عئاشلا فيضلا لوصو تالكشم فاشكتسأ اهحالصإو ISE ىلإ

تايوتحملا

قمدق ملا قمدق ملا قمدخ تسمل ا تابل طتمل ممدخ تسمل ا تانوكمل قمدخ تسمل ا تانوكمل في ضل ا ق في ضل ا ق مرك تم لك شب اهته جاوم متت يتل الكاشمل لمعت ال لكاشمل معت ال لي مي جوتل ا قداع لمعت ال عن الما عن معت ال الما من معت ال الما من معت ال الما من معت ال الما من معت ال الما معت ال معت الما معت الما معت الما معت ال معت الما معت ال

ەمدقملا

رشنلاا يف امحالصإو ةعئاشلا فويضلا ءاطخأ فاشكتسأ ةيفيك دنتسملا اذه حضوي ةلواحملل ةطيسبلا ةليدبلا لولحلاو امنم ققحتلاو ةلكشملا لزع ةيفيكو.

ةيساسألا تابلطتملا

تابلطتملا

:ةيلاتلا عيضاوملاب ةفرعم كيدل نوكت نأب Cisco يصوت

- ISE فيض نيوكت •
- (NAD) ةكبشلا ىلإ لوصولا ةزهجأ ىلع CoA نيوكت •
- .لمعلا تاطحم ىلع طاقتلا تاودأ رفوت مزلي •

ةمدختسملا تانوكملا

:و ،2.6 رادصإلا، Cisco ISE ىلإ دنتسملا اذه يف ةدراولا تامولعملا دنتست

- WLC 5500
- لوحملا Catalyst 3850 15.x version
- Windows 10 لمع ةطحم •

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.

فيضلا قفدت

مادختسإ نكمي .ةيكلساللا وأ ةيكلسلا تارايخلل ةلثامم فيضلا قفدت ىلع ةماع ةرظن روصت ىلع دعاست يەف .دنتسملا ربع عجرمك قفدتلل يطيطختلا مسرلا نم ةروصلا ەذە .نايكلاو ةوطخلا



الجس ىلع قفدتلا ةعباتم نكمي امك ISE تالجس ىلع قفدتلا ةعباتم نكمي امك RADIUS تالجس < تايل معلاً] ةرشابملاً RADIUS تالجس < تايلخ نم [قرشابملاً]

- ىلِ URL عفد متي -MAC ناونع ىلع مدختسملا مسا لقح يوتحي -ةحجان MAB ققداصم NAD - قباوبلا ىلع مدختسملا لصحي NAD - قباوبلا ي
- دقو ،فيضلا مدختسمل مسا ىلع مدختسمل مسا لقح يوتحي -ةحجان فيضلا ةقداصم مساب ەفيرعت مت (فيضلا مدختسملل ەنيوكت مت يذلا عونلا وأ) GuestType_Daily مساب ەفيرعت مت
- َ يليصُفَتلاً رَّيرقَتلاً رەظي ،غرافُ مدَختسُملاً مسا -ەليغشت ءدب مت يَذلاً CoA لَقحلاً حاجنب "يكيمانيدلاً ضيوفتلاً"
- فيضلا لوصو ريفوت مت •

(ىلءألاا ىلإ لفسألاا نم) ةروصلا يف ثادحألا لسلست

May 18, 2020 01:34:18.298 A	и 🛃	0	testguest	84.96.91.26:DD.6D	Windows 10	Guest Access	Guest Acces	PermitAccess	10.106.37.18	DefaultNetwork	TenGigabitEther	User Identity Groups:G	sotumu26
May 18, 2020 01:34:18:269 A	a 🛛	0		84 96 91 26 DD 6D						DefaultNetwork			sotumu26
May 18, 2020 01:34:14.446 A	a 🛛	0	testguest	84.96.91.26.DD.6D					10.106.37.18			GuestType_Daily (defa	sotumu26
May 18, 2020 01:22:50.904 A	/	0	84.96.91.26.00.60	84.96.91.26.DD.6D	Intel-Device	Guest Acces	Guest Acces	Guest_redirect	10.106.37.18	DefaultNetwork	TenGigabitEther	Profiled	solumu26

ةعﺉاشﻝﺍ ﻣﺎﺩﺧﺖﺱﺍﻝﺍ ﺓﻝﺩﺃ

فاشكتسأ ةيلمع يأل ةبسنلاب .نيوكتلا يف ةدعاسملل تاطابترالا ضعب يلي اميف ةعقوتملا وأ ةيلاثملا قئيهتلا كاردإ يلع دعاست اهنإف ،اهحالصإو ةنيعم مادختسإ قلاح ءاطخأ.

- <u>يكلسلا فيضلا نيوكت</u> •
- <u>يكلسال فيض نيوكت</u> •
- <u>CWA Wireless Guest لوصول طاقن عم FlexAuth APs</u>

رركتم لكشب اەتەجاوم متت يتلا لكاشملا

اياضقلا هذه يساسأ لكشب دنتسملا اذه لوانتي:

لمعت ال Guest لخدم ىلإ ەيجوتلا ةداعإ

:يلي امم ققحتف ،ISE نم لوصولا يف مكحتلا مئاوقو هەيجوت داعملا URL ناونع عفد درجمب

ا مادختساب (يكلسلا فيضلا لوصو ةلاح يف) لوحملا ىلع ليمعلا ةلاح 1. authentication session int <interface> **ليصافت**

muse and a half all south hard and	
guestlab#sh auth sess i	nt T1/0/48 de
Interface:	TenGigabitEthernet1/0/48
IIF-ID:	0x1096380000001DC
MAC Address:	b496.9126.dd6d
IPv6 Address:	Unknown
IPv4 Address:	10.106.37.18
User-Name:	B4-96-91-26-DD-6D
Status:	Authorized
Domain:	DATA
Oper host mode:	single-host
Oper control dir:	both
Session timeout:	N/A
Restart timeout:	N/A
Common Session ID:	0A6A2511000012652C64B014
Acct Session ID:	0x0000124F
Handle:	0x5E00014D
Current Policy:	POLICY_Te1/0/48
Local Policies:	
Service Templat	e: DEFAULT LINKSEC POLICY SHOULD SECURE (priority 150)
Security Policy:	Should Secure
Security Status:	Link Unsecure
Server Policies:	
URL Redirect:	https://10.127.197.212:8443/portal/gateway?sessionId=0A6
A2511000012652C64B0144p	ortal=26d19560-2e58-11e9-98fb-0050568775a3saction=cwastok
en=66bbfce930a43142fe26	b9d9577971de
URL Redirect ACL:	REDIRECT_ACL
Method status list:	
Method	State
mab	Autho Success

فيضلا لوصو ةلاح يف) ةيكلساللا ةيلحملا ةكبشلا يف مكحتلا ةدحو ىلع ليمعلا ةلاح .2 MAC ناونع < ليمع < قشاش :(يكلساللا

Security Policy Completed	No	
Policy Type	N/A	
Auth Key Mgmt	N/A	
Encryption Cipher	None	
EAP Type	N/A	
SNMP NAC State	Access	
Radius NAC State	CENTRAL_WEB_AUTH	
CTS Security Group	Not Applicable	
AAA Override ACL	cwa_redirect	
AAA Override ACL Applied Status	Yes	
AAA Override Flex ACL	none	
AAA Override Flex ACL Applied Status	Unavailable	
Redirect URL	dittp:///itin-to-interaction:8443/portal/gateway?session	nId=0

ا يل قياهنلا، قطقن نم لوصولا، قيناكما، 3. SE هجوم ةدعاسمب TCP 8443 SE دفنم يلع ISE دماوألا، :ماوألا، C:**\Users\user>Teinet <ISE-IP> 8443**

4. ليمعلا ناك اذا امم ققحتف ،FQDN ىلع يوتحي ةباوبلا ميجوت ةداعإل URL ناونع ناك اذا . رماوألا مجوم نم لحلا ىلع ارداق: **C:\Users\user>nslookup guest.ise.com**

هسفن (ACL) لوصولاا يف مكحتلا ةمئاق مسا نيوكت نم دكأت ،نرملا لاصتالا دادعإ يف .5 قوحت .ةنرملا (ACL) لوصولا يف مكحتلا مئاوقو (ACL) لوصولا يف مكحتلا مئاوق تحت ليلد عجار .(APs) لوصولا طاقن ىلع (ACL) لوصولا يف مكحتلا ةمئاق نييعت نم اضيأ .تامولعملا نم ديزم ىلع لوصحلل c و ب 7 تاوطخلا-قباسلا مسقلا نم نيوكتلا

CISCO	MONITOR	WLANs	CONTROLLER	WIRELESS	SECURITY
Wireless	FlexConr	nect Acc	ess Control L	ists	
Access Points All APs	Acl Name				
 Radios 802.11a/n 802.11b/g/n Dual-Band Radios Global Configuration 	flexred				
Advanced					
Mesh					
RF Profiles					
FlexConnect Groups FlexConnect ACLs					

6. تمزحلا محفص ريشت .هيجوتلا مداعا نم ققحتلاو ،ليمعلا نم ممزح طاقتلا لبق نم هيلا لوصولا مت يذلا عقوملل ههيجوت داعملا URL كلا اهلقن مت يتلا لبق نم هيل العصول مت يذلا عقوملل ما يا عال العلي العلي الملقن مت يتلا

, ij	.addr==2.2.2.2						
No.	Arrival Time	Source	Destination	Protocol	Info		
-	190 May 18, 2020 14:29:13.49400500	10.106.37.18	2.2.2.2	TCP	54571 → 80 [SYN] Seg=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1		
	191 May 18, 2020 14:29:13,49657400		10.106.37.18	TCP	80 → 54571 [SYN, ACK] Seg=0 Ack=1 Win=4128 Len=0 MSS=1460		
	192 May 18, 2020 14:29:13,49670300		2.2.2.2	TCP	54571 → 80 [ACK] Seg=1 Ack=1 Win=64240 Len=0		
	194 May 18, 2020 14:29:13.69293900	2.2.2.2	10.106.37.18	ТСР	[TCP Dup ACK 191#1] 80 → 54571 [ACK] Seg=1 Ack=1 Win=4128 Len=0		
	218 May 18, 2020 14:29:16.34762700	10.106.37.18	2.2.2.2	HTTP	GET / HTTP/1.1		
	219 May 18, 2020 14:29:16.35025300		10.106.37.18	HTTP	HTTP/1.1 302 Page Moved		
	220 May 18, 2020 14:29:16.35047200		10.106.37.18	TCP	80 → 54571 [FIN, PSH, ACK] Seq=279 Ack=329 Win=3800 Len=0		
	221 May 18, 2020 14:29:16.35050600	. 10.106.37.18	2.2.2.2	TCP	54571 → 80 [ACK] Seg=329 Ack=280 Win=63962 Len=0		
	222 May 18, 2020 14:29:16.35064600	10.106.37.18	2.2.2.2	TCP	54571 → 80 [FTN, ACK1 Seg=329 Ack=280 Win=63962 Len=0		
L	224 May 18, 2020 14:29:16 35466100	2 2 2 2 2	10 106 37 18	TCP	80 → 54571 [ACK] Seq=280 Ack=330 Win=3800 Len=0		
<	219 May 18, 2020 14:29:16.3502 2.2.2.2 10.	106.37.18	HTTP HTTP/1.1 302	Page Moved			
> Fr > Et > Ir > Tr	Frame 219: 332 bytes on wire (2656 bits), 332 bytes captured (2656 bits) on interface 0 Ethernet II, Src: Cisco_ca:0e:c5 (00:87:31:ca:0e:c5), Dst: IntelCor_26:dd:6d (b4:96:91:26:dd:6d) Internet Protocol Version 4, Src: 2.2.2, Dst: 10:106.37.18 Transmission Control Protocol, Src Port: 880, Dst Port: 54571, Seq: 1, Ack: 329, Len: 278						
× H	Pertext Transfer Protocol						
1	Location: https://10.127.197.212:8443/portal/gateway?	sessionId=0A6A25110000120	652C648014&portal=26	d19560-2e58-	11e9-98fb-00505568775a3&action=cwa&token=66bbfce930a43142fe26b9d9577971de&redirect=http://2.2.2.2/\r\n		
	Pragma: no-cache\r\n						
	Cache-Control: no-cache\r\n						
	[HTTP response 1/1]						
	[Time since request: 0.002626000 seconds]						
	[Request in frame: 218]						
	Request URI: http://2.2.2.2/1						

:ةكبشلا ىلإ لوصولا ةزهجأ ىلع HTTP (تاكرحم) كرحم نيكمت مت .7

ىلع	:لّدبُمل							
gue	estlak)#sh	run		in	ip	http	
ip	http	serv	<i>v</i> er					
ip	http	secu	ire-s	sei	rvei	<u>-</u>		

(WLC): ةيكلساللا ةيلحملا ةكبشلا يف مكحتلا رصنع ىلع

uluilu cisco	MONITOR	<u>W</u> LANs	CONTROLLER	WIRELESS	SECURITY	MANAGEMENT
Management	HTTP-HT	TPS Cor	figuration			
Summary SNMP HTTP-HTTPS Telnet-SSH Serial Port Local Management Users	HTTP Ac HTTPS A WebAuth HTTPS F Web Sessio	cess Access ² SecureW Redirection on Timeout	Enabled Enabled Disabled 20	V V 4 V Minutes		

، يجراخ ءاسرا دادعإ يف (WLC) ةيكلساللاا ةيلحملا ةكبشلا يف مكحتلا رصنع ناك اذا. يلي امم ققحتف:

العام لك ىلع اەسفن يە ليمعلا ةلاح نوكت نأ بجي .1 ةوطخلا WLCs.

ة العام العام العامية عنه العام ا العام الع

.WLC طبرلا رصنع ىلع RADIUS ةبساحم ليطعت بجي .3 ةوطخلا



يكيمانيدلا ضيوفتلا لشف

نإف ،حاجنب لوخدلا ليجستو فيضلا لخدم ىلإ لوصولا ىلع ارداق يئاەنلا مدختسملا ناك اذا مل اذا .مدختسملل لماكلا فيضلا لوصو حنمل ضيوفتلا رييغت نوكتس ةيلاتلا ةوطخلا ةجلاعملو .ISE Radius Live تالجس ىلع "يكيمانيدلا ضيوفتلا" لشف ىرتسف ،كلذ حجني يلي امم ققحت ،ةلأسملا

Overview		Steps
Event	5417 Dynamic Authorization failed	11204 Received reauthenticate request
Lyon		11220 Prepared the reauthenticate request
Username		11100 RADIUS-Client about to send request - (port = 1700 , type = Cisco CoA)
Endpoint Id	MAC ADDRESS	11104 RADIUS-Client request timeout expired (1110 Step latency=10003 ms)
Endpoint Profile		11213 No response received from Network Access Device after sending a Dynamic Authorization request
Authorization Result		



،،ا،،،ا،، cısco	MONITOR WLANS CONTROL	ler w <u>i</u> reless <u>s</u> e	ECURITY MANAGEMENT	C <u>O</u> MMANDS	HELP FEEDBACK
Security	RADIUS Authentication Se	rvers > New			
 AAA General RADIUS Authentication Accounting Fallback DNS Downloaded AVP TACACS+ LDAP Local Net Users MAC Filtering Disabled Clients User Login Policies Password Policies Local EAP Advanced EAP Priority Order Certificate Access Control Lists Wireless Protection Policies Web Auth TrustSec SXP Local Policies Advanced 	Server Index (Priority) Server IP Address(Ipv4/Ipv6) Shared Secret Format Shared Secret Confirm Shared Secret Key Wrap Bost Number Server Status Support for CoA Server Timeout Network User Management Management Retransmit Timeout Tunnel Proxy IPSec	12 V 10.127.197.212 ASCII V (Designed for FIPS 1912 Enabled V 2 seconds V Enable 2 seconds Enable Enable Enable	S customers and requires a key	y wrap compliant i	RADIUS server)

.ةيامحلا رادج ىلع UDP 1700 ذفنمب حامسلا بجي .2

3. كال عام NAC كال عام تادادعا تحت .قحيحص ريغ WLC كال علاء NAC ويغي NAC ويغي NAC ويغي NAC ولاء . عال قالود ISE NAC.

Advanced		
	802.11a/n (1 - 255) 1	
T	802.11b/g/n (1 - 255) 1	
	NAC	
	NAC State ISE NAC V	
	Load Balancing and Band Select	
es	Client Load Balancing	
	Client Band Select	

SMS/ينورتكلإلا ديربلا تامالعإ لاسرإ متي مل

1. تادادغ[الا < ماظنالا < قرادالا تحت SMTP نيوكت نم ققحت .

2. ديربلا/SMS لئاسر تاباوب نع اثحب (API) تاقيبطتلا ةجمرب ةمجاو نم ققحتلا جراخ ينورتكلإلا ISE:

لدبتساو ،حفصتم وأ API ليمع ىلع دروملا اهرفوي يتلاا URL (نيوانع) ناونع ربتخا ةيلباق ربتخاو لومحملا فتاهلا مقرو رورملا تاملكو نيمدختسملا ءامسأ لثم تاريغتملا [SMS تاباوب < تادادعإلا < ماظنلا < قرادإلاا] .لوصولا

SMS Gateway Provider List > Global	Default
SMS Gateway Provider	
SMS Gateway Provider Name: *	Global Default
Select Provider Interface Type:	
O SMS Email Gateway	
SMS HTTP API	
URL: * http://api.clickatell.c	om/http/sendmsg?user=[USERNAME]&password=[PASSWORD]&api_i
Data (Url encoded portion):	\$message\$
	/
Use HTTP POST method	I for data portion

< فيضلا لوصو < لمعلا زكارم] ISE ةمدخ يمدقم تاعومجم نم رابتخالاب تمق اذإ ،كلذ نم الدب قباوبو ISE ىلع ةمزح طاقتلا كيلعف ،[**فويضلا عاوناً < تانوكملاو تاباوبلا** اذإ امم ققحتلل

- ا. رييغت نود مداخلاً ىلإ بلطلاً ةمزح لصت.
- ةجلاعمل ةرابعلل دروملا لبق نم اهب ىصوملا تازايتمالا/تانوذألا ىلع ISE مداخ يوتحي .2 بلطلا اذه.

Account Expiration Notification				
	Send account expiration notification 3 days	es (j)		
	View messages in: English - English			
	Email			
	Send a copy of the notification email to the Sponsor			
	Use customization from: Sponsred Portal (Default)			
	Messages:	Copy text from:		
	Your account is going to expire in 3 days. Please notify your sponsor to extend y	our account now to avoid any delays.		
		//		
	Send test email to me at: myemail@cisco.com Send Configure SMTP server at: Work Centers > Guest Access > Administration > SM	TP server		
✓	SMS			
	Messages:	Copy text from:		
	Your account is going to expire in 3 days. Please notify your sponsor to extend your account now to avoid any delays.			
	(160 character limit per message*)*Over 160 characters requires multiple messa	/		
	Bend test SMS to me at:			
	08123456789 Global Default 🗸	Send		
	Configure SMS service provider at: Work Centers > Guest Access > Administration	on > SMS Gateway Providers		

تاباسحلا ةحفص ىلإ لوصولا نكمي ال

قرادإ رز هجوي ،Manage Accounts Button (فيضلا لوصو) > Manage Accounts Button قرادإ رز هجوي ،

ةباوب ىلإ لوصولا نم ISE FQDN لوؤسم نكمتي يكل ،9002 ذفنملا ىلع ISE FQDN ىل**إ تاباسحلا** ليفكلا:



ةباوب ىلإ اەلالخ نم لوصولا متي يتلا لمعلا ةطحم ةطساوب FQDN لح مت اذإ امم ققحت .2 رمألا مادختساب ليفكلا ISE PAN>.

ا ناك اذإ امم ققحت .3 ISE TCP الانم ISE تاك ان انم الحوتفم 9002 ءانيم ISE TCP ال ال انم ققحت .3 Show ports (مألا عم ISE لا انم الحوتفم 9002 ءانيم ISE TCP ال

ةباوبلا ةداهشل تاسرامملا لضفأ

- يف ةمدختسملا ةداهشلا عيقوت متي نأ بجي ،ةسلسلا مدختسملا ةبرجت لجأ نم و DigiCer و GoDaddy لثم) ةفورعم ةماع تاداهش تائيه لبق نم لوؤسملا رودو تاباوبلا لثم) نيضرعتسملا لبق نم اهب قوثولا متي ام ةداع يتلاو ،(كلذ ىلإ امو VeriSign Google Chrome و Firefox . لكلذ ىلإ امو Firefox و
- ال صاخلا IP لعجي كلذ نأل فيضلا هيجوت ةداعإل تباثلا IP مادختساب ىصوي ال ةيجراخ ةهج لبق نم ةعقوم تاداهش نيدروملا مظعم رفوي ال .نيمدختسملا عيمجل ايئرم صاخلا تنرتنإلا لوكوتوربل.
- فورعم أطخ كانه ،p9 وأ p9 كلإ p9 نم تنأ لقني امدنع تنأ لقني امدنع id <u>CSCvp75207</u> نم تنأ لقني امدنع sid <u>CSCvp75207</u> و ليمعلا ققداصمل تقثل و id <u>CSCvp75207</u> و تيح نوكي نأ بجي قودنص syslog و ليمعلا ققداصمل تقثلا و ISE لخاد تقداصملل تقثلاً ثيح قلسلس لاسراب ISE موقي نأ نمضي اذهو .جيحصتلاً تيقرت دعب ايودي تصحف فيضلاً لخدم علاً لوصولاً دنع TLS قفدتل قلماكلاً تاداهشلاً

مادختساب TAC ىلا لوصولا ىجريف ،فيضلا ىل لوصولا لكاشم تاءارجإلا هذه لحت مل اذا <u>ISE</u>. معد قمزح العام تعامجم معد قمزح العام القليبي العام القليبي الم الم الم الم العام المالي الم

ةلص تاذ تامولعم

<u>Cisco نم تاليزنتلاو ينقتلا معدلا</u> •

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