配置ISE 2.0第三方與Aruba Wireless的整合

目錄

簡介

本文檔介紹如何對思科身份服務引擎(ISE)上的第三方整合功能進行故障排除。

注意：請注意，思科不負責配置或支援其他供應商提供的裝置。

必要條件

需求

思科建議您瞭解以下主題：

- Aruba IAP配置
- ISE上的自帶裝置流
- 用於密碼和證書身份驗證的ISE配置

採用元件

本文檔介紹如何對思科身份服務引擎(ISE)上的第三方整合功能進行故障排除。

它可以用作與其他供應商和流程整合的指南。ISE版本2.0支援第三方整合。

本配置示例展示如何將Aruba IAP 204管理的無線網路與ISE整合到自帶裝置(BYOD)服務中。

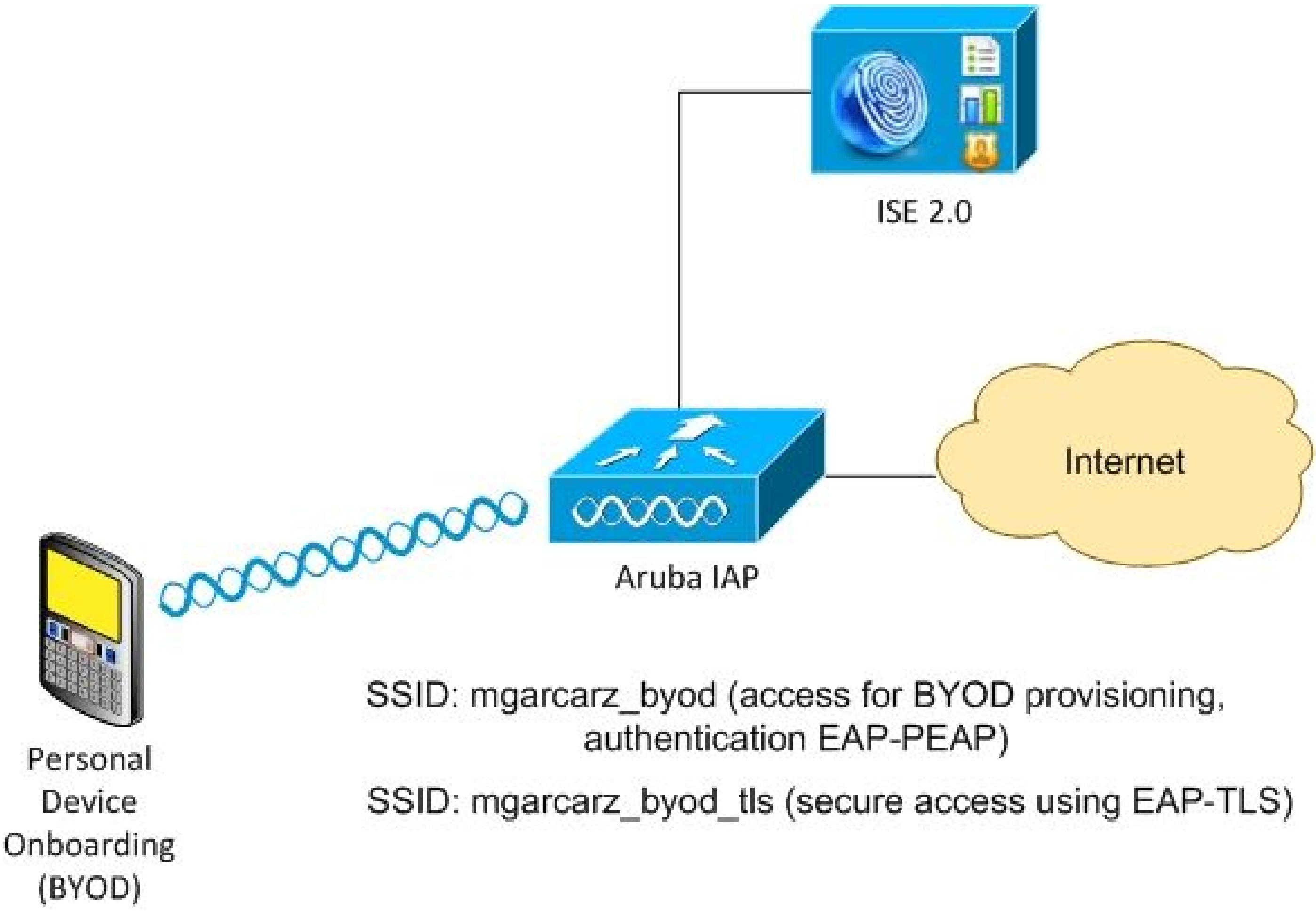
本檔案中的資訊是根據以下軟體版本：

- Aruba IAP 204軟體6.4.2.3
- Cisco ISE 2.0版及更高版本

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路運作中，請確保您瞭解任何指令可能造成的影響。

設定

網路圖表


ISE 2.0
Internet
Aruba IAP
Personal Device Onboarding (BYOD)
SSID: mgarcarz_byod (access for BYOD provisioning, authentication EAP-PEAP)
SSID: mgarcarz_byod_tls (secure access using EAP-TLS)

有兩個由Aruba AP管理的無線網路。

第一個(mgarcartz_byod)用於802.1x可擴展身份驗證協定保護的EAP(EAP-PEAP)訪問。

身份驗證成功後，Aruba控制器必須將使用者重定向到ISE BYOD門戶 — 本機請求方調配(NSP)流
。

將重定向使用者，執行網路設定助理(NSA)應用程式，並在Windows客戶端上設定並安裝證書。

ISE內部CA用於該流程（預設配置）。

NSA還負責為Aruba(mgarz_byod_tls)管理的第二個服務集識別符號(SSID)建立無線配置檔案 — 該配置檔案用於802.1x可擴展身份驗證協定 — 傳輸層安全(EAP-TLS)身份驗證。

因此，企業使用者能夠執行個人裝置自註冊並安全訪問企業網路。

您可以很容易地為不同型別的訪問修改此示例，例如：

- 採用BYOD服務的中央Web驗證(CWA)
- 採用狀態和BYOD重定向的802.1x身份驗證
- 通常，對於EAP-PEAP身份驗證，使用Active Directory（為了讓本文保持使用短的內部ISE使用者）
- 通常，對於使用證書調配外部簡單證書註冊協定(SCEP)伺服器的證書，通常使用Microsoft網路裝置註冊服務(NDES)來縮短本文的篇幅，使用內部ISE CA。

第三方支援的挑戰

將ISE訪客流(例如BYOD、CWA、NSP、客戶端調配門戶(CPP))與第三方裝置配合使用時存在挑戰。

作業階段

思科網路存取裝置(NAD)使用名為audit-session-id的Radius cisco-av配對，將作業階段ID告知驗證、授權及記帳(AAA)伺服器。

ISE使用該值跟蹤會話並為每個流提供正確的服務。其他廠商不支援cisco-av配對。

ISE必須依賴於在訪問請求和記帳請求中接收的IETF屬性。

收到訪問請求後，ISE會構建綜合的思科會話ID（從呼叫站ID、NAS埠、NAS-IP地址和共用金鑰）。該值僅具有本地意義（不通過網路傳送）。

因此，希望每個流(BYOD、CWA、NSP、CPP)都附加正確的屬性，因此ISE能夠重新計算思科會話ID並執行查詢，以便將其與正確的會話關聯並繼續流。

URL重新導向

ISE使用名為url-redirect和url-redirect-acl的Radius cisco-av-pair通知NAD必須重定向特定流量。

其他廠商不支援cisco-av配對。通常，這些裝置必須使用指向ISE上特定服務（授權配置檔案）的靜態重定向URL進行配置。

使用者啟動HTTP會話後，這些NAD重定向到URL，並附加其他引數（如IP地址或MAC地址），以允許ISE識別特定會話並繼續流程。

CoA

ISE使用Radius cisco-av-pair called subscriber:command， subscriber:reauthenticate-type來指示特定會話的NAD必須執行的操作。

其他廠商不支援cisco-av配對。通常，這些裝置使用RFC CoA（3576或5176）和以下兩個定義的消息之一：

- 斷開連線請求（也稱為斷開連線的資料包）— 用於斷開會話的連線（通常用於強制重新連線）
- CoA推送 — 用於透明地更改會話狀態而不斷開連線（例如，應用了VPN會話和新ACL）

ISE同時支援Cisco CoA和cisco-av-pair以及RFC CoA 3576/5176。

ISE解決方案

為了支援第三方供應商，ISE 2.0引入了網路裝置配置檔案概念，描述了特定供應商的行為方式 — 如何支援會話、URL重定向和CoA。

授權配置檔案屬於特定型別（網路裝置配置檔案），身份驗證發生後，ISE行為即從該配置檔案派生。

因此，ISE可以輕鬆管理其他供應商的裝置。此外，ISE上的配置也很靈活，允許調整或建立新的網路裝置配置檔案。

本文介紹了Aruba裝置預設配置檔案的用法。

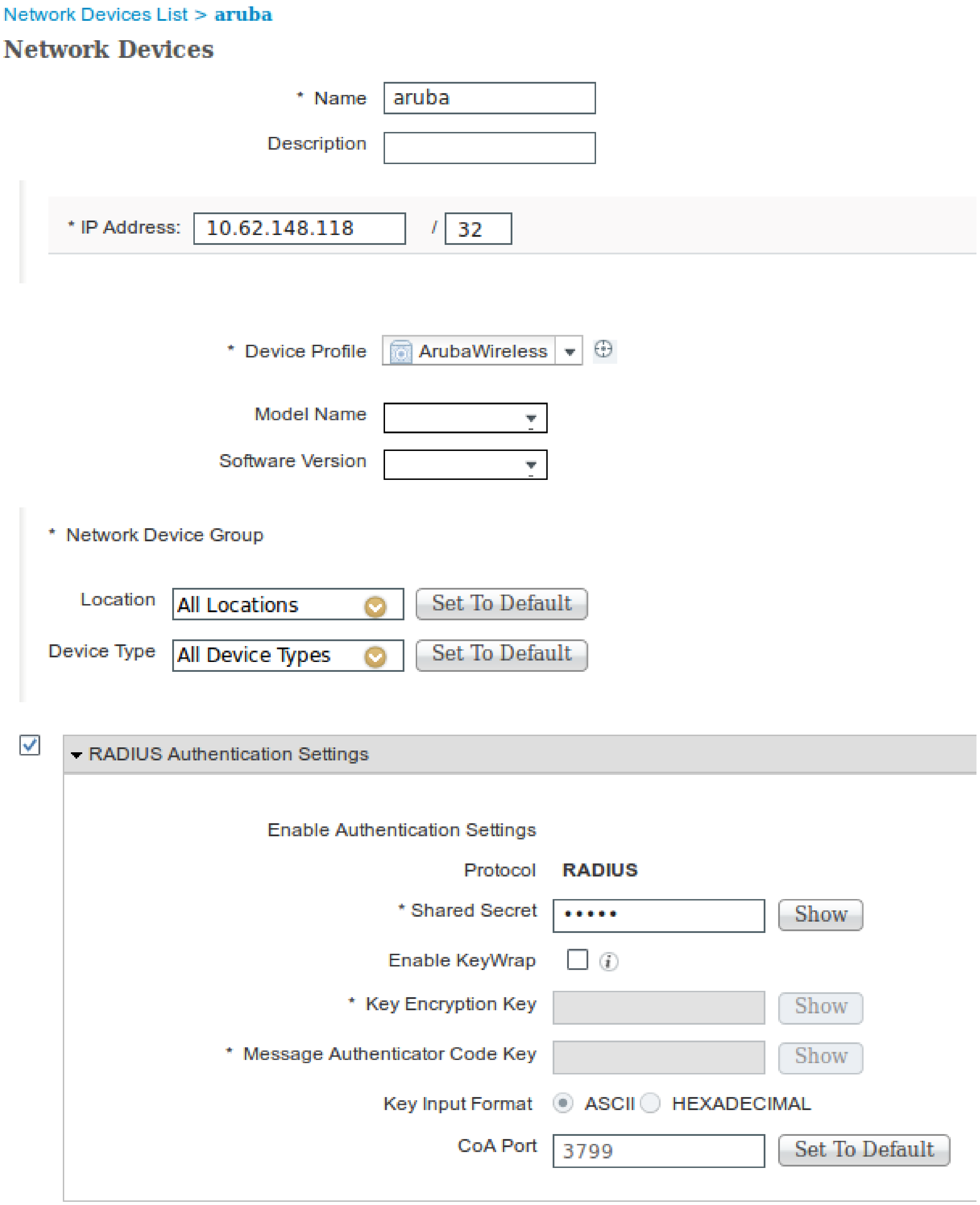
有關功能的詳細資訊：

使用思科身份服務引擎的網路訪問裝置配置檔案

思科ISE

步驟 1.向網路裝置新增Aruba無線控制器

導覽至Administration > Network Resources > Network Devices。為所選供應商(本例中為ArubaWireless)選擇正確的裝置配置檔案。 確保配置Shared Secret和CoA埠，如下圖所示。



Network Devices List > **aruba**

Network Devices

* Name: aruba

Description:

* IP Address: 10.62.148.118 / 32

* Device Profile: AubaWireless

Model Name:

Software Version:

* Network Device Group

Location: All Locations — Set To Default

Device Type: All Device Types — Set To Default

☑ RADIUS Authentication Settings

Enable Authentication Settings

Protocol: **RADIUS**

* Shared Secret: ••••• — Show

Enable KeyWrap: □

* Key Encryption Key: — Show

* Message Authenticator Code Key: — Show

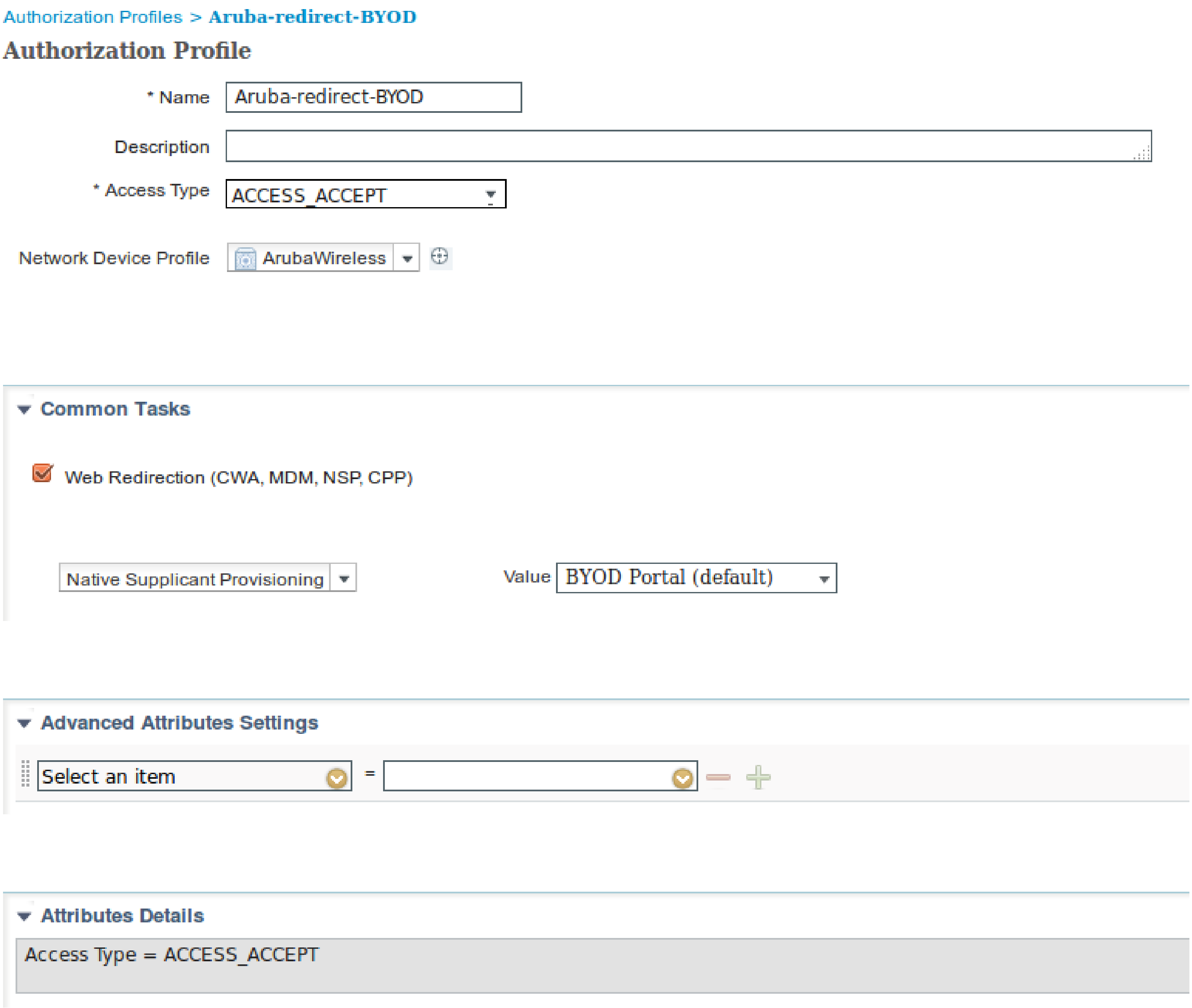
Key Input Format: ● ASCII ○ HEXADECIMAL

CoA Port: 3799 — Set To Default

如果所需供應商沒有可用的配置檔案，可以在管理>網路資源>網路裝置配置檔案下配置該配置檔案。

步驟 2.配置授權配置檔案

導航到Policy > Policy Elements > Results > Authorization > Authorization Profiles，選擇與步驟1中相同的Network Device Profile。 ArubaWireless。 配置的配置檔案是Aruba-redirect-BYOD with BYOD Portal，如下圖所示。



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 Supplicant Provisioning — Value: BYOD Portal (default)

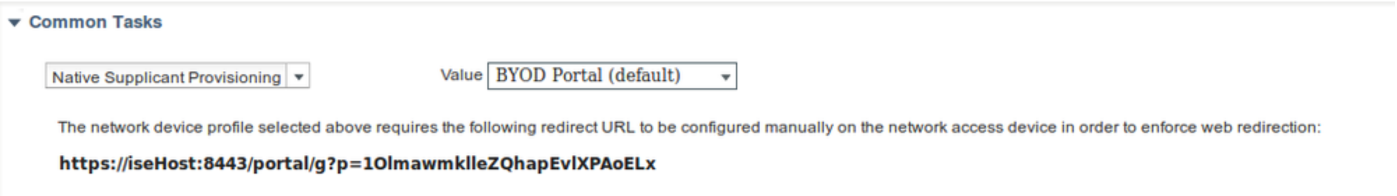
Advanced Attributes Settings

Select an item =

Attributes Details

Access Type = ACCESS_ACCEPT

缺少Web重新導向配置的一部分，其中生成到授權配置檔案的靜態連結。雖然Aruba不支援動態重定向到訪客門戶，但每個授權配置檔案都分配有一個連結，該連結隨後在Aruba上配置，如下圖所示。



Common Tasks

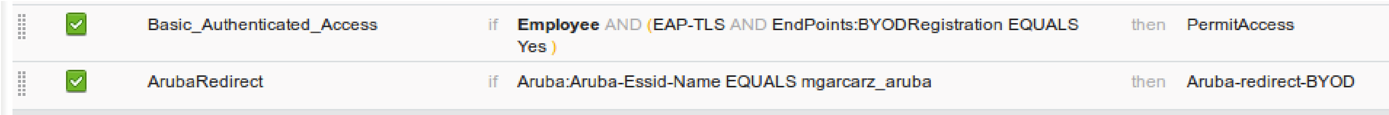
Native Supplicant Provisioning — Value: BYOD Portal (default)

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=10lmawmklleZQhapEvlXPAoELx

步驟 3.設定授權規則

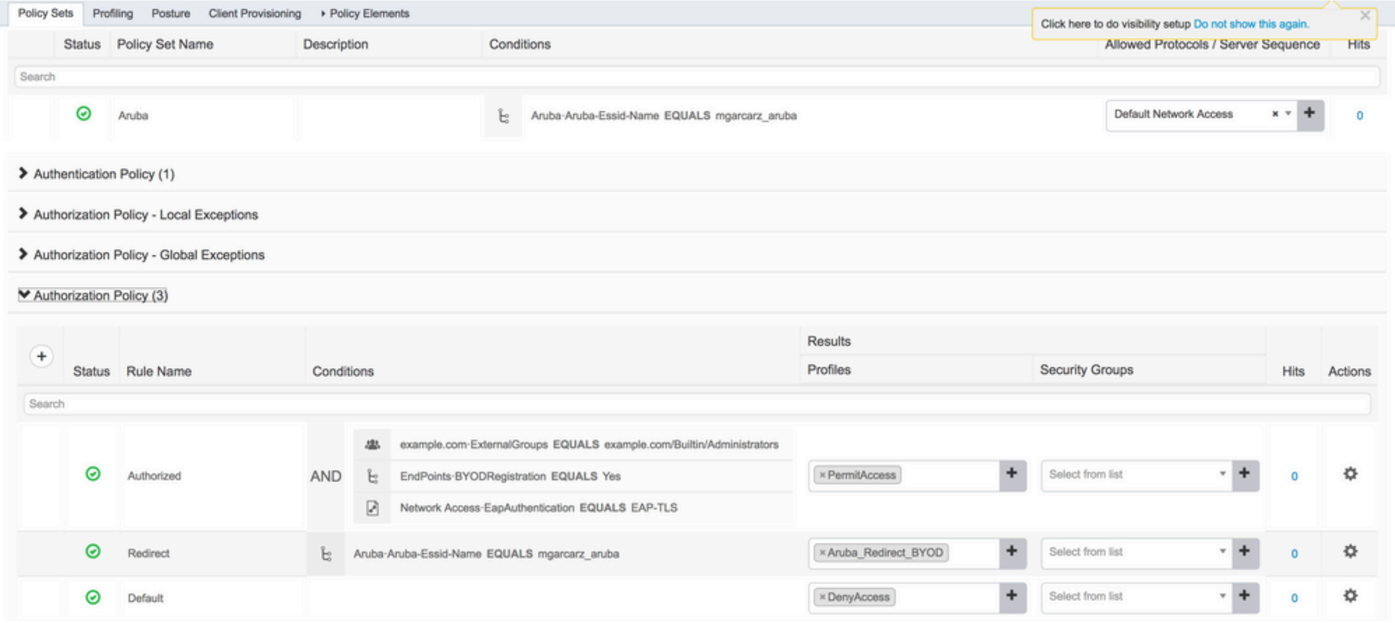
導覽至Policy > Authorization Rules，組態如下圖所示。



☑	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

首先，使用者連線到SSID mgracarz_aruba，ISE返回授權配置檔案Aruba-redirect-BYOD，它將客戶端重定向到預設自帶裝置門戶。完成BYOD流程後，客戶端將連線EAP-TLS，並授予對網路的完全訪問許可權。

在ISE的較新版本中，同一策略可能如下所示：



Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits
✓	Aruba		Aruba·Aruba-Essid-Name EQUALS mgarcarz_aruba	Default Network Access	0

- Authentication Policy (1)
- Authorization Policy - Local Exceptions
- Authorization Policy - Global Exceptions
- Authorization Policy (3)

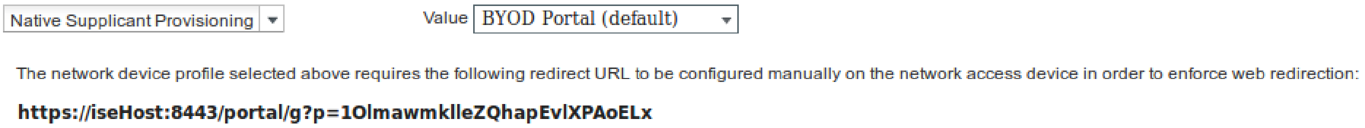
Status	Rule Name	Conditions	Results: Profiles	Results: Security Groups	Hits	Actions
✓	Authorized	AND example.com·ExternalGroups EQUALS example.com/Builtin/Administrators EndPoints·BYODRegistration EQUALS Yes Network Access·EapAuthentication EQUALS EAP-TLS	× PermitAccess	Select from list	0	⚙
✓	Redirect	Aruba·Aruba-Essid-Name EQUALS mgarcarz_aruba	× Aruba_Redirect_BYOD	Select from list	0	⚙
✓	Default		× DenyAccess	Select from list	0	⚙

阿魯巴美聯社

步驟 1.強制網路門戶配置

要在Aruba 204上配置強制網路門戶，請導航到Security > External Captive Portal並新增新的強制網路門戶。輸入以下資訊以進行正確組態並如下圖所示。

- 型別：Radius身份驗證
- IP或主機名：ISE伺服器
- URL：在授權配置檔案配置下在ISE上建立的連結；它特定於特定的授權配置檔案，可以在此處的Web重定向配置下找到

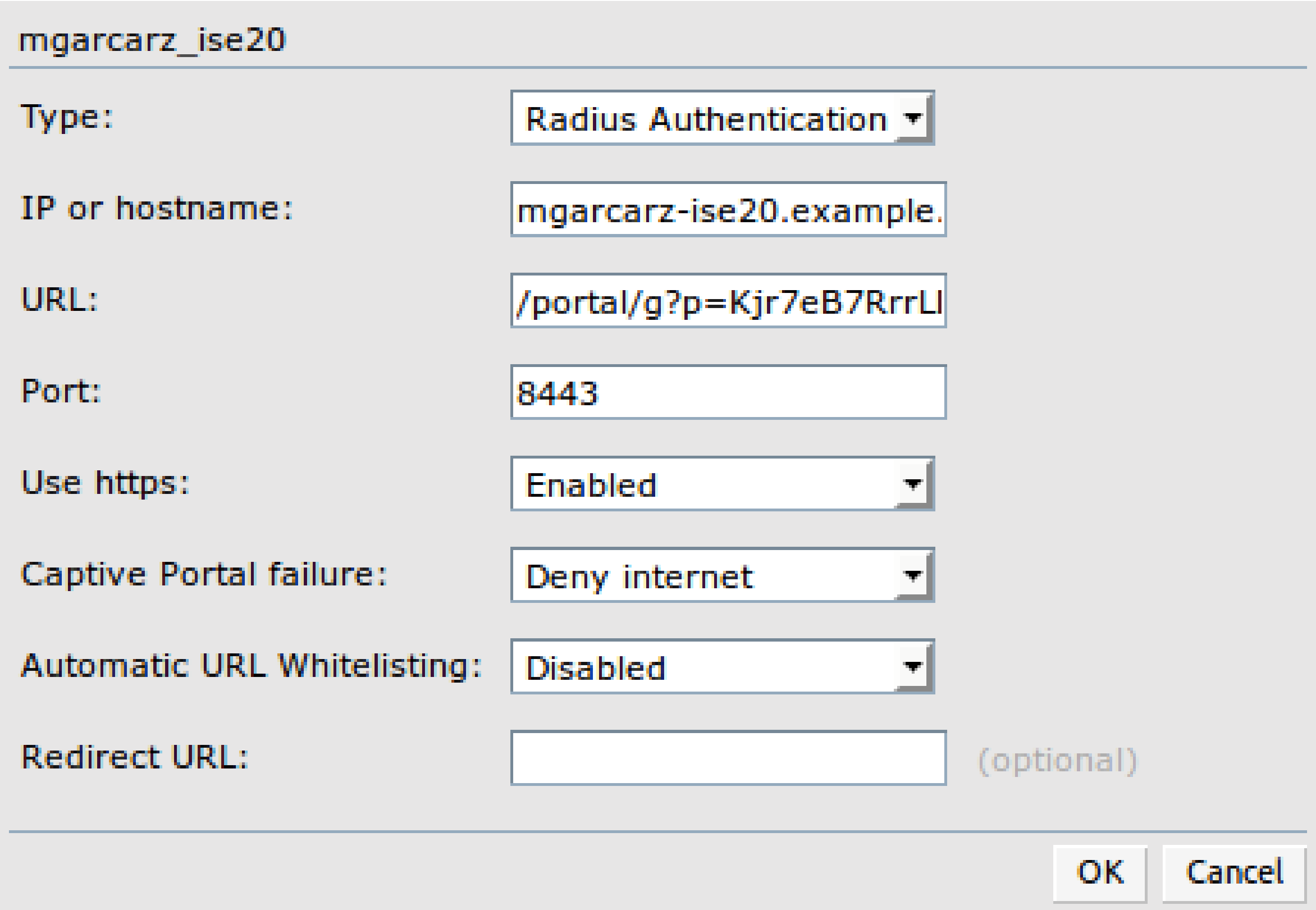


Native Supplicant Provisioning　Value BYOD Portal (default)

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=1OlmawmklleZQhapEvlXPAoELx

- 埠：在ISE上託管選定門戶的埠號（預設值為8443），如下圖所示。



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

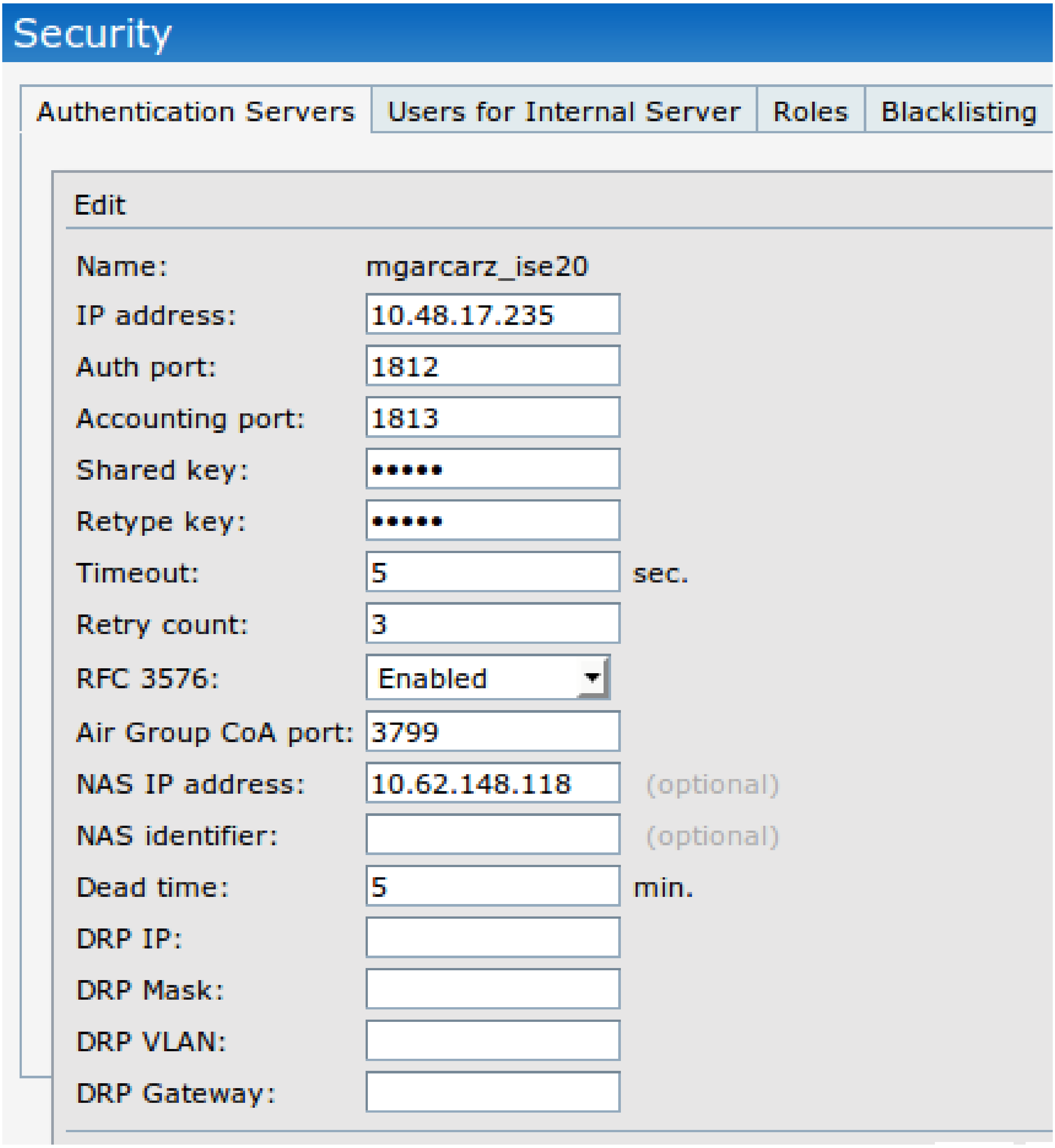
Automatic URL Whitelisting: Disabled

Redirect URL: (optional)

步驟 2.Radius伺服器配置

導覽至Security > Authentication Servers，確保CoA埠與ISE上配置的埠相同，如下圖所示。

預設情況下，在Aruba 204上，它設定為5999，但這與RFC 5176不相容，而且它也不與ISE一起使用。

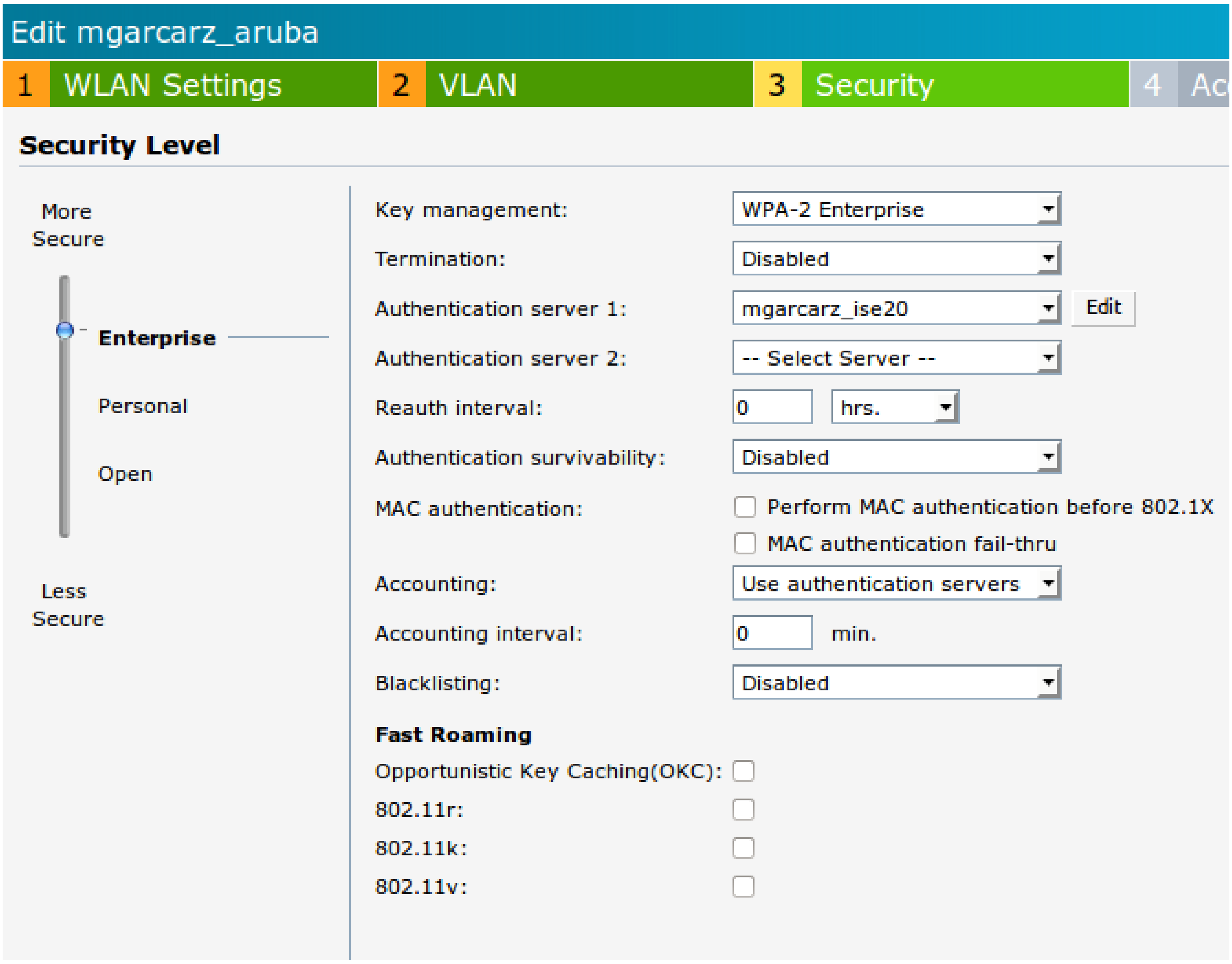


Name:	mgarcarz_ise20	
IP address:	10.48.17.235	
Auth port:	1812	
Accounting port:	1813	
Shared key:	•••••	
Retype key:	•••••	
Timeout:	5	sec.
Retry count:	3	
RFC 3576:	Enabled	
Air Group CoA port:	3799	
NAS IP address:	10.62.148.118	(optional)
NAS identifier:		(optional)
Dead time:	5	min.
DRP IP:		
DRP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

注意：在Aruba版本6.5和更新版本中，選中「Captive Portal」覈取方塊。

步驟 3.SSID配置

- 安全標籤如下圖所示。



Edit mgarcarz_aruba

Security Level

Key management: WPA-2 Enterprise

Termination: Disabled

Authentication server 1: mgarcarz_ise20

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): □

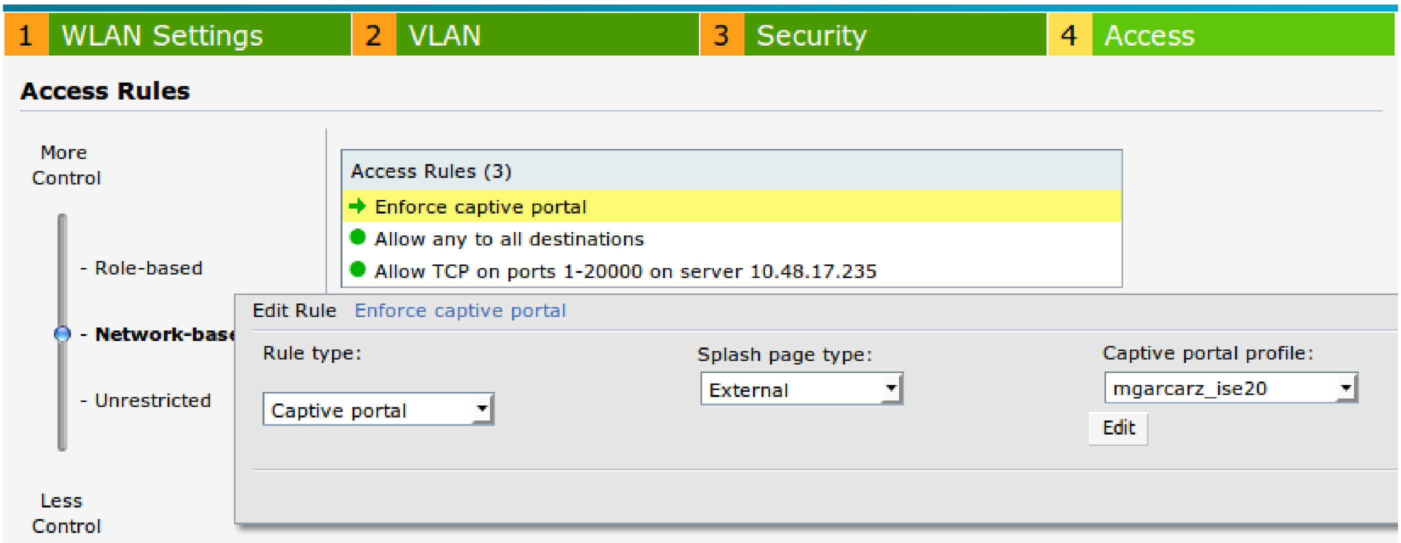
802.11r: □

802.11k: □

802.11v: □

- Access頁籤：選擇Network-based Access Rule，以便在SSID上配置強制網路門戶。

使用在步驟1中配置的強制網路門戶。按一下「New」，選擇「Rule type: Captive portal」、「Splash page type: External」，如下圖所示。



Access Rules

Access Rules (3)

➔ Enforce captive portal

● Allow any to all destinations

● Allow TCP on ports 1-20000 on server 10.48.17.235

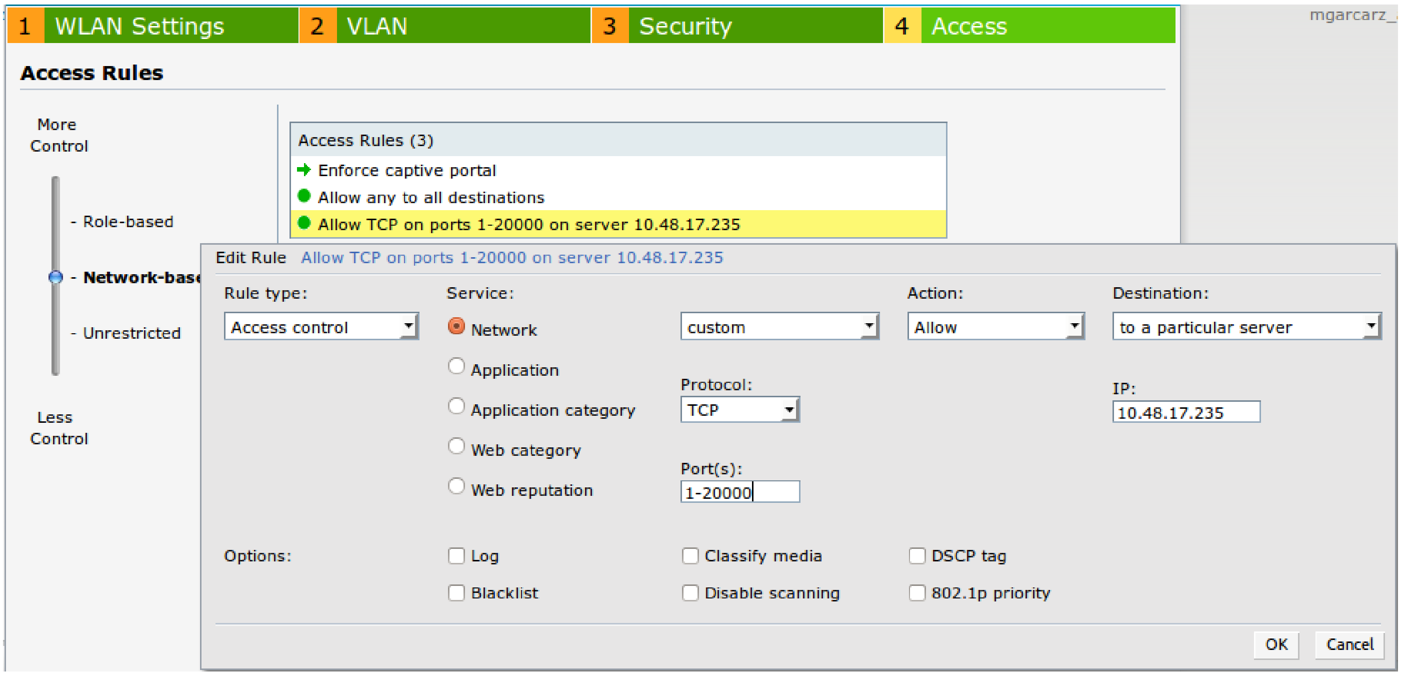
Edit Rule Enforce captive portal

Rule type: Captive portal

Splash page type: External

Captive portal profile: mgarcarz_ise20

此外，允許所有流量到達ISE伺服器(範圍1-20000的TCP埠)，而預設情況下在Aruba上配置規則：Allow any to all destinations似乎無法正常工作，如圖所示。



Access Rules

More Control

- Role-based
- Network-base
- 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 Allow TCP on ports 1-20000 on server 10.48.17.235

Rule type: Access control

Service: ● Network ○ Application ○ Application category ○ Web category ○ Web reputation

custom

Protocol: TCP

Port(s): 1-20000

Action: Allow

Destination: to a particular server

IP: 10.48.17.235

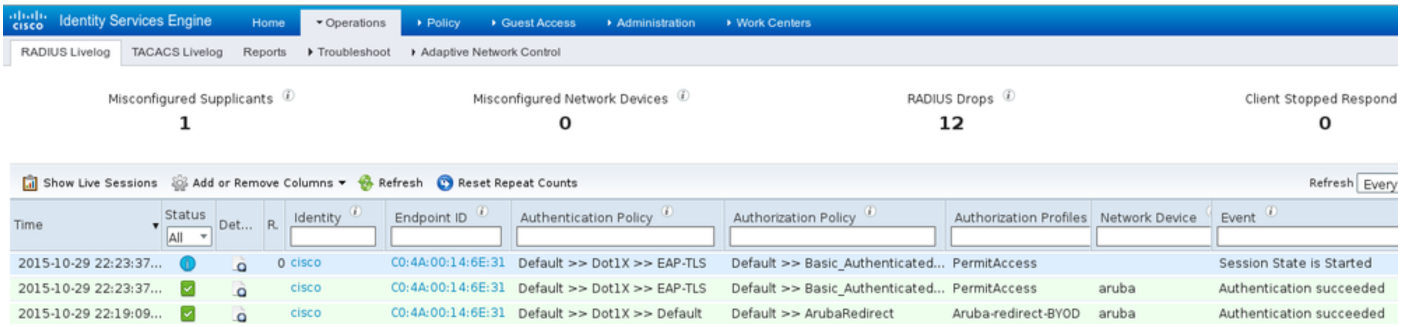
Options: □ Log □ Blacklist □ Classify media □ Disable scanning □ DSCP tag □ 802.1p priority

驗證

使用本節內容，確認您的組態是否正常運作。

步驟 1.使用EAP-PEAP連線到SSID mgarcarz_aruba

出現ISE上的第一個身份驗證日誌。已使用預設身份驗證策略，已返回Aruba-redirect-BYOD授權配置檔案，如下圖所示。



Misconfigured Supplicants 1

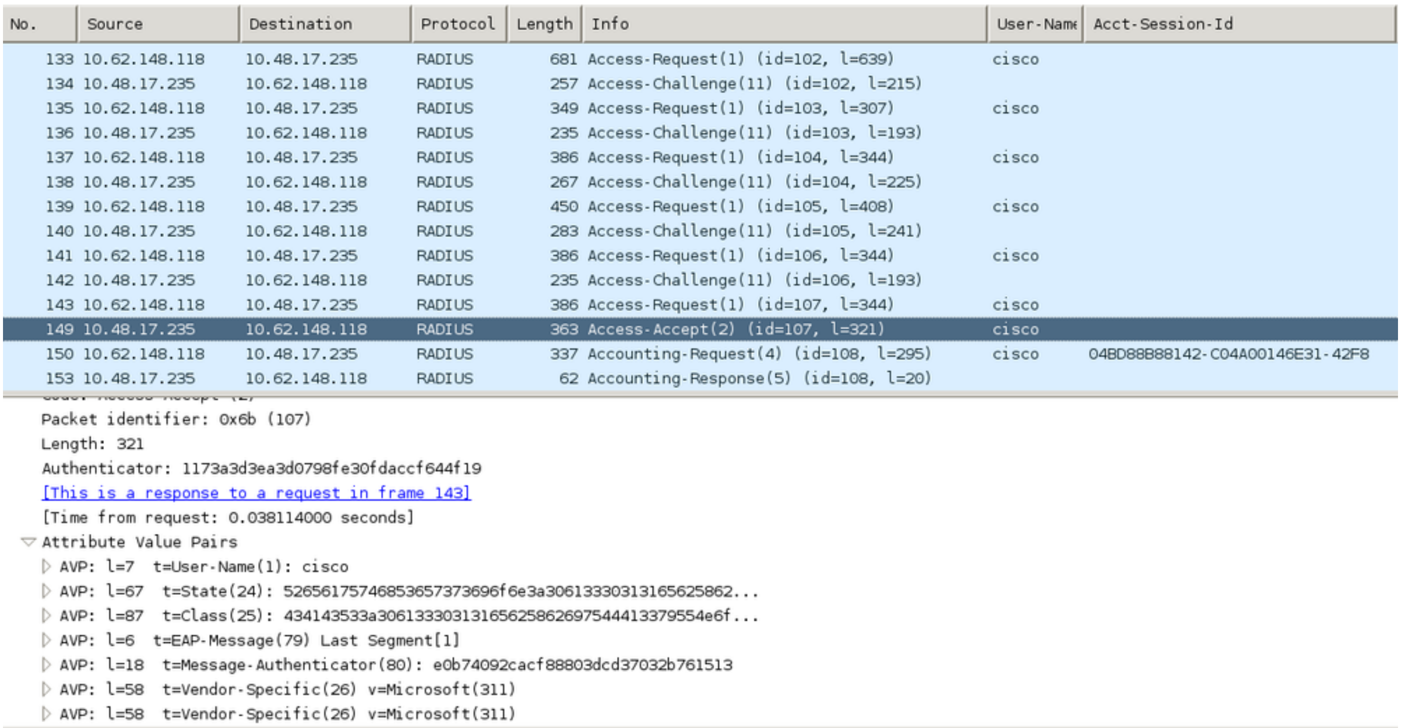
Misconfigured Network Devices 0

RADIUS Drops 12

Client Stopped Respond 0

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

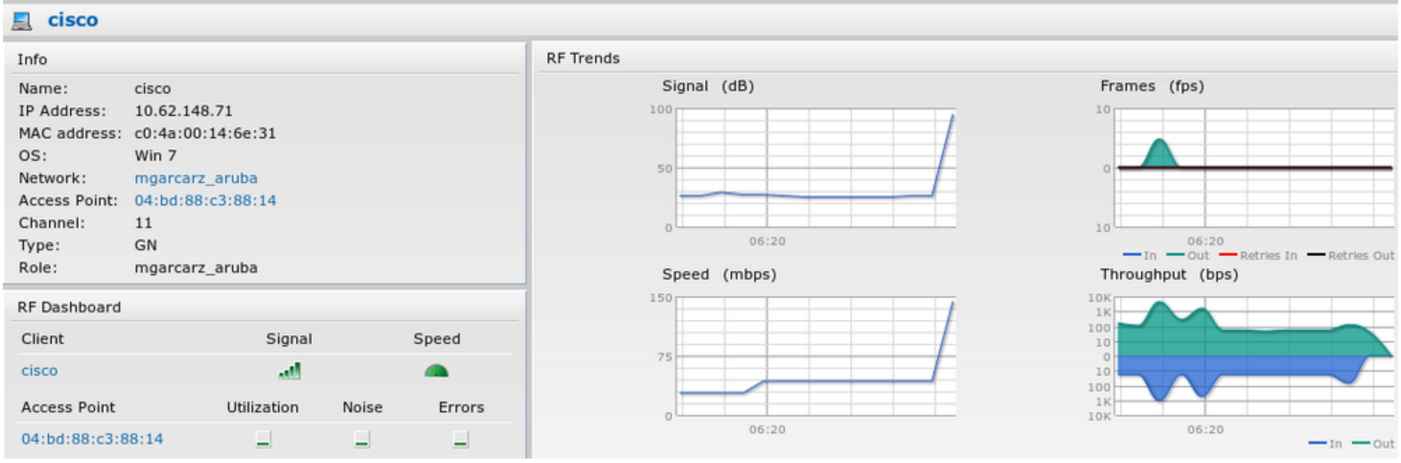
ISE返回Radius Access-Accept消息，EAP成功。 請注意，不會傳回其他屬性（無Cisco av配對url-redirect或url-redirect-acl），如下圖所示。



```
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      04BD88B88142-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): 526561757468536573736f6e3a30613330313165625862...
    ▷ 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)
```

Aruba報告會話已建立(EAP-PEAP標識為cisco)，並且選定角色為mgarcarz_aruba，如下圖所示。



cisco

Info

Name:	cisco
IP Address:	10.62.148.71
MAC address:	c0:4a:00:14:6e:31
OS:	Win 7
Network:	mgarcarz_aruba
Access Point:	04:bd:88:c3:88:14
Channel:	11
Type:	GN
Role:	mgarcarz_aruba

RF Dashboard

Client	Signal	Speed
cisco		

Access Point	Utilization	Noise	Errors
04:bd:88:c3:88:14			

RF Trends

該角色負責重定向到ISE（Aruba上的強制網路門戶功能）。

在Aruba CLI中，可以確認該會話的當前授權狀態：

<#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
--------------- ----------------- ------- --------- -------- ----- --------- -----     ----  --
```

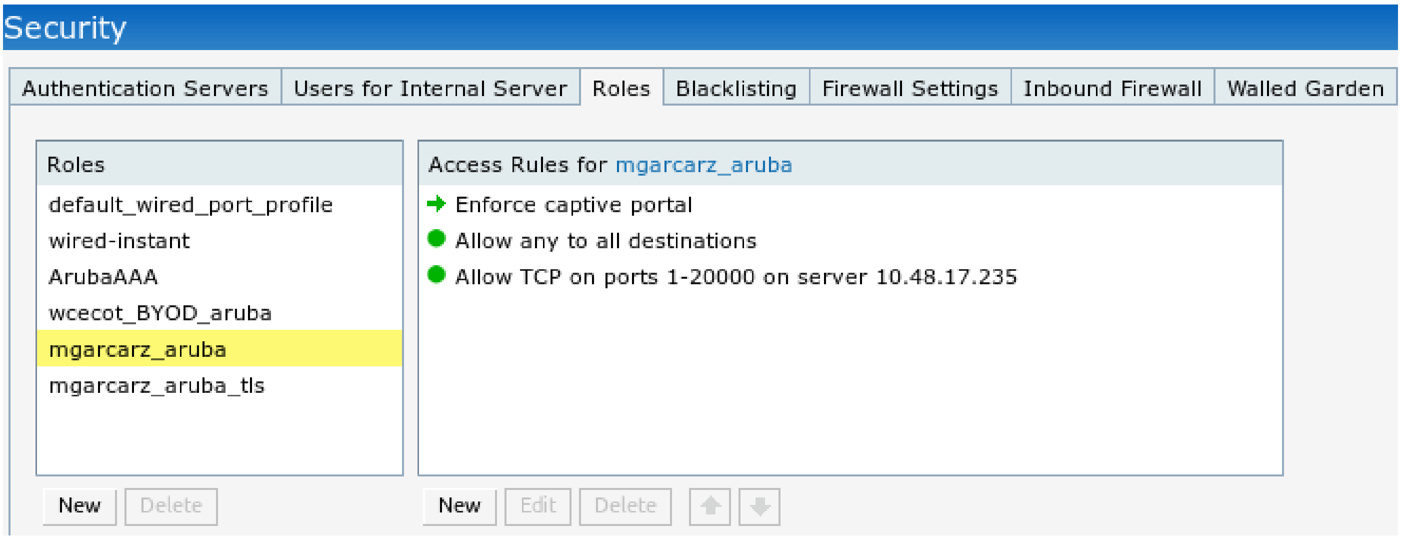
```
10.62.148.118    04:BD:88:C3:88:14   105/0      0/0     0         1        0/65535  P            1   N

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#
```

為了檢查ACL ID 138的當前許可權：

<#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 ... >
```

該配置與GUI中為該角色配置的配置相匹配，如圖所示。



Roles

default_wired_port_profile

wired-instant

ArubaAAA

wcecot_BYOD_aruba

mgarcarz_aruba

mgarcarz_aruba_tls

Access Rules for mgarcarz_aruba

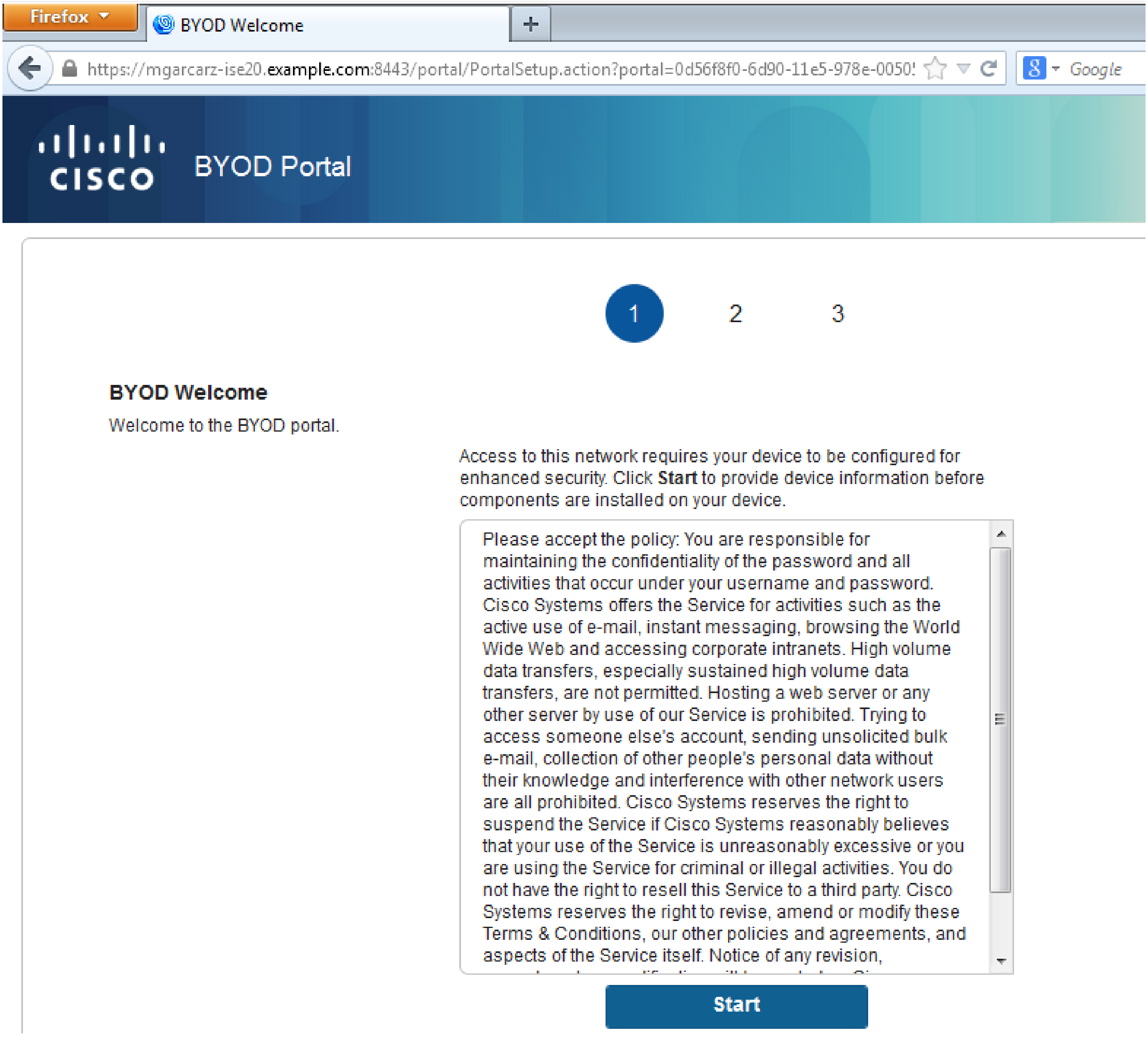
➜ Enforce captive portal

● Allow any to all destinations

● Allow TCP on ports 1-20000 on server 10.48.17.235

步驟 2.適用於BYOD的Web瀏覽器流量重定向

使用者開啟網頁瀏覽器並鍵入任何位址後，便會進行重新導向，如下圖所示。



Firefox
BYOD Welcome
https://mgarcarz-ise20.example.com:8443/portal/PortalSetup.action?portal=0d56f8f0-6d90-11e5-978e-0050!
Google
CISCO
BYOD Portal
1
2
3

BYOD Welcome

Welcome to the BYOD portal.

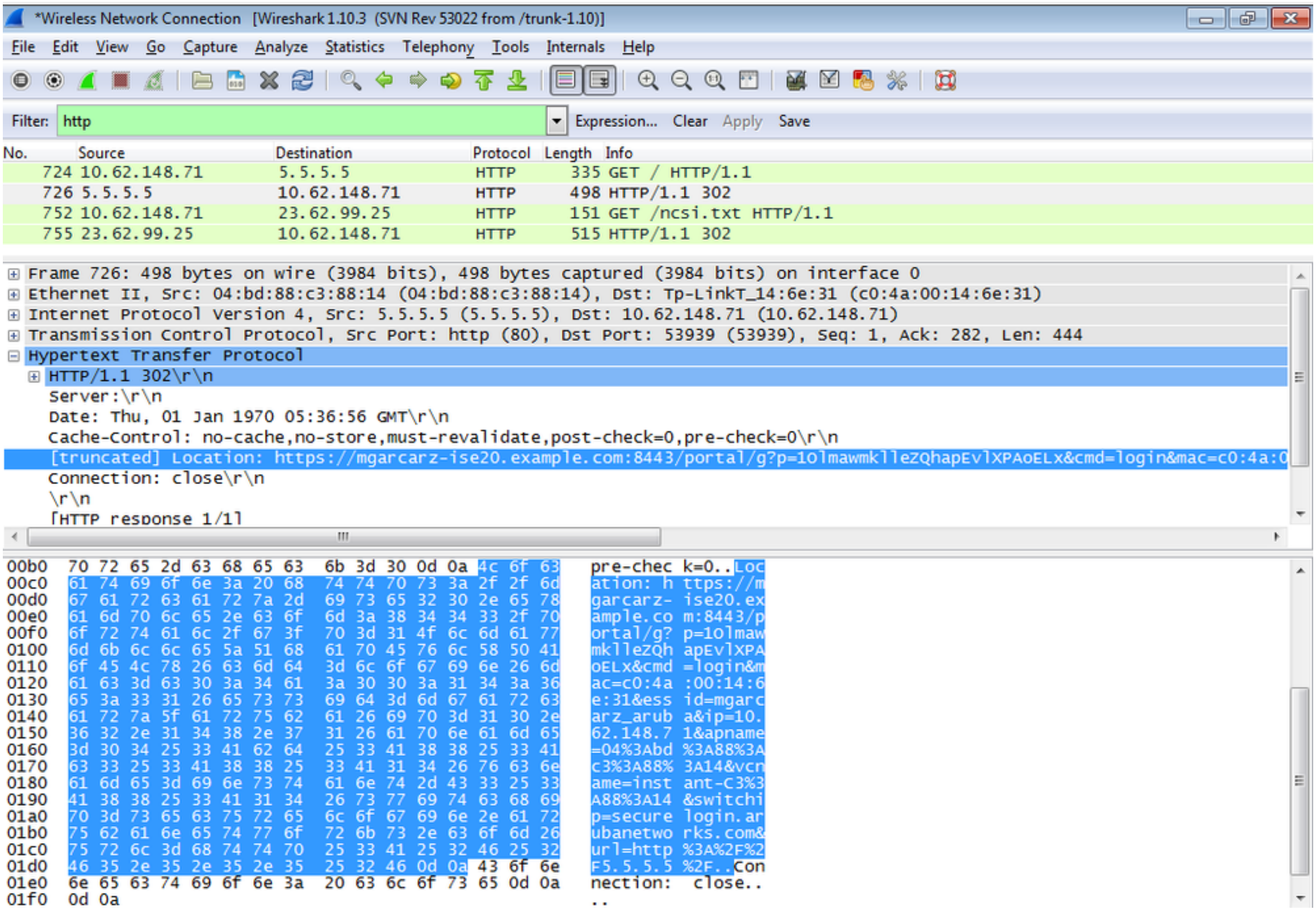
Access to this network requires your device to be configured for enhanced security. Click **Start** to provide device information before components are installed on your device.

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,

檢視資料包捕獲，確認Aruba欺騙目標(5.5.5.5)並返回HTTP重定向至ISE。

請注意，它與ISE中配置的靜態URL相同，並複製到Aruba上的Captive Portal — 但另外新增多個引數，如下所示，如下圖所示：

- cmd =登入
- mac = c0:4a:00:14:6e:31
- essid = mgarcarz_aruba
- ip = 10.62.148.7
- apname = 4bd88c38814(mac)
- url = http://5.5.5.5


*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
 724 10.62.148.71    5.5.5.5         HTTP     335 GET / HTTP/1.1
 726 5.5.5.5         10.62.148.71    HTTP     498 HTTP/1.1 302
 752 10.62.148.71    23.62.99.25     HTTP     151 GET /ncsi.txt HTTP/1.1
 755 23.62.99.25     10.62.148.71    HTTP     515 HTTP/1.1 302
```

```
⊞ Frame 726: 498 bytes on wire (3984 bits), 498 bytes captured (3984 bits) on interface 0
⊞ Ethernet II, Src: 04:bd:88:c3:88:14 (04:bd:88:c3:88:14), Dst: Tp-LinkT_14:6e:31 (c0:4a:00:14:6e:31)
⊞ Internet Protocol Version 4, Src: 5.5.5.5 (5.5.5.5), Dst: 10.62.148.71 (10.62.148.71)
⊞ Transmission Control Protocol, Src Port: http (80), Dst Port: 53939 (53939), Seq: 1, Ack: 282, Len: 444
⊟ Hypertext Transfer Protocol
  ⊞ HTTP/1.1 302\r\n
    Server:\r\n
    Date: Thu, 01 Jan 1970 05:36:56 GMT\r\n
    Cache-Control: no-cache,no-store,must-revalidate,post-check=0,pre-check=0\r\n
    [truncated] Location: https://mgarcarz-ise20.example.com:8443/portal/g?p=10lmawmklleZQhapEvlXPAoELx&cmd=login&mac=c0:4a:0
    Connection: close\r\n
    \r\n
    [HTTP response 1/1]
```

```
00b0  70 72 65 2d 63 68 65 63  6b 3d 30 0d 0a 4c 6f 63   pre-chec k=0..Loc
00c0  61 74 69 6f 6e 3a 20 68  74 74 70 73 3a 2f 2f 6d   ation: h ttps://m
00d0  67 61 72 63 61 72 7a 2d  69 73 65 32 30 2e 65 78   garcarz- ise20.ex
00e0  61 6d 70 6c 65 2e 63 6f  6d 3a 38 34 34 33 2f 70   ample.co m:8443/p
00f0  6f 72 74 61 6c 2f 67 3f  70 3d 31 4f 6c 6d 61 77   ortal/g? p=1Olmaw
0100  6d 6b 6c 6c 65 5a 51 68  61 70 45 76 6c 58 50 41   mklleZQh apEvlXPA
0110  6f 45 4c 78 26 63 6d 64  3d 6c 6f 67 69 6e 26 6d   oELx&cmd =login&m
0120  61 63 3d 63 30 3a 34 61  3a 30 30 3a 31 34 3a 36   ac=c0:4a :00:14:6
0130  65 3a 33 31 26 65 73 73  69 64 3d 6d 67 61 72 63   e:31&ess id=mgarc
0140  61 72 7a 5f 61 72 75 62  61 26 69 70 3d 31 30 2e   arz_arub a&ip=10.
0150  36 32 2e 31 34 38 2e 37  31 26 61 70 6e 61 6d 65   62.148.7 1&apname
0160  3d 30 34 25 33 41 62 64  25 33 41 38 38 25 33 41   =04%3Abd %3A88%3A
0170  63 33 25 33 41 38 38 25  33 41 31 34 26 76 63 6e   c3%3A88% 3A14&vcn
0180  61 6d 65 3d 69 6e 73 74  61 6e 74 2d 43 33 25 33   ame=inst ant-C3%3
0190  41 38 38 25 33 41 31 34  26 73 77 69 74 63 68 69   A88%3A14 &switchi
01a0  70 3d 73 65 63 75 72 65  6c 6f 67 69 6e 2e 61 72   p=secure login.ar
01b0  75 62 61 6e 65 74 77 6f  72 6b 73 2e 63 6f 6d 26   ubanetwo rks.com&
01c0  75 72 6c 3d 68 74 74 70  25 33 41 25 32 46 25 32   url=http %3A%2F%2
01d0  46 35 2e 35 2e 35 2e 35  25 32 46 0d 0a 43 6f 6e   F5.5.5.5 %2F..Con
01e0  6e 65 63 74 69 6f 6e 3a  20 63 6c 6f 73 65 0d 0a   nection:  close..
01f0  0d 0a                                              ..
```

由於這些引數，ISE能夠重新建立思科會話ID，在ISE上查詢相應的會話，並繼續進行BYOD（或任何其他已配置的）流程。

對於Cisco裝置，通常使用audit_session_id，但其他供應商不支援該功能。

為了確認從ISE調試，可能會看到生成稽核會話ID值（從不通過網路傳送）：

<#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`

然後，在BYOD第2頁上註冊裝置後進行關聯：

<#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
```

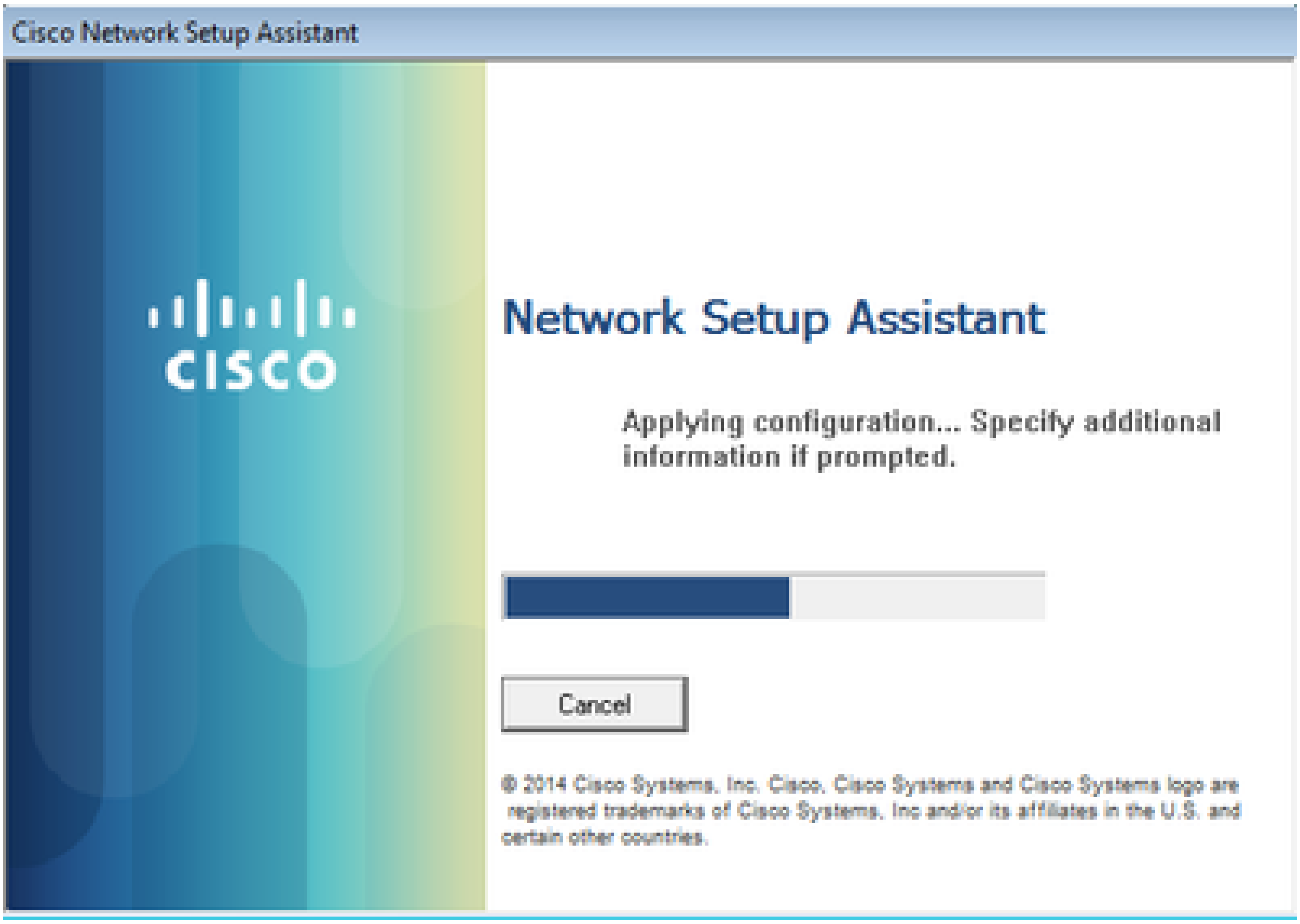
`MyDevices: Successfully registered/provisioned the device`

```
(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

在後續請求中，客戶端被重定向到BYOD第3頁，在該頁中下載並執行NSA。

步驟 3.網路設定助理執行



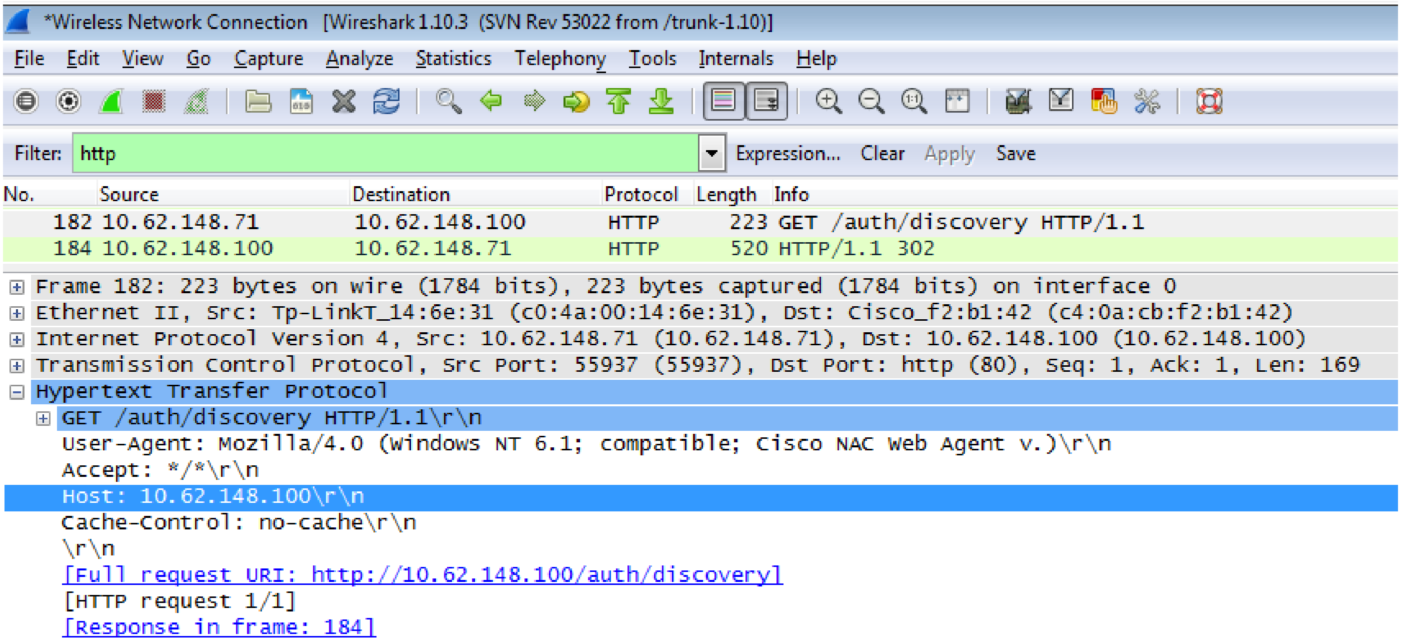
Applying configuration... Specify additional information if prompted.

© 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.

NSA的任務與網路瀏覽器相同。首先，它需要檢測ISE的IP地址。這是通過HTTP重定向實現的。

由於這一次，使用者無法鍵入IP地址（如在Web瀏覽器中），因此該流量會自動生成。

使用預設閘道(也可使用enroll.cisco.com)，如下圖所示。


*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\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]
```

響應與Web瀏覽器的響應完全相同。

這樣，NSA可以連線到ISE，獲取帶配置的xml配置檔案，生成SCEP請求，將其傳送到ISE，獲取簽名證書（由ISE內部CA簽名），配置無線配置檔案，最後連線到配置的SSID。

從客戶端收集日誌(在Windows上位於%temp%/spwProfile.log)。為清楚起見，省略了部分輸出：

<#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.xm
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: 0a3011ebXbiuDA3yUNoLUvtCRyuPFxkqYJ7TT06foOZ7
```

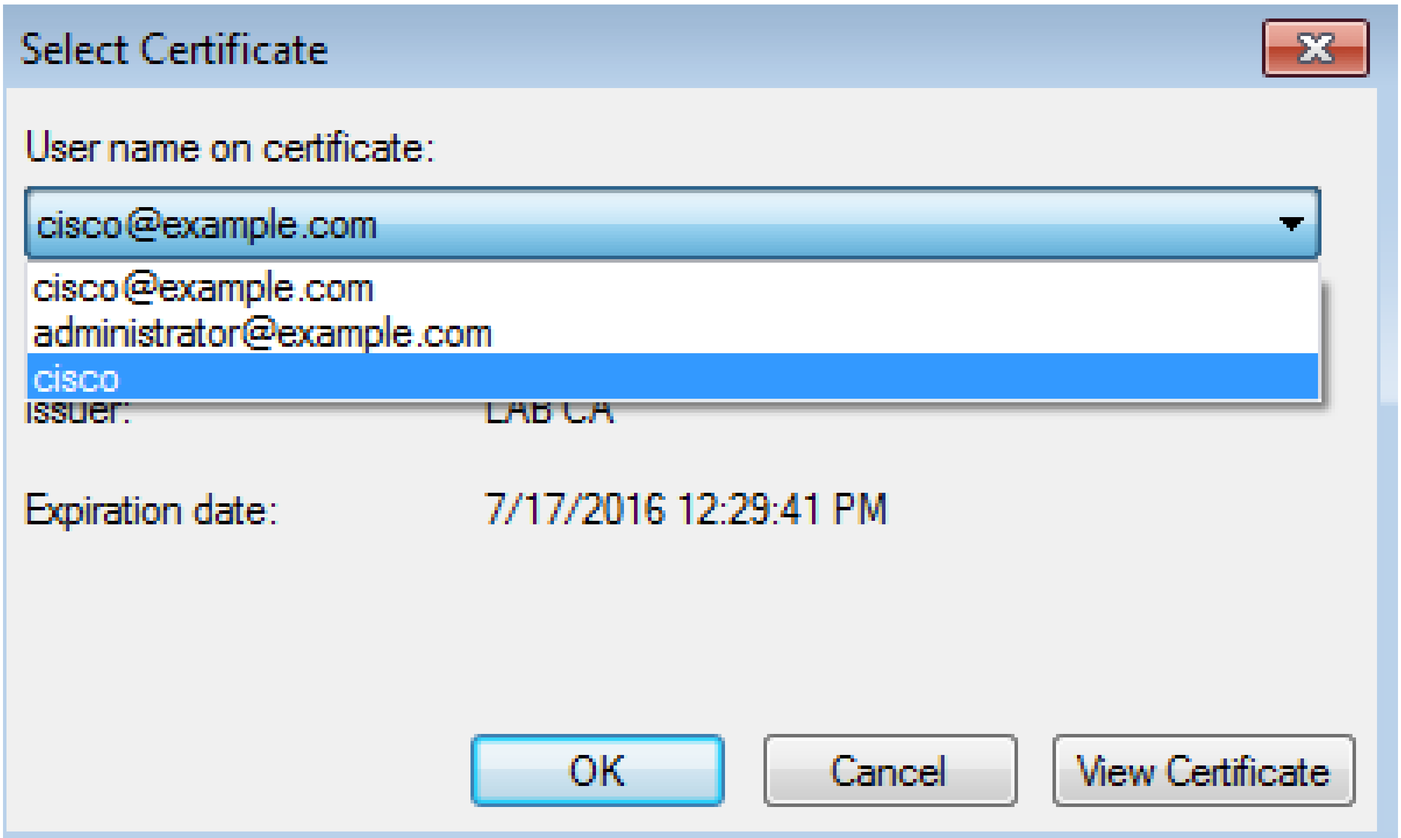
```
DiscoverISE - end

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
```

這些日誌與使用思科裝置的BYOD流程完全相同。

註：此處不需要Radius CoA。強制重新連線到新配置的SSID的是應用程式(NSA)。

在此階段，使用者會看到系統嘗試與最終的SSID關聯。如果您有多個使用者證書，則必須選擇正確的證書（如圖所示）。



Select Certificate

User name on certificate:

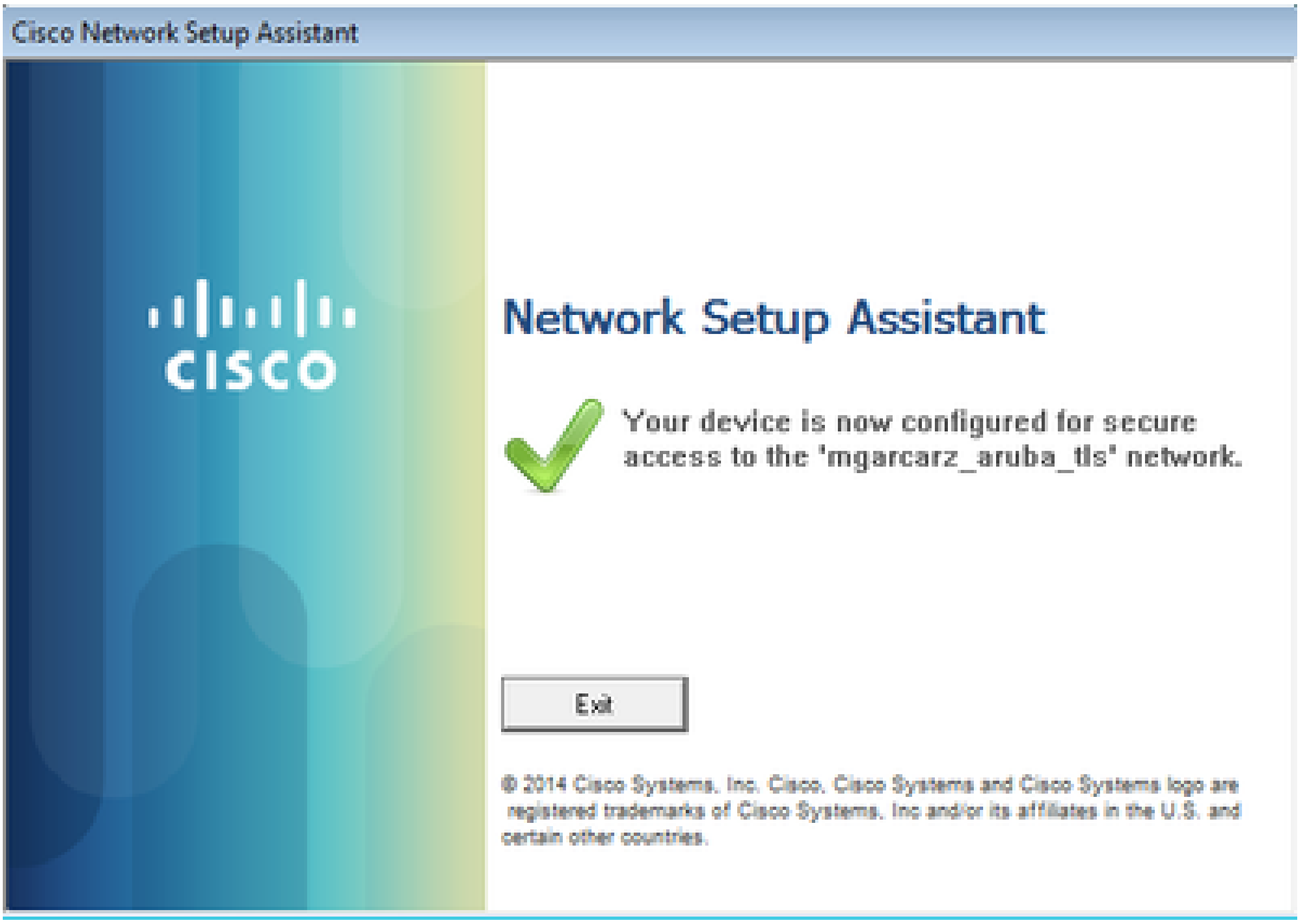
cisco@example.com

cisco@example.com
administrator@example.com
cisco

Issuer: LAB CA

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

成功連線後，NSA報告如下圖所示。



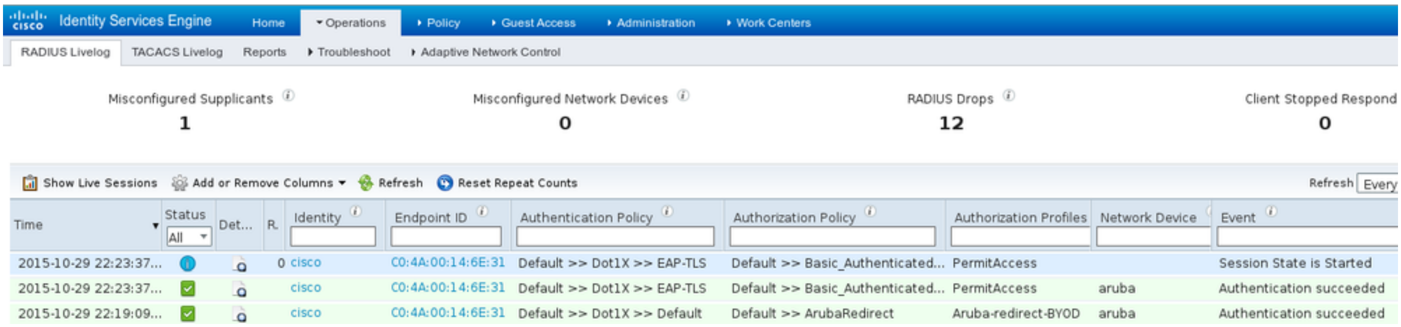
Cisco Network Setup Assistant

Network Setup Assistant

Your device is now configured for secure access to the 'mgarcarz_aruba_tls' network.

© 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.

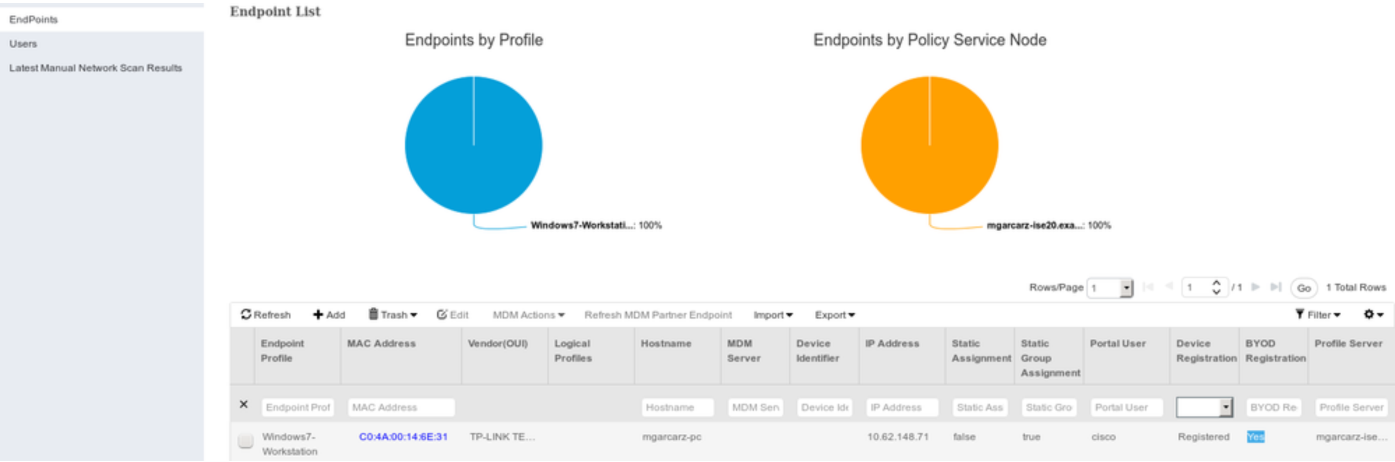
可在ISE上確認 — 第二個日誌命中EAP-TLS身份驗證，該身份驗證與Basic_Authenticated_Access的所有條件匹配（EAP-TLS、Employee和BYOD Registered true）。



Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Respond
1	0	12	0

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...	✓			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

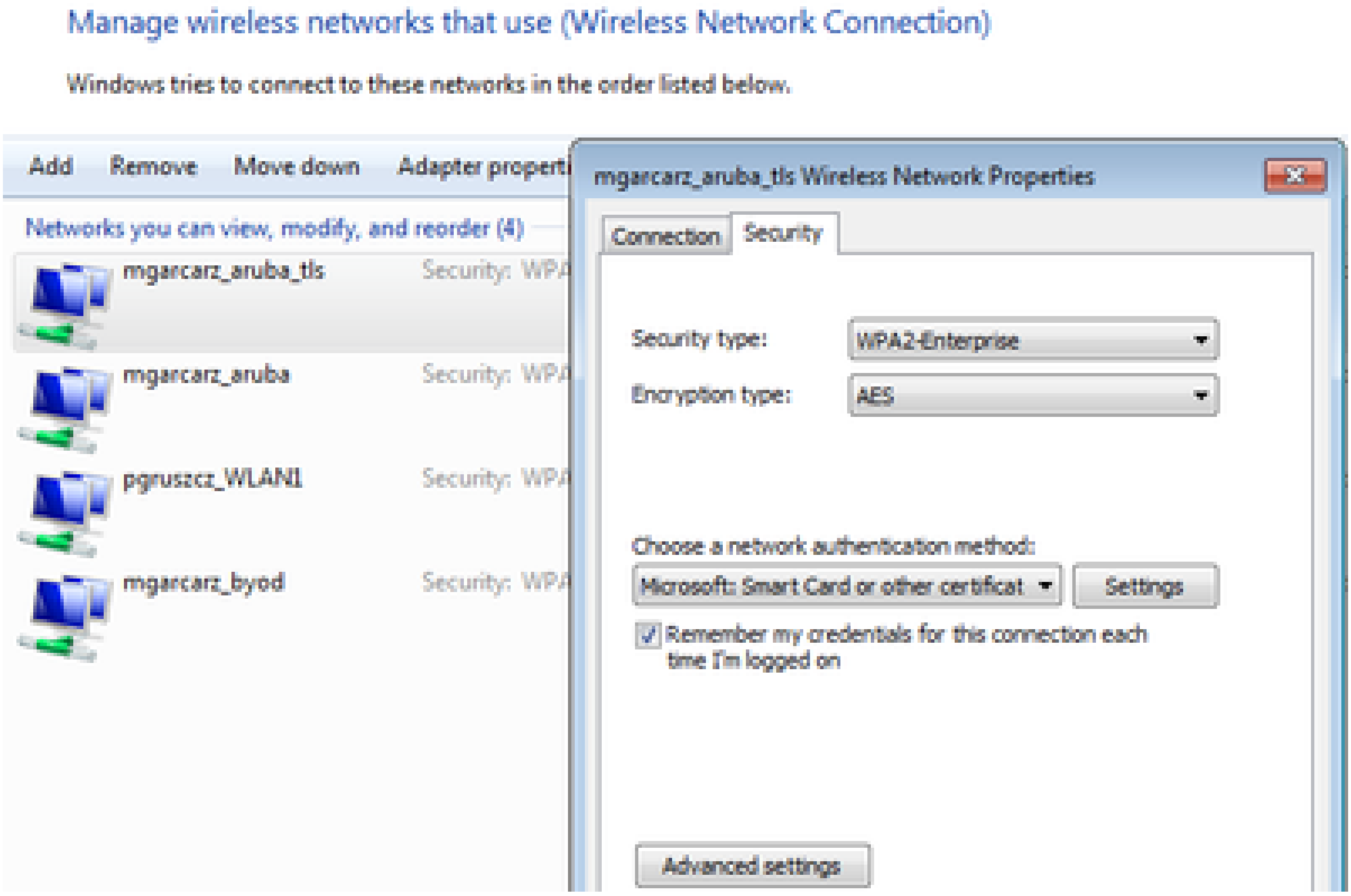
此外，終端身份檢視可以確認終端的BYOD註冊標誌設定為true，如圖所示。



EndPoints
Users
Latest Manual Network Scan Results
Endpoint List
Endpoints by Profile
Windows7-Workstati...: 100%
Endpoints by Policy Service Node
mgarcarz-ise20.exa...: 100%
Rows/Page 1
1 /1
Go
1 Total Rows
Refresh
Add
Trash
Edit
MDM Actions
Refresh MDM Partner Endpoint
Import
Export
Filter

Endpoint Profile	MAC Address	Vendor(OUI)	Logical Profiles	Hostname	MDM Server	Device Identifier	IP Address	Static Assignment	Static Group Assignment	Portal User	Device Registration	BYOD Registration	Profile Server
Windows7-Workstation	C0:4A:00:14:6E:31	TP-LINK TE...		mgarcarz-pc			10.62.148.71	false	true	cisco	Registered	Yes	mgarcarz-ise...

在Windows PC上，新的無線配置檔案已自動建立為首選（並配置為EAP-TLS）並如圖所示。



Manage wireless networks that use (Wireless Network Connection)

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

Security type: WPA2-Enterprise

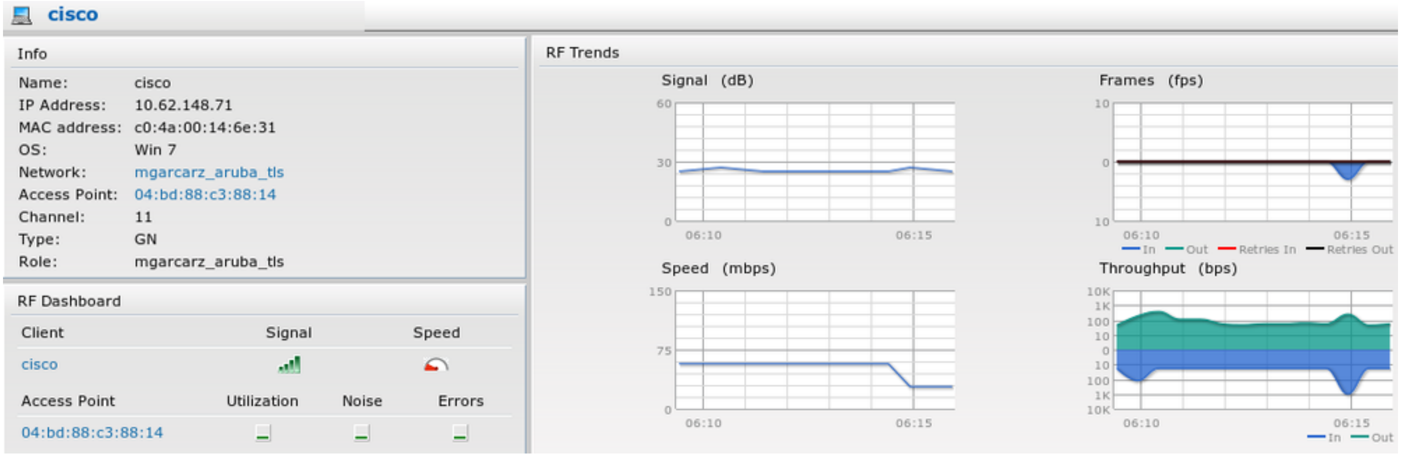
Encryption type: AES

Choose a network authentication method:

Microsoft: Smart Card or other certificat

☑ Remember my credentials for this connection each time I'm logged on

在此階段，Aruba確認使用者已連線到最終的SSID。



cisco

Info

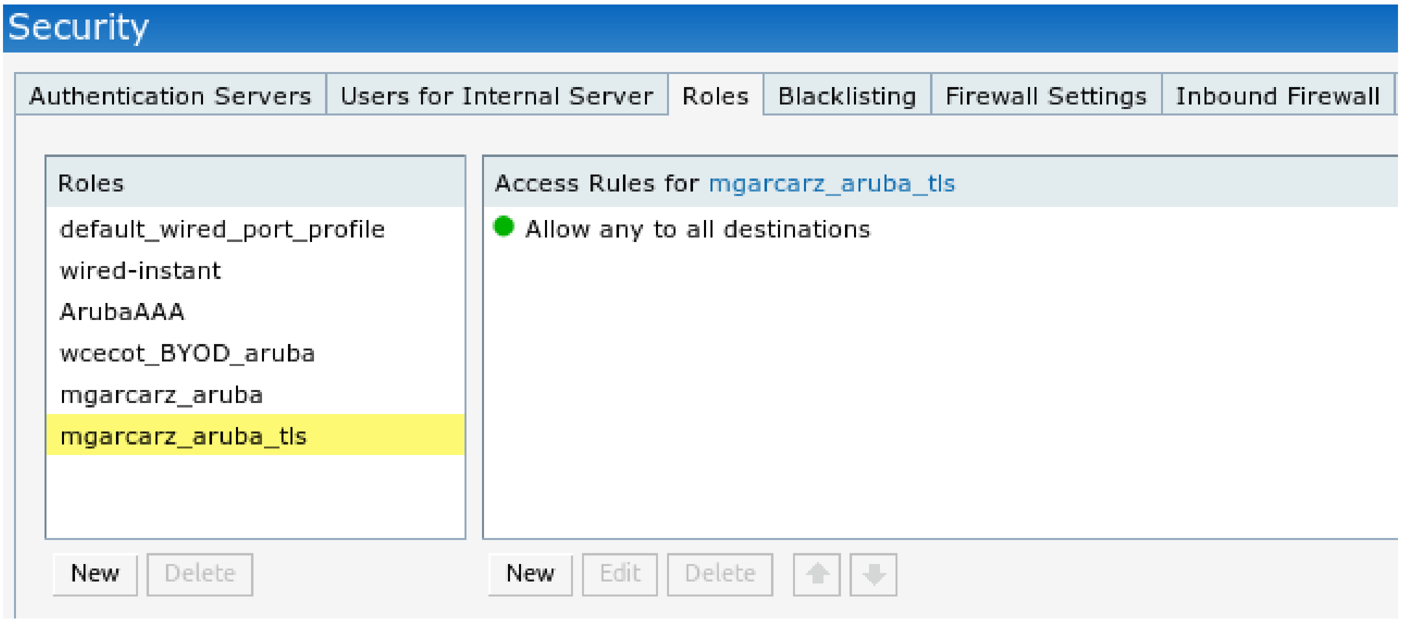
Name:	cisco
IP Address:	10.62.148.71
MAC address:	c0:4a:00:14:6e:31
OS:	Win 7
Network:	mgarcarz_aruba_tls
Access Point:	04:bd:88:c3:88:14
Channel:	11
Type:	GN
Role:	mgarcarz_aruba_tls

RF Dashboard

Client	Signal	Speed
cisco		

Access Point	Utilization	Noise	Errors
04:bd:88:c3:88:14			

自動建立並命名為「與網路相同」的角色提供完整的網路訪問。



Security

Roles

default_wired_port_profile

wired-instant

ArubaAAA

wcecot_BYOD_aruba

mgarcarz_aruba

mgarcarz_aruba_tls

Access Rules for mgarcarz_aruba_tls

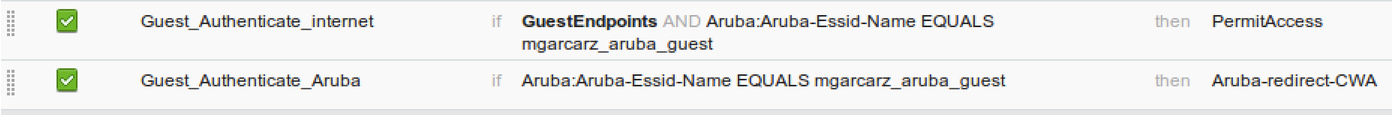
● Allow any to all destinations

其他流量和CoA支援

帶CoA的CWA

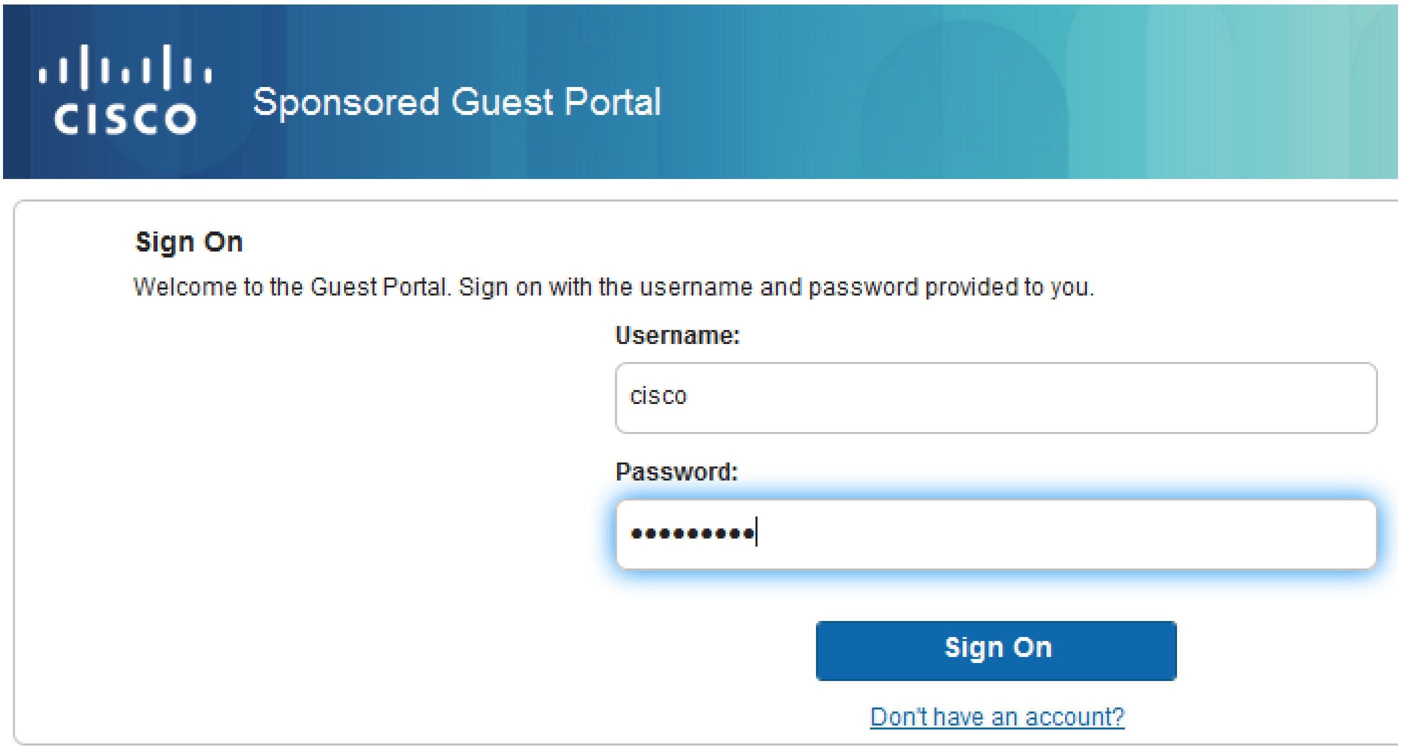
雖然在BYOD流中沒有CoA消息，但此處演示了具有自註冊訪客門戶的CWA流：

已配置的授權規則如下圖所示。



☑	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

使用者通過MAB身份驗證連線到SSID，一旦嘗試連線到某個網頁，就會重定向到自行註冊的訪客門戶，訪客可以在其中建立新帳戶或使用當前帳戶。



Sponsored Guest Portal

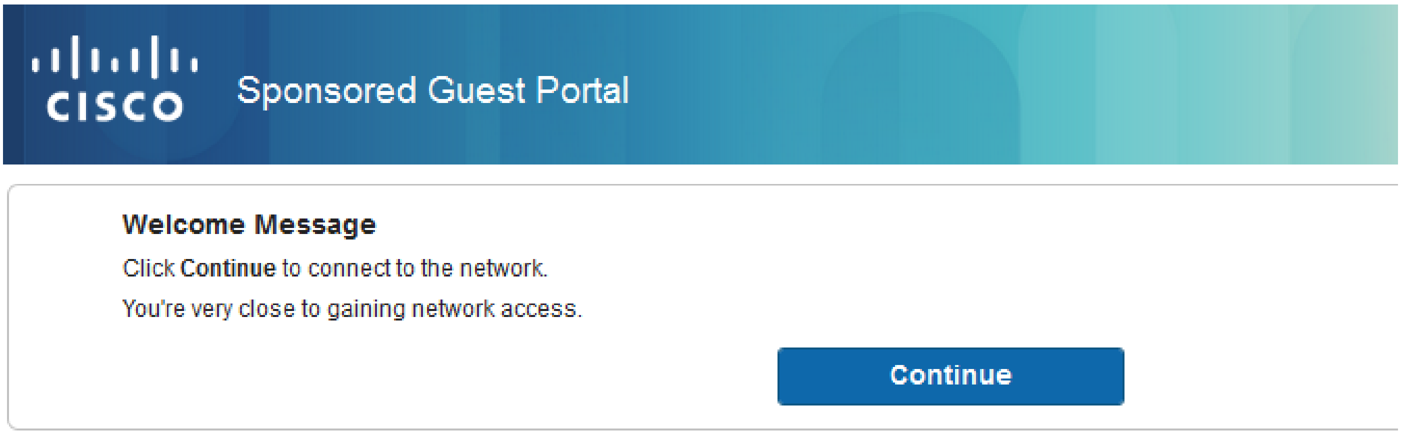
Sign On

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

Username: cisco

Password: ●●●●●●●●●

成功連線訪客後，會將CoA消息從ISE傳送到網路裝置以更改授權狀態。



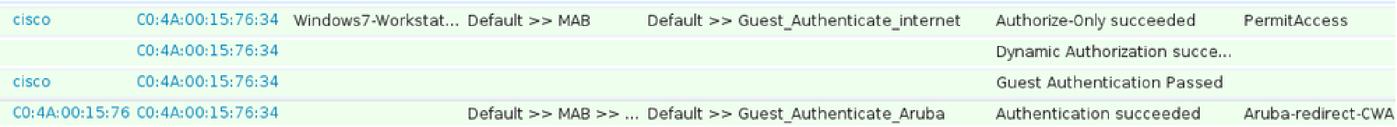
Sponsored Guest Portal

Welcome Message

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

You're very close to gaining network access.

可以在Operations > Authentications下驗證它，如下圖所示。



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調試中的CoA消息：

<#root>

```
2015-11-02 18:47:49,553 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
```

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=0a3011ebisZXypODwqjB6j64GeFiF7RwvyocneEia17ckjtU1HI.,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

和Aruba提供的Disconnect-ACK:

<#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,
```

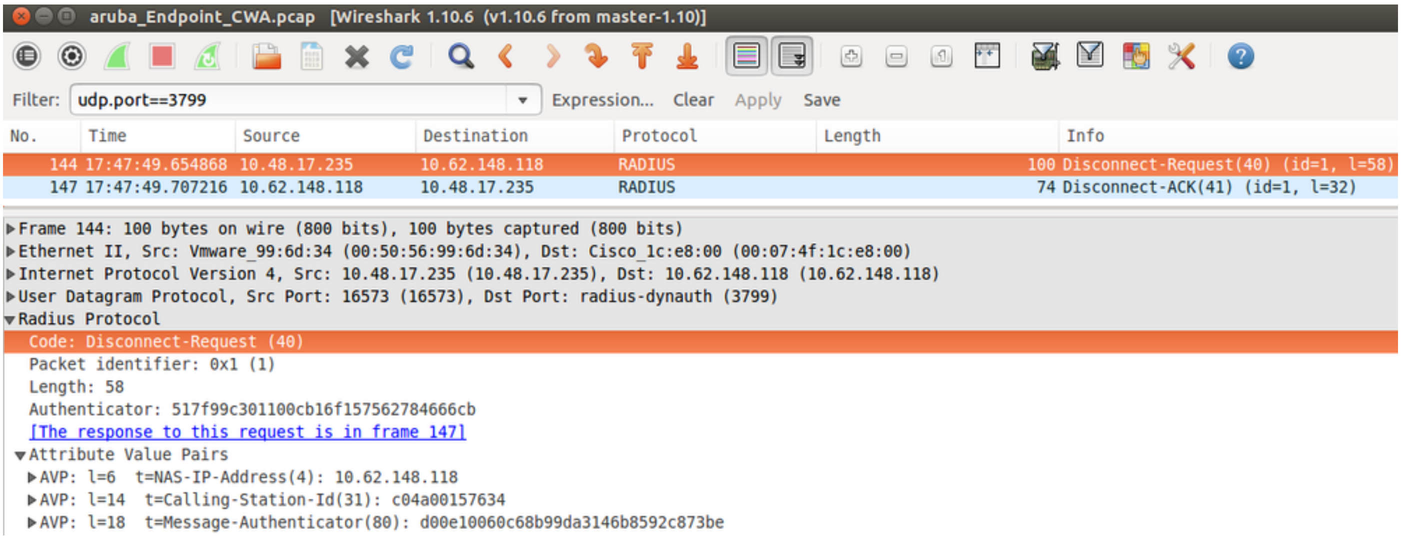
CallingStationID=c04a00157634

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

Packet type 41(DisconnectACK).

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

圖中所示為CoA Diconnect-Request(40)和Diconnect-ACK(41)資料包捕獲。



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

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 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)
```

```
▶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
```

注意:RFC CoA已用於與裝置配置檔案Aruba（預設設定）相關的身份驗證。對於與Cisco裝置相關的身份驗證，應該是Cisco CoA型別重新進行身份驗證。

疑難排解

本節提供的資訊可用於對組態進行疑難排解。

具有IP地址而不是FQDN的Aruba強制網路門戶

如果Aruba上的強制網路門戶配置了IP地址而不是ISE的FQDN，則PSN NSA失敗：

<#root>

```
Warning - [HTTPConnection]

Abort the HTTP connection due to invalid certificate



CN
```

原因是在連線到ISE時進行嚴格的證書驗證。當您使用IP地址連線到ISE時（由於重定向URL使用IP地址而不是FQDN），並且會顯示ISE證書，主題名稱= FQDN驗證失敗。

注意:Web瀏覽器繼續運行BYOD門戶（帶有需要使用者批准的警告）。

Aruba強制網路門戶訪問策略不正確

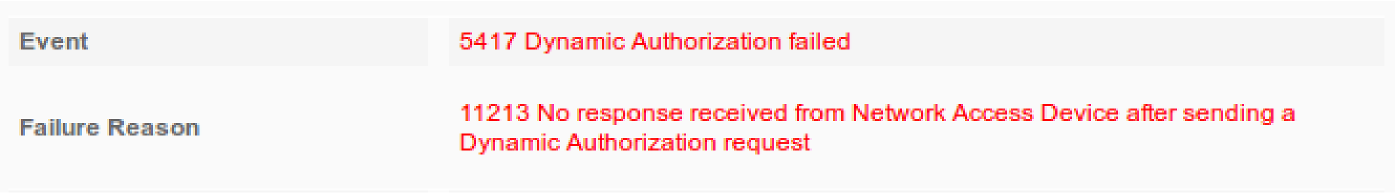
預設情況下，配置了Captive Portal的Aruba Access-Policy允許tcp埠80、443和8080。

NSA無法連線到tcp埠8905以便從ISE獲取xml配置檔案。報告以下錯誤：

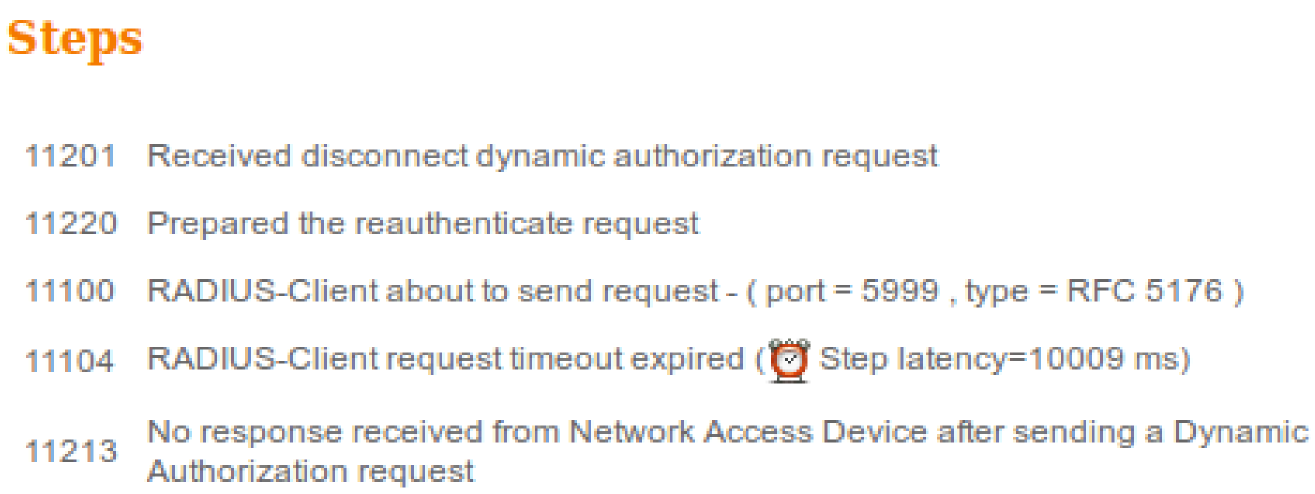
```
<#root>
Failed to get spw profile url using - url

[

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=0a3011ebXbiuDA3yUNoLUvtCRyuPFxkqYJ7TT06foOZ7G1HXj1M&os=Windows All]
- http Error: [2]

HTTP response code: 0

]
GetProfile - end
Failed to get profile. Error: 2
```

Aruba CoA埠號

預設情況下，Aruba為CoA Air Group CoA埠5999提供端口號。遺憾的是，Aruba 204沒有回應這些請求（如圖所示）。



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

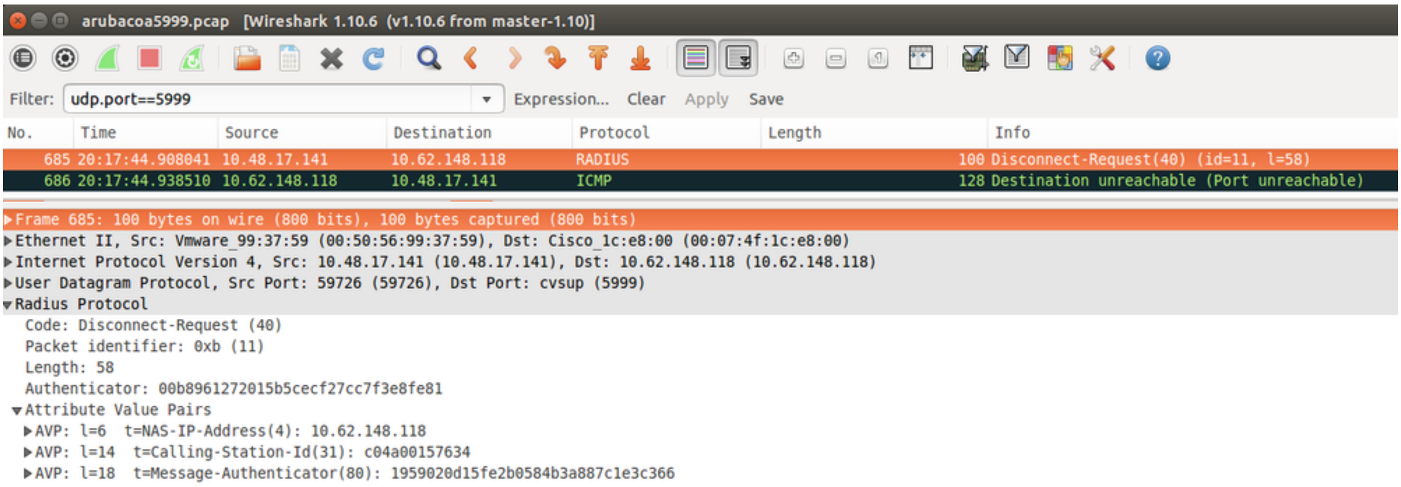
11220 Prepared the reauthenticate request

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

封包擷取如圖所示。

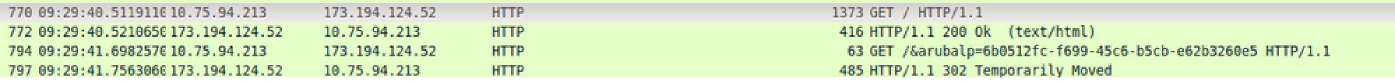


```
arubacoa5999.pcap  [Wireshark 1.10.6  (v1.10.6 from master-1.10)]
Filter: udp.port==5999                     Expression...  Clear  Apply  Save

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
```

此處使用的最佳選項可以是CoA連線埠3977，如RFC 5176所述。

某些Aruba裝置上的重新導向

在搭載v6.3的Aruba 3600上，我們注意到重新導向的運作方式與其他控制器略有不同。資料包捕獲和解釋可以在此處找到。



```
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 /&arubalp=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/
```

&arubalp=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&essid=SC%2DWiFi&apname=LRC-006&apgroup=default&url=http%3A%2F%2Fww

相關資訊

- 思科身份服務引擎管理員指南2.0版
- 使用思科身份服務引擎的網路訪問裝置配置檔案
- 技術支援與文件 - Cisco Systems