

عئاشلا فيضلا لوصو تالكشم فاشكتسا اهحالصا و ISE لى

تايوتحمل

[عمدقمل](#)

[ةيساسألا تابلطتملا](#)

[تابلطتملا](#)

[عمدختسملا تانوكملا](#)

[فيضلا قفدت](#)

[عئاشلا مادختسالا ةلدأ](#)

[رركتم لكشب اهتهجاوم مت يتلا لكاشملا](#)

[لمعت ال Guest لخدم لى لهجوتلا ةداع](#)

[يكيمانيدلا ضيوفتلا لشف](#)

[SMS/ينورتكلال ديربلا تامالعل لاسرا متي مل](#)

[تابلطتملا ةحفص لى لوصولا نكمي ال](#)

[قباوبلا ةداهشل تاسرامملا لصفأ](#)

[قلص تاذا تامولعم](#)

عمدقمل

رشنلا في اهلصا و عئاشلا فويضلا ءاطخأ فاشكتسا ةيفيك دنتسملا اذه حضوي
ةلواحملل ةطيسبلا ةليدبلا لولحل او اهنم ققحتلا و ةلكشملا لزع ةيفيكو.

ةيساسألا تابلطتملا

تابلطتملا

ةيلاتلا عيضاوملاب ةفرعم كيدل نوكت ناب Cisco ي صوت:

- ISE فيض نيوكت
- (NAD) ةكبشلا لى لوصولا ةزهجأ لىل CoA نيوكت
- لمعلل تاطحم لىل طاقتلل تاودأ رفوت مزلي.

عمدختسملا تانوكملا

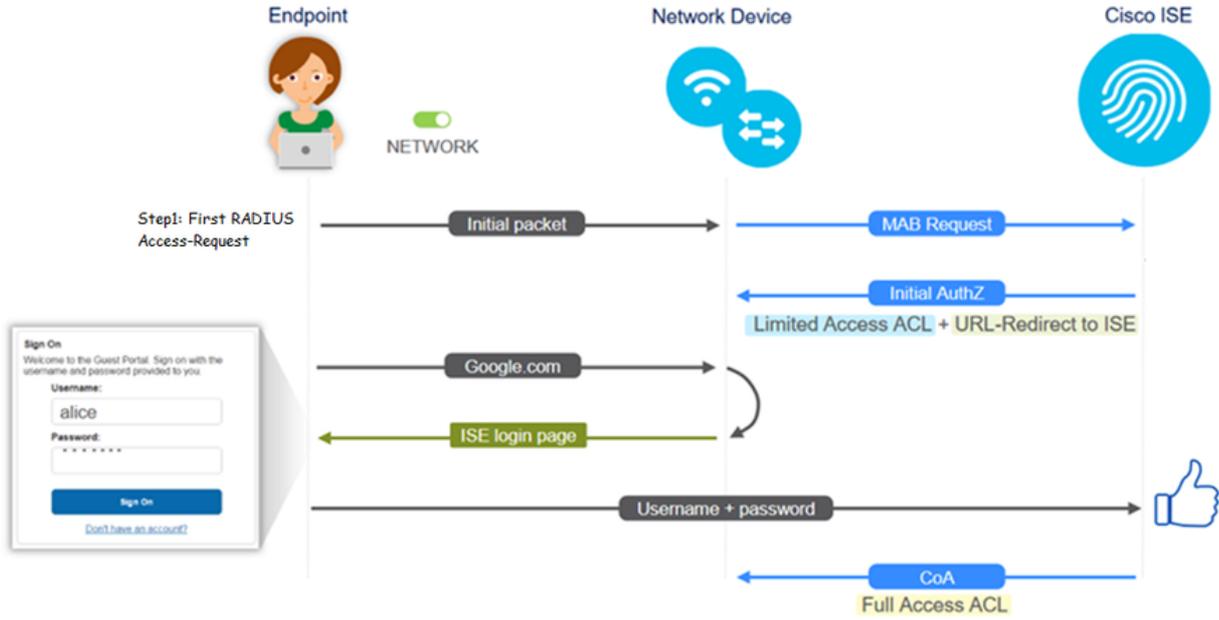
و، 2.6 رادصإلا، Cisco ISE لى دنتسملا اذه في ةدراولا تامولعملا دنتست

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

ةصاخ ةيلمعم ةئيب في ةدوجوملا ةزهجألا نم دنتسملا اذه في ةدراولا تامولعملا ءاشنإ مت
تناك اذإ. (يضا رتفا) حوسمم نيوكتب دنتسملا اذه في عمدختسملا ةزهجألا عيمج تادب
رما يال لم تحملا ريثاتلل كمهف نم دكأتف، ليغشتلا ديقتك تشبش

فيضال قفدت

مادختسا نكمي. ةيكلسالل وأ ةيكلسالل تارايللل ةلثامم فيضال قفدت لىل ةماع ةرطن روصت لىل دعاست يهف. دنتسمال ربع عجرمك قفدتلل يطيطلتال مسرلا نم ةروصلال هذه نايلال ووطخلال.



RADIUS تالچس > تايلمعلال ةرشابمال ISE تالچس لىل قفدتال ةعباتم نكمي امك ةياهنال ةطقن فرعم ةيفصت لالځ نم [ةرشابمال

- لىل URL ةفدمتي -MAC ناوئع لىل مدختسمال مسال لىل قوتحي -ةحجان MAB ةقداصم ةباوبال لىل مدختسمال لصحي - NAD
- دقو، فيضال مدختسمال مسال لىل مدختسمال مسال لىل قوتحي -ةحجان فيضال ةقداصم (فيضال مدختسمال لهنويكت مت يذال ةونال وأ) GuestType_Daily مساب هفیرعت مت
- لىل صفتال ريرقتال رهظي، غراف مدختسمال مسال -هلېغشت ادب مت يذال CoA لىل حانج نب "يكيمايذال ضيوفتال"
- فيضال لوصو ريرفوت مت

(لىل ةلال لىل لفسال نم) ةروصلال ي فثادألال لسلسل

May 15, 2020 01:34:15.280 AM	testquest	84:96:91:26:DD:6D	Windows 10...	Guest Access	Guest Acces...	PermAccess	10.106.37.15	DefaultNetwork...	TenGigabitEther...	User Identity Groups G	solumu26
May 15, 2020 01:34:15.269 AM	testquest	84:96:91:26:DD:6D						DefaultNetwork...			solumu26
May 15, 2020 01:34:14.446 AM	testquest	84:96:91:26:DD:6D					10.106.37.15			GuestType_Daily (defa	solumu26
May 15, 2020 01:22:50.904 AM	testquest	84:96:91:26:DD:6D	Intel-Device	Guest Acces...	Guest Acces...	Guest_redirect	10.106.37.15	DefaultNetwork...	TenGigabitEther...	Profiled	solumu26

ةعئاشلال مادختسالال ةلدأ

فاشكتسا ةيلمع يال ةبسنلاب. نيوكتال ي ف ةدعاسمالل تاطابتالال ضعب لىل امي ف ةعقوتمال وأ ةيلاثلال ةئيهتال كاردل لىل دعاست اهانف، اهلصا و ةنيمع مادختسا لالځ اطاخأ.

- [يكلسالل فيضال نيوكت](#)
- [يكلسالل فيض نيوكت](#)
- [FlexAuth APs لوصولال طاقن عم CWA Wireless Guest](#)

رركتم لكشب اهتهجاوم متت يلال لكاشمال

ايضا قلا هذه ياساسا لكش ب دن تسملا اذ لوان تي

لمعت ال Guest لخدم لى | هيجوتلا ةداع |

يلي امم ققحتف ISE، نم لوصولا يف مكحتلا مئاوقو ههيجوت داعملا URL ناونع عفد درجم ب

1. **show** رمألا مادختساب (يكلسلا فيضلا لوصولا في) لوجملا لىل ع ليمعلا ةلاح .
authentication session int <interface> ليصافت:

```
questlab#sh auth sess int 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_Tel/0/48

Local Policies:
  Service Template: 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
A2511000012652C64B014&portal=26d19560-2e58-11e9-98fb-0050568775a3&action=cwa&tok
en=66bbfce930a43142fe26b9d9577971de
  URL Redirect ACL: REDIRECT_ACL

Method status list:
  Method      State
  mab         Authc Success
```

2. فيضلا لوصولا في (كلسلا لىل حملا ةكبشلا في مكحتلا ةدحو لىل ع ليمعلا ةلاح .
MAC ناونع > ليمع > ةشاش : (يكلسلا لىل ع ليمعلا ةلاح .

Security Information	
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 Tag	Not Applicable
AAA Override ACL Name	cwa_redirect
AAA Override ACL Applied Status	Yes
AAA Override Flex ACL	none
AAA Override Flex ACL Applied Status	Unavailable
Redirect URL	<http://10.10.10.10:8443/portal/gateway?sessionId=0

3. هجوم دعاية اسم ب TCP 8443 ذف نم ىلع ISE ىلى اىة اهنلا ةطقن نم لوصول اىة ناكم ا. رماو األ: C:\Users\user>Telnet <ISE-IP> 8443

4. لىم علال ناك اذ اام ققحت ف FQDN ىلع ىوتحى ةباوبلا هىجوت ةداع األ URL ناوع ناك اذ ا. رماو األ: C:\Users\user>nslookup guest.ise.com

5. هسفن (ACL) لوصول اى ف مكحت ل اءاق مسا نىوكت نم دكأت ،نرمل لاصتال اءاع اى ف ققحت .ةنرمل ل (ACL) لوصول اى ف مكحت ل اءاق و (ACL) لوصول اى ف مكحت ل اءاق تحت لىل دءار . (APs) لوصول اءاقن ىلع (ACL) لوصول اى ف مكحت ل اءاق نىىعت نم اضى اءامول عمال نم دىزم ىلع لوصول ل ل c و ب 7 تاو طءال-ق باسلا مسقلا نم نىوكتلا

The screenshot shows the Cisco FlexConnect configuration interface. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', and 'SECURITY'. The 'WIRELESS' section is active. On the left, a sidebar menu shows 'Access Points' expanded, with sub-items like 'All APs', 'Radios', and 'Advanced'. The main area displays 'FlexConnect Access Control Lists' with a table containing one entry: 'flexred' under the 'Acl Name' column.

6. ةمزل ءحفص رىشت .هىجوتلا ةداع ا نم ققحتلا او ،لىم علال نم ةمزل طاقنلا . HTTP/1.1 302 ءمزل ءحفص رىشت .هىجوتلا ةداع ا نم ققحتلا او ،لىم علال نم ةمزل طاقنلا . WLC/Switch لىل لوصول اءاقن مت ىذلا عوملل هىجوت ءاعمل URL ىلى اهل قن مت ىتلا (ههىجوت ءاعمل URL ناوع) ISE فىض لءدم ىلى

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] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM=1
191	May 18, 2020 14:29:13.49657400...	2.2.2.2	10.106.37.18	TCP	80 → 54571 [SYN, ACK] Seq=0 Ack=1 Win=4128 Len=0 MSS=1460
192	May 18, 2020 14:29:13.49670300...	10.106.37.18	2.2.2.2	TCP	54571 → 80 [ACK] Seq=1 Ack=1 Win=64240 Len=0
194	May 18, 2020 14:29:13.69293900...	2.2.2.2	10.106.37.18	TCP	[TCP Dup ACK 191#1] 80 → 54571 [ACK] Seq=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...	2.2.2.2	10.106.37.18	HTTP	HTTP/1.1 302 Page Moved
220	May 18, 2020 14:29:16.35047200...	2.2.2.2	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] Seq=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 [FIN, ACK] Seq=329 Ack=280 Win=63962 Len=0
224	May 18, 2020 14:29:16.35466100...	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

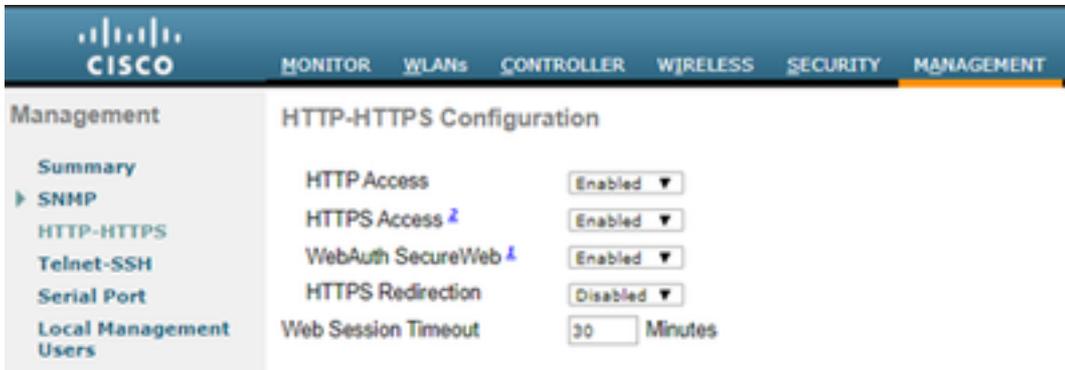
> Frame 219: 332 bytes on wire (2656 bits), 332 bytes captured (2656 bits) on interface 0
 > Ethernet II, Src: Cisco_ca:0e:c5 (00:07:31:ca:0e:c5), Dst: IntelCor_26:dd:6d (b4:96:91:26:dd:6d)
 > Internet Protocol Version 4, Src: 2.2.2.2, Dst: 10.106.37.18
 > Transmission Control Protocol, Src Port: 80, Dst Port: 54571, Seq: 1, Ack: 329, Len: 278
 > Hypertext Transfer Protocol
 > HTTP/1.1 302 Page Moved\r\n
 Location: https://10.127.197.212:8443/portal/gateway?sessionId=046A2511000012652C648014&portal=26d19560-2e58-11e9-98fb-0050568775a3&action=cwa&token=66bbfce930a43142fe26b9d957791de&redirect=http://2.2.2.2/\r\n
 Pragma: no-cache\r\n
 Cache-Control: no-cache\r\n
 \r\n
 [HTTP response 1/1]
 [Time since request: 0.002626000 seconds]
 [Request in frame: 218]
 [Request URI: http://2.2.2.2/]

7. توكبشالال لوصولا ؤزهأ لىل HTTP (تاكرحم) كرحم نيكم ت م ت:

لؤدبم ل لىل:

```
guestlab#sh run | in ip http
ip http server
ip http secure-server
```

ةك لىل سلال الة لىل ؤكبشالال لىل ف مكحتال رصنع لىل (WLC):

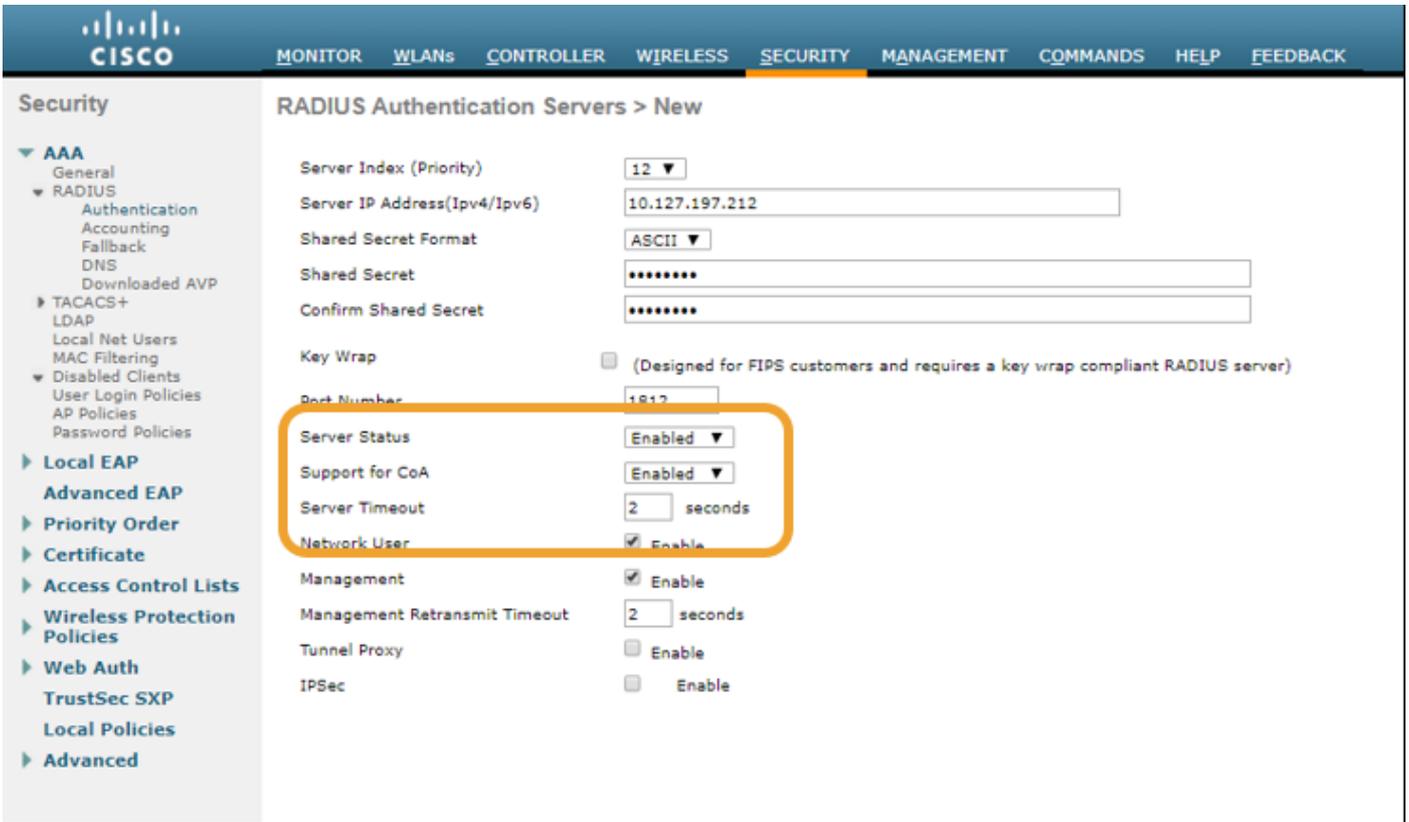


8. لىل ؤكبشالال الة لىل ؤكبشالال لىل ف مكحتال رصنع ناك اذا. لىل امم ققحت:

1. ؤوطخلال WLCs نم لك لىل ؤه لىل ؤلا ح نوك ت نأ ب لىل.

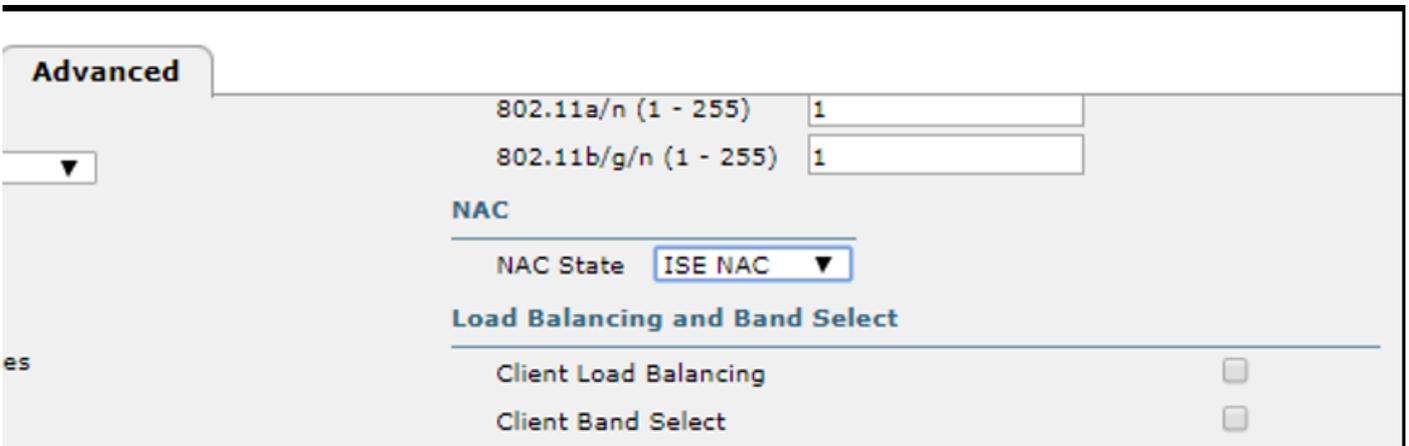
2. ؤوطخلال ؤكبشالال لىل ف مكحتال لىل ؤه لىل ؤلا ؤال URL ناونع ؤه لىل ب لىل (WLCs).

3. ؤوطخلال WLC طبرال رصنع لىل RADIUS ؤب سالح لىل طعت ب لىل.



2. ةيامحل رادج لىل 1700 UDP ذفنم بحامس لل بجي .

3. NAC ريغي WLC GUI>WLAN لىل ةمدقتم تادادع| تحت . ةححص ريغ WLC لىل NAC ةلاح . ISE NAC لىل ةلود



SMS/ي نورتك لىل دي ربل ا تامال ع لاسر ا متي مل

1. SMTP > تادادع| ا > ماظنل ا > ةرادل ا تحت SMTP نيوكت نم ققحت .

2. دي ربل/ SMS لئاسر ت اباوب نع ا تحب (API) اتا قيبطت لل ةحمر ب ةهجاو نم ققحت لل . ISE جراخ ي نورتك لىل ا:

ل دبتساو ، حفصتم و API ليمع لىل درومل اهر فوي ي لل URL (ني وانع) ناو نع ربتخا ةيلباق ربتخاو لومحم لل فتاهل ا مورو رورم لل تاملكو ني مدختسم لل ا م س ا لثم تاريغتم لل [SMS ت اباوب > تادادع| ا > ماظنل ا > ةرادل ا] . لوصول

SMS Gateway Provider

SMS Gateway Provider Name: * Global Default

Select Provider Interface Type:

 SMS Email Gateway SMS HTTP APIURL: * Data (Url encoded portion): Use HTTP POST method for data portion

> فيضال لوصول > لمعل زكارم] ISE م د خ ي م د ق م تاع و م ج م ن م راب ت خ ال اب تم ق اذا ، كل ذ ن م ال دب SMS/SMTP ة با و ب و ISE ل ع م ز ح ط ا ق ت ل ا ك ي ل ع ف ، [فويضال عاونأ > تانوك م ل او ت اب و ب ل ا اذا م م ق ق ح ت ل ل

1. ريغت نود م داخ ل ا ل بل ل ط ل ا م ز ح ل ص ت .

2. ة ل ا م ل ة ر ا ب ع ل ل در و م ل ل ب ق ن م ا ه ب ي ص و م ل ا ت ا ز ا ي ت م ا ل / ت ا ن و ذ ا ل ا ل ع ISE م دا خ ي و ت ح ي . ب ل ل ط ل ا ا ذ ه

Account Expiration Notification

 Send account expiration notification days before account expires [?](#)

View messages in:

 Email Send a copy of the notification email to the SponsorUse customization from:

Messages:

Copy text from:

Send test email to me at:

[Configure SMTP server at: Work Centers > Guest Access > Administration > SMTP server](#) SMS

Messages:

Copy text from: (160 character limit per message)*Over 160 characters requires multiple messages.

Send test SMS to me at:

[Configure SMS service provider at: Work Centers > Guest Access > Administration > SMS Gateway Providers](#)

ت ا ب ا س ح ل ا ة ح ف ص ي ل ل ل و ص و ل ا ن ك م ي ال

1. ة ر ا د ا ر ز ه ج و ي ، Manage Accounts Button > (فيضال لوصول) > Guest Access (لمعل زكارم) تحت .

ةمچرتل هذه لوج

ةللأل تاي نقتل نمة ومة مادختساب دن تسمل اذة Cisco تمةرت
ملاعلاء انء مء مء نء مء دختسمل معد و تمة مء دقتل ةر شبل او
امك ةق قء نوك ت نل ةللأل ةمچرت لصف أن ةظحال مء ءرء. ةصاأل مء تءل ب
Cisco ةللخت. فرتمة مچرت مء مء دقء ةللأل ةل فارتحال ةمچرتل عم لاعل او
ىل إلمءءء ءوچرلاب ةصوء و تاملرتل هذه ةقء نء اهءل وئس م Cisco
Systems (رفوتم طبارل) ةلصلأل ةزىل ءنل اءل دن تسمل