

Extreme AirDefense Essentials Setup Guide

ExtremeCloud IQ Essentials Documentation

Published: May 2021

Extreme Networks, Inc. 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. All other registered trademarks, trademarks, and service marks are property of their respective owners. For additional information on Extreme Networks trademarks, see www.extremenetworks.com/company/legal/trademarks

Contents

Introduction to Extreme AirDefense Essentials	2
Initial Setup for Extreme AirDefense Essentials	2

Introduction to Extreme AirDefense Essentials

Extreme AirDefense Essentials is a cloud-based management tool you can use to configure, implement and review security protocols that evaluate and monitor threat detection for devices in your network.

Extreme AirDefense Essentials displays various data and statistics for the locations managed in your network including. Use it to track alarms detected through the life cycle and view documented details, such as whether alarms are currently active or inactive, the types of alarm categories, Live and Expired alarms details and the total number of alarms detected in Extreme AirDefense Essentials.

Extreme AirDefense Essentials includes an Impact Percentile Map, Use the map to select a location and display details about the alarms at the site, including the threat score and percentile, the total number of alarms, and a break-down of the alarms by alarm severity: Critical, Major, Minor, and Info.

Initial Setup for Extreme AirDefense Essentials

To set up Extreme AirDefense Essentials, you will create a network policy, onboard a device, and launch the Extreme AirDefense Essentials app.. Follow these steps:



2. In ExtremeCloud IQ, select ML Insights > Add network plan.

← →	C i va.extremecloudiq.com/	#/plan/539581036463833/overvi	iew 🔞 Sian in Denk	😵 System Dashboard., 🖪 G7-EstremeCloud IO 🔎 G882-EstremeClou., 📮 G	281-ExtremeClou		_ u ☆	0
-	ExtremeCloud IQ Pilot	-	-	_		9 O	a qa qa QA-test	E
•	III ML INSIGHTS	Search Maps	Q	IMPORT MAP ADD LOCATION				
•	Network 360 Plan	Global View	B H H	Map Satellite	Arctic Ocean		Arctic Ocean	
*>	Network 360 Monitor	🖂 🖗 Karnataka	17 +					
1	Network Scorecard	田 圓 Domiur	12 +	+ en andre 🖓	1. S. S. P.		ALC: NOT	
	Client 360	田 圓 JayaNagar	0′ + ···				1 A	
	Comparative Analytics	E 🛛 Maharashtra	₫ + …		Desister a	entend		
•	Proximity & Presence	田田 mumbal	12 +	Frand	Lach Star De l		Finland	
	VPN Topology	+ Add		Russe			Norway	1
		÷		Peland Germany Ukrahite Kazakinstan Ukrahite	Canada	×	Poland Germany Ukranie Kazakiv	
				nay Turkey Chica South Kees	North United States No	orth	France Spain Raly Turkey	
				Prej kan Pakster	Ocean Oc	ean /	Algeria Libya Egypt Tool Andre	
				Neer Chad Sadar			Mall Niger Chad Suden	

3. Select Manage devices > Create network policy.

E ExtremeCloud IQ × +						- 0	
\leftrightarrow \rightarrow C a va.extremecloudiq.com	/#/config					* 0	ł
Apps 🕲 Index of /images 🕲 Index of /	(dalybuild. 🔄 CLOUD-ExtremeClou. 🧕 Sign in (Jenkins) 😵 System Dashboard 🖪 G7-ExtremeCloud IQ 📮 G8R2-ExtremeClou 📮 G2R1-ExtremeClou						
ExtremeCloud IQ Pilo	t	Q	0	≜ ∎	e qa qa QA-test	1	E
🔹 🏚 CONFIGURE	* Network Policies - New Poli						
> Network Policies	POLICY DETAILS WIRELESS NETWORKS DEVICE TEMPLATES ROUTER SETTINGS ADDITIONAL SETTINGS DEPLOY POLICY						
Applications							
II > Common Objects	New Policy						
Users	What type of policy are you creating?						
•	Viveless Switches Routing						
0							
	Please name your policy						1
	Policy Name* Network Policy Name						l
	Description						
	Enable Presence Analytics OFF						

4. In the Network Policy window, do the following:



ExtremeCloud IQ × +									-	a ×
← → C 🔒 va.extremecloudiq.com	n/#/config								☆	Θ:
Apps 🕲 Index of /images 🧐 Index of	i /dailybuild 🖪 CLOUD-ExtremeClo 🗕 Sign in [Jenki	ns] 😵 System Dashboard 🖪 G7-Extrem	neCloud IQ 🖪 GBR2-ExtremeClo	u E G2R1-ExtremeClou						
ExtremeCloud IQ Pilc	ot					Q (J 🖡 🛙	e qa qa QA-test	1	E
🔹 🏚 CONFIGURE	Network Policies test-NP All SSIDs									
Network Policies	POLICY DETAILS WIRELESS NET	WORKS DEVICE TEMPLATES	ROUTER SETTINGS	ADDITIONAL SETTINGS	DEPLOY POLICY					
Applications										
II > Common Objects	Wireless Networks									
Users	+ 📻 📋 🗌 Assign SSIDs using Classific	ation Rules								
A	SSID	GUEST ACCESS		A	CCESS SECURITY		VLAN			
•	test	🔁 Edit		U	insecured (Open) Network		1			
•										

b. Add the corresponding device template:

- Enable WifiO and WifiI as Client access mode.
- Enable Wifi2 by configuring a dummy address and port number.
- Save the device template.

c. Select Additional Settings > WIPS.

d. Select the existing WIPS policy, or create a new WIPS policy by selecting **Configure > Common Objects > Security**.



e. For the WIPS policy, enable AirDefense Essentials.



5. Onboard an AP by selecting Manage Devices > Onboard AP.

	+											-	٥
$ \rightarrow$ C \cong va.extremecloudid	q.com/#/devices												4 (
Apps 📀 Index of /images 📀 Inde	dex of /dailybuild 🖪	CLOUD-ExtremeClo	Sign in [Jenkins] 🔗	System Dashboar	rd 🖪 G7-ExtremeCloud IQ 🔳 G8R2-ExtremeC	lou E G2R1-ExtremeClo	NJ						
ExtremeCloud IQ P	Pilot								Q	0	•	qa qa QA-test	
Evaluate & Buy													
> Onew European General	Data Protection Regula	stions (GDPR) are here!	Please review our Clo	ud Terms of Ser	rvice. Learn more about GDPR and related feature	s In ExtremeCloud IQ here.							
> C CONNECTION ST 3 Online / 0 Offlin	TATUS	🖸 TOTAL A	PPS 2		CLIENTS 1	USERS 0		ALARMS 0	3 0		SI 2 Rogue AP	ECURITY Ps 0 Rogue Clien	ts
CONNECTION STA 8 Online / 0 Office	ne	🖸 TOTAL A	PPS 2		CLIENTS 1	USERS 0		ALARMS 0	3 0 Showing 3 of	3 O Selecte	2 Rogue AP	ECURITY Ps 0 Rogue Clien	ts e
CONNECTION ST. 3 Online / 0 Offlin T pefault View	na	C TOTAL A	PPS 2		CLIENTS 1	USERS 0	idr or Sertal # Q	ALARMS 0] UTILITIES	3 0 Showing 3 of ACTIONS	3 O Selecte UPDATE	SI 2 Rogue AP d Select: DEVICES	ECURITY I O Rogue Clien All Pages, Non	e
CONNECTION ST. 3 Online / 0 offlie 1 Default View + 1 × 1 5 status	HOST NAME		MGT IP ADDRESS	CLIENTS MAG	CLIENTS 1	USERS 0	idr or Sertal # Q MODEL OS VERS	ALARMS O J UTILITIES	3 0 Showing 3 of ACTIONS WIFIO CHANNEL	3 0 Selecte UPDATE WIFIT CHANNEL	SI 2 Rogue AP d Select: DEVICES IQAGEN	ECURITY S 1 0 Rogue Clien All Pages, Non III © AT NTP STATE	e
CONNECTION ST. 3 Colline / 0 Office Perfault View + 1 / 1 STATUS	HOST NAME	C) TOTAL A POLICY UPTIME 460C-NP Od 3h Im	MGT IP ADDRESS 1 1601610.48	CLIENTS MAG	CLIENTS 1 C LOCATION F3102A950 GA-test >> Karnataka >> JayaNay	USERS 0	MODEL OS VERS	ALARMS 0 UTILITIES ON UPDATED 10- 2020-10-01 02:52:27	Showing 3 of ACTIONS WIFIO CHANNEL 1	3 O Selecte UPDATE WIFT CHANNEL 161	SI 2 Rogue AP d Select: DEVICES IQAGEN N/A	All Pages, Non	e
CONNECTION ST. 3 Colline / 0 Office T patient View + ± / 1 Status Califier / 0 office Califier / 0 office C	HOST NAME AH-2a9500	C) TOTAL A POLICY UPTIME 460C-NP Od 3h Im 460C-NP Od 2h 9a	MGT IP ADDRESS 1603610.48 192368.20.21	CLIENTS MAC 1 BCI 0 BCI	CLIENTS 1 c LOCATION F3102A950 QA-test >> Karnataka >> JayaNar F3102A950 QA-test >> Maharashtra >> mund	USERS 0	dr or Sertal # Q MODEL OS VERS AP460C 10.2.2.0 AP460C 10.2.2.0	ALARMS 0 UTILITIES ON UPDATED 10 2020-10-01 02:52:27 10 2020-10-01 03:44:55	Showing 3 of ACTIONS WIFIO CHANNEL II II	3 O Selecte UPDATE WIFI CHANNEL 161	SI 2 Rogue AP d Select: DEVICES JQAGEN N/A N/A	All Pages, Non	e

6. When the AP is reported online in ExtremeCloud IQ, assign the location and the network policy you created earlier.

E Extremel	eCloud I	IQ.	>	+																		-
+ → C	с і	i va.ex	tremeclou	idiq.com/#/	devices																	Q \$
🗄 Apps 🧯	🕑 Inde	lex of /ima	ges 🔕	Index of /dail	/build	E CLOUD-E	xtremeClo	🛛 Sign in (Jenkins	s] 😵 Syst	em Dashboard.	🖪 G7-ExtremeCloud IQ 🔳 G8R2	ExtremeClou	G2R1-	ExtremeClou								
Extre	reme	Cloud I	Q Pilot																Q	0	. 0;	qa qa QA-test
2			CONNECT	ION STATUS			13 10	TAL APPS 2			CLIENTS 1		USERS	0		ALARP	501310			3 Rog	SECURITY Jue APs 0 Rog	r gue Clients
DEVIC	Ŧ	De	tault View															s	howing 3 of 3	0 Selected	Select: All Pr	ages, Nonr
		+	1 /													Serve R. Q.	UTILITIES	A	CTIONS	UPDATE DE	VICES	шC
MAN			STATUS	HOST N	ML .	POLICY	UPTIME	MGT IP ADDRESS	CLIENTS M	uic (LOCATION	SERIAL #	MODEL	OS VERSION	UPDATED	WIFIO CHANNEL	WIFIT CHANNEL	IGAGENT	NTP STATE	WIFID POWER	WIFII POWER	MGT VLAN
			- 5	AH-2a5	500	460C-NP	Od 3h SOm	100.10.10.48	1 6	3CF3102A9500	QA-test >> Kamataka >> JayaNagar >> Jay	24602001/0028	AMGOC	10.2.2.0 (10	2020-10-01 02:52:27	11	363	N/A	Enabled	20	20	1
			- 5	AH-2as	9c0	460C-NP	Od 2h 58m	192368.20.21	0 6	BCF3102A99C	QA-test >> Maharashtra >> mumbal >> mur	246020011/0047	AP460C	10.2.2.0 (10	2020-10-01 03:44:55	п	157	N/A	Enabled	20	20	1
				AH-Sco	580	4100	Od 2h 36m	192.168.2015	0 6	BCF3105CC680	QA-test >> Karnataka >> Domiur >> Domiu	04102005200197	AIMIOC.	10.2.2.0 (10	2020-10-01 04:06:40	6	149	N/A	Enabled	20	18	1
			• 5	AH-Sco	580	4100	Od 2h 36m	192.168.2015	0 6	BCF3105CC680	QA-test >> Kamataka >> Domiur >> Domiu	04102005200197	APMIOC	10.2.2.0 (10	04:06:40	6	149	N/A	Enabled	20		18

7. After the *very first* onboarding and assignment of the network policy, perform a complete CONFIG PUSH on the onboarded AP.

Extrem	neCloud	IQ Pilot	N STATUS Diffinie		CI 101	AL AIRPS 2	Device Update	×	ALAR	s 0 a 0		ų	3.900	SECURITY	PA-test v
GE - DEVI	T 4	ataut View					1 device will be updated	- -	for families at , Q	UTEMES	5	Showing 3 <2	(1 Selected) UPDATE DE	Select: An P	Indext Notes
HANA		STATUS	HOST NAME	+ POLICY	UPTIME	HGT IP ADDRE	Update Network Policy and Configuration		WIFTO	WIFTS CHANNEL	IGAGENT	NTP STATE	WIFID POWER	WIFR	NGT. VLAN
			AH-2a9500	460C NP	Oct (Rt 50m	80.8530.48	Detta Configuration Update	2252.2	n H	367	14/A	Frictient	20	-20.	
		-5	AH-Za99c0	460C NP	Od 2N 58m	192,668,20,25	O Complete Configuration Update	12.445	5 11		14/75	Frabled	20	20	
			AH-Sec680	HOC.	Oct 20:30m	192368.2015	uppara device with all configurations. Used to reset device to instremectous ta configuration settings. (Supported only on devices running HOS or NZE Firmware)	- 185	6	149	14/24	Ended	20	38	
							Upgrade IQ Engine and Extreme Network Switch images	- 188							
							Articulton Time for Extrame Neberty's Davices Bunning Images								

8. Launch Extreme AirDefense Essentials by selecting the **AirDefense** Icon in the left panel. Then select the **Subscribe** button.



9. Verify that AirDefense Essentials is enabled for the WIPS policy. Then select Apply.



The AirDefense Esstentials Summary page opens. As alarms are reported by onboarded sensors, the Summary page displays analytics data.



To view additional details, select More Insights.

End of document

7