	Pood Credential	Write Crede	atial Max Accore (reductial Pead Ser	with Lewel	Minite Security Louis	May Arrest Constitutional	Cliffredential
Analytics	nublic ut Profile	SNMD/1	nublic ut	oublic ut	nublic vd	Read Sect	any Level	write secondy cever	max Access secondy Level	Default
S Wireless	EVTR vd. Brofile	SNMD/1	public_v1	private v1	private v1					Default
1.1.0	public v2 Profile	ENMP/2	public_v1	private_v1	private_v1					Default
Lill Reports	EVTR v2 Profile	SNMD-2	public v2	private v2	private v2					Default
Tasks	somo v2 profile	SNMD/2	default somo v3	default som	private_v2	v3 AuthPriv		AuthDriv	AuthDriv	Default
Administration	VOS vi profile	SNMD/1	oublic ut	orivate v1	private v1				Autor III	Default PWA
≓ Connect	BOSS FSM v1 Profile	SNMD/1	public_v1		product of					Default BOSS ESM
	BOSS 4800 v1 Profile	SNMPv1	public v1	Add Profile				×)		Default BOSS 48
	BOSS v1 Profile	SNMD/1	public v1	Profile Name:	VOSS_v3_Profile					Default BOSS
	VOSS v2 Profile	SNMPv2	public v2	SNMP Version:	SNMPv3					Default RWA
			paracte	Read:	VOSS snmp v3	* Read Security:	AuthPriv	-		
	« < Page 1	of 1 > >>	C 🖪 Reset	Writer	VOSS comp v2	w Write Security	AuthDriv	4		
	SNMD Gradastials	ndontiale Davies	Manoing	vince.	v035_smip_v3	- Write Secondy.	Ruciente			
	Siving Credendals	edentials Device	mapping	Max Access:	VOSS_snmp_v3	 Max Security: 	AuthPriv			
	🗿 Add 💹 Edit	Delets		CLI Credential:	VOS5_CLI			· ·		
	Name	SNMP Version	Community Name	ų			Save	Cancel acy Pa	ssword 1	
	public_v1	SNMPv1	*****							
	default_snmp_v3	SNMPv3		snmpuser	SHA	******	AES	********	***	
	private_v1	SNMPv1	******							
	Cisco_SNMP_v3	SNMPv3		snmpuser	MD5	*********	DES	*******	***	
	VOS5_snmp_v3	5NMPv3		snmpuser	MD5	*********	DES	********	***	
	public_v2	SNMPv2	*****							
	private_v2	SNMPv2	******							
	XCC_v3_authnopriv	SNMPv3		snmpuser	MD5	*******				
	XCC_v3_authpriv_AES	SNMPv3		snmpuser	MD5	*********	AES	********	******	
Help	« < Page 1	of1 > >>	🖸 🎆 Reset							

After the Device Profile is set up, navigate to the **Network** menu from the left pane of ExtremeCloud IQ - Site Engine and select the **Devices** tab. Select the relevant Site for the VOSS/Fabric Engine switch to be added in and then right click on that Site and select "Add Devices".



Alternatively, if there are multiple switches that need to be onboarded, a more convenient method is to use the "Discover" operation under the Site as illustrated in Figure 20. The Discover type can be a Subnet, a Seed Address, or an Address Range.

ExtremeClo	ud IQ Site Engine Q 🛆 🔂	2 3101	1 I 0 O root XIQ-SE Administratio	. E
A Network	Dashboard Devices Discovered Firmware Archives Configuration Templates Reports			
🔔 Alarms & Events	< Stes *> Devices VDS 2 the Summary Endpoint Locations Elevelanorte			
Gentrol				
Analytics	Ovorid			
🗢 Wireless		Profiles		
Litel Reports		0.44	Tala Dalara	
Tasks	♦ ThirdParty		. Z com Veece	
Section 4	I Topology Definitions Enabled Discover Type Address Cover Type Address Cover Type Address Cover Type Address	Accept	Name	Reject
- Connort	FCJest DS Subnet 10.8.0.0/10	0	EVTR ut Brofile	0
- connecc	▼ Di Service Definitions	0	public v2 Profile	0
	• Q) FC_Services	0	EXTR v2 Profile	0
	Add Address ×	0	snmp v3 profile	0
			VOSS_v1_Profile	
	Discover ripe: Subnet • 5	0	BOSS_ESM_v1_Profile	0
	subnet/Masic 10.8.0.0/16	0	BOSS_4800_v1_Profile	0
	OX Careel	0	BOSS_v1_Profile	0
			VOSS_v2_Profile	
		0	BOSS_ESM_v2_Profile	0
			BOS5_4800_v2_Profile	
			BOSS_v2_Profile	
			san_security_profile	
		G	VOSS_v3_Profile	0
			XCC_v3	
		0	Cisco	0
		0	Cisco_v3_Profile	
			PoC SNMPv2 Profile	0
				7
Help			Save	Cancel
<	Last Updated: 50/2021 2:2503 PM - Updrei, 7 Days 31:36-46			9

Option 2: Automated Discovery through ZTP+

Adding or discovering switches manually can be cumbersome for the network operator and require followup configuration after the switches are added to the ExtremeCloud IQ - Site Engine database. A better method of discovery for VOSS/Fabric Engine switches is through the use of Zero Touch Provisioning Plus (ZTP+). VOSS/Fabric Engine devices, starting from version 8.2.5, support ZTP+, which enables them to send information to ExtremeCloud IQ - Site Engine automatically after they are initially powered up with factory default settings. When a VOSS/Fabric Engine device is discovered in ExtremeCloud IQ - Site Engine through ZTP+, it can quickly be added to the ExtremeCloud IQ - Site Engine database with minimal to no manual configuration. This process minimizes the amount of time needed to configure a new device and deploy it on the network.

For the ZTP+ process to work properly, there are some prerequisites which are listed below:

- The switch should have a factory default configuration. After a configuration file is saved, the ZTP+ process will not run on the next reboot of the switch.
- The switch should be able to reach the DHCP server and receive IP address through its OOB interface or Management VLAN.
- The switch should obtain one or more DNS servers and a domain name from the DHCP server.
- The switch will make a DNS query to resolve *extremecontrol.domain* to start the ZTP+ process and reach ExtremeCloud IQ Site Engine. *extremecontrol.domain* should resolve to the ExtremeCloud IQ Site Engine IP address.

When the prerequisites are fulfilled and the switch is powered up, it will appear in the Discovered tab as shown in Figure 21.



Select the switch and select **Configure Devices**. In the resulting pop-up window, modify the ZTP+ settings as needed. If the site is already configured with "**Add Device Actions**", the default site can be selected as illustrated in Figure 22, such that all the site settings related to ZTP+ are inherited automatically.

Device ID	System Name	Device Nickname	Device Type	Poll Type	Site Precedence	Site	Firmware	Serial Number
2024G-00139			5520-48T-VOSS	SNMP		/World/Extreme/VO	8.4.2.0	2024G-00139
_1								
Device Add D	evice Actions Device Annota	tion VLAN Definitions Po	rts ZTP+ Device Settin	igs	4 2			
System Name:	5520-48T	Default Site:	/World/Extreme/V0	oss 👻 🖌				
Contact:	administrator	Site Assignment	/Topology Definition	ans 🖉				
		Precedence:	AWorld					
ocation:	Reading CTC	Poll Group:	/World/Extreme	*				
Administration	VO55_v3_Profile *	Poll Type:	/World/Extreme/W	oss 3 🖕				
The second se			/World/ThirdParty					
		SNMP Timeout:	2	÷				
		SNMP Retries:	3	\$				

To automatically add the VOSS/Fabric Engine switch to the policy domain and Access Control Engine group, navigate to Add Device Actions and select the appropriate Policy Domain and Access Control settings as shown in Figure 23. Then select Save.

vice ib	System Name	Device Nickname	Device Type	Poll
24G-00139			5520-48T-VOSS	SNN
	1			
Device Add Device	e Actions Device Anno	tation VRF Definitions V	LAN Definitions CLIP /	Address
Policy				
Add Device to Po	olicy Domain 2			
Policy Domain: VO	DSS_Domain 3	▼ Import	VLANs	
Access Control				
Access Control		201		
Add Device to Ad	ccess Control Engine Grou	p		
Access Control Engir	ne Group: Default		*	
Switch Type:	Layer 2	Out-Of-Band	*	
Primary Engine:	Control-	1/10.8.255.106	÷	
Secondary Engine:	None		*	4
Auth. Access Type:	Network	Access	•	
Virtual Router Name	2:			
RADIUS Attributes to	o Send: Extreme	VOSS - Per-User ACL	*	
RADIUS Accounting:	Enabled			
Management RADIU	IS Server 1: None		*	
Management RADIU	15 Server 2: None		v	
Network RADIUS Ser	rver: None		*	
Network IN DIOD DE				
Policy Enforcement	Point 1: None		X .	

NOTE

Auth Access Type "Network Access", "Management Access" and "Any Access" for VOSS/Fabric Engine switches are supported starting from ExtremeCloud IQ - Site Engine version 21.11.

NOTE

If the shared secret will be different from Access Control's default shared secret, select **Advanced Settings** under Access Control in Figure 23 and set the shared secret to match the one that will be configured on the VOSS/Fabric Engine switch. Otherwise, the default shared secret (*ETS_TAG_SHARED_SECRET*) will be used.

After saving the ZTP+ settings, the status should change to **ZTP+ Staged** as shown in Figure 24, meaning that ExtremeCloud IQ - Site Engine will now push the configured settings to the VOSS/Fabric Engine switch. If there are no issues during this process, after a couple of minutes the switch will disappear from the **Discovered** tab and will automatically be added to the respective Site under Devices.

C ExtremeClo	oud IQ Site E	ingine							90	1 4	3 0 1 0 🛛 Oroot X0Q-SE Administrator
A Network	Dashboard	Devices Discovered Firmv	vare Archives Configura	ition Templates Re	eports						
Alarms & Events	O Clear	Clear All Devices O Pre-R	egister Device 🌍 Load Co	onfiguration O	Add Devices	Configure Devices					😪 🖻 Q Refresh 30 secs 👻
Control	IP Address	Connected IP Address	Family	Туре	Serial Number	Base MAC	Profile	Status	Details	Firmware	System Description
Analytics	Discovered	ID: 2024G-00139									
🗢 Wireless	10.8.2.31	10.8.2.31	Unified Switching VOSS	5520-48T-VOSS	2024G-00139	00:04:96:f1:54:00	VOSS_v3_Profile	ZTP+ Staged	Configurati	8.4.2.0	5520-48T-VOSS (8.4.2.0_8016) (PRIVATE)
and Reports											
Tasks											
Main Administration											
₩ Connect											

Figure 24 - Status change from ZTP+ Pending Edit to ZTP+ Staged

NOTE

The initial step of configuring the ZTP+ default settings and adding the VOSS/Fabric Engine switch to the appropriate Site can also be automated with the Global IP to Site Mapping feature. Follow the steps highlighted in Figure 25 to map a subnet to a specific site such that when the switch is initially discovered, ExtremeCloud IQ - Site Engine will assign the switch to the correct Site according to this mapping.

vents	Pauline Made	manager and the second		Florid consta						
sites	Devices World Site Su	nmary Endpoir	nt Locations	Hexkeports		-4				
Name	Discover Actions VRF/	VLAN Topologie	s Service	rs Port Templates Z	TP+ Device Default	s Endpo	int Locations Analytics	Custom Variables		
▼ ♦ Extreme	Ending IP Address:			DNS Server 3:			Poll Group:	Default	*	
VOSS	Gateway Address:			DNS Search Suffix:			Poll Type:	SNMP	*	
ThirdParty	Management Interface:	Default	*	NTP Server:			Site Assignment	IP Range, LLDP	*	
tion	CLI Recovery Mode Only:	C Enabled		NTP Server 2:			Precedence:			
▼ Service Definitions	Configuration/Upgrad	de								
FC_Services	Configuration Updates:	Always	*	Firmware Upgrades:	Always	Ψ.				
	Update Date:			Upgrade Date:						
	Update Time:			Upgrade Time:						
	Update UTC Offset:			Upgrade UTC Offset:						
	Device Protocols									
	Telnet: 🕑 Enabled	HTTP:	🕑 Enabl	ed LACP:	Enabled	3	MSTP: 🐨 Enabled			
	SSH: 🕑 Enabled	HTTPS	: 🕑 Enabl	ed LLDP:	Enabled	3	POE: 🕑 Enabled			
	SNMP: 🐨 Enabled	FTP:	🕑 Enabl	ed MVRP:	Enabled		/XLAN: 🗌 Enabled			
	Global IP to Site Map	oing								
	🙆 Add 5 Edit	Delete	~ ~							
	IP Range	Associated S	ite	6 P	riority					
	10.8.0.0/16	/World/Extre	me/VOSS	• 1		_	7 _			
						Update	Cancel			



CAUTION

When a device is added to the ExtremeCloud IQ - Site Engine database, the license is checked before the Site Discover Actions are performed. The onboard status and license state of the switch can be checked from Diagnostics / System / Device Message Details, and Site Discover Actions can be verified from the Operations tab as shown in Figure 26.

											10121210	CO XIQ-SE Administrator	
Network	Profiles Users Server Information	on Licenses Certi	ficates Options Devi	ce Types Backup/Re	estore Diagnos	stics Clien	t API Access						
Alarms & Events	< Level: Diagnostic 🔻 Diagnosti	Ac > ExtremeC	loud IQ Device Messa	ge Details									
	Access Control		1 martine and a										
Analytics	Application Analytics	C Refresh	Keset Auto C	inboard ExtremeCloud IQ	ų - Site Engine	Force Onboar	rd to ExtremeLi	oud IQ !	end Statistics to	ExtremeCloud IQ Show ExtremeCloud IQ	2 Messages		9
Wireless	Flows	IP Address	Туре	Serial Number	Quality	Total	Success	Failed	Onboard	Onboard Status	License State	Health Last Sent	
	Beta Features	20.0.209.20	Cisco 3750	FOC0937U1VR	100	1	1	0	true	DEVICE_ALREADY_REPORTED_BY_XM	XIQ_NAVIGATOR	11/01/2021 04:14:11 PM	
eports	Client	10.8.255.106	Virtual Access Cont	0050568654E9	100	1	1	0	true	DEVICE_ALREADY_REPORTED_BY_XM	XIQ_PILOT	N/A	
asks	Experimental Features	10.8.255.105	XIQ_SE	XIQSE-81AE2844	70 100	1	1	0	true	SUCCESS	XIQ_PILOT	11/01/2021 04:14:11 PM	
dministration	Historical Statistic Collector	10.8.9.32	E1120		N/A	0	0	0	false	UNKNOWN	DO_NOT_ONB	N/A	
	Server	10.8.9.31	E1120		N/A	0	0	0	false	UNKNOWN	DO_NOT_ONB	N/A	
	Support	10.8.3.12	5520-48T-VOSS	2024G-00139	100	1	1	0	true	SUCCESS	XIQ_PILOT	11/01/2021 04:14:11 PM	
	Add Device Thread Alarm/Event Details Device Status Details Endpoint Cache												
	Add Device Thread Alarm/Event Details Device Status Details Endpoint Cache ExtremeCloud IQ Device Messag	ge Det	Reset				-					Display	ting
	Add Device Thread Alarm/Event Details Device Status Details Endpoint Cache ExtremeCloud (Q Device Messa Start Time	ge Det , Ø Type	Reset Target Result	Progress L	.ast Time	в	- Message					Display User	ring
	Add Device Thread Alarm/Event Details Device Status Details Endpoint Cache ExtremeCloud (Q Device Messar Start Time Discover Site Actions - Mee Mon Nivo (3 2021 14-55:14	ge Det , 20 1 14:55:05 Nixcover Site Action	Reset Target Result GMT+0100 (Central Europ 1 Devices Success	Progress L eean Standard Time) =	.ast Time → Progress: 1009	6 - Success 14:56:1	Message	ction: Trao B	ereiver Repistra	tion		Display User Server	ring
	Add Device Thread Alarm/Event Details Device Status Details Endpoint Cache ExtremeCloud (Q Device Messay Start Time Discover Site Actions - Mer Mon Nov 01 2021 14:55:14 Mon Nov 01 2021 14:55:14	Type Nev 01 2021 14:55:05 Discover Site Acti	Reset Target Result GMT-0100 (Central Europ 1 Devices Success 1 Devices Success	Progress L ean Standard Time) = 100% N	.ast Time ⇒ Progress: 1009 Von Nov 01 2021 Von Nov 01 2021	No - Success 14:55:1 5 14:55:3 5	Message Site Discover Ar	ction: Trap F	eceiver Registra Receiver Rezist	tion		Display User Server Server	ring
	Add Device Thread Alarm/Event Details Device Status Details Endpoint Cache ExtremeCloud (Q Device Messay Start Time Discover Site Actions - Mee Mon Nov 01 2021 14:55:14 Mon Nov 01 2021 14:55:14	se Det Type Nov 01 2021 14:55:05 Discover Site ActL Discover Site ActL	Reset Target Result GMT-0100 (Central Europ 1 Devices Success 1 Devices Success	Progress L exan Standard Time) = 100% // 100% // 100% //	.ast Time → Progress: 1009 Vion Nov 01 2021 Vion Nov 01 2021 Vion Nov 01 2021	6 - Success 14:56:1 5 14:55:3 5	Message Site Discover Ai Site Discover Ai	ction: Trap F ction: Syslog	eceiver Registra Receiver Regist	tion ration		Display User Server Server Server	ring
	Add Device Thread Alarm/Event Details Device Status Details Endpoint Cache ExtremeCloud () Device Messag Start Time Discover Site Actions - Mon Mon Nov 01 2021 14-55:14 Mon Nov 01 2021 14-55:14 Mon Nov 01 2021 14-55:14	ge Det Type C G Nov 01 2021 14:55:05 Discover Site ActL. Discover Site ActL.	Reset Target Result GMT-0109 (Central Europ 1 Devices Success 1 Devices Success 1 Devices Success	Progress L exan Standard Time) = 100% // 100% // 100% // 100% //	.ast Time → Progress: 1009 Vion Nov 01 2021 Vion Nov 01 2021 Vion Nov 01 2021 Vion Nov 01 2021	6 - Success 14:56:1 S 14:55:3 S 14:55:3 S 14:55:3 S	Vessage Site Discover Ar Site Discover Ar Site Discover Ar Site Discover Ar	ction: Trap R ction: Syslog ction: Add to	eceiver Registra Receiver Registra Archive (Comp Policy Domain	tion ration (eta)	Enforce Complete)	Display User Server Server Server	ring
	Add Device Thread Alarm/Event Details Device Status Details Endpoint Cache ExtremeCloud IQ Device Messay Start Time Discover Site Actions - Mori Mon Nov 01 2021 14:55:14 Mon Nov 01 2021 14:55:14 Mon Nov 01 2021 14:55:14 Mon Nov 01 2021 14:55:14	ge Det Type Nov 01 2021 1425:05 Discover Site ActL. Discover Site ActL. Discover Site ActL.	Reset Target Result GMT-0100 (Central Europ 1 Devices Success 1 Devices Success 1 Devices Success 1 Devices Success	Progress L exan Standard Time) = 100% N 100% N 100% N 100% N		Ne - Success 14:56:1 5 14:55:3 5 14:55:3 5 14:56:0 5 14:56:0 5	Message Site Discover A Site Discover A Site Discover A Site Discover A	ction: Trap R ction: Syslog ction: Add to ction: Add to ction: Port D	eceiver Registra Receiver Registr Archive (Comp Policy Domain efault Role (Domain	ition ration ieta] / Enforce [Successfully added to domain / I	Enforce Complete)	Display User Server Server Server Server	ring
	Add Device Thread Alarm/Event Details Device Status Details Endpoint Cache StartsmeCloud IO Device Messay Start Time Discover Site Actions - Mori Mon Nov 01 2021 14:55:14 Mon Nov 01 2021 14:55:14 Mon Nov 01 2021 14:55:14 Mon Nov 01 2021 14:55:14 Mon Nov 01 2021 15:51:4	ge Det Type Nov 01 2021 14:55:05 Discover Site ActL Discover Site ActL Discover Site ActL Discover Site ActL	Reset Target Result GMT-0100 (Central Europ 1 Devices Success 1 Devices Success 1 Devices Success 1 Devices Success 1 Devices Comple	Progress L exan Standard Time) = 100% // 100% // 100% // 100% // te 100% //	Last Time → Progress: 1009 Mon Nov 01 2021 Mon Nov 01 2021 Mon Nov 01 2021 Mon Nov 02 2021 Mon Nov 02 2021 Mon Nov 02 2021	b Success 14:56:1 5 14:55:3 5 14:55:3 5 14:55:3 5 14:55:3 5	Message Site Discover A Site Discover A Site Discover A Site Discover A Site Discover A	ction: Trap F ction: Syslog ction: Add to ction: Add to ction: Port D	eceiver Registra Receiver Registra Archive (Comp Policy Domain efault Role (Por	tion ration ete) / Enforce [Successfully added to domain / I t default role set successfully]	Enforce Complete]	Display User Server Server Server Server Server	ring
	Add Device Thread Alarm/Event Details Device Status Details Endpoint Cache ExtremeCloud (O Device Messay Start Time Discover Site Actions - Mao Mon Nov 01 2021 14:55:14 Mon Nov 01 2021 14:55:14 Mon Nov 01 2021 14:55:14 Mon Nov 01 2021 14:55:14 Mon Nov 01 2021 14:55:14	Type Type New 01 2021 145:305 Discover Site ActL. Discover Site ActL. Discover Site ActL. Discover Site ActL. Discover Site ActL.	Reset Target Result GMT-9100 (Central Europs) 1 Devices Success 1 Devices Success 1 Devices Success 1 Devices Complet Devices Complet	Progress L Rean Standard Time) = 100% M 100% M 100% M 100% M 100% M	Last Time => Progress: 100 ¹ Won Nov 01 2021 Won Nov 02 2021	h Success 14:56:1 S 14:55:3 S	Message Site Discover Ar Site Discover Ar Site Discover Ar Site Discover Ar Site Discover Ar Site Discover Ar	ction: Trap F ction: Syslog ction: Add to ction: Add to ction: Port D ction: Enable ction: Add d	eceiver Registra Receiver Registra Archive [Comp Policy Domain Policy Domain Fault Role (Por Collection Collection	tion ration fetg] / Enforce [Successfully added to domain / i default role set successfully]	Enforce Complete)	Display User Server Server Server Server Server Server	ring
	Add Device Thread Alarm/Event Details Device Status Details Endpoint Cache EstremeCloud (Q Device Messar Start Time Discover Site Actions - Mer Mon Nov 01 2021 14:55:14 Mon Nov 01 2021 14:55:14	Type Type Nev of 2021 14:55:05 Discover Site ActL Discover Site ActL Discover Site ActL Discover Site ActL Discover Site ActL Discover Site ActL Discover Site ActL	Reset Target Result GMT-6100 (Central Europ 1 Devices Success 1 Devices Success 1 Devices Success 1 Devices Comple 1 Devices Comple	Progress L Mean Standard Time) = 1004 A 1006 A 1006 A 1006 A 1006 A 1006 A 1006 A	Last Time → Progress: 100% Mon Nov 01 2021 Mon Nov 02 2021 Mon Nov 02 2021	6 - Success 14:56:1 5 14:55:3 5 14:55:3 5 14:55:3 5 14:55:3 5 14:55:3 5 14:55:3 5	Message Site Discover Ar Site Discover Ar Site Discover Ar Site Discover Ar Site Discover Ar Site Discover Ar Site Discover Ar	ction: Trap R ction: Syslog ction: Add to ction: Add to ction: Port D ction: Enable ction: Add d ction: Add to	eceiver Registra Receiver Regist Archive (Comp Policy Domain efault Role (Por Collection vice completer Access Control	tion ration 4 Enforce (Successfully added to domain / I default role set successfully) 1 Engine Group	Enforce Complete)	Display User Server Server Server Server Server Server Server	ring

Figure 26 - Switch Onboard Status and License State Verification

Navigate to the policy domain and select Devices/Port Groups as shown in Figure 27 to validate that the VOSS/Fabric Engine switch was added to the domain.

ExtremeClo	oud IQ Site Engine		
A Network	Dashboard Policy Access Control En	d-Systems Reports	
🜲 Alarms & Events	🌆 Open/Manage Domain(s) 👻 📑 Global D	lomain Settings 👻 🎆 Tools 👻	
	Domain: VOSS_Domain		
	Roles/Services	+ Ports General User Ses	sions Authentication RADIUS
Reports	Class of Service	+ 11 - € Export to CSV	
Tasks	VLANs	+ Name	Default Role Alia
😁 Administration	Network Resources	+ 5520-48T-VOSS [2 ports]	
≓ Connect	Devices Port Groups	 Slot 1 [48 ports] Slot 2 [4 ports] Slot 2 [4 ports] Ports [2 ports] 	
	by IP • IP (1 device) • 10.8.3.x (1 device) • VOSS_5520-48T 3	Gther Components	

Figure 27 - VOSS/Fabric Engine switch added to the policy domain via ZTP+

Finally, navigate to **Access Control** and select **Engines** to verify that the VOSS/Fabric Engine switch is also added to the Control Engine group.

C ExtremeClo	ud IQ Site Engine								△ 10 2 2 0	O root XIQ-SE Administrator	E
A Network	Dashboard Policy Access Control	End-Systems Reports									
🌲 Alarms & Events	Configuration	Engine - Contr	ol-1/10.8.255.106								
Control	÷	Details End G	there Candebar	2							
Analytics	Group Editor	E Details end-sy	sterns Switches	.							
🗢 Wireless	Engines 2	- Add	Edit 🤤 Delete	C Refresh							
[ili] Reports	 Engine Groups 	IP Address 1	Nickname	Status	System Name	Primary Engine	Policy/VLAN	Policy Domai	a Autř	hentication Access Type	
Tasks	▼ Default	10.8.3.12	VOS5_5520-48T	Contact Established	VOS5_5520-48T	10.8.255.106	Extreme VOSS - Per-User ACL	VOSS_Domain	n Neti	work Access 4	
Mainistration	Control-1/10.8.255.106										
	 All Engines 										



CAUTION

In the tested version of ExtremeCloud IQ - Site Engine (21.11.10.57), when VOSS/Fabric Engine devices are added to ExtremeControl through ZTP+ or through run site actions, the **Extreme Policy** attribute is assigned by default as **Radius Attributes to Send**. This will be corrected in a future release. As a workaround, manually change the attribute value to **Extreme VOSS - Per-User ACL** so that you can use Downloadable ACLs.

Access Control Preparation

Step 1: AAA Configuration

Under Access Control, select the Configuration section, expand AAA in the Configuration tree, and rightclick the Default AAA configuration. Select Make Advanced.

ExtremeClo	ud IQ Site Engine				
A Network	Dashboard Policy Access Control	End-Systems Reports			
🔔 Alarms & Events	Configuration	Basic AAA Configuration -	Test		
Control	▼ Configurations	Authenticate Requests Loca	IIV for: MAC (All) MAC (PAP) MAC (CHAP)	MAC (MsCHAP)	MAC (EAP-MD5)
Analytics	▼ Default	<u> </u>			
< Wireless	Rules	Primary RADIUS Server:	None	•	
Lini Reports	AAA: Default	Secondary RADIUS Server:	None	~	
📰 Tasks	Portal: Default	LDAP Configuration:	None	-	
🐸 Administration	▼ AAA	Local Password Repository:	Default	Ŧ	
≓ Connect	Test	Update Trusted Authorities	No information available.		
	LDAP Con Local Pass RADIUS Servers Profiles Captive Portals Notifications Vendor RADIUS Attributes Global & Engine Settings	uration 4			
	Group Editor	•			
	Engines 🕇	•			
Help	Enforce C Refresh				

Figure 29 - AAA Configuration - 1

Select the Any authentication rule and then select Edit.

NELWORK	Dashboard Policy Access Control En	d-Systems Re	ports											
Alarms & Events	Configuration -	Advanced	AAA Configura	tion - Defau	lt									
Control Analytics	 ✓ Configurations ▶ Default 	Authentic	ate Requests Loca rd Repository:	ally for: 🕑 M	IAC (All)									
Reports	▼ AAA Default	Join AD Doma	in:	Auto Deter	ct			Ŧ						
Tasks Administration	LDAP Configurations Local Password Repository RADIUS Servers 	Update Tr Authentica	usted Authorities	No inform	nation available.									
	 Profiles 	🔾 Add 🌘	📑 Edit 😂	Delete	▲ Up ▼ Do	n								
	Captive Portais Notifications Vendor RADIUS Attributes	Authentica Type	User/MAC/ Match	Location	Authentica Method	Primary RADIUS Server	Secondary RADIUS Server	3rd RADIUS Server	4th RADIUS Server	inject Authentica Attrs	Inject Accounting Attrs	LDAP Configurati	LDAP Policy Mapping	Fall-through
	Global & Engine Settings	Any	*	Any	LDAP Auth	None	None	None	None	None	None	Reading ADs	Default	

Figure 30 – AAA Configuration - 2

In this section, LDAP Authentication will be used. In the **Edit User to Authentication Mapping** window, change the **Authentication Method** to **LDAP Authentication** and then select **OK**.

thentication Type:	Any	
er/MAC/Host: 💿 Pattern 🔿	Group *	
cation:	Any	1
thentication Method:	Proxy RADIUS (Failover)	
Primary RADIUS Server:	Proxy RADIUS (Failover)	
Secondary RADIUS Server:	LDAP Authentication	
3rd RADIUS Server:	Local Authentication	
4th RADIUS Server:	None	*
5th RADIUS Server:	None	-
6th RADIUS Server:	None	-
7th RADIUS Server:	None	Ť
8th RADIUS Server:	None	*
Inject Authentication Attrs:	None	•
Inject Accounting Attrs:	None	*

Figure 31 - AAA Configuration - LDAP Authentication Setting

After you select **LDAP Authentication**, a new LDAP configuration needs to be created so that Extreme Control can communicate with Active Directory. Select the drop-down menu in **LDAP Configuration** and then select **New** as shown in Figure 32.

dit User to Authentica	tion Mapping	
uthentication Type:	Any	*
Iser/MAC/Host: 💿 Pattern	O Group *	
ocation:	Any	*
uthentication Method:	LDAP Authentication	*
LDAP Authentication Type	4	
Supported RADIUS Type:		
DAP Configuration:	None	÷
DAP Policy Mapping;	New	
	Manage None	
	Reading ADs	ø

Figure 32 - AAA Configuration - Add LDAP Configuration - 1

Follow the steps illustrated in Figure 33 to populate LDAP configuration fields.

- 1- Configuration Name: Give a name to the LDAP Configuration
- 2- LDAP Connection URL: Select the Add button and provide the IP address of the LDAP server(s). The URL format must be the following: Idap://a.b.c.d:389 or Idaps://a.b.c.d:636. More than 1 LDAP Server is recommended for high availability.
- 3- Administrator Username and Password: *DOMAIN\Username* of LDAP user to perform LDAP lookups and password of username.
- 4- Search settings: To create the search roots, FQDN of the domain needs to be broken into separate DC= statements, command delimited. And add CN=Users and CN=Computers at the beginning of User and Computer search roots respectively.
- 5- Populate Default Values: At the bottom , select Populate Default Values, select Active Directory User Defaults, and then select Save.

iguration Name:	teading ADs
DAP Connection URLs	
2 Edit	🤤 Delete 🔺 Up 🔻 Down
ldap://10.8.255.160:389	
authentication Settings	
Administrator Username:	READING\xmc
Administrator Password:	(
Timeout (seconds):	4 🌲
earch Settings	
1	
User Search Root:	CN=Users.DC=reading.DC=ctc.DC=local
User Search Root: Host Search Root:	CN=Users,DC=reading,DC=ctc,DC=local CN=Computers,DC=reading,DC=ctc,DC=local
User Search Root: Host Search Root: OU Search Root:	CN=Users,DC=reading,DC=ctc,DC=local CN=Computers,DC=reading,DC=ctc,DC=local DC=reading,DC=ctc,DC=local
User Search Root: Host Search Root: OU Search Root: Schema Definition	CN=Users,DC=reading,DC=ctc,DC=local CN=Computers,DC=reading,DC=ctc,DC=local DC=reading,DC=ctc,DC=local
User Search Root: Host Search Root: OU Search Root: Schema Definition User Object Class:	CN=Users,DC=reading,DC=ctc,DC=local CN=Computers,DC=reading,DC=ctc,DC=local DC=reading,DC=ctc,DC=local user
User Search Root: Host Search Root: OU Search Root: Schema Definition User Object Class: User Search Attribute:	CN=Users.DC=reading.DC=ctc.DC=local CN=Computers.DC=reading.DC=ctc.DC=local DC=reading.DC=ctc.DC=local user sAMAccountName
User Search Root: Host Search Root: OU Search Root: Schema Definition User Object Class: User Search Attribute: Keep Domain Name for User	CN=Users.DC=reading.DC=ctc.DC=local CN=Computers.DC=reading.DC=ctc.DC=local DC=reading.DC=ctc.DC=local user sAMAccountName Lookup:
User Search Root: Host Search Root: OU Search Root: Schema Definition User Object Class: User Search Attribute: Keep Domain Name for User User Authentication Type:	CN=Users.DC=reading.DC=ctc.DC=local CN=Computers.DC=reading.DC=ctc.DC=local DC=reading.DC=ctc.DC=local user sAMAccountName r Lookup: NTLM Authentication
User Search Root: Host Search Root: OU Search Root: Schema Definition User Object Class: User Search Attribute: Keep Domain Name for User User Authentication Type: User Password Attribute:	CN=Users.DC=reading.DC=ctc.DC=local CN=Computers.DC=reading.DC=ctc.DC=local DC=reading.DC=ctc.DC=local user sAMAccountName r Lookup: NTLM Authentication *

Figure 33 - AAA Configuration - Add LDAP Configuration - 2

Save the configuration, and Enforce again as shown in Figure 34.

A Network	Dashboard Policy Access Control E	End-Systems Rej	orts												
Alarms & Events	Configuration –	Advanced A	AA Configura	ition - Default	t										
Control Analytics Wireless Mreports Tasks	Configurations Default AAA Default LDAP Configurations	Authentica Local Passwor Join AD Doma Updste Tri	te Requests Loo d Repository: n: sted Authorities	ally for: I MA Default Auto Detect	AC (All) I M			() MAC (MSCH • •							
😁 Administration	 Local Password Repository RADIUS Servers 	Authentica	Authentication Rules												
	 Profiles 	Add	👿 Edit 🧯	Delete	⊾Up ▼ Dov	vin									
	Captive Portals Notifications Vendor RADIUS Attributes	Authentica Type	User/MAC/ Match	Location	Authentica Method	Primary RADIUS Server	Secondary RADIUS Server	3rd RADIUS Server	4th RADIUS Server	Inject Authentica Attrs	Inject Accounting Attrs	LDAP Configurati	LDAP Policy Mapping	Fall-through	
	 Global & Engine Settings 	Any	*	Any	Local Auth	None	None	None	None	None	None	None	Default		
			Acces	s Control Engi Engine Control-1 Reconfiguration	IP Address 10.8.255.106	Status Audit Comp	Result Pass	Detail: Captive Portal	Enforce All	* ×					
	Group Editor +														
	Engines +														

Figure 34 – How to enforce the configuration in ExtremeControl

Step 2: Create Rules

In order to test the Downloadable ACL configuration, 802.1X authentication will be used and an LDAP User Group will be created and added as a Rule Condition. To accomplish this, select the **Access Control** tab and expand **Configurations > Default**. Select **Rules** and then add a new rule.

C ExtremeClo	ud IQ Site Engine				
A Network	Dashboard Policy Access Control	d-Systems Report	5		
Alarms & Events	Configuration –	Rules			
Analytics	Configurations Default	Enabled	Edit 👸 Copy 🥥 Delete	Profile	dvanced Locations Descripti
🗢 Wireless	Rules 2	• •	Blacklist	Quarantine NAC Profile	
III Reports	AAA: Default	• •	Assessment Warning	Notification NAC Profile	
🧱 Tasks	Portal: Default	0	Access Point	Access Point NAC Profile	
警 Administration	AAA	0	Server	Server NAC Profile	
≓ Connect	Profiles	0	Printer	Printer NAC Profile	
	Captive Portais	0	VoIP Phone	VolP Phone NAC Profile	
	Notifications Vendor RADIUS Attributes	« < Pag	ge 1 of 1 > > C		-
	 Global & Engine Settings 	Accept Policy	- Role Details (Domain: Cisco_Wi	red)	
		Specify/Chang	e Domain 🔅 View/Edit Domain		
		Role / Service / Ru	le	Summary	

Figure 35 - How to add a new rule in Access Control - 1

Name the rule **Contractor_Rule**. Then select the **User Group** drop-down list and select **New**. Select **LDAP User Group** as the Type, and name the User Group **Contractor_Users**.

Name:	Contractor_Rule	⊠ R	ule Enabled
Description:			
Group Label:	None		Ŧ
Conditions			
Authentication Method:	Any	*	🗍 Invert
User Group:	Any	٣	🗌 invert
End-System Group:	New		Invert
Device Type Group:	Any		🗌 Invert
Location Group:	Local Password Repository		🗍 Invert
Time Group:	Users		Invert
Actions	Administrators Contractor Users	0	
ACTIONS .			

Figure 36 - How to add a new rule in Access Control - 2

Name:	A unique name for this group	liis	Description:	Optionally add a description to	
Гуре:	User: LDAP User Group	Ŧ]	uns grou	ab.
Mode:	User: LDAP User Group User: RADIUS User Group				
🗿 Add 👩	User: Username		ribute Lookup	OU Import	4
			noute cookup	oo importaa	
Attribute Name		Attribute Value	indue coordp	oo mporen	Description

Figure 37 - How to create an LDAP User Group in Access Control - 1

At this point, there is no link between the created User Group and LDAP Server. Therefore, Attribute Name and Value pair need to be added to this LDAP User Group in order to look the user up in LDAP Server during the authentication process. Easiest way to add Attribute Name and Value pair is to select **Attribute Lookup** as shown in Figure 38 and search for a known user name belonging to the relevant LDAP User group, which is in our example Contractors.

Create Gro	oup				×	
Name:	Contractor_Users		Description:	: Optionally add a description to this group.		
Type:	User: LDAP User Group	T .,		uns group.		
Mode:	Match Any O Match	All O Exists				
🗿 Add	📑 Edit 📴 Copy 🤤	Delete Attr	ibute Lookup	OU Import	₹.	
Attribute Na	ame	Attribute Value	Qu	ery LDAP for attributes to add to	this grou	
				No data tr		
« <	Page 0 of 0 > 22		ier.	No data to	display	

Figure 38 How to create an LDAP User Group in Access Control - 2

Select the LDAP Configuration created in Figure 33 and search for an Active Directory user belonging to Contractors OU. Then add the **memberOf** attribute name and value pair as shown in Figure 39.

L	DAP Attribute Lookup	×
U	Iser Search Connection Test	
sAN	AccountName contractor1	1 Search
	Attribute Name	Attribute Value
	lastLogon	0
	lastLogonTimestamp	132338602216801604
	logonCount	• 2
S	memberOf	CN=Contractors,CN=Demo and Test,CN=Users,DC=reading,DC=ctc,DC=I
	name	contractor1
	objectCategory	CN=Person.CN=Schema.CN=Configuration.DC=reading.DC=ctc.DC=local
	objectClass	top
	objectClass	person
	objectClass	organizationalPerson
	objectClass	user 3 -

Figure 39 - How to create an LDAP User Group in Access Control - 3

The LDAP User Group and the Access Control rule will look like the ones depicted in Figure 40 and Figure 41, respectively.

Name:	Contra	actor_Users	Description:	Optionally add a descripti	on to
Туре:		LDAP User Group 👻		this group.	
Mode:	⊙ Mat	ch Any O Match All O Exists			
🗿 Add	👩 Edit	🛃 Copy 🤤 Delete 🖪 Attri	ibute Lookup	OU Import	V .
Attribute Na	ame	Attribute Value			Descri
memberOf		CN=Contractors,CN=Demo and Test,CN=	Users.DC=reading,	DC=ctc.DC=local	
« <	Page 1	of 1 > > 🞜 🚃 Res	et	Displayir	ng 1 - 1 of ′
	-	-			

Figure 40 – LDAP User Group Example

Name:	Contractor_Rule	∀ R	tule Enabled
Description:			
Group Label:	None		•
Conditions			
Authentication Method:	Any		🗍 Invert
User Group:	Contractor_Users	Ŧ	🗌 Invert
End-System Group:	Алу	Ŧ	[] Invert
Device Type Group:	Any		🗍 Invert
Location Group:	Any	Ŧ	🗍 Invert
Time Group:	Any	*	🗌 invert
ctions			
Profile:	Contractor Profile (Auto)		-
	-		More

Figure 41 - Rule example with User Group condition

Additional conditions can be added to the rule depending on the use-case. When the rule is created, remember to enforce this configuration to Access Control Engine(s).

Note

Profiles for each role created in the policy domain are auto-created when a switch is added to the Access Control Engine group with the same policy domain.

VOSS/Fabric Engine Switch Configuration

The main goal is to minimize manual CLI configuration of the VOSS/Fabric Engine switch as much as possible. Below are snippets of CLI commands needed for specific features. When ZTP+ is used as the switch discovery method, which is the preferred method for this guide, both SNMP and RADIUS configurations will also be automated. All the rest of the configuration is automated through ZTP+ and Auto-sense functionalities.

SNMP Configuration

SNMP configuration is sent to the switch during onboarding via ZTP+. Below are the CLI commands in case manual configuration is preferred.

```
conf t
cli password xmc read-write-all
Do you want to change username for the default RWA user ?
(y/n) ? y
Enter the old password : rwa
Enter the New password : password
Re-enter the New password : password
snmp-server user snmpuser sha snmpauthcred aes snmpprivcred
snmp-server user snmpuser group initial
no snmp-server user initial
```

RADIUS Configuration

```
config terminal
radius server host 10.8.255.106 key ETS_TAG_SHARED_SECRET used-by eapol
radius enable
radius accounting enable
radius dynamic-server client 10.8.255.106 secret ETS_TAG_SHARED_SECRET enable
eapol enable
end
```

Verification - Client Testing

Clients that are attached to the VOSS/Fabric Engine switch with 802.1X supplicants properly configured will be 802.1X authenticated. When the user logs-in with the appropriate user credentials that belong to Contractors OU in the Active Directory, the Rule Engine processes the authentication request. The Rule Engine selects the rule for which all the conditions are "True" (conditions are logically "AND"ed), and the respective profile is applied.

If for some reason the desired rule and profile are not applied, the **Configuration Evaluation Tool** can help you troubleshoot the Rule Engine settings. The tool can be accessed directly from the End-Systems table by right clicking on the end-system in question as shown in Figure 42.

ExtremeClo	oud IQ Site Engine											Q 0 0 4	10 4 2 0 🛛 🛪	ot 2-SE Administrator	E
A Network	Dashboard Policy	Access Control End-S	stems Reports												
🔔 Alarms & Events	🍰 Add To Group 🙀	Force Reauthentication	Tools •	• Live •	All End-Syste	m Events						Devices: All	• 00:50:56:86:5D:F1		x Q
Control			MAC OUI	Device							-				
Analytics	S. Last Seen 1	MAC Address	Vendor	Family	Device Type	IP Address		tost Name	User Name		Authentication Type	Reason	Profile	Policy	Site
🗢 Wireless	11/5/2021 9:23:12	00:50:56:86:5D:F1	VMware, Inc.	Windows	Windows 8	20.2.220.82		Show Details	READINGVO	ontractor1	802.1X (PEAP)	Rule: "Contractor_Rule"	Contractor Profile (Auto)		/Worl
Land Reports								Add To Group							
📰 Tasks								Edit Custom Infor	mation						
🐸 Administration							۲	Lock MAC							
							1	Force Reauthentic	ation						
							100	Force ReAuth and	Scan						
							•	Delete							
							0	WebView							
								Ping							
								PortView							
								Search Maps							
	×	and a set		l 🖻 Realman			10	Export Selection						Diselacion	*
	<	ori >	C D Reset	Bookma	ink		G	Configuration Eva	luation Tool					Uisplaying 1	- 1 07 1
	End-System Events a	and Health Results					-	Policy							*
	등 🛞 Export End-Sys	stem Events 🛛 🕄 Refr	esh				Ľ.	Policy	Sim	ulate running t	the NAC rule engine using	g the selected end-system re	cord.	Υ.	Q

Figure 42 - Configuration Evaluation Tool

The assigned profile and ACL entries can be verified on the VOSS/Fabric Engine switch by issuing the command **show eapol sessions eap** *PortNum* verbose and **show filter acl.** See Figures 43 and 44. More VOSS/Fabric Engine CLI commands to verify and troubleshoot authentication and authorization steps can be found in the troubleshooting appendix.

voss_	5520-48T:1 show eap	ol sessions eap 1/	5 verb	ose						
*****	*********				*******	*********	******			
	Command	Execution Time: Tu	e Nov	02 11	:13:45 202	1 GMT				
*****	*************	******	*****	*****	*******	**********	******			
						Eap Oper Stat	us Verbose			
PORT	MAC	PAE	VLAN	PRI	Flex-UNI	I-SID	VLAN: I-SID	AC	L ACEs	RADIUS DYNAMIC
NUM		STATUS	ID		Enable	SOURCE				SETTINGS
								<mark>-</mark>		
1/5	00:50:56:86:5d:f1	authenticated	N/A		true	radius	0:2800210	1	1,2,3,4,	
								(5,6)
Total	Number of EAP sess	ions : 1								

Figure 43 - Verify EAP Session Details from the VOSS/Fabric Engine CLI

1088	_5520 *****	-48T:1tshow filter acl	ace	****** e Nov 0	*******	****	********)21 GMT	*****
***	*****	******	******	******	******	****	******	*****
		Ace A	ction Tabl	e (Part	I) 			
\cl	Ace	AceName	Admin	Oper	Mode	Mlt	Remark	Remark
d	Id		State	State		Id	DSCP	Dot1p
	1	1 Deny Telnet	Enable	Up	deny	0	disable	disable
	2	2 Deny SSH	Enable	Up	deny	0	disable	disable
	3	3 Deny FTP	Enable	Up	deny	0	disable	disable
	4	4 Deny TFTP	Enable	Up	deny	0	disable	disable
	5	5 Deny Server RDP	Enable	Up	deny	0	disable	disable
	~					~		-141-1 -

Figure 44 - Verify Downloadable ACL Details from the VOSS/Fabric Engine CLI

The End-System table Authorization column also shows the Downloadable ACL which is sent to the VOSS/Fabric Engine switch as seen in Figure 45.

	oard Policy Ac	cess Control End-Sy	stems Reports											
5 🔬 Ad	d To Group 🏼 🔏 I	Force Reauthentication	🍪 Tools 💌	● Live ▼	All End-Sy	ystem Events					🌏 📔 Devic	es: All 👻 00:50	0:56:86:5D:F1	
S. La	st Seen ↓	MAC Address	MAC OUI Vendor	Device Family	Device Type	IP Address	Host Name	User Name	Authentication Type	Reason	Profi	le	Authorization	n
© 11,	/2/2021 11:08:41	00:50:56:86:5D:F1	VMware, Inc.	Windows	Windows B	20.2.220.82	WIN10-C	READING\contractor1	802.1X (PEAP)	Rule: "Contractor	_R Cont	ractor Profile A	Extreme-Dyna	amic-ACL
											_		Extreme-Dyn	namic-AC
													Contractor Extreme-Dyn	namic-AC
													Extreme-Dyn 1 Deny Teln	namic-AC
													0x800 & ip ip	p-protoci
													Extreme-Dyn 2 Denv SSH	namic-AC
													0x800 & ip ip	p-protoc
×	2 A 1			1 - 1									Extreme-Dyn	namic-A(
~	C Page 1	of1 > >>	C 📑 Rese	t 🙀 Bookm	ark								& ip ip proto	col-type
End-S	ystem Events and	d Health Results											Extreme-Dyn	namic-A
£	Export End-Syster	n Events C Refre	sh										4_Deny_TFTF 0x800 & ip ip	P ethern p-protoc
e e			Device									Switch	Extreme-Dyn 5 Deny Serv	namic-A ver RDP
		MAC Address	Family	Device Type	P Address	Host Name	User Na	me Auth Type	Reason	Profile	Switch IP	Nickname	eq 0x800 & ij protocol dst-	ip ip-pro
50	5. Time Stamp													
Events	5. Time Stamp 11/2/2021 11:08	.22 00:50:56:86:50	F1 Windows	Windows 8.		WIN10-C	READIN	G\cont 802.1X (PEA)	P) Rule: "Cont	Contractor	10.8.3.12	VOSS_5520-481	20.1.110.100	0 & actio
Events	5. Time Stamp 11/2/2021 11:08 11/2/2021 11:08	22 00:50:56:86:50	:F1 Windows	Windows 8. Windows 8.		WIN10-C WIN10-C	READIN READIN	G\cont 802.1X (PEA) G\cont 802.1X (PEA)	P) Rule: "Cont P) Rule: "Cont	Contractor	10.8.3.12 10.8.3.12	VOSS_5520-481	20.1.110.100 Extreme-Dyn action permi	0 & actio namic-Al it
Events	S Time Stamp 11/2/2021 11:08 11/2/2021 11:08 11/2/2021 11:06	22 00:50:56:86:50 22 00:50:56:86:50 11 00:50:56:86:50	::F1 Windows ::F1 Windows ::F1 Windows	Windows 8. Windows 8. Windows 8.	 	WIN10-C WIN10-C 2 WIN10-C	READIN READIN host/Wi	G\cont 802.1X (PEA) G\cont 802.1X (PEA) N10-C 802.1X (PEA)	P) Rule: "Cont. P) Rule: "Cont P) Rule: "Dom	Contractor Contractor Operator P	10.8.3.12 10.8.3.12 10.8.3.12	VOSS_5520-481 VOSS_5520-481 VOSS_5520-481	20.1.110.100 Extreme-Dyn action permi FA-VLAN-ISIC	0 & actio namic-A it' D='0:280
Events	S Time Stamp 11/2/2021 11:08 11/2/2021 11:08 11/2/2021 11:06 11/2/2021 11:05	22 00:50:56:86:50 22 00:50:56:86:50 11 00:50:56:86:50 58 00:50:56:86:50	kF1 Windows kF1 Windows kF1 Windows kF1 Windows	Windows 8. Windows 8. Windows 8. Windows 8.		WIN10-C WIN10-C 2 WIN10-C 2 WIN10-C	READIN READIN host/Wi	G\cont 802.1X (PEA) G\cont 802.1X (PEA) N10-C 802.1X (PEA) MAC (PAP)	P) Rule: "Cont P) Rule: "Cont P) Rule: "Dom Rule: "Unre.	Contractor Contractor Operator P Unregister	10.8.3.12 10.8.3.12 10.8.3.12 10.8.3.12	VOSS_5520-481 VOSS_5520-481 VOSS_5520-481 VOSS_5520-481	20.1.110.100 Extreme-Dyn action permi FA-VLAN-ISIC 1/5	D & actio namic-Al it' D='0:280
Events	S Time Stamp 11/2/2021 11:08 11/2/2021 11:08 11/2/2021 11:06 11/2/2021 11:05 11/2/2021 11:05	22 00:50:56:86:50 22 00:50:56:86:50 211 00:50:56:86:50 558 00:50:56:86:50 53 00:50:56:86:50	EFI Windows EFI Windows EFI Windows EFI Windows EFI Windows EFI Windows	Windows 8. Windows 8. Windows 8. Windows 8.		WIN10-C WIN10-C 2 WIN10-C 2 WIN10-C 2 WIN10-C 2 WIN10-C 2 WIN10-C	READIN READIN host/Wi	Sicont 802.1X (PEA) Sicont 802.1X (PEA) N10-C 802.1X (PEA) MAC (PAP) MAC (PAP)	P) Rule: "Cont P) Rule: "Cont P) Rule: "Cont P) Rule: "Cont Rule: "Unre Rule: "Unre	Contractor Contractor Operator P Unregister Unregister	10.8.3.12 10.8.3.12 10.8.3.12 10.8.3.12 10.8.3.12	VOSS_5520-481 VOSS_5520-481 VOSS_5520-481 VOSS_5520-481 VOSS_5520-481	20.1.110.100 Extreme-Dyn action permi FA-VLAN-ISIC T 1/5 T 1/5	0 & actio namic-A it' D='0:280
Events	S Time Stamp 11/2/2021 11:08 11/2/2021 11:08 11/2/2021 11:08 11/2/2021 11:05 11/2/2021 11:05 11/2/2021 11:05	22 00:50:56:86:50 22 00:50:56:86:50 11 00:50:56:86:50 58 00:50:56:86:50 553 00:50:56:86:50 49 00:50:56:86:50	xF1 Windows xF1 Windows xF1 Windows xF1 Windows xF1 Windows xF1 Windows	Windows 8. Windows 8. Windows 8. Windows 8. Windows 8. Windows 8.	- 20.2.220.8: - 20.2.220.8: - 20.2.220.8: - 20.2.220.8:	WIN10-C WIN10-C 2 WIN10-C 2 WIN10-C 2 WIN10-C 2 WIN10-C WIN10-C WIN10-C WIN10-C WIN10-C	READIN READIN host/Wi	Sixont 802.1X (PEA) Gixont 802.1X (PEA) N10-C 802.1X (PEA) MAC (PAP) MAC (PAP) N10-C 802.1X (PEA)	P) Rule: "Cont P) Rule: "Cont P) Rule: "Dom Rule: "Unre Rule: "Unre P) Rule: "Dom	Contractor Contractor Operator P Unregister Unregister Operator P	10.8.3.12 10.8.3.12 10.8.3.12 10.8.3.12 10.8.3.12 10.8.3.12	VOSS_5520-481 VOSS_5520-481 VOSS_5520-481 VOSS_5520-481 VOSS_5520-481 VOSS_5520-481	20.1.110.100 Extreme-Dyn action permi FA-VLAN-ISIC T 1/5 T 1/5 T 1/5	0 & actio namic-Al it' D='0:280
Events	S Time Stamp 11/2/2021 11:08 11/2/2021 11:08 11/2/2021 11:06 11/2/2021 11:05 11/2/2021 11:05 11/2/2021 11:05 11/2/2021 11:05 11/2/2021 11:05	222 00:50:56:86:50 222 00:50:56:86:50 111 00:50:56:86:50 58 00:50:56:86:50 53 00:50:56:86:50 44 00:50:56:86:50 49 00:50:56:86:50	kF1 Windows	Windows B. Windows B. Windows 8. Windows 8. Windows 8. Windows 8.	- 20.2.220.8: - 20.2.220.8: - 20.2.220.8: - 20.2.220.8:	WIN10-C	READIN READIN host/Wi host/Wi host/Wi	Sicont 802.1X (PEA) Sicont 802.1X (PEA) MAC (PAP) MAC (PAP) MAC (PAP) MAC (PAP) N10-C 802.1X (PEA)	P) Rule: "Cont P) Rule: "Cont P) Rule: "Dom Rule: "Unre Rule: "Unre P) Rule: "Dom P) Rule: "Dom	Contractor Contractor Operator P Unregister Operator P Operator P	10.8.3.12 10.8.3.12 10.8.3.12 10.8.3.12 10.8.3.12 10.8.3.12 10.8.3.12	VOSS_5520-481 VOSS_5520-481 VOSS_5520-481 VOSS_5520-481 VOSS_5520-481 VOSS_5520-481 VOSS_5520-481 VOSS_5520-481	20.1.110.100 Extreme-Dyn action permi FA-VLAN-ISIC T 1/5 T 1/5 T 1/5 T 1/5 T 1/5	D & actic namic-A it D='0:280
Events	S Time Stamp 11/2/2021 11:08 11/2/2021 11:08 11/2/2021 11:06 11/2/2021 11:05 11/2/2021 11:05 11/2/2021 11:05 11/2/2021 11:05 11/2/2021 11:05 11/2/2021 11:05 11/2/2021 11:05 11/2/2021 11:05 11/2/2021 11:05 11/2/2021 11:05 11/2/2021 11:05 11/2/2021 11:05 11/2/2021 11:05	22 00:50:56:86:50 22 00:50:56:86:50 11 00:50:56:86:50 55 00:50:56:86:50 53 00:50:56:86:50 49 00:50:56:86:50 49 00:50:56:86:50 49 00:50:56:86:50	KF1 Windows	Windows B. Windows B. Windows 8. Windows 8. Windows 8. Windows 8. Windows 8. Windows 8.	20.2.220.8: 20.2.220.8: 20.2.220.8:	WIN10-C	READIN READIN host/WI host/WI host/WI	Sicont 802.1X (PEA) Sicont 802.1X (PEA) N10-C 802.1X (PEA) MAC (PAP) MAC (PAP) N10-C 802.1X (PEA) N10-C 802.1X (PEA) N10-C 802.1X (PEA)	P) Rule: "Cont P) Rule: "Cont P) Rule: "Dom Rule: "Unre Rule: "Unre Rule: "Dom Rule: "Dom P) Rule: "Dom	Contractor Contractor Operator P Unregister Unregister Operator P Operator P Operator P	10.8.3.12 10.8.3.12 10.8.3.12 10.8.3.12 10.8.3.12 10.8.3.12 10.8.3.12 10.8.3.12	VOSS_5520-481 VOSS_5520-481 VOSS_5520-481 VOSS_5520-481 VOSS_5520-481 VOSS_5520-481 VOSS_5520-481	20.1.110.100 Extreme-Dyn action permi FA-VLAN-ISID T 1/5 T 1/5 T 1/5 T 1/5 T 1/5 T 1/5 T 1/5	D & actio namic-Ai it D=10:280 F F F F
Events	S Time Stamp 11/2/2021 11:08 11/2/2021 11:08 11/2/2021 11:08 11/2/2021 11:05 11/2/2021 11:05 11/2/2021 11:05 11/2/2021 11:05 11/2/2021 11:05 11/2/2021 11:05 11/2/2021 11:05	222 00:50:56:86:50 222 00:50:56:86:50 111 00:50:56:86:50 53 00:50:56:86:50 49 00:50:56:86:50 49 00:50:56:86:50 49 00:50:56:86:50 49 00:50:56:86:50	KF1 Windows	Windows B. Windows 8. Windows 8. Windows 8. Windows 8. Windows 8. Windows 8. Windows 8. Windows 8.	- 20.2.220.8: 20.2.220.8: 20.2.220.8: 	WINTD-C WINTD-C 2 WINTD-C 2 WINTD-C 2 WINTD-C	READIN READIN host/Wi host/Wi host/Wi	Sicont 802.1X (PEA) Sicont 802.1X (PEA) N10-C 802.1X (PEA) MAC (PAP) MAC (PAP) N10-C 802.1X (PEA) N10-C 802.1X (PEA)	P) Rule: "Cont P) Rule: "Cont P) Rule: "Dom P) Rule: "Unre Rule: "Unre Rule: "Dom P) Rule: "Dom	Contractor Contractor Operator P Unregister Operator P Operator P Operator P Operator P Unregister	10.8.3.12 10.8.3.12 10.8.3.12 10.8.3.12 10.8.3.12 10.8.3.12 10.8.3.12 10.8.3.12	V055_5520-481 V055_5520-481 V055_5520-481 V055_5520-481 V055_5520-481 V055_5520-481 V055_5520-481 V055_5520-481 V055_5520-481	20.1.110.100 Extreme-Dyn action permi FA-VLAN-ISIC T 1/5 T 1/5 T 1/5 T 1/5 T 1/5 T 1/5 T 1/5 T 1/5 T 1/5	D & action namic-A it D=0:280
Events	S Time Stamp 11/2/2021 11:08 11/2/2021 11:08 11/2/2021 11:06 11/2/2021 11:05 11/2/2021 11:05 11/2/2021 11:05 11/2/2021 11:05 11/2/2021 11:05 11/2/2021 11:05 11/2/2021 11:05 11/2/2021 11:05 11/2/2021 11:05	222 00530548650 222 00530568650 111 00530568650 533 00530568650 634 00530568650 449 00530568650 449 00530568650 441 00530568850	KF1 Windows KF1 Windows	Windows 8. Windows 8.	- 20.2.220.8; - 20.2.220.8; - 20.2.220.8; - 20.2.220.8; 	WINTO-C WINTO-C 2 WINTO-C 2 WINTO-C 2 WINTO-C 2 WINTO-C WINTO-C WINTO-C WINTO-C WINTO-C WINTO-C WINTO-C WINTO-C WINTO-C WINTO-C WINTO-C WINTO-C WINTO-C	READIN READIN host/Wi host/Wi host/Wi	Glcont 802.1X (РЕА) Glcont 802.1X (РЕА) N10-С 802.1X (РЕА) MAC (РАР) MAC (РАР) N10-С 802.1X (РЕА) N10-С 802.1X (РЕА) MAC (РАР) MAC (РАР)	P) Rule: "Cont P) Rule: "Cont P) Rule: "Cont P) Rule: "Cont Rule: "Unre Rule: "Unre P) Rule: "Dom P) Rule: "Dom P) Rule: "Dom Rule: "Unre Rule: "Unre	Contractor Contractor Operator P Unregister Operator P Operator P Operator P Operator P Unregister	10.8.3.12 10.8.3.12 10.8.3.12 10.8.3.12 10.8.3.12 10.8.3.12 10.8.3.12 10.8.3.12 10.8.3.12 10.8.3.12	V055_5520-48 V055_5520-48 V055_5520-48 V055_5520-48 V055_5520-48 V055_5520-48 V055_5520-48 V055_5520-48 V055_5520-48 V055_5520-48	20.1.110.100 Extreme-Dyn action permit FA-VLAN-ISIC T 1/5 T 1/5 T 1/5 T 1/5 T 1/5 T 1/5 T 1/5 T 1/5 T 1/5 T 1/5	0 & actio namic-Al it D='0:280

Figure 45 – Verify Downloadable ACLs from the End-Systems table in Access Control

ExtremeCloud IQ - Site Engine and ExtremeControl - VOSS/Fabric Engine Downloadable ACL Guide

Appendix - Troubleshooting

ZTP+ Troubleshooting

When troubleshooting ZTP+ from a VOSS/Fabric Engine switch, the following CLI commands are useful for understanding the state of the cloud connector on the switch.

show application auto-provision

VOSS_5520-48	OSS_5520-48T:l#show application auto-provision											
******	Comma:	nd Execution	Time: Fri Nov 05 15:27:10 2021 GMT ************************************									
		Auto	-provision Info									
Operational	Status	: C	omplete									

show logging file

Downloadable ACL Troubleshooting

When troubleshooting a VOSS/Fabric Engine switch, several commands are useful for verifying specifics related to client sessions and Downloadable ACLs.

show eapol session-stats interface gigabitEthernet <interface>

70SS_5520-48T:1#show eapol session-stats interface gigabitEthernet 1/5												
	Command Execution Time: Fri Nov 05 15:06:34 2021 GMT											
	Eap	Authentica	tor Session Stat	istics								
PORT	MAC	SESSION ID	AUTHENTIC METHOD	SESSION TIME	TERMINATE CAUSE	USER NAME						
L/5	00:50:56:86:5d:fl	0000004c	remote-server	0 day(s), 06:43:35	not-terminated	READING\contractor1						

show eapol sessions eap

				Eap Op	er Status		
PORT	MAC	PAE STATUS	VLAN PRI ID	Flex-UNI Enable	I-SID SOURCE	VLAN:I-SID	
./5	00:50:56:86:5d:fl	authenticated	N/A 0	true	radius	0:2800210	
'otal	 Number of EAP ses: show eapo 	sions : 1	ap verb	ose			

					1	Eap Oper Sta	tus Verbose				
PORT NUM	MAC	PAE STATUS	VLAN F ID	PRI	Flex-UNI Enable	I-SID SOURCE	VLAN:I-SID		ACL	ACEs	RADIUS DYNAMIC SETTINGS
1/5	00:50:56:86:5d:fl	authenticated	N/A O)	true	radius	0:2800210	8	1	1,2,3,4, 5,6	

Total Number of EAP sessions : 1

• show filter acl

VOSS	_5520-48	T:l#show fil	ter acl								
****	******	Command	Execution T	ime: Fri Nov 0	5 15:22	:13 20	021 GMT	******	*****	**	
			Vlan	/VSN ACL Table							
Acl Id	Туре	AclName	Pk	tType State	Origin	‡ of ACEs	Default Action	CtrPkt Rule	Vlan/3 Id	(-sid	
			Vlan ACL	Global-Action	Table						
Acl Id	Туре	Ipfix	Monitor Dst-Mlt	Monitor Dst-Port							
			Po	rt ACL Table							
Acl Id	Type	AclName	Pk	tType State	Origin	‡ of ACEs	Default Action	CtrPkt Rule	Port		
1	Ingress	Contractor	no	nipv6 enabled	eap	6	permit	permit	1/5)	
			Port ACL	Global-Action	Table						
Acl Id	Туре	Ipfix	Monitor Dst-Mlt	Monitor Dst-Port							
1	Ingress	Disable	0								
Disp	layed 1	of 1 Entries									

• show eapol sessions eap <interface> verbose

VOSS_5520-48T:l‡show eapol sessions eap 1/5 verbose

						Eap Oper Sta	tus Verbose			
PORT NUM	MAC	PAE STATUS	VLAN ID	PRI	Flex-UNI Enable	I-SID SOURCE	VLAN:I-SID	ACL	ACEs	RADIUS DYNAMIC SETTINGS
1/5	00:50:56:86:5d:fl	authenticated	N/A	0	true	radius	0:2800210	1	1,2,3,4, 5,6	

Total Number of EAP sessions : 1

802.1X Supplicant Configuration for Windows Clients

Below are the Windows 10 802.1X supplicant settings for Protected EAP (EAP-PEAP) authentication by using the Windows logon name and password as credentials.



Figure 46 - Windows 10 802.1X supplicant settings for EAP-PEAP authentication

Terms and Conditions of Use

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

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

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