(CWA) بيولل ةيزكرملا ةقداصملا نيوكت ISE و Catalyst 9800 WLC ىلع

تايوتحملا

<u>ةمدقملا</u> <u>قيساسألا تابلطتملا</u> <u>تابلطتملا</u> <u>ةمدختسملا تانوكملا</u> <u>قيساسأ تامولعم</u> <u>نى وك ت ل ا</u> <u>ةكېشلل يطيطختلا مسرلا</u> <u>AAA نېوكت AAA مايوكت</u> <u>WLAN ةكېش نيوكت</u> <u>ةساىسلا فيرعت فلم نيوكت</u> <u>ةسايسلا ةمالع نيوكت</u> <u>قساي سلامة مالع نيي عت</u> (ACL) لوصولا يف مكحتانا قمئاق نيوكت ميجوت قداعا HTTPS وأ HTTP ل ميجوتاا قداع نيكمت <u>ISE نېوكت</u> <u>(ISE) ةيوەلا فشك تامدخ كرحم ىل| 9800 WLC ةفاض|</u> <u>ISE ىلع دىدج مدختسم ءاشنا</u> <u>ضيوفتالا فيرعت فالم ءاشنا</u> <u>ةقداصملا ةدعاق نىوكت</u> <u>ققداصملا دعاوق نيوكت</u> طقف قيل حمل Flexconnect تال ديم عال ل وصول ا طاقين <u>تاداەش لا</u> <u>قحصاا نم ققحتاا</u> <u>اهحالصاو ءاطخألا فاشكتسا</u> <u>ققحتاا قمئاق</u> RADIUS ل ةمدخلا ذفنم معد <u> ءاطخألا جيحصت عيمجت</u> <u>ةلثمألا</u>

ةمدقملا

.ISE و 9800 WLC ةزافح ةدام ىلع CWA Wireless LAN لكشي نأ فيك ةقيثو اذه فصي

ةيساسألا تابلطتملا

تابلطتملا

دisco يكشت (WLC) مكحت زاهج lan يكلسال 9800 نم ةفرعم تنأ ىقلتي نأ يصوي.

ةمدختسملا تانوكملا

ةيلاتلا ةيداملا تانوكملاو جماربلا تارادصإ ىلإ دنتسملا اذه يف ةدراولا تامولعملا دنتست

- 9800 WLC رادصإلا Cisco IOS® XE Gibraltar جمانرب 17.6.x
- Identity Service Engine (ISE) v3.0

ةصاخ ةيلمعم ةئيب يف ةدوجوملا ةزهجألاا نم دنتسملا اذه يف ةدراولا تامولعملا ءاشنإ مت. تناك اذإ .(يضارتفا) حوسمم نيوكتب دنتسملا اذه يف ةمدختسُملا ةزهجألا عيمج تأدب رمأ يأل لمتحملا ريثأتلل كمهف نم دكأتف ،ليغشتلا ديق كتكبش.

ةيساسأ تامولعم

:لاثمك Apple زاهجل CWA ةيلمع ةيؤر كنكمي ثيح انه CWA ةيلمع ضرع متي



نيوكتلا

ةكبشلل يطيطختلا مسرلا



9800 WLC دلع AAA نيوكت

.9800 WLC نيوكت ىلإ ISE مداخ ةفاضإ .1 ةوطخلا

وہ امك RADIUS > Servers > + Add مداخ تامول عم لخدأو RADIUS > Servers > + Add مداخ تامول عم لخدأو RADIUS > Servers > + Add مداخ تامول عم لخدأو و

Q Search Menu Items	Configuration - > Security - > AAA
Dashboard	AAA Wizard Servers / Groups AAA Method List AAA Advanced
Monitoring >	
Configuration	+ Add × Delete
Administration	RADIUS Servers Server Groups
C Licensing	TACACS+ Name Y Address
X Troubleshooting	LDAP Id ■ 0 ► ► 10 ▼ items per page

عاونأ نم عون يأ وأ) ةيزكرملا بيولا ةقداصم مادختسال ططخت تنك اذإ (CoA)ضيوفتلا رييغت ةيلمع معد نيكمت نم دكأت للبقتسملا يف (CoA بلطتي نامألاا.

Create AAA Radius Server	·····			×
Name*	ISE-server	Support for CoA (i)	ENABLED	
Server Address*	10.00100-001	CoA Server Key Type	Clear Text	•
PAC Key	0	CoA Server Key (i)		
Кеу Туре	Clear Text 🔻	Confirm CoA Server Key		
Key* (i)		Automate Tester	D	
Confirm Key*				
Auth Port	1812			
Acct Port	1813			
Server Timeout (seconds)	1-1000			
Retry Count	0-100			
Cancel				Apply to Device



مداخ نيوكت دنع CoA مداخ حاتفم نيوكت نم اضيأ دكأت ،ثدجألا تارادصإلاو T7.4.x رادصإلاا يف :^{مَظ}حالم ايرايتخ! لكشي نأ وه ضرغلا .(ISE ىلع ريصقتلا سفن مه) كرتشملا رسلا لثم هسفن حاتفملا مدختسأ مداخ ماق ام وه اذه نوكي ن! كرتشملا حاتفملان نم CoA ل فلتخم حاتفم Cisco IOS XE 17.3، مداخ ماق ام وه اذه نوكي ن! كرتشمل حاتفملا نم CoA ل فلتخم حاتفم CoA. حاتفم لثم كرتشملا سفن ةطاسبب بيولا مدختسم قمجاو تمدختسأ

ليوختلا بيلاسأ ةمئاق ءاشنإ .2 ةوطخلا.

. قروصلا يف حضوم وه امك Configuration > Security > AAA > AAA Method List > Authorization > + Add كلإ لقتنا.

Q Search Menu Items	Authentication Authoriza	tion and Accounting
Dashboard	+ AAA Wizard	
Monitoring >	AAA Method List	Servers / Groups AAA Advanced
🔨 Configuration >	General	Add W Delete
() Administration >	Authentication	
X Troubleshooting	Authorization	Name v Type v Group Type v Group
	Accounting	default network local N/A

Quick Setup: AAA Authorization

Method List Name*	CWAauthz		
Type*	network	v	
Group Type	group	v	
Fallback to local			
Authenticated			
Available Server Groups	Assi	gned Server Groups	
ldap tacacs+	\rightarrow	radius	Ā
	<		<u> </u>
	>		~
	«		_ <u> </u>

ةروصلا يف حضوم وه امك ةبساحملا بيلاسأ ةمئاق ءاشنإب مق (يرايتخإ) .3 ةوطخلا.



کب ةصاخلاا RADIUS مداوخ (Cisco IOS XE نم رماوألاا رطس ةهجاو نيوكت نم) نزاوتت نأ تررق اذإ CWA لمعت ال :^{قظ}حالم نأ نم دكأت ،كلذ عمو .ةيجراخلاا لاامحألاا نزاوم مادختساب سأب ال .Cisco <u>CSCvh03827</u> نم ءاطخألاا حيحصت فرعم ببسب ذفنم ىلع دامتعالاا .ءاعدتسالاا قطحملاا فرعمل RADIUS قمس مادختساب ليمع لك ساسأ ىلع لمعي كيدل لمحلاا نزاوم UDP ردصم

اذإ ةديفم نوكت نأ نكمي يتلااو ،Call-station-id قمسك SSID مسا لاسرال AAA قسايس ديدحت كنكمي (يرايتخ|) .4 قوطخلا قيلمعلا يف اقحال ISE ىلع طرشلا اذه نم قدافتسالا ديرت تنك.

.ديدج جەن ءاشنإب مق وأ يضارتفالاا AAA جەن Configuration > Security > Wireless AAA Policy ىل| لقتنا



ناونع قاحلاٍ لازي ال ىعدتسملا ةطحملا فرعم ناف ،طقف SSID راتخت امدنع ىتح منأ ركذت .1 رايخك SSID رايتخالاا كنكمي MAC مساب لوصولا قطقنل SSID.

Edit Wireless AAA Policy

Policy Name*	default-aaa-policy
Option 1	SSID
Option 2	Not Configured 🔹
Option 3	Not Configured

WLAN ةكبش نيوكت

WLAN. ةكبش ءاشنإب مق .1 ةوطخلا

.ةجاحلا بسرح اەنيوكتو Configuration > Tags & Profiles > WLANs > + Add ةكبشلا ىل القتنا.



الخدأ .2 ةوطخل WLAN. تكبشل ةماعلا تامولعمل لخدأ .2 ةوطخل

Add WLAN			×
General Security	Advanced		
Profile Name*	cwa-ssid	Radio Policy (i)	
SSID*	cwa-ssid	Show slot configuration	
WLAN ID*	4	5 GHz	
Status		2.4 GHz	
Broadcast SSID	ENABLED	802.11b/g Policy 802.11b/g (2.4 GHz)	

ىل| طقف ةجاح كانه نوكت ،ةلاحلا هذه يف .ةبول طملا نامألا ةقيرط رتخاو بيوبتلا ةمالع Security ىل لقتنا .3 ةوطخلا (مسقلا AAA Configuration يف .2 ةوطخلا يف اهئاشناب تمق يتلا) AAA ضيوفت ةمئاقو 'MAC قيفصت'.

Add WLAN			×
General Security Advanc	ed		
Layer2 Layer3 AAA			
Layer 2 Security Mode	None	Lobby Admin Access	0
MAC Filtering		Fast Transition	Disabled v
OWE Transition Mode	0	Over the DS	
Authorization List*	CWAauthz 🔻 🤅	Reassociation Timeout	20

CLI:

#config t
(config)#wlan cwa-ssid 4 cwa-ssid
(config-wlan)#mac-filtering CWAauthz
(config-wlan)#no security ft adaptive

(config-wlan)#no security wpa (config-wlan)#no security wpa wpa2 (config-wlan)#no security wpa wpa2 ciphers aes (config-wlan)#no security wpa akm dot1x (config-wlan)#no shutdown

ةسايسلا فيرعت فلم نيوكت

لثم) ىرخألا تادادعإلا نيب نم ،VLAN ةكبش مەيدل نيذلا ءالمعلا صيصخت ررقت نأ كنكمي ،ةسايس فيرعت فلم لخاد (كلد ىلا امو ،تيقوتلا ةزەجأ ،Mobility Anchor) ةمدخلا ةدوج ،(ACLs) لوصولا يف مكحتلا ةمئاق).

.ديدج فيرعت فلم ءاشنإ وأ كب صاخلا يضارتفالا ةسايسلا فيرعت فلم مادختسا امإ كنكمي

GUI:

.ديدج Policy Profile ءاشنإ .1 ةوطخلا

.ديدج دحاو ءاشنإ default-policy-profile وأ نيوكتب مقو Configuration > Tags & Profiles > Policy ىل| لقتنا



فيرعتلا فلم نيكمت نم دكأت.

Ed	it Policy Profile					3
	Disabling a Policy or con	figuring it in 'Enabled' state, will	result in	loss of connectivity for clients	associated with	this Policy profile.
Ge	eneral Access Policies	QOS and AVC Mobili	ity	Advanced		
	Name*	default-policy-profile		WLAN Switching Police	су	
	Description	default policy profile		Central Switching	ENAE	3LED
	Status			Central Authentication	ENAE	3LED
	Passive Client	DISABLED		Central DHCP	ENAE	3LED
	Encrypted Traffic Analytics	DISABLED		Flex NAT/PAT		DISABLED
	CTS Policy					
	Inline Tagging	D				
	SGACL Enforcement	D				
	Default SGT	2-65519				

.VLAN لا ترتخأ .2 ةوطخلا

ال .ايودي VLAN فرعم بتكا وأ ةلدسنملا ةمئاقلا نم VLAN ةكبش مسا رتخاو بيوبتلا ةمالع Access Policies ىلإ لقتنا ةسايسلا فيرعت فلم يف (ACL) لوصولا يف مكحتلا ةمئاق نيوكتب مقت.

Edit Policy Profile									
Disabling a Policy or co	Disabling a Policy or configuring it in 'Enabled' state, will result in loss of connectivity for clients associated with this Policy profile.								
General Access Policies	QOS and AVC Mobility Advanced								
RADIUS Profiling	O	WLAN ACL							
HTTP TLV Caching		IPv4 ACL	Search or Select 👻						
DHCP TLV Caching	O	IPv6 ACL	Search or Select						
WLAN Local Profiling		URL Filters							
Global State of Device Classification	Disabled (i)	Pre Auth	Search or Select						
Local Subscriber Policy Name	Search or Select	Post Auth	Search or Select 🔹						
VLAN									
VLAN/VLAN Group	VLAN1416 🗸								
Multicast VLAN	Enter Multicast VLAN								

ةلاح) (CoA) ضيوفتلاا رييغتو (AAA زواجتب حامسلا) ISE تايطخت لوبقل ةسايسلا فيرعت فلم نيوكتب مق .3 ةوطخلا NAC). اًضيأ يرايتخا لكشب ةبساحم ةقيرط ديدحت كنكمي.

Edit Policy Profile

Disabling a Policy or co	nfiguring it in 'Enabled' state, will result in I	oss of connectivity for clier	nts associated with this Policy profile.
General Access Policies	QOS and AVC Mobility	Advanced	
WLAN Timeout		Fabric Profile	Search or Select
Session Timeout (sec)	1800	Link-Local Bridging	0
Idle Timeout (sec)	300	mDNS Service Policy	default-mdns-ser
Idle Threshold (bytes)	0	Hotspot Server	Search or Select 🚽
Client Exclusion Timeout (sec)	60	User Defined (Priva	te) Network
Guest LAN Session Timeout	0	Status	0
DHCP		Drop Unicast	0
IPv4 DHCP Required	0	DNS Layer Security	1
DHCP Server IP Address		DNS Layer Security Parameter Map	Not Configured Clear
AAA Policy		Flex DHCP Option for DNS	
Allow AAA Override		Flex DNS Traffic Redirect	IGNORE
NAC State		WLAN Flex Policy	
NAC Type	RADIUS	VLAN Central Switchi	ing 🖸
Policy Name	default-aaa-policy × 🔻	Split MAC ACL	Search or Select 🔹
Accounting List	CWAacct 🗸 (i) 🗙	Air Time Fairness P	olicies
WGB Parameters		2.4 GHz Policy	Search or Select 🗸
Broadcast Tagging		5 GHz Policy	Search or Select
WGB VLAN	0	EoGRE Tunnel Profi	les
Policy Proxy Settings		Tunnel Profile	Search or Select
ARP Proxy	DISABLED		

IPv6 Proxy

None

•

config # wireless profile policy <policy-profile-name> # aaa-override
nac
vlan <vlan-id_or_vlan-name>
accounting-list <acct-list>

no shutdown

ةسايسلا ةمالع نيوكت

ةمالع ءاشنإ امإ كنكمي .كب صاخلا ةسايسلا فيرعت فلمب SSID طبرب هيف موقت يذلا ناكملا وه ةسايسلا ةمالع لخاد ةيضارتفالا ةسايسلا ةمالع مادختسا وأ ةديدج ةسايس.

GUI:

.ةروصلا يف حضوم وه امك رمألا مزل اذإ اديدج ادحاو فضأو Configuration > Tags & Profiles > Tags > Policy ىلإ لقتنا

Со	nfigu	uration •	> Tags &	Profiles > Tags]			
Po	licy	Site	RF	AP				
	+	Add						
		Policy Tag	g Name				Ŧ	Description
		default-po	olicy-tag					default policy-tag
		local-site-	-policy-tag					
	M	۰ 1		10 🔻 items per	page			

.بولطملا ةسايسلا فيرعت فلمب WLAN فيرعت فلم طبرب مق

Add Policy Tag				×
Name*	cwa-policy-tag			
Description	Enter Description			
V WLAN-POLIC	Y Maps: 1			
+ Add × De	ete			
WLAN Profile		T	Policy Profile	Т
Cwa-ssid			default-policy-profile	
	10 🔻 items per page			1 - 1 of 1 items
RLAN-POLIC	/ Maps: 0			
Cancel				Apply to Device

CLI:

config t # wireless tag policy <policy-tag-name> # wlan <profile-name> policy <policy-profile-name>

ةسايسلا ةمالع نييعت

ةبولطملا لوصولا طاقنل ةسايسلا ةمالع نييعتب مق.

GUI:

مقو ،Configuration > Wireless > Access Points > AP Name > General Tags كل لقت نا ،ةدجاو لوصو قطقن ىل قمالعلا نييعتل رقنا مث ،ةبول طملا قمهملا نييعتب Update & Apply to Device.

General Interfaces High Availability Inventory ICap Advanced Support Bundle	
General Tags	
AP Name* ▲ Changing Tags will cause the AP to momentarily los association with the Controller. Writing Tag Config to AF not allowed while changing Tags.	se P is
Base Radio MAC	
Ethernet MAC cwa-policy-tag	•
Admin Status Site default-site-tag	•
AP Mode Local	•
Operation Status Registered Write Tag Config to AP	

ا قكبشلا يف مكحتلا رصنع عم اهطابترا دقفت اهنإف ،لوصو قطقن ىلع قسايسلا قمالع رييغت دعب هنأ ملعا :**نظح**لم ابيرقت قدحاو ققيقد نوضغ يف مامضنالل عجرتو 9800 زارط (WLC) ةيكلساللاا قيلحملا

ىك تنا ،قددعتم لوصو طاقن ىل جەنلا قمالع سەن نييعتل Configuration > Wireless > Wireless Setup > Advanced > Start Now.



Configuration • > Wireless Setup • > Advanced	d Show M	le How 📀								
« Start	+ Tag APs Number of APs: 2									
Tags & Profiles	Selected Number	of APs: 2								
🚯 WLAN Profile 🔠 +-	AP T Name	AP T Model		Serial Y Number	AP T Mode	Admin Y Status	Operation Y Status	Policy Y Tag	Site T ag	RF Tag
Policy Profile		AIR- AP1815I- E-K9	****	-	Flex	Disabled	Registered	local- site- policy-tag	flex- site-tag	defa rf-ta
● Policy Tag ● III +		AIR- AP1815I- E-K9	-		Local	Enabled	Registered	default- policy-tag	default- site-tag	defa rf-ta
AP Join Profile H	R 4 1	▶ ►	10 🔻 items per	page				1 - 2 c	of 2 items	¢
 Policy Tag		AIR- AP1815I- E-K9	10 y items per	page	Local	Enabled	Registered	default- policy-tag 1 - 2 c	default- site-tag	defa rf-ta

. قروصلا يف حضوم وه امك Save & Apply to Device رقناو ضيبألا نوللا تاذ زييمتلا قمالع رتخأ.

ľ	Tag APs		×
	Tags		
	Policy	cwa-policy-tag	
	Site	Search or Select 🔻	
	RF	Search or Select	
	Changing AP Tag connected client	g(s) will cause associated AP(s) to rejoin and disrupt (s)	
	Cancel	Apply to Devi	ce

CLI:

(ACL) لوصولا يف مكحتلا ةمئاق نيوكت هيجوت ةداعإ

.ةديدج (ACL) لوصولا يف مكحت ةمئاق ءاشنإل Configuration > Security > ACL > + Add لوصولا يف مكحت المئات المعالي المحتان.

يف حضوم وه امك لسلستك ةدعاق لك فيضتو بتكت IPv4 Extended اهل عجو ،(ACL) لوصول اب مكحتال ةمئاقل مسا رتخأ ةروصلا

Add ACL Setup				x
ACL Name*	REDIRECT	ACL Type	IPv4 Extended	
Rules				
Sequence*	1	Action	deny	
Source Type	any 🔻			
Destination Type	Host 🗸	Host Name*	<ise-ip></ise-ip>	is field is mandatory
Protocol	ip v			
Log		DSCP	None	
+ Add × Delete				
Sequence v Action v	Source × Source × Wildcard	Destination v Destination v IP Wildcard	Protocol v Port Port	tion × DSCP × Log ×
I 0 F F 10) 🔻 items per page			No items to display
Cancel				

مكحتلا ةمىناق .يقابلاب حامسلاو DNS ضفر كلذكو ISE كرحمل (PSN) ةسايسلا ةمدخ دقُع ىلا رورملا ةكرح ضفر ىل إجاتحت ىل لوصولا يف مكحت ةمئاق اەنكلو قينمأ (ACL) لوصولا يف مكحت ةمئاق تسيل ەذە اەەيجوت داعملا (ACL) لوصولا يف ةداع لثم) قجلاعملا نم ديزمل (صيخارتلا ىلع) قيزكرملا قجلاعملا قدحو ىل لقتنت يتلا رورملا قكرح ددحت يتلا ةطقنلا .ويجوتلا

: (لاثملا اذه يف كب صاخلا IP ناونعب 10.48.39.28 لدبتسا) يلي امك (ACL) لوصولاا يف مكحتلا ةمئاق ودبت نأ بجي

	Sequence ~	Action ~	Source v IP	Source v Wildcard	Destination ~ IP	Destination ~ Wildcard	Protocol 🗸	Source ~ Port	Destination ~ Port	DSCP v	Log ~
	10	deny	any		10.48.39.28 ip		ip	q			Disabled
	20	deny	10.48.39.28		any		ip			None	Disabled
	30	deny	any		any		udp		eq domain	None	Disabled
	40	deny	any		any		udp eq domain			None	Disabled
	50	permit	any		any		tcp		eq www	None	Disabled
M	≪ 1 >	▶ 10	▼ items per p	bage						1 - 5 of 5	5 items

ن صفرلل هيجوت قداع| عارج|ل| deny ربتعا ،هيجوتلا قداع|ب قصاخلا (ACL) لوصولا يف مكحتلا قمئاقل قبسنلاب :**نظح**الم قيلحملا قكبشلا يف مكحتلا رصنع رظنت .اهب حومسملا هيجوتلا قداع| وه عارج|لاواpermit (رورملا قكرح ضفر مدع) (يضارتفا لكشب 443 و 80 ذفانملا) هيجوتلا قداع| اهنكمي يتلا رورملا قكرح يف طقف (WLC) ةيكلساللاا. ip access-list extended REDIRECT deny ip any host <ISE-IP> deny ip host<ISE-IP> any deny udp any any eq domain deny udp any eq domain any permit tcp any any eq 80

.ISE مداخ ىلإ طقف 8443 فيضلا ذفنم ضفرل ءارجإلا لالخ نم (ACL) لوصولا يف مكحتلا ةمئاق نيسحت كنكمي

HTTPS وأ HTTP ل هيجوتلا ةداعإ نيكمت

،كلذل .ەيجوتلاا ةداعإل 80 ذفنملاا ىلع عمتسي نأ بجيو بيولاا ةقداصم لخدم نيوكتب بيولاا لوؤسم لخدم نيوكت طبر متي ip http مرالاا مادختساب) ماع لكشب ەنيكمت رايتخإ امإ كنكمي .حيحص لكشب ەيجوتلاا قداعإ لمعت ىتح HTTP نيكمت بجي server) قطيرخ لفسأ webauth-http-enable رمألاا مادختساب) طقف بيولاا ققداصمل ةيطمنلاا قدحولل HTTP نيكمت كنكمي وأ (قملعملا).



ل وه نأ امب .FlexConnect ل يلحمل ليوحتلا قلاح يف ىتح ،CAPWAP لخاد HTTP رورم ةكرح هيجوت ةداعإ ثدحت :قلّحالم WLC لا نم redirection لا ملتسيو قفن capwap لا لخاد طبر (HTTP(s) ل لسري ap لا ،ضارتعالا لمعب موقي WLC يف فلخلا

لفسأ intercept-https-enableرمألاا ةفاضإب مقف ،HTTPS ل URL ناونع ىلإ لوصولا ةلواحم دنع ميجوتلا ةداعإ يف بغرت تنك اذإ يف مكحتلا ةدحوب ةصاخلا ةيزكرملا ةجلاعملا ةدحو ىلع رثؤي منأو ،لثمألا نيوكتلا سيل اذه نأ ظحال نكلو ةملعملا ةطيرخ لاح ةيأ ىلع ةداهشلا يف ءاطخأ دلويو (WLC) ةيكلساللا قيلحملا ةكبشلا.

<#root>

parameter-map type webauth global

type webauth

intercept-https-enable

trustpoint xxxxx

أطيرخ ةملعملا يف قيقدت'HTTPS ضرتعي Web Auth رايخلا عم iu ل ربع كلذ تلعف اضيأ عيطتسي تنأ (Configuration > Security > Web Auth).

O Search Menu Items	Con	Configuration • > Security • > Web Auth				> V	Veb Auth	Edit Web Auth Parameter					
C Ocaron Menta Renis		Add			•				Maximum HTTP connections	100			
Dashboard									Init-State Timeout(secs)	120			
	-	Parame	ter Ma	ap Nam	e				Turne	webauth	_		
	U	global					1		Туре	Webauti	•		
Configuration >	1	1	F	H	10	•	items per page	9	Virtual IPv4 Address				
Administration									Trustpoint	Select	•		
C Licensing									Virtual IPv6 Address	XIXIXIX			
<u> </u>									Web Auth intercept HTTPs	0			
X Iroubleshooting									Captive Bypass Portal	0			



ةجاح كانه تناك اذإ ،هيجوتـلا ةداعا قيلمع عدبـل HTTP بـيو عقوم تاضرعتسمـلا مدختست ،يضارتفا لكشب :**نظح**ائم منأل نيوكـتـلا اذهب ىصوي ال ،كـلـذ عمو ؛HTTPS بـيولـا ققـداصم ضارتعا نم قـقحتـلا بـجيف ،HTTPS هيجوت ةداعا ىلاً .قيزكرملاً قجـلاعمـلاً قدحو مادختساٍ نم ديزي

ISE نيوكت

(ISE) ةيوەلا فشك تامدخ كرحم ىلإ WLC ةفاضإ

يف حضوم وہ امك ISE اهيل| لقتناو Administration > Network Resources > Network Devices > Add اميل| لقتناو ISE مكحت قدحو حتفا. قروصلا

■ Cisco ISE	Administration • Network Resources	🛕 Evaluation Mode 85 Days Q 🕜 🕫 🚳
Network Devices	Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences	NAC Managers More \sim
Network Devices Default Device	Network Devices	
Device Security Settings	🖉 Edit 🕂 Add 🚺 Duplicate 🕁 Import 🛧 Export 🗸 🔒 Generate PAC 🌘 Delete 🗸	Selected 0 Total 1 🔗 🗔
	Name \wedge IP/Mask Profile Name Location Type	Description
	9800-WLC 10.48.38.86/ 🇰 Cisco 🕕 All Locations All Device Types	

.ةكبشلا زاهج نيوكتب مق .2 ةوطخلا

ىل| ادانتسا ةكبشلا ةزەجأ تاعومجم نييعتو ،ددحم فصو وأ جمانرب رادص| وأ ددحم زارط مسا نوكي نأ نكمي ،يرايتخإ لكشبو قيكلساللا ةيلحملا ةكبشلا يف مكحتلا تاودأ وأ عقوملا وأ ةزەجألاا عاونأ (WLC).

يف حضوم وه امك ةرادإلا ةمجاو يه نوكت ،يضارتفا لكشب .ةقداصملا تابلط لسرت يتلا WLC ةمجاو انه IP ناونع لثامي ةروصلا

■ Cisco ISE	Administration - Network Resources	🛦 Evaluation Mode 24 Days Q 🕥 균 🕸
Network Devices	Network Device Groups Network Device Profiles External RADIUS Servers RADIUS Server Sequences	NAC Managers More \vee
Network Devices	Network Devices List > nschyns-WLC	
Device Security Settings	* Name WLC	
	IP Address V * IP : / 32	
	Model Name Software Version Network Device Group	
	Location All Locations V Set To Default IPSEC No V Device Type All Device Types V Set To Default Set To Default	
	RADIUS Authentication Settings RADIUS UDP Settings Protocol RADIUS	
	* Shared Secret Show	

.<u>ةكبشلا ةزمجأ تاعومجم - ISE</u> :ةكبشلا ةزمجأ ةرادا :ISE ةرادا ليلد لصف عجار ،ةكبشلا ةزمجأ تاعومجم لوح تامولعملا نم ديزمل

ISE ىلع ديدج مدختسم ءاشنإ

. قوطخلا Administration > Identity Management > Identities > Users > Add القتنا.

E Cisco ISE	Administration • Identity Management	🛦 Evaluation Mode 85 Days Q 🕜 🕫 🚭
Identities Groups	External Identity Sources Identity Source Sequences Settings	
Users Latest Manual Network Scan Res	Network Access Users	Selected 0 Total 0 🧭 🔕
	🖉 Edit 🕂 Add 🛞 Change Status 💛 🕁 Import 🏠 Export 🗸 🌘 Delete 💛 🌔 Duplicate	all \sim $~$ ∇
	Status Name Description First Name Last Name Email Address	User Identity Grou Ad
	No data available	

.تامولعملا لخدأ .2 ةوطخلا

حضوم وه امك ،ةجاحلا بسح اهطبض نكمي نكلو ALL_ACCOUNTS ىمست ةعومجم ىلإ مدختسملا اذه يمتني ،لاثملا اذه يف .ةروصلا يف

=	Cisco	ISE		Administration · Identity	Management		Evaluation Mode 85 Days	Q	0	R	ø
Ider	tities	Groups	External Identity Sources	Identity Source Sequences	Settings						
Users Latest N	lanual Netw	ork Scan Res	Network Access Users Lis	t > New Network Access User							
Latest M	lanual Netw	Scan Res	 Network Access Name user1 Status Enable Email Passwords Password Type: Ir Login Password Login Password User Informat Account Optic Account Disal User Groups ALL_ACCOUND 	ss User	Re-Enter Password	Generate Passwo	rd () rd ()				

ضيوفتلا فيرعت فلم ءاشنإ

دامتعالاا تانايبو MAC ناونع لثم) هب ةصاخلا تاملعملا ىلإ ادانتسا ليمعل ةنيعملا ةجيتنلا وه جهنلا فيرعت فلم (VLAN) ةيرهاظلا ةيلحملا ةقطنملا الله عن شكر منادادع! نييعت منكمي .(كلذ ىلإ امو ةمدختسملا WLAN قكبشو .كلذ ىلإ امو (URL) دحوملا دراوملا عقوم ددحم هيجوت ةداعإو (ACL) لوصولا يف مكحتلا مئاوقو

مسا ليدعتل ەريرحت كنكمي نآلاا .لعفلاب Cisco_Webauth ضيوفت ةجيتن دجوت ،ISE نم ةثيدحلا تارادصإلاا يف ەنأ ظحال عال عنيوكتب تمق ام ةقباطمل ميجوتال ةداعإل (ACL) لوصولا يف مكحتال ةمئاق

		Polic	cy · Policy Elements	A Evaluation Mode 24 Days	2 0 50 4					
Dictionaries Condit	tions	Results								
Authentication	>	Standard Authoriza	ation Profiles							
Authorization Authorization Profiles	~	For Policy Export go to Administration > System > Backup & Restore > Policy Export Page Selected 0 Total 11 😥 🝕								
Downloadable ACLs		🖉 Edit 🕂 Add 📋 Duplicate 🕴	Delete		All \sim					
Profiling	>	Name	Profile							
Desture		Blackhole_Wireless_Access	👬 Cisco 🕕	Default profile used to blacklist wireless devices. Ensure	a that you config					
Posture	/	Cisco_IP_Phones	ដ Cisco ()	Default profile used for Cisco Phones.						
Client Provisioning	>	Cisco_Temporal_Onboard	ដ Cisco 🥡	Onboard the device with Cisco temporal agent						
		Cisco_WebAuth	🗰 Cisco 🕧	Default Profile used to redirect users to the CWA portal.						

ىلع ەنپوكت مت پذلا ەسفن وە (ACL) لوصولاا يف مكحتلا ةمئاق مسا نأ نم دكأت .ەيچوتلا ةداعإ تامولعم لخدأ .2 ةوطخلا 9800. زارط (WLC) ةيكلساللا قيلحملا ةكبشلا يف مكحتلا رصنع

■ Cisco ISE		Policy · Policy Elements	Evaluation Mode 24 Days	Q (0 59	0
Dictionaries Condit	tions Results					
Authentication	Authorization Profiles Authorization Pr	Cisco_WebAuth ofile				
Authorization Profiles	* Name	Cisco_WebAuth				
Downloadable ACLs	Description	Default Profile used to redirect users to the CWA portal.				
Profiling	> * Access Type	ACCESS_ACCEPT ~				
Posture	> Network Device Profi	e ⇔aCisco ∨⊕				
Client Provisioning	> Service Template					
	Track Movement					
	Agentless Posture					
	Passive Identity Tracl	ing 🗌 🕕				
	Common Tas Web Redirectio Centralized Web Display Certifit Message Static IP/Host	KS (CWA, MDM, NSP, CPP) () with V ACL REDIRECT Value Self-Registered Guest Portal (c v ates Renewal				8

ةقداصملا ةدعاق نيوكت

قوف رقنا ،Policy > Policy Sets ىل القتنا ،ةدجاو ءاشنإل .ضيوفتلاو ةقداصملا دعاوق نم ةعومجم جەنلا ةعومجم ددحت .1 ةوطخلا جەنلا ةعومجم رايتخال نيميلا ىلع دوجوملا قرزالا مەسلا رتخأ مث Insert new row ةمئاقلا يف جەن ةعومجم لوأ نييعت ةمالع .ةيضارتفالا

E Cisco ISE	Policy · Policy Sets	▲ Evaluation Mode 24 Days Q ⑦ ₅@ ۞
Policy Sets		Reset Policyset Hitcounts Save
Status Policy Set Name Description	Conditions	Allowed Protocols / Server Sequence Hits Actions View
Q Search		
	+	
Oefault Default policy set		Default Network Access 🗷 >+ 70 🔅 🕨

ترتخاو ،Options تددم ،(يكلسال وأ يكلس MAB ىلع ققباطم) MAB ةدعاقلل .Authenticationجەنلا عيسوت .2 قوطخلا رايخلا.

\sim Authentication Policy (3)								
(+) S	itatus R	tule Name	Cond	itions	Use	Hits	Actions	
Q	Search							
	O N	МАВ	OR	Wired_MAB Wireless_MAB	Internal Endpoints (X) ~ ~ Options If Auth fail REJECT (X) ~ If User not found CONTINUE (X) ~ If Process fail DROP (X) ~	0	¢\$	

.تارييغتلا ظفحل Save قوف رقنا .3 ةوطخلا

ةقداصملا دعاوق نيوكت

ىلع اەقيبطت متي يتلا (ضيوفت فيرعت فلم يأ) تانوذألا ةجيتن يأ ديدحتل ةلوؤسملا ةدعاقلا يە ضيوفتلا ةدعاق ليمعلا

يف حضوم وه امك Authorziation Policy عسوتالاو Authentication Policy قالغإب مق ،جەنالا ةعومجم ةحفص سفن يف 1. ةوطخلا .

Policy Sets-	→ Default				Reset	Reset Policyset Hitcounts	Save		
Status	Policy Set Name	Description	Conditions			Allowed Protocols / Server Sequence	Hits		
Q Searc	h								
۲	Default	Default policy set				Default Network Access 🛛 🖂 +	70		
> Authentica	tion Policy (3)								
> Authorization Policy - Local Exceptions									
> Authorization Policy - Global Exceptions									
\vee Authorizat	on Policy (13)								

عم ابلاغ قباطتت يتلاو Wifi_Redirect_to_Guest_Loginىمست اقبسم اەؤاشن| مت ةدعاقب ةريخألاا ISE تارادص| أدبت .2 ةوطخلا علامات المال عندوجومل ايدامرلا قمالع ليغشتب مق انتاجايتحإ enable.

Wi- Fi_Redirect_to_Guest_Login Image: Wireless_MAB Cisco_WebAuth × + Select from list > +	• {ố}
--	-------

فافتلاا ةفاضإ ايرايتخإ كنكمي ،نآلاا .CWA ميجوت ةداعإ تامس عجرتو طقف Wireless_MAB عم ةدعاقلاا هذه قباطتت .3 ةوطخلا طرش ةفاض|ب مق .Sudio طرشلا راهظال (نآلاا نم ارابتعا Wireless_MAB) طرشلا رتخأ .طقف ددحملا SSID قباطي ملعجو ريغص قيقدتلاب مق .كب صاخلا SSID مسا عم قباطتي ملعجا .Called-Station-ID قمسلا مادختساب سوماقلا Radius رتخاو نيميلا يل .قروصلا يف حضوم وه امك قشاشلا لفسأب دوجوملا يه لاهد تساب

Conditions Studio				
Library	Editor			
Search by Name		E Wirele	ess_MAB	$^{\otimes}$
			Radius-Called-Station-ID	\otimes
BYOD_is_Registered		무	Contains 🗸 cwa-ssid	
Catalyst_Switch_Local_Web_Aut	ANDV			
Compliance_Unknown_Devices				
Compliant_Devices		Set to 'Is i	not'	Duplicate Save
E MAC_in_SAN				
				Close

ىلا لوصول ليصافت عاجرال طرشلا Guest Flow قباطت ،ىلعأ ةيولوأب اهفيرعت متي ،ةيناث ةدعاق ىلا نآلا جاتحت .4 ةوطخلا اضيأ اقبسم اهؤاشنا متي Wifi Guest Accessيتلا ةدعاقل مادختسا كنكمي .لخدملا ىلع مدختسملا ةقداصم درجمب ةكبشلا .راسيلا ىلع عارضخ ةمالع عضوب ةدعاقلا نيكمت طقف ٍذئنيح كيلع نوكيس .قريخالا ISE تارادصا ىلع يضارتفا لكشب .ققد رثكألا لوصولا قمئاق دويق نيوكت وأ يضارتفالا PermitAccess عاجرا كنكمي

۲	Wi-Fi_Guest_Access	AND		Guest_Flow Wireless_MAB	PermitAccess ×	~+	Guests	<u> </u>	0	錼
	Wi		-	Wireless_MAB						
0	Fi_Redirect_to_Guest_Login	AND	₽	Radius-Called-Station-ID CONTAINS cwa-ssid	Cisco_WebAuth ×	+	Select from list	+	0	\$ <u>\$</u> }

.دعاوقلا ظفحب مق .5 ةوطخلا

طقف ةيلحملا Flexconnect تالدبم ىلإ لوصولا طاقن

عمو .ةحلاص لازت ال ةقباسلا ماسقألاا ؟ةيلحملا Flexconnect تالدبم ىلإ لوصولا طاقنو WLAN تاكبش كيدل تناك ول اذام (AP) لوصولا طاقن ىلإ ميجوتلا ةداعإل (ACL) لوصولا يف مكحتلا ةمئاق عفد لجأ نم ةيفاضإ ةوطخ ىلإ ةجاحب تنأف ،كلذ اقبسم.

بيوبتلا ةمالع Policy ACL ىل لقتنا ،كلذ دعب .Flex فيرعت فلم رتخاو Configuration > Tags & Profiles > Flex ىل لقتنا.

.ةروصلا يف حضوم وه امك Add رقنا

Edit Flex Profile									
General	Local Au	thentication	Policy ACL	VLAN	DNS Layer Se	curity			
+ Add				•					
ACL Name		▼ Ce	ntral Web Auth	▼ URL Filter	T				
H 4 0		10 🗸 items p	ber page	No items to	o display				

رايتخالاا ةناخ سكعي .بيولل ةيزكرملا ةقداصملا نيكمتب مقو مهيجوت داعملا (ACL) لوصولاا يف مكحتلا ةمئاق مسا رتخأ ةداعاب مقت ال' ينعت 'deny' قرابع نأل كلذو) امسفن لوصولا قطقن ىلع ايئاقلت (ACL) لوصولا يف مكحتلا ةمئاق مذه "ضفرلا" نايب نأ ريغ Cisco IOS XE. يف (WLC) ةيكلساللا ةيلحملا قكبشلا يف مكحتلا رصنع ىلع 'IP اذه ىلا ميجوتلا امدنع امضفرو حيراصتلا عيمج ليدبتب ايئاقلت موقت مذه رايتخالا ةناخ ناف ،اذل .سرب دتيشوسألا ىلع سكعلا ينعي قطقنل (CII) قطق مل من عنه العنه من المدنع الما يف مكحتلا مي الما يف مكحتلا مي من العامي المدنع امدنع امضفرو حيراصتلا عيمج ليدبتب ايئاقلت موقت منه رايتخالا قناخ ناف ،اذل .سرب دتيشوسألا ىل ع سكعلا ينعي قطقنل (CII) في من الما يفي الما موقت منه ما يتخالا المناح الما الما الما الما الما الما موقت المونا الما من من من من من الما موقت من الما موقت من ما من الما مي الما مي ما ما الما ما من ما ما مول الما ما م ومولا مولا مول (ACL).

Update and apply to the device. برضت نأ سنت ال

Edit Flex Profile		
General Local Authentication Policy ACL	VLAN	DNS Layer Security
+ Add × Delete		
ACL Name	▼ URL Filter	r T
I I I V Items per page	No items to	to display ACL Name* REDIRECT V
		Central Web Auth
		URL Filter Search or Select 🔻
		✓ Save

تاداەشلا

ةحصلا نم ققحتلا

.يلاحلا نيوكتلا نم ققحتلل رماوألا هذه مادختسا كنكمي

<#root>

- # show run wlan # show run aaa # show aaa servers # show ap config general # show ap name <ap-name> config general
- # show ap tag summary
- # show ap name <AP-name> tag detail
- # show wlan { summary | id | nme | all }
- # show wireless tag policy detailed <policy-tag-name>
- # show wireless profile policy detailed <policy-profile-name>

لاتملا اذه لثامي يذلا (WLC) ةيكلساللا ةيلحملا ةكبشلا يف مكحتلا رصنع نيوكت نم ةلصلا وذ ءزجلا انه:

<#root>

aaa new-model ! aaa authorization network CWAauthz group radius aaa accounting identity CWAacct start-stop group radius ! aaa server radius dynamic-author client <ISE mac-filtering CWAauthz no security ft adaptive no security wpa no security wpa wpa2 no security wpa wpa2 ciphers aes no security wpa akm dot1x no shutdown ip http server (or "webauth-http-enable" under the parameter map) ip http secure-server اهحالصإو ءاطخألا فاشكتسا

ققحتلا ةمئاق

• ديلع هلوصحو حلاص IP ناونعو ليمعلاا لاصتا نم دكأت.

ليبس ىلع .يئاوشع IP ناونع مادختسإ لواحو ضرعتسملا حتفاف ،ةيئاقلت ەيجوتلا ةداعإ ةيلمع نكت مل اذا . DNS مداخ رفوت نم ققحت .DNS لح يف ةلكشم كيدل نوكت نأ لمتحملا نمف ،هيجوتلا قداعا تلمع اذا .10.0.01 ،لاثملا فيضملا عامساً لح يلع متردق نمو DHCP ربع كيدل حلاص.

• لخدم نيوكت طبر متي .لمعلى HTTP ىلع ميجوتلا ةداعإل منيوكت مت يذلا ip http server رمألاا كيدل نأ نم دكأت منيكمت رايتخإ امإ كنكمي .ميجوتلا قداعإل 80 ذفنملا ىلع مجاردا بجيو بيولا ققداصم لخدم نيوكتب بيولا لوؤسم مادختساب) طقف بيولا ققداصمل ةيطمنلا قدحولل HTTP نيكمت كنكمي وأ (ip http serverرمألا مادختساب) ماع لكشب رمألا.

• ل URL ل نا نم كلذ دعب ققحتف ،بول طم وهو URL ل URL ناونع ىل لوصول ا قلواحم دنع كهيجوت قداع متت مل اذا تامل عمل ا قطيرخ لفسأ intercept-https-enable رمأل ا:

<#root>

parameter-map type webauth global type webauth

intercept-https-enable

trustpoint xxxxx

:ةطيرخ ةملعملا يف تصحف 'HTTPS ضرتعي Web Auth رايخلا ىقلتت تنأ نأ gui لا قيرط نع تصحف اضيأ عيطتسي تنأ

Q. Search Menu Items	Con	figuratio	n•>	Secu	urity • >	Web Aut	i.	Edit Web Auth Parameter	
			×		e			Maximum HTTP connections	100
🚃 Dashboard		Decem	ator M	an Nam				Init-State Timeout(secs)	120
Monitoring		global			6		<	Туре	webauth 🗸
Configuration	14		F		10	✓ items per	page	Virtual IPv4 Address	
() Administration >								Trustpoint	Select 🔻
© Licensing								Virtual IPv6 Address	XIXIXIX
								Web Auth intercept HTTPs	
Noubleshooting								Captive Bypass Portal	O

RADIUS ل ةمدخلا ذفنم معد

تيكلساللا مكحتال قدحو يوتحت Cisco Catalyst 9800 Series مساب هيلإ راشي ةمدخ ذفنم ىلع Cisco Catalyst 9800 Series ميال ا مكحتال قدحو يوتحت معد متي ،17.6.1 رادصإلا نم (CoA) معد متي ،17.6.1 معد متي ،17.6.1 معد متي ،17.6.1 معد متي ،17.6.1 معد متي ،17.6

:نيوكتلا اذه ىل| ةجاحب تنأف ،RADIUS ل ةمدخلا ذفنم مادختس| يف بغرت تنك اذا

<#root>

aaa server radius dynamic-author client 10.48.39.28

vrf Mgmt-intf

server-key cisco123

interface GigabitEthernet0

vrf forwarding Mgmt-intf

ip address x.x.x.x x.x.x.x

!if using aaa group server: aaa group server radius group-name server name nicoISE

ip vrf forwarding Mgmt-intf

ip radius source-interface GigabitEthernet0

ءاطخألا حيحصت عيمجت

اهثودح دعب لشف ةلااح وأ ةثداحب ةصاخلا تالجسلا ضرع كنكمي امك ،رمتسم لكشب راعشإلا ىوتسم.

اهؤاشن| مت يتلا تالجسلا مجح ىلع دمتعت اەنكلو تالجسلا يف مايأ ةدع ىلا تاعاس عضب عوجرلا كنكمي :🗃 🕪

يربع لاصتالا كنكمي ،يضارتفا لكشب 9800 WLC قطساوب اهعيمجت مت يتلا تاراسملا ضرعل SSH/Telnet ب 9800 WLC ربع لاصتال (يصن فلم ىلا قسلجلا ليجست نم دكأت) تاوطخلا هذه ءارجاو).

. ثدح رادصإلا امدنع back to تقولاا يف لجسلا تعبتت عيطتسي تنأ كلذل تقو يلاح WLC لا تصحف 1. ةوطخلا

<#root>

show clock

كلذ رفوي .ماظنلا نيوكت ةطساوب ددحم وه امك يجراخلا syslog وأ WLC ل تقوملا نزخملا نم syslog عيمجتب مق .2 ةوطخلا تدجو نإ ءاطخالاو ماظنلا قمالسل ةعيرس ضرع ةقيرط.

<#root>

show logging

.ءاطخأ حيحصت طورش يأ نيكمت مت اذإ ام قوّحت .3 ةوطخلا

<#root>

show debugging Cisco IOS XE Conditional Debug Configs: Conditional Debug Global State: Stop Cisco IOS XE Packet Tracing Configs: Packet Infra d

راعشإلاا ىوتسم راثآ عيمجتب مق ،.3 ةوطخلا يف طرشك مجاردا متي مل رابتخالا تحت MAC ناونع نأ ضارتفاب .4 ةوطخلا ددحملا MAC ناونعل امئاد ةدوجوملا # show logging profile wireless filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file always-on-<FILENAME.txt>

.يچراخ TFTP مداخ ىلإ فلملا خسن كنكمي وأ ةسلجلا ىلع ىوتحملا ضرع امإ كنكمي

<#root>

more bootflash:always-on-<FILENAME.txt>
or
copy bootflash:always-on-<FILENAME.txt> tftp://a.b.c.d/path/always-on-<FILENAME.txt>

يلكلس اللااطش نلاعبت الويطرش لاحي حصت لا

ءاطخألاا حيحصت نيكمت كنكمي ،قيقرحتلا ديق ةلكشملا لغشم ديدحتل ةيفاك تامولعم ةمئادلا تاراسملا كحنمت مل اذا عم لعافتت يتلا تايلمعلا عيمجل ءاطخألاا حيحصت ىوتسم عبتت رفوي يذلا ،(RA) Radio Active عبتت طاقتلاو طورشملا .تاوطخلا هذه يف رمتسا ،طورشملا ءاطخألا حيحصت نيكمتل .(قلاحلا هذه يف ليمعلل MAC ناونع) ددحملا طرشلا

.ءاطخألا حيحصت طورش نيكمت مدع نم دكأت .5 ةوطخلا

<#root>

clear platform condition all

.هتبقارم ديرت يذلا يكلساللا ليمعلل MAC ناونعل ءاطخألا حيحصت طرش نيكمتب مق .6 ةوطخلا

اًيرايتخا تقولا اذه ةدايز كنكمي .(ةيناث 1800) ةقيقد 30 ةدمل رفوتملا mac ناونع ةبقارمب رماوألا هذه أدبت .قيناث 2085978494 يتح

<#root>

debug wireless mac <aaaa.bbbb.cccc> {monitor-time <seconds>}

💊 ناونع لكل<debug wireless mac<aaaa.bbbb.cccc رمألا ليغشتب مق ،ةرم لك يف دحاو ليمع نم رثكأ ةبقارم لجأ نم :ظطلم

.اقحال ەضرعل ايلخاد اتقۇم ءيش لك نيزخت متي ثيح ،ةيفرطلا لمعلا ةسلج ىلع ليمعلا طاشن جارخإ ىرت ال :💐 🕪

ەتبقارم ديرت يذلا كولسلا وأ ةلكشملا جاتنا ةداعإب مق .'7 ةوطخلا.

.نوكملا وأ يضارتفالاا ةبقارملاا تقو ءاهتنا لبق ةلكشملا خسن مت اذإ ءاطخألا حيحصت فاقيإب مق .8 ةوطخلا

<#root>

no debug wireless mac <aaaa.bbbb.cccc>

:مسإلا عم يلحم دربم دلي WLC WLC لا ،نوكي يكلسال debug لا وأ بردملا تقو ىضقنا نإ ام

ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log

ىلع ةرشابم اەضرع وأ يڃراخ مداخ ىلا تاجرخملra trace .log خسن اما كنكمي .MAC ناونع طاشن فلم عيمجت .9 ةوطخلا ةشاشلا.

RA. راسم عبتت فلم مسا نم ققحتلا

<#root>

dir bootflash: | inc ra_trace

يجراخ مداخ ىلإ فلملا خسن:

<#root>

 $\label{eq:copy} white the the the test of test o$

:ىوتحملا ضرع

<#root>

more bootflash: ra_trace_MAC_aaaabbbbcccc_HHMMSS.XXX_timezone_DayWeek_Month_Day_year.log

ربكأ ةيحيضوت ضرع ةقيرط دعت يتلا ةيلغادلا تالجسلا عمجب مقف ،حضاو ريغ لازي ال يرذجلا ببسلا ناك اذإ .10 ةوطخلا اليصفت رثكأ ةرظن يقلن اننا ثيح ىرخأ ةرم ليمعلا ءاطخأ حيحصت ىلإ جاتحت ال .ءاطخألا حيحصت ىوتسم ىلع تالجسلل ايلخاد اهنيزختو لعفلاب اهعيمجت مت يتلا ءاطخألا حيحصت تالجس ىلع.

<#root>

show logging profile wireless internal filter { mac | ip } { <aaaa.bbbb.cccc> | <a.b.c.d> } to-file ra-internal-<FILENAME>.txt

.ةشاشلا ىلع ةرشابم اهضرع وأ يجراخ مداخ ىلإ تاجرخملra-internal-FILENAME.txtl خسن امإ كنكمي

يجراخ مداخ ىلإ فلملا خسن:

<#root>

copy bootflash:ra-internal-<FILENAME>.txt tftp://a.b.c.d/ra-internal-<FILENAME>.txt

:ىوتحملا ضرع

<#root>

more bootflash:ra-internal-<FILENAME>.txt

.ءاطخألاا حيحصت طورش ةلازاب مق .11 ةوطخلا

<#root>

clear platform condition all

.اەحالصاو ءاطخألا فاشكتسأ ةسلج دعب امئاد ءاطخألا حيحصت طورش ةلازا نم دكأت :نَظْحالم

ةلثمألا

ليصافت ىلع لوصحلاو ISEOperations > Live logs قحفص ىلإ لاقتنالا مەملا نمف ،عقوتت امك ققداصملا قجيتن نكت مل اذا ققداصملا قجيتن.

.ISE اهاقلت يتلا Radius تامس عيمجو (لشف كانه ناك اذإ) لشفلا ببس عم كيلع ضرعت

ىرت كنأل كلذو .ةقباطم ضيوفت ةدعاق دجوت ال ەنأل ةقداصملا (ISE) ةيوەلا فشك تامدخ كرحم ضفر ،يلاتلا لائملا يف SSID مسال امامت اقباطم ليوختلا نوكي امنيب ،AP MAC ناونعب قحلم SSID مساك ةلسرم ىعدتسملا ةطحملا فرعم ةمس يواسي" نم الدب "يوتحي" ىلا ةدعاقلا ەذە رييغت عم اەحالصا متي.

Event	5400 Authentication failed
Failure Reason	15039 Rejected per authorization profile
Resolution	Authorization Profile with ACCESS_REJECT attribute was selected as a result of the matching authorization rule. Check the appropriate Authorization policy rule- results.
Root cause	Selected Authorization Profile contains ACCESS_REJECT attribute
Username	E8:36:17:1F:A1:62

 15048
 Queried PIP - Radius.NAS-Port-Type

 15048
 Queried PIP - Network Access.UserName

 15048
 Queried PIP - IdentityGroup.Name (2 times)

 15048
 Queried PIP - EndPoints.LogicalProfile

 15048
 Queried PIP - Radius.edled_StationElD

 15048
 Queried PIP - Radius.edled_StationElD

 15048
 Queried PIP - Network Access.AuthenticationStatus

 15016
 Selected Authorization Profile - DenyAccess

 15039
 Rejected per authorization profile

 11003
 Returned RADIUS Access-Reject

Other Attributes

ConfigVersionId	140
Device Port	58209
DestinationPort	1812
RadiusPacketType	AccessRequest
Protocol	Radius
NAS-Port	71111
Framed-MTU	1485
OriginalUserName	e836171fa162
NetworkDeviceProfileId	b0699505-3150-4215-a80e-6753d45bf56c
IsThirdPartyDeviceFlow	false
AcsSessionID	nicolse26/356963261/1
UseCase	Host Lookup
SelectedAuthenticationIdentityStores	Internal Endpoints
IdentityPolicyMatchedRule	MAB
AuthorizationPolicyMatchedRule	Default
EndPointMACAddress	E8-36-17-1F-A1-62
ISEPolicySetName	Default
IdentitySelectionMatchedRule	MAB
DTLSSupport	Unknown
Network Device Profile	Cisco
Location	Location#All Locations
Device Type	Device Type#All Device Types
IPSEC	IPSEC#Is IPSEC Device#No
RADIUS Username	E8:36:17:1F:A1:62
NAS-Identifier	cwa-ssid
Device IP Address	10.48.71.120
CPMSessionID	7847300A0000012DFC227BF1
Called-Station-ID	00-27-e3-8f-33-a0:cwa-ssid
CiscoAVPair	service-type=Call Check, audit-session-id=7847300A0000012DFC227BF1, method=mab, client-iif-id=3003124185, vlan-id=1468, cisco-wid=cura-seid

Q Search Menu Items		Troubleshooting - > Radioactive Trace		
🚃 Dashboard		Conditional Debug Global State: Stopped		
Monitoring	>	+ Add × Delete ✓ Start	Stop	
	>	MAC/IP Address	Trace file	
Administration	>	e836.171f.a162 H	debugTrace_e836.171f.a162.txt 📥	► Generate
X Troubleshooting				

لوصولاا يف مكحتلا ةمئاق مسا ءاشناب تمق امدنع يئالمإ أطخ لمعب تمق كنأ ةقيقح يف ةلكشملا نمكت ،ةلاحلا هذه يف ةيلحملا ةكبشلا يف مكحتلا رصنع نأ وأ ISE لبق نم هعاجرا مت يذلا لوصولا يف مكحتلا ةمئاق مسا قباطي ال وهو ISE: امبلط يتلا كلتك (ACL) لوصولا يف مكحتلا ةمئاق دوجو مدع نم يكتشي (WLC) ةيكلساللا

<#root>

2019/09/04 12:00:06.507 {wncd_x_R0-0}{1}: [client-auth] [24264]: (ERR): MAC: e836.171f.a162 client authz result: FAILURE 2019/09/04 12:00:06.51

ةمجرتاا مذه لوح

تمجرت Cisco تايان تايانق تال نم قعومجم مادختساب دنتسمل اذه Cisco تمجرت ملاعل العامي عيمج يف نيم دختسمل لمعد يوتحم ميدقت لقيرشبل و امك ققيقد نوكت نل قيل قمجرت لضفاً نأ قظعالم يجرُي .قصاخل امهتغلب Cisco ياخت .فرتحم مجرتم اممدقي يتل القيفارت عال قمجرت اعم ل احل اوه يل إ أم اد عوجرل اب يصوُتو تامجرت الاذة ققد نع اهتي لوئسم Systems الما يا إ أم الا عنه يل الان الانتيام الال الانتيال الانت الما