

How To: ExtremeControl for ExtremeCloud IQ – Site Engine and ExtremeCloud IQ APs

Abstract: This document covers implementation of ExtremeCloud IQ APs in ExtremeControl. This guide provides guidance on configuring wireless devices to integrate with ExtremeControl. However, it does not cover implementation of ExtremeControl functionalities.

Part Number: 9037364-01 Rev AA

Published: December 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

©2021 Extreme Networks, Inc. All rights reserved.

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 are the property of their respective owners. For additional information on Extreme Networks trademarks, see <u>www.extremenetworks.com/company/legal/trademarks</u>.

Contents

Prerequisites and Limitations	3
Overview	4
Part 1: Wireless Configuration of ExtremeCloud IQ	5
Step 1 – Configure SNMP	6
Step 2 – Enable SNMP on the Device Template.	8
Step 3 – Configure RADIUS	10
Step 4 – Configure User Profiles	11
Create an EnterpriseUser User Profile	13
Create a GuestAccess User Profile with Firewall	13
Create an Unregistered User Profile with Firewall and Captive Portal	16
Step 5 – Configuring SSIDs for ExtremeControl	17
Create a Secure 802.1X SSID	18
Create an Open / Guest SSID	22
Part 2: Configuring ExtremeControl	24
Step 1 – Create an SNMP Profile for Access Points	24
Step 2 – Add the Access Point to ExtremeControl	25
Step 3 – Configure Captive Portal Settings	28
Step 4 – Configure Rules, Roles, and Policy Mappings	30
Part 3: Validation	33
Secure SSID Validation	33
Guest SSID Validation	35
Appendix A: Creating RFC 3576 Configurations	42
Appendix B: Enable RFC 3576 Reauthentication on ExtremeCloud IQ	44
Appendix C: DHCP Fingerprint for ExtremeCloud IQ Access Points	46
Appendix D: RADIUS Reponse Formatting	47
Appendix E: ExtremeCloud IQ - Site Engine Licensing Note	50
Revision History	51

Prerequisites and Limitations

This document is intended for SEs and partners who are familiar with both ExtremeCloud IQ and ExtremeControl. Only the primary touchpoints between the two products are covered in this document; all other settings are considered out of scope.

This document was originally written using the following firmware and software versions.

- ExtremeCloud IQ Site Engine 21.4.10.99 and later
- ExtremeControl 21.4.10.99 and later
- ExtremeCloud IQ Build Version 19.11.1.7 with AP Firmware 10.0r7a

Due to the nature of adding access points as devices that can authenticate against ExtremeControl, a few design limitations and suggestions should be followed.

- It is highly recommended that DHCP Reservations are created for access points that connect to the network. If an access point changes its IP Address, it needs to be re-added to ExtremeCloud IQ Site Engine and ExtremeControl.
- While this guide shows how to add individual access points to ExtremeControl, when adding multiple access points, it is recommended to use one of the Device Discovery methods in ExtremeCloud IQ Site Engine.
- An ExtremeCloud IQ Site Engine workflow, available through GitHub, can assist with the discovery and addition of ExtremeCloud IQ APs to ExtremeCloud IQ Site Engine. The workflow called "Import APs from XIQ" can be found at this site:

https://github.com/extremenetworks/ExtremeScripting/blob/master/XMC_XIQ-SE/oneview_workflows/README.md

Overview

This document is broken up into three major sections. The first is configuring the Wireless Network to authenticate against ExtremeControl. The second handles configuration of ExtremeControl to recognize requests from the wireless network and respond in a format that can be properly interpreted by the access point. Lastly, the third section validates the configuration of the entire solution.

A brief summary of the interactions between the access point and ExtremeControl can be broken down into the following steps:

- 1. As the device connects to the wireless SSID, either MAC-based authentication or 802.1X authentication occurs.
- 2. The access point sends a RADIUS request destined to the Access Control Engine for authentication.
- 3. The Access Control Engine authenticates and authorizes the RADIUS request per its configuration. It passes back a RADIUS Accept message with attributes that the access point can interpret such as Filter-ID.
- 4. The access point matches the attributes to a User Profile.
- 5. If the User Profile is set to redirect the client's web traffic, the access point intercepts the web requests and redirects based on IP Filter rules.
- 6. Upon change of access, such as successful Web Registration, the Access Control Engine sends a Change of Authorization (CoA) message to the access point to change the User Profile assigned to the device.

Note

In addition to following the steps in this guide, it is also recommended that you have IP helper addresses pointed to the Access Control Engine and SNMP Read-Only credentials configured on the router. The Access Control Engine can query these to assist with IP resolution.

Part 1: Wireless Configuration of ExtremeCloud IQ

The following must be configured on ExtremeCloud IQ in order to integrate with ExtremeControl:

- SNMPv3 Polling
- RADIUS Authentication
- RADIUS Accounting
- RFC 3576/5176 Reauthentication
- External Captive Portal Redirection

The configuration of the access point is done through ExtremeCloud IQ. When the configuration is complete, all processing and authentication occur between the access point and ExtremeControl. The configuration consists of the following parts:

- 1. Configure an SNMP Server profile so that ExtremeCloud IQ Site Engine and the Access Control Engines can poll the AP.
- 2. Enable SNMP on the Device Templates for all APs.
- 3. Configure the RADIUS settings to authenticate against the Access Control Engines.
- 4. Configure the User Profiles that will be assigned from Access Control. This also includes the IP Filters that are used within the profiles.
- 5. Configure the SSID for authentication against ExtremeControl.

Step 1 - Configure SNMP

Configuration of the SNMP profile should contain ExtremeCloud IQ – Site Engine and all Access Control Engines. To configure the SNMP Profile, edit the **Network Policy** in the **Configure** menu. The settings are configured in the Additional Settings tab. In the **Management Server** section, the **SNMP Server** configuration is found.

Network Policies > XIQ-Ex	tr > SNMP Server					_					
POLICY DETAILS	WIRELESS NETWORKS		DEVICE TEM	MPLATES	ROUTER SE	TTINGS	ADDITIONAL S	ETTINGS	DEPLOY POL	ICY	
MANAGEMENT SERVER		SNM	Serve	r							
DNS Server		SNMP Se	erver		ON						
NTP Server											
SNMP Server		Re-use S (Pick exis	NMP Server sting setting	Settings s)	: <u>,</u> =						
Syslog Server		Name *									
POLICY SETTINGS					XIQ-SE+Coi	ntrol					
NETWORK SERVICES		Descripti	on			1					
QOS OPTIONS					5	6					
SECURITY		SNMP Co	ontact								
		Disa	ble to Send	Traps over CAP	WAP	aster					
		+ /									
		SN	MP SERVER	IP ADDRESS / HOST NAME	VERSION	OPERATION	COMMUNITY	ADMIN	AUTH	ENCRYPTION	ORDER
		XIC	Q-SE	10.120.85.80	V3	GET_TRAP		snmpuser	MD5	DES	↑ ↓
		Ex	tremeContr	(10.120.85.81	∨3	GET		snmpuser	MD5	DES	↑ ↓

When adding a new SNMP Server entry, if the IP of the server does not exist in ExtremeCloud IQ, a new IP Object needs to be created. Otherwise, an existing IP can be selected. Note that when configuring the SNMP Server for ExtremeCloud IQ - Site Engine, both the **Get and Trap** operations are configured.

Network Policies > XIQ-Ex	tr > SNMP Server							1		
POLICY DETAILS	WIRELESS NETWORKS	DEVICE TER	MPLATES	ROUTER SI	ETTINGS	ADDITIONAL S	ETTINGS	DEPLOY PC	DLICY	
MANAGEMENT SERVER		SNMP Serve	r							
DNS Server		SNMP Server		ON						
NTP Server										
SNMP Server		Re-use SNMP Server (Pick existing setting	Settings .s)							
Syslog Server		Name *		VIO SELCI						
POLICY SETTINGS				XIQ-SE+CO	ntrol					
NETWORK SERVICES		Description								
QOS OPTIONS					le					
SECURITY		SNMP Contact		Cloud IQ M	laster					
		Disable to Send	Traps over CAP	WAP						
		+ / 1								
		SNMP SERVER	IP ADDRESS / HOST NAME	VERSION	OPERATION	COMMUNITY	ADMIN	AUTH	ENCRYPTION	ORDER
		XIQ-SE	10.120.85.80	V3	GET_TRAP		snmpuser	MD5	DES	↑ ↓
		ExtremeContr	(10.120.85.81	V3	GET		snmpuser	MD5	DES	↑ ↓

Add SNMP Server

When configuring the SNMP Profile for the Access Control Engine, the same SNMP credentials that were used for ExtremeCloud IQ - Site Engine are used for the Access Control Engine. A new IP Object might need to be created for each Access Control Engine that will be used. In addition, the Operation should be set to **Get** because Access Control Engines do not process SNMP Traps from the APs.

SNMP Server *	ExtremeControl1 F 🕂 🗹
Version	V3 •
Operation	Get
Admin *	Snmpuser (HiveOS swithes: 1-32 characters, others: 1-20 characters)
*	Disable SNMP V1/V2 default community (hivecommunity
Auth	MD5 🔻
Password *	snmpauthcred Show Password
Encryption	DES -
Password *	snmpprivcred
	Show Password

Step 2 - Enable SNMP on the Device Template.

The default setting for access points is to not allow SNMP. To enable SNMP on the access points, SNMP needs to be enabled on the wired uplink port. Because default templates cannot be edited in ExtremeCloud IQ, a new template must be created. This process is most easily performed by cloning the existing object and then adjusting it as needed.

Navigate to the Device Templates by editing the **Network Policy** in the **Configure** menu. In the Device Templates, each AP Template needs to be added or modified if it already exists. Select the Template to edit:

OLICIES	POLICY DETAILS	WIRELESS NETWORKS	DEVICE TEMPLATES	ROUTER SE
IWORK PC	AP Templates	L		-
- NET	+ 🖅 🕯			
URE	DEVICE MODEL	TEMPLATE	CLASSIFICATIO	N RULES
IFIG!	AP150W	🔽 AP150 (Defaul	t)	
Ő	AP630	🗔 AP630 (Defau	lt)	

At the **Wired Interfaces** section, find the interface which will be used to communicate to the Access Control Engine. If the default port type of **Uplink Port** is in use, then the Port Type will need to be cloned. If a non-default port type is in use, skip the next steps with instructions on creating a custom Port Type.



To clone the default Port Type, navigate to **Common Objects** under the Configure tab. Select **Port Types** from the **Policy** section. Select the default port type that was previously configured and then clone.

≏	CONFIGURE	COMMON OBJECTS			
\$	Network Policies	V Policy Clone	Port Types		
* >	Applications	AP Template	i i		
.lu >	Common Objects	Auto Provisioning	PORT TYPE NAME	DEVICE SERIES	DEVICE FAMILY
			Uplink Port	AP_ROUTER	AP
	Users	Bonjour Gateway Settings	Access Port	SWITCH	Extreme IQ Engine
<mark>€</mark> >	Guest Essentials Users	Classification Rules	Trunk Port	SWITCH	Extreme IQ Engine
*>		Cloud Config Groups 💽	Phone Data Port	SWITCH	Extreme IQ Engine
0		10.000	Access Port	SWITCH	Dell Switch
V		Hives	Access Port	SWITCH	Extreme Switch
6		Port Types	Trunk Port	SWITCH	Dell Switch

Name the new Port Type and select **Clone**.

Clone			×
You are about t	o create a copy of the selected object. Uplink SNMP Port		
		Clone	Cancel

After cloning the port, navigate back to the **Device Templates** and **Wired Interfaces** section. From the drop-down list, select the newly created Port Type and then select **Edit**.

Wired Interfaces Control actions from the Access Point's Ethernet ports											
Interface State	Port Type			Native VLAN	Allowed VLANs	Transmissio	n Type	Speed		LLDP	CDP
	Uplink SN 🔺	+	۲,	1	all	Auto	-	Auto	-		<
	Uplink Port Access Port	+	ľ	1	all	Auto	•	Auto	•		
	Uplink SNMP Port										

Check the **Enable SNMP** option under **Traffic Filter Management**. Finish by selecting the **Save Port Type** box. Repeat the Port Type selection for any other Device Templates that are used.

Traffic Filter Management		
Control the following types of traffic to Extreme Networks devices		
Enable SSH		
Enable Teinet		
Enable Ping		
C Enable SNMP		
Enable Inter-station Traffic Caution: Uncheck this option will prevent inter-station traffic		
	CANCEL	SAVE PORT TYPE

Step 3 - Configure RADIUS

The RADIUS Server configuration can be performed in two unique ways. One method is to create it while creating the SSID. However, the method shown below is to create the Common Object before creating the SSID.

Note

The Access Control Engines are added to ExtremeCloud IQ as A3 servers rather than External RADIUS Servers. The reason they are added this way is that the RFC 3576 Change of Authorization settings are automatically configured using this method. If added as an External RADIUS Server, RFC 3576 needs to be manually configured as referenced in Appendix B.

Under the **Configure** menu, select **Common Objects**. On the left panel, expand **Authentication** and select **Extreme Networks A3 Servers**. With this section selected, select **Add** to create a new entry for the Access Control Engines.

≏	CONFIGURE	COMMON OBJECTS		
۵	Network Policies	> Policy	Extreme Networks A3 RADIUS Servers	;
*>	Applications	> Basic	+ / 5 1	
alı >	Common Objects	> Security	NAME ExtremeControl1	Access Control Engine #1
	Users	> QOS		Access control Englise in
e >	Guest Essentials Users	> Management		
*>		> Network		
•		V Authentication		
ଡ		AAA Server Settings		
•		AD Servers		
		Captive Web Portals		
		External Radius Servers		
		Extreme Networks A3 Servers		

In the new entry, select the **IP Object** that was previously created when enabling SNMP. Leave the default port settings. Specify a **Shared Secret** to be used with ExtremeControl. **ETS_TAG_SHARED_SECRET** is the default Shared Secret used by ExtremeControl and can be used for testing and proof of concepts. For a real deployment, it is expected that the Shared Secret will be changed from the defaults. Save the new server and repeat the process for all Access Control Engines.

Extreme Networks A3 Servers Create External RADIUS Server

External RADIUS Server

Name *	ExtremeControl1
Description	Access Control Engine #1
IP/Host Name *	ExtremeControl1 F
Server Type *	Port:* 1812 Select existing IP Object Authentication Port:* 1813
Shared Secret	ETS_TAG_SHARED_SECRET Image: Show Password
	CANCEL SAVE EXTREME NETWORKS A3

Step 4 - Configure User Profiles

User Profiles define the access that a user or device has when connected to the network via ExtremeCloud IQ. These profiles can be dynamically assigned and contain many definitions including Firewall Rules, VLAN assignment, and QoS settings. These profiles need to be defined

before the assignment and should represent the Accept Policies that are assigned from ExtremeControl via the rules engine.

The minimum recommended User Profiles to be created are:

- Unregistered This profile limits traffic and redirects web traffic to ExtremeControl
- GuestAccess This profile limits internal traffic but allows full access to the Internet.
- EnterpriseUser This profile allows full access to the network.

The User Profiles can be found under the **Common Objects** in the **Configure** menu. Select **User Profiles** in the **Policy** section.



Create an EnterpriseUser User Profile

To create a new User Profile, select **Add**. Define the **User Profile Name** and **VLAN** (or VLAN Group). When selecting a VLAN, a new VLAN Object needs to be created or selected. Additional settings can be configured if desired. However, this is an example of only a VLAN being assigned to a user or device.

	♪	OBJECTS	Auto Provisioning Bonjour Gateway Settings	User Profiles > EnterpriseUser Create User Profile
2	₩ -> .ll >	KE - COMMON	Classification Rules Cloud Config Groups 🔘	User Profile
4		FIGUR	Hives	User Profile Name * EnterpriseUser
	• >	CON	Port Types	Connect to ' 💿 VLAN 🌑 VLAN Group
	* >		Radio Profiles	Wireless50 诺 🕇 🖬
	Ð		SDR Profiles	
	(b)		Schedules	SECURITY TRAFFIC TUNNELING QoS AVAILABILITY SCHEDULE CLIENT SLA DATA/TIME LIMIT
	•		SSIDs	OFF Firewall Rules
			Switch Template	CANCEL SAVE USER PROFILE
			URL Filtering Detail	
			URL Filtering	
			User Profiles	
	?		> Basic	

Create a GuestAccess User Profile with Firewall

When adding a Firewall to a User Profile, it can be added in line with the profile, or a Common Object for IP Firewall can be created before the User Profile. For common configurations such as Guest Access firewalls or Redirection firewalls, it is often helpful to clone the default objects to save time and configuration.

To create or clone an IP Firewall Policy, choose IP Firewall Policies from the Security section of the Common Objects.

۵	ST	COMMON OBJECTS		
\$	OBJEC	> Policy	IP Firewall Policies	
	NOM	> Basic	+ / 1	
.l i >	- COM	Security	NAME	Description
	GURE	AirDefense Policies	Redirect-Only	Default IP policy that al
a >	CONFI	IP Firewall Policies		
×>		MAC Firewall Policies	_	

Name the new policy and select **Edit**. In the new policy, some rules need to be adjusted or added. In particular, for the GuestAccess policy, ensure that web traffic can reach

ExtremeControl so that the registration success page can be displayed. To add a new rule, select Add.

8	Guest-Internet-O	only-Control				
EWALL	Name * Guest-Int	ernet-Only-Control				
P FIRE	Description Allows Int	ternet access and Captive Portal				
	+ / =					
	SOURCE IP	DESTINATION IP	SERVICE	ACTION	LOGGING	ORDER
	Any Any	Any	DHCP-Server	PERMIT	BOTH	↑ ↓
	Any Any	Any	DNS	PERMIT	вотн	↑ Ψ
	Any	ExtremeControl1	Any	PERMIT	BOTH	↑ ↓
	Any Any	10.0.0/255.0.0.0	Any	DENY	DROPPED_PACKETS	↑ Ψ
	Any	172.16.0.0/255.240.0.0	Any	DENY	DROPPED_PACKETS	↑ ↓
	Any Any	192.168.0.0/255.255.0.0	Any	DENY	DROPPED_PACKETS	↑ Ψ
	- Anv	Anv	Anv	DEDMIT	BOTH	↑ ↓

While creating a new rule to allow traffic to the Access Control Engine, set the Destination IP to the IP Object previously created for the Access Control Engines. Repeat this process for each engine that will be used.

IP Firewall Policies	Guest-Internet-Only-Control New IP Firewall Rule	
New IP Firew	wall Rule Select services such as	
Service	HTTP or HTTPS if desired	
Source IP *	Any 🌾 🕂 🗹	
Destination IP *	ExtremeControl1 😴 + 🗹	
Action	Permit Select IP Object	
Logging	Off	
		CANCEL

When the rule is saved, ensure it is placed correctly in the Firewall Policy. Because the list is ordered, you can use the up and down arrows to position the rule appropriately.

IP Firewall Policies > Guest-Internet-Only-Control

Gue	st-Internet-Only-Control				
Allo	ws Internet access and Captive	e Portal			
ADD 📝 🛅 Source IP	Destination IP	Service	Action	Logging	Order
Any	Any	DHCP-Server	PERMIT	BOTH	Υ
Any	Any	DNS	PERMIT	BOTH	↑ ↓
Any	ExtremeControl1	Any	PERMIT	вотн	小 ↓
Any	10.0.0/255.0.0.0	Any	DENY	DROPPED_PACKETS	↑ ↓
Any	172.16.0.0/255.240.0.0	Any	DENY	DROPPED_PACKETS	Λ Ψ
	192.168.0.0/255.255.0.0	Any	DENY	DROPPED_PACKETS	^ ↓
Any					

In the User Profiles, create a profile with the name GuestAccess. In addition to setting the VLAN, select the IP Firewall Name defined in the previous step.

MMON OBJECTS	Auto Provisioning Bonjour Gateway Settings Classification Rules	User Profile GuestAccess Create User Profile
-li> 0 -	Cloud Config Groups 🖸	User Profile
FIGUR	Hives	User Profile Name ' GuestAccess
CON <	Port Types	Connect to * VLAN VLAN Group
* >	Radio Profiles	Wireless50 😽 🕇 🖬
•	SDR Profiles	
Q	Schedules	SECURITY TRAFFIC TUNNELING QoS AVAILABILITY SCHEDULE CLIENT SLA DATA/TIME LIMIT
•	SSIDs	
	Switch Template	
	URL Filtering Detail	IP Firewall MAC Firewall
	URL Filtering	IP Firewall Name 1 Guest-Internet-Only-Control
	User Profiles	+ 1 5 Permit
0	> Basic	SOURCE IP DESTINATION IP SERVICE ACTION LOGGING ORDER

Create an Unregistered User Profile with Firewall and Captive Portal

Similar to a GuestAccess User Profile, the Unregistered User Profile needs to have an IP Firewall added to limit access as well as redirect web traffic to ExtremeControl.

In the **Security** menu, choose **IP Firewall Policies** and create an IP Firewall Policy or clone the default Redirect-Only policy. Set the name and add rules by selecting **Add**.

	CTS	> Basic			
\$ >	OBJE	Security	IP Firewall Policies		
*>	NOMM	AirDefense Policies	NAME	DESCRIPTION	
ult >	Со - Со	IP Firewall Policies	Guest-Internet-Access-Only	Default IP policy that allows Internet access only	+
	IGUR	MAC Firewall Policies	Redirect-Only	Default IP policy that allows redirect only	+

For the captive portal to work, the following rules need to be configured. This example shows one Access Control Engine. However, all Access Control Engines that provide a captive portal should be configured.

Order	Source IP	Destination IP	Service	Action
1	ANY	ANY	DHCP-Server	PERMIT
2	ANY	ANY	DHCP-Client	PERMIT
3	ANY	ANY	DNS	PERMIT
4	ANY	ExtremeControl1	HTTP	PERMIT
5	ANY	ANY	HTTP	REDIRECT
6	ANY	ExtremeControl1	HTTPS	PERMIT
7	ANY	ANY	HTTPS	REDIRECT

IP Firewall Policies Redirect-2-Control

Redirect-2-Control

Name *	Redirect-2-Control				
Description	Policy that redirects web traffic to Extra	emeControl			
ADD 📝					
Source IP	Destination IP	Service	Action	Logging	Order
Any	Any	DHCP-Server	PERMIT	OFF	↑ ↓
Any	Any	DHCP-Client	PERMIT	OFF	↑ ↓
Any	Any	DNS	PERMIT	OFF	↑ ↓
Any	ExtremeControl1	HTTP	PERMIT	OFF	↑ ↓
Any	Any	HTTP	REDIRECT	OFF	↑ ↓
Any	ExtremeControl1	HTTPS	PERMIT	OFF	↑ ↓
Any	Any	HTTPS	REDIRECT	OFF	↑ ↓

CANCEL SA

Note

The REDIRECT Action is visible only when the HTTP or HTTPS Services are configured.

In the User Profiles, create a new profile with the name Unregistered, set the VLAN, and select the IP Firewall Name defined in the previous step. The Redirection URL should contain the FQDN of the Access Control Engine.

••	Extre	emeClo	oud IQ Pilot					(۹ 🖬	¢	● Ke	enn Jones 1E Lab	E	=
	10N OBJECTS	SER PROFILES	User Profiles >Unregis	stered rofile										
**>	- COMP	S	User Profile											
:::> €>	CONFIGURI		User Profile Name * Connect to *	Unregistered VLAN VLAN Gro Wireless50										
			SECURITY	TRAFFIC TUNNELING C	Dos AVAILAB	ILITY SCHEDULE C	LIENT SLA DATA/TIME LIM	IIT						•
			ON Firewal	ll Rules										
			IP Firewall	MAC Firewall										
			IP Firewall Name *	ect-2-Control										
			Redirecting http://	//eac1.extremetme.com	Prevent App	ole CNA (Captive Network A	ssistant) application from requestin	g cred	entials					
			+ 🖉 🧊				Outbound Traffic	•	Permit		•			
8			SOURCE IP	DESTINATION IP	SERVICE	ACTION	LOGGING	OF	RDER					

Step 5 - Configuring SSIDs for ExtremeControl

The creation of the SSID is configured as part of the Network Policy under Wireless Networks. To create a new Wireless Network, it's recommended to select **All other Networks (standard)** from the drop-down options.

Network Policies > XIQ-Ex	tr > All SSIDs				
POLICY DETAILS	WIRELESS NETWORKS	DEVICE TEMPLATES	ROUTER SETTINGS	ADDITIONAL SETTINGS	DEPLOY POLICY
Wireless Networks					
+ 📁 🖌 Assign St	SIDs using Classification Rules				
Guest Access Network	GUEST	ACCESS		ACCESS SECURITY	VLAN
All Other Networks (stand	lard)		No records found.		

Create a Secure 802.1X SSID

To create a secure SSID that uses 802.1X authentication, set the name of the wireless network and select **Enterprise WPA / WPA2 / WPA3** under SSID Authentication. The default settings for Key Management, Encryption Method, and Captive Web Portal can be left unchanged.

€	ß	Network Policies > XIQ-Ex	tr > All SSIDs > XIQ-Contro	I-Secure				
۵	POLICI	POLICY DETAILS	WIRELESS NETWORKS	DEVICE TEMPLATES	ROUTER SETTINGS	ADDITIONAL SETTIN	IGS DEPLOY POL	ICY
*>	TWORK	CONFIGURATION GUIDE	Wireless Netw	ork				
•lt >	- NEI	Policy Name						
	URE	XIQ-ExtremeControl	Name (SSID) *	XIQ-Control-Secure		roadcast SSID Using		
€ >	NFIG	RADIUS Server Group	Broadcast Name *	XIQ-Control-Secure	•	WIFIO Radio (2.4 GHz o	v)	
~	8	ExtremeControl						
		User Profile	SSID Usage					
Q		EnterpriseOser						
()			SSID AUTHENTICATI	ON MAC AUTHENTI	CATION			
•			ooo Enterprise ∭ wpa / wpa2 / wi	O Personal → WPA / WPA2	e / wpa3 Private	Pre-Shared	WEP	Open Unsecured
			Key Management	WPA2-802.1>	X -			
			Encryption Method	CCMP (AES)	Ŧ			
0			Enable Captive Web Pe	ortal OFF				

When the Enterprise SSID Authentication method is selected, you are given the option (further down the screen) to configure Authentication Settings. If a RADIUS Server Group has not yet been created, select **Add** to create a new one.

Authentication Settings							
Authentication with ExtremeCloud IQ Authentication Service OFF							
Default RADIUS Server Group							
Name	Туре	IP/Host Name	Order				
	No i	records found.					
Apply RADIUS server groups to devices via classification							

In the **Configure RADIUS Servers** window, set a name for the RADIUS Server Group and select the previously configured Access Control Engine from the Extreme Networks A3 tab.

Configure RADIUS Servers	S			×
ADIUS Server Group Name * ExtremeControl	RADIUS Server Group Descriptio	on 🍂		
EXTERNAL RADIUS SERVER (0)	EXTREME NETWORKS A3 (1)	EXTREME NETWORKS RADIUS SERVER (0)	EXTREME NETWORKS RADIUS PROXY (0)	
7 + 🗇				
Name		IP/Host Name		
ExtremeControl1		10.120.85.81		
			CANCEL	RADIU

With the RADIUS Servers configured, the **User Access Settings** section needs to be configured to assign the correct User Profiles based on the authorization results from ExtremeControl. First, select the **Default User Profile** to be used if no other profiles match. Next, select the two check boxes shown below to apply different user profiles based on a Filter-ID. With the check boxes enabled, the User Profiles that were previously created need to be selected so they can be utilized.

Authentication Settings						
Authentication with ExtremeCloud IQ A	uthentication Service OFF					
Authenticate via RADIUS S	erver					
Default RADIUS Server ExtremeControl Group	+ =					
Name	Туре	IP/Host Name	Order			
ExtremeControl1	Extreme Networks A3	10.120.85.81	↑ ↓			
User Access Settings Configure your QoS, VLAN, Firewall policies, an Default User Profile EnterpriseUser	nd Traffic Tunneling					
VLAN : Wireless5	o T ->-					
Apply a different user profile to various cli	ents and user groups.	ree tunnel DADUIS attributes				
Allow user profile assignment using RADIUS attributes in addition to the three tunnel RADIUS attributes.						
Standard RADIUS Attribute	11_Filter-Id 👻					
Vendor specific RADIUS Attribute						
+ 📻 🔋 The IQ Engine with version pri	or to 8.1r1 only support 16 user profile	policy rules.				
USER PROFILE NAME VLAN/VLAN GRO	OUP ASSIGNMENT RUL	.ES ASSIGNMENT DESCRIPTION	ORDER			

In the User Profiles window, enable the desired User Profiles and then click Select.

User I	Profiles	×
Ē		
	User Profile	VLAN
	default-guest-profile	1
	default-profile	1
	EnterpriseUser	Wireless50
	GuestAccess	Wireless50
	Unregistered	Wireless50
10	20 50 500	14 4 1 🕨 H 🔽 Go
		CANCEL SELECT COPY

With the User Profiles added, select the + option to create a new User Profile Assignment Rule for each User Profile. If an assignment rule was previously created, use the arrow icon next to the plus icon to re-use the assignment rules.

Use	er Access Setting igure your QoS, VLAN,	S Firewall policies, and Traffic Tunneli	ng		
Defa	ult User Profile	EnterpriseUser VLAN : Wireless50			
	Apply a different user p	rofile to various clients and user gro	oups.		
	Allow user profile a	ssignment using RADIUS attributes i	in addition to the three tu	nnel RADIUS attributes.	
	Standard RADII	JS Attribute 11_Filter-Id	•		
	Vendor specific	RADIUS Attribute			
+	📻 🔋 The IQ Engi	ne with version prior to 8.1r1 only su	pport 16 user profile polic	:y rules.	
	USER PROFILE NAME	VLAN/VLAN GROUP	ASSIGNMENT RULES	ASSIGNMENT DESCRIPTION	ORDER
	EnterpriseUser	Wireless50	IF R		↑ ↓
	GuestAccess	Wireless50	G R		* Ψ
	Unregistered	Wireless50	GF CR		↑ Ψ

Name the User Profile Assignment, select the + button, and then select RADIUS Attribute.

User Profile Assignment	
Name EnterpriseUser	
Assign user profiles to clients or users connect	ing to an SSID according to authentication and other client classification. All conditions must match for th
Advanced Guest Policy	VALUE
Client OS Type	No rules found
Client MAC Address Client Location	

Enter the Filter-ID that will be returned from ExtremeControl as part of the Authorization rules.

RADIUS Attribute	×
RADIUS Attribute	
Assign user profile based on RADIUS attribute value pairs returned in Access-Accept response message	
Three standard RADIUS Attribute Value Pairs	
IETF 64 (Tunnel-Type) = GRE(10)	
IETF 65 (Tunnel-Medium-Type) = IP(1)	
IETF 81 (Tunnel-Private-Group-ID) = admin-defined-attribute-value	
Attribute Values ⑦ (1-4095)	
A single standard RADIUS Attribute Value Pair	
RADIUS Attribute 11_Filter-Id	
Attribute Values EnterpriseUser	
	CANCEL

Note

Do not use spaces in the Filter-ID name. They will not be matched correctly during authentication.

Repeat the process of creating assignment rules for each User Profile. To easily see all rule assignments, the arrow in each rule can be selected to expand the rule. The rules are ordered for assignment as well. If the order needs to be changed, select the up or down arrows to the right of the rule.

User Access Settings Configure your QoS, VLAN, Firewall policies, and Traffic Tunneling							
Default User Profile EnterpriseUser VLAN : Wireless50 + :==							
Apply a different user pro	file to various clients and user grou	ips.					
Allow user profile ass	ignment using RADIUS attributes ir	addition to the three tunr	el RADIUS attribute	S.			
Standard RADIUS	Attribute 11_Filter-Id	•					
Vendor specific R	ADIUS Attribute						
🕂 🎏 🔋 The IQ Engine	e with version prior to 8.1r1 only sup	port 16 user profile policy	rules.				
USER PROFILE NAME	VLAN/VLAN GROUP	ASSIGNMENT RULES	ASSIGNMENT DESCR	IPTION	ORDER		
		∓ 🖬 EnterpriseUser	V				
EnterpriseUser	Wireless50		Туре	Value	↑ ↓		
			RADIUS Attribute	EnterpriseUser			
			v				
			Туре	Value	↑ ↓		
GuestAccess	Wireless50	L+ LK GuestAccess	RADIUS Attribute	GuestAccess			
			_				
			•				
Unregistered	Wireless50	🕂 🖪 Unregistered	Type	Value	↑ ↓		
		LT LK Offregistered	RADIUS Attribute	Unregistered			

Create an Open / Guest SSID

Creating an open SSID is very similar to configuring a secure SSID. The primary difference is in the **SSID Usage** section. In this section, select either **Personal** or **Open** for the SSID Authentication type. Ensure that **Enable Captive Web Portal** is disabled.

Network Policies > XIQ-E>	xtr > All SSIDs > XIQ-Cont	rol-Open					
POLICY DETAILS	WIRELESS NETWORKS	DEVICE TEMPLATES	ROUTER SETTINGS	ADDITIONAL SETTINGS	DEPLOY POLICY		
CONFIGURATION GUIDE	Wireless Net	work					
Policy Name XIQ-ExtremeControl	Name (SSID) *	XIQ-Control-Open	В	roadcast SSID Using			
User Profile Unregistered	Broadcast Name *	XIQ-Control-Open		 WiFil Radio (2.4 GHz or 5 GHz) WiFil Radio (5 GHz only) 			
	SSID Usage						
	SSID AUTHENTICA	TION MAC AUTHENTIC	CATION				
	⁰ / ₂ Enterprise ⁰ / ₁	VPA3 Personal WPA / WPA2	/ WPA3 Private	Pre-Shared 💮 WEP	P Open Unsecured		
	Enable Captive Web	Portal OFF					

/22

Select the MAC Authentication tab to the right of the SSID Authentication tab, and enable MAC Authentication. Select MS CHAPV2 as the Authentication protocol and select the RADIUS Server Group (e.g. ExtremeControl) previously created for the Secure SSID.

SSID Usage			
SSID AUTHENTICATION	MAC AUTHENTICATION		
ON MAC AUTHEN Enable MAC au password to au clients. Authentication Protocol	TICATION thentication that uses the MAC address as the thenticate clients. This is typically used to su MS CHAP V2 ADIUS Server	e username and pport legacy	
Default RADIUS Server Extre Group	emeControl + ;		
Name	Туре	IP/Host Name	Orc
ExtremeControl1	Extreme Networks A3	10.120.85.81	个

Adjust the User Access Settings so the authorization rules match the Filter-ID that is returned from ExtremeControl. The Assignment Rules can be reused by selecting the arrow icon next in the Assignment Rule as shown below.

User Access Settings Configure your QoS, VLAN, Firewall policies, and Traffic Tunneling							
Default User Profile Unregistered VLAN : Wireless50 +							
Apply a different user p	rofile to various clients and user gro	oups.					
Allow user profile as	ssignment using RADIUS attributes	in addition to the three tunr	el RADIUS attributes	5.			
Standard RADIU	In S Attribute 11_Filter-Id	•					
Vendor specific	RADIUS Attribute						
+ 🥽 🕯 The IQ Engir	ne with version prior to 8.1r1 only su	pport 16 user profile policy	rules.				
USER PROFILE NAME	VLAN/VLAN GROUP	ASSIGNMENT RULES	ASSIGNMENT DESCR	IPTION	ORDER		
			•				
EnterpriseUser	Wireless50	EnterpriseUser	Туре	Value	↑ ↓		
			RADIUS Attribute	EnterpriseUser			
			▼				
GuestAccess	Wireless50		Туре	Value	↑ ↓		
			RADIUS Attribute	GuestAccess			
			•				
			Туре	Value	A 14		
Unregistered	Wireless50	L+ LK Unregistered	RADIUS Attribute	Unregistered	-1. W.		

Part 2: Configuring ExtremeControl

In this section, the access point will be added to ExtremeControl as a switch so that clients can be authenticated and controlled.

Note

This section assumes that the Access Control Engine is already configured and added to ExtremeControl and that Guest Registration is already enabled.

Step 1 - Create an SNMP Profile for Access Points

In ExtremeCloud IQ - Site Engine, select the Profiles tab under Administration and select Add for SNMP Credentials. Create new SNMP credentials that correlate with the credentials configured in ExtremeCloud IQ. The default SNMP credentials can be used if desired.

C ExtremeClo	oud IQ Site Engi	ne								
A Network	Profiles Users	Server In	formation	Certifica	tes	Options	Device Types	Back	up/Restore	Dia
🜲 Alarms & Events	🔘 Add 📝 Ed	lit 🤤	Delete	Default P	rofile:	public_v1_	Profile 💌	Defau	lt Access Co	ontrol I
Gentrol	Name		SNMP Ver	sion f	Read C	redential	Write Cred	lential	Max Acc	ess Cre
Analytics	public_v1_Profile		SNMPv1	F	oublic_v	v1	public_v1		public_v	1
	EXTR_v1_Profile		SNMPv1	Ŗ	oublic_v	v1	private_v1		private_\	r1
🗹 Compliance	public_v2_Profile		SNMPv2	F	oublic_v	v2	public_v2		public_v2	2
lill Reports	EXTR_v2_Profile		SNMPv2	F	public_v	v2	private_v2		private_\	/2
📑 Tasks	snmp_v3_profile		SNMPv3	c	lefault <u></u>	_snmp_v3	default_sn	mp_v3	default_s	nmp_
Administration	« < Page 1 of 1 > » 2 🗟 Reset									
⇄ Connect	SNMP Credentials	CLI Cred	entials D)evice Map	ping					
	🕥 Add 📝 Ed	it 🤤	Delete							
	Name	Edit S	NMP Crea	dential: d	lefaul	t_snmp_v	3		×	ation
	public_v1									
	default_snmp_v3	Credent	ial Name:	defa	default_snmp_v3					
	private_v1	SNMP V	ersion:	SNM	Pv3				~	
	public_v2	User Na	me:	snm	puser					
	private_v2	Authent	ication Type	: MD5					*	
	default_snmp_v3s	Authent	ication	snm	pauthc	red			۲	
	CheckPoint	Password:		DES						
	VMware	Privacy	Password:	snm	opriver	ed			۲	
				24111	ppriver				-	
							S	ave	Cancel	

With the SNMP Credentials configured, create a **Profile** to assign to the access points. Ensure that the SNMP settings are configured for **AuthPriv** for the SNMP Read.

C ExtremeClo	ud IQ Site Engine			
A Network	Profiles Users Serv	ver Information C	Certificates Options	Device Types
🔔 Alarms & Events	💿 Add 🔯 Edit	😑 Delete 🛛 De	efault Profile: public_v1	I_Profile 🔻
Control	Name	SNMP Version	n Read Credential	Write Crede
Analytics	public_v1_Profile	SNMPv1	public_v1	public_v1
🛜 Wireless	EXTR_v1_Profile	SNMPv1	public_v1	private_v1
Compliance	public_v2_Profile	SNMPv2	public_v2	public_v2
lil Reports	≪ < Page 1	of1 > >>	🔿 🛛 🔁 🛛 📠 Reset	
Tasks	SNMP Credentials CLI	Credentials Devi	ice Mapping	
Administration	🗿 Add 🔯 Edit	🖨 Delete		
Edit Profile: S	NMPv3_IQ			×
Profile Name:	SNMPv3_IQ			
SNMP Version:	SNMPv3			-
Read:	default_snmp_v3 🔹	Read Security:	AuthPriv	~
Write:	default_snmp_v3 🔹	Write Security:	AuthPriv	-
Max Access:	default_snmp_v3 🔹	Max Security:	AuthPriv	-
CLI Credential:	XIO APs			-

Step 2 – Add the Access Point to ExtremeControl

In **Control**, select the Access Control tab, followed by the **Default** Access Control Engine Group. In the group configuration, select the Switches tab and then select **Add...**.

C ExtremeClo	ExtremeCloud IQ Site Engine								
A Network	Dashboard Policy	Access Control En	nd-Systems Reports						
🔔 Alarms & Events	Configuration	+	Engine Group - [Default					
🔓 Control	0								
Analytics	Group Editor	+	Details Switches	End-Systems					
奈 Wireless	Engines	0-	🕒 Add 🔯 Ed	dit 🤤 Delete					
Compliance	 Engine Groups 		IP Address 🕇	Nickname					
Lill Reports	Default								

Cancel

In the Add Switches dialog, if the access point has not been added to ExtremeCloud IQ - Site Engine, select Add Device to add the IP address of the access point and the SNMP Profile to use for communication.

Add Switch	es to Access Cor	ntrol Engine	Group: De	fault
Add Devic	e		c	2
Add Device	e		? X	•
IP Address:	192.168.3.168			L
Profile:	SNMPv3_IQ		*	
Nickname:				
Poll Status	Only			1
	ОК	Apply	Close	

After the access point is added to ExtremeCloud IQ - Site Engine, select the access point from the device list and select the Access Control Engine from the **Primary Engine** drop-down list. If there is more than one Access Control Engine, do the same for the **Secondary Engine**. Set the **RADIUS Attributes to Send** field to a value of **Filter-ID** and enable **RADIUS Accounting**.

Add Switches to Access Control Engine Group	: Defai	ult		×
Add Device	Q	Switch Type:	Layer 2 Out-Of-Band	~
 All Devices (61 devices) 	-	Primary Engine:	ControlEngine/ 10.120.85.81	-
□ ▼ 192-168-101-52-DPortGroup-V5	- 1	Secondary Engine:	None	-
□ ▼ 192-168-130-50-DPortGroup-VS	- 1			
□ ▼ 192.168.130.147	- 1	Auth. Access Type:	Manual RADIUS Configuration	~
C V ACE	- 1	Virtual Router Name:		
✓ ● AP-99		RADIUS Attributes to Send:	Filter-Id	-
☐ ▼ AH-150W	- 1			
AH-245X		RADIUS Accounting:	Enabled	~

Before saving the configuration, select Advanced Settings and set the Reauthentication Type to RFC 3576 - Generic CoA Hyphen Delimited as shown below. (This step is not necessary in ExtremeCloud IQ - Site Engine 21.11 and later.) If the RADIUS Shared Secret was set to a value other than the default ETS_TAG_SHARED_SECRET, set the value to match what was configured in ExtremeCloud IQ.

vice	Q	Switch Type:		Layer 2 Out
' All Devices (61 devices)	^	Primary Engine:		ControlEng
ed Switch Settings				None
t for IP Resolution: N	one		~	Manual RAD
ide RADIUS Security				
d is blank, the default RADIUS	shared secret from Eng	ine Settings will be used	d instead.	Filter-Id
ecret:			Ð	Enabled
ide Reauthentication Bel	havior			None
field set to <i>None</i> to determine	e the reauthentication i	type automatically.		None
tication Type:	C 3576 - Generic CoA F	lyphen Delimited	~	None
ort Link Control:				None
		ОК	Cancel	None
▼ CHKP-mgmt		Policy Domain:		Do Not Se
▼ D2				
CHKP-mgmt	_	Policy Domain:		

Note

In ExtremeCloud IQ – Site Engine version 21.4 the reauthentication method needs to be set manually on a per-device basis, or a mapping to the SysObject ID can be created. See Appendix A for reference.

The final settings should look similar to the following image. When complete, select Save.

Configure Device:		×
Switch Type:	Layer 2 Out-Of-Band	
Primary Engine:	ControlEngine/10.120.85.81	
Secondary Engine:	None 💌	
Auth. Access Type:	Manual RADIUS Configuration	
Virtual Router Name:		
RADIUS Attributes to Send:	Filter-Id 💌	
RADIUS Accounting:	Enabled 💌	
Management RADIUS Server 1:	None 💌	
Management RADIUS Server 2:	None 💌	
Network RADIUS Server:	None	
Policy Domain:	Do Not Set 👻	
Advanced Settings		
	Save	Close

Step 3 - Configure Captive Portal Settings

Assuming that Guest Registration is already configured, the Network Settings for the Captive Portal need to be verified. Under the **Configuration** section, expand the captive portal that is in use. Typically, this is the **Default** captive portal. Select **Network Settings** and verify that **Use Fully Qualified Domain Name** is selected as well as **Redirect User Immediately**.

C ExtremeClo	ud IQ Site Engine		
A Network	Dashboard Policy Access Control En	d-Systems Reports	
Alarms & Events	Configuration –	Network Settings	
Control	 Configurations 	Allowed Web Sites:	Open Editor
Analytics	► AAA	Use Fully Qualified Domain	
🛜 Wireless	Profiles	Name:	
Compliance	 Captive Portals 	Use Mobile Captive Portal:	ſ €
Lill Reports	Customized	Display Welcome Page:	
Tasks	▼ Default	Portal HTTP Port:	80 2
administration	Network Settings		
	Administration	Portal HTTPS Port:	443
	 Website Configuration 	Force Captive Portal HTTPS:	
	 Randomized MAC Portal 	Redirection	
	 Notifications 	Redirect User Immediately	*: 🔽
	Vendor RADIUS Attributes		
	 Global & Engine Settings 	Test Image URL:	https://www.google.com/favicon.ico
		Redirection:	To URL 👻
		Destination:	http://www.extremenetworks.com
		* When used as the portal in an	Advanced Location configuration, all fields except Redirect User Immediately are inherited from the Access Cont

Verify that Guest Registration is also enabled by selecting Website Configuration.

ExtremeClo	ud IQ Site Engine	
🚠 Network	Dashboard Policy Access Control En	d-Systems Reports
Alarms & Events	Configuration –	Website Configuration
Control	 Configurations 	✓ Guest Settings
Analytics	▶ AAA	O Guest Web Access:
🛜 Wireless	Profiles	Allows presentation of an Acceptable Use Policy to the guest user and allows guest access to the network for the duration
Compliance	 Captive Portals 	Guest Web Access login page.
III Reports	 Customized 	O Guest Registration:
Tasks	▼ Default	Allows unauthenticated access to the network for the length of the registration. Registration also has provisions for captur
Administration	Network Settings	O Secure Guest Access:
	Administration	Allows a guest to gain secure wireless access to your network via 802.1x (PEAP) authentication using credentials that are co
	 Website Configuration 	desired to anow only temporary access to your network.
	Look & Feel	Authentication Settings
	Guest Registration	Survivable Registration
	 Randomized MAC Portal 	This option will allow for a temporary Registration when communication to NAC Manager fails. During this time, any regist
	 Notifications 	communication is restored, the user will be put through the normal Registration process.
	 Vendor RADIUS Attributes 	Assessment/Remediation
	 Global & Engine Settings 	

Step 4 - Configure Rules, Roles, and Policy Mappings

With the captive portal settings verified, the authorization rules need to be adjusted to match the Filter-ID settings that the access points are expecting. Following the examples that were used in this guide, Enterprise User, Guest Access, and Unregistered should be verified.

Select the **Rules** section under **Configurations**. Enabling Guest Registration auto-generates multiple rules in the rules engine. Additional rules can be added to match the authorization criteria desired. In the example below, a rule matching **802.1X** authentication is added and the **Default NAC Profile** assigned, which applies the **Enterprise User** Accept Policy. To verify which Filter-ID is being passed back to the access point, select the Accept Policy name to show the **Policy Mapping** window.

ExtremeClo	ud IQ Site Engine		
A Network	Dashboard Policy Access Control E	d-Systems Reports	
Alarms & Events	Configuration –	Rules	
Control	 Configurations 	😮 Add 🔯 Edit 🔃 Copy 👄 Delete 📔 🛊 Up	Down View
Analytics	▼ Default	Enabled Rule Name	Description
🛜 Wireless	Rules	System Rules (2 rules)	
Compliance	AAA: Default	Device Rules (4 rules)	
Reports	Portal: Default	User Rules (2 rules)	
Tasks	 X-config 	Device Rules (1 rules)	
😤 Administration	► AAA	 Uncategorized (1 rules) 	
	Profiles	■ ✓ 802.1X	
	Captive Portals	Conditions A	ctions
	 Notifications 	Authentication is 802.1X P	rofile: Default NAC Profile
	 Vendor RADIUS Attributes 		Accept Policy: Enterprise User

In the **Edit Policy Mapping** window, the **Filter** should be adjusted to match the Filter-ID that was configured in the Assignment Rules in ExtremeCloud IQ.

Edit Policy Mappi	ng	×
Name:	Enterprise User	
Map to Location:	Any	
Policy Role:	Enterprise User 💌	
VLAN [ID] Name:	None	
VLAN Egress:	Untagged 💌 U	- 1
Filter:	EnterpriseUser	

Note

Many of the Accept policies will match correctly without adjustment. However, any multi-word Accept policies such as "Enterprise User" or "Guest Access" need to be adjusted so that no spaces are included in the Filter-ID (The RADIUS attribute sent by the Access Control Engine must exactly match the mapping configured on the access point). Alternatively, see Appendix D for steps to format the attribute values at runtime rather than individually.

If additional policy mapping rules are required, they can be added via the Policy Mappings section under Profiles. This screen is also useful to easily verify all policy mappings.

ExtremeClo	ud IQ Site Engine		
👬 Network	Dashboard Policy Access Control	End-Systems Reports	
🔔 Alarms & Events	Configuration	Default	
🔓 Control	 Configurations 	▲ Add Edit ⊜ Delete	Switch to Advanced
Analytics	► AAA		
奈 Wireless	▼ Profiles	Access Point	Policy Role
Compliance	Access Point NAC Profile	Administrator A	Administra
III Reports	Administrator NAC Profile	Assessing A	Assessing
Tasks	Allow NAC Profile	Deny Access E	Deny Access
🐸 Administration	Default NAC Profile	Enterprise Access E	interprise
≓ Connect	Enterprise Access NAC Profile	Enterprise User E	interprise
	Guest Access NAC Profile	Enterprise User (Administrator) E	Interprise
	Notification NAC Profile	Enterprise User (Read-Only Manag E	Interprise
	Pass Through NAC Profile	Failsafe F	ailsafe
	Printer NAC Profile	∢ Guest Access G	Suest Access
	Quarantine NAC Profile	Notification	votification
	Registration Denied Access NAC Pro	Printer P	Printer
	Secure Guest Access NAC Profile	Quarantine C	Quarantine
	Server NAC Profile	Server S	Server
	Unregistered NAC Profile	Unregistered	Jnregistered
	VoIP Phone NAC Profile	VoIP Phone V	/oIP Phone
	 Policy Mappings 		
	Default	•	

After enforcing the changes to ExtremeControl, validation of the configuration can be performed.



Part 3: Validation

Two validation steps should be performed. The first is for the secure SSID, ensuring that 802.1X is working as expected. The second point of validation is for the Guest Network. This validation includes Captive Portal Redirection, Change of Authorization based on registration, and User Profile assignment based on the state of the end system.

Secure SSID Validation

Assuming that ExtremeControl is properly configured to authenticate 802.1X requests, the secure SSID can be tested. Select the SSID from the available SSID list.



When prompted for a username and password, enter valid credentials. If prompted, also trust or ignore any certificate warnings.



When connected, validate that traffic can be passed as expected.



In ExtremeControl, navigate to the End-Systems tab and validate that all of the information is properly populated for the newly connected client.

D	ashboard Policy	Access Control	End-Systems	Reports				Q	? ≡
48	Add To Group 🔬	Force Reauthenticatio	n 🌼 Tools 👻 🕯	Live 👻 📔 📶 All	End-System Events			🛛 Devices: All	+ Q
s	Last Seen ↓	IP Address	MAC Address	MAC OUI Vendor	Host Name	Device Family	Device Type	User Name	Site
0	1/22/2020 3:43:47 PM	192.168.50.150	68:1C:A2:04:9A:3A	Rosewill Inc.	desktop-cbq501h.c	Windows	Windows 8/ 8.1/ 10/ 2012	user1	/World

Open the **End-System Details** screen by double-clicking the client. This screen shows information regarding the connected client. In particular, the policy and profile assigned to the client as well as the username that authenticated to the network.



Selecting the End-System tab shows additional information including the Reason (rule) that the end system hit as well as the raw Filter-ID that was returned in the RADIUS Accept message.

Dashboard Policy	Access Control End	d-Systems Reports	End-System Details:	desktop-cbq501h.c	se.ets.com	Q	? ≡
Access Profile End-S	ystem End-System E	vents Health Results					
🝰 Add To Group 🛛 🔏 For	ce Reauthentication 🦼	Force Reauthentication and	Scan 🚯 Lock MAC 🛛	b Edit Registration	2 Refresh End System	n	
End-System Details							
End-System: User Name: Activity: Device Information:	68:1C:A2:04:9A:3A, 192. user1 Last seen 01/22/2020 03: Windows (Windows 8/ 8.1	168.50.150, desktop-cbq501 43:47 PM, First seen 01/22/ // 10/ 2012)	h.cse.ets.com 2020 03:43:36 PM				
Location							
Location: Access Control Engine: ELIN:	192.168.3.165/34-85-84-0 Default, 10.120.85.81	06-65-D4:XIQ-Control-Secur	e, change_me				
Authentication Sessions							
Session Time: Policy: RFC 3580 VLAN:	01/22/2020 03:43:47 PM EnterpriseUser	State: Extended State: State Description:	Accept				
Profile: Reason:	Default NAC Profile Rule: "802.1X"	Last Scan Result: Authorization:	Filter-Id='EnterpriseUser'	1			
Begistration							
NetSight Administrator/root] Last Up	dated: 1/22/2020 3:46:11 PM Uptime	: 14 Days 01:35:55			Operations	a 4 0	0 0 0

In ExtremeCloud IQ, select **Clients** under the Manage tab and note the username of the client, the SSID, and the assigned User Profile.

▼₀ ►	REAL	TIME HISTORIC	AL 1 Conne	cted Clients. Last	Jpdated at 2020	0-01-22 16:14:1	3			Default	View	• 0	3 山 11
	Status Health	Connection Type	Host Name	Connection Status	IPv4	MAC	User Name	OS Type	VLAN	SSID	Organization	User Profile	Location
	۵	WIRELESS	DESKTOP-C	CONNECTED	192.168.50.150	681CA2049A3A	user1	Windows 10	50	XIQ-Control-Secure		EnterpriseUser	

Guest SSID Validation

Prior to starting the Guest SSID validation, ensure that any previously known SSID is forgotten.

Select the open SSID from the available SSID list.



When connected, an automatic redirection can occur based on the operating system. Ignore any certificate warnings and continue.



The web traffic for the client is redirected to the captive portal hosted by the Access Control Engine.

Extreme networks	
Icome to the Enterprise Registration Center	
You have been denied network access because this device is not registered to the network.	
To obtain network access, you must complete registration using the form below	
By registering to the network, you are agreeing to the terms and conditions explained in the <u>Enterprise Network</u>	etwork and Computer Acceptable-Use Policy
First Name:	
Middle Name:	
Last Nama:	
Last Name.	
E-Mail Address:	
Complete Registration	
Please press the Complete Registration button only once.	
	Powered by
	LEXTERNIE networks

At this point, ExtremeControl assigns the **Unregistered NAC Profile** and returns the Filter-ID of **Unregistered**. This can be verified in the End-Systems tab in ExtremeControl.

D	ashboard Policy	Access Control	End-Systems	Reports							Qī	? ≡
đ	Add To Group 🥻	Force Reauthentication	on 💮 Tools 💌 📔	• Live 👻 📔 All	End-System Events					▽.	Devices: All 💌	Q
s	Last Seen ↓	IP Address	MAC Address	MAC OUI Vendor	Host Name	Device Family	Device Type	User Name	Switch IP	Switch Nickname	Authorization	
2	1/23/2020 9:38:18 AM	192.168.50.150	68:1C:A2:04:9A:3A	Rosewill Inc.	desktop-cbq501h.c	Windows	Windows 8/ 8.1/ 10/ 2012		192.168.3.165	AP-99	Filter-Id='Unregis	tered'

In ExtremeCloud IQ, the User Profile assigned to the client is also shown as Unregistered.

Extr	remeCloud [®] IQ	ONBOARD	CONFIGURE	MANAGE ML IN	NSIGHTS DAS	HBOARD	CLOUD VIEW	A3				Q	9 O	-
	Connection Sta	atus (2)		DEVICES		Clie	ents & Users 🗍) ()	Alar	rms 0 5 0		ļ	Security 0	
r +	REAL TIME HISTORIO	CAL 1 Conne	cted Clients. La	USERS	3 09:41:18							Default Vie	9W	
	Status Health Connection Type	Host Name	Connection Sta	EVENTS ALARMS		User Name	OS Type	VLAN	SSID	Organization	User Profile	Location	Last Sess Start Time	ilon e
	S WIRELESS	DESKTOP-C	CONNECTED	SECURITY	A2049A3A		Windows 10	50	XIQ-Control-Open		Unregistered		2020-01-2 16:21:56	2

On the web page on the client, fill out the fields and select **Complete Registration** to submit the registration to ExtremeControl.

/37



A Change of Authorization (CoA) is sent with a new Filter-ID based on the rules engine configuration. Depending on the configuration of the Captive Portal, the client's web traffic is redirected to a success page after the User Profile is changed. Looking at the **End-Systems** table in ExtremeControl, the Authorization column shows that the GuestAccess Filter-ID is assigned to the client.

D	ashboard Policy	Access Control	End-Systems	Reports							Q	? ≡
-	Add To Group	Force Reauthenticatic	in 🔮 Tools 👻	Live 👻 📶 All	End-System Events					▽.	Devices: All 👻	- I Q
s	Last Seen ↓	IP Address	MAC Address	MAC OUI Vendor	Host Name	Device Family	Device Type	User Name	Switch IP	Switch Nickname	Authorization	
2	1/23/2020 9:43:19 AM	192.168.50.150	68:1C:A2:04:9A:3A	Rosewill Inc.	desktop-cbq501h.c	Windows	Windows 8/ 8.1/ 10/ 2012	Doe, John	192.168.3.165	AP-99	Filter-Id='Guest/	Access'

The End System Details for the client are populated with the additional information that was entered in the captive portal.



When looking at the End-System Details, additional information can be verified in regards to the Registration and Authentication information.

Dashboard P	olicy	Access Control End-	Systems Reports	End-System Details: desktop-cbq501h.cse.ets.com
Access Profile	End-Sy	stem End-System Eve	ents Health Result	S
🖂 Add To Group	🚑 Forc	e Reauthentication 🛛 🚑 F	orce Reauthentication an	d Scan 🛭 🐞 Lock MAC 🛛 👵 Edit Registration 🛛 🤁 Refresh End System
End-System Deta	ails			
End-System: User Name: Activity: Device Informatio	on:	68:1C:A2:04:9A:3A, 192.16 Doe, John Last seen 01/23/2020 09:4 Windows (Windows 8/ 8.1/	68.50.150, desktop-cbq50 3:19 AM, First seen 01/2 10/ 2012)	01h.cse.ets.com 2/2020 03:43:36 PM
Location				
Location: Access Control E ELIN:	Ingine:	192.168.3.165/34-85-84-06 Default, 10.120.85.81	3-65-D5:XIQ-Control-Ope	n, change_me
Authentication Se	essions			
Session Time: Policy: RFC 3580 VLAN	:	01/23/2020 09:43:19 AM GuestAccess	State: Extended State: State Description:	Accept Authenticated Rule 0 [Any, ***, Any] , Auth Method: LOCAL_AUTH
Reason:		Rule: "Registered Guests"	Authorization:	Filter-Id='GuestAccess'
Registration				
State: User Name: User Email:		Approved Doe, John jdoe@extremenetworks.co	Group: Sponsor Group: m Sponsor:	Registered Guests
User Phone: Registration Type	9:	Guest Registration	Registration Time: Start Time:	01/23/2020
Max Devices: Description:		2	Expires Time:	02/22/2020

In the End-System Events for the device, the historical audit trail is available.

	Dashboard P	olicy A	ccess Control	End-System	s Reports E	nd-System Details:	desktop-cbq501	h.cse.ets.com				Q
	Access Profile	End-Syst	tem End-Syst	em Events	lealth Results							
8	🔒 Add To Group	🔏 Force I	Reauthentication	对 Force Real	uthentication and Scan	illi Lock MAC	Edit Registration	Refresh End	I System			
	Export End-Syst	tem Events to	CSV									
s.	Time Stamp	Ac	cess Control	Profile	IP Address	MAC Address	User Name	Host Name	Device Family	Device Type	Switch Port	
0	1/23/2020 9:43:	19 AM 10	.120.85.81	Guest Acces	192.168.50.150	68:1C:A2:04:9A:3A	Doe, John	desktop-cbq501	Windows	Windows 8/	34-85-84-06-65-D5:XIQ-Control-O	pen
0	1/23/2020 9:38:	18 AM 10	.120.85.81	Unregistered	192.168.50.150	68:1C:A2:04:9A:3A		desktop-cbq501	Windows	Windows 8/	34-85-84-06-65-D5:XIQ-Control-O	pen
5	1/23/2020 9:35:	05 AM 10.	.120.85.81	Unregistered	192.168.50.150	68:1C:A2:04:9A:3A		desktop-cbq501	Windows	Windows 8/	34-85-84-06-65-D5:XIQ-Control-O	pen
0	1/22/2020 4:22:	06 PM 10.	.120.85.81	Unregistered	192.168.50.150	68:1C:A2:04:9A:3A		desktop-cbq501	Windows	Windows 8/	34-85-84-06-65-D5:XIQ-Control-O	pen
0	1/22/2020 4:21:	55 PM 10.	.120.85.81	Unregistered		68:1C:A2:04:9A:3A		desktop-cbq501	Windows	Windows 8/	34-85-84-06-65-D5:XIQ-Control-O	pen
0	1/22/2020 4:21:	55 PM 10.	.120.85.81	Unregistered		68:1C:A2:04:9A:3A		desktop-cbq501	Windows	Windows 8/	34-85-84-06-65-D5:XIQ-Control-O	pen
N	1/22/2020 4:21:	42 PM 10.	.120.85.81	Default NAC	192.168.50.150	68:1C:A2:04:9A:3A	user1	desktop-cbq501	Windows	Windows 8/	34-85-84-06-65-D4:XIQ-Control-S	ecure
0	1/22/2020 4:12:	48 PM 10.	.120.85.81	Default NAC	192.168.50.150	68:1C:A2:04:9A:3A	user1	desktop-cbq501	Windows	Windows 8/	34-85-84-06-65-D4:XIQ-Control-S	ecure
0	1/22/2020 4:12:	38 PM 10.	.120.85.81	Default NAC		68:1C:A2:04:9A:3A	user1	desktop-cbq501	Windows	Windows 8/	34-85-84-06-65-D4:XIQ-Control-S	ecure
0	1/22/2020 4:12:	38 PM 10	.120.85.81	Default NAC		68:1C:A2:04:9A:3A	user1	desktop-cbq501	Windows	Windows 8/	34-85-84-06-65-D4:XIQ-Control-S	ecure
5	1/22/2020 4:11:2	25 PM 10.	.120.85.81	Default NAC	192.168.50.150	68:1C:A2:04:9A:3A	user1	desktop-cbq501	Windows	Windows 8/	34-85-84-06-65-D4:XIQ-Control-S	ecure
0	1/22/2020 3:43:	47 PM 10	.120.85.81	Default NAC	192.168.50.150	68:1C:A2:04:9A:3A	user1	desktop-cbq501	Windows	Windows 8/	34-85-84-06-65-D4:XIQ-Control-S	ecure
0	1/22/2020 3:43:	46 PM 10.	.120.85.81	Default NAC		68:1C:A2:04:9A:3A	user1	DESKTOP-CBQ	Windows	Windows 8/	34-85-84-06-65-D4:XIQ-Control-S	ecure
0	1/22/2020 3:43:	36 PM 10.	.120.85.81	Default NAC		68:1C:A2:04:9A:3A	user1				34-85-84-06-65-D4:XIQ-Control-S	ecure
0	1/22/2020 3:43:	36 PM 10.	.120.85.81	Default NAC		68:1C:A2:04:9A:3A	user1				34-85-84-06-65-D4:XIQ-Control-S	ecure

Even though the User Profile is correctly assigned, ExtremeCloud IQ does not show the updated information until the client fully reauthenticates either by disconnecting from the network or by an administrator selecting Force Reauthentication. Furthermore, ExtremeCloud IQ periodically updates the information. Lastly, the profile can be verified in the CLI using the commands **show station** and **show user-profile**.

AP-99#show station Chan=channel number; Pow=Pow A-Mode=Authentication mode; A-Time=Associated time; Auth UPID=User profile Identifier	ver in dBm; Cipher=Encrypti n=Authenticated; r; Phymode=Physi	ion mode; ; ical mode;																
Ifname=wifi0.1, Ifindex=19, Mac Addr IP Addr	SSID=XIQ-Contro Chan Tx Rate	ol-Secure: e Rx Rate Po	w(SNR)	A-Mode	Cipher	A-Time	VLAN	Auth	UPID	Phymode	LDPC	Tx-STB(C Rx-STBC	SM-PS	Chan-width	MU-MIMO R	elease	Station-State
Ifname≕wifil.1, Ifindex=21, Mac Addr IP Addr	SSID=XIQ-Contro Chan Tx Rate	ol-Secure: e Rx Rate Po	w(SNR)	A-Mode	Cipher	A-Time	VLAN	Auth	UPID	Phymode	LDPC	Tx-STB(C Rx-STBC	SM-PS	Chan-width	MU-MIMO R	elease	Station-State
Ifname≕wifi0.2, Ifindex=22, Mac Addr IP Addr	SSID=XIQ-Contro Chan Tx Rate	ol-Open: e Rx Rate Po	w(SNR)	A-Mode	Cipher	A-Time	VLAN	Auth	UPID	Phymode	LDPC	Tx-STB(C Rx-STBC	SM-PS	Chan-width	MU-MIMO R	elease	Station-State
681c:a204:9a3a 192.168.50.15	50 11 65M	M 72.2M -	28(66)	open	none	00:02:53	50	Yes	1	11ng	No	No	No	static	20MHz	No	No	Good
Ifname=wifi1.2, Ifindex=23, Mac Addr IP Addr	SSID=XIQ-Contro Chan Tx Rate	ol-Open: e Rx Rate Po	w(SNR)	A-Mode	Cipher	A-Time	VLAN	Auth	UPID	Phymode	LDPC	Tx-STB(C Rx-STBC	SM-PS	Chan-width	MU-MIMO R	elease	Station-State
AP-99#show user-profile ◀━ User Profile Table VLAN(*) means User Profile u Total Entries = 4	use a VLAN GROUF	».																
No. User Profile Name	VLAN	Attribute																
1 default-profile 2 GuestAccess 3 EnterpriseUser 4 Unregistered AP-99#	1 50 50 50	0 1 2 3																

Navigating to ExtremeCloud IQ, when the client is reauthenticated, the User Profile can be verified in the Clients view.

1	REAL TIME HISTORICAL 1 Connected Clients. Last Updated at 2020-01-23 09:54:11										D	efault View	•	0 4 1	
	Status Health	Connection Type	Host Name	Connection Status	IPv4	MAC	User Name	OS Type	VLAN	SSID	Organization	User Profile	Location	Last Session Start Time	Device
	0	WIRELESS	DESKTOP-C	CONNECTED	192.168.50.150	681CA2049A3A		Windows 10	50	XIQ-Control-Open		GuestAccess	3	2020-01-23 09:54:06	AP-99

The information is also available when client details are displayed.

DESKTOP-CBQ501H VLAN: 50				
CURRENT CONNECTION STATUS OS TYPE Windows 10 IP ADDRESS 192,168.50.150 MAC ADDRESS 681CA2049A3A USER N/A CONNECTED TO AP-99 51 Secs VLAN CAPTIVE WEB PORTAL	Time Range: Day I Hour 2 Hours Usage (Click timeline to change SELECTED time Usage (Click timeline to change SELECTED time Usage (Slick timeline to change SELECTED timeline to change SELECTED timeline to c	4 Hours 8 Hours 24 Hours ne, drag to change time range) 09:14 09:24 00:54:57	09:34 09	
Unused USER PROFILE GuestAccess	Selected Time Most Time Spent Most Us	MOST USAGE TOP SESSI	ION VIEW	
SID XIQ-Control-Open RADIO 802_11ng 2.4G CHANNEL 11	100 % AP-09 AP with most data sent and received	Total Usage 21.14 KB Session Start 01/22/2020 08:54:57 Session Duration 59 MINS 8 SECS Average RSSI - 22 dBm Average SNR 72 dB	Avera	ge RSSI 🧄
LOCATION Unassigned	Session Details >	~		

/41

Appendix A: Creating RFC 3576 Configurations

This step is not needed in ExtremeCloud IQ - Site Engine version 21.11 and later.

Instead of configuring the Reauthentication Type for each access point as it is added to ExtremeControl, the Reauthentication type can be set based on the SNMP SysObject ID for the AP. This is a more scalable approach when adding multiple access points. To add the entry, right click on the **Default** Engine Group and select **Engine Settings**. Choose the **Reauthentication** menu item and **Add** a new Reauthentication Configuration.

Dashl	board Policy Access Control	End	l-Systems Reports					
Conf	iguration	+	Engine Group - Defau	ılt				
Grou	p Editor	+	Details Switches Er	nd-Systems Access Control Engines G	uest and IoT	Managers		
Engir	les	_	Engine Settings - Def	ault				
▼ Er	ngine Groups		Credentials	Reauthentication				
-	Default		Network Settings	Set reauthentication time for Acce	ment interval			
•	Add Engine		Device Type Detection	Accept Session Timeout (in minute	s)		Enabled for All Switch	es 🔍
•	Enforce Access Control Configuration		IP Address Resolution	I Quarantine Session Timeout (in mi	nutes)	10	Enabled for Session-T	imeout Switches 🔍
	Delete Engine Group		Hostname Resolution	🕑 Unregistered Session Timeout (in r	ninutes)	3	Enabled for Session-T	imeout Switches 📼
	Engine Group Properties		Username Resolution	Session Timeout (in seco	nds)	30	Enabled for Session-T	imeout Switches 🔍
	Choose Settings		Reauthentication	Session Deactivate Timeout (in mir	iutes)			
L	Engine Settings: Default		Miscellaneous	Switch Reauthentication Config	uration			
			Auditing	Add 🕞 Edit 😑 Del	ete			
				sysObjectId	Reauther	ntication Type		Port Link Control
			1	1.3.6.1.4.1.388.11.1.1	RFC 3576	- Extreme Wire	eless WiNG	Disabled

Set the sysObjectID to **1.3.6.1.4.1.26928.1**; it is the same for all ExtremeCloud IQ APs. Set the Reauthentication Type to **RFC 3576** and the Configuration to **Generic CoA Hyphen Delimited**.

Add Switch Reauthentication Configuration								
sysObjectId:	1.3.6.1.4.1.26928.1							
Reauthentication Type:	RFC 3576	~						
RFC 3576 Configuration:	Generic CoA Hyphen Delimited	-						
Manage RFC 3576 Configu	irations							
Enable Port Link Contr	ol							
	ок	Cancel						

When complete, the configuration should look similar to this.

Engine Settings - Defa	ault					×
Credentials	Reauthentication					^
Network Settings	Set reauthentication time for Accepted end-systems to Assessment interval					
Device Type Detection	Accept Session Timeout (in minutes)	Accept Session Timeout (in minutes)			S T	
IP Address Resolution	🕑 Quarantine Session Timeout (in minu	utes)	10	Enabled for Session-Tir	•	
Hostname Resolution	S Unregistered Session Timeout (in min	nutes)	3	Enabled for Session-Tir	neout Switches	-
Username Resolution	Session Timeout (in second	ds)	30	Enabled for Session-Tir	neout Switches	~
Reauthentication	Session Deactivate Timeout (in minut	tes)	10			
Miscellaneous						
Auditing	Switch Reauthentication Configur	ation				
	🕞 Add 🔯 Edit 🤤 Delete	e				
	sysObjectId 👃	Reauthenti	cation Type		Port Link Control	
	1.3.6.1.4.1.26928.1	RFC 3576 -	Generic CoA Hy	yphen Delimited	Disabled	
	1.3.6.1.4.1.14525.3.3	RFC 3576 -	Juniper Wireles	s	Disabled	
	1.3.6.1.4.1.14525.3.2 RFC 3576 - Juniper Wireless Disabled					
	1.3.6.1.4.1.14525.3.1 RFC 3576 - Juniper Wireless Disable				Disabled	
	1.3.6.1.4.1.5624.2.1.92 SNMP				Disabled	
	1 2 6 1 / 1 562/ 2 1 6/	CNIMD			Nisahlad	-
					Save	Cancel

Appendix B: Enable RFC 3576 Reauthentication on ExtremeCloud IQ

By default, if the RADIUS Server was added as an Extreme Networks A3 server, RFC 3576 is already enabled. However, if it was added as an External RADIUS Server, then it will need to be enabled manually. To do this, edit the **Network Policy** in the **Configure** menu, choose the SSID in Wireless Networks, and find the Authentication Settings section. Edit the RADIUS Server Group. For Enterprise WPA / WPA2 / WPA3, the screen will look similar to this:

Network Policies > XIQ-ExtremeContr	rol > All SSIDs > XIQ-Control-Se	cure			
Policy Details	Wireless Networks		Device Templates		Router Se
CONFIGURATION GUIDE	Wireless Network				
Policy Name XIQ-ExtremeControl RADIUS Server Group ExtremeControl User Profile EnterpriseUser	Name (SSID) * Broadcast Name * SSID Usage	XIQ-Control-Secure	9	Broadcast ViiFi0 VViFi1	SSID Using Radio (2.4 GHz or 5 GHz) Radio (5 GHz only)
	SSID Authentication	MAC Authenticat	Personal WPA/WPA2/WPA3		nivate Pre-Shared
	Key Management WPA2-802		2.1X -		
	Enable Captive Web Portal	OFF	S)	•	
	Authentication Setting	S			
	Authentication with Extre Authenticate via				
	Default RADIUS Server Group ExtremeControl				
	Name		Тур	e	
	ExtremeControl1		Extr	eme Networks A3	

Select the gear icon as shown below for advanced settings.

xtremeControl				×
ADIUS Server Group Name * ExtremeControl	RADIUS Server Group Description	~		
EXTERNAL RADIUS SERVER (0)	EXTREME NETWORKS A3 (1)	EXTREME NETWORKS RADIUS SERVER (0)	EXTREME NETWORKS RADIUS PROXY (0)	
7 + 🗇				
Name		IP/Host Name		
ExtremeControl1		10.120.85.81		

Select the check box labeled Permit Dynamic Change Of Authorization Messages (RFC 3576).

ExtremeControl		×
SelectRadiusSettings		
Note: These settings only apply for Hive	eOS devices. These settings are ignored for non-HiveOS devices.	
Retry Interval	600	
	Range: 60 - 100000000 (seconds)	
Accounting Interim Update Interval	600 Range. 10 - 100000000 (seconds)	
Permit Dynamic Change Of Author	rization Messages (RFC 3576)	
Inject Operator-Name attribute		
Message Authenticator attribute		
Not Supported for Extreme Networks R	ADIUS Proxy	
	CANCEL SAVE RADIO	JS SETTINGS

Appendix C: DHCP Fingerprint for ExtremeCloud IQ Access Points

For the ExtremeCloud IQ access point to be recognized as an appropriate device type in the **End-Systems** table, a DHCP fingerprint needs to be added. Select **Administration** in the main menu and **Device Types** in the top menu. Then select **Detection and Profiling** and select **Import**.

Profiles Users Server Inf	ormation Certificates Options Device Types	Backup/Restore Diagn
Detection and Profiling MAG	OUI Vendors	
🗿 Add 💮 Edit 🥥	Delete/Reset 🏝 Import	
Device Type 🕇		
Family: Amazon Kindle	Import Device Type Profiles	×
Amazon Kindle	File: CloudAP-fingerprint.xml	Select File
E Family: Android		
Amazon Kindle Fire		Import Cancel

The following content should be imported through the file with XML extension:

Appendix D: RADIUS Reponse Formatting

As of version 8.3, ExtremeControl can format RADIUS Attributes at runtime. This means that rather than modifying the Policy Mappings for each Accept policy to remove spaces, the RADIUS Attribute configuration can be modified to modify the response at run time.

The available modifications are:

- UPPER Changes the response variable to all uppercase. For example: **Guest Access** becomes **GUEST ACCESS**.
- LOWER Changes the response variable to all lowercase. For example: **Guest Access** becomes **guest access**.
- STRIP Removes all whitespace from the variable including spaces. For example: **Guest Access** becomes **GuestAccess**.
- UPPER-STRIP Removes all whitespace and changes the response to uppercase. For example: **Guest Access** becomes **GUESTACCESS**.
- LOWER-STRIP Removes all whitespace and changes the response to lowercase. For example: **Guest Access** becomes **guestaccess**.

The modifications are applied to the variable portion of the RADIUS Attribute Configuration. Using a simple Filter-ID configuration as an example, The value of **Filter-Id=%FILTER_NAME%** would be changed to **Filter-Id=%FILTER_NAME:STRIP%** to remove the whitespace from the variable.

The configuration is adjusted when assigning the RADIUS Configuration in the Add Switch dialog. In the RADIUS Attributes to Send drop-down menu, select New.

Configure Device: 192.168.3.165			×
Switch Type:	Layer 2 Out-Of-Band	•	
Primary Engine:	10.120.85.81/10.120.85.81	•	
Secondary Engine:	None	•	
Auth. Access Type:	Manual RADIUS Configuration	•	
Virtual Router Name:			
RADIUS Attributes to Send:	Filter-Id	•	
RADIUS Accounting:	New		
Management RADIUS Server 1:	Manage		
Management RADIUS Server 2:	None		
	Cisco Per-User ACL		
Network RADIUS Server:	Cisco Wired Dynamic ACL	<i></i>	
Policy Domain:	Cisco Wired RFC 3580 and Dynamic ACL	<i></i>	
Advanced Settings	Cisco Wireless Dynamic ACL	*	
	Cisco Wireless RFC 3580 and Dynamic ACL	<i></i>	_
	Extreme BOSS	\$	Close

In the new window, keep the same variable, however add **:STRIP** to the end to remove whitespace.

Edit RADIUS Attribute Configuration				
Name:	Filter-Id (Strip)			
Enable Port Link Control:				
Attributes :	•	Substitutions :	÷	
Filter-Id=%FILTER_NAME	STRIP%			
			Save Clo	se
			Save Clo	se

Ensure the new configuration is selected when saving the Switch configuration.

Configure Device: 192.168.3.16	5		×
Switch Type:	Layer 2 Out-Of-Band	•	
Primary Engine:	10.120.85.81/10.120.85.81	~	
Secondary Engine:	None	•	
Auth. Access Type:	Manual RADIUS Configuration	-	
Virtual Router Name:			
RADIUS Attributes to Send:	Filter-Id (Strip)	-	
RADIUS Accounting:	Enabled	•	
Management RADIUS Server 1:	None		
Management RADIUS Server 2:	None	~	
Network RADIUS Server:	None		
Policy Domain:	Do Not Set	-	
Advanced Settings			
		Save	Close

After enforcing, the next time the Policy is assigned, the modification to the RADIUS Attribute is applied automatically.

	E	dit Policy Mapping	g				×	
		Name:	Guest Access					
		Map to Location:	Any			•		
		Policy Role:	Guest Access			•		
		VLAN [ID] Name:	None			-		
		VLAN Egress:	Untagged	*	U			
		Filter:	Guest Access					
		Port Profile:						
		Virtual Router:						
		Login-LAT- Group:	Guest Access					
		Login-LAT-Port:	1					
		Custom 1:						
		Custom 2:						
					Sa	ve Cano	el	
Dashboard Pol	licy Ac	cess Control	End-Systems F	leports Er	d-System Details	: desktop-cb	q501h.	cse.ets.com
Access Profile	End-Syste	End-System	n Events Health	Results				
Add To Group	🔏 Force F	leauthentication	Force Reauthentic	ation and Scan	🐌 Lock MAC	ili Edit Regis	stration	2 Refresh End Syster
End-System Detail	s							
End-System: User Name: Activity: Device Information:	6 D L	8:1C:A2:04:9A:3A, 1 ooe, John ast seen 01/24/2020 Vindows (Windows 1	192.168.50.150, deskto 0 11:15:47 AM, First se 00)	op-cbq501h.cse en 01/24/2020	.ets.com 10:46:05 AM			
Location								
Location: Access Control Eng ELIN:	1 gine: D	92.168.3.165/34-85- 9efault, 10.120.85.81	-84-06-65-D5:XIQ-Con	trol-Open, char	ge_me			
Authentication Ses	sions							
Session Time: Policy:	0 G	1/24/2020 11:15:47 auestAccess	AM State: Extended State	<i>)</i> e:	Accept			
RFC 3580 VLAN: Profile: Beason:	G	uest Access NAC P	State Description	on: A ult:	Authenticated Rule 0	[Any, "*", Any] , /	Auth Meth	nod: LOCAL_AUTH
166301.		alo. Tiegistereu du	Putrionzation.	r	mor-iu- GuestAcces			

Registration

Appendix E: ExtremeCloud IQ - Site Engine Licensing Note

Each RADIUS Client (the source of the RADIUS request, or the NAS) must be added to the ExtremeCloud IQ - Site Engine database. The number of added devices contributes to the total cost of ownership. Because ExtremeCloud IQ APs are expected to be managed through ExtremeCloud IQ, they will not consume any additional licenses (a license is tied to a serial number). However, any non-ExtremeCloud IQ native device will consume a Pilot or Navigator license if managed with SNMP. The exception to this is when **Poll Status Only** is selected. In this case, no license will be consumed by ExtremeCloud IQ - Site Engine for this device.