

ثلاشلا فرطلاب صاخلا ISE 2.0 لماكت نيوكت مع Aruba Wireless

تاي وتحمل

[قمدقملا](#)

[قيس اس آلا تابلطتملا](#)

[تابلطتملا](#)

[قمدختس ملاباتانوكملا](#)

[نيوكتللا](#)

[كلب شيللي طخت لامس دللا](#)

[قيچرا خلاتا هاجلا مع دب قولي عتملا تاي دحفللا](#)

[تسا لجللا](#)

[ميوجوت قداعا URL](#)

[CoA](#)

[ايلع لج ISE](#)

[Cisco ISE](#)

[كلب شيللا قنهجأ دللا Aruba قيكلس اللالا مكحتلا ودحو فاضا 1. ووطخللا](#)

[ليوكتللا فيرعت فلام نيوكت 2. ووطخللا](#)

[وقدادص ملاب دعاوقة نيوكت 3. ووطخللا](#)

[سربر دتيشوس آبلورا](#)

[فديو قملاب اوبلاب نيوكت 1. ووطخللا](#)

[مداخ RADIUS 2. ووطخللا](#)

[لاب SSID نيوكت 3. ووطخللا](#)

[فتح كلابن قفتحتلا](#)

[ب ليصوتلا 1. ووطخللا SSID Mqarcarz arubawith EAP-PEAP](#)

[ل بىولاب حفص بت روم فكرح ميوجوت قداعا 2. ووطخللا BYOD](#)

[كلب شيللا دادعاب دعا سمخيفنت 3. ووطخللا](#)

[مع دوى رخأت اقفت CoA](#)

[CWA عم COa](#)

[احالص او عاطخألا فاشكتس](#)

[نم الدب IP Address ع قباوب FQDN](#)

[فديو قملاب اوبلاب Aruba جي حص، ريج لوص، وجهن](#)

[ذفنتم مقر Aruba CoA](#)

[قنهجأ ضعب ايلع ميوجوتلا قداعا Aruba](#)

[قلص تاذ تامولعم](#)

قمدقملا

ىلع احالص او ثلاشلا فرطلاب لماكت ةزييم عاطخأ فاشكتسأ ةيفيك دنتسملا اذه فصي
مع Cisco ISE.



ةيسيس اسألا تاپل طتملا

تابلطتما

- Aruba IAP نیوکت
 - BYOD ىلع قفدت ISE
 - ISE نیوکت ڈاچاصل مل ک اورورملا ڈاھن

ةم دختس ملا تان وكملا

ىلע احصالص او ثلاثلا فرطلال ماكت ئازيم ئاشكىتسا ئيفيك دنتسىملا اذه فصىي نم Cisco (ISE) ئىوهلا تامىد خىرەم.

Aruba ټس اوپ اه تردا مرت یتل اے کل ساللا ڈک بشلا جمد ڈی فیک حضوی نیوکت لاثم اذه IAP 204 ISE عوم چل لوطص حلل (BYOD) کب ڈس اخلا ڈزه جالا تامد خیل عوم.

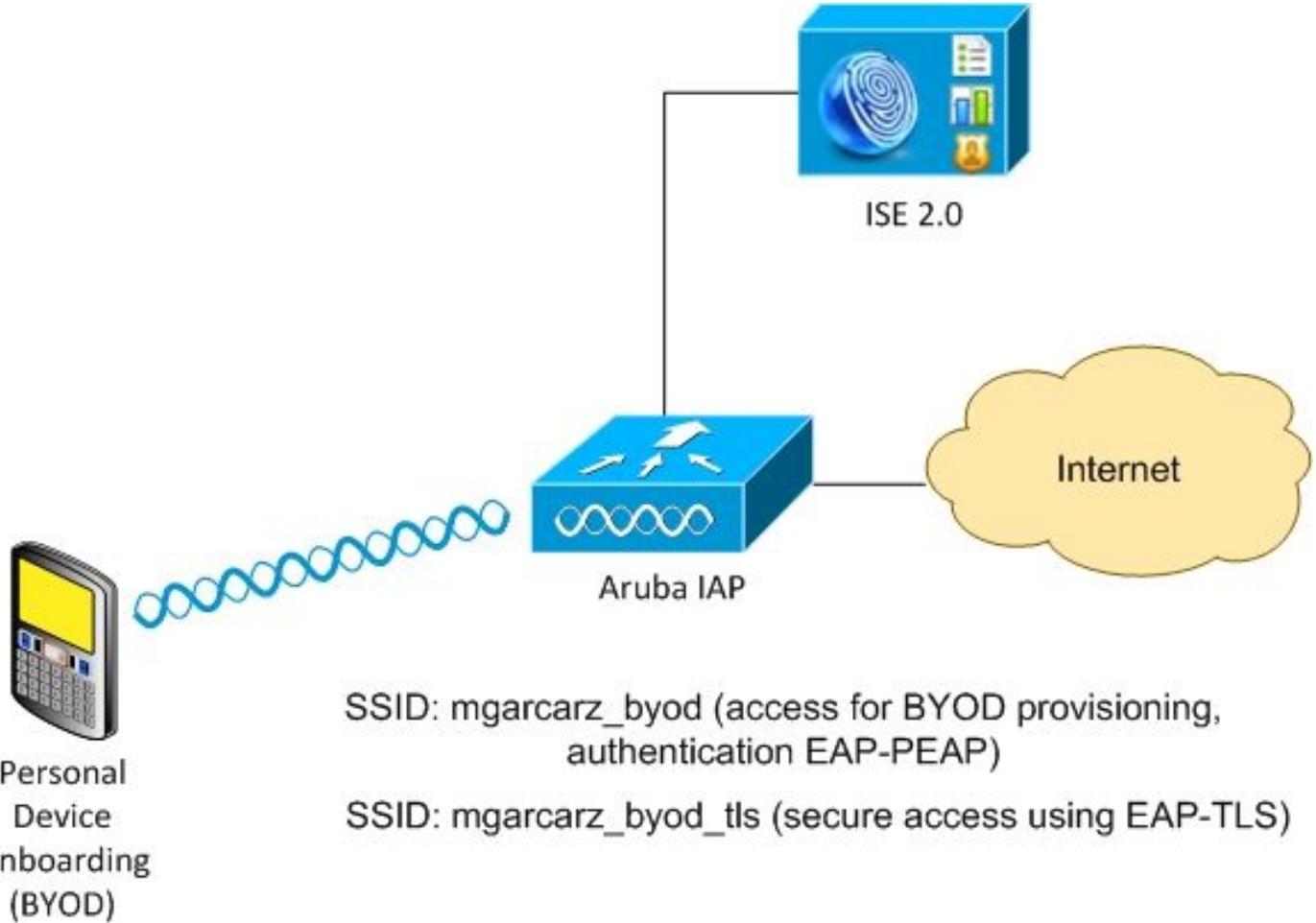
ءىلاتلا جماربلا تارادصا يلى دنتسىملا اذه يف ئدراولما تامولعملانىتست

- Cisco ISE 2.0 رادص إلأ او ثدح إلأ تارادص إلأ
 - Aruba IAP 204 6.4.2.3 جم ان رب

ڦڻا خ ڦيلمعم ڦئيپ يف ڦدوجوملا ڙزهچ ڳالا نم دنتس ملما اذه يف ڦدراولما تامولعملما ٽاشنإ مت
تناك اذا (يضارتفا) حوس مم نيوكت ب دنتس ملما اذه يف ڦمدختس ملما ڙزهچ ڳالا عيمج تأداب
رمأ ي ٻآل لمرتحملما ريرثأت لـ ڪمـ هـ فـ نـ مـ دـ ڪـ أـ تـ فـ ،ـ لـ يـ غـ شـ تـ لـ اـ دـ يـ قـ ڪـ تـ كـ بـ شـ

نیوکل

ةكبس للي طي طختلا مس رلا



ةطس او بامه ترادا مدت نيت يك لسال نيت كبس كانه Aruba AP.

ةقداص ملا لوك وربب يمحمل ا EAP ىلا لوصول (mgarcarz_byod) لوا لا راي خلا مدخلت سی عسو تمل (EAP-PEAP).

لخدم ىلا مدخلت سمل هيجوت ةداعاب Aruba يف مكحتلا ةدحو موقت نأ بجي، ٰحجان ةقداص م دعب ISE BYOD (NSP).

متي و (NSA) ةكبشلا دادع ا دعاسم قي بطب ذيفن متي و، مدخلت سمل هيجوت ةداع ا مدت ليمع ىلع اهتي بثت و ةداهشلا ريفوت Windows.

(ي ضارف الـ نـيـوـكـرـتـلـا) ةـيـلـمـعـلـاـ هـذـهـلـاـ ISEـ لـ يـلـخـادـلـاـ قـدـصـمـلـاـ عـجـرـمـلـاـ مـادـخـتـسـاـ مـتـيـ.

رادمل (SSID) يـنـاـثـلـاـ تـاـمـدـخـلـاـ ةـعـوـجـمـ فـرـعـمـلـ يـكـلـسـاـلـ فـيـصـوـتـ عـاـشـنـاـ نـعـ لـوـفـسـمـ نـأـ اـمـكـ ةـقدـاصـمـلـاـ لـوـكـوـرـبـ ةـقدـاصـمـلـ ـهـمـادـخـتـسـاـ مـتـيـ يـذـلـاوـ - لـقـنـلـاـ ةـقـبـطـ نـيـمـأـتـ - (EAP-TLS).

لوـصـحـلـاوـ يـصـخـشـ زـاهـجـ ىـلـاـ مـاـمـضـنـاـلـاـ ةـيـلـمـعـ ذـيـفـنـتـ ةـكـرـشـلـاـ مـدـخـتـسـمـلـ نـكـمـيـ،ـ كـلـذـلـ ةـجـيـتـنـ وـ ةـكـرـشـلـاـ ةـكـبـشـ ىـلـاـ نـمـآـ لـوـصـوـ ىـلـعـ.

لـاـثـمـلـاـ لـيـبـسـ ىـلـعـ،ـ فـلـتـخـمـلـاـ لـوـصـوـلـاـ عـاـونـأـلـ ةـلـوـهـسـبـ لـاـثـمـلـاـ اـذـهـ لـيـدـعـتـ نـكـمـيـ:

- بـيـوـلـلـ ةـيـزـكـرـمـلـاـ ةـقـدـاصـمـلـاـ (CWA) ةـمـدـخـ عـمـ BYOD
- وـعـضـوـلـاـ هـيـجـوـتـ ةـدـاعـاـعـ 802.1xـ رـايـعـمـلـ اـقـفـوـ ةـقـدـاصـمـ
- ـهـذـهـ بـظـافـتـحـاـلـلـ (EAP-PEAP) ةـقـدـاصـمـلـاـ ةـمـدـخـ مـادـخـتـسـاـ مـتـيـ اـمـ ةـدـاعـوـ

- رصت خملـا يـلـخـادـلـا ISEـا يـمـدـخـتـسـمـ مـادـخـتـسـا مـتـيـ،ـةـلـاقـمـلـاـ صـاخـلـاـ (SCEP)ـ يـجـرـاخـلـاـ طـيـسـبـلـاـ لـيـجـسـتـ لـوـكـوـتـورـبـ مـداـخـ مـادـخـتـسـاـ مـتـيـ،ـةـدـاعـوـ نـمـ (NDES)ـ ةـكـبـشـلـاـ ةـزـهـجـأـ لـيـجـسـتـ ةـمـدـخـ مـادـخـتـسـاـ مـتـيـ مـاعـ لـكـشـبـوـ،ـةـدـاهـشـلـاـ دـادـمـاـبـ Microsoftـ يـلـخـادـلـاـ ISEـCAـ مـادـخـتـسـاـ مـتـيـ اـمـكـ،ـةـرـيـصـقـ ةـلـاقـمـلـاـ هـذـهـ عـاقـبـإـلـ.

ةـيـجـرـاخـلـاـ تـاهـجـلـاـ مـعـدـبـ ةـقـلـعـتـمـلـاـ تـايـدـحـتـلـاـ

فـيـضـ تـاـقـفـدـتـ مـادـخـتـسـاـ دـنـعـ تـايـدـحـتـ دـجـوـتـ ثـلـاثـلـاـ فـرـطـلـاـ ةـزـهـجـأـ عـمـ Client Provisioning Portal (CPP)ـ.

تـاسـلـجـلـاـ

ىـمـسـمـلـاـ RADIUSـ جـوـزـ Ciscoـ نـمـ (NAD)ـ ةـكـبـشـلـاـ ئـلـاـ لـوـصـوـلـاـ ةـزـهـجـأـ مـدـخـتـسـتـ.ـةـسـلـجـلـاـ فـرـعـمـبـ (AAA)ـ ةـبـسـاحـمـلـاـوـ ضـيـوـفـتـلـاـوـ ةـقـدـاصـمـلـاـ مـداـخـ مـالـعـإـلـ.

لـكـلـ ةـحـيـحـصـلـاـ تـامـدـخـلـاـ رـيـفـوـتـوـ تـاسـلـجـلـاـ بـقـعـتـلـاـ ISEـ لـبـقـ نـمـ ةـمـيـقـلـاـ هـذـهـ مـادـخـتـسـاـ مـتـيـ جـوـزـ نـورـخـآـلـاـ نـوـدـوـمـلـاـ معـديـ إـلـ.ـقـفـدـتـ

ةـبـسـاحـمـلـاـ بـلـطـ وـلـوـصـوـلـاـ بـلـطـ يـفـ ةـمـلـتـسـمـلـاـ IETFـ دـمـتـعـيـ نـأـ بـجـيـ.

نـمـ Ciscoـ call-station-idـ نـمـ اـرـتـمـلـاـ فـرـعـمـ عـاـشـنـابـ ISEـ مـوـقـيـ،ـلـوـصـوـلـاـ بـلـطـ يـقـلـتـ دـعـبـ مـتـيـ إـلـ)ـ طـقـفـ ةـيـلـحـمـ ةـيـمـهـأـ اـهـلـ ةـمـيـقـلـاـ هـذـهـ (ـكـرـتـشـمـلـاـ رسـلـاـوـ NAS-Portـ،ـNAS-IP-addressـ).ـةـكـبـشـلـاـ رـبـعـ اـهـلـاسـراـ.

تـامـسـ قـافـرـابـ (BYODـ،ـ CWAـ،ـ NSPـ،ـ CPPـ)ـ قـفـدـتـ لـكـ مـوـقـيـ نـأـ عـقـوـتـمـلـاـ نـمـ،ـكـلـذـلـ ةـجـيـتـنـوـ ةـسـلـجـلـاـبـ هـطـبـرـلـ ثـحـبـ عـارـجـاـوـ Ciscoـ فـرـعـمـ بـاـسـحـ ةـدـاعـاـ نـمـ ISEـ نـكـمـتـيـ يـتـحـ -ـةـحـيـحـصـ قـفـدـتـلـاـ ةـعـبـاتـمـوـ ةـحـيـحـصـلـاـ.

هـيـجـوـتـ ةـدـاعـاـ URLـ

ةـرـوـضـبـ NADـ مـالـعـإـلـ url-redirectـ وـ url-redirect-aclـ Ciscoـ نـمـ RADIUSـ جـوـزـ url-redirectـ مـدـخـتـسـيـ ةـنـيـعـمـ رـوـرـمـ ةـكـرـحـ هـيـجـوـتـ ةـدـاعـاـ.

نـاـونـعـبـ ةـزـهـجـأـلـاـ هـذـهـ نـيـوـكـتـ بـجـيـ،ـةـدـاعـلـاـ يـفـ كـلـذـلـ Cisco-AVـ.ـ جـوـزـ نـورـخـآـلـاـ نـوـدـوـمـلـاـ معـديـ إـلـ URLـ ISEـ ئـلـعـ (ضـيـوـفـتـلـاـ فـيـرـعـتـ فـلـمـ)ـ ةـنـيـعـمـ ةـمـدـخـ ئـلـاـ رـيـشـيـ يـذـلـاـ هـيـجـوـتـلـاـ ةـدـاعـإـلـ تـبـاـثـ.

URLـ ئـلـاـ هـيـجـوـتـلـاـ دـيـعـتـ كـلـتـ NADsـ نـإـفـ،ـ HTTPـ ةـسـلـجـ ةـئـيـهـتـبـ مـدـخـتـسـمـلـاـ مـوـقـيـ نـأـ دـرـجـمـبـ ةـسـلـجـ فـيـرـعـتـبـ ISEـ حـامـسـلـلـ (MACـ نـاـونـعـ وـأـ IPـ نـاـونـعـ لـثـمـ)ـ ةـيـفـاـضـاـ تـاطـيـسـوـاضـيـأـ قـفـرـتـوـ قـفـدـتـلـاـ ةـعـبـاتـمـوـ ةـنـيـعـمـ.

CoA

رـمـأـ:ـكـرـتـشـمـ ،ـرـمـأـ:ـreauthentication-typeـ Cisco-AVـ RADIUSـ CISCO-AVـ جـوـزـ كـرـتـشـمـ ةـنـيـعـمـ لـمـعـ ةـسـلـجـلـاـهـذـخـتـتـ نـأـ بـجـيـ يـتـلـاـ تـاءـاـرـجـإـلـاـ ئـلـاـ ةـرـاشـإـلـلـ.

وـأـ RFCـ CoAـ (3576ـ)ـ ةـزـهـجـأـلـاـ هـذـهـ مـدـخـتـسـتـ،ـةـدـاعـ كـلـذـلـ Cisco-AVـ.ـ جـوـزـ نـورـخـآـلـاـ نـوـدـوـمـلـاـ معـديـ إـلـ 5176ـ:ـةـدـدـحـمـلـاـ لـئـاسـرـلـاـ ئـدـحـاـوـ.

- عطقل بلطلا اذه مدخلتسى - (لاصتالا عطق ةمزح اضيأ مىسى) لاصتالا عطق بلط
لاصتالا ةداعا ضرفل ابلاغ) لمعلالا ةسلج لاصتا
- لاصتالا عطق نود ئيفافشب لمعلالا ةسلج ةلاح رئيغتل كلذ مادخلتسا! متي - عفد
ةدىدج (ACL) لوصولاي ف مكحت ةمئاق قيبطتو VPN ةسلج، لاثملالا ليبس ىلع)

نام الك اضيأو Cisco CoA جوز عم Cisco-AV RFC CoA 3576/5176.

ح اىلع ISE

يذلا ئكبشلا ةزهجأ فيرعت تافلم موهفم 2.0 ISE تمدق، ئيجراخلا تاهجلا يدروم معدلجأ نام و، هيجوتلا ةداعإ URL و، لمعلالا تاسلح معدمتى فيك - ددحملالا دروملا فرصتى فيك فرصي CoA.

ةقداصملالا ثدحت نأ درجمبوا (ئكبشلا زاهج فيصوت) نيعمعون نام ليوطتلاتافيصوت نوكت فيصوتلا كلذ نام ISE كولس قاقتشا متى.

نأ امك ISE. ئمدخ ئطساوب ئلوهسب نيرخآ نيدروم نام ئدراولا ةزهجألا ئرادا نكمي، كلذ ئجيتن وأ ئدىدجلالا ئكبشلا ةزهجأ تافيصوت طبضب حمسىو ئنورملاب مسستى ISE اىلع نيوكتلا اهؤاشنا.

زاهجيضارتفالا فيرعتلما فلم مادخلتسا! ئلاقملالا هذه ضرعت

:ةزيملا لوح تامولعملانم ديزم

[Cisco نام ئيوجلا تامدخ كرحم مادخلتسا! ئكبشلا اىلاروصولالا زاهج فيرعت تافلم](#)

Cisco ISE

ةكبشلا ةزهجأ ايل ارuba ئيكليساللا مكحتلارا ةدحو ةفاضا 1. ئوطخلالا

دروملل حيحص زاهج فيرعت فلم رتختأ. ئكبشلا ةزهجأ > ئكبشلا دراوم > ئرادا ايل ارقتنان وه امك ئانيم CoA و كرتشم يرس لكشى نأ تنمض. ArubaWireless: ئلاحلا هذه يف، ددحملالا روصولاي ف حضوم.

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 HEXADECIMALCoA Port

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

ليوختلا فيرعت فلم نيوكت 2. ٖوطخلأ

لیوختلا فیرعت تافلم > جئاتنلا > ئاسایسلا رصانع > ئاسایسلا ىلإ لقتنا
فیرعتلا فلم ۋە ئاسایسلا ىلإ لقتنا > ئاسایسلا ىلإ لقتنا
فیرعتلا فلم ۋە ئاسایسلا ىلإ لقتنا > ئاسایسلا ىلإ لقتنا

Authorization Profiles > Aruba-redirect-BYOD

Authorization Profile

* Name	Aruba-redirect-BYOD
Description	
* Access Type	ACCESS_ACCEPT
Network Device Profile	ArubaWireless

Common Tasks

- Web Redirection (CWA, MDM, NSP, CPP)

Native Suplicant Provisioning	Value	BYOD Portal (default)
-------------------------------	-------	-----------------------

Advanced Attributes Settings

Select an item	=		-	+
----------------	---	--	---	---

Attributes Details

Access Type = ACCESS_ACCEPT

فیرعت فلمل تباث طابترا عاشنا متي ثيچ، بىوھيچوت ۋە داعا نىوكت نم دوقىم عز كانه، فييىضلى لخدمل يكيمانىدلا ھيچوتلا ۋە داعا معدت ال Aruba نأ نم مغىرلا ىلע. لیوختلا وە امك ىلع كىلذ دىع بىنۇوكت متي يىذلار، لیوخت فیرعت فلم لىكل نىعوم دح او طابترا ۋە روصىلا يف حضوم.

Common Tasks

Native Suplicant 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=1OlmawmkleZQhapEvlXPAoELx>

ۋە داعا نىوكت 3. ۋە ئاسایسلا ىلإ لقتنا

روصلار يف حضوم وە امك نىوكتلا متي وضيوفتلا داعا > ئاسایسلا ىلإ لقتنا.

<input checked="" type="checkbox"/>	Basic_Authenticated_Access	if Employee AND (EAP-TLS AND EndPoints:BYODRegistration EQUALS Yes)	then PermitAccess
<input checked="" type="checkbox"/>	ArubaRedirect	if Aruba:Aruba-Essid-Name EQUALS mgarcarz_aruba	then Aruba-redirect-BYOD

لیوختلا فیرعت فلم عجرت مل ا لصتی ، الـAruba-redirect-BYOD لامتكا دعب . یضارتفا لـBYOD ہیجوت دیمعلا لـBYOD یـBYOD، کـکـبـشـلـاـ لـMـاـکـلـاـ لـWـوـصـوـلـاـ لـصـتـیـ .

یـلـیـ اـمـکـ ةـسـایـسـلـاـ سـفـنـ وـدـبـتـ دـقـ ISE نـمـ ثـدـحـأـلـاـ تـارـادـصـإـلـاـ یـفـ .

The screenshot shows the Aruba ISE Policy Elements interface. At the top, there are tabs for Policy Sets, Profiling, Posture, Client Provisioning, and Policy Elements. The Policy Elements tab is selected. Below the tabs, there are columns for Status, Policy Set Name, Description, and Conditions. A search bar is present above the table.

Status	Policy Set Name	Description	Conditions	Actions
<input checked="" type="checkbox"/>	Aruba		Aruba:Aruba-Essid-Name EQUALS mgarcarz_aruba	Default Network Access

Below the table, there are sections for Authentication Policy (1), Authorization Policy - Local Exceptions, Authorization Policy - Global Exceptions, and Authorization Policy (3). The Authorization Policy (3) section is expanded, showing three rules:

- Authorized:** AND condition: example.com-External/Groups EQUALS example.com/Builtin/Administrators; EndPoints-BYODRegistration EQUALS Yes; Network Access-EapAuthentication EQUALS EAP-TLS. Result: PermitAccess.
- Redirect:** Condition: Aruba:Aruba-Essid-Name EQUALS mgarcarz_aruba. Result: Aruba_Redirect_BYOD.
- Default:** Result: DenyAccess.

سـربـ دـتـیـشـوـسـأـ اـبـوـرـاـ

ةـدـيـقـمـلـاـ ةـبـاوـبـلـاـ نـيـوـكـتـ . 1. ةـوـطـخـلـاـ

ةـیـجـرـاخـلـاـ ةـدـيـقـمـلـاـ ةـبـاوـبـلـاـ > نـامـأـلـاـ لـقـتـنـاـ , 204 یـلـعـ ةـدـيـقـمـلـاـ ةـبـاوـبـلـاـ نـيـوـكـتـلـ . رـوـصـلـاـ یـفـ حـضـوـمـ وـهـ اـمـکـ وـبـسـانـمـلـاـ نـيـوـكـتـلـلـ تـامـوـلـعـمـلـاـ هـذـهـ لـخـأـ . ةـدـيـجـ ةـبـاوـبـ تـفـضـأـوـ .

- ةـقـدـاصـمـ عـونـلـاـ RADIUS
- IP مـداـخـ : فـيـضـمـلـاـ مـسـاـ وـأـ ISE
- URL: صـاخـ وـهـ ؛ لـیـوـخـتـلـاـ فـيـرـعـتـ فـلـمـ نـيـوـكـتـ نـمـضـ ISE یـلـعـ ھـؤـاشـنـاـ مـتـیـ يـذـلـاـ طـابـتـرـالـاـ بـیـوـلـاـ ہـیـجـوـتـ ۃـدـاعـاـ نـيـوـكـتـ نـمـضـ انـھـ ہـیـلـعـ روـثـعـلـاـ نـکـمـیـ وـنـیـعـمـ لـیـوـخـتـ فـلـمـبـ

Native Suplicant 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=10lmawmkleZQhapEvIXPaoELx>

- لـکـشـبـ (ISE) یـلـعـ ہـیـلـعـ دـدـحـمـلـاـ لـخـدـمـلـاـ ةـفـاضـتـسـاـ مـتـیـ ذـلـاـ ذـفـنـمـلـاـ مـقـرـ (ذـفـنـمـلـاـ) . رـوـصـلـاـ یـفـ حـضـوـمـ وـهـ اـمـکـ (8443: یـضارـتـفـاـ).

mgarcarz_ise20

Type:	Radius Authentication
IP or hostname:	mgarcarz-ise20.example.
URL:	/portal/g?p=Kjr7eB7RrrLl
Port:	8443
Use https:	Enabled
Captive Portal failure:	Deny internet
Automatic URL Whitelisting:	Disabled
Redirect URL:	(optional)

OK **Cancel**

مدادخ نیوکت 2. ۋەطخلا RADIUS

ىلע هنیوکت مىت يىذلا هسفن وە COa ذفنم نأ نم دكأت ۋەقىداصملە مدادخ > نامألا ئىلا لىقتنا
رۇصلالا يىف حىضوم وە امك ISE.

عەم قىفاوتت ال، كىلذۇمۇ، 5999 ىلۇغ اهنېيىعت مىتى، Aruba 204، يىف، يىضاارتىفاللىكشىب و
5176 ISE.

Security

Authentication Servers	Users for Internal Server	Roles	Blacklisting
------------------------	---------------------------	-------	--------------

Edit

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

لخدمـا" رـايـتـخـاـلاـ ةـنـاخـ دـيـدـحـتـبـ اـضـيـأـ مـقـ ،ـثـدـحـأـلـاـ رـادـصـإـلـاـ اوـ Arubaـ نـمـ 6.5ـ رـادـصـإـلـاـ يـفـ ظـحـاـلـمـ "ـنـمـضـمـلـاـ".

3. ةـوطـخـلـاـ نـيـوـكـتـ SSIDـ

- رـوـصـلـاـ يـفـ حـضـوـمـ نـيـمـأـتـلـاـ بـيـوـبـتـ ئـمـالـعـ.

Edit mgarcz_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: mgarcz_ise20 Edit Authentication server 2: -- Select Server -- Reauth interval: 0 hrs. Authentication survivability: Disabled MAC authentication: <input type="checkbox"/> Perform MAC authentication before 802.1X <input type="checkbox"/> MAC authentication fail-thru Accounting: Use authentication servers Accounting interval: 0 min. Blacklisting: Disabled
Fast Roaming Opportunistic Key Caching(OKC): <input type="checkbox"/> 802.11r: <input type="checkbox"/> 802.11k: <input type="checkbox"/> 802.11v: <input type="checkbox"/>	

- لخدملا نيوكتل ةكبشلا يلإ ةدنتسملا لوصولـا ةدعـاق دـرح: "لـوصـولـا" بـيـوبـتـلـا ئـمـالـعـ ئـلـعـ لـقـنـتـمـلـا SSID.

ةـدعـاقـلـا عـونـ رـتـخـأـ ،ـديـجـ قـوـفـ رـقـنـاـ .ـةـوطـخـلـاـ يـفـ اـهـنـيـوـكـتـ مـتـ يـتـلـاـ ةـدـيـقـمـلـاـ ئـبـاـوـبـلـاـ مـدـخـتـسـأـ ئـرـوـصـلـاـ يـفـ حـضـوـمـ وـهـ اـمـكـ يـجـراـخـ :ـةـيـادـبـلـاـ ئـحـفـصـ عـونـ ،ـلـقـنـتـمـلـاـ لـخـدمـلـاـ.

1 WLAN Settings 2 VLAN 3 Security 4 Access

Access Rules

More Control - Role-based - Network-based - Unrestricted Less Control	<div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 10px;"> Access Rules (3) <ul style="list-style-type: none"> ➔ Enforce captive portal ● Allow any to all destinations ● Allow TCP on ports 1-20000 on server 10.48.17.235 </div> <div style="border: 1px solid #ccc; padding: 5px; background-color: #f0f0f0;"> Edit Rule Enforce captive portal </div> <table border="0"> <tr> <td style="width: 33%;">Rule type:</td> <td style="width: 33%;">Splash page type:</td> <td style="width: 33%;">Captive portal profile:</td> </tr> <tr> <td>Captive portal</td> <td>External</td> <td>mgarcz_ise20 Edit</td> </tr> </table>	Rule type:	Splash page type:	Captive portal profile:	Captive portal	External	mgarcz_ise20 Edit
Rule type:	Splash page type:	Captive portal profile:					
Captive portal	External	mgarcz_ise20 Edit					

قـاطـنـلـاـ يـفـ TCPـ ذـفـانـمـ (ISEـ)ـ مـدـاخـبـ روـمـلـاـ ةـكـرـحـ عـيـمـجـ حـامـسـلـاـ ،ـكـلـذـ يـلـإـ ئـفـاضـإـلـابـ.

ال ةهجو يأْ حامسلا نأْ ودبـي: Aruba: ىـلـع يـصـارـتـفـا لـكـشـبـ اـهـنـيـوـكـتـ مـتـ يـتـلـا ـةـدـعـاـقـلـا اـمـنـيـبـ ـةـرـوـصـلـا يـفـ حـضـوـمـ وـهـ اـمـكـ حـيـحـصـ لـكـشـبـ لـمـعـيـ.

The screenshot shows the Aruba Access Rules configuration interface. The top navigation bar has tabs: 1 WLAN Settings, 2 VLAN, 3 Security, and 4 Access. The 'Access' tab is selected. On the left, there's a sidebar with 'More Control' at the top, followed by 'Role-based', 'Network-based' (which is selected), and 'Unrestricted'. Below that is 'Less Control'. The main area shows 'Access Rules (3)' with three items: 'Enforce captive portal', 'Allow any to all destinations', and 'Allow TCP on ports 1-20000 on server 10.48.17.235'. A yellow box highlights the third item. Below this is a detailed 'Edit Rule' dialog for 'Allow TCP on ports 1-20000 on server 10.48.17.235'. The dialog fields are: Rule type: Access control, Service: Network, Action: Allow, Destination: to a particular server (IP: 10.48.17.235). Under 'Protocol': TCP, under 'Port(s)': 1-20000. Under 'Options': Log (unchecked), Classify media (unchecked), DSCP tag (unchecked), Blacklist (unchecked), Disable scanning (unchecked), 802.1p priority (unchecked). At the bottom right are 'OK' and 'Cancel' buttons.

ـحـصـلـا نـمـ قـقـحـتـلـا

ـحـصـلـا نـيـوـكـتـلـا لـمـعـ دـيـكـأـتـلـ مـسـقـلـا اـذـهـ مـدـخـتـسـا.

ـحـصـلـا نـيـوـكـتـلـا بـ لـاصـتـالـا 1. ـوـطـخـلـا EAP-PEAP مـعـ SSID Mgarcarz_aruba

ـفـلـمـ عـاجـرـاـ مـتـ ،ـيـصـارـتـفـاـ لـمـعـ ـقـدـاـصـمـلـاـ جـهـنـ مـادـخـتـسـاـ مـتـ. ISE: ـىـلـعـ ـقـدـاـصـمـ لـجـسـ لـوـأـ رـهـظـيـ. ـرـوـصـلـاـ يـفـ حـضـوـمـ وـهـ اـمـكـ Aruba-redirect-BYODـ لـيـوـخـتـ فـيـرـعـتـ.

The screenshot shows the Cisco Identity Services Engine (ISE) RADIUS LiveLog interface. The top navigation bar includes Home, Operations, Policy, Guest Access, Administration, and Work Centers. The 'Operations' tab is selected. Below it, the 'RADIUS LiveLog' tab is active. The log displays four categories: Misconfigured Suplicants (1), Misconfigured Network Devices (0), RADIUS Drops (12), and Client Stopped Respond (0). The main table lists RADIUS sessions with columns: Time, Status, Det., R, Identity, Endpoint ID, Authentication Policy, Authorization Policy, Authorization Profiles, Network Device, and Event. The table shows three entries: 1. Session started for user 'cisco' with endpoint 'C0:4A:00:14:6E:31' using 'Default >> Dot1X >> EAP-TLS' policy, authorized via 'Basic_Authenticated...' and 'PermitAccess', session state is 'Started'. 2. Session succeeded for user 'cisco' with endpoint 'C0:4A:00:14:6E:31' using 'Default >> Dot1X >> EAP-TLS' policy, authorized via 'Basic_Authenticated...', 'PermitAccess', network device 'aruba', and event 'Authentication succeeded'. 3. Session succeeded for user 'cisco' with endpoint 'C0:4A:00:14:6E:31' using 'Default >> Dot1X >> Default' policy, authorized via 'ArubaRedirect', network device 'aruba', and event 'Authentication succeeded'.

ـتـامـسـ يـأـ عـاجـرـاـ مـتـيـ الـ هـنـأـ ظـحـالـ EAPـ حـاجـنـبـ RADIUSـ ـىـلـاـ لـوـصـولـاـ لـوـبـقـ ـةـلـاسـرـ ISEـ عـجـرـتـ ـىـلـاـ لـوـصـولـاـ يـفـ مـكـحـتـلـاـ ـقـمـئـاـقـ وـأـ نـيـوـانـعـ جـوـزـلـ Ciscoـ URLـ نـاـونـعـ ـهـيـجـوـتـ ـةـدـاعـ ـدـجـوـيـ الـ (ـيـفـاـضـاـ). ـرـوـصـلـاـ يـفـ حـضـوـمـ وـهـ اـمـكـ (ـيـجـوـتـلـاـ ـةـدـاعـ ـعـرـفـاـ) URLـ ـةـدـاعـ ـعـرـفـاـ.

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)	cisco	
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)	cisco	
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)	cisco	
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)	cisco	
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)	cisco	
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	04BD88B88142-C04A00146E31-42F8
153	10.48.17.235	10.62.148.118	RADIUS	62	Accounting-Response(5) (id=108, l=20)		

..... Access-Accept (2)

Packet identifier: 0x6b (107)

Length: 321

Authenticator: 1173a3d3ea3d0798fe30fdaccf644f19

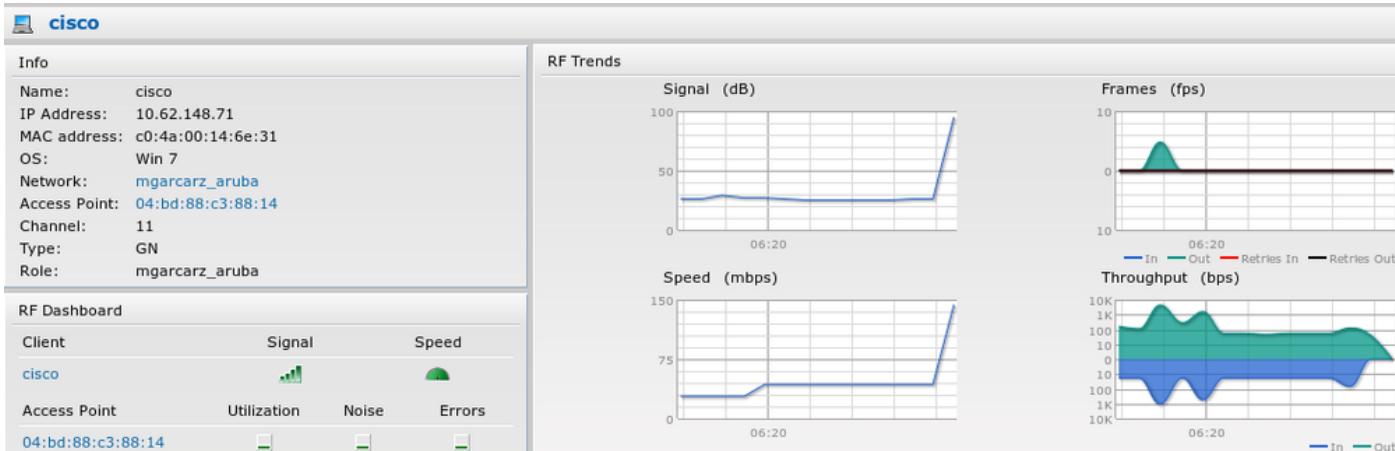
[This is a response to a request in frame 143]

[Time from request: 0.038114000 seconds]

Attribute Value Pairs

- ▷ AVP: l=7 t=User-Name(1): cisco
- ▷ AVP: l=67 t=State(24): 52656175746853657373696f6e3a30613330313165625862...
- ▷ AVP: l=87 t=Class(25): 434143533a30613330313165625862697544413379554e6f...
- ▷ AVP: l=6 t=EAP-Message(79) Last Segment[1]
- ▷ AVP: l=18 t=Message-Authenticator(80): e0b74092cacfb88803dc37032b761513
- ▷ AVP: l=58 t=Vendor-Specific(26) v=Microsoft(311)
- ▷ AVP: l=58 t=Vendor-Specific(26) v=Microsoft(311)

وه ددحمل رودل او (EAP-PEAP) اه واشنا مـت ظـلـجـلـا نـأـبـ دـيـفـتـ Aruba
mgarcarz_aruba يـفـ حـضـوـمـ وـاـمـكـ.



يف ةديقمـلا ةـبـاوـبـلـا ةـفـيـظـوـ (ISE) ةـبـاوـبـ ةـفـيـظـوـ لـيـجـوـتـلـا نـعـ لـوـفـسـمـ روـدـلـا اـذـهـأـ (ابـورـأـ).

ةـسـلـجـلـا كـلـتـلـ ةـيـلـاحـلـا لـيـوـخـتـلـا ةـلـاحـ يـهـ اـمـ دـيـكـأـتـ نـكـمـمـلـا نـمـ يـفـ Aruba CLI:

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

ةيلاحلا تانوذألا ىلع لوصح لـ 138 مقر (ACL) لوصولـا يـف مـكـحـتـلـا ةـمـئـاـقـ فـرـعـمـ نـمـ قـقـحـتـلـلـ:

<#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 حضـومـ وـهـ اـمـكـ روـدـلـاـ اـذـهـلـاـ ةـيـمـوـسـرـلـاـ مـدـخـتـسـمـلـاـ ةـهـجـاـوـيـفـ ـهـنـيـوـكـتـ مـتـ اـمـ عـمـ كـلـذـقـفـاوـتـيـ رـوـصـلـاـ.

Security

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

Roles	Access Rules for mgarcarz_aruba
default_wired_port_profile	→ Enforce captive portal
wired-instant	● Allow any to all destinations
ArubaAAA	● Allow TCP on ports 1-20000 on server 10.48.17.235
wcecot_BYOD_aruba	
mgarcarz_aruba	
mgarcarz_aruba_tls	

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

ل بـيـولـا حـفـصـتـم روـرـم ةـكـرـح هـيـجـوـت ةـدـاعـا 2. ةـوـطـخـلـا BYOD

ةـيـلـمـع ثـدـحـت ،نـاـونـع يـأ ةـبـاتـكـب مـوـقـيـو بـيـولـا ضـرـعـتـسـمـ حـتـفـب مـدـخـتـسـمـلـا مـوـقـيـ نـأ درـجـمـبـ اـرـوـصـلـا يـف حـضـوـمـ وـهـ اـمـكـ هـيـجـوـتـلـا ةـدـاعـا.

The screenshot shows a Firefox browser window with the URL <https://mgarcarz-ise20.example.com:8443/portal/PortalSetup.action?portal=0d56f8f0-6d90-11e5-978e-0050!>. The page title is "BYOD Welcome". The main content area is titled "BYOD Portal" and features three numbered steps: 1, 2, and 3. Step 1 is highlighted with a blue circle. Below step 1, the section "BYOD Welcome" contains the text "Welcome to the BYOD portal." and "Access to this network requires your device to be configured for enhanced security. Click Start to provide device information before components are installed on your device." A large text box displays a policy acceptance message from Cisco Systems. At the bottom of the page is a blue "Start" button.

1 2 3

BYOD Welcome

Welcome to the BYOD portal.

Access to this network requires your device to be configured for enhanced security. Click **Start** to provide device information before components are installed on your device.

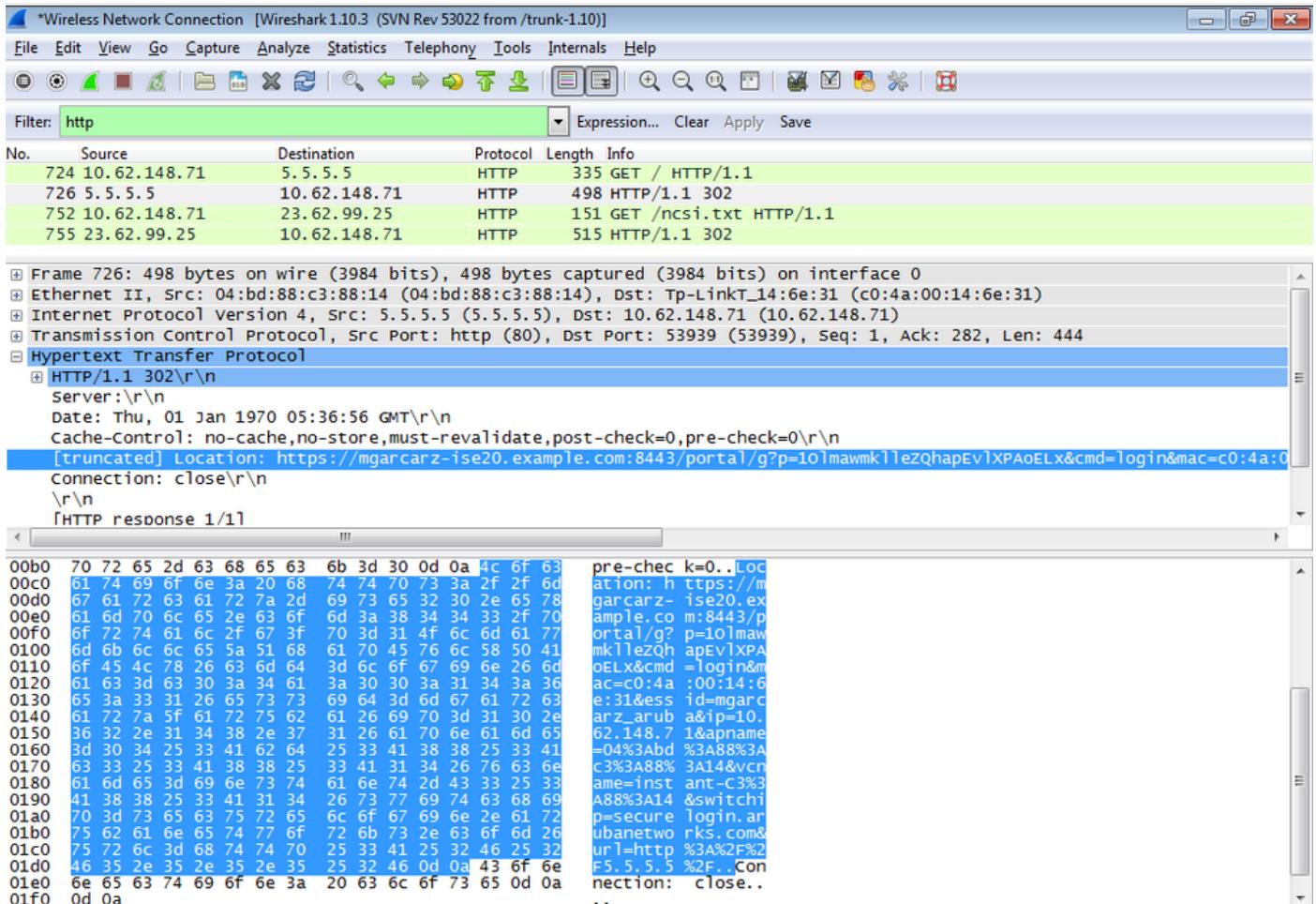
Please accept the policy: You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password. Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited. Cisco Systems reserves the right to suspend the Service if Cisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party. Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision,

Start

هـيـجـوـتـ وـدـاعـاـ دـيـعـيـوـ (5.5.5.5) عـزـتـنـيـ Arubaـ نـأـ دـكـفـمـلـاـ نـمـ ،ـمـزـحـلـاـ طـاقـتـلـاـ يـلـاـ رـظـانـلـابـ HTTPـ ىـلـاـ ISEـ.

Arubaـ لـخـدـمـ ىـلـاـ مـخـسـنـوـ Captiveـ ISEـ يـفـ هـنـيـوـكـتـ مـتـ اـمـكـ تـبـاـثـلـاـ URLـ سـفـنـ هـنـأـ ظـحـالـ:ـرـوـصـلـاـ يـفـ حـضـوـمـ وـهـ اـمـكـوـيـلـيـ اـمـكـ ـدـدـعـتـمـ تـاطـيـسـوـ وـفـاضـاـ مـتـ ،ـكـلـذـ ىـلـاـ ةـفـاضـإـلـابـ نـكـلـ.

- cmd = لـوـخـدـلـاـ لـيـجـسـتـ
- mac = c0:4a:00:14:6e:31
- ESSID = mgarcarz_aruba
- ip = 10.62.148.7
- APNAME = 4bd88c38814 (mac)
- url = <http://5.5.5.5>



لثامی ۋەسلىجلا فشتىكى، id ۋەسلىج cisco تىشىنى نأ عي طتىسى ISE، تاطىيىسولالا ھىزىمىسى قىفتى (لەكشىرخا يىأ واإ) BYOD عېباتىيەن ISE ىلىع.

نم موعدم رىغ اذه نكلىو ۋەداع ھەمادختىسى مەتىيەس Cisco، ۋەزەجأ ئەپسەنلىپ نىيرخآلانى دروملا لېبىق.

ال يتلى او (Audit-session-id) ۋەميق ئاشنە يىرت نأ نكمەملەنەم، ISE ئەطاخأ حىچھىت نم كىلذ دىكأتلىك بىشلەر بىرچەم ئەلەسرا مەتىي:

<#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: ۋەھفىص BYOD ىلىع زاھىجلا لېجىست دىعې كىلذ طېرى، مۇھىم وە.

<#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
```

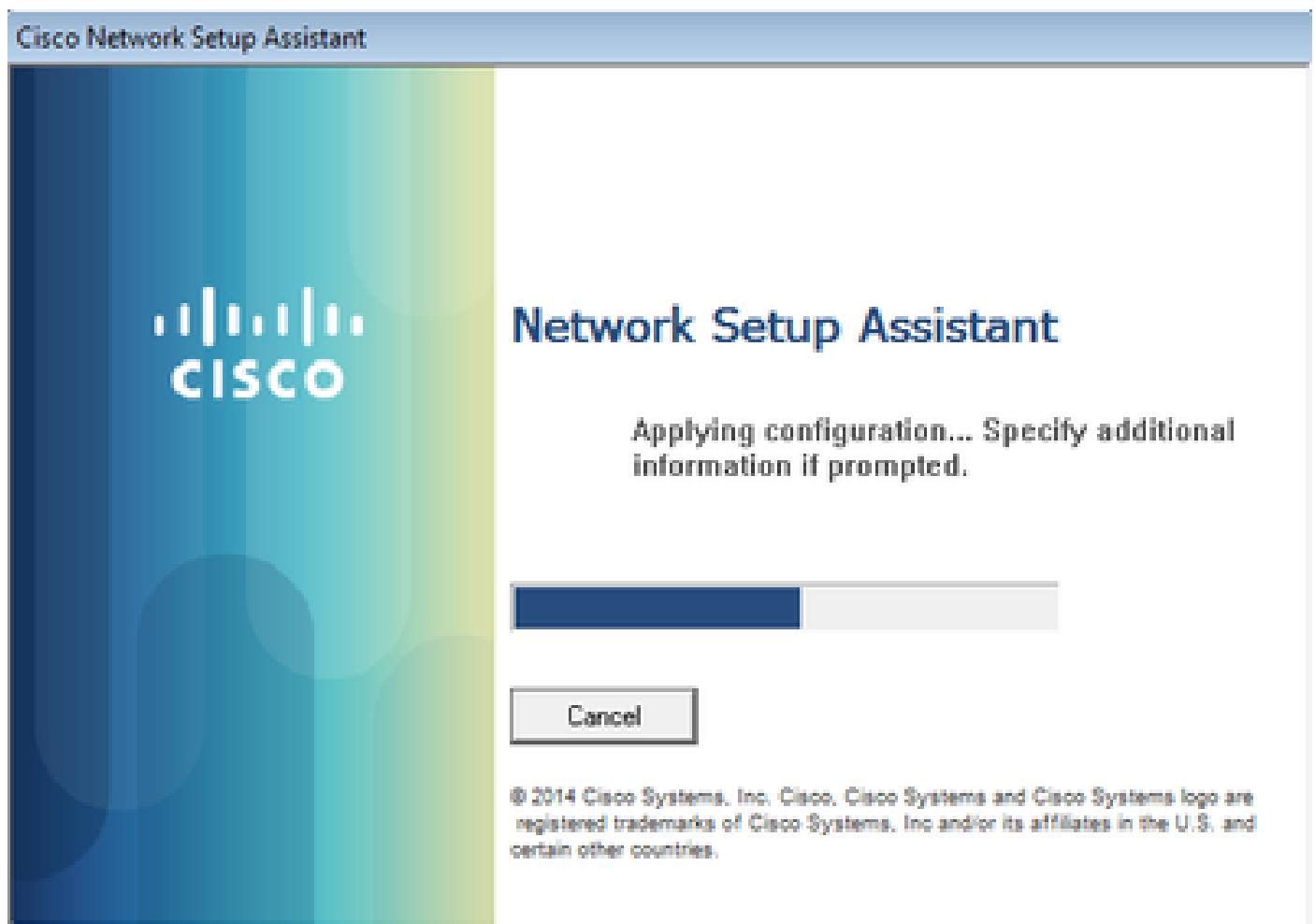
MyDevices: Successfully registered/provisioned the device

```
(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, EPIdentityGroup=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
```

لیزنٹ متي ثيح 3. مقر BYOD ڦھفص ىل ا هي جو ت ڏادع ا مرت ، ڦحال ل طلا يفو
ا.هڏي فن تو NSA.

ڦڪ بش ل ا ڏادع ا دعاسم ذي فن تو 3. ڦوط خ ل ا



متي و ISE IP ناونع فاشتكا مزلي ، ال وا . بي و لا ضرعتسم ڦم ڻ سفن NSA ىدل

ضرعتسم يف لاحلا و ه امك) IP ناونع ڦباتکل ڦيناكما مدخلتسملا ىدل سيل تقولا اذه نأ

ايئا قلت تان اي ب ل ا رورم ڦکرح عاشن ا متي هن اف ، (ب ي و ل ا

يـف حـضـوم وـه اـمـك (اـهـم اـدـخـتـسـا نـكـمـي اـضـيـا) ةـيـضـارـتـفـالـا ةـبـاوـبـلـا مـادـخـتـسـا مـتـيـةـرـوـصـلـا.

Wireless Network Connection [Wireshark 1.10.3 (SVN Rev 53022 from /trunk-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: http Expression... Clear Apply Save

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\nUser-Agent: Mozilla/4.0 (Windows NT 6.1; compatible; Cisco NAC Web Agent v.)\r\nAccept: */*\r\nHost: 10.62.148.100\r\nCache-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]

بـيـولـا ضـرـعـتـسـمـل ةـبـسـنـلـاـب لـاحـلـا وـه اـمـك اـمـامـت اـهـسـفـن يـه ةـبـاجـتـسـالـا.

نـيـوكـتـلـاـب XML فـيـرـعـت فـلـمـىـلـع لـوـصـحـلـاـو ISE بـلـاصـتـالـا NSA لـنـكـمـي ةـقـيـرـطـلـا هـذـهـبـ (ISE Internal CA) نـم ةـعـقـوم) ةـعـقـوم ةـدـاهـشـىـلـع لـوـصـحـلـاـو ISE ىـلـا هـلـاسـرـاـو SCEP بـلـطـعـاشـنـاـوـهـنـيـوكـتـمـتـ يـذـلـا SSID بـلـاصـتـالـا اـرـيـخـأـوـيـكـلـسـالـاـلـ فـيـرـعـت فـلـمـنـيـوكـتـوـهـ.

ضـعـبـ فـذـحـمـتـ يـف Windows ىـلـع) لـيـمـعـلـا نـم تـالـجـسـلـا عـيـمـجـتـ حـيـضـوـتـلـا لـجـأـنـم تـاجـرـخـمـلـا:

```
<#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.xml
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:MGARCARZ-ISE20]
```

```
set ChallengePwd
```

```
creating certificate with subject = cisco and subjectSuffix = OU=Example unit,O=Company name,L=City,ST=State,C=US, SAN:MGARCARZ-ISE20
```

```
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

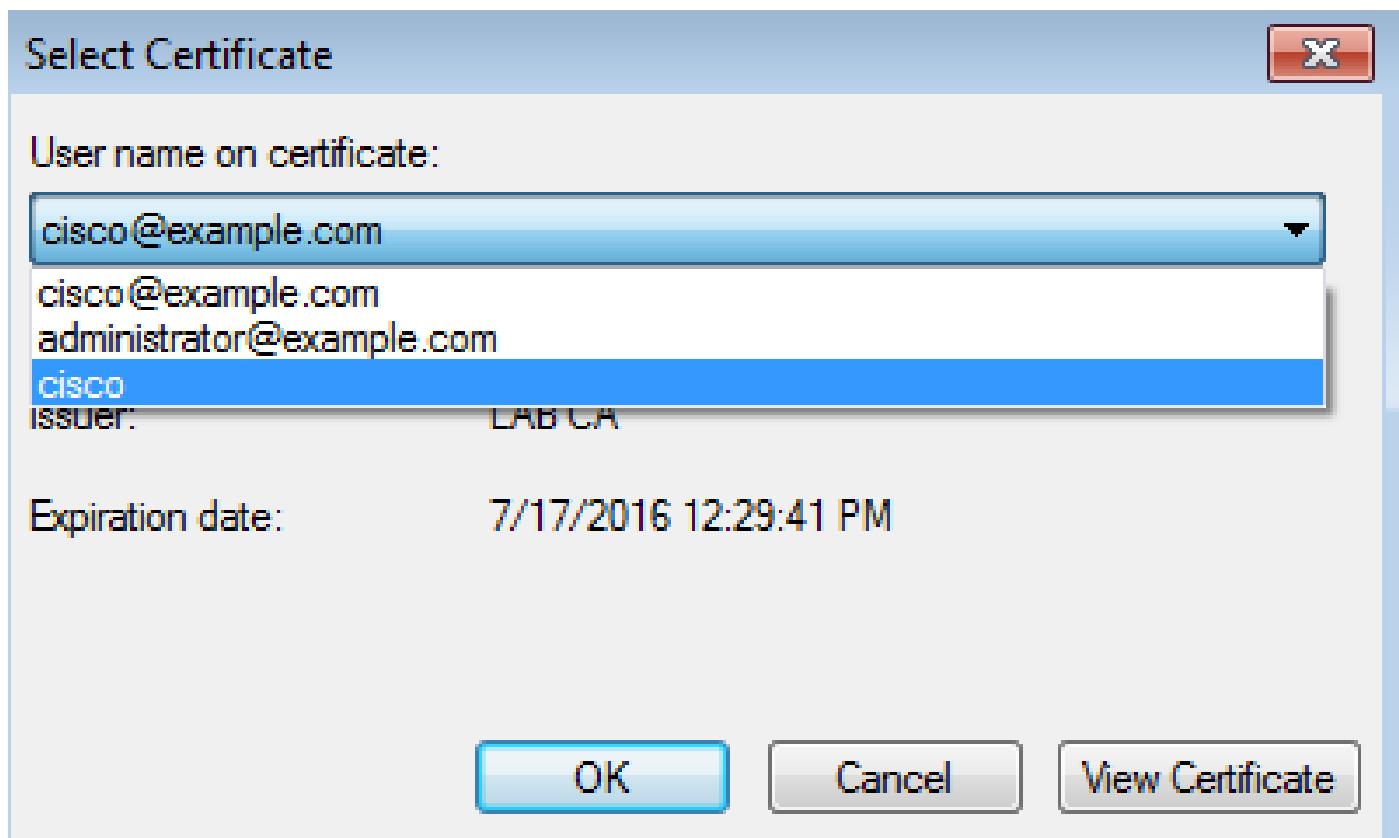
successfully connected profile: [mgarcarz_aruba_tls]

WirelessProfile::SetWirelessProfile. - End

هذا سل Cisco تالجسلا يه اوسفن امامت امك واه لاحلا بسناناب ملعم BYOD ئزهجأ عم.

لاصتاala ئداعا ضرفي يذلا (NSA) قيبطتللا وهو انه بولطم ريع ئظحالم ب SSID نوكم اثيدح.

اذا .يئاهن SSID فرعمب نارتقاala لواحي ماظنلا نأ ريري نأ مدخلتسملل نكمي ،ةلحرمللا هذه يف و وه امك) ئحيمصللا ئداهشلا ديدحت كيلع بجيـف ،ـدـحـاـوـمـدـخـتـسـمـ ئـدـاهـشـ نـمـ رـثـكـأـ كـيـدـلـ نـاـكـ (ـحـضـوـمـ).



روصلـاـ يـفـ حـضـوـمـ وـهـ اـمـكـ NSAـ رـيـرـاقـتـ ضـرـعـ مـتـيـ ،ـحـجـانـ لـاصـتاـ دـعـبـ.



عيمج قباطت يتلـا EAP-TLS ـق داصـم يـنـاـثـلـا لـجـسـلـا بـرـضـيـ - ISE ـلـعـ كـلـذـ نـمـ دـكـأـتـلـا نـكـمـيـ . حـيـحـصـ لـجـسـمـلـا BYOD وـ فـظـوـمـلـاـ Basic_AUTHENTICATED_ACCESS (EAP-TLS).

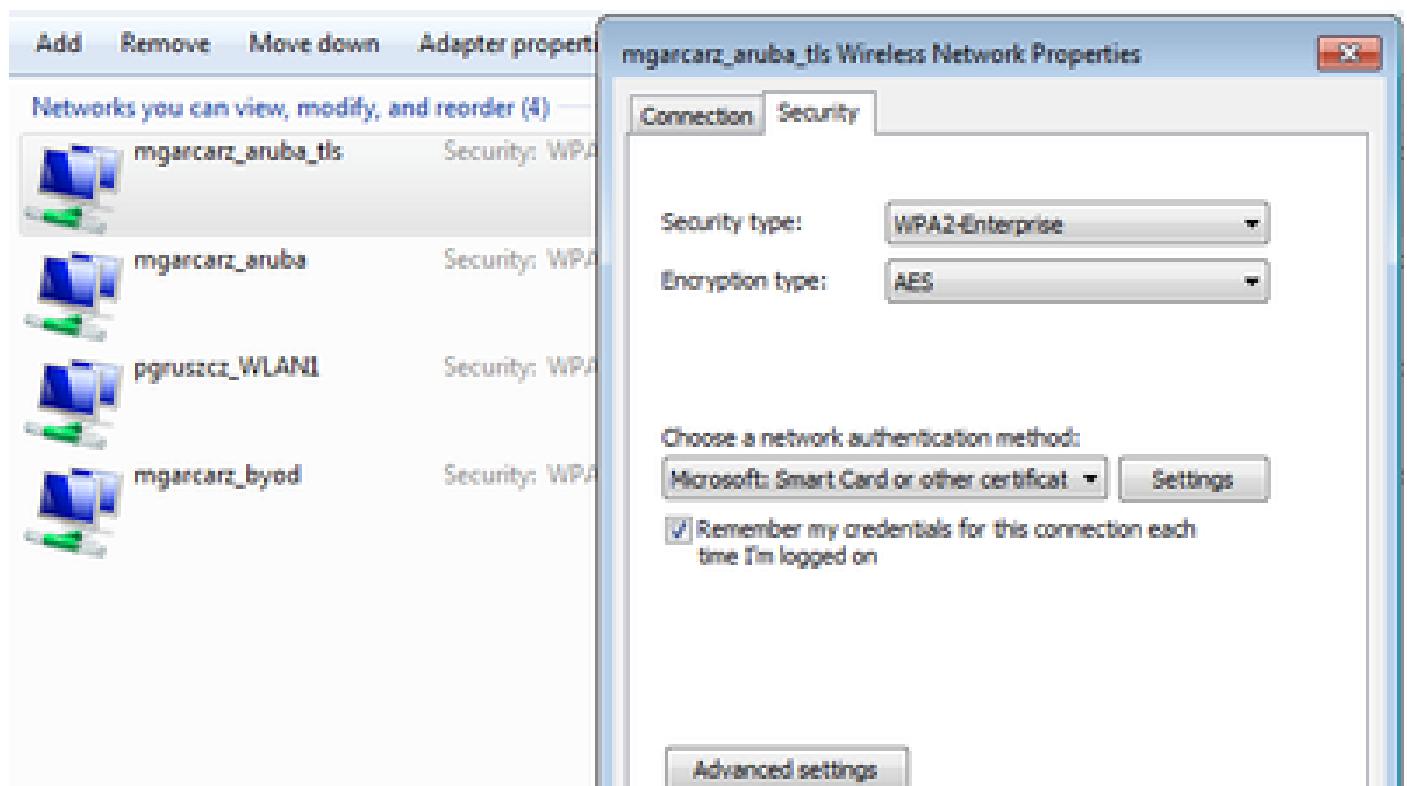
Identity Services Engine		Home	Operations	Policy	Guest Access	Administration	Work Centers	Real-time Monitoring			
RADIUS Livelog		TACACS Livelog	Reports	Troubleshoot	Adaptive Network Control			Real-time Monitoring			
Misconfigured Suplicants ⓘ		Misconfigured Network Devices ⓘ		RADIUS Drops ⓘ		Client Stopped Responding ⓘ					
1		0		12		0					
Show Live Sessions Add or Remove Columns Refresh Reset Repeat Counts		Refresh Every 5 minutes									
Time	Status	Det...	R.	Identity ⓘ	Endpoint ID ⓘ	Authentication Policy ⓘ	Authorization Policy ⓘ	Authorization Profiles	Network Device	Event ⓘ	
▼	All										
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...			0	cisco	C0:4A:00:14:6E:31	Default >> Dot1X >> EAP-TLS	Default >> Basic_Authenticated...	PermitAccess	aruba	Authentication succeeded	
2015-10-29 22:19:09...			0	cisco	C0:4A:00:14:6E:31	Default >> Dot1X >> Default	Default >> ArubaRedirect	Aruba-redirect-BYOD	aruba	Authentication succeeded	



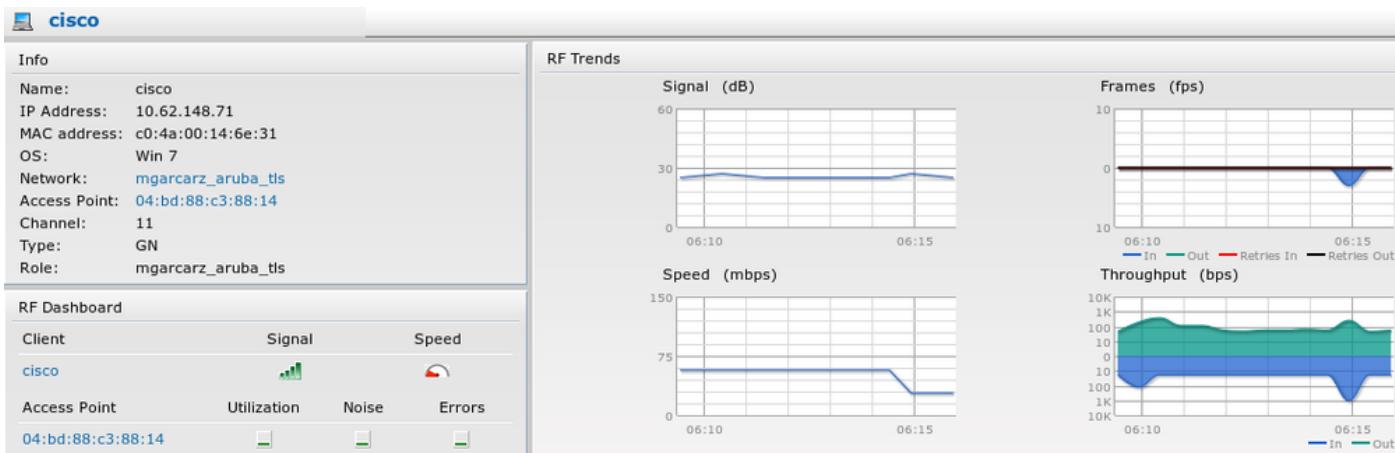
وھ امکو) لضفملہ وحنلما یلع ایئاقلت دی دج یکلساں فیصوت عاشنا مٹ، یف Windows PC (.

Manage wireless networks that use (Wireless Network Connection)

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



یئاھنلما SSID ب لصتم مدخلت سملما نأ Aruba دکؤت، ۃلحرملما هذھ یف.



ىلإ لماكلا لوصولـا ئـكـبـشـلـا مـسـا سـفـنـ ٥ـتـيـمـسـتـوـ اـيـئـاـقـلـتـ ٥ـؤـاشـنـا مـتـيـ يـيـذـلـا رـوـدـلـا رـفـوـيـ ٤ـكـبـشـلـا.

Authentication Servers		Users for Internal Server	Roles	Blacklisting	Firewall Settings	Inbound Firewall
Roles						
default_wired_port_profile		Access Rules for mgarczarz_aruba_tls				
wired-instant		<ul style="list-style-type: none">Allow any to all destinations				
ArubaAAA						
wcecot_BYOD_aruba						
mgarczarz_aruba						
mgarczarz_aruba_tls						

CoA مع دوی خأتا قفدت

CWA م& COa

فیضلا لخدم CWA قفت ضرع متی، BYOD قفت یف COa لئاسر دجوت ال امنیب
انه ایتاذ لجسملا

ةروصلـا يـف حـضـوم وـه اـمـك اـهـنـيـوـكـت مـت يـتـلـا لـيـوـخـتـلـا دـعـاـوـقـ.

Guest_Authenticate_internet	if GuestEndpoints AND Aruba:Aruba-Essid-Name EQUALS mgarcarz_aruba_guest	then PermitAccess
Guest_Authenticate_Aruba	if Aruba:Aruba-Essid-Name EQUALS mgarcarz_aruba_guest	then Aruba-redirect-CWA

بـيـولـا تـاحـفـص ضـعـبـب لـاصـتـالـا لـواـحـي نـأ درـجـمـبـو MAB ـقـدـاصـمـبـ SSID بـمـدـخـتـسـمـلـا لـصـتـيـ وـأ دـيـدـجـ باـسـحـ عـاـشـنـا Guest لـنـكـمـيـ ثـيـحـ ،ـاـيـتـاـذـ لـجـسـمـلـا Guest لـخـدـمـىـلـا هـيـجـوـتـلـا ـدـادـعـاـ ـثـدـحـيـ يـلـاـحـ باـسـحـ مـاـدـخـتـسـاـ.



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?](#)

قلح رئيغتل ةكبشلا زاهج ىلإ CoA نم ISE متسا ، حاجن بف يضلا ليصوت دعب ليوختلا.



Sponsored Guest Portal

Welcome Message

Click Continue to connect to the network.

You're very close to gaining network access.

Continue

ةروصلان يف حضوم واه امك وOperations > Authitions 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

ءاطخأ حيحصت يف CoA ةراسر ISE:

<#root>

```
2015-11-02 18:47:49,553 DEBUG [Thread-137][] cisco.cpm.prert.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.prrt.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.prrt.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=0a3011ebisZXyp0DwqjB6j64GeFiF7RwyocneEia17ckjtU1HI.,DynamicAuthorizationFlow.cpp
2015-11-02 18:47:49,584 DEBUG [Thread-137][] cisco.cpm.prrt.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.prrt.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.prrt.impl.PrRTLoggerImpl -::::-
DynamicAuthorizationFlow,DEBUG,0x7fc0e9cb2700,cntx=0000000561,sesn=c59aa41a-e029-4ba0-a31b
-44549024315e,CallingStationID=c04a00157634,[DynamicAuthorizationFlow::onLocalHttpEvent]: invoking DynamicAuthorization,DynamicAuthorizationFlow.cpp:246

```

ابورأ نم يجيء يللا لاثمتل ا لصـف و

<#root>

```

2015-11-02 18:47:49,737 DEBUG [Thread-147][] cisco.cpm.prrt.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

```

حصوصم و ه امك (41) CoA Compact-Request و (40) Diconnect-ACK طاقتلا متي

The Wireshark interface displays a capture of RADIUS traffic. The packet list shows two RADIUS messages: a Disconnect-Request (Frame 144) and a corresponding Disconnect-ACK (Frame 147). The details pane provides a breakdown of the captured frame, including the Ethernet II header, IP and UDP layers, and the RADIUS message structure. The RADIUS message itself is expanded to show the 'Code: Disconnect-Request (40)' and its attributes, such as the NAS-IP-Address and Calling-Station-Id.

Filter: `udp.port==3799`

No. Time Source Destination Protocol Length Info

144 17:47:49.654868 10.48.17.235 10.62.148.118 RADIUS 100 100 Disconnect-Request(40) (id=1, l=58)

147 17:47:49.707216 10.62.148.118 10.48.17.235 RADIUS 74 74 Disconnect-ACK(41) (id=1, l=32)

► Frame 144: 100 bytes on wire (800 bits), 100 bytes captured (800 bits)
► Ethernet II, Src: Vmware_99:6d:34 (00:50:56:99:6d:34), Dst: Cisco_1c:e8:00 (00:07:4f:1c:e8:00)
► Internet Protocol Version 4, Src: 10.48.17.235 (10.48.17.235), Dst: 10.62.148.118 (10.62.148.118)
► User Datagram Protocol, Src Port: 16573 (16573), Dst Port: radius-dynauth (3799)
▼ Radius Protocol
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

(ةيضاـرتـفـالـاـ تـادـادـعـإـ) Aruba بـةـقـلـعـتـمـلـاـ ةـقـدـاصـمـلـلـ RFC CoA مـادـخـتـسـإـ مـتـ: ةـظـاحـالـمـ ةـدـاعـإـ تـمـتـ دقـ نـوـكـتـ، Cisco زـاهـجـبـ ةـقـلـعـتـمـلـاـ ةـقـدـاصـمـلـلـ ةـبـسـنـلـابـ. زـاهـجـلـاـ فـيـرـعـتـ فـلـمـلـ عـونـ ةـقـدـاصـمـ Cisco CoA.

اھالص او عاطخآل ا فاشکتسا

اوهالص او نیوکتل اه طاخ فاش کتس اه ادختس کن کمی تامولع مسقله اذه رفوي.

نم الدب IP ناونع عم ةديقملا Aruba ةبأوب FQDN

لشفی، ISE ب ۀصاخلا FQDN نم الدب IP ناونع ب Aruba یلع ۀدیقملا ۀب اوبلا نیوکت مت اذا PSN NSA:

<#root>

Warning - [HTTPConnection]

Abort the HTTP connection due to invalid certificate

CN

نانونع مدخلتست امدنع .ISE ب لاصتالا دناع ڏداهشلا ڦحص نم ڦيقيق دلا ڦققحتلا وه ڪلذ ببس و
ع م اهمي دق ت مت يو (IP نام الدب FQDN URL هيجوت ڏداعا إل ڦجيتن) ISE ب لاصتالل IP
ڦحص نم ڦققحتلا لشف = عوض وملما مساب ISE ڏداهش FQDN.

 **وقاوم إلـا جاتحي رـيـذـحـت رـادـصـاـعـم** BYOD ةـبـاـوـبـعـم بـيـوـلـا ضـرـعـتـسـم لـصـاـوـتـيـ: ظـاحـلـمـاـمـدـخـتـسـمـلـاـ.

ةديقملا ةبأوبل حيحص ريغ لوصحن

ةديقملا ةبأوبل مادختساب هنيوكت مت يذلا Aruba Access-Policy حمسى ، يضارتفا لكشب 8080 و 443 و 80 ذفانمب TCP ذفانمب.

مت NSA نم XML فيرعت فلم ىلع لوصح لـ TCP 8905 ذفنب لاصتا لـ IKE. اذه نع غالب إلـا:

```
<#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 All  
- http Error: [2]
```

```
HTTP response code: 0
```

```
]
```

```
GetProfile - end
```

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

ذفنم مقر Aruba CoA

نم نكلو. CoA Air Group CoA 5999. ذفنمل ذفنملار فوت ، يضارتفا لكشب (حصوم وـ امـك) تابـلـ طـلـا هـذـه لـثـمـل بـجـتـسـت مـل 204 اـبـورـأ ةـكـرش نـأ فـسـؤـمـلـا.

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

ةروصلـا يـف حـضـوم وـه اـمـك ـمـزـحـلـا طـاقـتـلـا.

arubacoa5999.pcap [Wireshark 1.10.6 (v1.10.6 from master-1.10)]

Filter: udp.port==5999

No.	Time	Source	Destination	Protocol	Length	Info
685	20:17:44.908041	10.48.17.141	10.62.148.118	RADIUS	100	Disconnect-Request(40) (id=11, l=58)
686	20:17:44.938510	10.62.148.118	10.48.17.141	ICMP	128	Destination unreachable (Port unreachable)

Frame 685: 100 bytes on wire (800 bits), 100 bytes captured (800 bits)
► Ethernet II, Src: Vmware_99:37:59 (00:50:56:99:37:59), Dst: Cisco_1c:e8:00 (00:07:4f:1c:e8:00)
► Internet Protocol Version 4, Src: 10.48.17.141 (10.48.17.141), Dst: 10.62.148.118 (10.62.148.118)
► User Datagram Protocol, Src Port: 59726 (59726), Dst Port: cvsup (5999)
▼ Radius Protocol
Code: Disconnect-Request (40)
Packet identifier: 0xb (11)
Length: 58
Authenticator: 00b8961272015b5cecf27cc7f3e8fe81
▼ 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): 1959020d15fe2b0584b3a887c1e3c366

يـف حـضـوم وـه اـمـك CoA 3977 ذـفـنـم وـه اـنـه مـادـخـتـسـالـل لـضـفـأـلـا رـايـخـلـا نـوـكـي نـأـنـكـمـي 5176.

Aruba ـجـهـجـأـ ضـعـبـ ـلـعـ هـيـجـوـتـلـا ـدـاعـإـ

الـيـلـقـ فـلـتـخـمـ لـكـشـبـ لـمـعـتـ هـيـجـوـتـلـا ـدـاعـإـ ـيـلـمـعـ نـأـ ظـحـالـيـ، رـادـصـإـلـا عـمـ 6.3ـ رـادـصـإـلـا عـمـ Aruba 3600ـ يـفـ.

انـه اـحـرـشـوـ ـمـزـحـلـا طـاقـتـلـا ـلـعـ روـثـعـلـا نـكـمـيـ. يـرـأـلـا مـكـحـتـلـا تـادـوـنـعـ

770 09:29:40.511911 10.75.94.213	173.194.124.52	HTTP	1373 GET / HTTP/1.1
772 09:29:40.521065 173.194.124.52	10.75.94.213	HTTP	416 HTTP/1.1 200 OK (text/html)
794 09:29:41.698257 10.75.94.213	173.194.124.52	HTTP	63 GET /&arubalp=6b0512fc-f699-45c6-b5cb-e62b3260e5 HTTP/1.1
797 09:29:41.756306 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/
```

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

'>\npacket 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&essid=SC%2DWiFi&apname=LRC-006&apgroup=default&url=http%3A%2F%2Fwww

ةلص تاذ تامولعم

- رادصا، Cisco نم ۋەلەتامدۇخ كىرەم لەۋەسم لىلىد [Cisco 2.0](#)
- Cisco نم ۋەلەتامدۇخ كىرەم مادختساب ئەكبىشلىلىلا لەۋەصۇلە زاھەج فېرىعەت تافلەم
- [تادنەتسەملەوايىنقتلىامعدىلە - Cisco Systems](#)

هـ لـ وـ لـ جـ رـ تـ لـ اـ هـ ذـ هـ

ةـ يـ لـ آـ لـ اـ تـ اـ يـ نـ قـ تـ لـ اـ نـ مـ مـ جـ مـ وـ عـ مـ اـ دـ خـ تـ سـ اـ بـ دـ نـ تـ سـ مـ لـ اـ اـ ذـ هـ تـ مـ جـ رـ تـ
لـ اـ عـ لـ اـ ءـ اـ حـ نـ اـ عـ يـ مـ جـ يـ فـ نـ يـ مـ دـ خـ تـ سـ مـ لـ لـ مـ عـ دـ ئـ وـ تـ حـ مـ يـ دـ قـ تـ لـ ةـ يـ رـ شـ بـ لـ اـ وـ
اـ مـ كـ ةـ قـ يـ قـ دـ نـ وـ كـ تـ نـ لـ ةـ يـ لـ آـ ةـ مـ جـ رـ تـ لـ ضـ فـ اـ نـ اـ ةـ ظـ حـ اـ لـ مـ ئـ جـ رـ يـ .ـ صـ اـ خـ لـ اـ مـ هـ تـ غـ لـ بـ
يـ لـ خـ تـ .ـ فـ رـ تـ حـ مـ مـ جـ رـ تـ مـ اـ هـ دـ قـ يـ يـ تـ لـ اـ ةـ يـ فـ اـ رـ تـ حـ اـ لـ اـ ةـ مـ جـ رـ تـ لـ اـ عـ مـ لـ اـ حـ لـ اـ وـ
ىـ لـ إـ أـ مـ ئـ اـ دـ عـ وـ جـ رـ لـ اـ بـ يـ صـ وـ تـ وـ تـ اـ مـ جـ رـ تـ لـ اـ هـ ذـ هـ ةـ قـ دـ نـ عـ اـ هـ تـ يـ لـ وـ ئـ سـ مـ
(رـ فـ وـ تـ مـ طـ بـ اـ رـ لـ اـ)ـ يـ لـ صـ أـ لـ اـ يـ زـ يـ لـ جـ نـ إـ لـ اـ دـ نـ تـ سـ مـ لـ اـ).