

# Aruba Wireless와 ISE 2.0 서드파티 통합 구성

## 목차

---

### [소개](#)

#### [사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

#### [구성](#)

[네트워크 다이어그램](#)

[타사 지원 관련 문제](#)

[세션](#)

[URL 리디렉션](#)

[CoA](#)

[ISE의 솔루션](#)

[Cisco ISE](#)

[1단계. 네트워크 디바이스에 Aruba Wireless Controller 추가](#)

[2단계. 권한 부여 프로파일 구성](#)

[3단계. 권한 부여 규칙 구성](#)

[아루바 AP](#)

[1단계. 중속 포털 컨피그레이션](#)

[2단계. Radius 서버 컨피그레이션](#)

[3단계. SSID 컨피그레이션](#)

[다음을 확인합니다.](#)

[1단계. EAP-PEAP를 사용하여 SSID mgarcarz\\_aruba에 연결](#)

[2단계. BYOD를 위한 웹 브라우저 트래픽 리디렉션](#)

[3단계. 네트워크 설정 도우미 실행](#)

[기타 플로우 및 CoA 지원](#)

[CoA가 포함된 CWA](#)

[문제 해결](#)

[FQDN 대신 IPAddress를 사용하는 Aruba 중속 포털](#)

[Aruba 중속 포털의 잘못된 액세스 정책](#)

[Aruba CoA 포트 번호](#)

[일부 Aruba 디바이스에서 리디렉션](#)

[관련 정보](#)

---

## 소개

이 문서에서는 Cisco ISE(Identity Services Engine)에서 서드파티 통합 기능을 트러블슈팅하는 방법에 대해 설명합니다.



참고: Cisco는 다른 벤더의 장치를 구성하거나 지원할 책임이 없습니다.

---

# 사전 요구 사항

## 요구 사항

다음 주제에 대한 지식을 보유하고 있으면 유용합니다.

- Aruba IAP 컨피그레이션
- BYOD는 ISE에서 흐름
- 비밀번호 및 인증서 인증을 위한 ISE 컨피그레이션

## 사용되는 구성 요소

이 문서에서는 Cisco ISE(Identity Services Engine)에서 서드파티 통합 기능을 트러블슈팅하는 방법에 대해 설명합니다.

다른 공급업체 및 흐름과의 통합을 위한 지침으로 사용할 수 있습니다. ISE 버전 2.0은 서드파티 통합을 지원합니다.

Aruba IAP 204에서 관리하는 무선 네트워크를 BYOD(Bring Your Own Device) 서비스를 위해 ISE와 통합하는 방법을 보여주는 구성 예입니다.

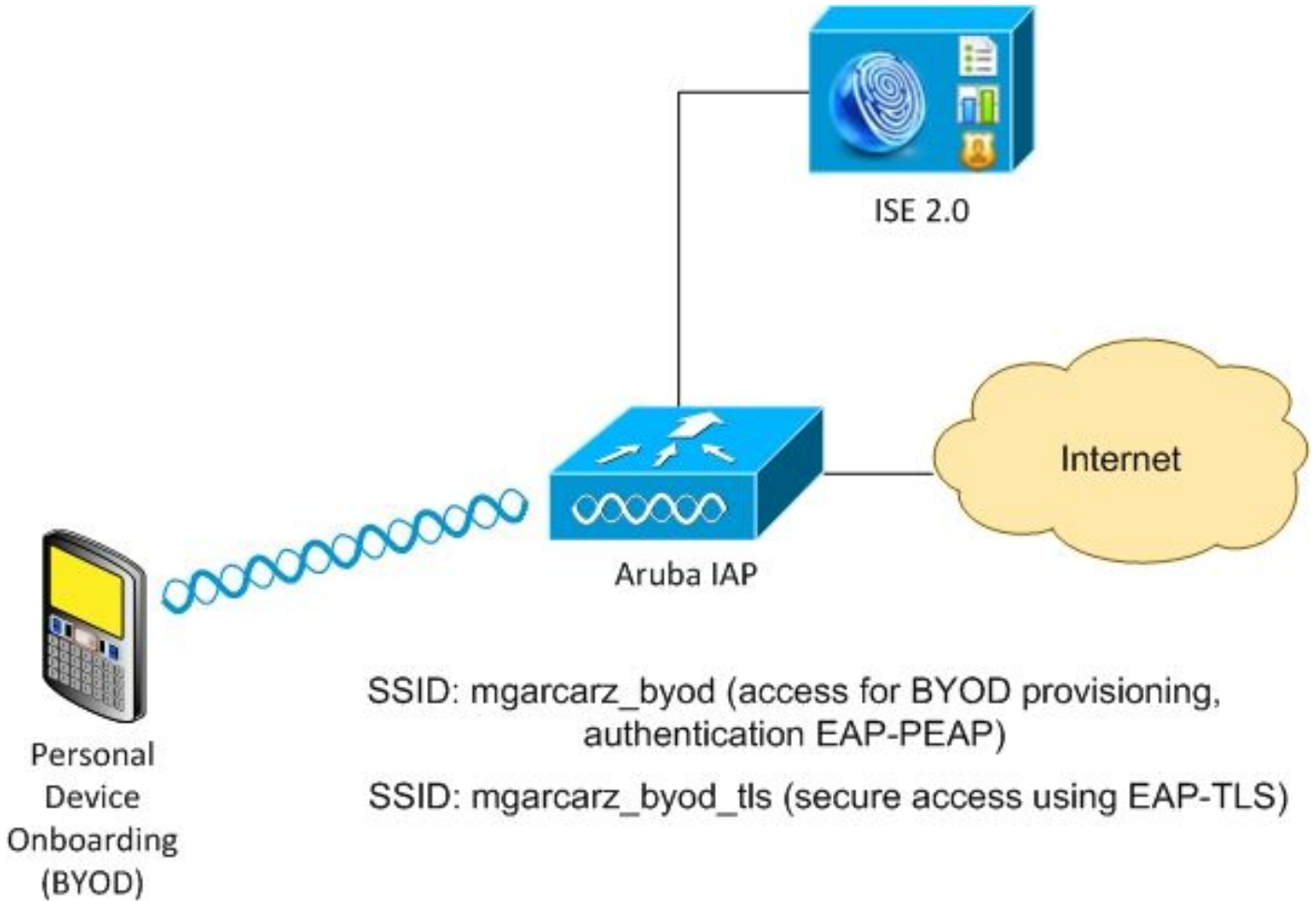
이 문서의 정보는 다음 소프트웨어 버전을 기반으로 합니다.

- Aruba IAP 204 소프트웨어 6.4.2.3
- Cisco ISE, 릴리스 2.0 이상

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

## 구성

### 네트워크 다이어그램



Aruba AP에서 관리하는 무선 네트워크는 2개입니다.

첫 번째 항목(mgarcarz\_byod)은 802.1x EAP-PEAP(Extensible Authentication Protocol-Protected EAP) 액세스에 사용됩니다.

인증에 성공한 후 Aruba 컨트롤러는 사용자를 ISE BYOD 포털 - NSP(Native Supplicant Provisioning) 플로우로 리디렉션해야 합니다.

사용자가 리디렉션되고 NSA(Network Setup Assistant) 애플리케이션이 실행되며 인증서가 프로비저닝되어 Windows 클라이언트에 설치됩니다.

ISE 내부 CA가 해당 프로세스(기본 컨피그레이션)에 사용됩니다.

또한 NSA는 Aruba(mgarcarz\_byod\_tls)가 관리하는 두 번째 SSID(Service Set Identifier)에 대한 무선 프로파일 생성을 담당합니다. 이 SSID는 802.1x EAP-TLS(Extensible Authentication Protocol-Transport Layer Security) 인증에 사용됩니다.

그 결과, 기업 사용자는 개인 장치의 온보딩을 수행할 수 있고 기업 네트워크에 안전하게 액세스할 수 있습니다.

이 예는 다양한 액세스 유형에 대해 쉽게 수정할 수 있습니다. 예를 들면 다음과 같습니다.

- BYOD 서비스를 통한 CWA(Central Web Authentication)
- 포스터 및 BYOD 리디렉션을 통한 802.1x 인증
- 일반적으로 EAP-PEAP 인증을 위해 Active Directory가 사용됩니다(이 문서를 짧게 유지하려

면 내부 ISE 사용자가 사용됨).

- 일반적으로 SCEP(Certificate Provisioning external Simple Certificate Enrollment Protocol) 서버가 사용됩니다. 일반적으로 이 문서를 짧게 유지하기 위해 Microsoft NDES(Network Device Enrollment Service)가 사용됩니다. 내부 ISE CA가 사용됩니다.

## 타사 지원 관련 문제

ISE 게스트 플로우(예: BYOD, CWA, NSP, CPP(Client Provisioning Portal))를 서드파티 디바이스와 함께 사용할 경우 문제가 발생합니다.

## 세션

Cisco NAD(Network Access Device)는 세션 ID에 대해 AAA(Authentication, Authorization, and Accounting) 서버에 알리기 위해 audit-session-id라는 Radius cisco av 쌍을 사용합니다.

이 값은 ISE에서 세션을 추적하고 각 흐름에 대해 올바른 서비스를 제공하기 위해 사용됩니다. 다른 벤더는 cisco-av 쌍을 지원하지 않습니다.

ISE는 Access-Request 및 Accounting Request에서 받은 IETF 특성에 의존해야 합니다.

액세스 요청을 받은 후 ISE는 Cisco 세션 ID(Calling-Station-ID, NAS-Port, NAS-IP-Address 및 공유 암호)를 합성하여 생성합니다. 이 값은 로컬에서만 의미가 있습니다(네트워크를 통해 전송되지 않음).

따라서 모든 플로우(BYOD, CWA, NSP, CPP)에서 올바른 특성을 연결해야 합니다. 따라서 ISE는 Cisco 세션 ID를 다시 계산하고 조회를 수행하여 올바른 세션과 상관 관계를 분석하고 플로우를 계속할 수 있습니다.

## URL 리디렉션

ISE는 NAD에 특정 트래픽이 리디렉션되어야 함을 알리기 위해 url-redirect 및 url-redirect-acl이라는 Radius cisco-av 쌍을 사용합니다.

다른 벤더는 cisco-av 쌍을 지원하지 않습니다. 따라서 일반적으로 이러한 디바이스는 ISE의 특정 서비스(권한 부여 프로파일)를 가리키는 고정 리디렉션 URL로 구성해야 합니다.

사용자가 HTTP 세션을 시작하면 NAD는 URL로 리디렉션되고 추가 인수(예: IP 주소 또는 MAC 주소)를 추가하여 ISE가 특정 세션을 식별하고 흐름을 계속할 수 있도록 합니다.

## CoA

ISE는 NAD가 특정 세션에 대해 수행해야 하는 작업을 나타내기 위해 subscriber:command, subscriber:reauthenticate-type이라는 Radius cisco av 쌍을 사용합니다.

다른 벤더는 cisco-av 쌍을 지원하지 않습니다. 따라서 일반적으로 이러한 디바이스는 RFC CoA(3576 또는 5176)와 두 개의 정의된 메시지 중 하나를 사용합니다.

- disconnect request(disconnect의 패킷이라고도 함) - 세션 연결을 끊는 데 사용되는 요청(재연

결을 강제로 시행하는 경우가 많음)

- CoA 푸시 - 연결 끊김 없이 투명하게 세션 상태를 변경하는 데 사용됩니다(예: VPN 세션 및 새 ACL 적용됨).

ISE는 cisco av 쌍으로 Cisco CoA를 모두 지원하며 RFC CoA 3576/5176도 모두 지원합니다.

## ISE의 솔루션

서드파티 벤더를 지원하기 위해 ISE 2.0에는 특정 벤더의 동작 방식(세션, URL 리디렉션 및 CoA 지원 방식)을 설명하는 네트워크 디바이스 프로파일 개념이 도입되었습니다.

권한 부여 프로파일은 특정 유형(네트워크 디바이스 프로파일)이며 인증이 발생하면 ISE 동작이 해당 프로파일에서 파생됩니다.

따라서 다른 벤더의 디바이스를 ISE에서 쉽게 관리할 수 있습니다. 또한 ISE의 컨피그레이션은 유연하며 새로운 네트워크 디바이스 프로파일을 조정하거나 생성할 수 있습니다.

이 문서에서는 Aruba 디바이스의 기본 프로파일 사용을 소개합니다.

기능에 대한 자세한 정보:

[Cisco Identity Services Engine으로 네트워크 액세스 장치 프로파일](#)

## Cisco ISE

1단계. 네트워크 디바이스에 Aruba Wireless Controller 추가



Administration(관리) > Network Resources(네트워크 리소스) > Network Devices(네트워크 디바이스)로 이동합니다. 선택한 벤더에 대해 올바른 디바이스 프로파일을 선택합니다(이 경우: ArubaWireless). 이미지에 표시된 대로 공유 암호 및 CoA 포트를 구성해야 합니다.

## Network Devices

\* Name

Description

\* IP Address:  /


\* Device Profile   

Model Name

Software Version

\* Network Device Group

Location  

Device Type  



### ▼ RADIUS Authentication Settings

Enable Authentication Settings

Protocol **RADIUS**

\* Shared Secret

Enable KeyWrap  

\* Key Encryption Key

\* Message Authenticator Code Key

Key Input Format  ASCII  HEXADECIMAL

CoA Port

원하는 공급업체에 대해 사용 가능한 프로필이 없는 경우 Administration(관리) > Network Resources(네트워크 리소스) > Network Device Profiles(네트워크 디바이스 프로필)에서 구성할 수 있습니다.

## 2단계. 권한 부여 프로파일 구성

Policy(정책) > Policy Elements(정책 요소) > Results(결과) > Authorization(권한 부여) > Authorization Profiles(권한 부여 프로파일)로 이동하여 1단계와 동일한 Network Device Profile(네트워크 디바이스 프로파일)을 선택합니다. ArubaWireless. 구성된 프로파일은 Aruba-redirect-BYOD with BYOD Portal이며 그림에 나와 있습니다.

Authorization Profiles > Aruba-redirect-BYOD

### Authorization Profile

\* Name

Description

\* Access Type

Network Device Profile

#### Common Tasks

Web Redirection (CWA, MDM, NSP, CPP)

Value

#### Advanced Attributes Settings

=  - +

#### Attributes Details

Access Type = ACCESS\_ACCEPT

권한 부여 프로파일에 대한 고정 링크가 생성되는 웹 리디렉션 컨피그레이션의 일부가 없습니다. Aruba는 게스트 포털에 대한 동적 리디렉션을 지원하지 않지만, 각 권한 부여 프로파일에 하나의 링크가 할당되어 있으며, 그런 다음 이미지에 표시된 대로 Aruba에 구성됩니다.

#### Common Tasks

Value

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

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

## 3단계. 권한 부여 규칙 구성

Policy(정책) > Authorization Rules(권한 부여 규칙)로 이동하고 컨피그레이션이 이미지에 표시된 대로 표시됩니다.

<input checked="" type="checkbox"/>	Basic_Authenticated_Access	if <b>Employee</b> 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

먼저, 사용자가 SSID mgarcarz\_aruba에 연결하고 ISE는 클라이언트를 기본 BYOD 포털로 리디렉션하는 Authorization Profile Aruba-redirect-BYOD를 반환합니다. BYOD 프로세스가 완료되면 클라이언트는 EAP-TLS에 연결되며 네트워크에 대한 전체 액세스 권한이 부여됩니다.

새로운 버전의 ISE에서는 동일한 정책이 다음과 같을 수 있습니다.

Status	Rule Name	Conditions	Results	Security Groups	Hits	Actions
<input checked="" type="checkbox"/>	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	⚙️
<input checked="" type="checkbox"/>	Redirect	Aruba:Aruba-Essid-Name EQUALS mgarcarz_aruba	Aruba_Redirect_BYOD	Select from list	0	⚙️
<input checked="" type="checkbox"/>	Default		DenyAccess	Select from list	0	⚙️

## 아루바 AP

### 1단계. 종속 포털 컨피그레이션

Aruba 204에서 종속 포털을 구성하려면 Security(보안) > External Captive Portal(외부 종속 포털)로 이동하여 새 종속 포털을 추가합니다. 이미지에 표시된 대로 올바른 컨피그레이션을 위해 이 정보를 입력합니다.

- 유형: Radius 인증
- IP 또는 호스트 이름: ISE 서버
- URL: ISE에서 Authorization Profile(권한 부여 프로파일) 컨피그레이션에 따라 생성되는 링크입니다. 이 링크는 특정 권한 부여 프로파일과 관련이 있으며 웹 리디렉션 컨피그레이션에서 여기에서 찾을 수 있습니다.

Native Supplicant Provisioning  Value

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

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



- 포트: 이미지에 표시된 대로 선택한 포털이 ISE에서 호스팅되는 포트 번호(기본값: 8443)입니다.

mgarcarz\_ise20

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

## 2단계. Radius 서버 컨피그레이션

Security(보안) > Authentication Servers(인증 서버)로 이동하여 CoA 포트가 이미지에 표시된 ISE에 구성된 포트와 동일한지 확인합니다.

기본적으로 Aruba 204에서는 5999로 설정되지만, 이는 RFC 5176을 준수하지 않으며 ISE에서도 작동하지 않습니다.

# Security

Authentication Servers

Users for Internal Server

Roles

Blacklisting

Edit

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

참고: Aruba 버전 6.5 이상에서는 "종속 포털" 확인란도 선택합니다.

3단계. SSID 컨피그레이션

- Security(보안) 탭은 그림과 같습니다.

Edit mgarcarz\_aruba

1 WLAN Settings 2 VLAN 3 Security 4 Access

### Security Level

More Secure

Enterprise

Personal

Open

Less Secure

Key management: WPA-2 Enterprise

Termination: Disabled

Authentication server 1: mgarcarz\_ise20 Edit

Authentication server 2: -- Select Server --

Reauth interval: 0 hrs.

Authentication survivability: Disabled

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

Accounting: Use authentication servers

Accounting interval: 0 min.

Blacklisting: Disabled

**Fast Roaming**

Opportunistic Key Caching(OKC):

802.11r:

802.11k:

802.11v:

- Access(액세스) 탭: Network-based Access Rule(네트워크 기반 액세스 규칙)을 선택하여 SSID에서 종속 포털을 구성합니다.

1단계에서 구성된 종속 포털을 사용합니다. 이미지에 표시된 대로 New(새로 만들기)를 클릭하고 Rule type(규칙 유형): Captive portal(종속 포털), Splash page type(스플래시 페이지 유형): External(외부)을 선택합니다.

1 WLAN Settings 2 VLAN 3 Security 4 Access

### Access Rules

More Control

Role-based

Network-based

Unrestricted

Less Control

Access Rules (3)

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

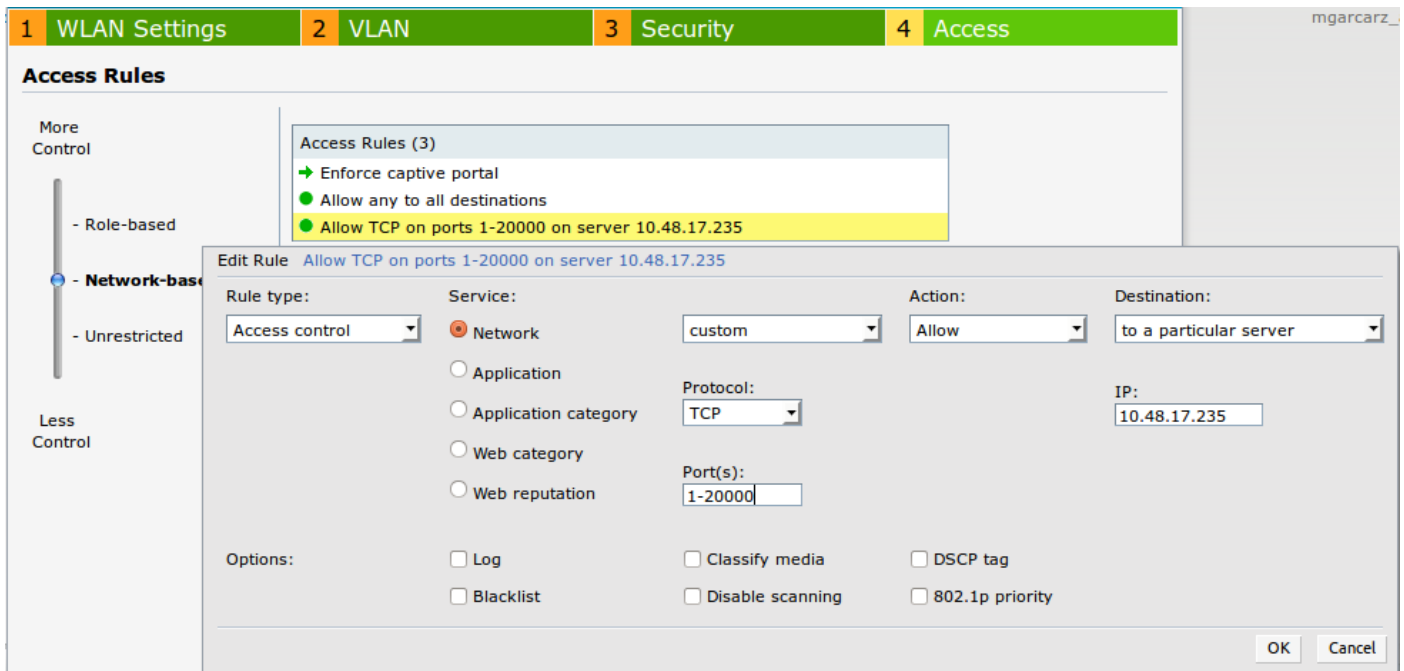
Edit Rule Enforce captive portal

Rule type: Captive portal

Splash page type: External

Captive portal profile: mgarcarz\_ise20 Edit

또한 Aruba에서 기본적으로 구성된 규칙이 있는 동안 ISE 서버(1~20000 범위의 TCP 포트)에 대한 모든 트래픽을 허용합니다. 모든 대상에 대한 모든 허용이 이미지에 표시된 대로 제대로 작동하지 않는 것 같습니다.

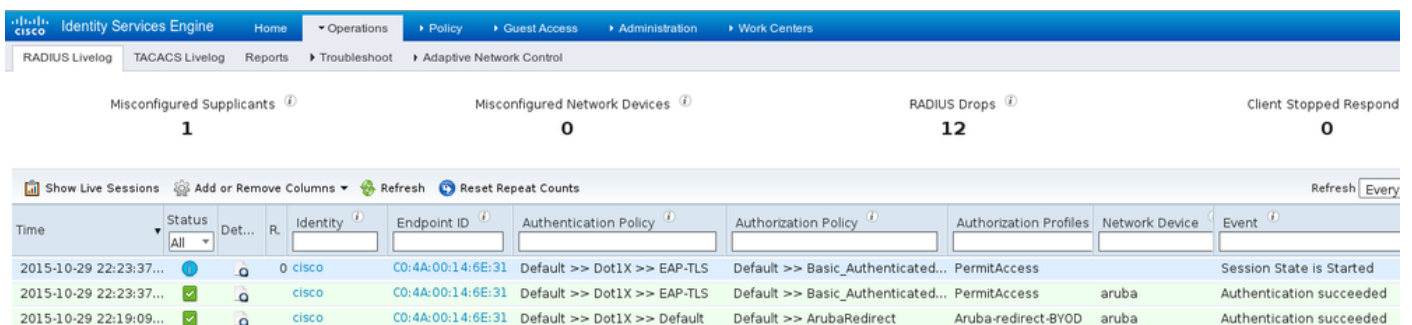


다음을 확인합니다.

구성이 올바르게 작동하는지 확인하려면 이 섹션을 활용하십시오.

1단계. EAP-PEAP를 사용하여 SSID mgarcarz\_aruba에 연결

ISE의 첫 번째 인증 로그가 나타납니다. 기본 인증 정책이 사용되었습니다. 이미지에 표시된 대로 Aruba-redirect-BYOD 권한 부여 프로파일이 반환되었습니다.



ISE는 EAP 성공 이 포함 된 RADIUS 액세스 수락 메시지를 반환 합니다. 이미지에 표시된 대로 추가 특성이 반환되지 않습니다(Cisco av 쌍 url-redirect 또는 url-redirect-acl 없음).

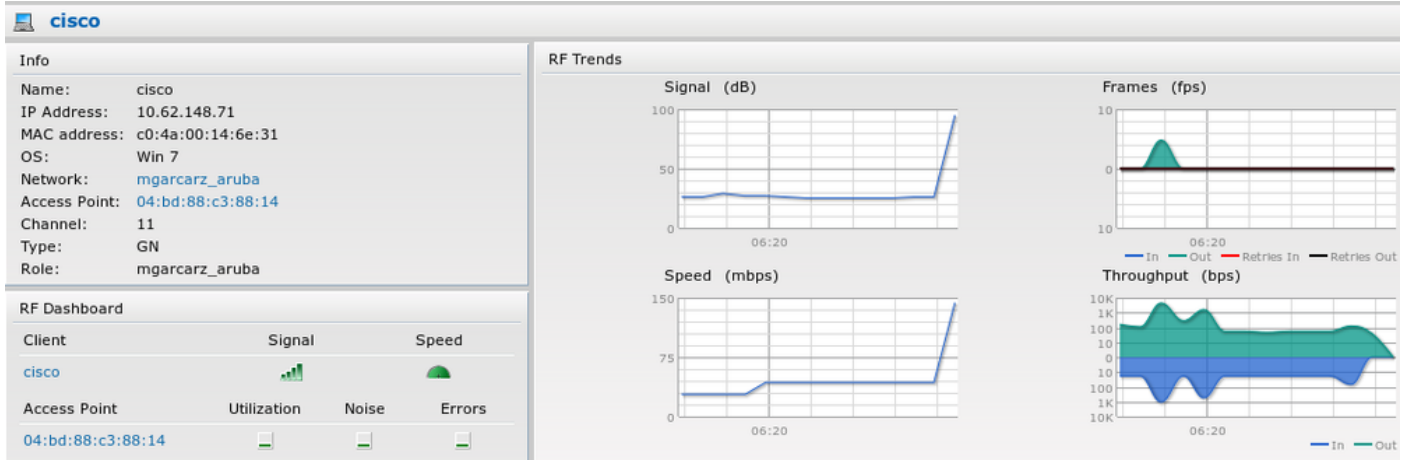
No.	Source	Destination	Protocol	Length	Info	User-Name	Acct-Session-Id
133	10.62.148.118	10.48.17.235	RADIUS	681	Access-Request(1) (id=102, l=639)	cisco	
134	10.48.17.235	10.62.148.118	RADIUS	257	Access-Challenge(11) (id=102, l=215)		
135	10.62.148.118	10.48.17.235	RADIUS	349	Access-Request(1) (id=103, 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	04BD8888142-C04A00146E31-42F8
153	10.48.17.235	10.62.148.118	RADIUS	62	Accounting-Response(5) (id=108, l=20)		

```

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

```

Aruba는 세션이 설정되었다고 보고하며(EAP-PEAP ID는 cisco) 선택한 역할은 이미지에 표시된 것처럼 mgarcarz\_aruba입니다.



이 역할은 ISE(Aruba의 종속 포털 기능)로의 리디렉션을 담당합니다.

Aruba CLI에서는 해당 세션에 대한 현재 권한 부여 상태를 확인할 수 있습니다.

```

<#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

현재 권한에 대해 ACL ID 138을 확인하려면 다음을 수행합니다.

```
<#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 ... >
```

이는 이미지에 표시된 것처럼 해당 역할에 대해 GUI에서 구성된 것과 일치합니다.

## Security

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

Roles

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

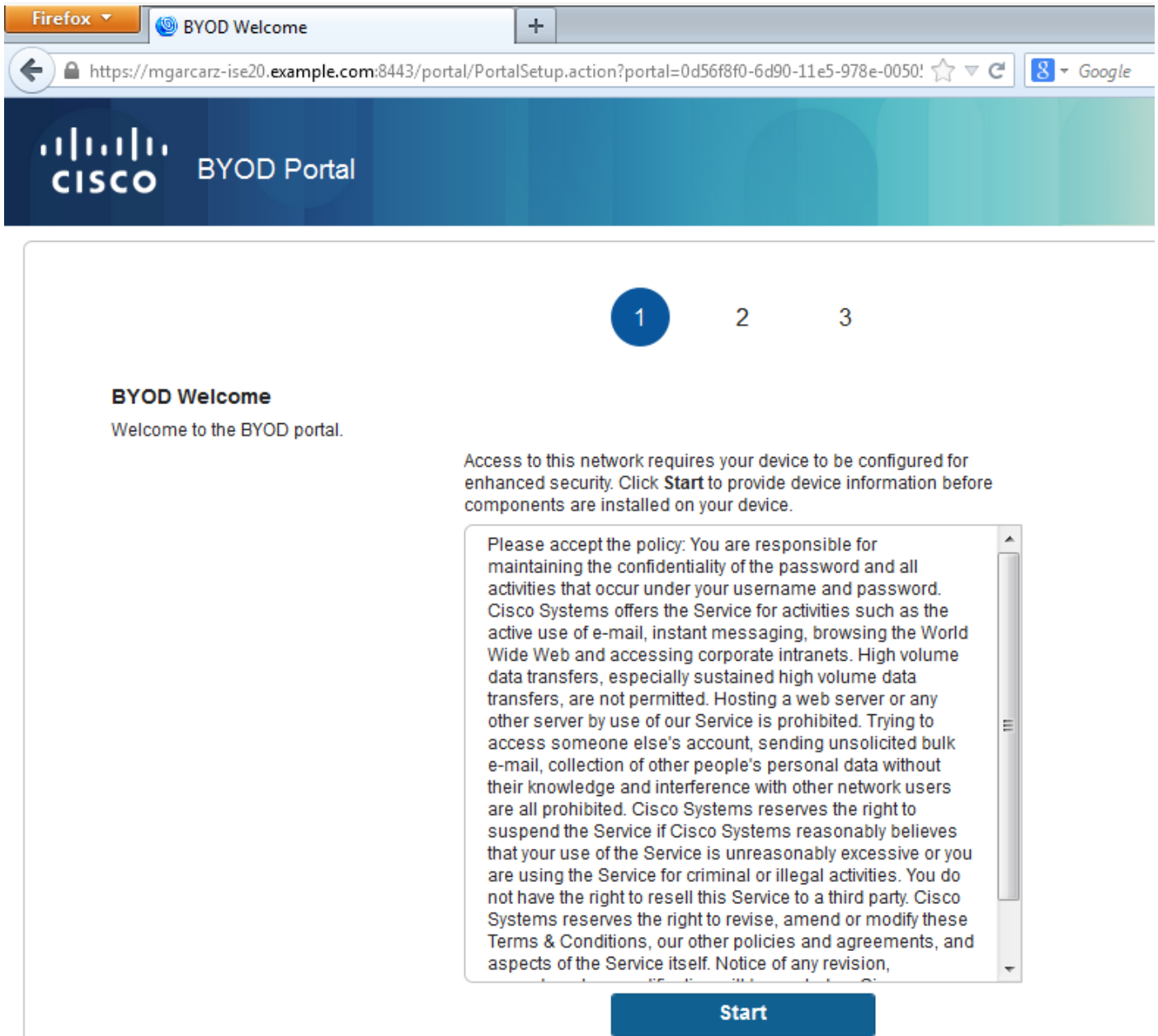
Access Rules for **mgarcarz\_aruba**

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

New Delete      New Edit Delete ↑ ↓

2단계. BYOD를 위한 웹 브라우저 트래픽 리디렉션

사용자가 웹 브라우저를 열고 주소를 입력하면 이미지에 표시된 대로 리디렉션이 발생합니다.

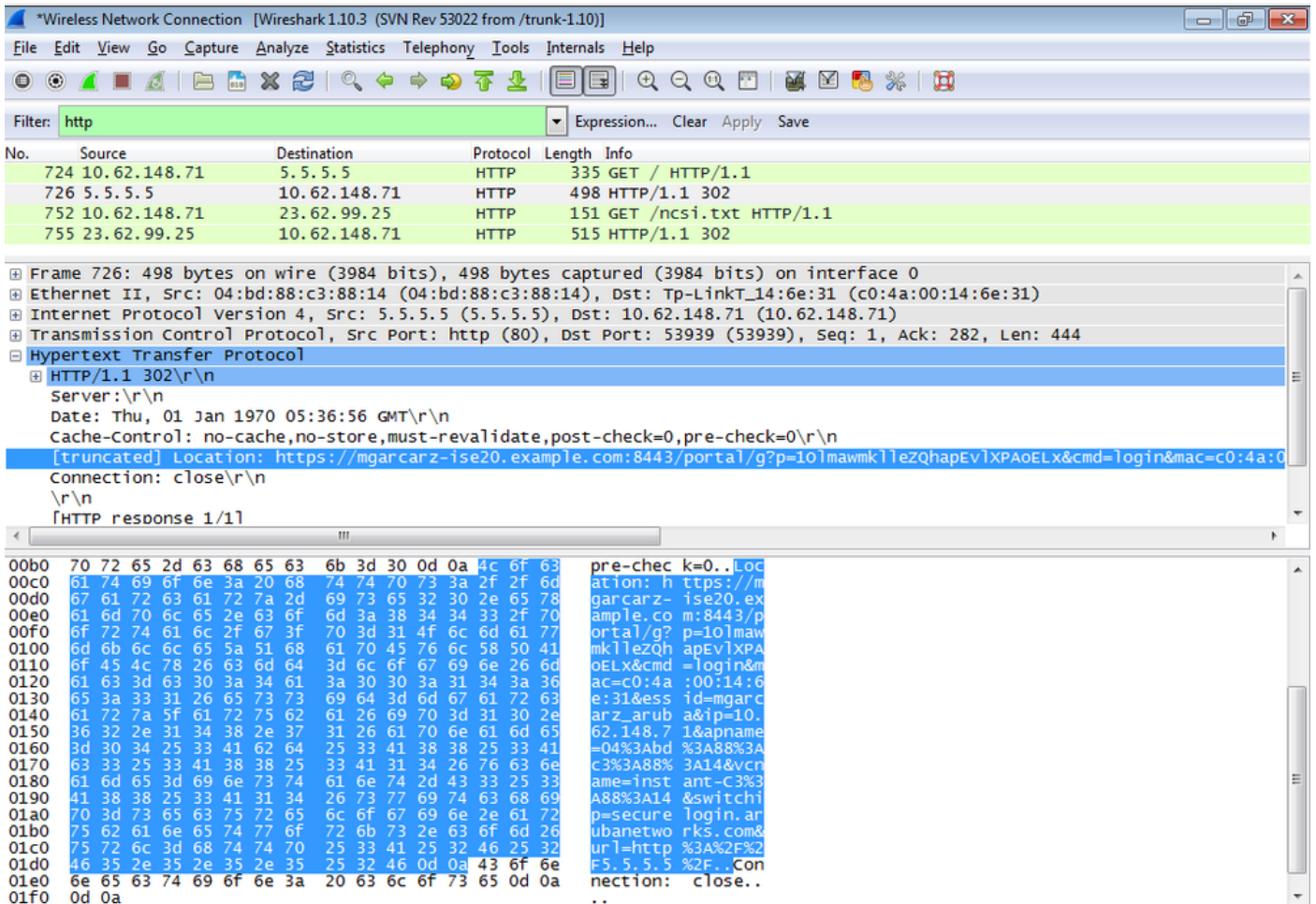


패킷 캡처를 살펴보면, Aruba가 목적지(5.5.5.5)를 스푸핑하고 HTTP 리디렉션을 ISE로 반환함을 확인합니다.

ISE에 구성되어 Aruba의 종속 포털에 복사된 것과 동일한 고정 URL입니다. 그러나 그림과 같이 여러 인수가 다음과 같이 추가됩니다.

- cmd = 로그인
- mac = c0:4a:00:14:6e:31
- essid = mgarcarz\_aruba
- ip = 10.62.148.7
- apname = 4bd88c38814(mac)
- url = <http://5.5.5.5>





이러한 인수로 인해 ISE는 Cisco 세션 ID를 다시 생성하고 ISE에서 해당 세션을 찾아 BYOD(또는 구성된 다른) 흐름을 계속할 수 있습니다.

Cisco 디바이스의 경우 audit\_session\_id가 일반적으로 사용되지만 다른 벤더에서는 지원되지 않습니다.

ISE 디버그에서 감사 세션 ID 값(네트워크를 통해 전송되지 않음)의 생성을 확인할 수 있습니다.

```
<#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
```

그리고 BYOD에 디바이스를 등록한 후 그 상관관계를 분석했습니다. 2페이지:

```
<#root>
```

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

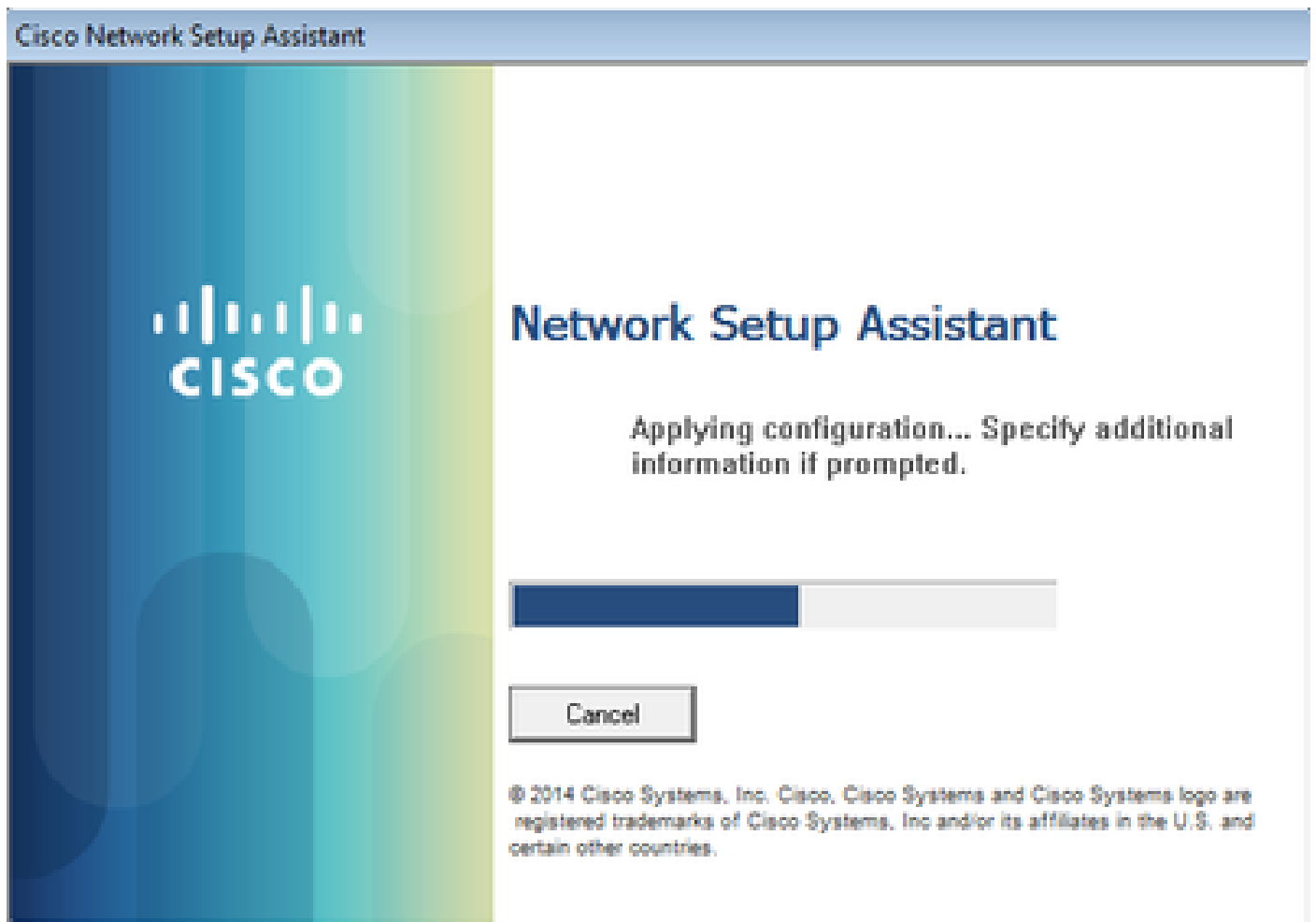
MyDevices: Successfully registered/provisioned the device

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

audit-session-id=0a3011ebXbiuDA3yUNoLUvtCRyuPFxkqYJ7TT06foOZ7G1HXj1M

후속 요청에서 클라이언트는 BYOD 3페이지로 리디렉션됩니다. 여기서 NSA가 다운로드되고 실행됩니다.

3단계. 네트워크 설정 도우미 실행



NSA는 웹 브라우저와 동일한 작업을 가지고 있습니다. 먼저 ISE의 IP 주소가 무엇인지 탐지해야 합니다. 이는 HTTP 리디렉션을 통해 구현됩니다.

이 시간 사용자는 (웹 브라우저에서처럼) IP 주소를 입력할 수 없으므로 해당 트래픽이 자동으로 생성됩니다.

이미지에 표시된 대로 기본 게이트웨이가 사용됩니다(enroll.cisco.com도 사용 가능).

The image shows a Wireshark capture of an HTTP GET request. The packet list pane shows two packets: packet 182 (223 bytes) and packet 184 (520 bytes). Packet 184 is selected, and the packet details pane shows the following structure:

- 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]

응답은 웹 브라우저와 정확히 동일합니다.

이 방법으로 NSA는 ISE에 연결하고, 컨피그레이션을 사용하여 xml 프로파일을 가져오고, SCEP 요청을 생성하고, 이를 ISE에 전송하고, 서명된 인증서(ISE 내부 CA에서 서명)를 가져오고, 무선 프로파일을 구성하고, 마지막으로 구성된 SSID에 연결할 수 있습니다.

클라이언트에서 로그를 수집합니다(Windows의 경우 %temp%/spwProfile.log). 명확성을 위해 일부 출력은 생략됩니다.

<#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:M

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

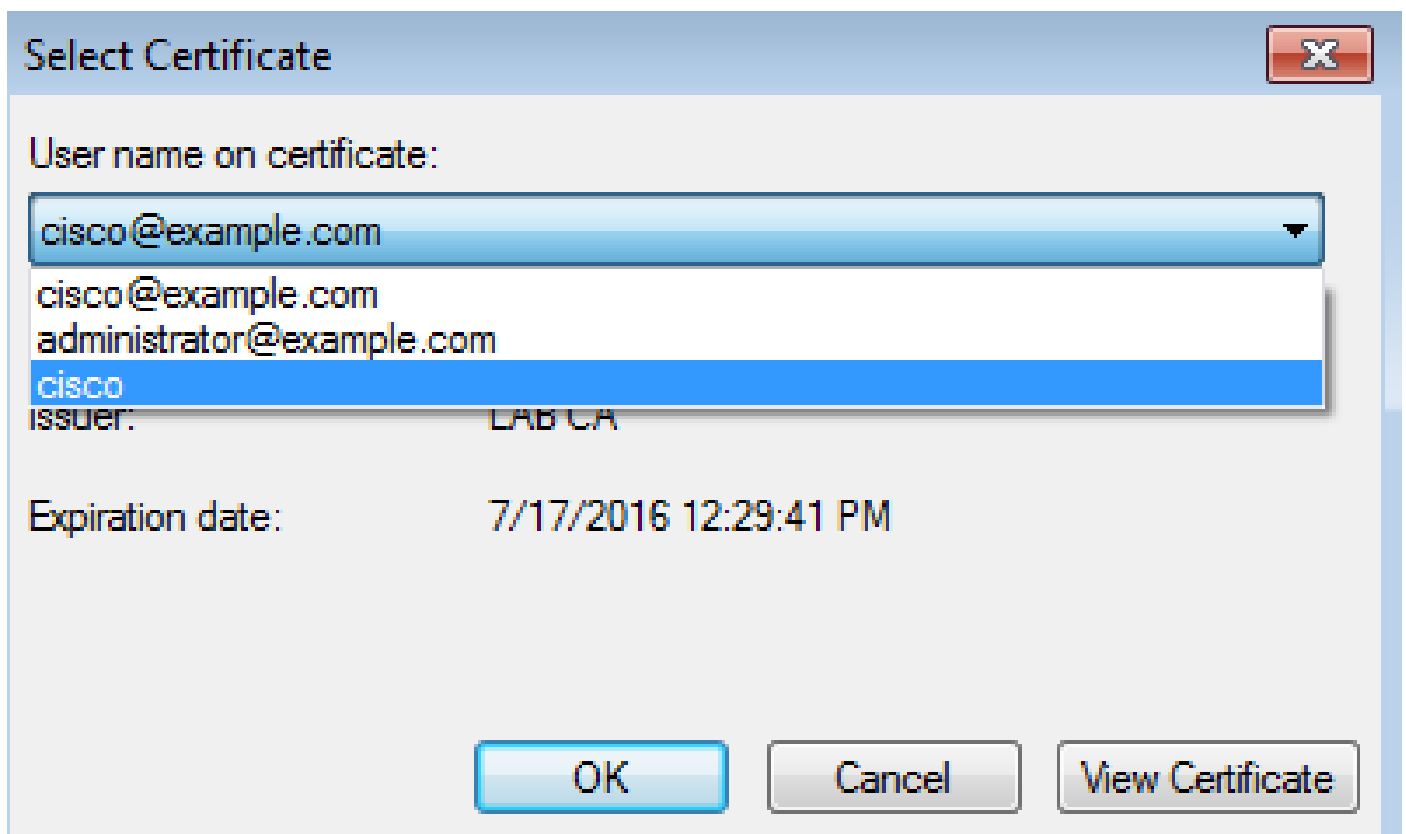
Successfully connected profile: [mgarcarz\_aruba\_tls]

WirelessProfile::SetWirelessProfile. - End

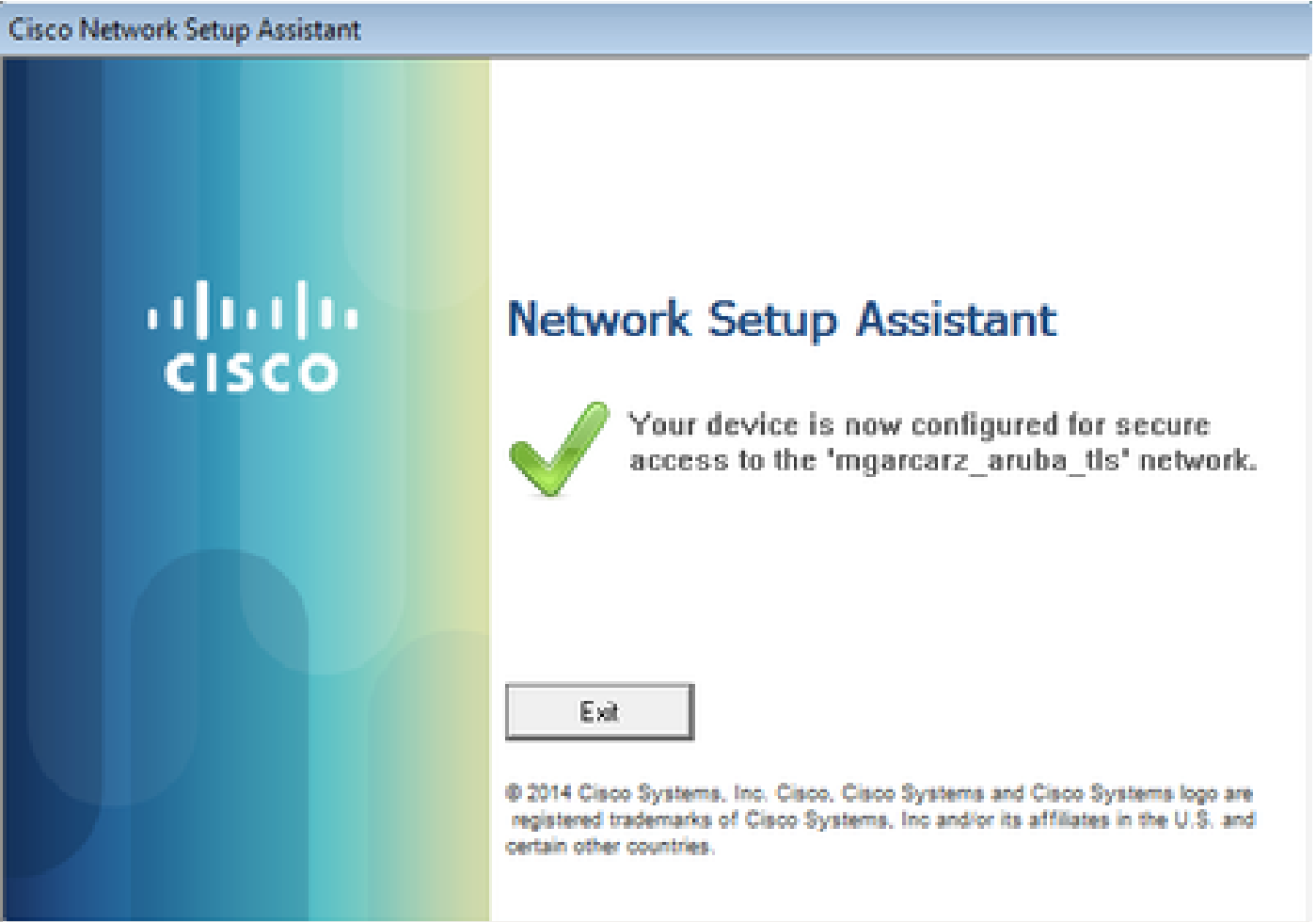
이러한 로그는 Cisco 디바이스를 사용하는 BYOD 프로세스와 동일합니다.

 참고: 여기서는 Radius CoA가 필요하지 않습니다. 새로 구성된 SSID에 다시 연결해야 하는 것은 애플리케이션(NSA)입니다.

이 단계에서 시스템이 최종 SSID에 연결을 시도하는지 확인할 수 있습니다. 사용자 인증서가 두 개 이상 있는 경우 (표시된 대로) 올바른 인증서를 선택해야 합니다.



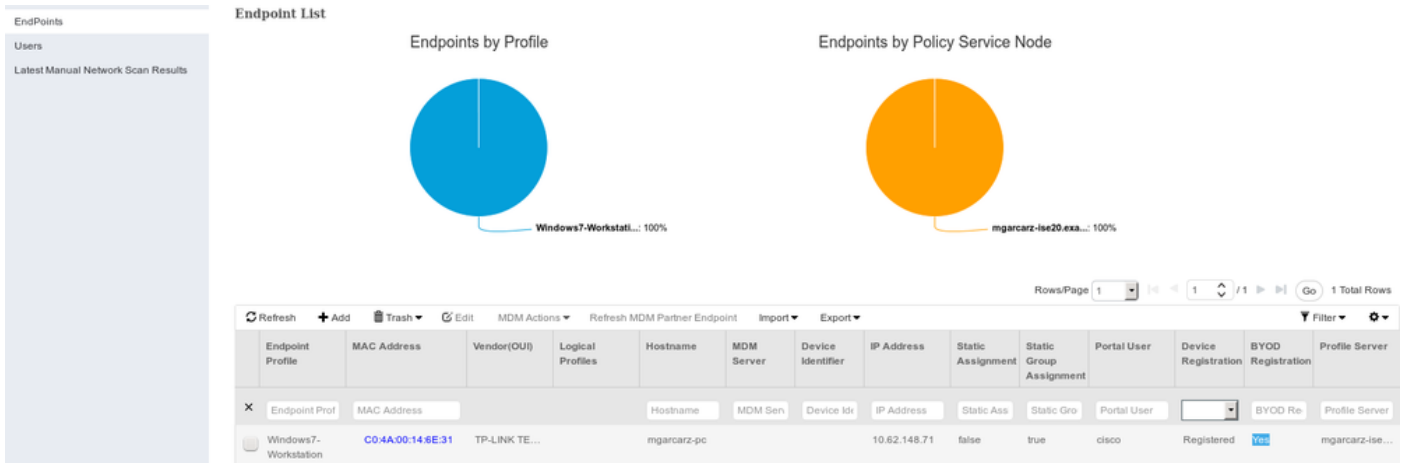
성공적인 연결 후, NSA의 보고는 이미지에 나타난 바와 같다.



이는 ISE에서 확인할 수 있습니다. 두 번째 로그는 EAP-TLS 인증에 도달하며, 이는 Basic\_Authenticated\_Access에 대한 모든 조건(EAP-TLS, Employee 및 BYOD Registered true)과 일치합니다.

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

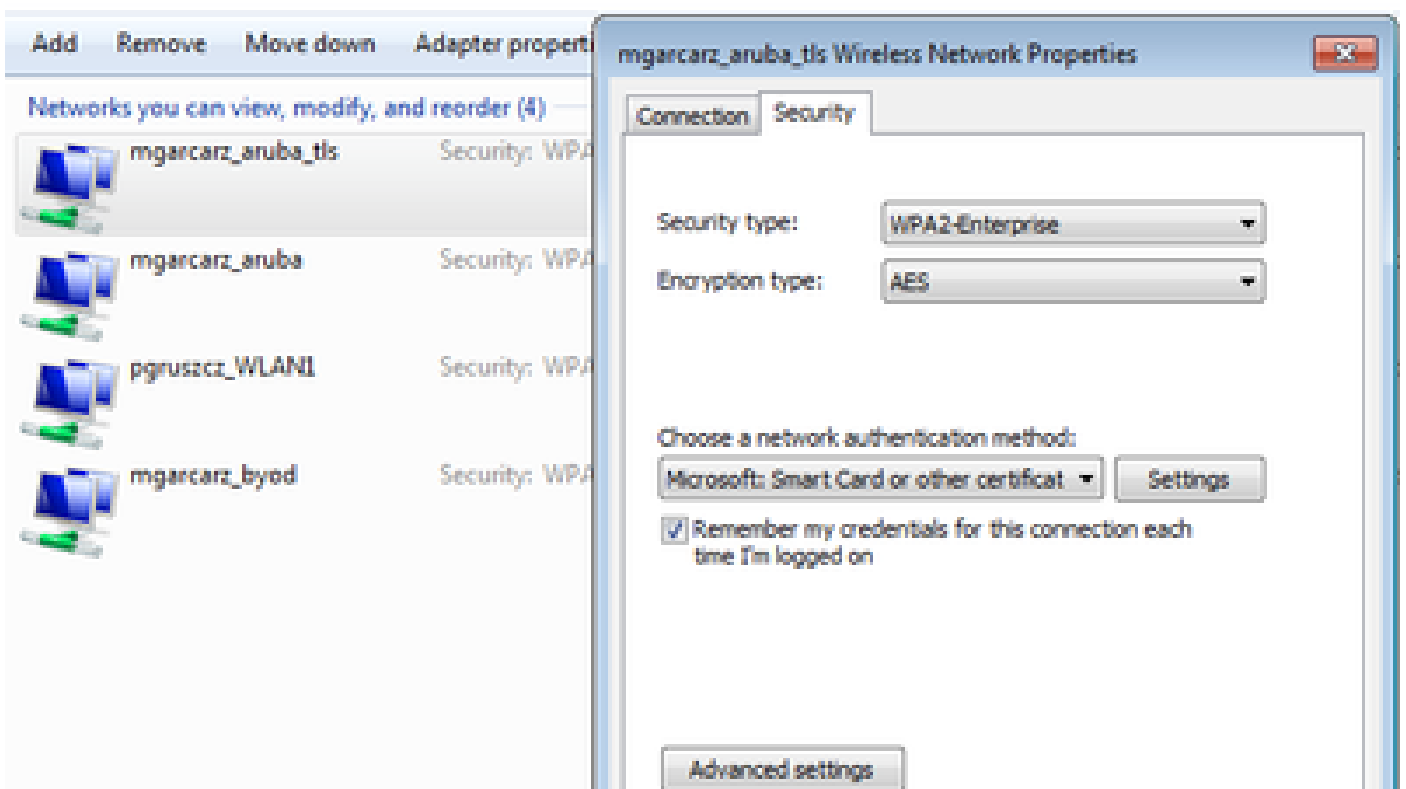
또한 엔드포인트 ID 보기에서 이미지에 표시된 대로 엔드포인트에 BYOD Registered 플래그가 true로 설정되어 있는지 확인할 수 있습니다.



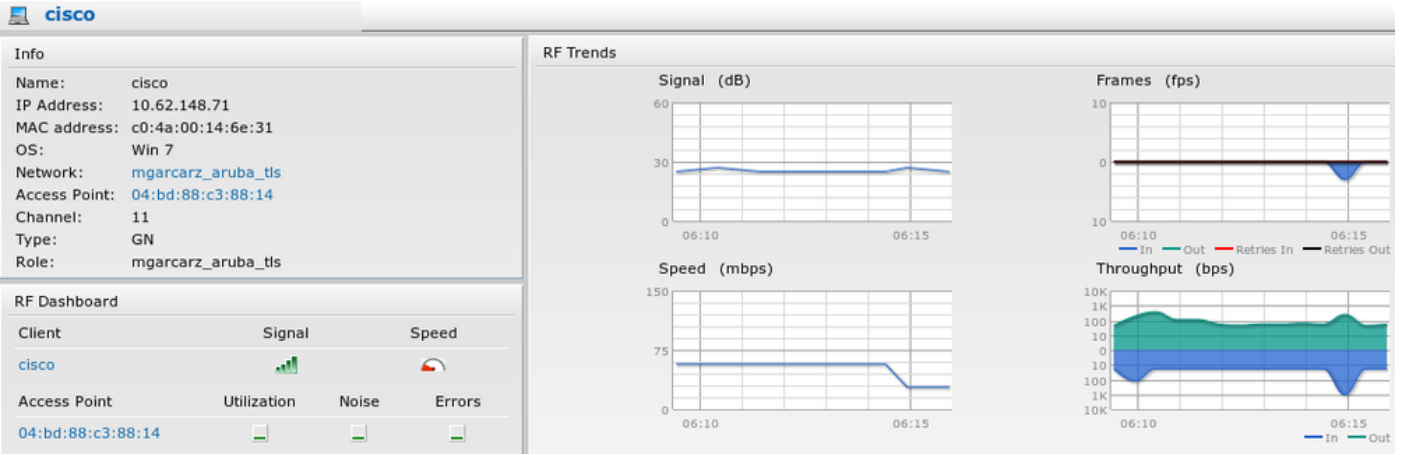
Windows PC에서 새 무선 프로파일이 기본 설정(EAP-TLS용으로 구성)으로 자동으로 생성되었으며, 이 그림과 같이 표시됩니다.

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

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



이 단계에서 Aruba는 사용자가 최종 SSID에 연결되었음을 확인합니다.



자동으로 생성되고 Network와 동일한 이름으로 지정된 역할은 전체 네트워크 액세스를 제공합니다

The image shows the Cisco Security configuration page for the role 'mgarcarz\_aruba\_tls'. The page has tabs for Authentication Servers, Users for Internal Server, Roles, Blacklisting, Firewall Settings, and Inbound Firewall. Under the Roles tab, a list of roles is shown, with 'mgarcarz\_aruba\_tls' highlighted. Below the list are 'New' and 'Delete' buttons. The Access Rules for 'mgarcarz\_aruba\_tls' are shown as 'Allow any to all destinations'. At the bottom, there are 'New', 'Edit', 'Delete', and arrow buttons.

## 기타 플로우 및 CoA 지원

### CoA가 포함된 CWA

BYOD 흐름에는 CoA 메시지가 없지만 셀프 등록 게스트 포털을 사용하는 CWA 흐름이 여기에 나와 있습니다.

구성된 권한 부여 규칙은 이미지에 표시된 것과 같습니다.

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

사용자는 MAB 인증을 사용하여 SSID에 연결되며, 어떤 웹 페이지에 연결을 시도하면 셀프 등록 게스트 포털로 리디렉션됩니다. 게스트는 새 계정을 생성하거나 현재 계정을 사용할 수 있습니다.





## 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?](#)

게스트가 성공적으로 연결되면 CoA 메시지가 권한 부여 상태를 변경하기 위해 ISE에서 네트워크 디바이스로 전송됩니다.



## Sponsored Guest Portal

### Welcome Message

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

You're very close to gaining network access.

Continue

이미지에 표시된 대로 Operations(작업) > Authentications(인증)에서 확인할 수 있습니다.

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

ISE의 CoA 메시지 디버깅:

<#root>

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

NAS-IP-Address, value=10.62.148.118

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

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

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

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

retries=2

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

invoking DynamicAuthorization,DynamicAuthorizationFlow.cpp:246

Aruba에서 제공하는 Disconnect-ACK:

<#root>

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

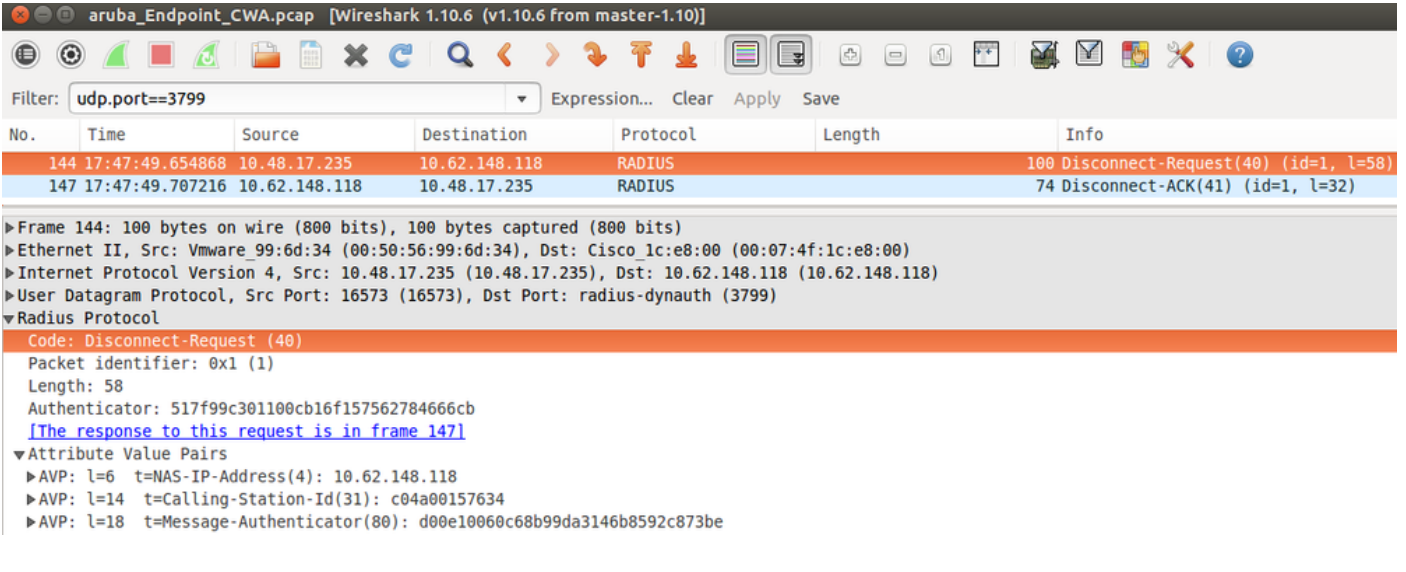
CallingStationID=c04a00157634

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


Packet type 41(DisconnectACK).

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

CoA Disconnect-Request(40) 및 Disconnect-ACK(41)를 이용한 패킷 캡처는 다음과 같습니다.



The image shows a Wireshark capture of a RADIUS session. The filter is set to 'udp.port==3799'. Two frames are highlighted: Frame 144, a RADIUS Disconnect-Request (40) from 10.48.17.235 to 10.62.148.118, and Frame 147, a RADIUS Disconnect-ACK (41) from 10.62.148.118 to 10.48.17.235. The details pane for frame 144 shows the RADIUS protocol structure, including the Code (Disconnect-Request (40)), Packet identifier (0x1 (1)), Length (58), Authenticator, and Attribute Value Pairs (AVP) for NAS-IP-Address, Calling-Station-Id, and Message-Authenticator.

 참고: RFC CoA는 장치 프로파일 Aruba(기본 설정)와 관련된 인증에 사용되었습니다. Cisco 디바이스와 관련된 인증의 경우 Cisco CoA 유형이 재인증되었을 것입니다.

## 문제 해결

이 섹션에서는 컨피그레이션 문제를 해결하는 데 사용할 수 있는 정보를 제공합니다.

### FQDN 대신 IP 주소를 사용하는 Aruba 종속 포털

Aruba의 종속 포털이 ISE의 FQDN 대신 IP 주소로 구성된 경우 PSN NSA가 실패합니다.


```
<#root>
```

```
Warning - [HTTPConnection]
```

```
Abort the HTTP connection due to invalid certificate
```

```
CN
```

그 이유는 ISE에 연결할 때 엄격한 인증서 검증입니다. ISE에 연결하기 위해 IP 주소를 사용하는 경우(FQDN 대신 IP 주소를 사용하여 URL을 리디렉션한 결과) 주체 이름 = FQDN 검증의 ISE 인증서와 함께 제공되면 실패합니다.

 참고: 웹 브라우저는 BYOD 포털을 계속 사용합니다(경고, 사용자가 승인해야 함).

### Aruba 종속 포털의 잘못된 액세스 정책

기본적으로 종속 포털로 구성된 Aruba Access-Policy는 tcp 포트 80, 443 및 8080을 허용합니다.

NSA는 ISE에서 xml 프로파일을 가져오기 위해 tcp 포트 8905에 연결할 수 없습니다. 이 오류가 보고되었습니다.

```
<#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 A11]
```

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

```
HTTP response code: 0
```

```
]
```

```
GetProfile - end
```

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

## Aruba CoA 포트 번호

기본적으로 Aruba는 CoA Air 그룹 CoA 포트 5999에 대한 포트 번호를 제공합니다. 안타깝게도 Aruba 204는 그러한 요청에 응답하지 않았습니다(그림과 같이).


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

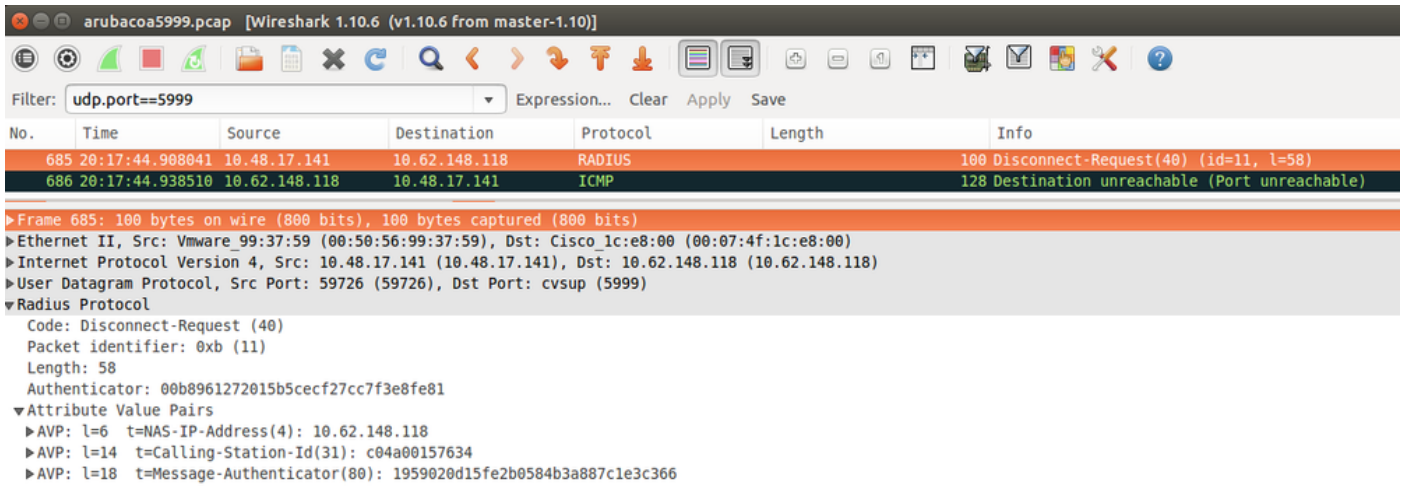
11220 Prepared the reauthenticate request

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

패킷 캡처는 그림과 같습니다.



여기서 사용하는 최상의 옵션은 RFC 5176에 설명된 대로 CoA 포트 3977일 수 있습니다.

## 일부 Aruba 디바이스에서 리디렉션

v6.3이 설치된 Aruba 3600에서는 리디렉션이 다른 컨트롤러와 약간 다르게 작동하는 것을 알 수 있습니다. 패킷 캡처 및 설명은 여기에서 확인할 수 있습니다.

770	09:29:40.5119116	10.75.94.213	173.194.124.52	HTTP	1373 GET / HTTP/1.1
772	09:29:40.5210656	173.194.124.52	10.75.94.213	HTTP	416 HTTP/1.1 200 Ok (text/html)
794	09:29:41.6982576	10.75.94.213	173.194.124.52	HTTP	63 GET /&arubaIp=6b0512fc-f699-45c6-b5cb-e62b3260e5 HTTP/1.1
797	09:29:41.7563066	173.194.124.52	10.75.94.213	HTTP	485 HTTP/1.1 302 Temporarily Moved

<#root>

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

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

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

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

'>\n

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

http://www.google.com/

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

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

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

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

## 관련 정보

- [Cisco Identity Services Engine 관리자 가이드, 릴리스 2.0](#)
- [Cisco Identity Services Engine으로 네트워크 액세스 장치 프로파일](#)
- [기술 지원 및 문서 - Cisco Systems](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.