# FlexConnect لوصو ةطقن لوحم نيمأت مادختساب

تايوتحملا

<u>قمدقملاا</u> <u>قمدقملاا</u> <u>تابلطتملاا</u> <u>قمدختسملاا تانوكملاا</u> <u>نيوكتلا</u> <u>قكبشللل يطيطختلاا مسرلاا</u>

<u>قحصلا نم ققحتلا</u> امحالصاو ءاطخألا فاشكتس<u>ا</u>

## ەمدقملا

قدصي (AP) ةطقن ذفنم FlexConnect ثيح switchports نمؤي نأ ليكشتلا ةقيثو اذه فصي ايلحم لوحي نم رورم ةكرح حمسي نأ traffic-class=switch radius VSA-قادأ لمعتسي dot1x عم LANs يكلسال WLANs).

# ةيساسألا تابلطتملا

## تابلطتملا

:ةيلاتا عيضاوملاب ةفرعم كيدل نوكت نأب Cisco يصوت

- FlexConnect زارط (WLC) ةيكلساللا (LAN) ةيلحملا ةكبشلا يف مكحتايا ةدجو •
- Cisco تالوحم ىلع Cisco •
- (NEAT) ةكبشلا ةفاح ةوداصم ططخم •

## ةمدختسملا تانوكملا

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

- WS-C3560CX-8PC-S، 15.2(4)E1
- AIR-CT-2504-K9، 8.2.141.0
- Identity Service Engine (ISE) 2.0
- المان الم

لاصتا طخ AP ليغشت ماظن ىلإ ةدنتسملا Wave 2 قلسلسلا نم لوصولا طاقن معدت ال AP ليغشت ماظن ىل FlexConnect dot1x ةباتكلا هذه تقو نم ارابتعا.

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

## نيوكتلا

## ةكبشلل يطيطختلا مسرلا



لباقم لوحملا ةطساوب اهتقداصم تمتو 802.1x مقلمك لوصولا ةطقن لمعت ،دادعإلاا اذه يف يأ حمسي ال حاتفملا، 802.1x ةقداصمل نوكي ءانيملا تلكش نإ ام EAP-FAST مادختساب قداصي ءانيملا ىلإ طبري ةادألا نأ ىلإ ءانيملا ربع رمي نأ رورم ةكرح 802.1x ريغ رورم ةكرح حاجنب

ةمس لوحملا لبقتسي ،ISE دض حاجنب لوصولا ةطقن ةقداصم متت نأ درجمبو Cisco VSA قمس لوحملا لبقتسي ،ISE دض حاجنب لوصول "device-traffic-class=switch لاصتالاً طخ يلإ ايئاقلت ذفنملاً لقنيو

نيوانع ىلع يوتحت تناكو FlexConnect عضو معدت لوصولا ةطقن تناك اذإ ،ينعي اذهو SSID زييمت تامالع تاذ رورم ةكرح لاسرا ىلع ةرداق نوكتس اهنإف ،اهنيوكت مت ايلحم ةلوحم. تلكش يعيبط يلهأ VLAN حصي لاو ap لا ىلع VLAN معد تنكم نأ تنمض.

#### -:لوصولا ةطقن نيوكت

ا قېل مل قەل قىل قىل تەناك اذا .1 لوصول ا قلق ن تەناك اذا .2 (WLC)، لوصول ا قلق تەن قەل بول قەل قەل يەل لۇت تەن لە تان يە تان يە تەر قەت تەرىكى تەركى تەركى يەركى تەركى تەركى تەركى يە تان يە تان يە تەرم دىم دىم يەركى يەركى يەركى يە تەركى يە تەركى يەركى يەركى يە قىل يەركى يە يەركى ي

cisco	<u>M</u> ONITOR <u>W</u> L	ANs <u>C</u> C	ONTROLLER	WIRELESS	<u>s</u> ecurity	M <u>A</u> NAGEMENT	C <u>O</u> MM/
Wireless	All APs > Det	ails for	Aks_desk	_3502			
<ul> <li>Access Points</li> <li>All APs</li> <li>Radios</li> </ul>	General	Credenti	als Inte	rfaces I	High Availabil	ity Inventory	/ Fle
802.11a/n/ac 802.11b/g/n Dual-Band Radios Global Configuration	Login Credent Over-ride G						
Advanced Mesh	802.1x Supplie	cant Cred	entials				
> ATF	Over-ride Gl						
RF Profiles	Username	-	ritmahaj				
FlexConnect Groups	Password		•••••				
FlexConnect ACLs FlexConnect VLAN Templates	Confirm Pa	assword	•••••				

تنرتقا نوكي نأ ةطقن ذفنم all the ل ةملكو username ةلصاف تتبث اضيأ عيطتسي تنأ قمئاق ليكشت لماشلا عم WLC لا يلإ

CISCO	MONITOR	<b>WLANs</b>	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT	COMMANDS	HELP	<b>FEEDBACK</b>	
Afferdance	CDP Stat	le			œ		to	3600)	, , , , , , , , , , , , , , , , , , ,	12
vireless	Etherne	et Interface	# CDP	State			AF	Primed	loin Timeout(120 -	
Access Deints	0		1				43	200 seco	onds)	0
All APs	1		1				Ba	ck-up Pr	imary Controller IP	-
<ul> <li>Radios</li> </ul>	2		1				Ac	idress(Ip	v4/Ipv6)	
802.11a/n/ac	3		1				Ba	ck-up Pr	imary Controller name	
Buz.11D/g/n Dual-Band Radios	4		1				Ba	ck-up Se	condary Controller IP	-
Global Configuration	Radio S	Slot#	CDP	State			Ac	Idress(Ip	v4/Ipv6)	_
Advanced	0		1				Ba	ack-up Se	condary Controller	1
Hurtaneeu	1		1				na	me		-
Mesh	2		1				TCD	MCC		
ATF	Login C	redential					TCP	M35		
RF Profiles	Login C	recentian	5				Glo	bal TCP	Adjust MSS (IPv4: 536	. 🛛
FlexConnect Group	s Userna	ame					13	65, IPV6.	1220 - 1331)	
FlexConnect ACLs	Passw	Password					AP Retransmit Config Parameters			
FlexConnect VLAN Templates	Epoble	Decemend		1			Pala	meters	•	
OFAD ACLE	Enable	e Password					AF	P Retrans	mit Count	5
OLAF ACLS	802.1x	Supplicar	nt Credentials				AF	P Retrans	mit Interval	3
Network Lists	OULIA	Supplicu	recontinuis				054	0.0.0	0	
802.11a/n/ac	802.1x	Authenticat	ion				UEA	P Confi	g Parameters	
802.11b/g/n	Userna	ame					Di	sable Loo	al Access	
Media Stream	Passw	ord					NO	TE:	his fasture could vial	ata c
Application Visibili And Control	ty Confir	m Password					wi	thin you	r organization. Please e with all regulations	e ma befo

ةيكلسالللا ةيلحملا ةكبشلا يف مكحت رصنع ىلإ تمضنا دق لوصولا ةطقن نكت مل اذإ .2 مادختساو دامتعالا تانايب نييعتل لوصولا ةطقن يف مكحت ةدحو كيلع بجيف ،دعب (WLC) اذه (CLI) رماوألا رطس ةهجاو رمأ:

LAP#debug Capwap Console CLI LAP#capwap ap dot1x username <username> ةملك <password>

-:لوحملا نيوكت

```
لوحملا ىلا ISE مداخ ةفاضإو ماع لكشب لوحملا ىلع dot1x نيكمتب مق .1
```

ديدج AAA جذومن

!

ةيضارتفالاا ةعومجملاا رطق فصن AAA1x ةقداصم ةطقن

!

AAA ضيوفت ةكبشل ةيضارتفالا ةعومجملا رطق فصن

!

dot1x system-auth-control

!

ISE مداخل RADIUS ו טופט IPv4 10.48.39.161 auth-port 1645 acct-port 1646 key 7 123a0c0411045d5679

AP لوحم ذفنم نيوكتب نآلا مق .2

interface GigabitEthernet0/4 switchport access vlan 231 switchport trunk allowed vlan 231،232 المحتويل لوصول المحتم فيضم مرا عضول ددعتم فيضم dot1x قوداصمل ذفنم يف يئاقلتل امكحتل dot1x Pae Authenticator قفاح ممل قرچشلل PortFast قفاح

-:ISE نيوكت

1. لوصولا ةطقن ليوخت فيرعت فلمل neat تنكم ةطاسبب دحاو عيطتسي ،ISE يف .in order لوصولا ةطقن ليوخت في عام .to تبث to اليودي تلكش عيطتسي تنأ ،لدان RADIUS رخآ يلع ،لاح يأ يلع ،حيحص ةمسلا تتبث

Authorization Profiles > AP_	Flex_Trunk
Authorization Profil	e
* Name	AP_Flex_Trunk
Description	
* Access Type	ACCESS_ACCEPT
Network Device Profile	ditte Cisco 💌 🕀
Service Template	
Track Movement	
Common Tasks     NEAT	

2. هذه يف .ليوختلا ةسايسو ةقداصملا ةسايس نيوكت ىلإ اضيأ عرملا جاتحي ،ISE يف . عرملل نكمي نكلو dot1x ةيكلس نوكت يتلا ةيضارتفالا ةقداصملا ةدعاق قبطن ،ةلاحلا تابلطتملل اقفو اهصيصخت.

ىلٍ AP دامتعا تانايب انفضأ ةلاحلا هذه يف ،(Port\_AuthZ) ضيوفتلا جەنل ةبسنلاب اذه ىلِ ادانتسا (AP\_Flex\_Trunk) ضيوفتلا فيرعت فلم انعفدو (APs) نيمدختسم ةعومجم.

#### Authorization Policy

or P	licy Export	t go to Administration > System	n > Backup & Restore	Policy Export Page	e the order.	
First	Matched R	ule Applies 🔹	]			
▶ E	xception	s (0)				
SI	andard					
	Status	Rule Name	Co	nditions (identity groups and other conditions)	Permissions	
	<b>~</b>	Port_AuthZ	if AP	s AND Wired_802.1X	then AP_Flex_Trunk	

## ةحصلا نم ققحتلا

حيحص لكشب نيوكتلا لمع ديكأتل مسقلا اذه مدختسا.

ا مادختسا ةدحاو ةرم نكمي ،لوحملا ىلع 1. "debug authentication feature autocfg all" ال وأ لاصتالا طخ ذفنم ىلإ ذفنملا لقن نم ققحتلل.

ىلإ ةلاحلا رىيغت مت ،GigabitEthernet0/4 ةەجاولا: LINK-3-UPDOWN: اىل قلاحلا رىيغت مت ىلعاً ةەجاولا ىلء طخلا لوكوتورپ :LINEPROTO-5-UPDOWN٪ 20 12:34:19.122 ريارپف ىلءاً ىلا ةلاحلا رىيغت مت ،GigabitEthernet0/4 akshat sw# akshat sw# 20 رىاربە 12:38:11.113: auth-feat-autocfg-event: in dot1x AutoCfg start\_fn، epm\_handle: 3372220456 لوحملا = زاهجلا عون [12:38:11.113: auth-feat-autocfg-event: [588d.0997.061d، gi0/4] رىاربف 20 دىدج لىمع (12:38:11.113: AUTH-FEAT-AUTOCFG-EVENT: [588d.0997.061d، Gi0/4] دىدج لىمع ل يلخادلا وركاملا قيبطت ةلاح [Gi0/4] 12:38:11.113: auth-feat-autoCFG-event: [Gi0/4] رياربف 20 AutoCFG:1 2 : زاهجلا عون [Gi0/4] 12:38:11.113: auth-feat-autocfg-event: [Gi0/4] رياريف 20 ةرجشلا لوكوتورب يوتحي :12:38:11.113: auth-feat-autocfg-event: [Gi0/4] Auto-config: ارياربف 20 port\_config 0x85777D8 ىلع (STP) ةعرفتملا BPDU هېدل BPDU ويارېف BPDU (Config: stp port\_config) auth-feat-autocfg-event: [Gi0/4] Auto-config: stp guard\_config 2 دفنملا يلع auto-cfg قريبطت auto-cfg-event: [Gi0/4] العامي 20 عنه 20. (ياربف 20 عنه 20) دفنمل ال 20 رىارىف 12:38:11.116: auth-feat-autocfg-event: [Gi0/4] VLAN: 231 VLAN-STR: 231 dot1x\_autocfg\_supp macro قىبطت [Gi0/4] dot1x\_autocfg\_supp macro يلع 'ino switchport access vlan 231 ..رمألا قىبطت :12:38:11.116 رىاربف 20 Gi0/4 يف 'switchport nonegotiate ذفنم دجوي ال' ...رمألا قَيْبُطت :12:38:11.127 رَيَارُبُف 20 Gi0/4 يف 'switchport mode trunk' ..رمألا قيبطت :12:38:11.127 رياربف 20 يلع 'gi0/4 يلع 'switchport trunk native vlan 231' ..رمْأَلاا قِيَبطت :12:38:11.134 رِيَارِبِفْ 20 Gi0/4 ىلع 'arbre-portfast trunk' رمألا قىبطت :12:38:11.134 رىاربف 20

2. لاصتا طخ ذفنم ىلإ ريغت دق ذفنملا نأ "show run int g0/4" جارخإ رەظيس.

نأ Radius Livelogs ةقداصمل نكمي<"تايلمعلا" دنب تحتو ،(ISE) ةيوهلا تامدخ كرحم ىلع .3 .هعفد متي يذلا حيحصلا ضيوفتلا فيرعت فلمو ةحجان ةقداصملا نوكت

Time	Status	Details	Repeat Count	Identity (	Endpoint ID	Endpoint Profile	Authentication Policy (1)	Authorization Policy	Authorization Profiles (1)
2017-02-20 15:05:48.991	0	ò	0	ritmahaj	58:8D:09:97:06:1D	Cisco-Device	Default >> Dot1X >> D	Default >> Port_AuthZ	AP_Flex_Trunk
2017-02-20 15:05:48.991		ò		ritmahaj	58:8D:09:97:06:1D	Cisco-Device	Default >> Dot1X >> D	Default >> Port_AuthZ	AP_Flex_Trunk a
2017-02-20 15:04:49.272	1	ò		ritmahaj	58:8D:09:97:06:1D	Cisco-Device	Default >> Dot1X >> D	Default >> Port_AuthZ	a

لوحم ذفنم ىلع ەب صاخلا MAC ناونع ملعت متيسف ،كلذ دعب ليمع ليصوتب انمق اذا .4 AP ناونع ملعت متيسف كالما المال المال من علي معليات مال المال المال المال المال م

akshat\_sw#sh mac address-table int g0/4 نيوانع لودج MAC

VLAN ةكبشل MAC ناونع عون ذفانم

231 588d.0997.061d يكيتاتسإ نكاس gi0/4 - AP 232 c0ee.fbd7.8824 Dynamic Gi0/4 - ليمعلا

نكمي ،ليمعلا ليصافت يف ،(WLC) ةيكلساللاا ةيلحملاا ةكبشلاا يف مكحتلا رصنع ىلع انه .ايلحم SSID ليوحت متيو 232 مقر VLAN ةكبش ىلإ يمتني ليمعلاا اذه نأ ةظحالم قصاصق.

ت راەظإ< (Cisco نم مكحتلا ةدحو)	c0:ee:fb:d7:88:24 ليمعلا ليصاف
ليمعل MAC ناونع	c0:ee:fb:d7:88:24
ليمعلا مدختسم مسا	رفوتم ريغ
لوصولا ةطقنل MAC ناونع	b4:14:89:82:cb:90
لوصولا ةطقن مسا	aks_desk_3502
AP ويدار ةحتف فرعم	1
َاللَّامِ اللَّامِ الْعَامَةِ الْعَامَةِ الْعَامَةُ الْعَامَةُ عَلَيْهُمْ عَلَى الْعَامَةُ عَلَيْهُمْ الْعَلَى	نترشاعت
ليمعلا يمدختسم ةعومجم	
ليمعلل NAC OOB ةلاح	لوصو

يكلساللا LAN ةكبش فرعم	2ق
ةيكلساللا LAN ةكبش مسا	(SSID) Port-Auth
LAN ةكبش فيرعت فلم مسا	Port-authةيڬڶڛاللاا
(802.11u) ةلاعف ةطقن	ةموعدم ريغ
يد سإ يب	b4:14:89:82:cb:9f
ل لصتم	42 ةيناث
ةانقلا	44
IP	192.168.232.90
ةباوبالا ناونغ	192.168.232.1
ةكبشلا عانق	
نارتقالا فرعم	
ةقداصما أ ةيمزراوخ	حوتفم ماظن
بېسلا زمر	
ةلاحا زمر	0

يل_حمFlexConnect تانايب ليوحت	
َيْلَحِمِ FlexConnect DHCPقَالَ اللهُ	
FlexConnect ةكبش ىلع مئاق يزكرم ليوحت	ال .
لارتنسFlexConnect ، المات	
الال FlexConnect ةينقت ربع يزكرملا طابترال	
FlexConnect ةينقتب ةصاخلاً VLAN ةكبش مسا	VLAN 232
00 ةكبش لزع	
232 VLAN ةكبش ىلإ لوصولًا	
232كبنوترا راج ككب المال المال المال التي المال الع	

## اهحالصإو ءاطخألا فاشكتسا

اهحالصإو نيوكتلا ءاطخأ فاشكتسال اهمادختسا كنكمي تامولعم مسقلا اذه رفوي.

- رماوأ مدختساف ،ةقداصملا تلشف اذا debug dot1x، debug authentication.
- رمألا لخدأف ،لاصتال اطخ ىلإ ذفنمل القن متي مل اذا debug authentication feature autocfg all.
- فيضملا ددعتم .(ددعتم فيضم عضو ةيوه ةحص) ددعتم فيضم عضو نيوكت نم دكأت ناونع كام يكلسال نوبز تحمس in order to تنكم تنك يغبني.
- مت يتلا تامسلا لوحملا لبقي نأ لجأ نم "AAA authorization network" رمألا نيوكت بجي اهقبطيو ISE ةطساوب اهلاسرا.

ثودح يف كلذ ببستي دق .طقف Cisco TLS 1.0 نم IOS ىلإ ةدنتسملا لوصولا طاقن معدت مداخ نيوكت مت اذإ ةلكشم RADIUS مداخ نيوكت مت اذإ قلكشم RADIUS مداخ نيوكت مت اذ

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