配置ISE 2.0第三方与Aruba无线集成

目录

简介

本文档介绍如何对思科身份服务引擎(ISE)上的第三方集成功能进行故障排除。

注意：请注意，思科不负责配置或支持其他供应商的设备。

先决条件

要求

Cisco 建议您了解以下主题：

- Aruba IAP配置
- ISE上的自带设备流
- 密码和证书身份验证的ISE配置

使用的组件

本文档介绍如何对思科身份服务引擎(ISE)上的第三方集成功能进行故障排除。

它可以作为与其他供应商和流程集成的指南。ISE版本2.0支持第三方集成。

本配置示例展示如何将Aruba IAP 204管理的无线网络与ISE集成以实现自带设备(BYOD)服务。

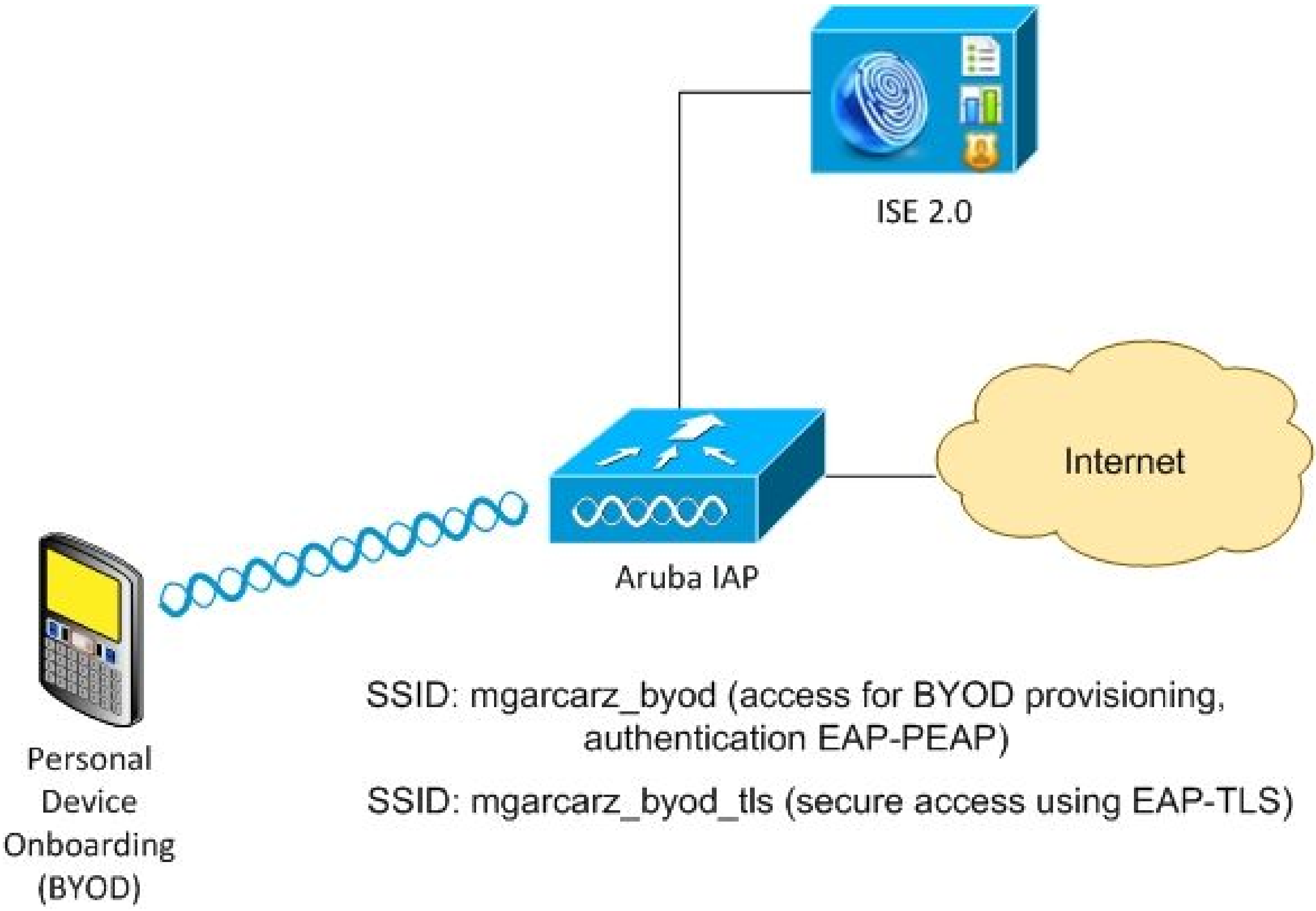
本文档中的信息基于以下软件版本：

- Aruba IAP 204软件6.4.2.3
- 思科ISE版本2.0及更高版本

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

配置

网络图


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

有两个无线网络由Aruba AP管理。

第一个(mgarcarz_byod)用于802.1x可扩展身份验证协议保护EAP(EAP-PEAP)访问。

身份验证成功后，Aruba控制器必须将用户重定向到ISE BYOD门户 — 本地请求方调配(NSP)流程。

用户被重定向，网络设置助理(NSA)应用被执行，证书被调配并安装在Windows客户端上。

ISE内部CA用于该进程（默认配置）。

NSA还负责为Aruba管理的第二个服务集标识符(SSID)(mgarz_byod_tls)创建无线配置文件 — 该配置文件用于802.1x可扩展身份验证协议 — 传输层安全(EAP-TLS)身份验证。

因此，企业用户可以执行个人设备自注册，并安全地访问企业网络。

本示例可以轻松地针对不同类型的访问进行修改，例如：

- 采用BYOD服务的集中式Web身份验证(CWA)
- 使用状况和BYOD重定向的802.1x身份验证
- 通常，对于EAP-PEAP身份验证，使用Active Directory（为了让本文使用短的内部ISE用户）
- 通常，对于使用证书调配外部简单证书注册协议(SCEP)服务器的证书，通常使用Microsoft网络设备注册服务(NDES)来缩短本文的篇幅，使用内部ISE CA。

第三方支持的挑战

将ISE访客流量(例如BYOD、CWA、NSP、客户端调配门户(CPP))与第三方设备配合使用时存在挑战。

会话

Cisco网络接入设备(NAD)使用名为audit-session-id的Radius cisco-av-pair向身份验证、授权和记帐(AAA)服务器通知会话ID。

ISE使用该值跟踪会话并为每个流提供正确的服务。其他供应商不支持cisco-av对。

ISE必须依赖于在访问请求和记帐请求中收到的IETF属性。

收到访问请求后，ISE会构建综合的思科会话ID（从Calling-Station-ID、NAS-Port、NAS-IP-Address和共享密钥）。该值仅具有本地意义（不通过网络发送）。

因此，希望每个流(BYOD、CWA、NSP、CPP)都附加正确的属性，因此ISE能够重新计算思科会话ID并执行查找，以便将其与正确的会话关联并继续流。

URL重定向

ISE使用名为url-redirect和url-redirect-acl的Radius cisco-av-pair通知NAD必须重定向特定流量。

其他供应商不支持cisco-av对。通常，这些设备必须使用指向ISE上特定服务（授权配置文件）的静态重定向URL进行配置。

用户启动HTTP会话后，这些NAD重定向到URL，并附加其他参数（如IP地址或MAC地址），以允许ISE识别特定会话并继续流程。

CoA

ISE使用Radius cisco-av-pair called subscriber:command， subscriber:reauthenticate-type来指示特定会话的NAD必须执行的操作。

其他供应商不支持cisco-av对。因此，这些设备通常使用RFC CoA（3576或5176）和以下两个定义的消息之一：

- 断开连接请求（也称为断开连接数据包）— 用于断开会话（经常用于强制重新连接）
- CoA推送 — 用于透明地更改会话状态而不断开连接（例如VPN会话和应用的新ACL）

ISE同时支持具有cisco-av-pair的Cisco CoA和RFC CoA 3576/5176。

ISE解决方案

为了支持第三方供应商，ISE 2.0引入了网络设备配置文件的概念，描述了特定供应商的行为方式 — 如何支持会话、URL重定向和CoA。

授权配置文件为特定类型（网络设备配置文件），身份验证发生后，ISE行为会从该配置文件派生。

因此，ISE可以轻松管理其他供应商的设备。ISE上的配置也很灵活，可以调整或创建新的网络设备配置文件。

本文介绍Aruba设备默认配置文件的用法。

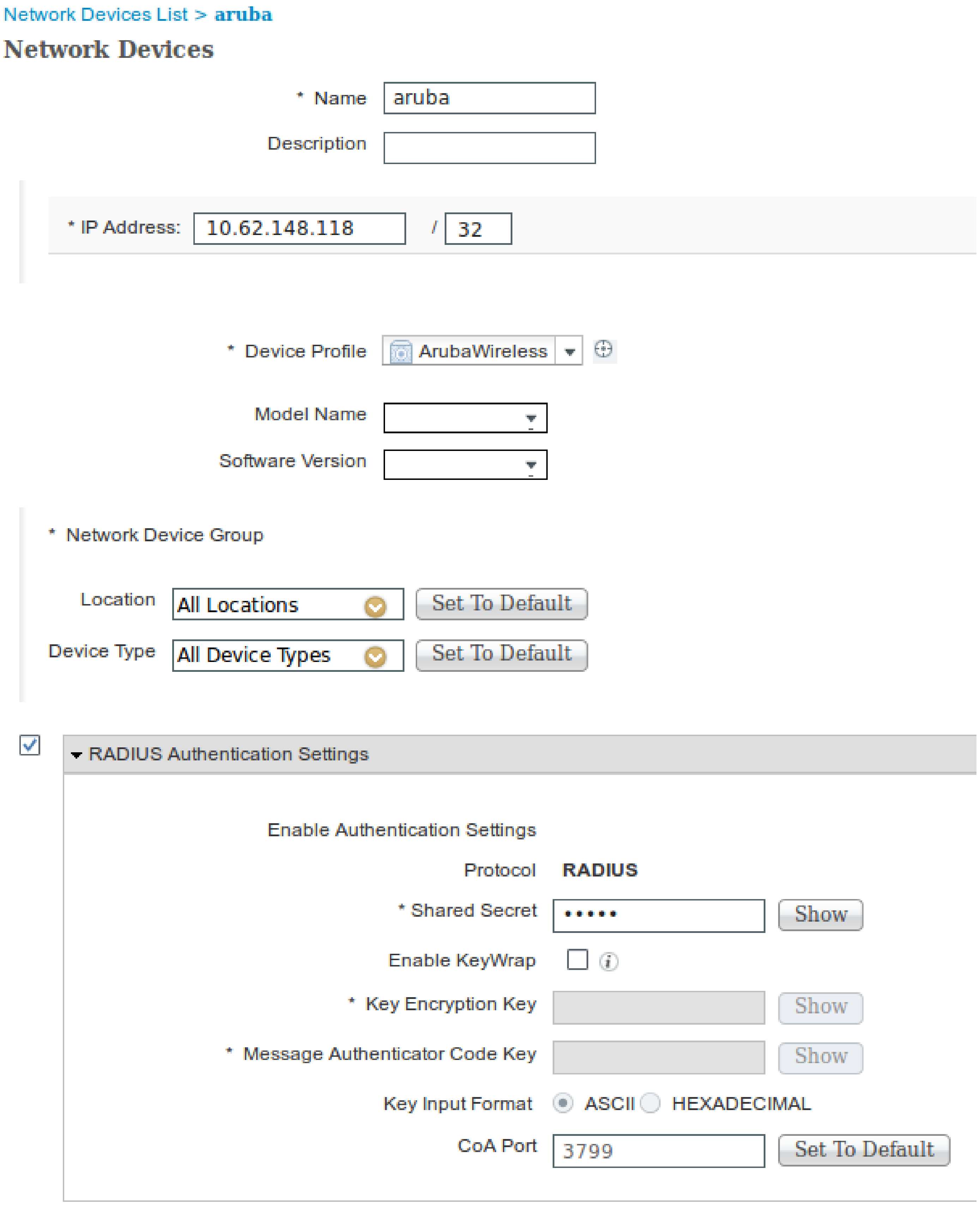
有关功能的详细信息：

使用思科身份服务引擎的网络访问设备配置文件

思科ISE

步骤1:将Aruba无线控制器添加到网络设备

导航到管理>网络资源>网络设备。为所选供应商选择正确的设备配置文件，在本例中为ArubaWireless。 确保配置Shared Secret和CoA端口，如图所示。



Network Devices List > **aruba**

Network Devices

* Name: aruba

Description:

* IP Address: 10.62.148.118 / 32

* Device Profile: ArubaWireless

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

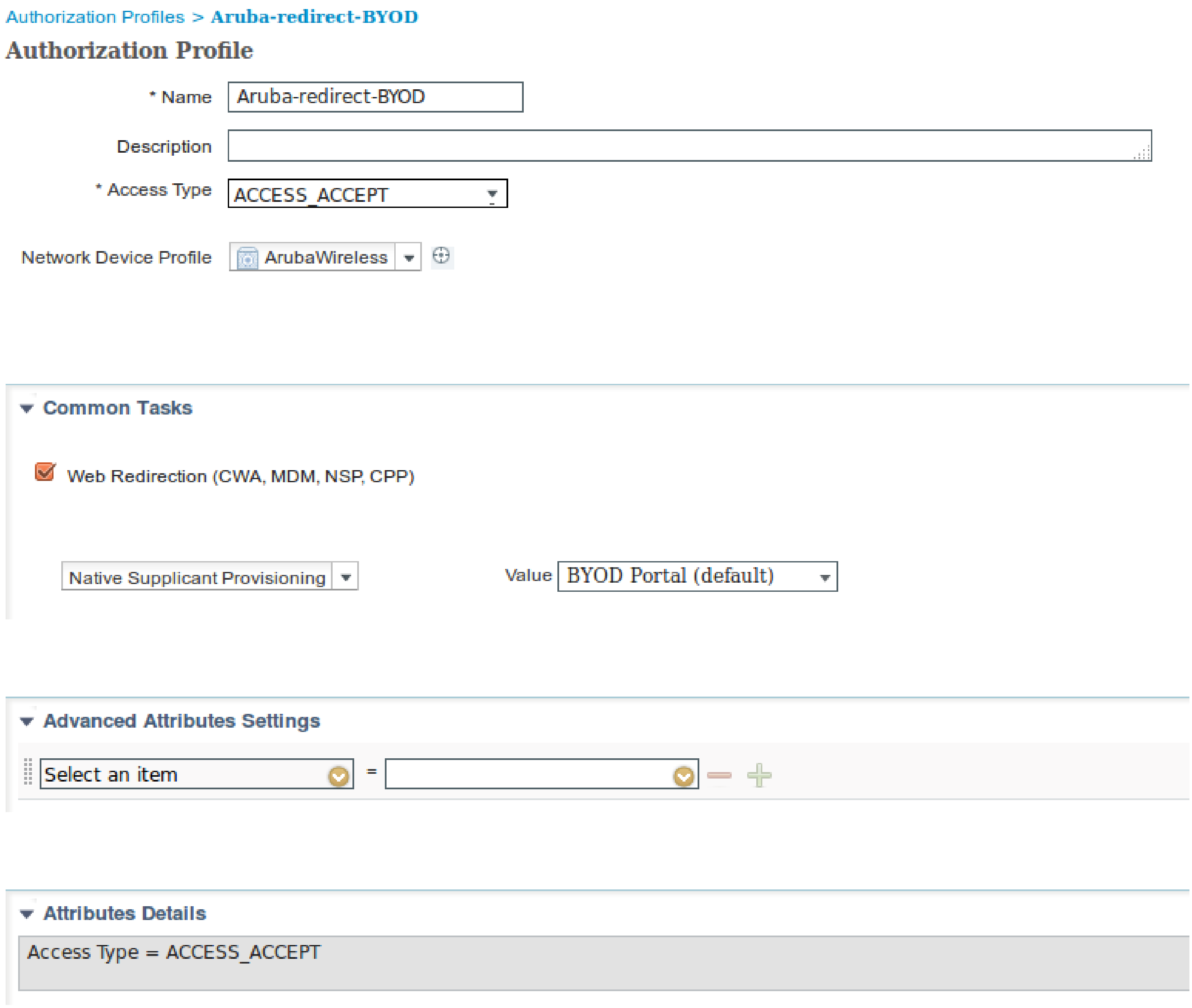
Key Input Format: ● ASCII ○ HEXADECIMAL

CoA Port: 3799 — Set To Default

如果所需供应商没有可用的配置文件，可以在Administration > Network Resources > Network Device Profiles下对其进行配置。

第二步：配置授权配置文件

导航到Policy > Policy Elements > Results > Authorization > Authorization Profiles，选择与步骤1中相同的Network Device Profile。 ArubaWireless。 配置的配置文件是Aruba-redirect-BYOD with BYOD Portal，如图所示。



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)

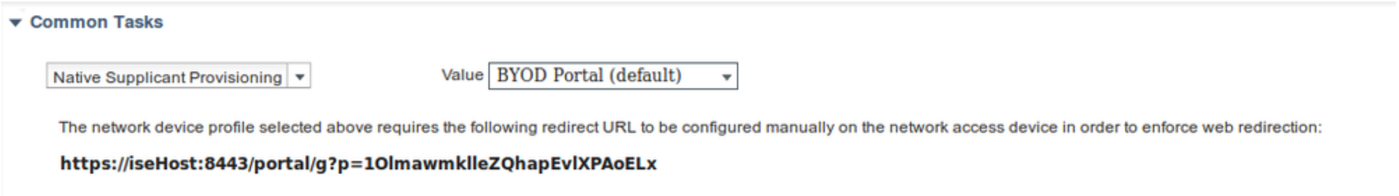
Advanced Attributes Settings

Select an item =

Attributes Details

Access Type = ACCESS_ACCEPT

缺少Web重定向配置的一部分，其中生成了到授权配置文件的静态链接。虽然Aruba不支持动态重定向到访客门户，但每个授权配置文件都分配有一个链接，然后在Aruba上配置该链接，如图所示。



Common Tasks

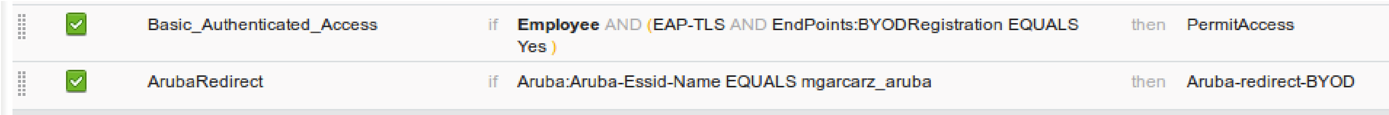
Native Supplicant Provisioning   Value BYOD Portal (default)

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=1OlmawmklleZQhapEvlXPAoELx

第三步：配置授权规则

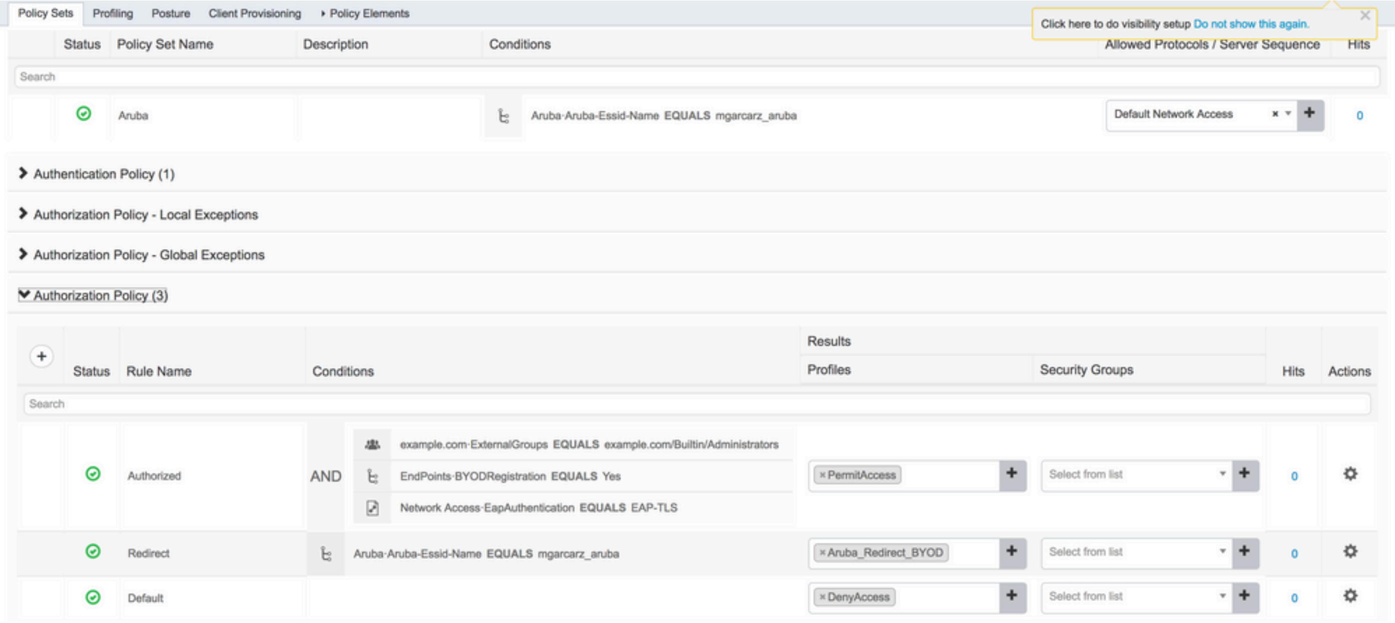
导航到Policy > Authorization Rules，配置如图所示。



	☑	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，用户连接到SSID mgracarz_aruba，ISE返回授权配置文件Aruba-redirect-BYOD，它将客户端重定向到默认BYOD门户。完成BYOD流程后，客户端将使用EAP-TLS进行连接，并授予对网络的完全访问权限。

在ISE的较新版本中，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)

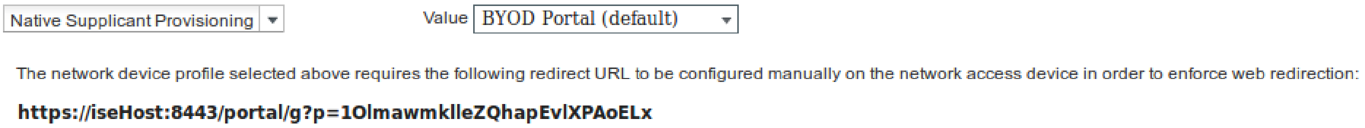
			Results			
Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
✓	Authorized	AND example.com·ExternalGroups EQUALS example.com/Builtin/Administrators EndPoints·BYODRegistration EQUALS Yes Network Access·EapAuthentication EQUALS EAP-TLS	PermitAccess	Select from list	0	⚙
✓	Redirect	Aruba·Aruba-Essid-Name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

Aruba AP

步骤1:强制网络门户配置

要在Aruba 204上配置强制网络门户，请导航到Security > External Captive Portal并添加新的强制网络门户。输入此信息以进行正确的配置，如图所示。

- 类型：Radius身份验证
- IP或主机名：ISE服务器
- URL：在授权配置文件配置下在ISE上创建的链接；它特定于特定的授权配置文件，可以在此处的Web重定向配置下找到

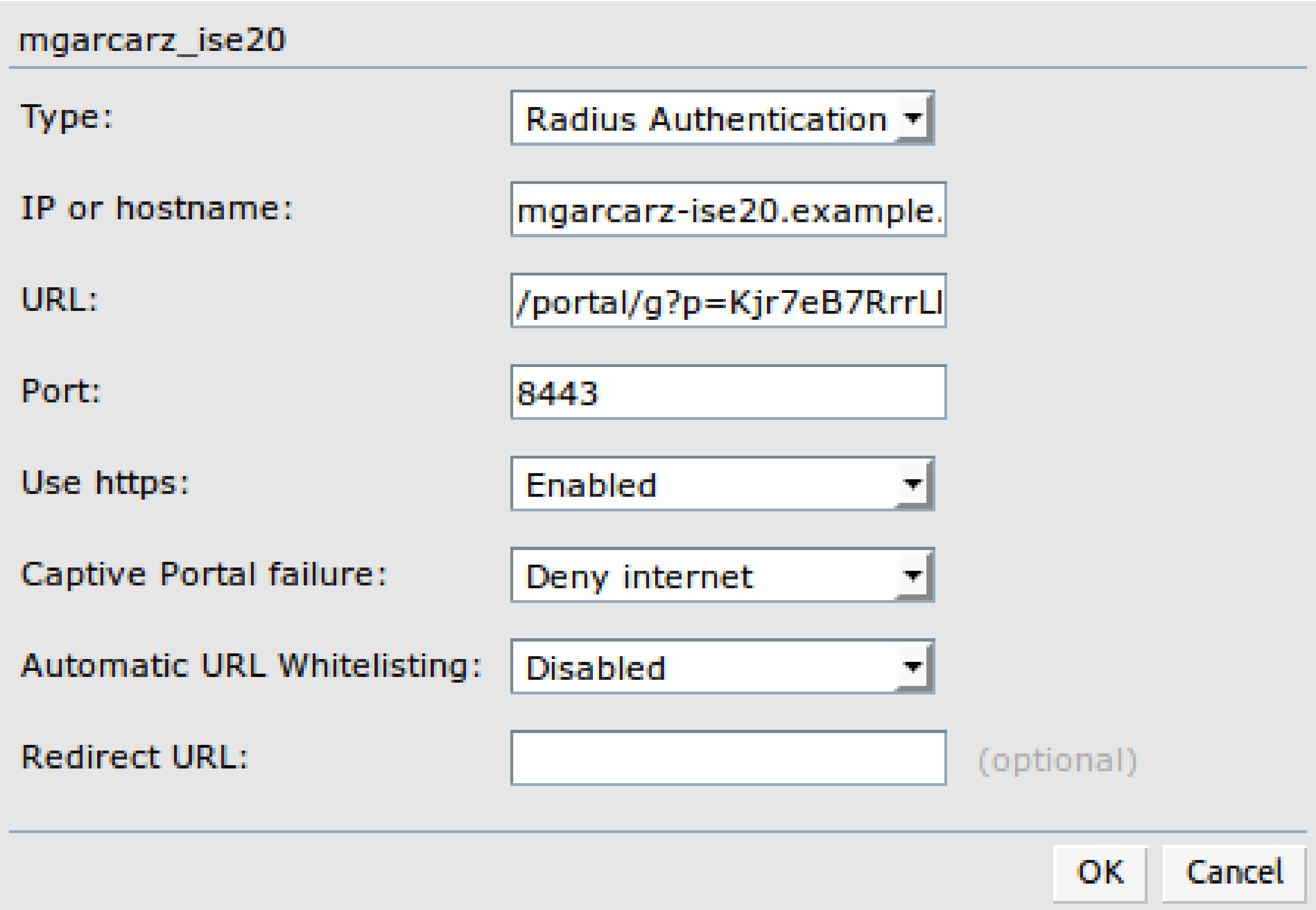


Native Supplicant Provisioning   Value BYOD Portal (default)

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=10lmawmklleZQhapEvlXPAoELx

- 端口：在ISE上托管所选门户的端口号（默认情况下：8443），如图所示。



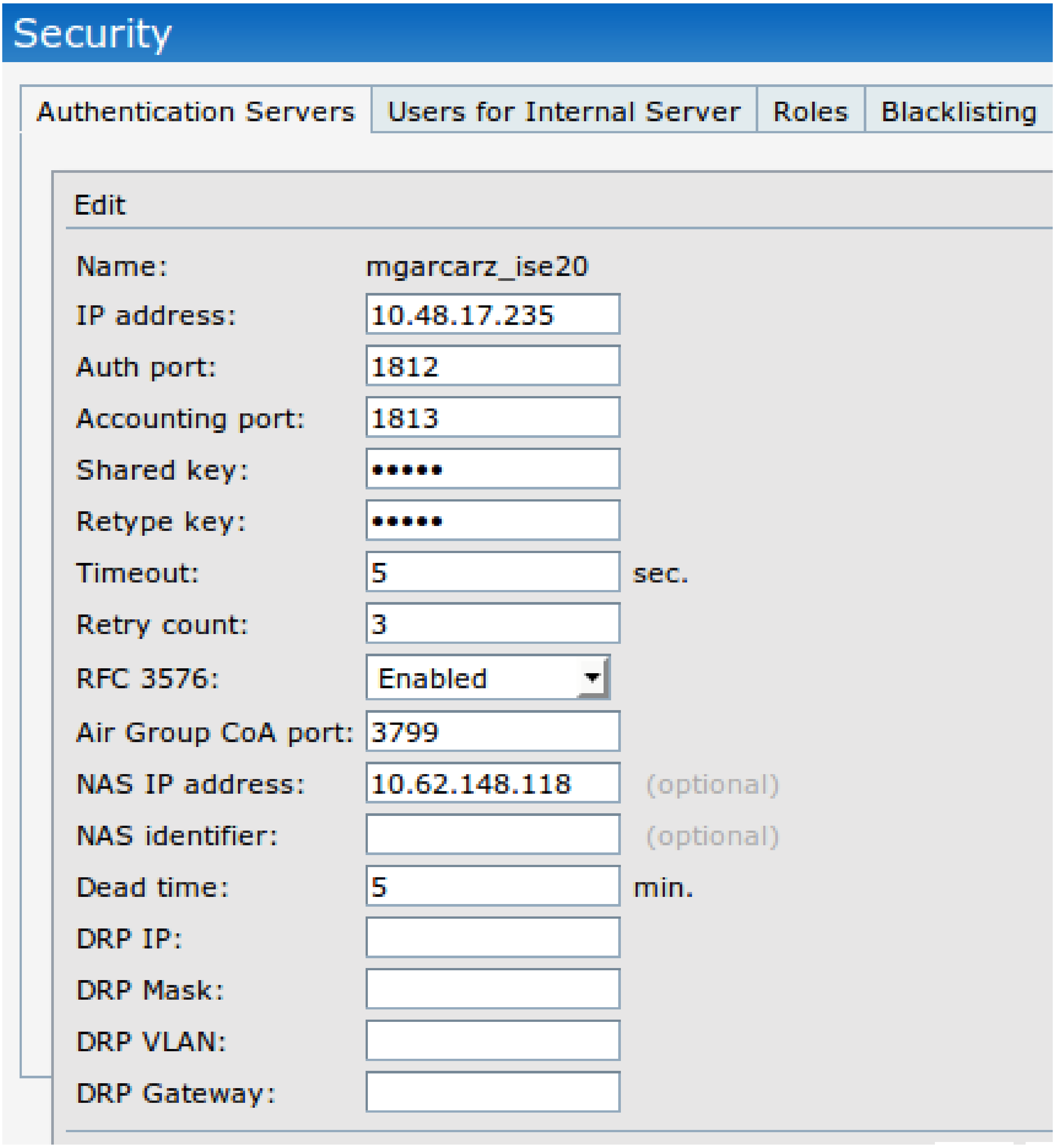
mgarcarz_ise20

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)

第二步：RADIUS 服务器配置

导航到安全>身份验证服务器，确保CoA端口与ISE上配置的端口相同，如图所示。

默认情况下，在Aruba 204上，它设置为5999，但这不符合RFC 5176，也不适用于ISE。



Security

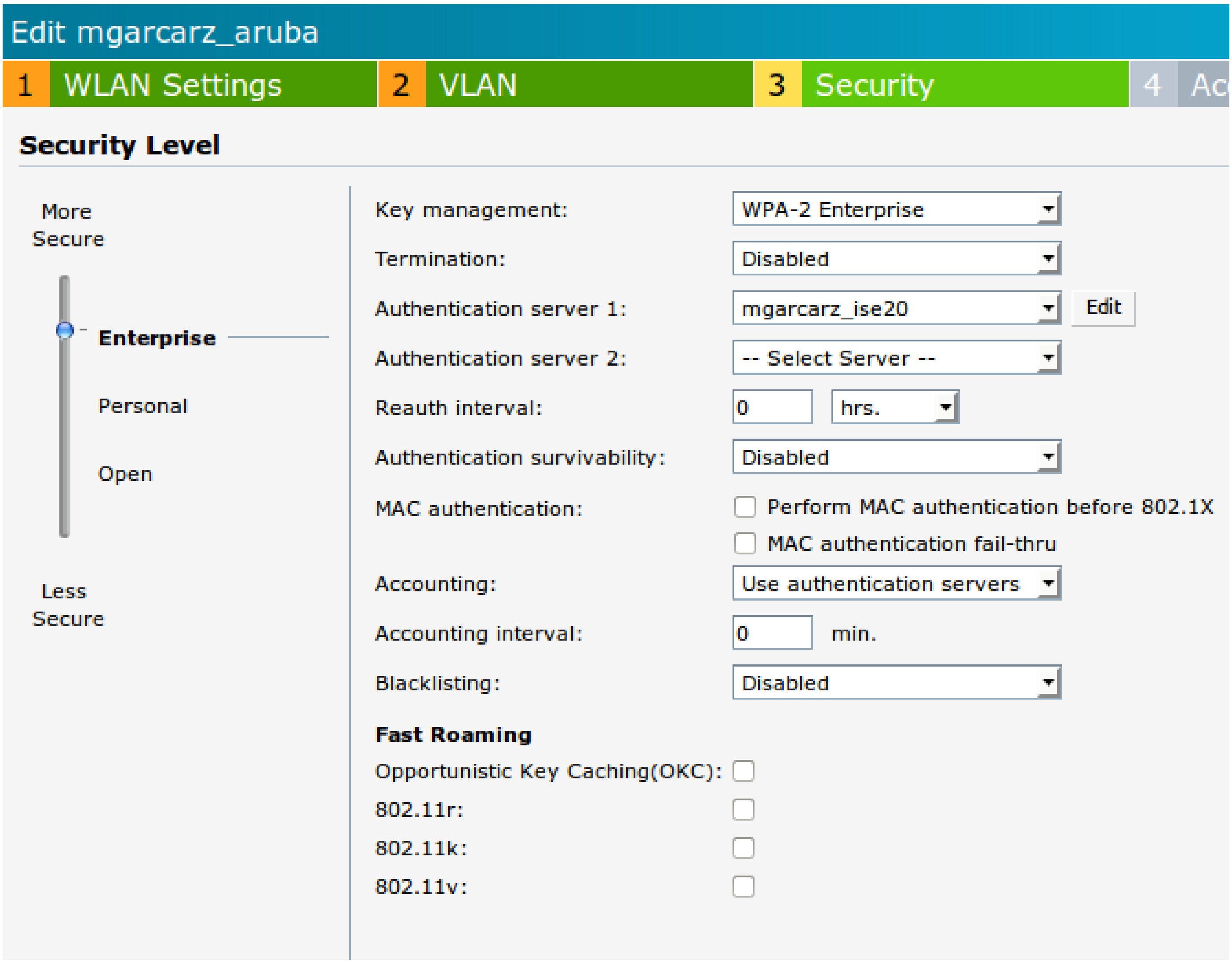
Edit

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:		

注意：在Aruba版本6.5及更高版本中，选中“Captive Portal”复选框。

第三步：SSID 配置

- “安全”选项卡如图所示。



Edit mgarcarz_aruba

1 WLAN Settings | 2 VLAN | 3 Security | 4 Ac

Security Level

Key management: WPA-2 Enterprise

Termination: Disabled

Authentication server 1: mgarcarz_ise20 Edit

Authentication server 2: -- Select Server --

Reauth interval: 0 hrs.

Authentication survivability: Disabled

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

Accounting: Use authentication servers

Accounting interval: 0 min.

Blacklisting: Disabled

Fast Roaming

Opportunistic Key Caching(OKC): ☐

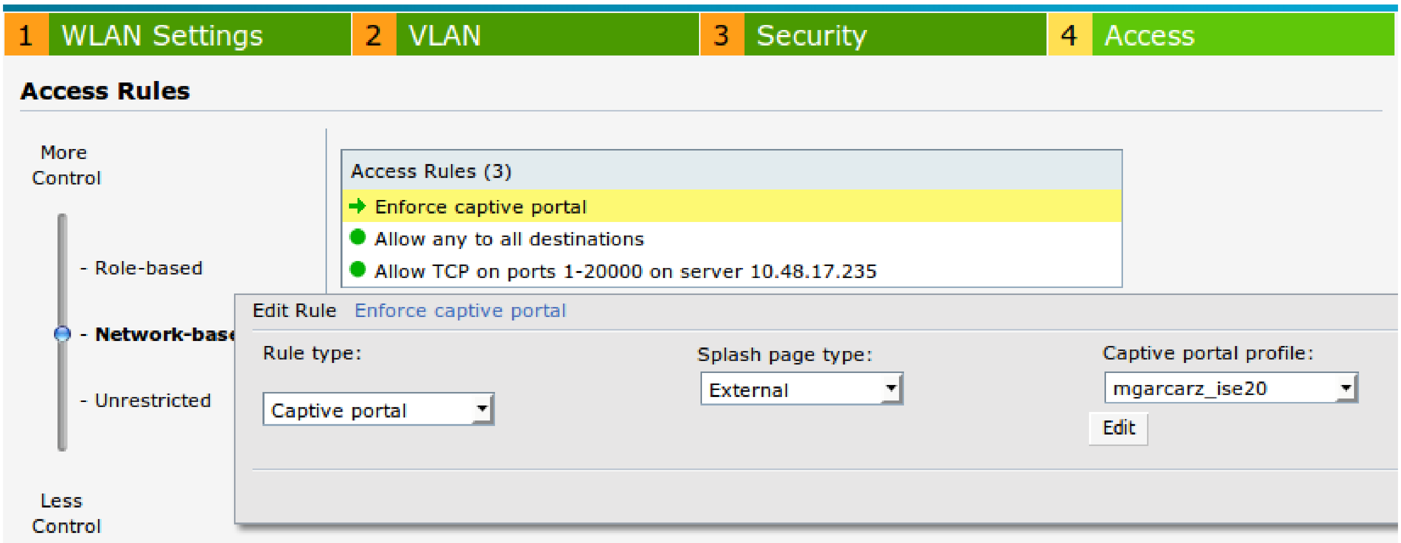
802.11r: ☐

802.11k: ☐

802.11v: ☐

- Access选项卡：选择Network-based Access Rule以在SSID上配置强制网络门户。

使用在步骤1中配置的强制网络门户。点击New，选择Rule type: Captive portal、Splash page type: External，如图所示。



1 WLAN Settings | 2 VLAN | 3 Security | 4 Access

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

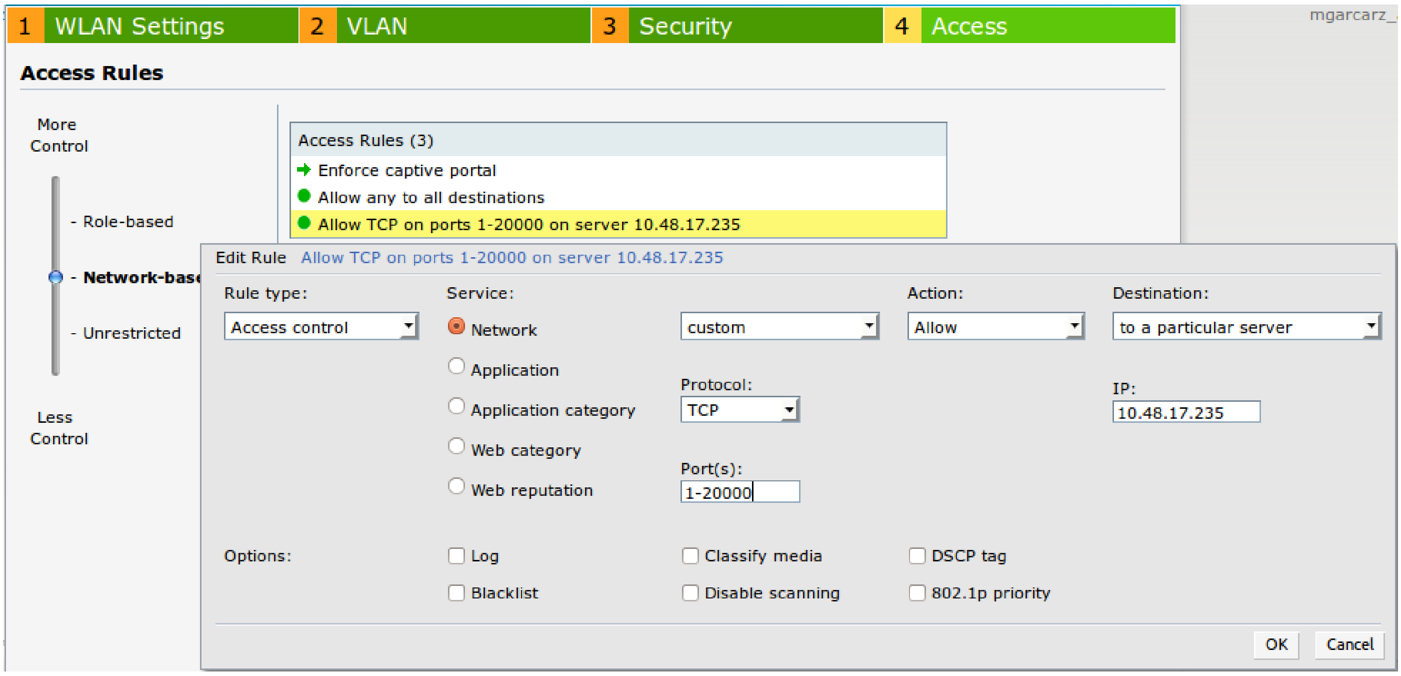
Edit Rule Enforce captive portal

Rule type: Captive portal

Splash page type: External

Captive portal profile: mgarcarz_ise20 Edit

此外，允许所有流量到达ISE服务器(范围为1-20000的TCP端口)，而默认情况下在Aruba上配置规则：Allow any to all destinations似乎无法正常工作，如图所示。



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 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

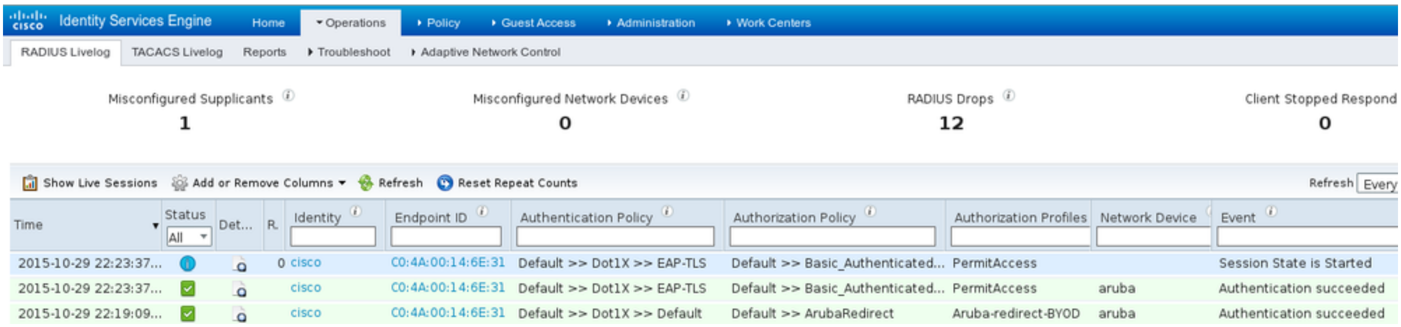
OK Cancel

验证

使用本部分可确认配置能否正常运行。

步骤1:使用EAP-PEAP连接到SSID mgarcarz_aruba

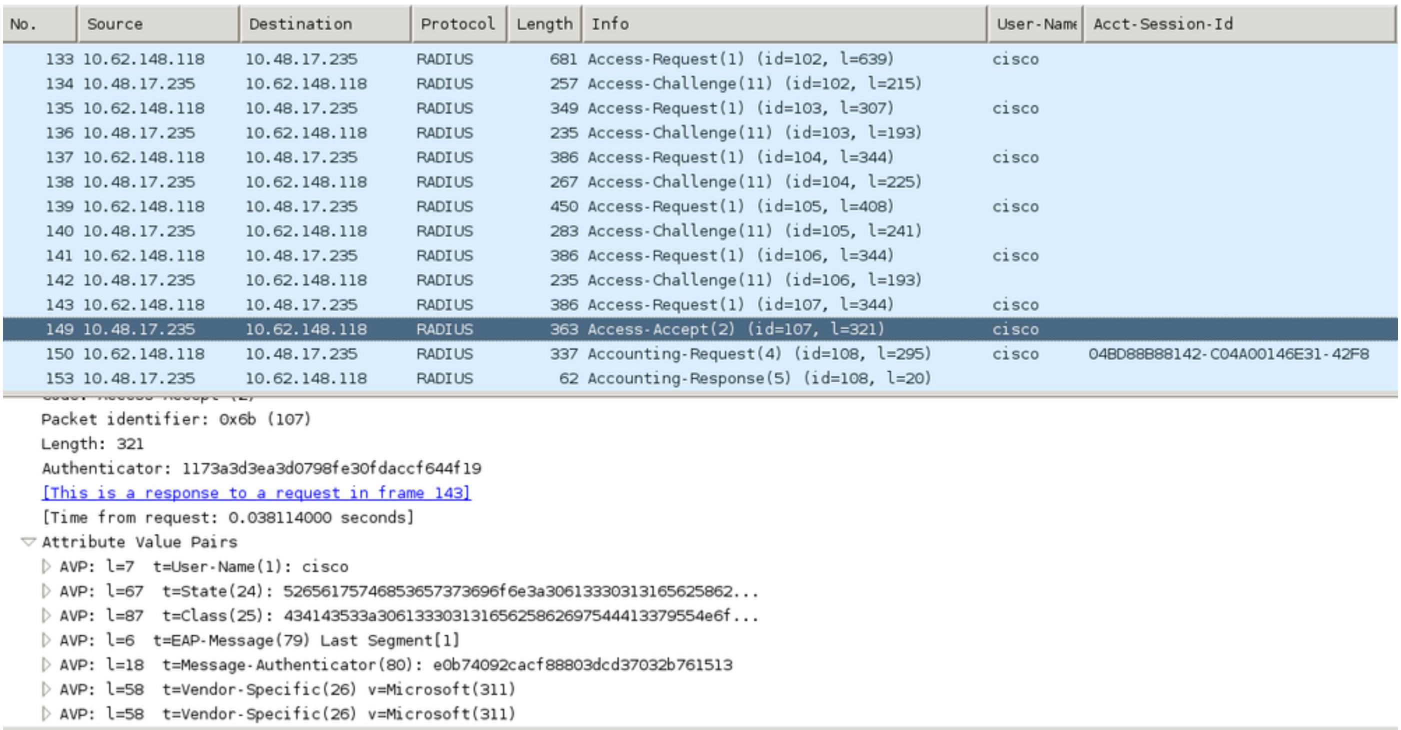
ISE上出现第一个身份验证日志。已使用默认身份验证策略，已返回Aruba-redirect-BYOD授权配置文件，如图所示。



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

Time	Status All	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

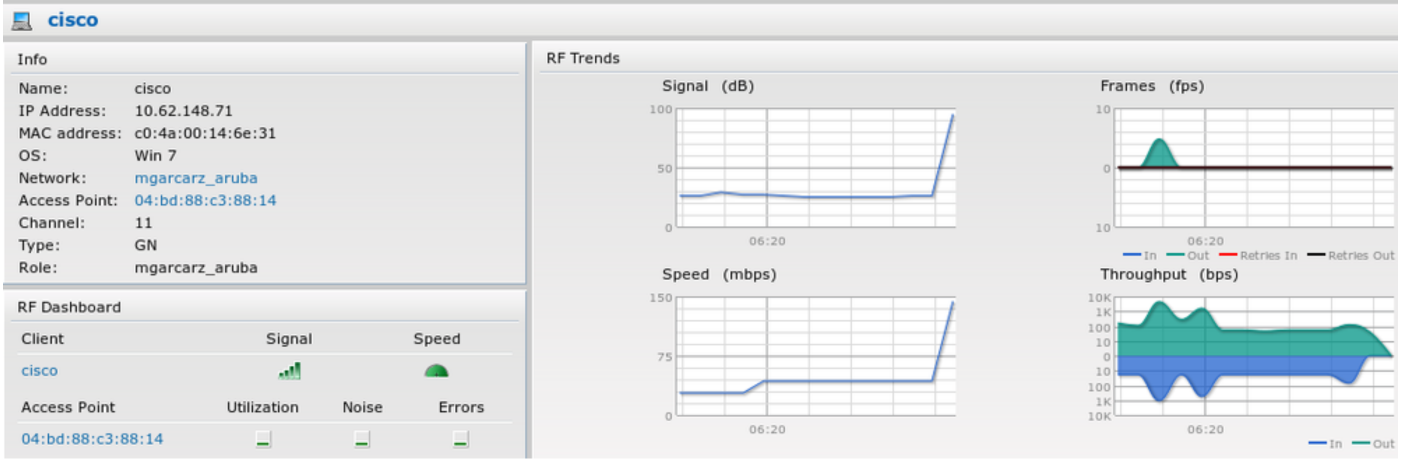
ISE返回Radius Access-Accept消息和EAP成功。 请注意，不会返回其他属性（无思科av-pair url-redirect或url-redirect-acl），如图所示。



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): 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): e0b74092cacf88803dcd37032b761513
  ▷ AVP: l=58  t=Vendor-Specific(26) v=Microsoft(311)
  ▷ AVP: l=58  t=Vendor-Specific(26) v=Microsoft(311)
```

Aruba报告会话已建立(EAP-PEAP身份为cisco)，并且选定的角色为mgarcarz_aruba，如图所示。



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			

该角色负责重定向至ISE（Aruba上的强制网络门户功能）。

在Aruba CLI中，可以确认该会话的当前授权状态：

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

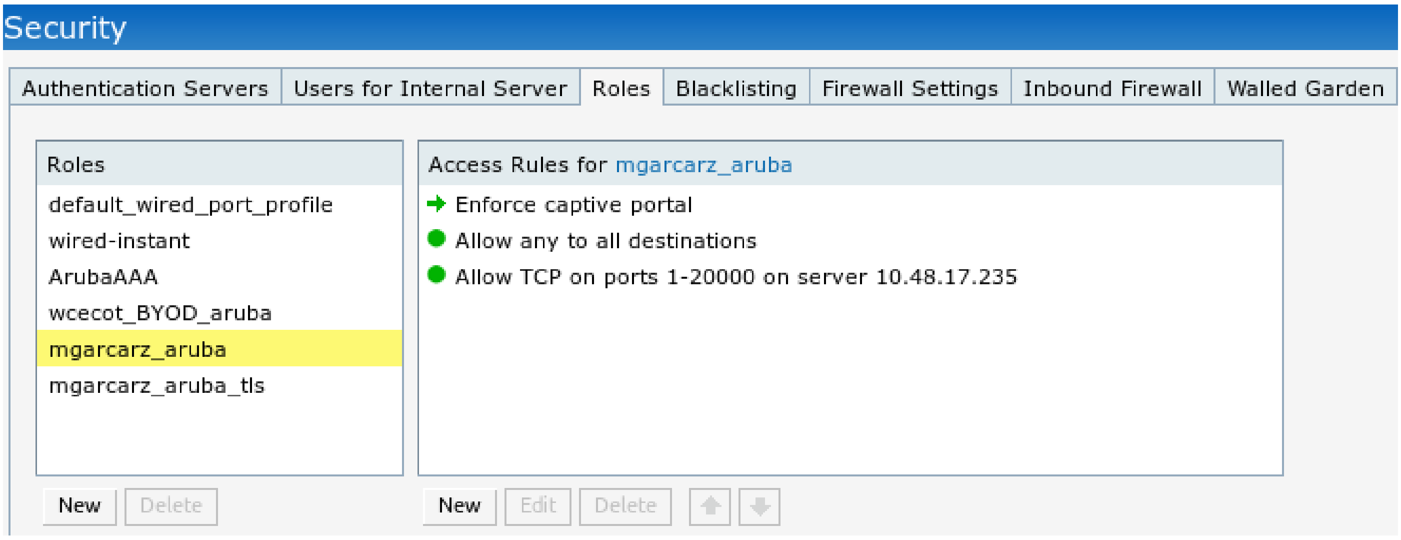
```
10.62.148.118    04:BD:88:C3:88:14   105/0      0/0     0         1        0/65535  P            1   N

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#
```

要检查ACL ID 138的当前权限，请执行以下操作：

<#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 ... >
```

该配置与GUI中为该角色配置的内容匹配，如图所示。



Roles

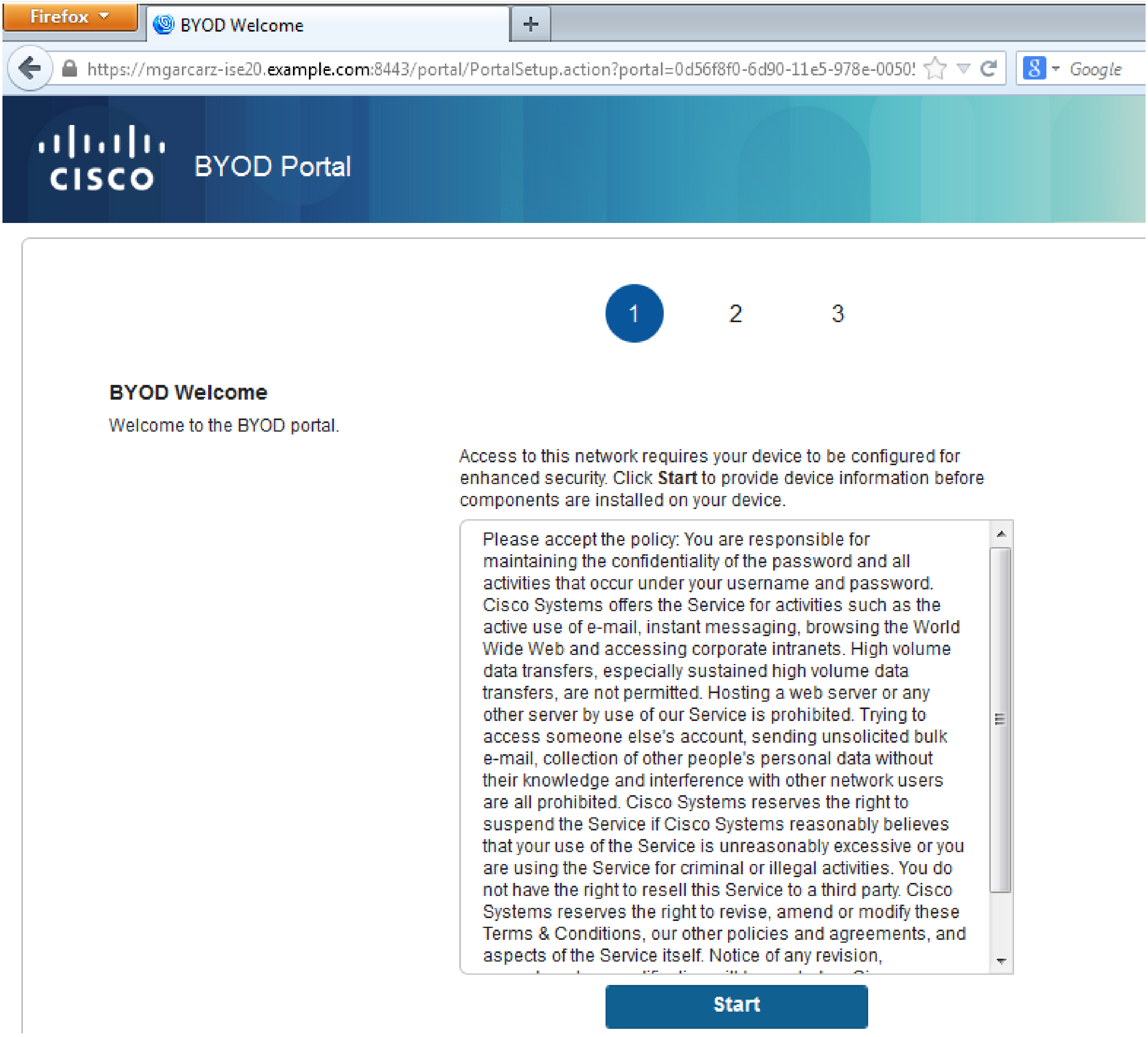
- default_wired_port_profile
- wired-instant
- ArubaAAA
- wcecot_BYOD_aruba
- mgarcarz_aruba
- mgarcarz_aruba_tls

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

第二步：BYOD的Web浏览器流量重定向

用户打开Web浏览器并键入任何地址后，就会发生重定向，如图所示。



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.

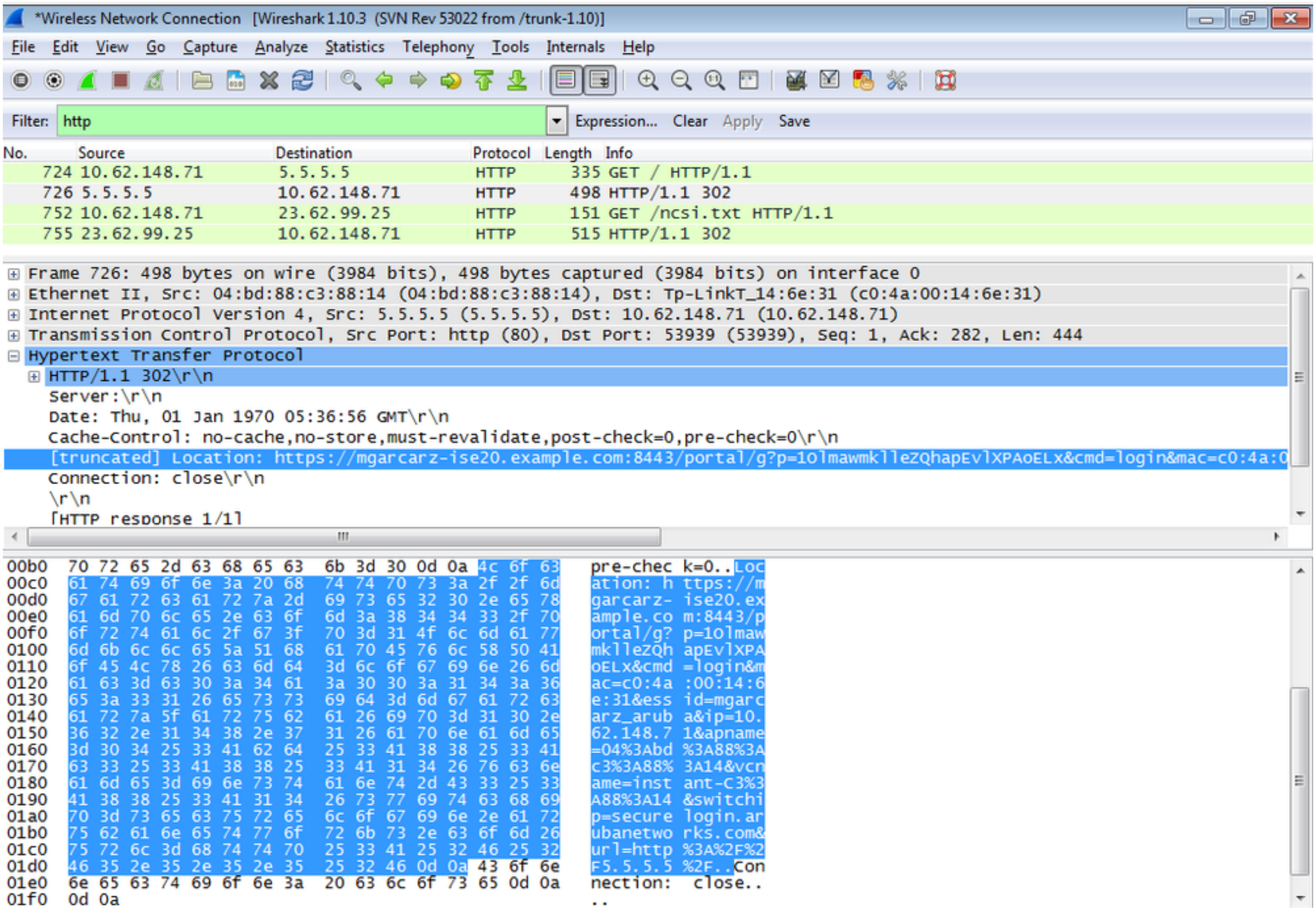
Access to this network requires your device to be configured for enhanced security. Click **Start** to provide device information before components are installed on your device.

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,

查看数据包捕获，确认Aruba欺骗目标(5.5.5.5)并返回HTTP重定向到ISE。

请注意，它与ISE中配置的静态URL相同，并复制到Aruba上的强制网络门户 — 但还会添加多个参数，如下所示，如图所示：

- cmd =登录
- 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:
Expression... Clear Apply Save

Filter: http

```
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                                              ..
```

由于这些参数，ISE能够重新创建思科会话ID，在ISE上查找相应的会话并继续执行BYOD（或任何其他已配置的）流程。

对于思科设备，通常使用audit_session_id，但其他供应商不支持该功能。

为了确认从ISE调试，可以看到生成audit-session-id值（从不通过网络发送）：

<#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
```

然后，在BYOD第2页中注册设备后进行关联：

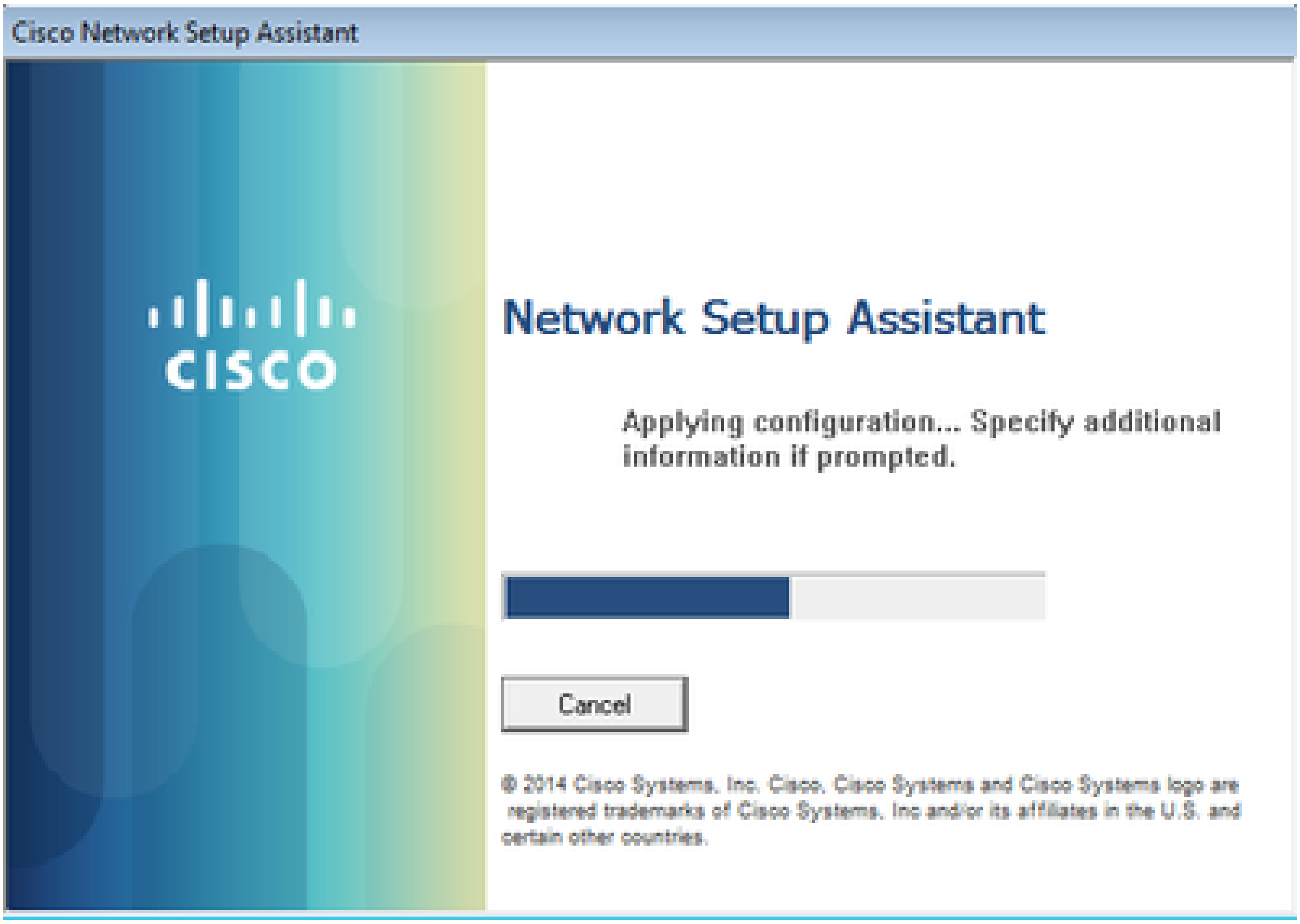
<#root>

```
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
```

在后续请求中，客户端被重定向到BYOD第3页，在该页中下载并执行NSA。

第三步：网络设置助理执行



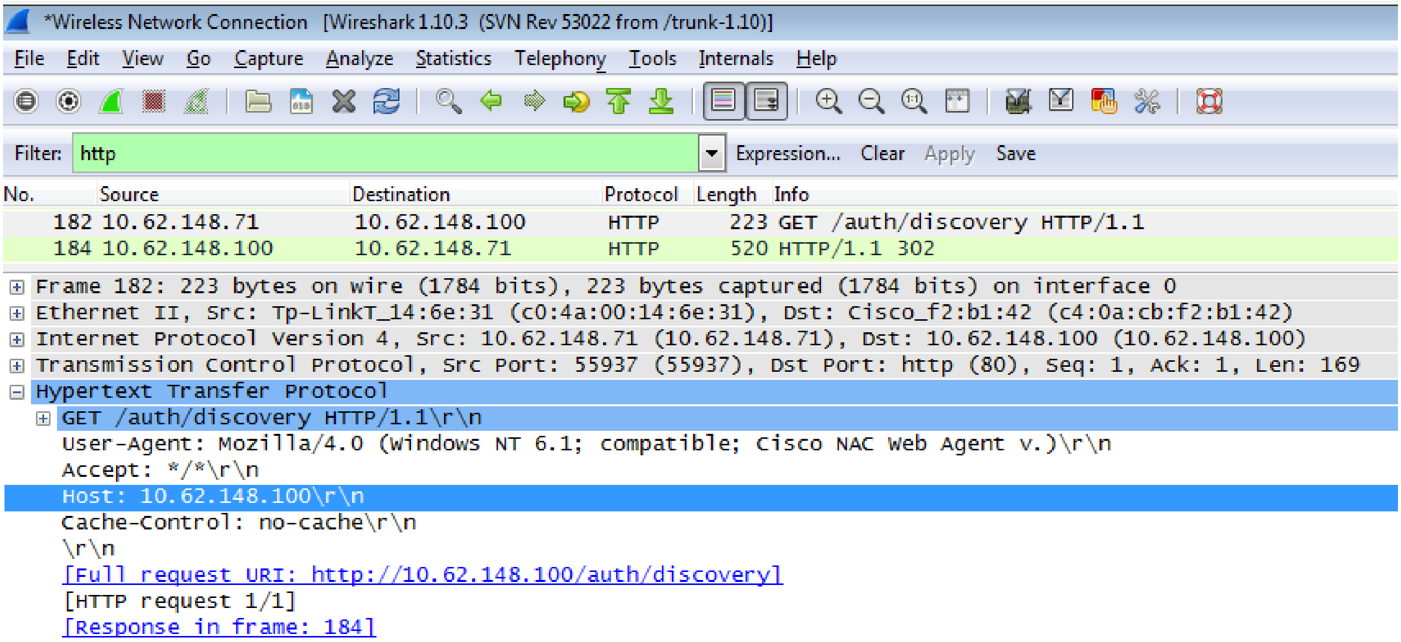
Applying configuration... Specify additional information if prompted.

© 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的任务与Web浏览器相同。首先，它需要检测ISE的IP地址。这是通过HTTP重定向实现的。

由于这次用户无法键入IP地址（如在Web浏览器中），因此该流量会自动生成。

使用默认网关(也可使用enroll.cisco.com)，如图所示。


*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]
```

响应与Web浏览器的响应完全相同。

这样，NSA可以连接到ISE，通过配置获取xml配置文件，生成SCEP请求，将其发送到ISE，获取签名证书（由ISE内部CA签名），配置无线配置文件，最后连接到配置的SSID。

从客户端收集日志(在Windows上%temp%/spwProfile.log中)。为清楚起见，省略了部分输出：

<#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
```

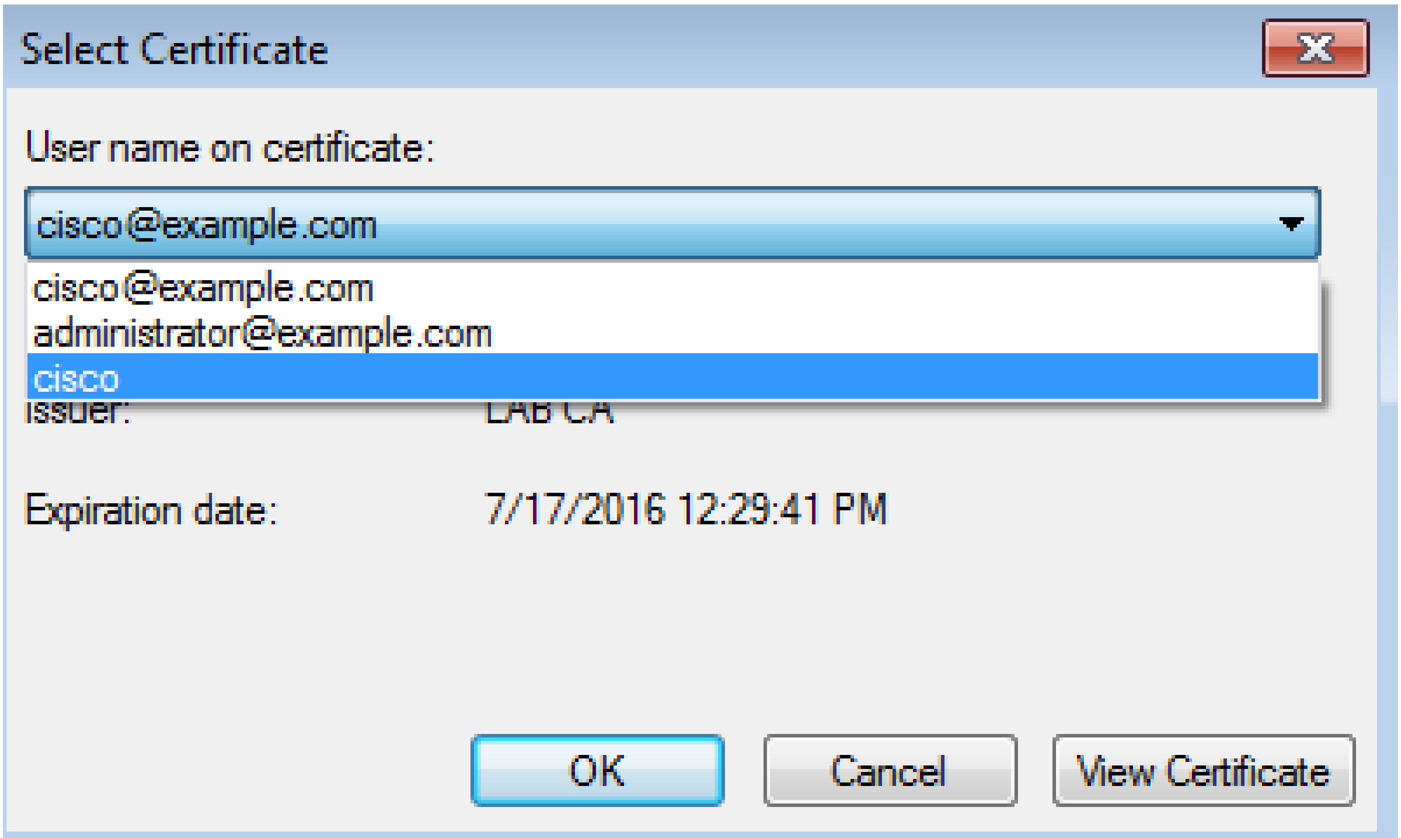
```
DiscoverISE - end

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=S
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
```

这些日志与使用思科设备的BYOD流程完全相同。

注意：此处不需要Radius CoA。它是强制重新连接到新配置的SSID的应用程序(NSA)。

在此阶段，用户可以看到系统尝试与最终SSID关联。如果您有多个用户证书，则必须选择正确的证书（如下所示）。



Select Certificate

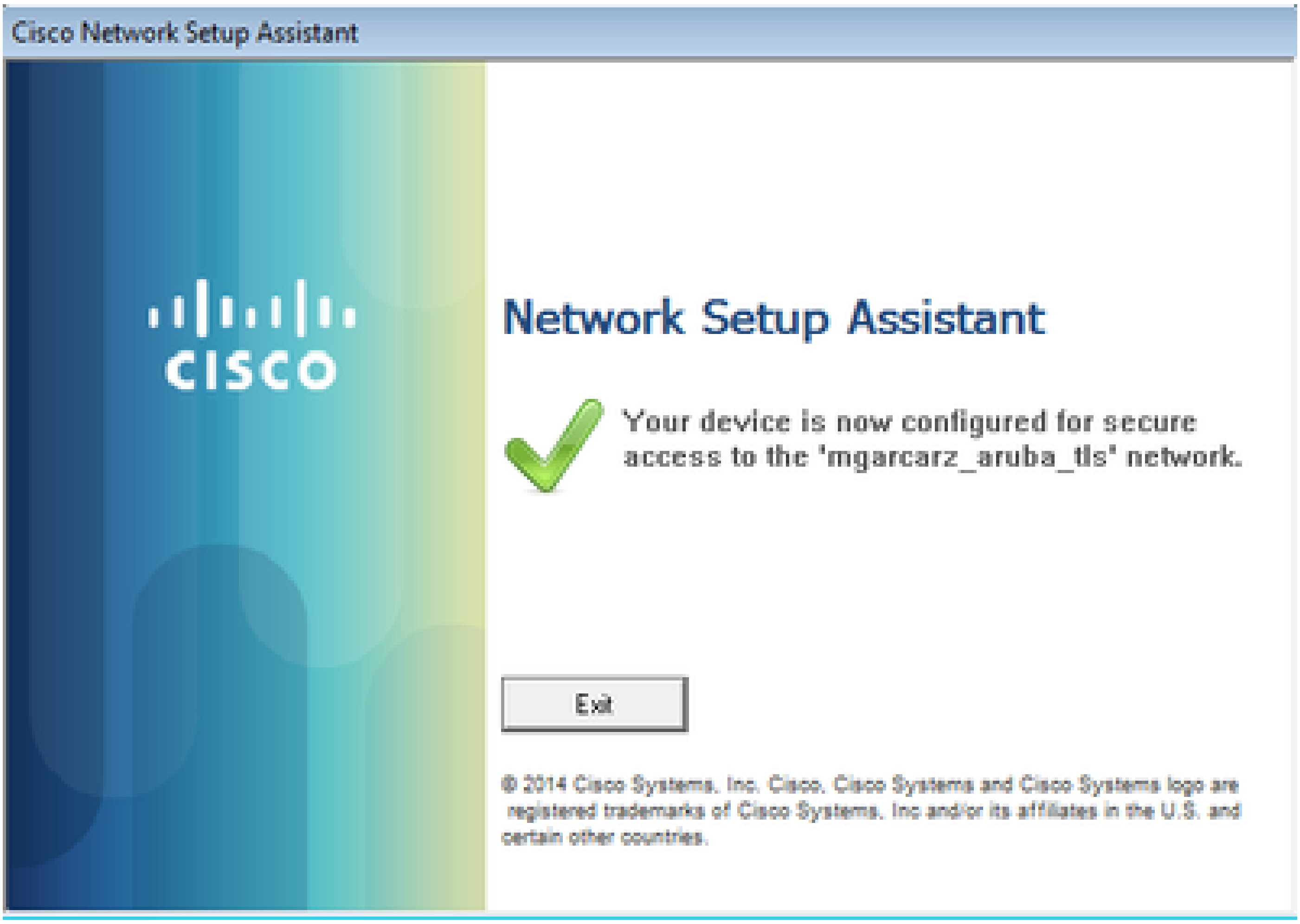
User name on certificate: cisco@example.com

cisco@example.com
administrator@example.com
cisco

Issuer: LAB CA

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

连接成功后，NSA报告如图所示。



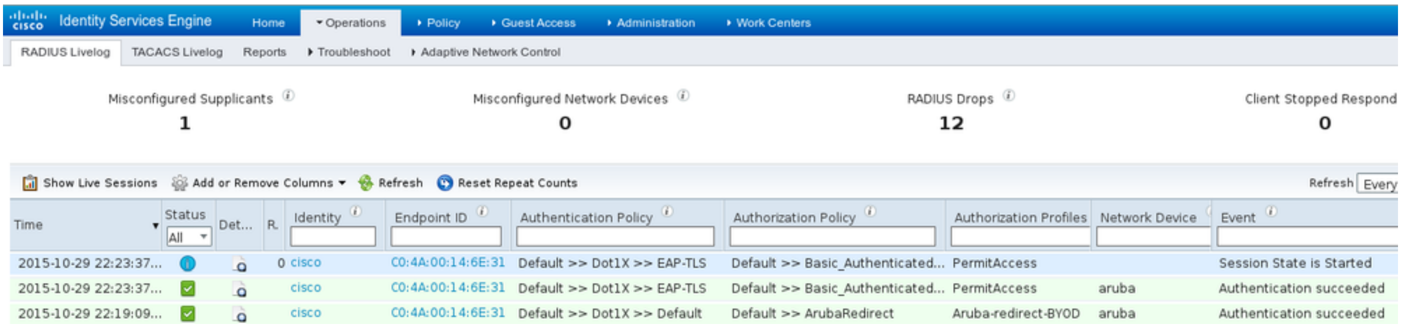
Cisco Network Setup Assistant

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.

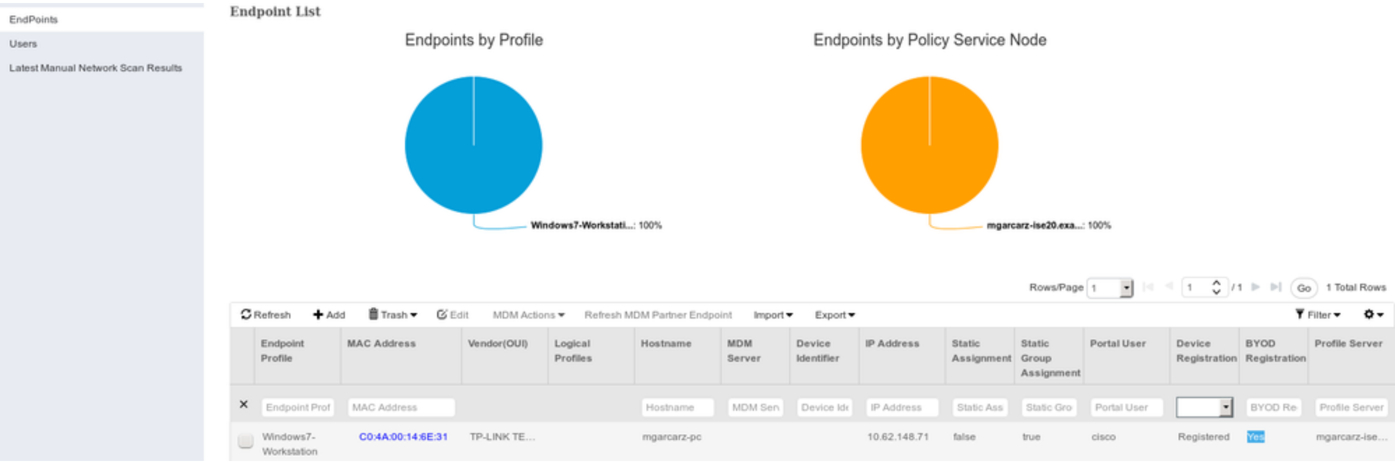
可以在ISE上确认 — 第二个日志命中EAP-TLS身份验证，该身份验证匹配Basic_Authenticated_Access的所有条件（EAP-TLS、Employee和BYOD Registered true）。



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

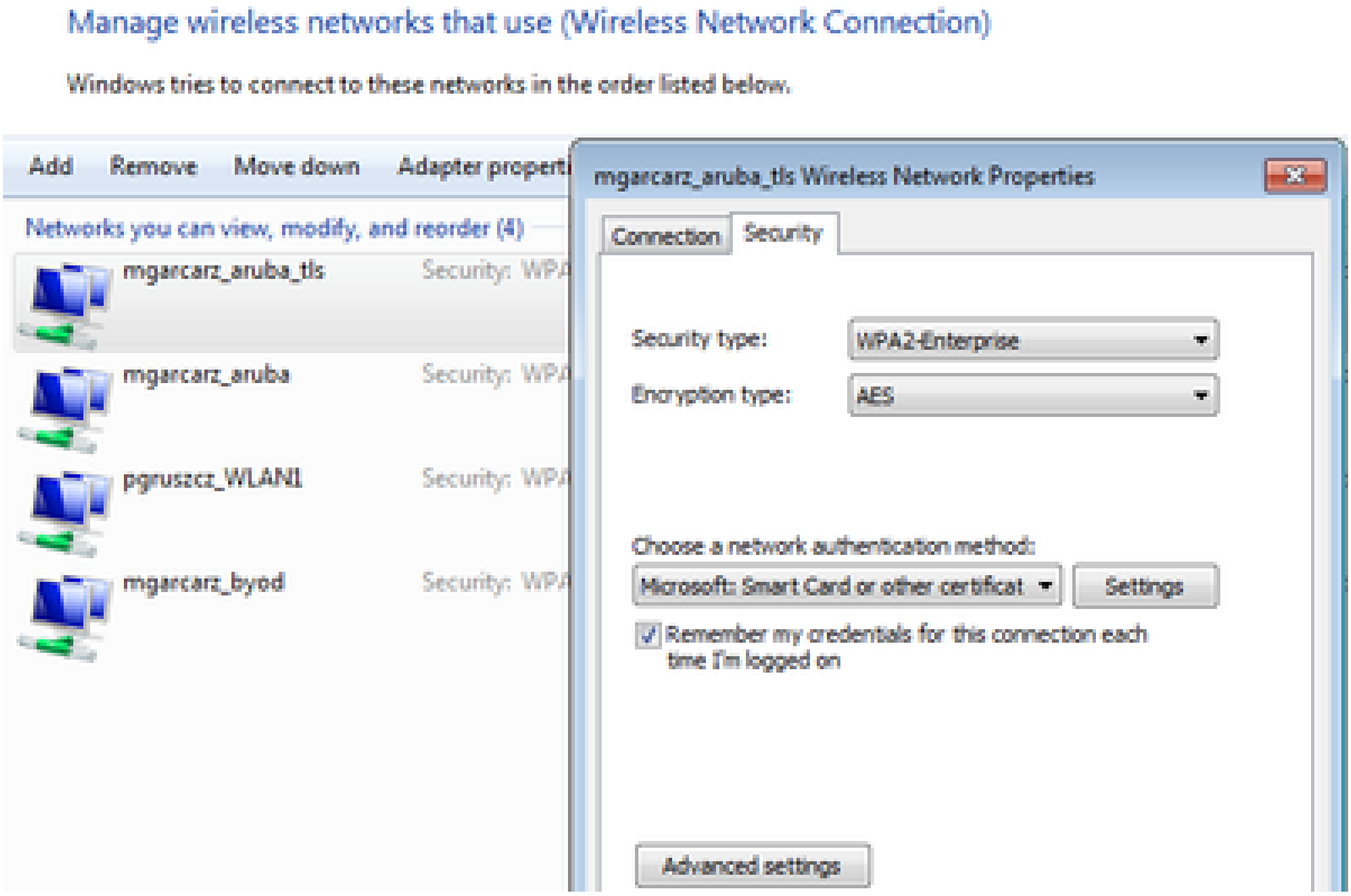
Time	Status All	Det...	R.	Identity	Endpoint ID	Authentication Policy	Authorization Policy	Authorization Profiles	Network Device	Event
2015-10-29 22:23:37...	●		0	cisco	C0:4A:00:14:6E:31	Default >> Dot1X >> EAP-TLS	Default >> Basic_Authenticated...	PermitAccess		Session State is Started
2015-10-29 22:23:37...	☑			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

此外，终端身份视图可以确认终端的BYOD注册标志设置为true，如图所示。


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，新的无线配置文件已自动创建为首选（并配置为EAP-TLS），如下所示。



Manage wireless networks that use (Wireless Network Connection)

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

Networks you can view, modify, and reorder (4)

mgarcarz_aruba_tls Security: WPA

mgarcarz_aruba Security: WPA

pgruszcz_WLAN1 Security: WPA

mgarcarz_byod Security: WPA

mgarcarz_aruba_tls Wireless Network Properties

Security type: WPA2-Enterprise

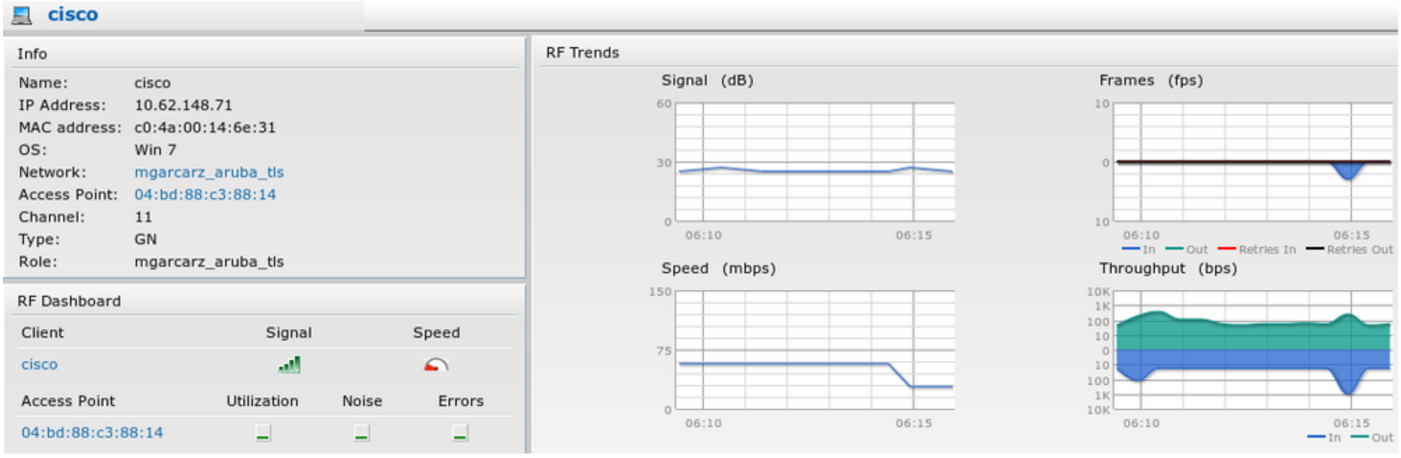
Encryption type: AES

Choose a network authentication method:

Microsoft: Smart Card or other certificat

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

在此阶段，Aruba确认用户已连接到最终SSID。



cisco

Info

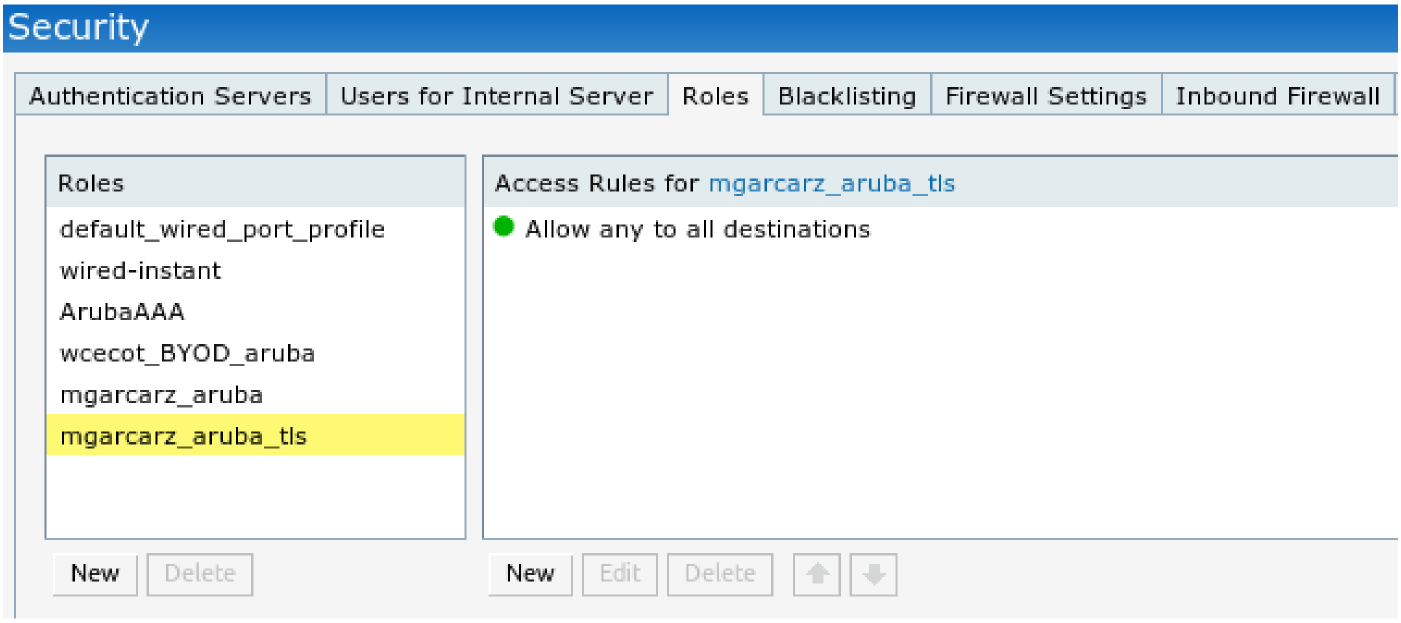
Name:	cisco
IP Address:	10.62.148.71
MAC address:	c0:4a:00:14:6e:31
OS:	Win 7
Network:	mgarcarz_aruba_tls
Access Point:	04:bd:88:c3:88:14
Channel:	11
Type:	GN
Role:	mgarcarz_aruba_tls

RF Dashboard

Client	Signal	Speed
cisco		

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

自动创建并命名为“与网络相同”的角色提供完整的网络访问。



Security

Roles

default_wired_port_profile

wired-instant

ArubaAAA

wcecot_BYOD_aruba

mgarcarz_aruba

mgarcarz_aruba_tls

Access Rules for mgarcarz_aruba_tls

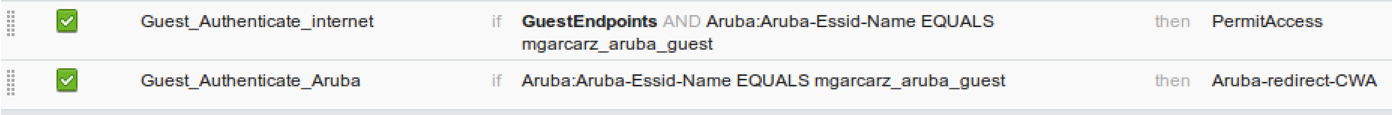
● Allow any to all destinations

其他流和CoA支持

带CoA的CWA

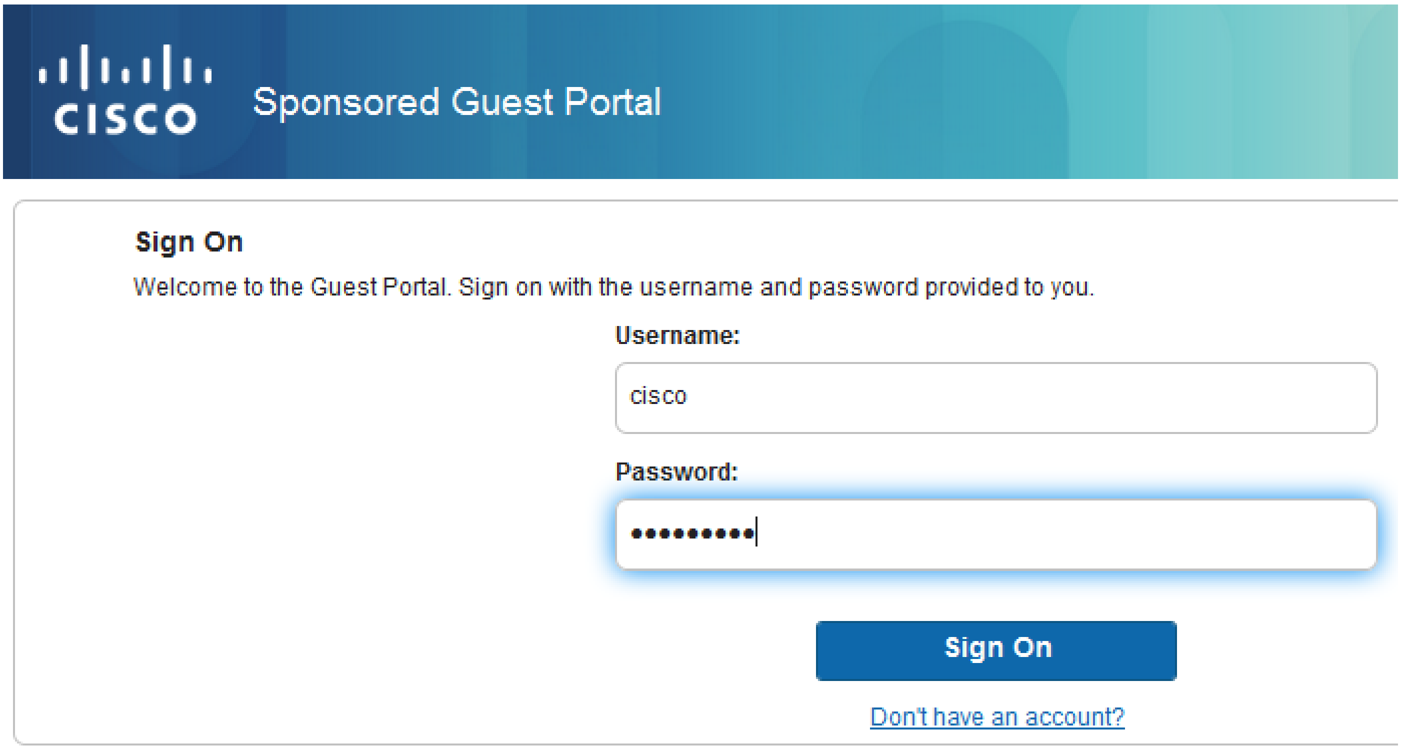
虽然在BYOD流程中没有CoA消息，但具有自助注册访客门户的CWA流程显示如下：

配置的授权规则如图所示。



☑	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

用户通过MAB身份验证连接到SSID，一旦尝试连接到某个网页，就会重定向到自助注册访客门户，访客可以在其中创建新帐户或使用当前帐户。



Sponsored Guest Portal

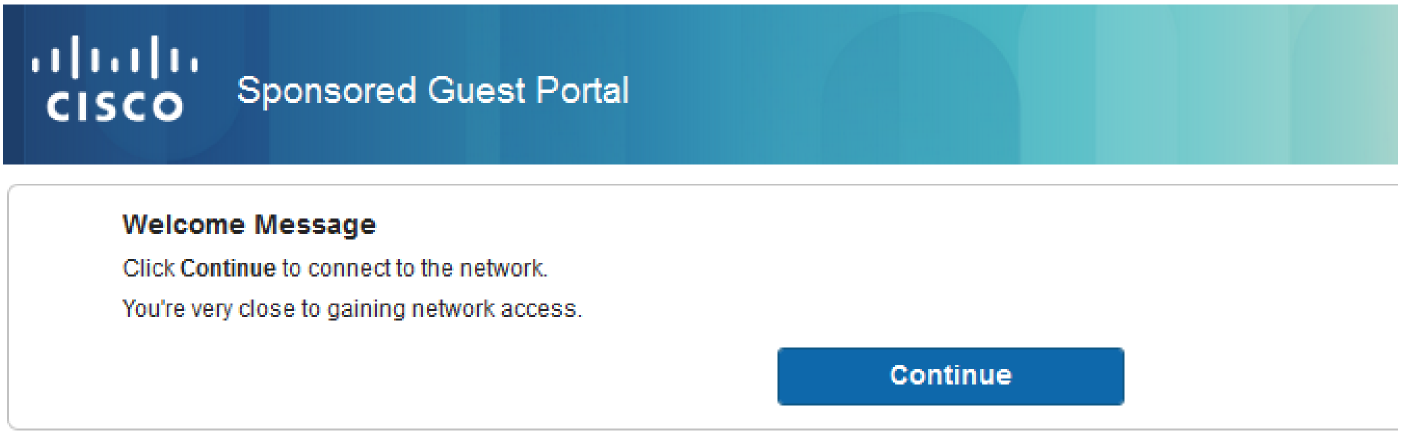
Sign On

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

Username: cisco

Password: ●●●●●●●●●

成功连接访客后，CoA消息将从ISE发送到网络设备，以更改授权状态。



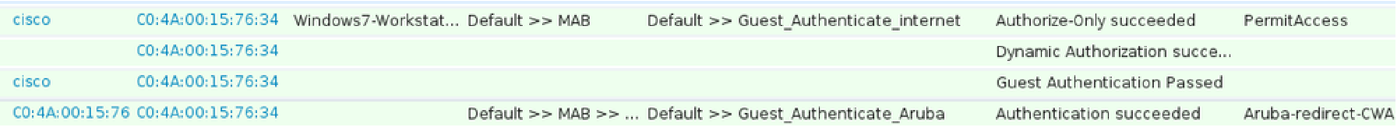
Sponsored Guest Portal

Welcome Message

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

You're very close to gaining network access.

可以在操作>身份验证下验证，如图所示。



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调试中的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

和来自Aruba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,
```

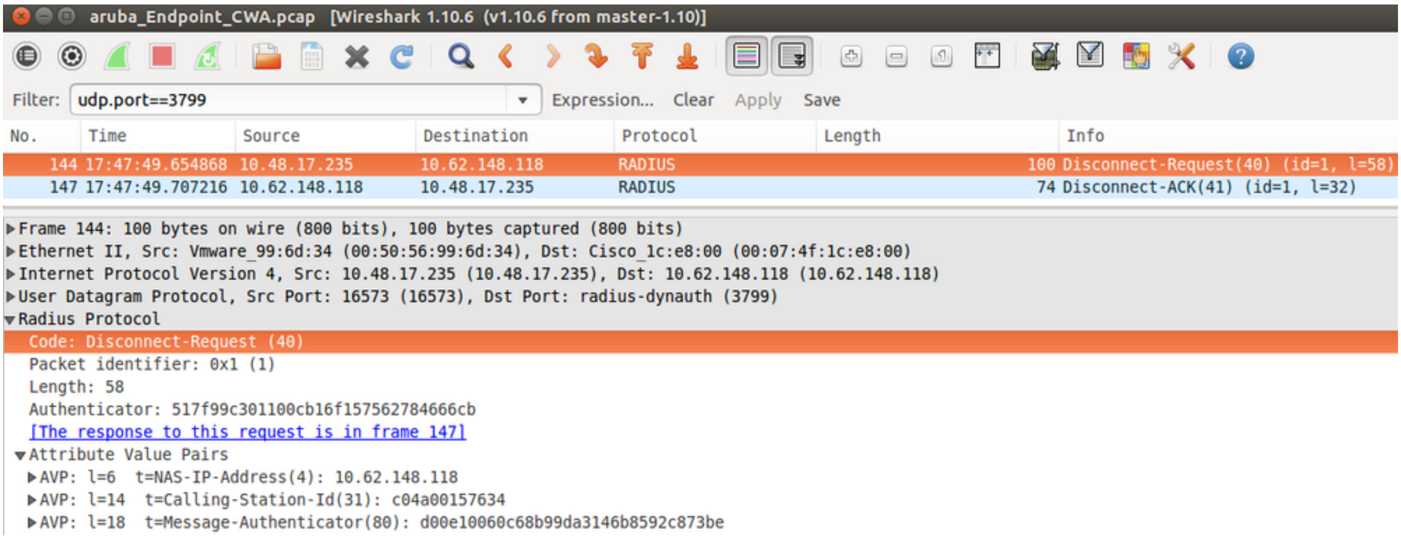
CallingStationID=c04a00157634

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

Packet type 41(DisconnectACK).

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

图中所示为CoA Diconnect-Request(40)和Diconnect-ACK(41)数据包捕获。


aruba_Endpoint_CWA.pcap [Wireshark 1.10.6 (v1.10.6 from master-1.10)]
Filter: udp.port==3799
Expression...
Clear
Apply
Save

```
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已用于与设备配置文件Aruba（默认设置）相关的身份验证。对于与思科设备相关的身份验证，应该是Cisco CoA类型重新进行身份验证。

故障排除

本部分提供了可用于对配置进行故障排除的信息。

Aruba强制网络门户，具有IP地址而不是FQDN

如果Aruba上的强制网络门户配置了IP地址而不是ISE的FQDN，则PSN NSA失败：

<#root>

```
Warning - [HTTPConnection]

Abort the HTTP connection due to invalid certificate


CN
```

原因是在连接到ISE时进行严格的证书验证。当您使用IP地址连接到ISE时（由于重定向URL使用IP地址而非FQDN），并且向ISE证书提供主题名称= FQDN验证失败。

注意:Web浏览器继续访问BYOD门户（带有需要用户批准的警告）。

Aruba强制网络门户访问策略不正确

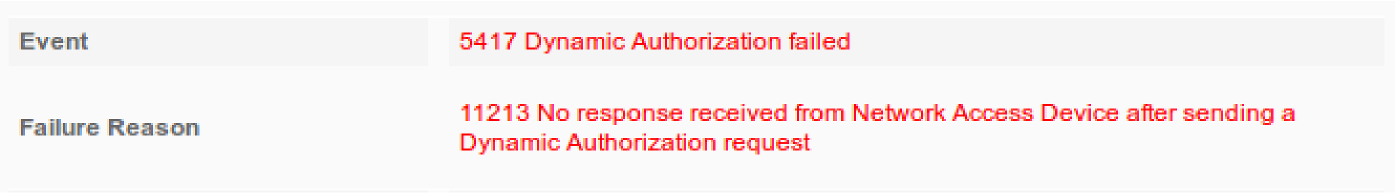
默认情况下，使用强制网络门户配置的Aruba访问策略允许tcp端口80、443和8080。

NSA无法连接到tcp端口8905以从ISE获取xml配置文件。报告此错误：

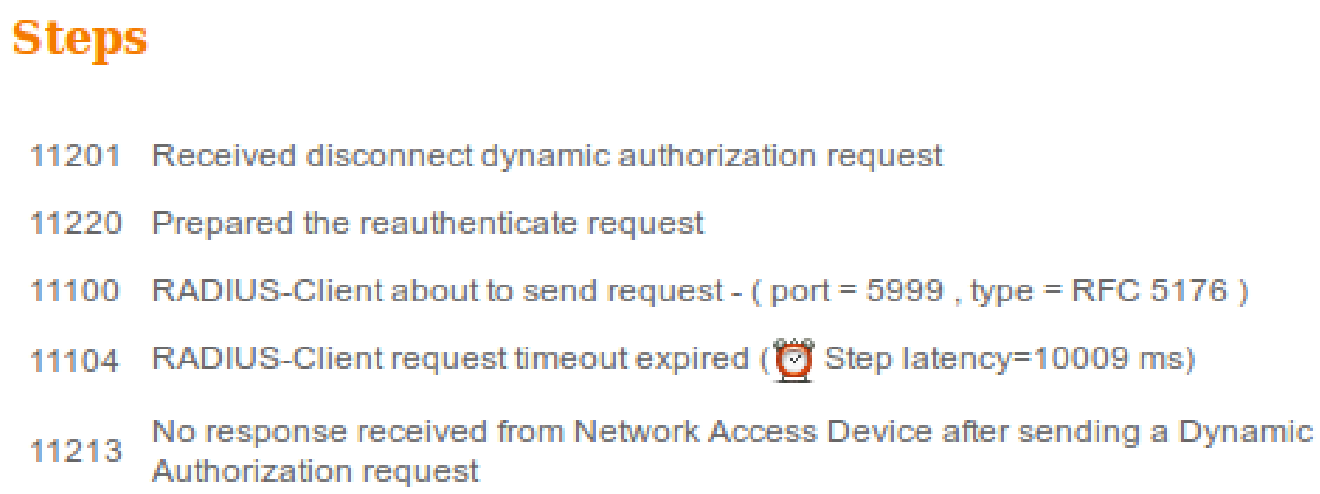
```
<#root>
Failed to get spw profile url using - url

[
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
```

Aruba CoA端口号

默认情况下，Aruba为CoA Air Group CoA端口5999提供端口号。遗憾的是，Aruba 204没有响应此类请求（如图所示）。



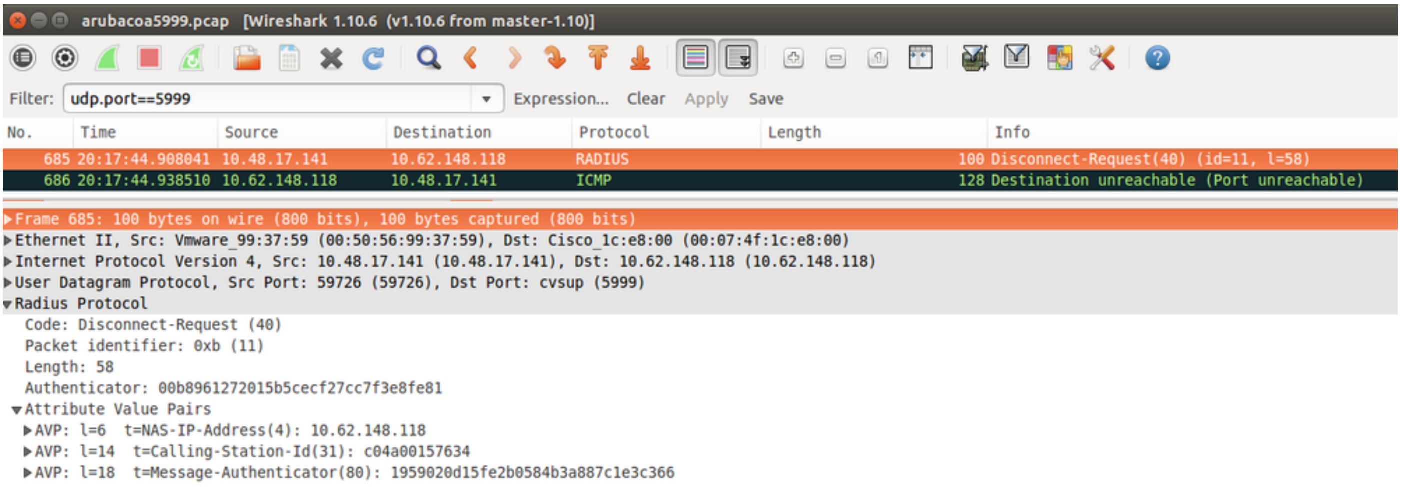
Event	5417 Dynamic Authorization failed
Failure Reason	11213 No response received from Network Access Device after sending a Dynamic Authorization request



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

数据包捕获如图所示。



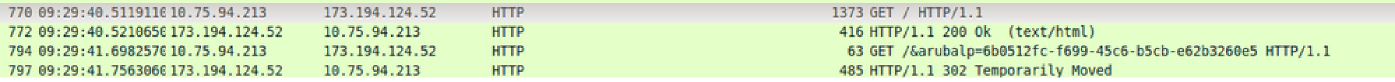
arubacoa5999.pcap [Wireshark 1.10.6 (v1.10.6 from master-1.10)]
Filter: udp.port==5999
Expression...
Clear
Apply
Save

```
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
```

此处使用的最佳选项可以是CoA端口3977，如RFC 5176中所述。

某些Aruba设备上的重定向

在使用v6.3的Aruba 3600上，我们注意到重定向的工作方式与其他控制器略有不同。数据包捕获和解释可以在此处找到。



```
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

相关信息

- 思科身份服务引擎管理员指南，版本2.0
- 使用思科身份服务引擎的网络访问设备配置文件
- 技术支持和文档 - Cisco Systems

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。