

# Configuración de la integración de ISE 2.0 de terceros con Aruba Wireless

## Contenido

---

### [Introducción](#)

### [Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

### [Configurar](#)

[Diagrama de la red](#)

[Retos con la asistencia de terceros](#)

[SESIONES](#)

[Redirección de URL](#)

[CoA](#)

[Solución en ISE](#)

[ISE de Cisco](#)

[Paso 1. Agregar el controlador inalámbrico de Aruba a los dispositivos de red](#)

[Paso 2. Configurar perfil de autorización](#)

[Paso 3. Configuración de las reglas de autorización](#)

[AP de Aruba](#)

[Paso 1. Configuración del portal cautivo](#)

[Paso 2. Configuración del servidor de RADIUS](#)

[Paso 3. Configuración de SSID](#)

### [Verificación](#)

[Paso 1. Conexión a SSID mgarcarz\\_arubacon EAP-PEAP](#)

[Paso 2. Redirección del tráfico del navegador web para BYOD](#)

[Paso 3. Ejecución de Network Setup Assistant](#)

### [Otros flujos y soporte de CoA](#)

[CWA con CoA](#)

### [Troubleshoot](#)

[Portal cautivo de Aruba con dirección IP en lugar de FQDN](#)

[Política de acceso incorrecta del portal cautivo de Aruba](#)

[Número de puerto CoA de Aruba](#)

[Redirección en algunos dispositivos de Aruba](#)

### [Información Relacionada](#)

---

## Introducción

Este documento describe cómo resolver problemas de la función de integración de terceros en Cisco Identity Services Engine (ISE).

---

 Nota: Tenga en cuenta que Cisco no se hace responsable de la configuración o el soporte de dispositivos de otros proveedores.

---

## Prerequisites

### Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Configuración de Aruba IAP
- Flujos de BYOD en ISE
- Configuración de ISE para autenticación de certificados y contraseñas

### Componentes Utilizados

Este documento describe cómo resolver problemas de la función de integración de terceros en Cisco Identity Services Engine (ISE).

Se puede utilizar como guía para la integración con otros proveedores y flujos. La versión 2.0 de ISE admite la integración de terceros.

Este es un ejemplo de configuración que presenta cómo integrar una red inalámbrica gestionada por Aruba IAP 2004 con ISE para servicios Bring Your Own Device (BYOD).

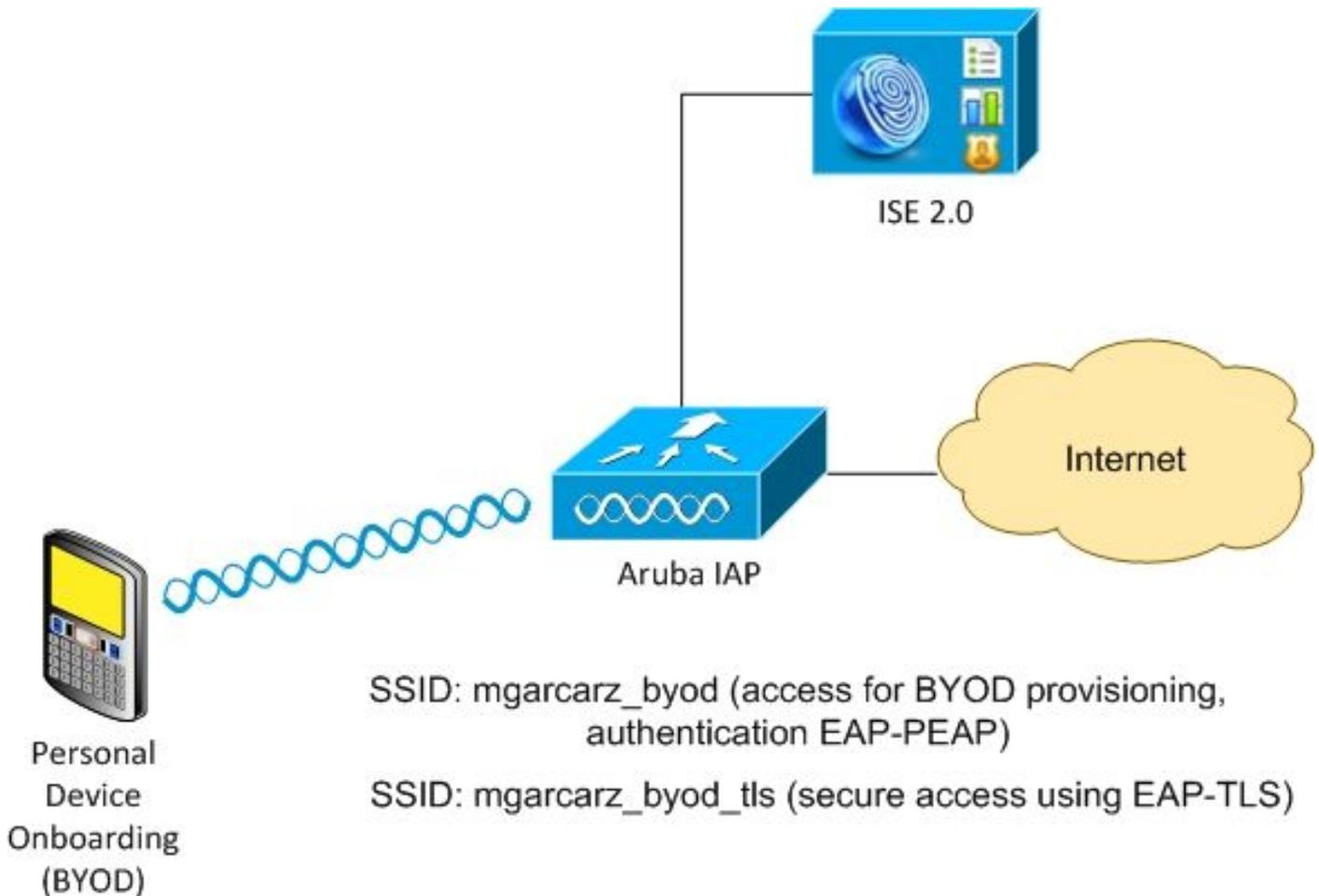
La información que contiene este documento se basa en estas versiones de software:

- Software Aruba IAP 204 6.4.2.3
- Cisco ISE, versión 2.0 y posteriores

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

## Configurar

### Diagrama de la red



Hay dos redes inalámbricas administradas por Aruba AP.

El primero (mgarcarz\_byod) se utiliza para el acceso EAP protegido por protocolo de autenticación extensible (EAP-PEAP) 802.1x.

Después de una autenticación correcta, el controlador de Aruba debe redirigir al usuario al portal BYOD de ISE: flujo de aprovisionamiento de suplicante nativo (NSP).

Se redirige al usuario, se ejecuta la aplicación Network Setup Assistant (NSA) y se aprovisiona e instala el certificado en el cliente Windows.

La CA interna de ISE se utiliza para ese proceso (configuración predeterminada).

La NSA también es responsable de la creación del perfil inalámbrico para el segundo identificador de conjunto de servicios (SSID) gestionado por Aruba (mgarcarz\_byod\_tls), que se utiliza para la autenticación de protocolo de autenticación extensible 802.1x con seguridad de capa de transporte (EAP-TLS).

Como resultado, el usuario corporativo puede incorporar dispositivos personales y obtener acceso seguro a la red corporativa.

Este ejemplo se puede modificar fácilmente para diferentes tipos de acceso, por ejemplo:

- Autenticación web central (CWA) con servicio BYOD
- Autenticación 802.1x con redirección de estado y BYOD

- Normalmente, para la autenticación EAP-PEAP se utiliza Active Directory (para abreviar este artículo se utilizan usuarios internos de ISE)
- Normalmente, para el aprovisionamiento de certificados se utiliza un servidor externo de Protocolo simple de inscripción de certificados (SCEP), normalmente el Servicio de inscripción de dispositivos de red (NDES) de Microsoft para que este artículo sea breve, se utiliza una CA ISE interna.

## Retos con la asistencia de terceros

Existen algunos retos a la hora de utilizar flujos de invitados de ISE (como BYOD, CWA, NSP, Client Provisioning Portal [CPP]) con dispositivos de terceros.

## SESIONES

Los Cisco Network Access Devices (NAD) utilizan Radius cisco-av-pair llamado audit-session-id para informar al servidor de Autenticación, Autorización y Contabilización (AAA) sobre el ID de sesión.

ISE utiliza ese valor para realizar un seguimiento de las sesiones y proporcionar los servicios correctos para cada flujo. Otros proveedores no admiten el par cisco-av.

ISE debe basarse en los atributos IETF recibidos en la solicitud de acceso y la solicitud de cuentas.

Después de recibir la solicitud de acceso, ISE crea una ID de sesión de Cisco sintetizada (a partir de ID de estación de llamada, puerto NAS, dirección IP de NAS y secreto compartido). Ese valor tiene un significado local solamente (no enviado vía red).

Como resultado, se espera que cada flujo (BYOD, CWA, NSP, CPP) adjunte los atributos correctos, por lo que ISE puede volver a calcular la ID de sesión de Cisco y realizar una búsqueda para correlacionarla con la sesión correcta y continuar el flujo.

## Redirección de URL

ISE utiliza un par cisco-av de RADIUS llamado url-redirect y url-redirect-acl para informar a NAD de que se debe redirigir el tráfico específico.

Otros proveedores no admiten el par cisco-av. Por lo general, estos dispositivos deben configurarse con una URL de redirección estática que señale a un servicio específico (perfil de autorización) en ISE.

Una vez que el usuario inicia la sesión HTTP, esos NAD se redirigen a la URL y también adjuntan argumentos adicionales (como la dirección IP o la dirección MAC) para permitir que ISE identifique la sesión específica y continúe el flujo.

## CoA

ISE utiliza el comando Radius cisco-av-pair called subscriber:command,

subscriber:reauthenticate-type para indicar qué acciones debe realizar NAD para una sesión específica.

Otros proveedores no admiten el par cisco-av. Por lo general, estos dispositivos utilizan RFC CoA (3576 o 5176) y uno de los dos mensajes definidos:

- pedido de desconexión (también llamado paquete de desconexión) - que se utiliza para desconectar la sesión (muy a menudo para forzar la reconexión)
- Transferencia CoA: se utiliza para cambiar el estado de la sesión de forma transparente sin desconexión (por ejemplo, sesión VPN y nueva ACL aplicada).

ISE admite tanto Cisco CoA con par av de Cisco como RFC CoA 3576/5176.

## Solución en ISE

Con el fin de ofrecer compatibilidad con proveedores externos, ISE 2.0 introdujo un concepto de perfiles de dispositivos de red que describe cómo se comporta un proveedor específico: cómo se admiten sesiones, redirección de URL y CoA.

Los perfiles de autorización son de un tipo específico (perfil de dispositivo de red) y una vez que se produce la autenticación, el comportamiento de ISE se deriva de ese perfil.

Como resultado, ISE puede gestionar fácilmente dispositivos de otros proveedores. Además, la configuración en ISE es flexible y permite ajustar o crear nuevos perfiles de dispositivos de red.

Este artículo presenta el uso del perfil predeterminado para el dispositivo Aruba.

Más información sobre la función:

[Perfiles de dispositivos de acceso a la red con Cisco Identity Services Engine](#)

## ISE de Cisco

Paso 1. Agregar el controlador inalámbrico de Aruba a los dispositivos de red

Vaya a Administración > Recursos de red > Dispositivos de red. Elija el perfil de dispositivo correcto para el proveedor seleccionado, en este caso: ArubaWireless. Asegúrese de configurar el secreto compartido y el puerto CoA como se muestra en las imágenes.

## 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

En caso de que no haya un perfil disponible para el proveedor deseado, se puede configurar en Administration > Network Resources > Network Device Profiles.

Paso 2. Configurar perfil de autorización

Vaya a Policy > Policy Elements > Results > Authorization > Authorization Profiles y elija el mismo perfil de dispositivo de red que en el paso 1. ArubaWireless. El perfil configurado es Aruba-redirect-BYOD with BYOD Portal y se muestra en las imágenes.

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

Falta parte de la configuración de redirección web, donde se genera un enlace estático al perfil de autorización. Aunque Aruba no admite la redirección dinámica al portal de invitados, hay un enlace asignado a cada perfil de autorización, que se configura en Aruba y se muestra en la imagen.

#### 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>**

### Paso 3. Configuración de las reglas de autorización

Navegue hasta Policy > Authorization Rules y la configuración es como se muestra en la imagen.

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

En primer lugar, el usuario se conecta al SSID mgarcarz\_aruba e ISE devuelve el perfil de autorización Aruba-redirect-BYOD, que redirige al cliente al portal BYOD predeterminado. Una vez finalizado el proceso de BYOD, el cliente se conecta con EAP-TLS y se concede acceso completo a la red.

En las versiones más recientes de ISE, la misma política podría parecerse a la siguiente:

## AP de Aruba

### Paso 1. Configuración del portal cautivo

Para configurar Captive Portal en Aruba 2004, navegue hasta Security > External Captive Portal y agregue uno nuevo. Ingrese esta información para una configuración adecuada y como se muestra en la imagen.

- Tipo: Autenticación Radius
- IP o nombre de host: servidor ISE
- URL: enlace que se crea en ISE en la configuración del perfil de autorización; es específico de un perfil de autorización concreto y se puede encontrar aquí en la configuración de redirección web

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=10lmawmkleZQhapEvIXPAoELx**

- Puerto: número de puerto en el que el portal seleccionado está alojado en ISE (de forma predeterminada: 8443), como se muestra en la imagen.

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)

---

## Paso 2. Configuración del servidor de RADIUS

Vaya a Security > Authentication Servers para asegurarse de que el puerto CoA sea el mismo que el configurado en ISE como se muestra en la imagen.

De forma predeterminada, en Aruba 2004, está configurado en 5999, sin embargo, no cumple con RFC 5176 y tampoco funciona con ISE.

# 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"/>	

Nota: En la versión 6.5 y posteriores de Aruba, seleccione también la casilla de verificación "Portal cautivo".

## Paso 3. Configuración de SSID

- La ficha Seguridad es la que se muestra en la imagen.

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:

- Ficha Acceso: seleccione Regla de acceso basada en red para configurar el portal cautivo en SSID.

Utilice el portal cautivo configurado en el paso 1. Haga clic en New, elija Rule type: Captive portal, Splash page type: External como se muestra en la imagen.

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

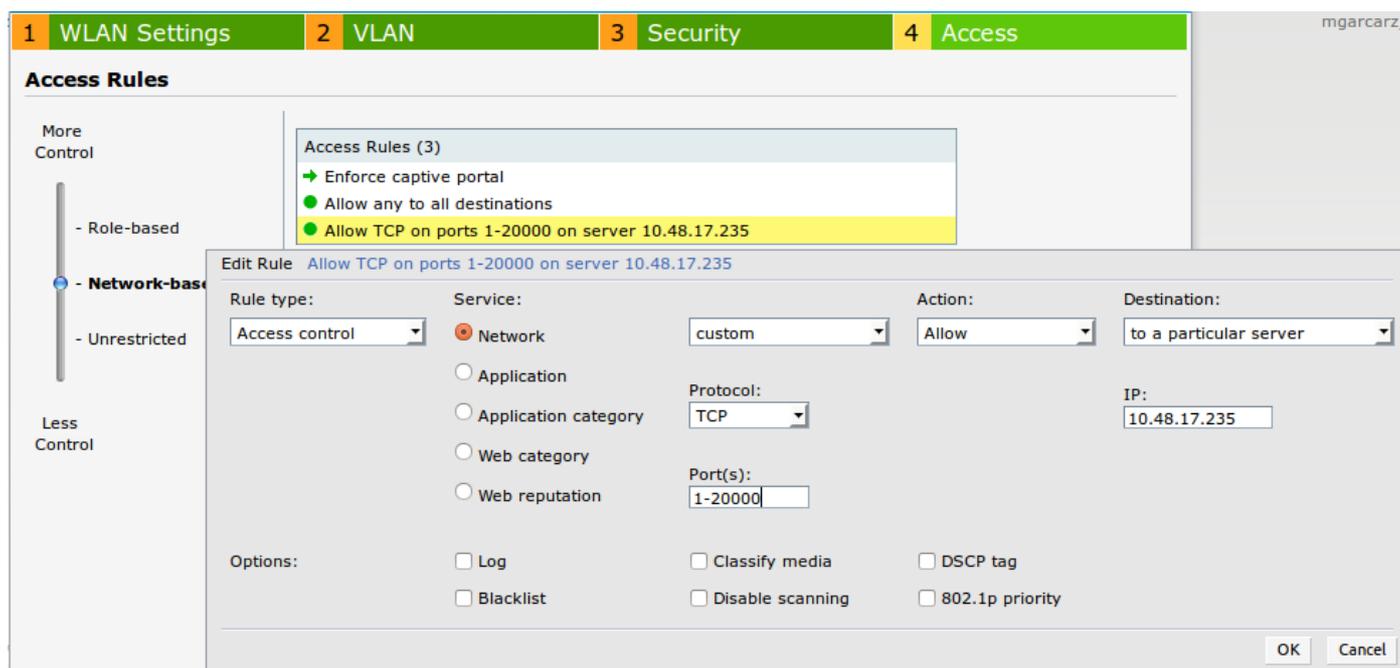
Rule type: Captive portal

Splash page type: External

Captive portal profile: mgarcarz\_ise20 [Edit](#)

Además, permite todo el tráfico al servidor ISE (puertos TCP en el rango 1-20000), mientras que

la regla configurada de forma predeterminada en Aruba: Permitir cualquiera a todos los destinos parece no funcionar correctamente como se muestra en la imagen.



## Verificación

Utilize esta sección para confirmar que su configuración funcione correctamente.

Paso 1. Conexión a SSID mgarcarz\_aruba con EAP-PEAP

Aparece el primer registro de autenticación en ISE. Se ha utilizado la política de autenticación predeterminada; el perfil de autorización de Aruba-redirect-BYOD se ha devuelto tal y como se muestra en la imagen.

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

ISE devuelve el mensaje de aceptación de acceso de RADIUS con EAP correcto. Tenga en cuenta que no se devuelven atributos adicionales (no se devuelve el URL-redirect o el URL-redirect-acl de Cisco av-pair), como se muestra en la imagen.

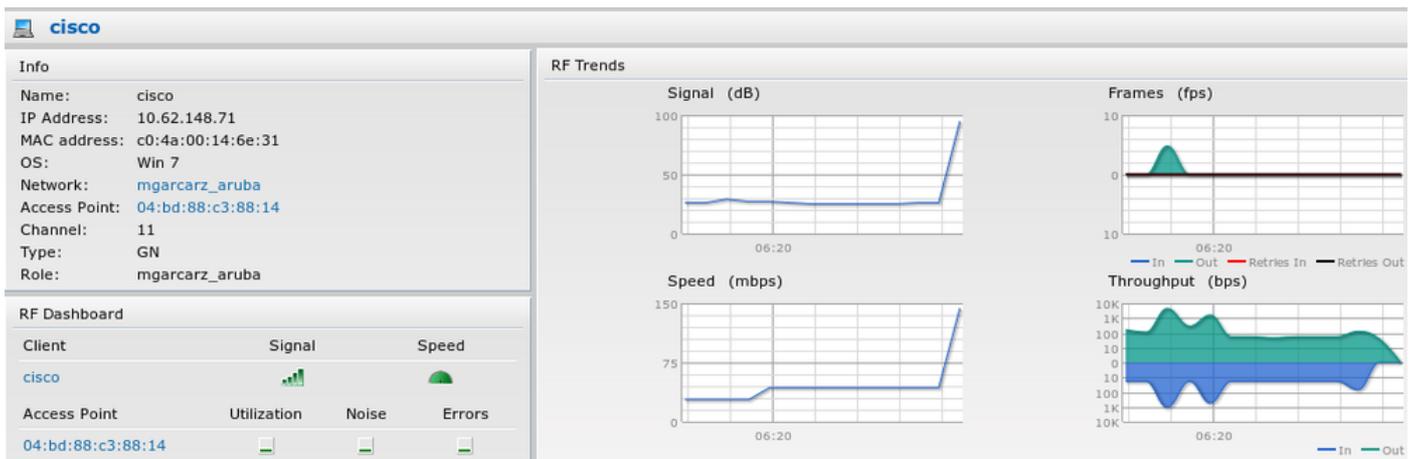
No.	Source	Destination	Protocol	Length	Info	User-Name	Acct-Session-Id
133	10.62.148.118	10.48.17.235	RADIUS	681	Access-Request(1) (id=102, l=639)	cisco	
134	10.48.17.235	10.62.148.118	RADIUS	257	Access-Challenge(11) (id=102, l=215)		
135	10.62.148.118	10.48.17.235	RADIUS	349	Access-Request(1) (id=103, 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)

```

Aruba informa de que se ha establecido la sesión (la identidad EAP-PEAP es cisco) y que la función seleccionada es mgarcarz\_aruba, como se muestra en la imagen.



Esa función es responsable de la redirección a ISE (funcionalidad de portal cautivo en Aruba).

En Aruba CLI, es posible confirmar cuál es el estado de autorización actual para esa sesión:

```

<#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

Y para verificar el ID de ACL 138 para los permisos actuales:

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

Que coincida con lo que se configuró en la GUI para ese Rol, como se muestra en la imagen.

## 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

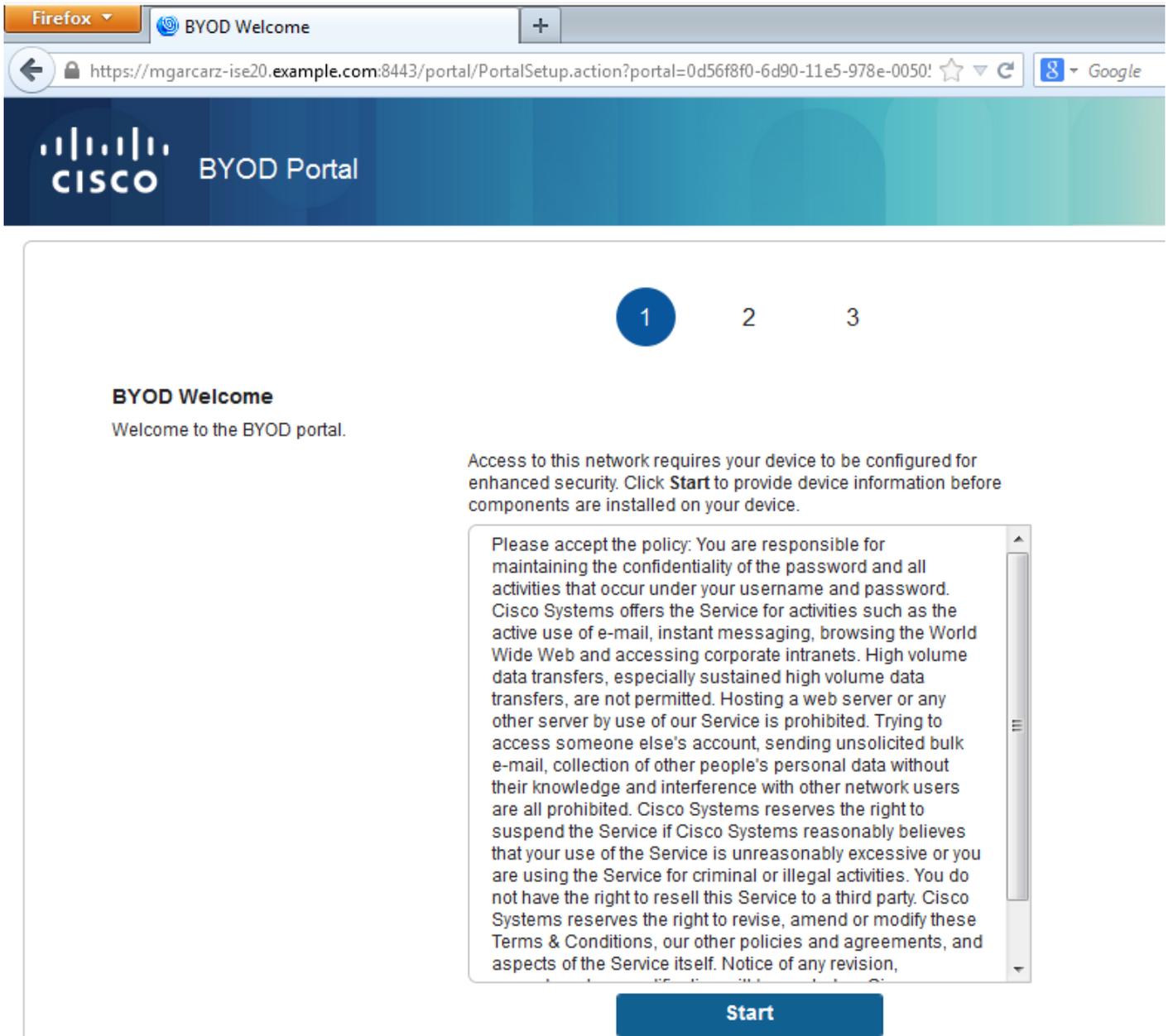
Access Rules for **mgarcarz\_aruba**

- 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 ↑ ↓

### Paso 2. Redirección del tráfico del navegador web para BYOD

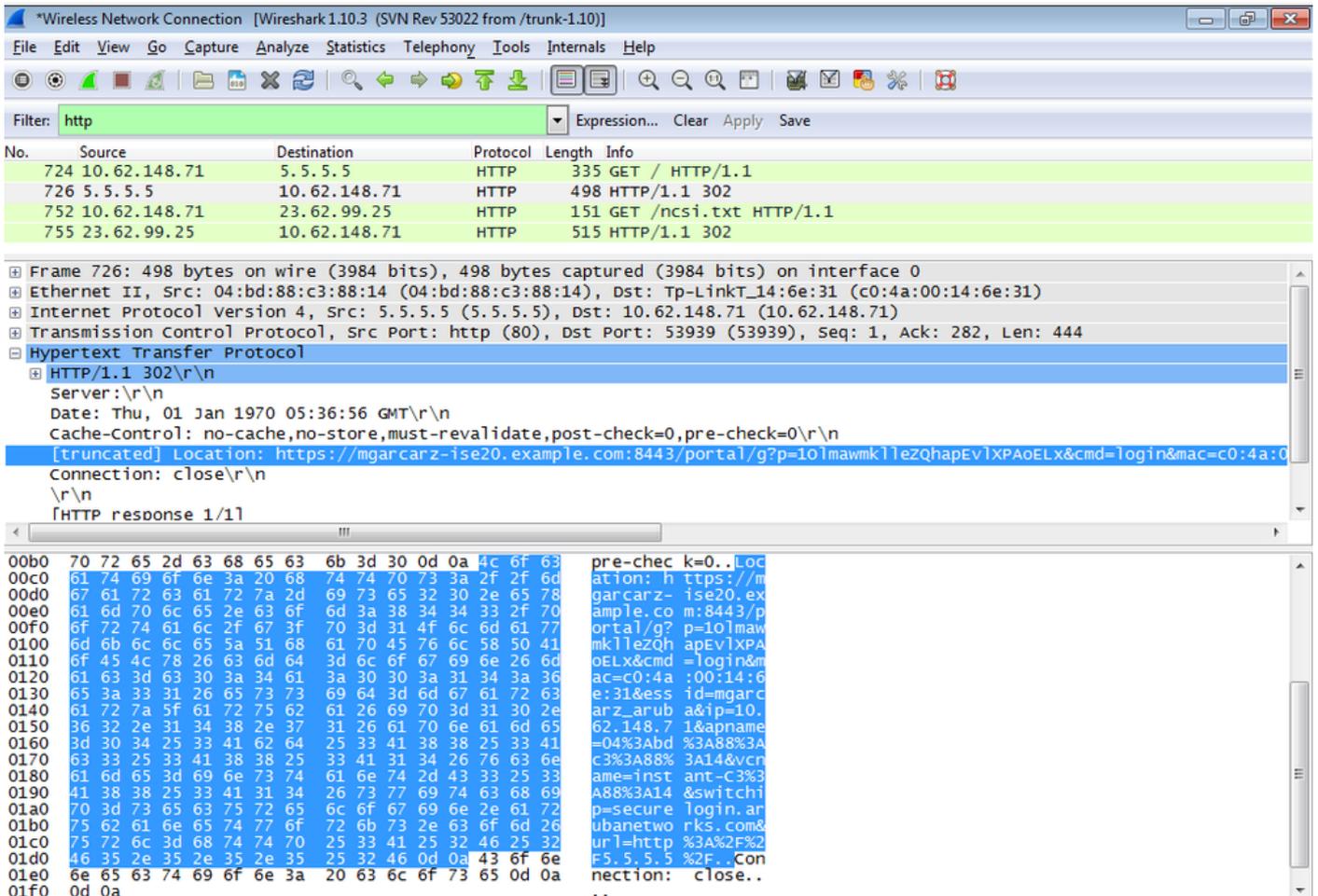
Una vez que el usuario abre el navegador web y escribe cualquier dirección, se produce la redirección como se muestra en la imagen.



Al observar las capturas de paquetes, se confirma que Aruba suplanta el destino (5.5.5.5) y devuelve la redirección HTTP a ISE.

Observe que es la misma URL estática configurada en ISE y copiada en Captive Portal en Aruba, pero además se agregan varios argumentos como se muestra a continuación en la imagen:

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



Gracias a estos argumentos, ISE puede recrear la ID de sesión de Cisco, averiguar la sesión correspondiente en ISE y continuar con el flujo de BYOD (o cualquier otro flujo configurado).

Para los dispositivos Cisco, audit\_session\_id se utilizaría normalmente, pero no es compatible con otros proveedores.

Para confirmar que a partir de las depuraciones de ISE, es posible ver la generación del valor audit-session-id (que nunca se envía a través de la red):

<#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
```

Y luego, la correlación de eso después del registro del dispositivo en BYOD Página 2:

<#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
```

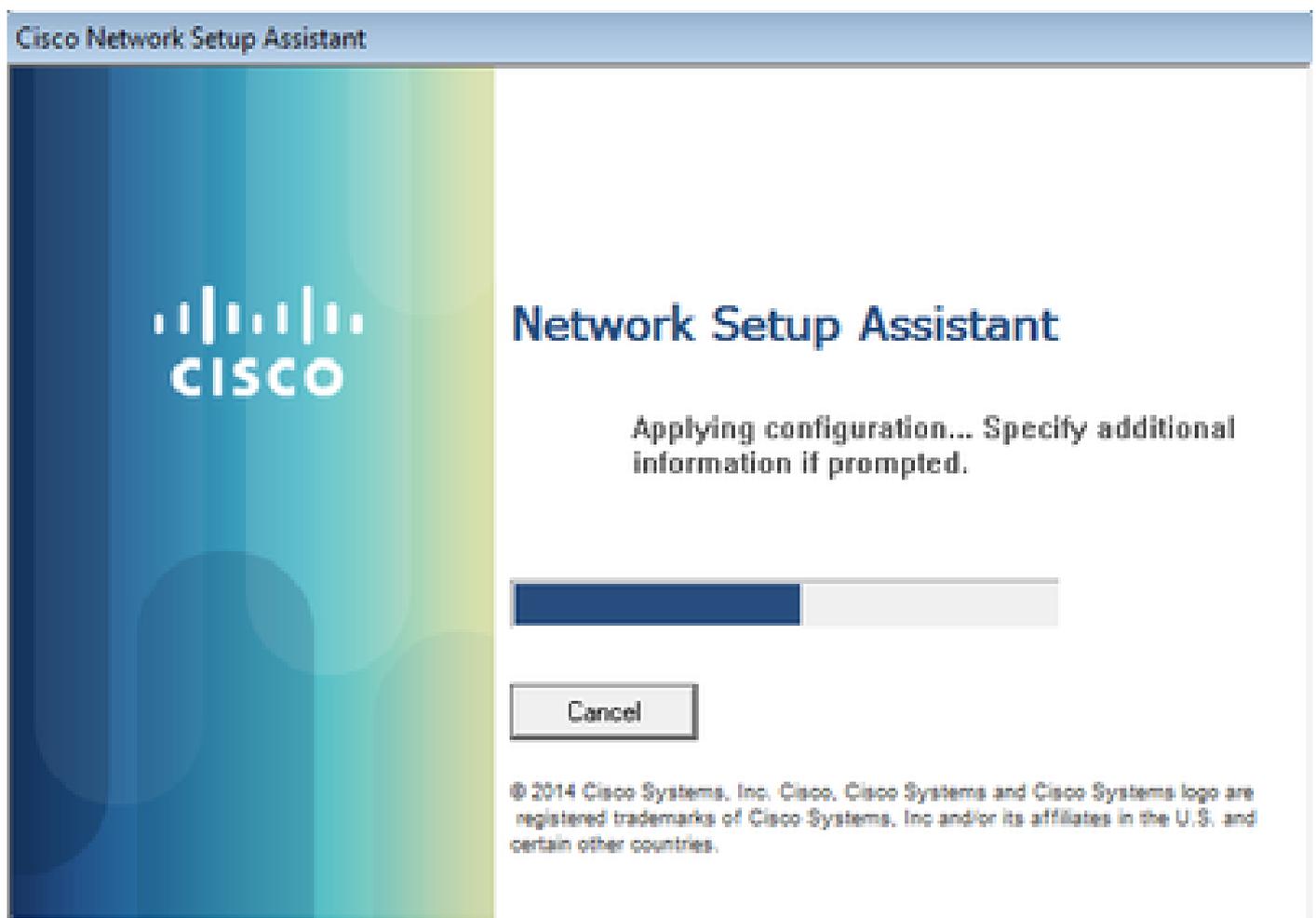
MyDevices: Successfully registered/provisioned the device

(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

En las solicitudes posteriores, el cliente se redirige a la página 3 de BYOD, donde se descarga y ejecuta la NSA.

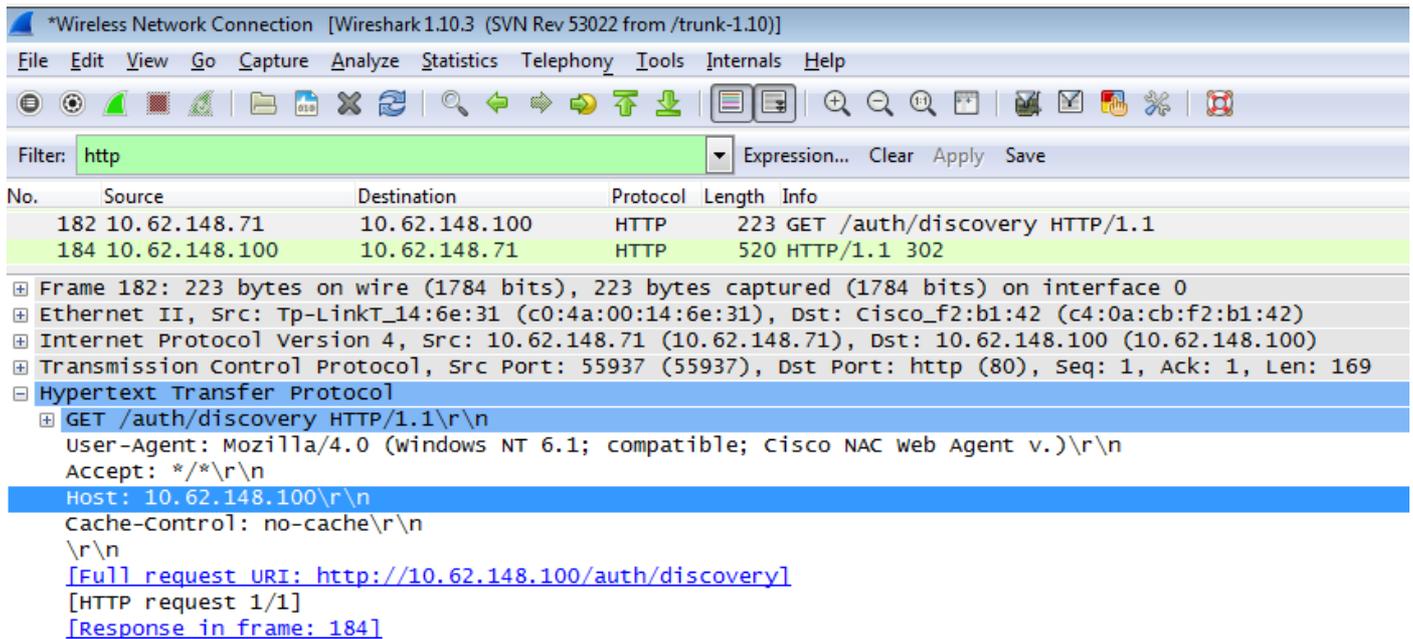
### Paso 3. Ejecución de Network Setup Assistant



La NSA tiene la misma tarea que el navegador web. En primer lugar, debe detectar cuál es la dirección IP de ISE. Esto se logra a través de la redirección HTTP.

Debido a que este usuario de tiempo no tiene la posibilidad de escribir la dirección IP (como en el navegador web), ese tráfico se genera automáticamente.

Se utiliza la puerta de enlace predeterminada (también se puede utilizar enroll.cisco.com), como se muestra en la imagen.



La respuesta es exactamente la misma que para el navegador web.

De esta manera, la NSA puede conectarse a ISE, obtener un perfil xml con la configuración, generar una solicitud SCEP, enviarla a ISE, obtener un certificado firmado (firmado por una CA interna de ISE), configurar un perfil inalámbrico y, finalmente, conectarse al SSID configurado.

Recopile registros del cliente (en Windows están en %temp%/spwProfile.log). Algunos resultados se omiten para mayor claridad:

```
<#root>
```

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

Downloading profile configuration...

Discovering ISE using default gateway

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

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

redirect attempt to discover ISE with the response url

DiscoverISE - start

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

DiscoverISE - end

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

GetProfile - start

GetProfile - end

Successfully retrieved profile xml

using V2 xml version

parsing wireless connection setting

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

set ChallengePwd

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

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

ec 8a 11 78^M

] as rootCA

Installed CA cert for authMode machineOrUser - Success

HttpWrapper::SendScepRequest

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

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

Certificate issued - successfully

ScepWrapper::InstallCert start

ScepWrapper::InstallCert: Reading scep response file

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

ScepWrapper::InstallCert GetCertHash -- return val 1

ScepWrapper::InstallCert end

Configuring wireless profiles...

Configuring ssid [mgarcarz\_aruba\_tls]

WirelessProfile::SetWirelessProfile - Start

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

Connect to SSID

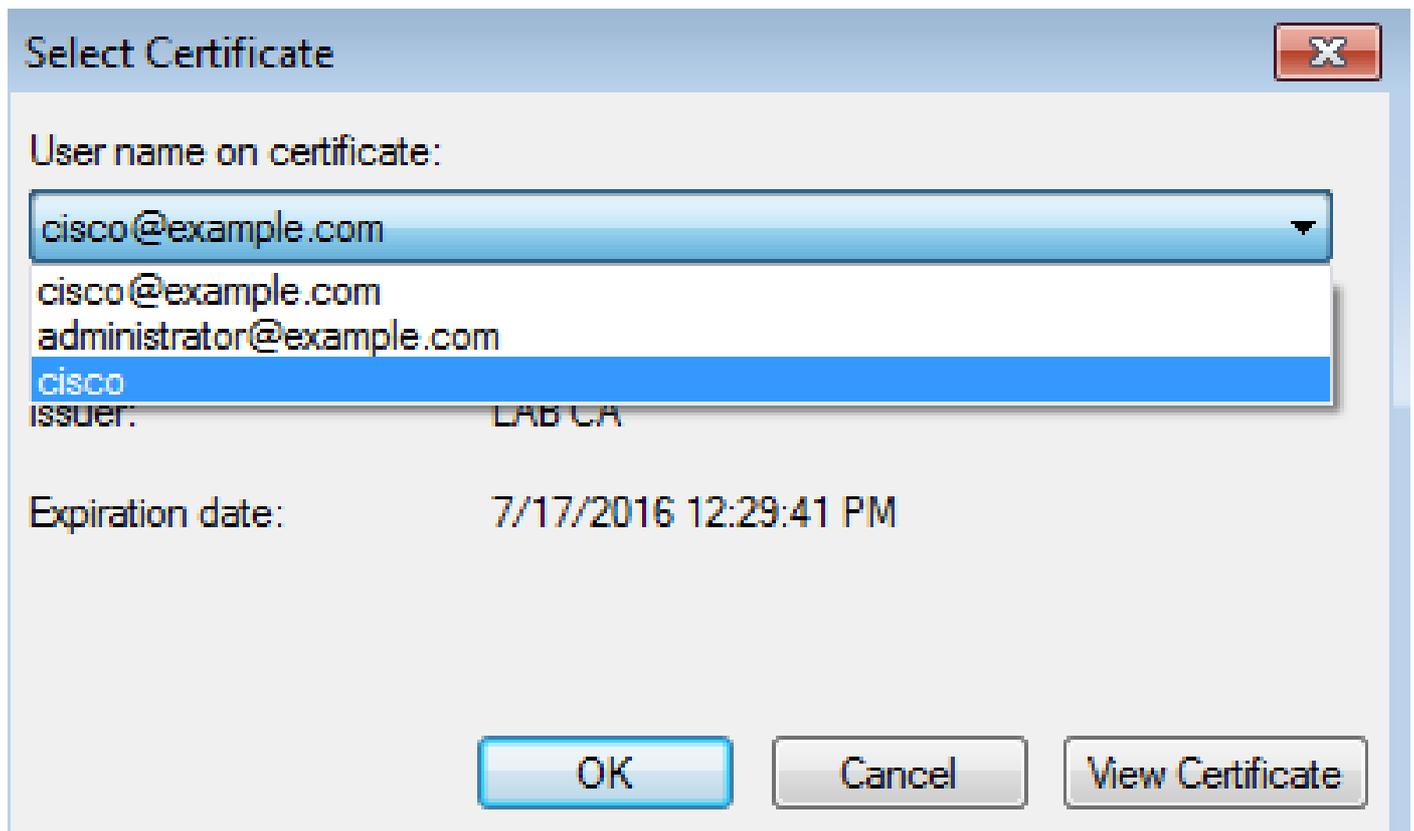
Successfully connected profile: [mgarcarz\_aruba\_tls]

WirelessProfile::SetWirelessProfile. - End

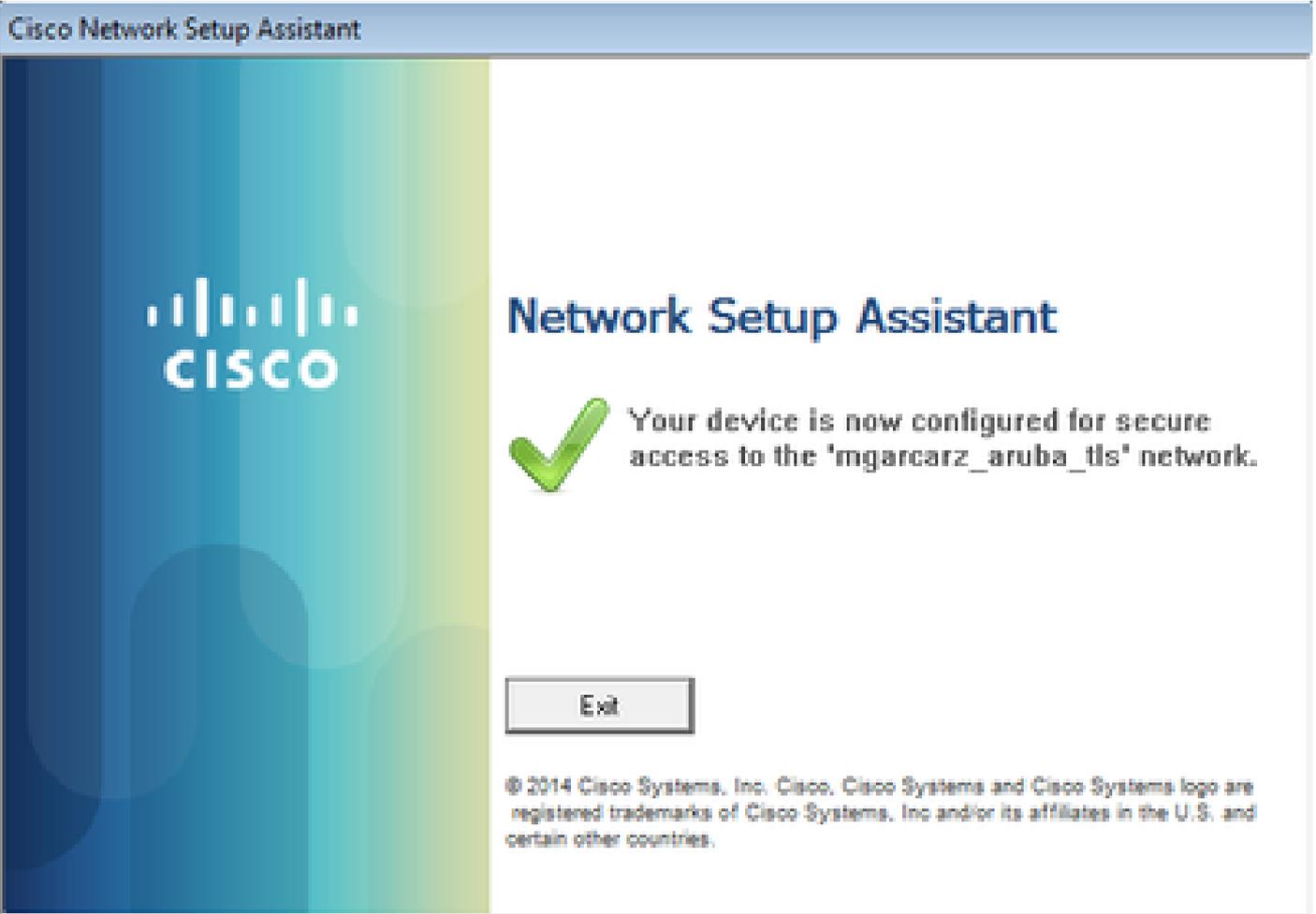
Estos registros son exactamente los mismos que para el proceso BYOD con dispositivos Cisco.

 Nota: Radius CoA no es necesario aquí. Es la aplicación (NSA) la que fuerza la reconexión a un SSID recién configurado.

En ese momento, el usuario puede ver que el sistema intenta asociarse a un SSID final. Si tiene más de un certificado de usuario, debe seleccionar el correcto (como se muestra en la imagen).



Después de una conexión exitosa, los informes de la NSA son como se muestra en la imagen.



Esto se puede confirmar en ISE: el segundo registro accede a la autenticación EAP-TLS, que cumple todas las condiciones de Basic\_Authenticated\_Access (EAP-TLS, Employee y BYOD Registered true).

Identity Services Engine										
RADIUS Livelog										
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
2015-10-29 22:23:37...				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

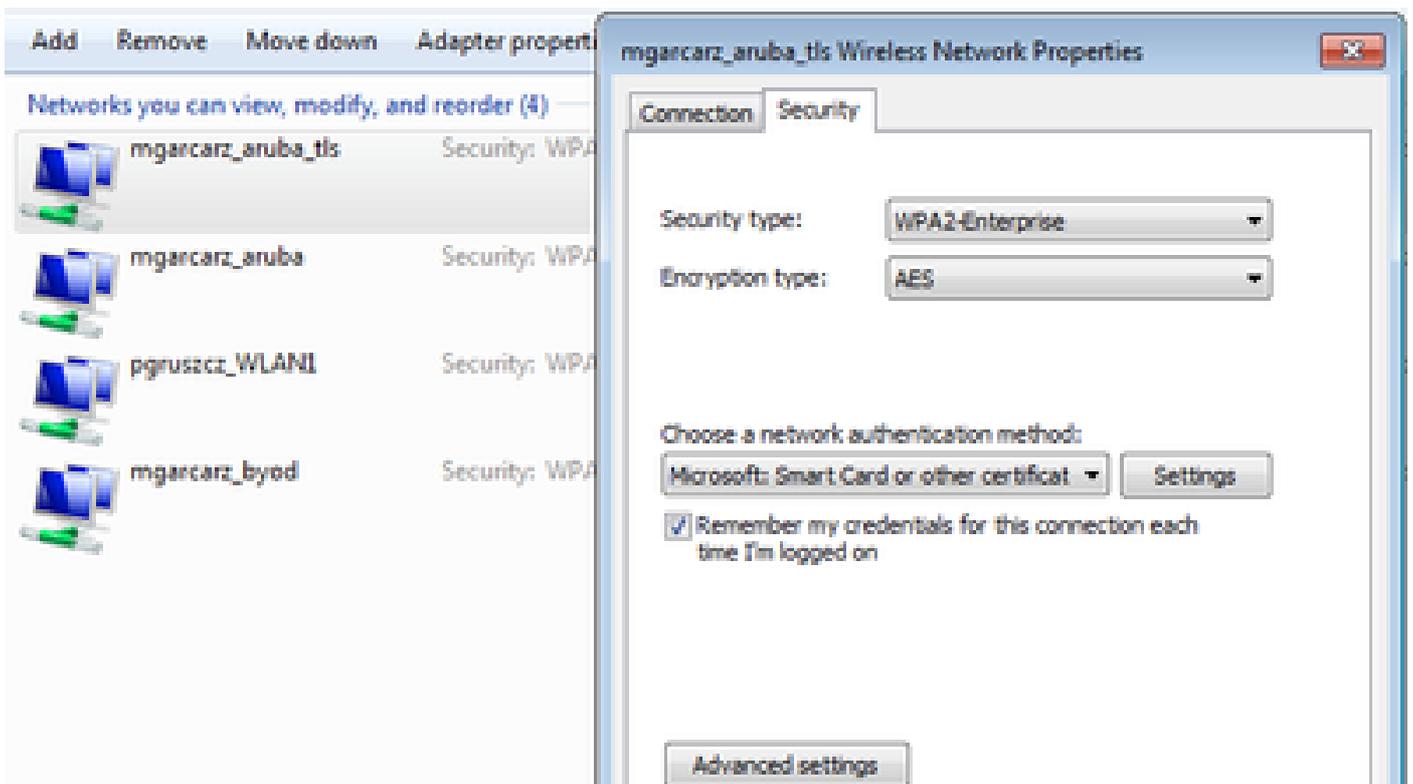
Además, la vista de identidad del terminal puede confirmar que el terminal tiene el indicador BYOD Registered establecido en true, como se muestra en la imagen.



En el PC con Windows, el nuevo perfil inalámbrico se ha creado automáticamente como se prefiere (y se ha configurado para EAP-TLS) y como se muestra.

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

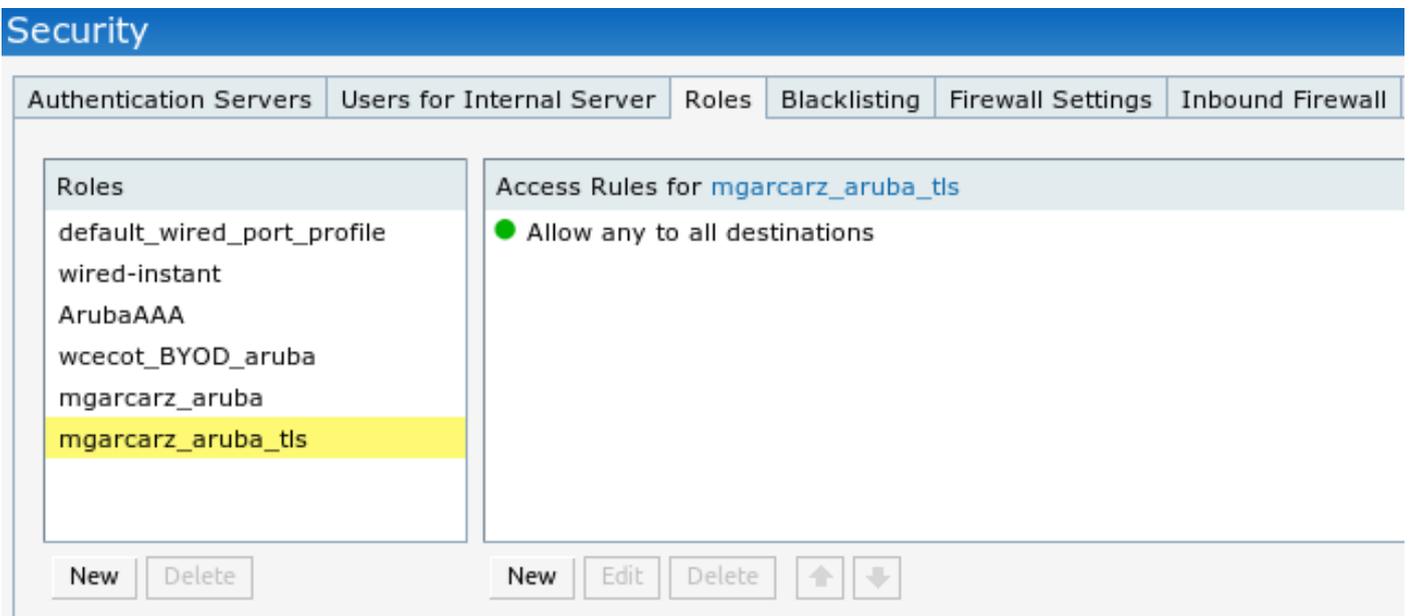
Windows tries to connect to these networks in the order listed below.



En ese momento, Aruba confirma que el usuario está conectado al SSID final.



La función que se crea automáticamente y se denomina igual que Red proporciona acceso completo a la red.



## Otros flujos y soporte de CoA

### CWA con CoA

Aunque en el flujo de BYOD no hay mensajes de CoA, el flujo de CWA con el portal de invitados registrados automáticamente se muestra aquí:

Las reglas de autorización configuradas son las que se muestran en la imagen.

<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

El usuario se conecta al SSID con autenticación MAB y una vez que intenta conectarse a alguna página web, se redirige al portal de invitados registrados automáticamente, donde el invitado puede crear una nueva cuenta o utilizar la actual.



## 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?](#)

Una vez que el invitado se ha conectado correctamente, se envía un mensaje CoA desde ISE al dispositivo de red para cambiar el estado de autorización.



## Sponsored Guest Portal

### Welcome Message

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

You're very close to gaining network access.

Continue

Se puede verificar en Operaciones > Autenticaciones y como se muestra en la imagen.

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

Mensaje CoA en depuraciones de ISE:

<#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

y Disconnect-ACK que proviene de Aruba:

<#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
```

Las capturas de paquetes con CoA, solicitud de desconexión (40) y desconexión-ACK (41) son como se muestra.

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

 Nota: RFC CoA se ha utilizado para la autenticación relacionada con Device Profile Aruba (parámetros predeterminados). Para la autenticación relacionada con el dispositivo de Cisco, habría sido Cisco CoA type reauthenticate.

## Troubleshoot

En esta sección se brinda información que puede utilizar para resolver problemas en su configuración.

### Portal cautivo de Aruba con dirección IP en lugar de FQDN

Si Captive Portal en Aruba se configura con la dirección IP en lugar del FQDN de ISE, PSN NSA falla:

```
<#root>
```

```
Warning - [HTTPConnection]
```

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

```
CN
```

El motivo es la validación estricta de certificados cuando se conecta a ISE. Cuando utiliza una dirección IP para conectarse a ISE (como resultado de una URL de redirección con una dirección IP en lugar de FQDN) y se le presenta un certificado de ISE con el nombre del sujeto = la validación de FQDN falla.



Nota: el navegador web continúa con el portal BYOD (con una advertencia que debe aprobar el usuario).

## Política de acceso incorrecta del portal cautivo de Aruba

De forma predeterminada, Aruba Access-Policy configurado con Captive Portal permite los puertos TCP 80, 443 y 8080.

La NSA no puede conectarse al puerto tcp 8905 para obtener el perfil xml de ISE. Se informa de este error:

```
<#root>
```

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

```
[
```

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

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

```
typeHint=SPWConfig&referrer=Windows&mac_address=C0-4A-00-14-6E-31&spw_version=
```

```
1.0.0.46&session=0a3011ebXbiuDA3yUNoLUvtCRyuPFxkqYJ7TT06fo0Z7G1HXj1M&os=Windows A11]
```

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

```
HTTP response code: 0
```

```
]
```

```
GetProfile - end
```

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

## Número de puerto CoA de Aruba

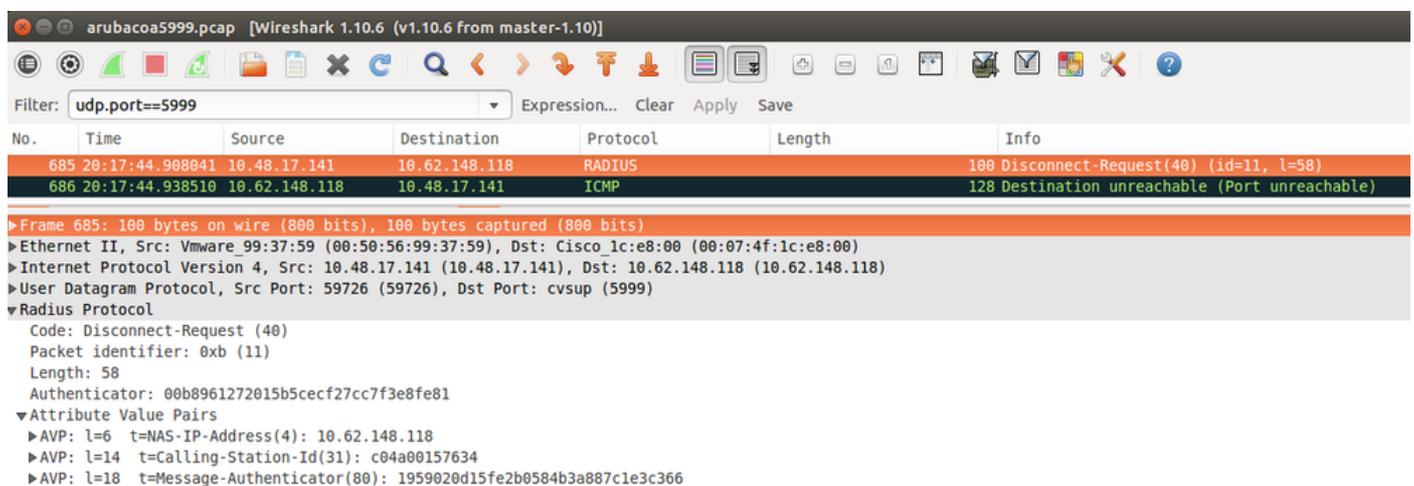
De forma predeterminada, Aruba proporciona el número de puerto para el puerto CoA Air Group CoA 5999. Lamentablemente, Aruba 2004 no respondió a esas solicitudes (como se indica).

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

## 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

La captura de paquetes es como se muestra en la imagen.



La mejor opción para utilizar aquí puede ser el puerto CoA 3977 como se describe en RFC 5176.

## Redirección en algunos dispositivos de Aruba

En Aruba 3600 con v6.3 se observa que la redirección funciona ligeramente diferente que en otros controladores. La captura y explicación de paquetes se puede encontrar aquí.

770	09:29:40.5119116	10.75.94.213	173.194.124.52	HTTP	1373	GET / HTTP/1.1
772	09:29:40.5210658	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/

&aruba1p=6b0512fc-f699-45c6-b5cb-e62b3260e5

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

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

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

## Información Relacionada

- [Guía del administrador de Cisco Identity Services Engine, versión 2.0](#)
- [Perfiles de dispositivos de acceso a la red con Cisco Identity Services Engine](#)
- [Soporte Técnico y Documentación - Cisco Systems](#)

## Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).