

# ثلاثال فرطالاب صاخلا ISE 2.0 لم اکت ني وکت عم Aruba Wireless

## تايوت حمل

---

[عمدق م](#)

[قيساس الاتابل طم](#)

[تابل طم](#)

[عمدخت س م تان وکت](#)

[ني وکت](#)

[کبش ل ل يطيطخت ل م س ر](#)

[قيجراخل تاهج ل م عدب ق ل عت م تاي دخت ل](#)

[تاس ل](#)

[URL هي جوت عدا](#)

[CoA](#)

[ISE ل ع ل ج](#)

[Cisco ISE](#)

[کبش ل ل قه ج ل ل Aruba ق ي ک ل س ال ل م ک ج ت ل ع د ح و ع فاض ل 1. ع و ط خ ل](#)

[ل ي و خ ت ل ل في ر ع ت ف ل م ن ي و ک ت 2. ع و ط خ ل](#)

[ق ق د اص م ل ل د ع ا و ق ن ي و ک ت 3. ع و ط خ ل](#)

[س ر ب د ت ي ش و س ا ا و ر ا](#)

[ع د ي ق م ل ل ق ب ا و ب ل ل ن ي و ک ت 1. ع و ط خ ل](#)

[RADIUS م د ا خ ن ي و ک ت 2. ع و ط خ ل](#)

[SSID ن ي و ک ت 3. ع و ط خ ل](#)

[ق ح ص ل ل ن م ق ق ج ح ت ل](#)

[SSID Mgarcarz\\_arubawith EAP-PEAP ب ل ي ص و ت ل ل 1. ع و ط خ ل](#)

[BYOD ل ب ي و ل ل ح ف ص ت م ر و ر م ک ر ح ه ي ج و ت ع د ا ل 2. ع و ط خ ل](#)

[کبش ل ل د ا د ع ل د ع ا س م ذ ي ف ن ت 3. ع و ط خ ل](#)

[CoA م ع د و ي ر خ ا ت ا ق ف د ت](#)

[CWA ع م CoA](#)

[اه ح ال ص ا و ع ا ط خ ا ل ل ف ا ش ک ت س ا](#)

[FQDN ن م ال د ب IP Address ع م Aruba Captive Portal ع ا و ب](#)

[ع د ي ق م ل ل Aruba ع ا و ب ل ل ح ي ص ر ي غ ل و ص و ج ه ن](#)

[Aruba CoA ذ ف ن م م ق ر](#)

[Aruba ق ه ج ا ض ع ب ي ل ع ه ي ج و ت ل ل ع د ا ل](#)

[ق ل ص ت ا ذ ت ا م و ل ع م](#)

---

## عمدق م

يلع اه ح ال ص ا و ثلاثال فرطال لم اکت قزيم عاطخأ فاشک تسأ ق ي ف ي ک د ن ت س م ل ا ا ذ ه ف ص ي Cisco ن م (ISE) ق ي و ه ل ا ت ا م د خ ک ر ح م

## ةيساسألا تابلطملا

### تابلطملا

ةيلال عيضاوملاب ةفرعم كيديل نوكت نأب Cisco ي صوت

- Aruba IAP نيوكت
- ISE لىل BYOD قفدت
- ةداهشلاو رورملا ةملك ةقداصم ل ISE نيوكت

### ةمدختسملا تانوكملا

لىل عاهال صاواو ثلاثلا فرطلا لم اكت ةزيم عاطخأ فاشك تسأ ةيفي ك دن تسملا اذه فص ي Cisco نم (ISE) ةيوهلا تامدخ كرحم

2.0 رادصإل ISE م عدي . رخأ تاقفدتو نيرخآ نيدررم عم لم اكتلل لي لدك هم ادختسإ نكمي و ثلاثلا فرطلا لم اكت

Aruba ةطساوب اهترادإ م تتي تلي ةيكل لساللا ةكبشلا جمد ةيفي ك حضوي نيوكت لاثم اذه (BYOD). كب ةصاخلا ةزهجألا تامدخ لىل لوصحلل ISE عم 204 IAP

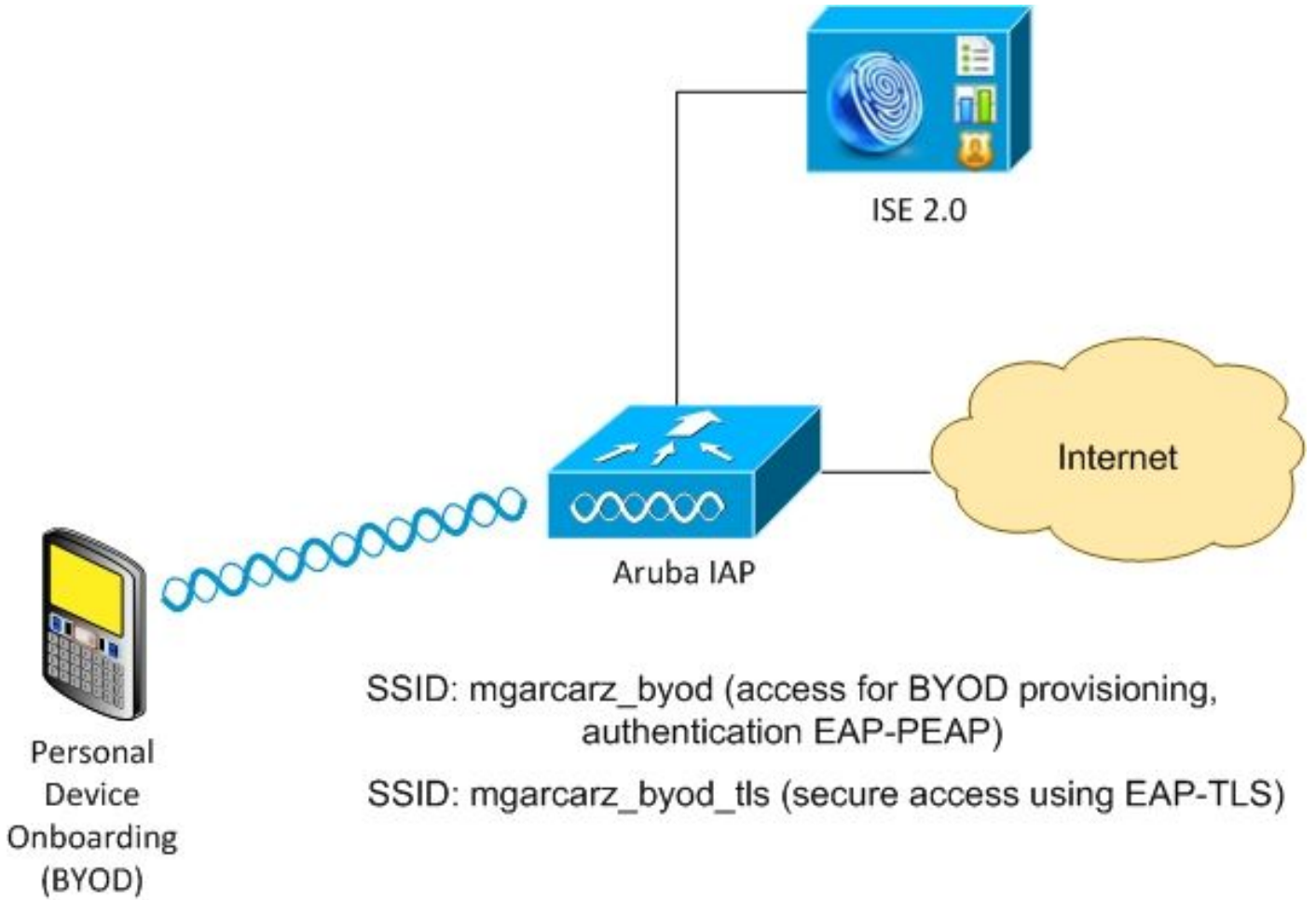
ةيلال جماربلا تارادصإ لىل دن تسملا اذه يف ةدراولا تامول عملا دن تست

- Aruba IAP 204 6.4.2.3 جمارب
- Cisco ISE، رادصإل او 2.0 رادصإل

ةصاخ ةيلم عم ةئيب يف ةدوجوملا ةزهجألا نم دن تسملا اذه يف ةدراولا تامول عملا عاشنإ م تناك اذإ . (يضا رتفا) حوسمم نيوكتب دن تسملا اذه يف ةمدختسملا ةزهجألا عي مج تادب رما يال لم تحملا ريثأتلل كمهف نم دكأتف ، ليغشتلا دي قكتك بش

## نيوكتلا

### ةكبشلل يطيختلا مسرلا



Aruba AP ةطساوب امهتارادا متت ني تيكللسال ني تيكلبش كانه

ةقداصملا لوكوتوربب يمحمل EAP لى لوصولل (mgarcarz\_byod) لوالا راىخلا مدختسي 802.1x (EAP-PEAP) عسوتملا

لخدم لى لمدختسملا هي جوت ةداعإ Aruba ي فمكحتلا ةدحو موقت نأ بجي، ةحجان ةقداصم دعب (NSP) ي لصلال ليمعلا ديوزت قفدت - ISE BYOD.

متي و (NSA) ةكبشلا دادعإ دعاسم قي ببطت ذي فننت متي و، مدختسملا هي جوت ةداعإ متت Windows ليمع لىل عاهت ي بشتو ةداهشلا ريفوت

(يضا رتفالال ني وكتلال) ةي لمعلا هذهل ISE ل ي لخالل قداصملا عجرملا مادختسا متي

رادملا (SSID) ي ناثللا تامدخال ةعومجم فرعمل يكللسال في صوت عاشنإ نع لوؤسم NSA نأ امك ةقداصملا لوكوتوربب ةقداصملا همادختسا متي يذلوا - (mgarcarz\_byod\_tls) Aruba لبق نم (EAP-TLS) لقلال ةقبط ني مات - 802.1x عسوتملا

لوصحلاو ي صخش زاى لى امامضنالا ةي لمع ذي فننت ةكرشلا مدختسملا نكمي، كلذل ةجيتنو ةكرشلا ةكبش لىل نم لوصول

لاثلما لىبس لىل ع، ةفلتخملا لوصولا عاونال ةلوهسب لائلما اذله ليدعت نكمي

- BYOD ةمدخ عم (CWA) بيولل ةي زكرملا ةقداصملا
- BYOD و عضولا هي جوت ةداعإ عم 802.1x رايعملا اقفو ةقداصم
- هذبه ظافتحالل (EAP-PEAP) ةقداصملا Active Directory ةمدخ مادختسا متي ام ةداعو

(رخصتخمل ي لخدال ISE يمدختسم مادختسإ متي ،ةلاقملا

- صاخلا (SCEP) يجرخال طيسبل ادهاشل ليجست لوكوتورب مداخ مادختسإ متي ،ةداعو نم (NDES) ةكبشل ازهجأ ليجست ةمدخ مادختسإ متي ماع لكشبو ،ةدهاشل دادمإب ي لخدال ISE CA مادختسإ متي امك ،ةريصق ةلاقملا هذه اءاقبال Microsoft

## ةيجرخال تاهجال معدب ةقلعتملا تايدحتلا

Client Provisioning و NSP و CWA و BYOD لثم) ISE فيض تاقفدت مادختسإ دنع تايدحت دجوت ثلاثل فرطلا ازهجأ عم ((CPP Portal

### تاسلجال

Audit-session-ID يمسمل RADIUS جوز Cisco نم (NAD) ةكبشلا لوصول ازهجأ مدختست ةسلجال فرعمب (AAA) ةبساحملاو ضيوفتلاو ةقداصملا مداخ مالعال

لكل ةحيجصل تامدخال ريفوتو تاسلجال بقعتل ISE لبق نم ةميقلا هذه مادختسإ متي Cisco-AV جوز نورخال نودروملا معددي ال .ققفدت

.ةبساحملا بلط و لوصول بلط ي ف ةملتسملا IETF تامس يلع ISE دمتعي نأ بجي

call-station-id. نم) نامزتملا Cisco ةسلج فرعم عاشنإب ISE موقوي ،لوصول بلط يقلت دعب متي ال) طقف ةي لحم ةيمهأ اهل ةميقلا هذه .(كرتشملا رسلال او NAS-IP-address ،NAS-Port ،(ةكبشلا ربع اهلاسلرا

تامس قافراب (BYOD، CWA، NSP، CPP) قفدت لك موقوي نأ عقوتملا نم ،كلذل ةحيجتنو ةسلجال اب هطبرل ثحب اءارء او Cisco ةسلج فرعم باسح ةداعإ نم ISE نكمتي ىتح - ةحيجصل قفدتلا ةعباتم و ةحيجصلال

### URL هي جوت ةداعإ

ةرورضب NAD مالعال url-redirect و url-redirect-acl يمس ي Cisco نم RADIUS جوز ISE مدختسي ةني عم رورم ةكره هي جوت ةداعإ

URL ناوعب ازهجال هذه نيوكت بجي ،ةداعلا ي ف كلذل Cisco-AV جوز نورخال نودروملا معددي ال ISE يلع (ضيوفتلا فيرعت فلم) ةني عم ةمدخ يلا ريشي يذلا هي جوتلا ةداعإل تباث

URL يلا هي جوتلا ديكت كلت NADs نإف ،HTTP ةسلج ةئي هتب مدختسملا موقوي نأ درجمب ةسلج فيرعتب ISE حامسلل (MAC ناوع و IP ناوع لثم) ةيفاضل اطيس و اضيأ قفرتو قفدتلا ةعباتم و ةني عم

### CoA

reauthentication-type: كرتشم ،رمأ: كرتشم يمسمل Cisco-AV RADIUS جوز ISE مدختسي ةني عم لمع ةسلجال اءذختت نأ بجي يتلا تاءارءال يلا ةراشلل

و RFC CoA (3576) ازهجال هذه مدختست ،ةداع كلذل Cisco-AV جوز نورخال نودروملا معددي ال :ةددملا لئاسرلا يدحإو (5176

- عطل بطل اذ م دختسي - (لاصتال عطق ة مزح اضي أ م سي) لاصتال عطق بطل (لاصتال ة داع | ضر فل اب لاغ) لمعلا ة سلج لاصتال
- لاصتال عطق نود ة يف افش ب لمعلا ة سلج ة لاج ري غت ل كلذ مادختس | م تي - CoA ع فد (ة دج (ACL) لوصولي ف م كحت ة مئاق قي بطت و VPN ة سلج ، لاثل م لا بس يلع)

RFC CoA 3576/5176 نم الك اضي أو Cisco-AV جوز عم Cisco CoA نم الك ISE م عدي

## ISE يلع ل

يذلا ة كبش ل ة زه ج أ في رعت تافل موه فم ISE 2.0 تم دق ، ة ج راخ ل تاهج ل ي دروم معد ل ج أ نم و ، هج و تال ة داع | URL و ، لمعلا تاسلج معد م تي في ك - ددحم ل دروم ل فرص تي في ك فص ي CoA.

ة قداصل م ل ث دحت نأ درجم ب و (ة كبش ل زاهج في صوت) ني عم عون نم لي و ختال تافي صوت نوك ت في صوت ل كلذ نم ISE كولس قاق تشا م تي.

نأ امك . ISE ة مدخ ة طساوب ة لوه سب ني رخ أ ني دروم نم ة دراو ل ة زه ج أ ل ة راد ا نكم ي ، كلذل ة جيت نو وأ ة دج ل ة كبش ل ة زه ج أ تافي صوت طبض ب حم سي و ة نورم ل اب مس تي ISE يلع ني وكتال اه و اش ن |

Aruba زاهج ل ي ضارت فالال في رعتال فلم مادختس | ة لاقم ل هذه ضرعت

: ة زيم ل لوح تامول عم ل نم ديزم

[Cisco نم ة يوه ل تامدخ كرحم مادختس اب ة كبش ل يلا لوصولا زاهج في رعت تافل م](#)

## Cisco ISE

ة كبش ل ة زه ج أ يلا Aruba ة يكل ل لال م كحتال ة دحو ة فاض | 1. ة و طخال

دروم ل ل ج حص زاهج في رعت فلم رتخ أ . ة كبش ل ة زه ج أ > ة كبش ل دراوم > ة راد ا يلا لقت نا وه امك ءاني م CoA و كرتشم يرس ل كشي نأ تنم ض . Aruba Wireless : ة لاج ل هذه ي ف ، ددحم ل روصولا ي ف حضورم .

## Network Devices

\* Name

Description

\* IP Address:  /

\* Device Profile

Model Name

Software Version

\* Network Device Group

Location

Device Type



### ▼ RADIUS Authentication Settings

Enable Authentication Settings

Protocol **RADIUS**

\* Shared Secret

Enable KeyWrap

\* Key Encryption Key

\* Message Authenticator Code Key

Key Input Format  ASCII  HEXADECIMAL

CoA Port

> ةكبشلا دراوم > ةرادا تحت هنيوكت نكمي ،بولطملا دروملل حاتم فيصوت دوجو مدع ةلاح يف ةكبشلا زاهج تافيصوت.

ليوختلا فيرعت فلم نيوكت 2. ةوطخلا

ليوختلا فيرعت تافل م > ليوختلا > جئاتنلا > ةسايسلا رصانع > ةسايسلا لىل لقتنا فيرعتلا فلم ArubaWireless. ةكرش 1. ةوطخلا يف هسفن ةكبشلا زاهج فيرعت فلم رتخأ روصلا يف حضورم وه امك BYOD لخدم عم Aruba-redirect-BYOD وه هنيوكت مت يذلا

Authorization Profiles > Aruba-redirect-BYOD

### Authorization Profile

\* Name

Description

\* Access Type

Network Device Profile

#### Common Tasks

Web Redirection (CWA, MDM, NSP, CPP)

Value

#### Advanced Attributes Settings

=  - +

#### Attributes Details

Access Type = ACCESS\_ACCEPT

فيرعت فلمل تباث طاابترا عاشنإ متي شيج، بي وهيجوت ةداعإ نيوكت نم دوقم ءزج كانه، فيضلا لخدملا يكيما نيذلا هيجوتلا ةداعإ معدت ال Aruba نأ نم مغرلا لىل. ليوختلا وه امك Aruba لىل كلذ دعب هنيوكت متي يذلاو، ليوخت فيرعت فلم لك ل نيعم دحاو طاابترا ةروصولا يف حضورم.

#### Common Tasks

Value

The network device profile selected above requires the following redirect URL to be configured manually on the network access device in order to enforce web redirection:

<https://iseHost:8443/portal/g?p=10lmawmkIleZQhapEvIXPAoELx>

ةقداصلما دعاوق نيوكت 3. ةوطخلا

ةروصولا يف حضورم وه امك نيوكتلا متي وضيوفتلا دعاوق > ةسايسلا لىل لقتنا

✓	Basic_Authenticated_Access	if Employee AND (EAP-TLS AND EndPoints:BYODRegistration EQUALS Yes )	then PermitAccess
✓	ArubaRedirect	if Aruba:Aruba-Essid-Name EQUALS mgarcarz_aruba	then Aruba-redirect-BYOD

Aruba-redirect-BYOD لي وختال فيرعت فلم عجرت ISE و SSID Mgarcarz\_aruba ب مدختسمال لصتتي، والأة لملمع لامتك دع ب. يضارتفالا BYOD لخدمى لليمعال هي جوت ديعي يذل Aruba-redirect-BYOD. ةك بشلا لى لملال لوصول حنم متي و EAP-TLS ب ليمعال لصتتي، BYOD.

يلي امك ةسايسال سفن ودبت دق ISE نم ثدحال تارادصال ي:

## سرب دتيشوسأ ابورأ

ةديقمال ةباوبال نيوكت 1. ةوطخال

ةجراخال ةديقمال ةباوبال > نامألا لى لقتنا، Aruba 204 لى ةديقمال ةباوبال نيوكت ل ةروصلال يف حضورم وه امك وبسانملا نيوكت لل تامولعملال هذه لخدأ. ةديج ةباوبت فضاو.

- RADIUS ةقداصم: عونلا
- ISE مداخ: فيضمال مسا وأ IP
- URL: لي وختال فيرعت فلم نيوكت نمض ISE لىع هؤاشنإ متي يذلا طابترالا: ببولال هي جوت ةداعإ نيوكت نمض انه هيلع روثعال نكمي ونيعم لي وخت فيرعت فلمب

Native Supplicant Provisioning Value BYOD Portal (default)

The network device profile selected above requires the following redirect URL to be configured manually on the network access device in order to enforce web redirection:

**https://iseHost:8443/portal/g?p=10ImawmkleZQhapEvIXPAoELx**

- لكش ب) ISE لىع هيلع ددحملال لخدمال ةفاضتسا متت يذل ذفنملا مقرر: ذفنملا ةروصلال يف حضورم وه امك (8443: يضارتفا).



mgarcarz\_ise20

Type:	Radius Authentication
IP or hostname:	mgarcarz-ise20.example.
URL:	/portal/g?p=Kjr7eB7RrrLI
Port:	8443
Use https:	Enabled
Captive Portal failure:	Deny internet
Automatic URL Whitelisting:	Disabled
Redirect URL:	<input type="text"/> (optional)

OK Cancel

## RADIUS مداخل نيوكوت 2. ةوطخال

ىلع هنيوكوت مت يذلا هسفن وه COa ذفنم نأ نم دكأت ةقداصملا مداوخ > نامألا ىلا لقتنا ةروصلال يف حضورم وه امك ISE.

RFC عم قفاوتت ال، كلذعمو، 5999 ىلع اهنبيعت متي، Aruba 204 يف، يضارتفا لكشبو ISE عم اضيا لمعت الو 5176.

# Security

Authentication Servers

Users for Internal Server

Roles

Blacklisting

Edit

Name:	mgarcarz_ise20	
IP address:	<input type="text" value="10.48.17.235"/>	
Auth port:	<input type="text" value="1812"/>	
Accounting port:	<input type="text" value="1813"/>	
Shared key:	<input type="password" value="*****"/>	
Retype key:	<input type="password" value="*****"/>	
Timeout:	<input type="text" value="5"/>	sec.
Retry count:	<input type="text" value="3"/>	
RFC 3576:	<input type="text" value="Enabled"/>	
Air Group CoA port:	<input type="text" value="3799"/>	
NAS IP address:	<input type="text" value="10.62.148.118"/>	(optional)
NAS identifier:	<input type="text"/>	(optional)
Dead time:	<input type="text" value="5"/>	min.
DRP IP:	<input type="text"/>	
DRP Mask:	<input type="text"/>	
DRP VLAN:	<input type="text"/>	
DRP Gateway:	<input type="text"/>	

لخدملا" رايتخالالا قناخ دي دحتب اضيا مق ، ثدحال رادصالاو Aruba نم 6.5 رادصالا يف :ةظحالم  
"نمضملا".

نويوكت 3. ةوطخالا SSID

- ةروصلا يف حضوم نيमतلا بيوبت ةمالع .

Edit mgarcarz\_aruba

1 WLAN Settings 2 VLAN 3 Security 4 Access

### Security Level

More Secure

Enterprise

Personal

Open

Less Secure

Key management: WPA-2 Enterprise

Termination: Disabled

Authentication server 1: mgarcarz\_ise20 Edit

Authentication server 2: -- Select Server --

Reauth interval: 0 hrs.

Authentication survivability: Disabled

MAC authentication:
  Perform MAC authentication before 802.1X
  MAC authentication fail-thru

Accounting: Use authentication servers

Accounting interval: 0 min.

Blacklisting: Disabled

**Fast Roaming**

Opportunistic Key Caching(OKC):

802.11r:

802.11k:

802.11v:

- لخدمال نيوكتل ةكبشلالا إلى ةدننستسملال لوصولال ةدعاق ددح: "لوصولال" بيبوبتال ةمالع ةل SSID لعل لقلننتمال

ةدعاقال ةون رتخأ، ةديج قوف رقنا 1 ةوطخالل يف اهاننيوكتل مت يتال ةديقمال ةباوبال مدختسأ ةروصلال يف حضوم وه امك يجراخ: ةيادبال ةحفص ةون، لقلننتمال لخدمال

1 WLAN Settings 2 VLAN 3 Security 4 Access

### Access Rules

More Control

Role-based

Network-based

Unrestricted

Less Control

Access Rules (3)

- Enforce captive portal
- Allow any to all destinations
- Allow TCP on ports 1-20000 on server 10.48.17.235

Edit Rule Enforce captive portal

Rule type: Captive portal

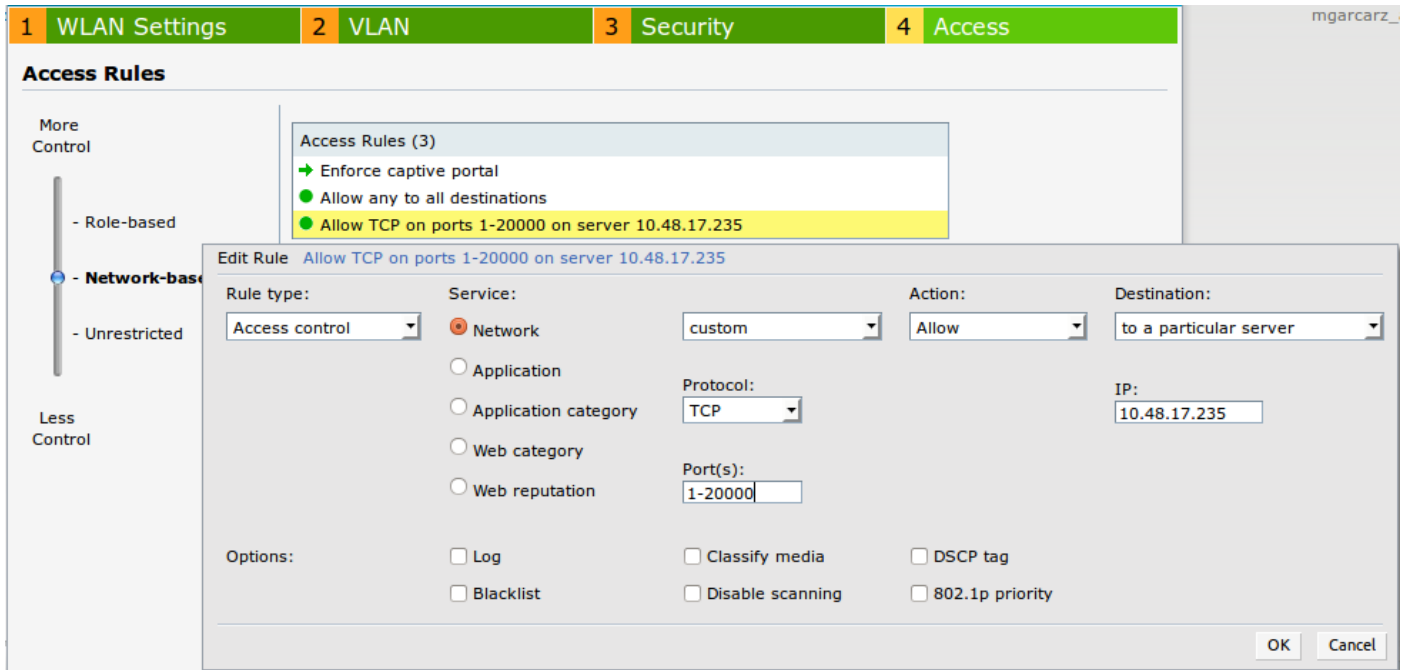
Splash page type: External

Captive portal profile: mgarcarz\_ise20

Edit

، (1-2000 قاطنلالا يف TCP ذفانم) ISE مداخب رورملا ةكرح ةيمجل حامسلا، كلذلى إلى ةفاضإلاب

ال أهجو يأل حامسلا نأ ودبي: Aruba ىلع يضارتفا لكشب انهنيوكت مت يتلا ةدعاقلا امنيب ةروصولا يف حضوم وه امك حيحص لكشب لمعي.



## ةحصلال نم ققحتلا

حيحص لكشب نيوكتلا لمع ديكأتل مسقلا اذه مدختسا

EAP-PEAP عم SSID Mgarcarz\_aruba ب لاصتالا 1. ةوطخلا

فلم عاجرا مت، يضارتفالا ةقداصملا جهن مادختسا مت. ISE ىلع ةقداصم لجس لوأ رهظي ةروصولا يف حضوم وه امك Aruba-redirect-BYOD ليوخت فيرعت.

Cisco Identity Services Engine										
RADIUS Livelog										
Time	Status	Det...	R.	Identity	Endpoint ID	Authentication Policy	Authorization Policy	Authorization Profiles	Network Device	Event
2015-10-29 22:23:37...	❌			0 cisco	C0:4A:00:14:6E:31	Default >> Dot1X >> EAP-TLS	Default >> Basic_Authenticated...	PermitAccess		Session State is Started
2015-10-29 22:23:37...	✅			cisco	C0:4A:00:14:6E:31	Default >> Dot1X >> EAP-TLS	Default >> Basic_Authenticated...	PermitAccess	aruba	Authentication succeeded
2015-10-29 22:19:09...	✅			cisco	C0:4A:00:14:6E:31	Default >> Dot1X >> Default	Default >> ArubaRedirect	Aruba-redirect-BYOD	aruba	Authentication succeeded

تامس يأ عاجرا متي ال هنأ طحال. EAP حاجنب RADIUS ىلإ لوصولا لوبق ةلاسرا ISE عجرت ىلإ لوصولا يف مكحتلا ةمئاق وأ Cisco نيوانع جوزل URL ناونع هيحوت ةداعإ دجوي ال) ةيفاضا ةروصولا يف حضوم وه امك (هيحوتلا ةداعإ-URL ناونع.

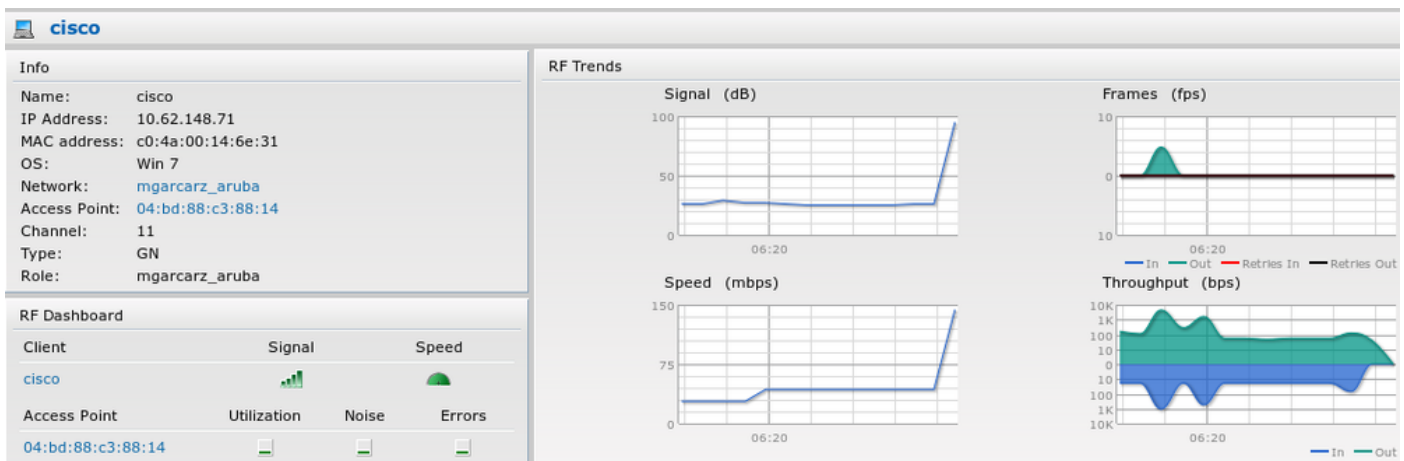
No.	Source	Destination	Protocol	Length	Info	User-Name	Acct-Session-Id
133	10.62.148.118	10.48.17.235	RADIUS	681	Access-Request(1) (id=102, l=639)	cisco	
134	10.48.17.235	10.62.148.118	RADIUS	257	Access-Challenge(11) (id=102, l=215)		
135	10.62.148.118	10.48.17.235	RADIUS	349	Access-Request(1) (id=103, l=307)	cisco	
136	10.48.17.235	10.62.148.118	RADIUS	235	Access-Challenge(11) (id=103, l=193)		
137	10.62.148.118	10.48.17.235	RADIUS	386	Access-Request(1) (id=104, l=344)	cisco	
138	10.48.17.235	10.62.148.118	RADIUS	267	Access-Challenge(11) (id=104, l=225)		
139	10.62.148.118	10.48.17.235	RADIUS	450	Access-Request(1) (id=105, l=408)	cisco	
140	10.48.17.235	10.62.148.118	RADIUS	283	Access-Challenge(11) (id=105, l=241)		
141	10.62.148.118	10.48.17.235	RADIUS	386	Access-Request(1) (id=106, l=344)	cisco	
142	10.48.17.235	10.62.148.118	RADIUS	235	Access-Challenge(11) (id=106, l=193)		
143	10.62.148.118	10.48.17.235	RADIUS	386	Access-Request(1) (id=107, l=344)	cisco	
149	10.48.17.235	10.62.148.118	RADIUS	363	Access-Accept(2) (id=107, l=321)	cisco	
150	10.62.148.118	10.48.17.235	RADIUS	337	Accounting-Request(4) (id=108, l=295)	cisco	04BD88888142-C04A00146E31-42F8
153	10.48.17.235	10.62.148.118	RADIUS	62	Accounting-Response(5) (id=108, l=20)		

```

Packet identifier: 0x6b (107)
Length: 321
Authenticator: 1173a3d3ea3d0798fe30fdaccf644f19
[This is a response to a request in frame 143]
[Time from request: 0.038114000 seconds]
Attribute Value Pairs
  AVP: l=7 t=User-Name(1): cisco
  AVP: l=67 t=State(24): 52656175746853657379696f6e3a30613330313165625862...
  AVP: l=87 t=Class(25): 434143533a30613330313165625862697544413379554e6f...
  AVP: l=6 t=EAP-Message(79) Last Segment[1]
  AVP: l=18 t=Message-Authenticator(80): e0b74092cacf88803dcd37032b761513
  AVP: l=58 t=Vendor-Specific(26) v=Microsoft(311)
  AVP: l=58 t=Vendor-Specific(26) v=Microsoft(311)

```

وهو يدعم الـ RADIUS و Cisco EAP-PEAP (وهو ما يُسمى بـ Aruba) في حوضه و هو امك mgarcarz\_aruba.



في هذه المقالة نناقش كيفية إعداد وإدارة RADIUS في Aruba (أو بشكل عام).

الخطوات لإعداد RADIUS في Aruba CLI، هي كما يلي:

```
<#root>
```

```
04:bd:88:c3:88:14#
```

```
show datapath user
```

```
Datapath User Table Entries
```

```

-----
Flags: P - Permanent, W - WEP, T- TKIP, A - AESCCM
      R - ProxyARP to User, N - VPN, L - local, I - Intercept, D - Deny local routing
FM(Forward Mode): S - Split, B - Bridge, N - N/A

```

IP	MAC	ACLs	Contract	Location	Age	Sessions	Flags	Vlan	FM
10.62.148.118	04:BD:88:C3:88:14	105/0	0/0	0	1	0/65535	P	1	N
10.62.148.71	C0:4A:00:14:6E:31	138/0	0/0	0	0	6/65535		1	B
0.0.0.0	C0:4A:00:14:6E:31	138/0	0/0	0	0	0/65535	P	1	B
172.31.98.1	04:BD:88:C3:88:14	105/0	0/0	0	1	0/65535	P	3333	B
0.0.0.0	04:BD:88:C3:88:14	105/0	0/0	0	0	0/65535	P	1	N

ةيلاحل تانوذألا لىل لوصولل 138 مقر (ACL) لوصولل يف مكحتل ةمئاق فرعم نم ققحتلل

<#root>

04:bd:88:c3:88:14#

show datapath acl 138

Datapath ACL 138 Entries

-----  
 Flags: P - permit, L - log, E - established, M/e - MAC/etype filter  
 S - SNAT, D - DNAT, R - redirect, r - reverse redirect m - Mirror  
 I - Invert SA, i - Invert DA, H - high prio, O - set prio, C - Classify Media  
 A - Disable Scanning, B - black list, T - set TOS, 4 - IPv4, 6 - IPv6  
 K - App Throttle, d - Domain DA  
 -----

```

1: any any 17 0-65535 8209-8211 P4
2: any 172.31.98.1 255.255.255.255 6 0-65535 80-80 PSD4
3: any 172.31.98.1 255.255.255.255 6 0-65535 443-443 PSD4

4: any mgarcarz-ise20.example.com 6 0-65535 80-80 Pd4

5: any mgarcarz-ise20.example.com 6 0-65535 443-443 Pd4

6: any mgarcarz-ise20.example.com 6 0-65535 8443-8443 Pd4 hits 37

7: any 10.48.17.235 255.255.255.255 6 0-65535 1-20000 P4 hits 18

```

<....some output removed for clarity ... >

يف حضوم وه امك رودلا اذهل ةي موسرللا مدختس مللا ةهجاو يف هنيوكت مت ام عم كلذ قفاوتي ةروصللا.

## Security

Authentication Servers | Users for Internal Server | Roles | Blacklisting | Firewall Settings | Inbound Firewall | Walled Garden

Roles

- default\_wired\_port\_profile
- wired-instant
- ArubaAAA
- wcecot\_BYOD\_aruba
- mgarcarz\_aruba**
- mgarcarz\_aruba\_tls

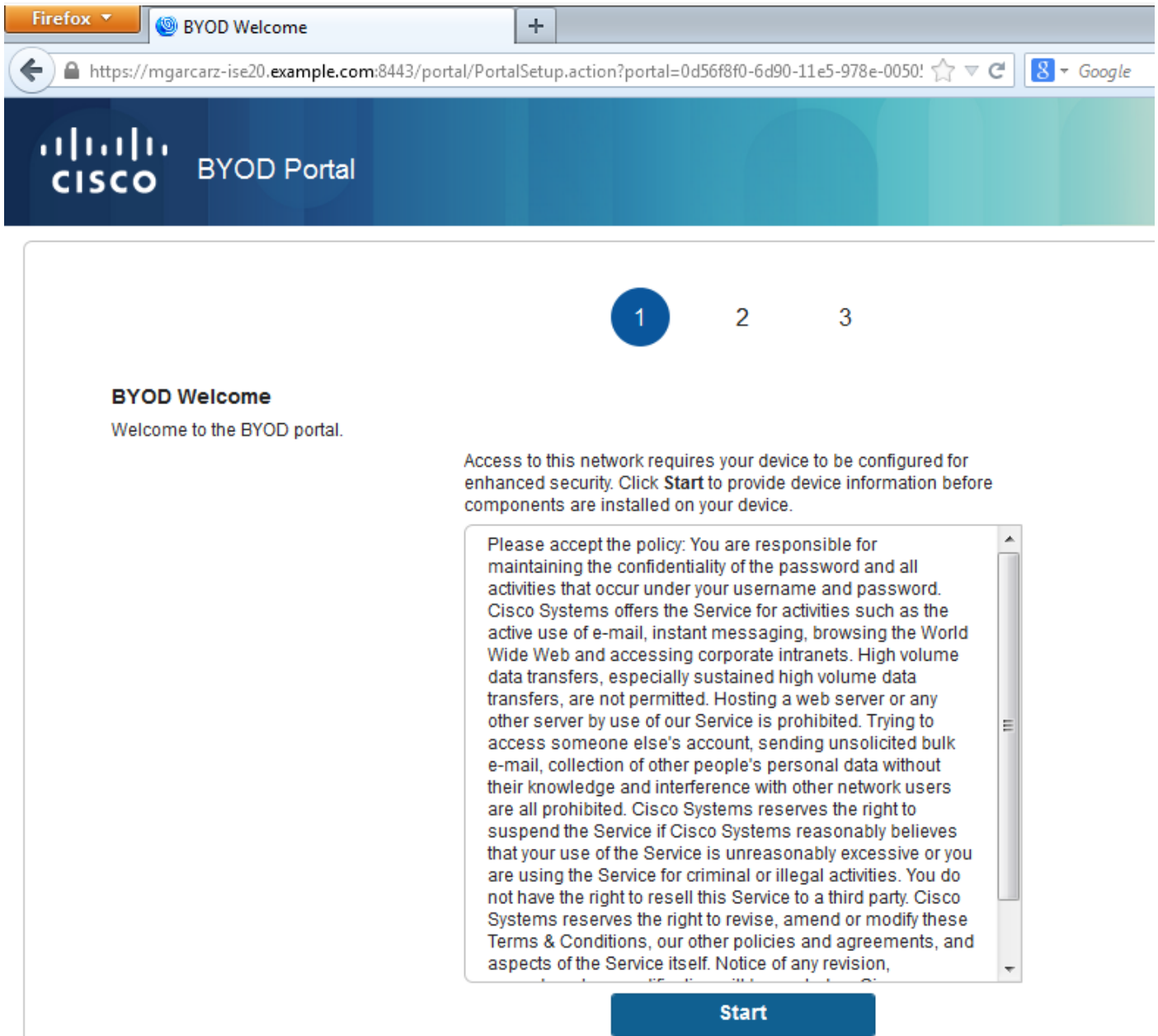
Access Rules for **mgarcarz\_aruba**

- Enforce captive portal
- Allow any to all destinations
- Allow TCP on ports 1-20000 on server 10.48.17.235

New Delete New Edit Delete ↑ ↓

BYOD ل بيولا حفصتم رورم ةكرح هيچوت ةداع | 2. ةوطخلا

ةي لمع ثدحت ، ناو نع يا ةباتك ب موقيو بيولا ضرعتسم حتفب مدختسم لا موقيو نا درجم ب ةروصلا يف حضورم وه امك هيچوتلا ةداع |

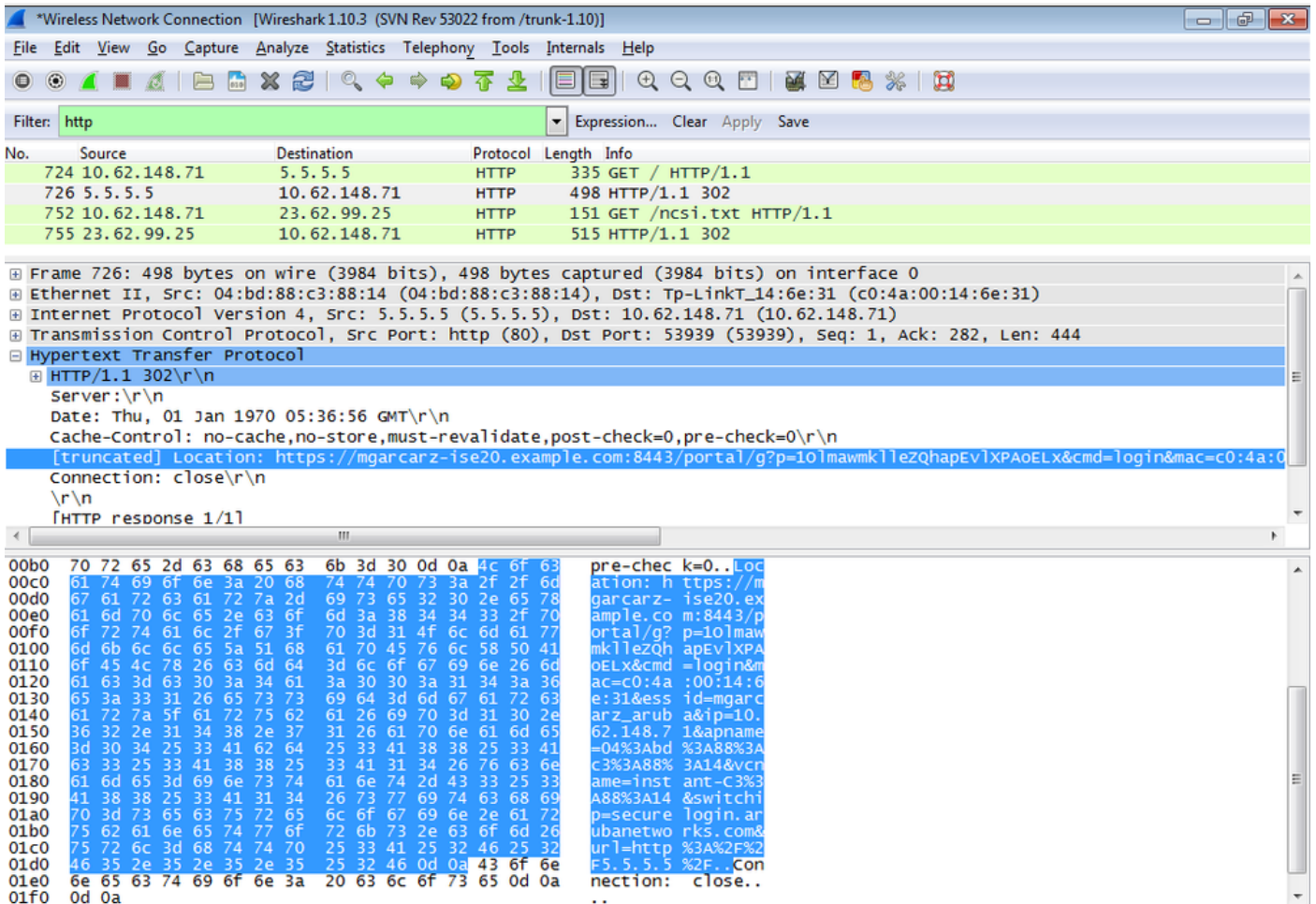


هيجوت ةداعإ ديعيو (5.5.5.5) ةهجولا عزتنې Aruba نأ دكؤملا نم ، ةمزحلا طاقتلا ىلإ رظنلاب HTTP ىلإ ISE.

Aruba - ىلع Captive لخدم ىلإ هخسنو ISE يف هنېوكت مت امك تباثلا URL سفن هنأ طحال ةروصلا يف حضورم وه امك ويلي امك ةددعت مت تاطيسو ةفاضإ مت ، لكذىلإ ةفاضإلاب نكلو:

- cmd = لوخدلا ليجست
- mac = c0:4a:00:14:6e:31
- ESSID = mgarcarz\_aruba
- ip = 10.62.148.7
- APNAME = 4bd88c38814 (mac)
- url = <http://5.5.5.5>





لثامي ةس لجال فشتك ي، id ةس لج Cisco تشعني نأ عي طتسي ISE، اتاطي سولا هذه ببسب قفدت (لكشي رخأ ي أ) BYOD عم عباتي و ISE لىل

نم موعدم ريغ اذه نكلو ةداع هم ادختسا متسي س audit\_session\_id ناك Cisco ةزهجأل ةبس نلابق نى رخأل نى دروملا لبق

ال يتلوا) Audit-session-id ةم يقي عاشن إرت نأ نكمملا نم، ISE ءاطخأ حيحصت نم كلذ ديكأتل (ةكبشلا ربع اقلطم اهل سلا متي

<#root>

```
AcSLogs,2015-10-29 23:25:48,538,DEBUG,0x7fc0b39a4700,cntx=0000032947,CallingStationID=c04a00146e31,FramedIPAddress=10.62.148.71,MessageFormatter::appendValue() attrName:cisco-av-pair appending value:
```

```
audit-session-id=0a3011ebXbiuDA3yUNoLUvtCRYuPFxkqYJ7TT06foOZ7G1HXj1M
```

2: ةحفص BYOD لىل زاهجلا ليجست دعب كلذ طبر، مئ نمو

<#root>

```
AcSLogs,2015-10-29 23:25:48,538,DEBUG,0x7fc0b39a4700,cntx=0000032947,CallingStationID=c04a00146e31,FramedIPAddress=10.62.148.71,Log_Message=[2015-10-29 23:25:48.533 +01:00 0000011874 88010 INFO
```

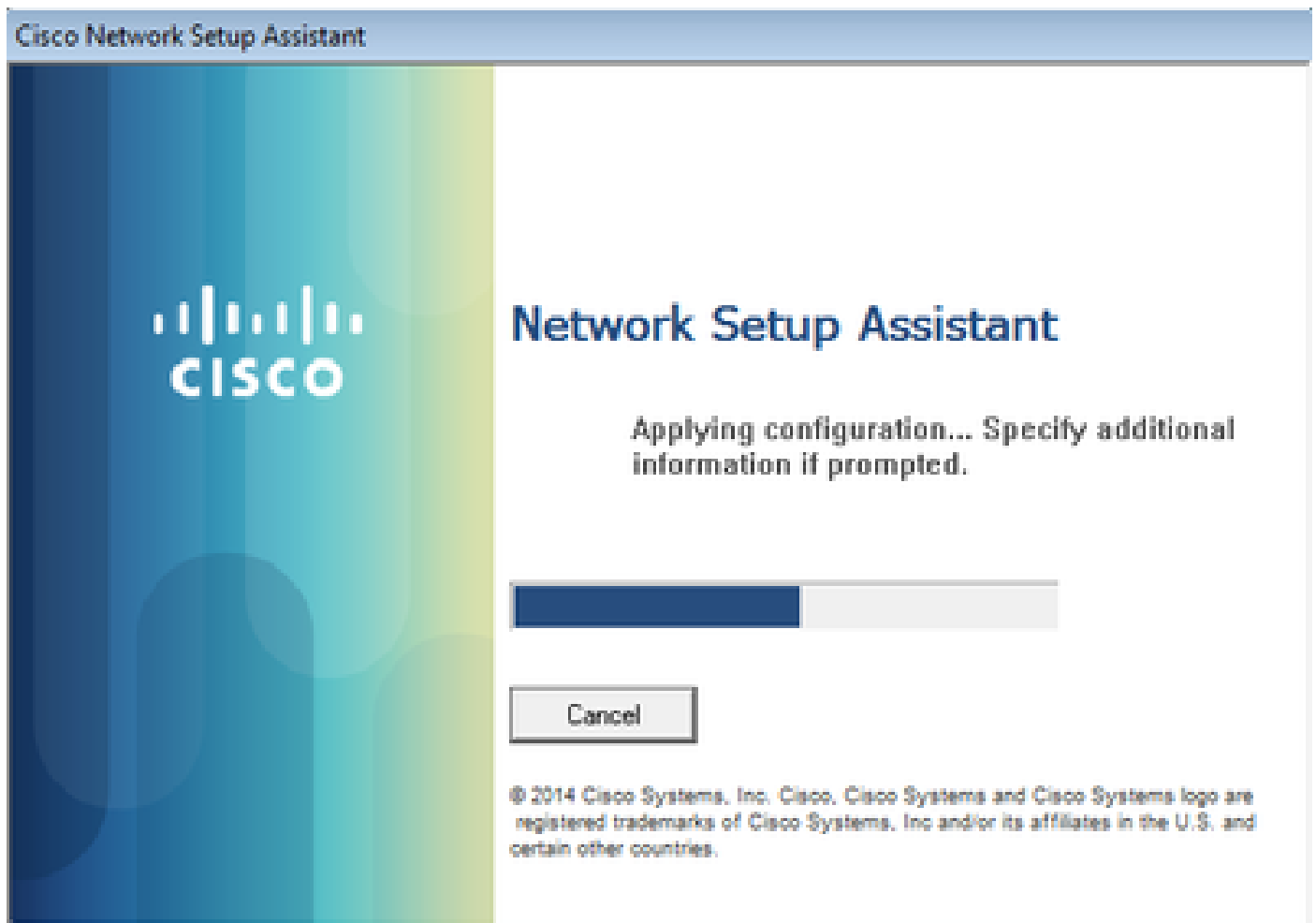
MyDevices: Successfully registered/provisioned the device

(endpoint), ConfigVersionId=145, UserName=cisco, MacAddress=c0:4a:00:14:6e:31, IpAddress=10.62.148.71, AuthenticationIdentityStore=Internal Users, PortalName=BYOD Portal (default), PsnHostName=mgarcarz-ise20.example.com, GuestUserName=cisco, EPMacAddress=C0:4A:00:14:6E:31, EPIIdentityGroup=RegisteredDevices Staticassignment=true, EndPointProfiler=mgarcarz-ise20.example.com, EndPointPolicy=Unknown, NADAddress=10.62.148.118, DeviceName=ttt, DeviceRegistrationStatus=Registered AuditSessionId=0a3011ebXbiuDA3yUNoLUvtCRyuPFxkqYJ7TT06foOZ7G1HXj1M, cisco-av-pair=

audit-session-id=0a3011ebXbiuDA3yUNoLUvtCRyuPFxkqYJ7TT06foOZ7G1HXj1M

ليزنت متي شيح 3. مقر BYOD ةحفص لى لى لمعل هيجوت ةداعإ متت ، ةقحلالا تاب لطلال يفو اهذيفنتو NSA.

ةكبشلال دادعإ دعاسم ذيفنت 3. ةوطخلا



متيو ISE ب صاخلا IP ناو نع فاشتكنا مزلي ،الوا ،ببول ضرعتسم ةمهم سفن NSA لىل HTTP هيجوت ةداعإ لالخنم كلذ قيقحت

ضرعتسم يف لالخال وه امك) IP ناو نع ةباتكل ةينام مدختسم لىل سئل تقولا اذه نأل اياقلا تانايبلا رورم ةكرح عاشن متي هناف ،(ببول

يف حضوره وه امك (اهم ادخ تس | نكمي login.cisco.com اضي) ة يضارت فالال ة ابو بلال مادختس | متي ة روصلال.

The image shows a Wireshark capture of network traffic. The filter is set to 'http'. The packet list shows two packets: packet 182 is a GET request for /auth/discovery, and packet 184 is the corresponding 302 response. The packet details pane for packet 182 shows the full request, including headers like User-Agent, Accept, and Host.

No.	Source	Destination	Protocol	Length	Info
182	10.62.148.71	10.62.148.100	HTTP	223	GET /auth/discovery HTTP/1.1
184	10.62.148.100	10.62.148.71	HTTP	520	HTTP/1.1 302

Frame 182: 223 bytes on wire (1784 bits), 223 bytes captured (1784 bits) on interface 0  
Ethernet II, Src: Tp-LinkT\_14:6e:31 (c0:4a:00:14:6e:31), Dst: Cisco\_f2:b1:42 (c4:0a:cb:f2:b1:42)  
Internet Protocol Version 4, Src: 10.62.148.71 (10.62.148.71), Dst: 10.62.148.100 (10.62.148.100)  
Transmission Control Protocol, Src Port: 55937 (55937), Dst Port: http (80), Seq: 1, Ack: 1, Len: 169  
Hypertext Transfer Protocol  
GET /auth/discovery HTTP/1.1\r\n  
User-Agent: Mozilla/4.0 (windows NT 6.1; compatible; Cisco NAC web Agent v.)\r\n  
Accept: \*/\*\r\n  
Host: 10.62.148.100\r\n  
Cache-Control: no-cache\r\n  
\r\n  
[Full request URI: http://10.62.148.100/auth/discovery]  
[HTTP request 1/1]  
[Response in frame: 184]

بيولا ضرعت سمل ة بس نلاب لال وه امك امامت اهس فن يه ة باحتس الال

نيوكت لالاب XML فيرعت فلم ىل لوصح لالاب ISE ب لالاصت الال NSA ل نكمي ة قيرطال هذبه  
ISE Internal CA نم ة قوم ة داهش ىل لوصح لالاب ISE ىل لالاسر ل SCEP ب ل ط عاشن ل  
هه نيوكت مت يذل SSID ب لالاصت الال اريخ لالاب فيرعت فلم نيوكت و

ضع ب فذح مت (%temp%/spwProfile.log في Windows ىل ع). ليمع الال نم تالچس الال عي مت  
حوضوت الال لچ ل نم تالچم الال

<#root>

```
Logging started
SPW Version: 1.0.0.46
System locale is [en]
Loading messages for english...
Initializing profile
SPW is running as High integrity Process - 12288
GetProfilePath: searched path = C:\Users\ADMINI~1\EXA\AppData\Local\Temp\ for file name = spwProfile.xml
GetProfilePath: searched path = C:\Users\ADMINI~1\EXA\AppData\Local\Temp\Low for file name = spwProfile
Profile xml not found Downloading profile configuration...

Downloading profile configuration...

Discovering ISE using default gateway

Identifying wired and wireless network interfaces, total active interfaces: 1
Network interface - mac:C0-4A-00-14-6E-31, name: Wireless Network Connection, type: wireless
Identified default gateway: 10.62.148.100

Identified default gateway: 10.62.148.100, mac address: C0-4A-00-14-6E-31
```

redirect attempt to discover ISE with the response url

DiscoverISE - start

Discovered ISE - : [mgarcarz-ise20.example.com, sessionId: 0a3011ebXbiuDA3yUNoLUvtCRyuPFxkqYJ7TT06fo0Z7

DiscoverISE - end

Successfully Discovered ISE: mgarcarz-ise20.example.com, session id: 0a3011ebXbiuDA3yUNoLUvtCRyuPFxkqYJ7

GetProfile - start

GetProfile - end

Successfully retrieved profile xml

using V2 xml version

parsing wireless connection setting

Certificate template: [keysize:2048, subject:OU=Example unit,O=Company name,L=City,ST=State,C=US, SAN:MA

set ChallengePwd

creating certificate with subject = cisco and subjectSuffix = OU=Example unit,O=Company name,L=City,ST=

Installed [LAB CA, hash: fd 72 9a 3b b5 33 72 6f f8 45 03 58 a2 f7 eb 27^M

ec 8a 11 78^M

] as rootCA

Installed CA cert for authMode machineOrUser - Success

HttpWrapper::SendScepRequest

- Retrying: [1] time, after: [2] secs , Error: [0], msg: [ Pending]

creating response file name C:\Users\ADMINI~1.EXA\AppData\Local\Temp\response.cer

Certificate issued - successfully

ScepWrapper::InstallCert start

ScepWrapper::InstallCert: Reading scep response file

[C:\Users\ADMINI~1.EXA\AppData\Local\Temp\response.cer].

ScepWrapper::InstallCert GetCertHash -- return val 1

ScepWrapper::InstallCert end

Configuring wireless profiles...

Configuring ssid [mgarcarz\_aruba\_tls]

WirelessProfile::SetWirelessProfile - Start

Wireless profile: [mgarcarz\_aruba\_tls] configured successfully

Connect to SSID

Successfully connected profile: [mgarcarz\_aruba\_tls]

WirelessProfile::SetWirelessProfile. - End

Cisco ةزهجأ عم BYOD ةي لم عمل ةبسنلاب لالحل وه امك امامت اهسفن يه تالجلسلا هذه

✎ لاصتالا ةداعإ ضرفي يذلا (NSA) قي بطتلا وهو. انه بولطم ريغ RADIUS CoA ةظالم اثيدح نوكم SSID ب.

إذ. يئاهن SSID فرعمب نارثقالا لواحي ماطنلا نأ يري نأ مدختسم لل نكمي، ةلحرمل هذه ي فو وه امك) ةححصلا ةداهشلا ديدحت كي لع بجيف، ةدحاو مدختسم ةداهش نم رثكأ كي دل ناك (حضوم).

### Select Certificate

User name on certificate:

cisco@example.com

cisco@example.com  
administrator@example.com  
cisco

Issuer: LAB CA

Expiration date: 7/17/2016 12:29:41 PM

OK Cancel View Certificate

ةروصللا ي ف حضوم وه امك NSA ريراقت ضرع متي، حجان لاصتلا دعب.



## Network Setup Assistant



Your device is now configured for secure access to the 'mgarcarz\_aruba\_tls' network.

Exit

© 2014 Cisco Systems, Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems, Inc and/or its affiliates in the U.S. and certain other countries.

عيج قباط يتل EAP-TLS ةقداصم يناتل لجلسل برضي - ISE لىل كلذ نم دكأتل نكمي (ححص لجلسل BYOD و، فظومل، ء Basic\_AUTHENTICATED\_ACCESS طورش).

Identity Services Engine										
RADIUS Livelog										
Misconfigured Supplicants: 1										
Misconfigured Network Devices: 0										
RADIUS Drops: 12										
Client Stopped Respond: 0										
Show Live Sessions										
Time	Status	Det...	R.	Identity	Endpoint ID	Authentication Policy	Authorization Policy	Authorization Profiles	Network Device	Event
2015-10-29 22:23:37...				0 cisco	C0:4A:00:14:6E:31	Default >> Dot1X >> EAP-TLS	Default >> Basic_Authenticated...	PermitAccess		Session State is Started
2015-10-29 22:23:37...				cisco	C0:4A:00:14:6E:31	Default >> Dot1X >> EAP-TLS	Default >> Basic_Authenticated...	PermitAccess	aruba	Authentication succeeded
2015-10-29 22:19:09...				cisco	C0:4A:00:14:6E:31	Default >> Dot1X >> Default	Default >> ArubaRedirect	Aruba-redirect-BYOD	aruba	Authentication succeeded

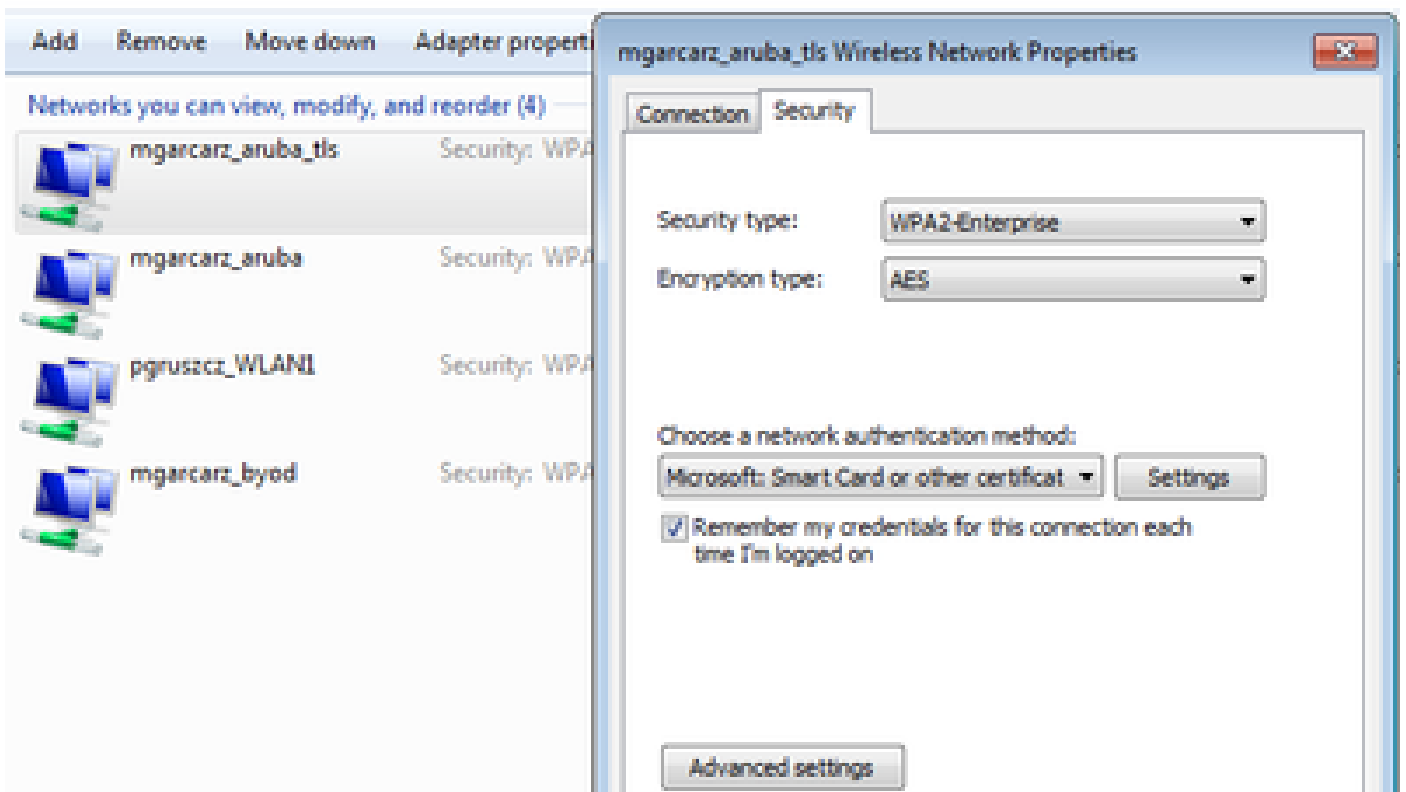
ةمالع لىل يوتحت ةياهنل ةطقن نأ ةيفرطال ةطقنل ءوه ضرع ةقيرط دكؤت نأ نكمي امك ءروصلل يف حضورم وه امك true لىل ءهنييت مت ةلجلسل BYOD.



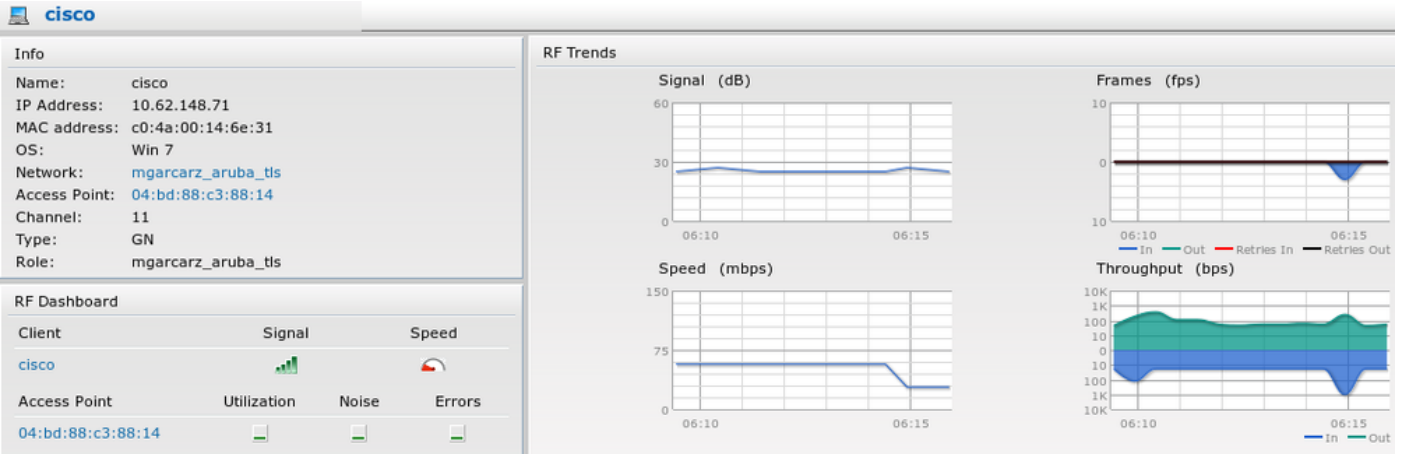
وهو (مات) لصفحة وحل الـ EAP-TLS (مات) في Windows PC.

### Manage wireless networks that use (Wireless Network Connection)

Windows tries to connect to these networks in the order listed below.



في هذه الحالة، سيتم محاولة الاتصال بالـ SSID mgarcarz\_aruba\_tls.



إلى لم اك ال لوصول ة ك ب ش ل م س ا س ف ن ه ت ي م س ت و ا ي ئ ا ق ل ت ه ؤ ا ش ن ا م ت ي ي ذ ل ا ر و د ل ا ر ف و ي ة ك ب ش ل ل .

### Security

Authentication Servers | Users for Internal Server | Roles | Blacklisting | Firewall Settings | Inbound Firewall

**Roles**

- default\_wired\_port\_profile
- wired-instant
- ArubaAAA
- wcecot\_BYOD\_aruba
- mgarcarz\_aruba
- mgarcarz\_aruba\_tls**

**Access Rules for mgarcarz\_aruba\_tls**

- Allow any to all destinations

New | Delete | New | Edit | Delete | ↑ | ↓

## CoA م عد و ي ر خ ا ت ا ق ف د ت

### CWA عم COa

ب ف ي ض ل ل ل خ د م عم CWA ق ف د ت ض ر ع م ت ي ، BYOD ق ف د ت ي ف COa ل ئ ا س ر د ج و ت ال ا م ن ي ب ا ن ه ا ي ت ا ذ ل ج س م ل :

ة ر و ص ل ل ي ف ح ز و م و ه ا م ك ا ه ن ي و ك ت م ت ي ت ل ل ل ي و خ ت ل ل د ع ا و ق .

<input checked="" type="checkbox"/>	Guest_Authenticate_internet	if <b>GuestEndpoints</b> AND Aruba:Aruba-Essid-Name EQUALS mgarcarz_aruba_guest	then PermitAccess
<input checked="" type="checkbox"/>	Guest_Authenticate_Aruba	if Aruba:Aruba-Essid-Name EQUALS mgarcarz_aruba_guest	then Aruba-redirect-CWA

ب ي و ل ا ت ا ح ف ص ض ع ب ب ل ا ص ت ا ل ل و ا ح ي ن ا د ر ج م ب و MAB ة ق د ا ص م ب SSID ب م د خ ت س م ل ل ص ت ي ، و ا د ي د ج ب ا س ح ء ا ش ن ا Guest ل ن ك م ي ث ي ح ، ا ي ت ا ذ ل ج س م ل Guest ل خ د م ل ا ه ي ج و ت ل ل ة د ا ع ا ث د ح ي . ي ل ل ا ح ب ا س ح م ا د خ ت س ا





## Sponsored Guest Portal

### Sign On

Welcome to the Guest Portal. Sign on with the username and password provided to you.

Username:

Password:

Sign On

[Don't have an account?](#)

قلاح رييغتلا ةكبشلا زاهج ىلا ISE نم CoA ةلاسرا لاسرا متي ،حاجنب فيضلا ليصوت دعبل ليوختلا.



## Sponsored Guest Portal

### Welcome Message

Click **Continue** to connect to the network.

You're very close to gaining network access.

Continue

ةروصللا في حضورم وه امك و Authtions > Operations نمض هنم ققحتلا نكمي.

cisco	C0:4A:00:15:76:34	Windows7-Workstat...	Default >> MAB	Default >> Guest_Authenticate_internet	Authorize-Only succeeded	PermitAccess
	C0:4A:00:15:76:34				Dynamic Authorization succe...	
cisco	C0:4A:00:15:76:34				Guest Authentication Passed	
C0:4A:00:15:76	C0:4A:00:15:76:34		Default >> MAB >> ...	Default >> Guest_Authenticate_Aruba	Authentication succeeded	Aruba-redirect-CWA

ISE: ءاطخأ حيحصت في CoA ةلاسرا

<#root>

```
2015-11-02 18:47:49,553 DEBUG [Thread-137] [] cisco.cpm.prtr.impl.PrRTLoggerImpl -:::-  
DynamicAuthorizationFlow,DEBUG,0x7fc0e9cb2700,cntx=0000000561,sesn=c59aa41a-e029-4ba0-a31b  
-44549024315e,CallingStationID=c04a00157634,[DynamicAuthorizationFlow::createCoACmd]  
Processing incoming attribute vendor , name
```

NAS-IP-Address, value=10.62.148.118

```
.,  
DynamicAuthorizationFlow.cpp:708  
2015-11-02 18:47:49,567 DEBUG [Thread-137] [] cisco.cpm.prvt.impl.PrRTLoggerImpl -:::::-  
DynamicAuthorizationFlow,DEBUG,0x7fc0e9cb2700,cntx=0000000561,sesn=c59aa41a-e029-4ba0-a31b-  
-44549024315e,CallingStationID=c04a00157634,[DynamicAuthorizationFlow::createCoACmd]  
Processing incoming attribute vendor , name
```

Acct-Session-Id, value=04BD88B88144-  
C04A00157634-7AD

```
.,DynamicAuthorizationFlow.cpp:708  
2015-11-02 18:47:49,573 DEBUG [Thread-137] [] cisco.cpm.prvt.impl.PrRTLoggerImpl -:::::-  
DynamicAuthorizationFlow,DEBUG,0x7fc0e9cb2700,cntx=0000000561,sesn=c59aa41a-e029-4ba0-a31b-  
-44549024315e,CallingStationID=c04a00157634,[DynamicAuthorizationFlow::createCoACmd]  
Processing incoming attribute vendor , name cisco-av-pair, v  
alue=audit-session-id=0a3011ebisZXypODwqjB6j64GeFiF7RwvyocneEia17ckjtU1HI.,DynamicAuthorizationFlow.cpp  
2015-11-02 18:47:49,584 DEBUG [Thread-137] [] cisco.cpm.prvt.impl.PrRTLoggerImpl -:::::-  
DynamicAuthorizationFlow,DEBUG,0x7fc0e9cb2700,cntx=0000000561,sesn=c59aa41a-e029-4ba0-a31b-  
-44549024315e,CallingStationID=c04a00157634,[DynamicAuthorizationRequestHelper::  
setConnectionParams]
```

defaults from nad profile : NAS=10.62.148.118, port=3799, timeout=5,

retries=2

```
.,DynamicAuthorizationRequestHelper.cpp:59  
2015-11-02 18:47:49,592 DEBUG [Thread-137] [] cisco.cpm.prvt.impl.PrRTLoggerImpl -:::::-  
DynamicAuthorizationFlow,DEBUG,0x7fc0e9cb2700,cntx=0000000561,sesn=c59aa41a-e029-4ba0-a31b-  
-44549024315e,CallingStationID=c04a00157634,[DynamicAuthorizationRequestHelper::set  
ConnectionParams] NAS=10.62.148.118, port=3799, timeout=5, retries=1,  
DynamicAuthorizationRequestHelper.cpp:86  
2015-11-02 18:47:49,615 DEBUG [Thread-137] [] cisco.cpm.prvt.impl.PrRTLoggerImpl -:::::-  
DynamicAuthorizationFlow,DEBUG,0x7fc0e9cb2700,cntx=0000000561,sesn=c59aa41a-e029-4ba0-a31b-  
-44549024315e,CallingStationID=c04a00157634,[DynamicAuthorizationFlow::onLocalHttpEvent]:
```

invoking DynamicAuthorization,DynamicAuthorizationFlow.cpp:246

ابوراً نم يچې بيللا لاثم تال لصف و

<#root>

```
2015-11-02 18:47:49,737 DEBUG [Thread-147] [] cisco.cpm.prvt.impl.PrRTLoggerImpl -:::::-  
DynamicAuthorizationFlow,DEBUG,0x7fc0e9eb4700,cntx=0000000561,sesn=c59aa41a-e029-4ba0-a31b-  
-44549024315e,
```

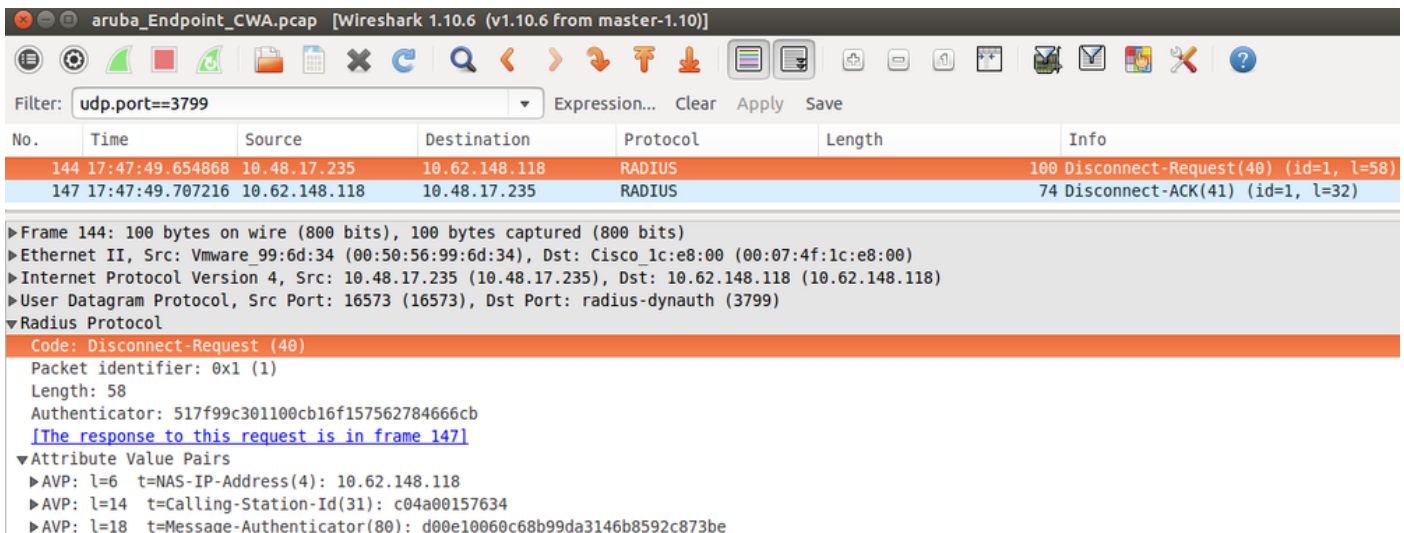
CallingStationID=c04a00157634

```
.,[DynamicAuthorizationFlow::  
onResponseDynamicAuthorizationEvent] Handling response  
ID c59aa41a-e029-4ba0-a31b-44549024315e, error cause 0,
```

Packet type 41(DisconnectACK).

```
,  
DynamicAuthorizationFlow.cpp:303
```

حضوره وه امك (41) Diconect-ACK و CoA Compact-Request (40) مادختساب ةمزحل طاقنل م تي.



No.	Time	Source	Destination	Protocol	Length	Info
144	17:47:49.654868	10.48.17.235	10.62.148.118	RADIUS		100 Disconnect-Request(40) (id=1, l=58)
147	17:47:49.707216	10.62.148.118	10.48.17.235	RADIUS		74 Disconnect-ACK(41) (id=1, l=32)

Code: Disconnect-Request (40)  
Packet identifier: 0x1 (1)  
Length: 58  
Authenticator: 517f99c301100cb16f157562784666cb  
[\[The response to this request is in frame 147\]](#)  
Attribute Value Pairs  
AVP: l=6 t=NAS-IP-Address(4): 10.62.148.118  
AVP: l=14 t=Calling-Station-Id(31): c04a00157634  
AVP: l=18 t=Message-Authenticator(80): d00e10060c68b99da3146b8592c873be

❏ ةيضا رت فال ا اءاع ا ا Aruba ب ةقل ةتم ل ةقءاصم ل RFC CoA مادختسا م ت: ةظءالم ةءاع ا تم ت ءق نوكت Cisco، زاهب ةقل ةتم ل ةقءاصم ل ةبسن ل اب. زاهل ء في رعت فل م Cisco CoA. ءون ةقءاصم

## اهءالص او ءاطءال فاش كتسا

اهءالص او نيوكنل ءاطءا فاش كتسا ل اهم اءختسا ل كنكمي تامول ءم مسقلا اءه رفوي

FQDN نم الءب IP ناو ن ءم ةءي قم ل Aruba ةب اوب

لش في ISE، ب ءصاءال FQDN نم الءب IP ناو ن ءب Aruba ل ءم ةءي قم ل ةب اوب ل نيوكنل م اءا PSN NSA:

<#root>

Warning - [HTTPConnection]

Abort the HTTP connection due to invalid certificate

CN

ناو ن ءم ءختست ام ءن ء. ISE ب لاصءال ءن ءءاهش ل ءءص نم قي قءءل ققءنل وه كل ءب بسو ءم اهمي ءق م تي و (FQDN نم الءب IP ناو ن ءب URL هي ءوت ءءاع ا ءءي ن) ISE ب لاصءال IP FQDN ءءص نم ققءنل لش ف = ءوضوم ل مساب ISE ءءاهش

❏ ةقءاوم ل ءاءءي ري ءءء راءص ا ءم) BYOD ةب اوب ءم بيول ا ضرءتسم ل صاوتي: ةظءالم (مءءتسم ل).

## ةديقملا ةباوبل حيحص ريغ لوصوحن

ةديقملا ةباوبل مادختساب هنيوكت مت يذل Aruba Access-Policy حمسي، يضا رتفا لكشب 8080 و 443 و 80 ذفانمب TCP ذفانمب.

مت ISE نم XML فيرعت فلم ىلع لوصحلل TCP 8905 ذفانمب لاصتالا NSA ل نكمي ال أطخلا اذه نع غالبال:

```
<#root>
```

```
Failed to get spw profile url using - url
```

```
[
```

```
https://mgarcarz-ise20.example.com:8905
```

```
/auth/provisioning/evaluate?
```

```
typeHint=SPWConfig&referrer=Windows&mac_address=C0-4A-00-14-6E-31&spw_version=1.0.0.46&session=0a3011ebXbiuDA3yUNoLUvtCRyuPFxkqYJ7TT06fo0Z7G1HXj1M&os=Windows A11]
```

```
- http Error: [2]
```

```
HTTP response code: 0
```

```
]
```

```
GetProfile - end
```

```
Failed to get profile. Error: 2
```

## Aruba CoA ذفانم مقرر

نم نكلو. CoA Air Group CoA 5999 ذفانم ذفانم مقرر Aruba رفوت، يضا رتفا لكشب (حضوم وه امك) تابللالا هذه لثمل بجتست مل 204 ابورا ةكرش نأ فسؤملا.

Event	5417 Dynamic Authorization failed
Failure Reason	11213 No response received from Network Access Device after sending a Dynamic Authorization request

## Steps

- 11201 Received disconnect dynamic authorization request
- 11220 Prepared the reauthenticate request
- 11100 RADIUS-Client about to send request - ( port = 5999 , type = RFC 5176 )
- 11104 RADIUS-Client request timeout expired (🕒 Step latency=10009 ms)
- 11213 No response received from Network Access Device after sending a Dynamic Authorization request

ةروصلال ي ف حضوم وه امك ةمزلال طاقتلال.

The image shows a Wireshark capture of a RADIUS Disconnect-Request packet. The packet list shows two packets: packet 685 is a RADIUS Disconnect-Request (40 bytes) and packet 686 is an ICMP Destination unreachable (Port unreachable) (128 bytes). The packet details for packet 685 show it is a RADIUS Disconnect-Request (40 bytes) with a packet identifier of 0xb (11) and a length of 58. The authenticator is 00b8961272015b5cecf27cc7f3e8fe81. The attribute value pairs include: AVP: l=6 t=NAS-IP-Address(4): 10.62.148.118, AVP: l=14 t=Calling-Station-Id(31): c04a00157634, and AVP: l=18 t=Message-Authenticator(80): 1959020d15fe2b0584b3a887c1e3c366.

RFC 5176 ي ف حضوم وه امك CoA 3977 ذفنم وه انه مادختسالل لرضألل رايلال نوكي نأ نكمي

Aruba ةزهجأ ضعب لىلع هيچوتلال ةداعإ

اليلق فلتخم لكشب لمعت هيچوتلال ةداعإ ةي لمع نأ ظحاليل ،6.3 رادصلإل عم Aruba 3600 ي ف انه احرشو ةمزلال طاقتلال لىلع روثعلال نكمي .ىرألل مكحتلال تادحو نع

No.	Time	Source	Destination	Protocol	Length	Info
770	09:29:40.5119116	10.75.94.213	173.194.124.52	HTTP	1373	GET / HTTP/1.1
772	09:29:40.5210656	173.194.124.52	10.75.94.213	HTTP	416	HTTP/1.1 200 Ok (text/html)
794	09:29:41.6982576	10.75.94.213	173.194.124.52	HTTP	63	GET /&arubaIp=6b0512fc-f699-45c6-b5cb-e62b3260e5 HTTP/1.1
797	09:29:41.7563066	173.194.124.52	10.75.94.213	HTTP	485	HTTP/1.1 302 Temporarily Moved

<#root>

packet 1: PC is sending GET request to google.com

packet 2: Aruba is returning HTTP 200 OK with following content:

<meta http-equiv='refresh' content='1; url=http://www.google.com/

&arubaIp=6b0512fc-f699-45c6-b5cb-e62b3260e5

'>\n

packet 3: PC is going to link with Aruba attribute returned in packet 2:

http://www.google.com/

&arubalp=6b0512fc-f699-45c6-b5cb-e62b3260e5

packet 4: Aruba is redirecting to the ISE (302 code):

https://10.75.89.197:8443/portal/g?p=4voD8q6W5Lxr8hpab77gL8VdaQ&cmd=login&

mac=80:86:f2:59:d9:db&ip=10.75.94.213&ssid=SC%2DWiFi&apname=LRC-006&apgroup=default&url=http%3A%2F%2Fwww

## ةلص تاذا تامولعم

- [2.0 رادصا، Cisco نم ةيوهلا تامدخ كرحم لوؤسم ليلد](#)
- [Cisco نم ةيوهلا تامدخ كرحم مادختساب ةكبش لال لوصولا زاغ فيرعت تافلّم](#)
- [Cisco Systems - تادنتس مل او ينقتلا معدلا](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذہ Cisco تچرت  
ملاعلاء انءمچي فني مدختسمل معدى وتحم مي دقتل ةيرشبل او  
امك ةقيقد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچري. ةصاخل مه تلبل  
Cisco يخلت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه  
ىل إأمئاد ةوچرلاب ي صؤت وتامچرتل هذه ةقد نع اهتيل وئسم Cisco  
Systems (رفوتم طبارل) ي لصلأل يزي لچن إل دن تسمل