

# Configurar a integração de terceiros do ISE 2.0 com o Aruba Wireless

## Contents

---

[Introdução](#)

[Pré-requisitos](#)

[Requisitos](#)

[Componentes Utilizados](#)

[Configurar](#)

[Diagrama de Rede](#)

[Desafios com suporte de terceiros](#)

[SESSÕES](#)

[Redirecionamento de URL](#)

[CoA](#)

[Solução no ISE](#)

[Cisco ISE](#)

[Etapa 1. Adicionar o controlador sem fio Aruba aos dispositivos de rede](#)

[Etapa 2. Configurar perfil de autorização](#)

[Etapa 3. Configurar regras de autorização](#)

[AP Aruba](#)

[Etapa 1. Configuração do portal cativo](#)

[Etapa 2. Configuração de servidor RADIUS](#)

[Etapa 3. Configuração de SSID](#)

[Verificar](#)

[Etapa 1. Conexão com SSID mgarcarz\\_arubawith EAP-PEAP](#)

[Etapa 2. Redirecionamento de tráfego do navegador da Web para BYOD](#)

[Etapa 3. Execução do Assistente de configuração de rede](#)

[Outros fluxos e suporte a CoA](#)

[CWA com CoA](#)

[Troubleshooting](#)

[Aruba Captive Portal com IPAddress em vez de FQDN](#)

[Política de acesso incorreta do Aruba Captive Portal](#)

[Número da porta de CoA da Aruba](#)

[Redirecionamento em alguns dispositivos Aruba](#)

[Informações Relacionadas](#)

---

## Introdução

Este documento descreve como solucionar problemas do recurso de integração de terceiros no Cisco Identity Services Engine (ISE).

---

 Observação: lembre-se de que a Cisco não é responsável pela configuração ou suporte de dispositivos de outros fornecedores.

---

## Pré-requisitos

### Requisitos

A Cisco recomenda que você tenha conhecimento destes tópicos:

- Configuração do Aruba IAP
- O BYOD flui no ISE
- Configuração do ISE para autenticação de senha e certificado

### Componentes Utilizados

Este documento descreve como solucionar problemas do recurso de integração de terceiros no Cisco Identity Services Engine (ISE).

Ele pode ser usado como um guia para integração com outros fornecedores e fluxos. O ISE versão 2.0 oferece suporte à integração de terceiros.

Este é um exemplo de configuração que apresenta como integrar a rede sem fio gerenciada pelo Aruba IAP 2004 com os serviços ISE para BYOD (Bring Your Own Device).

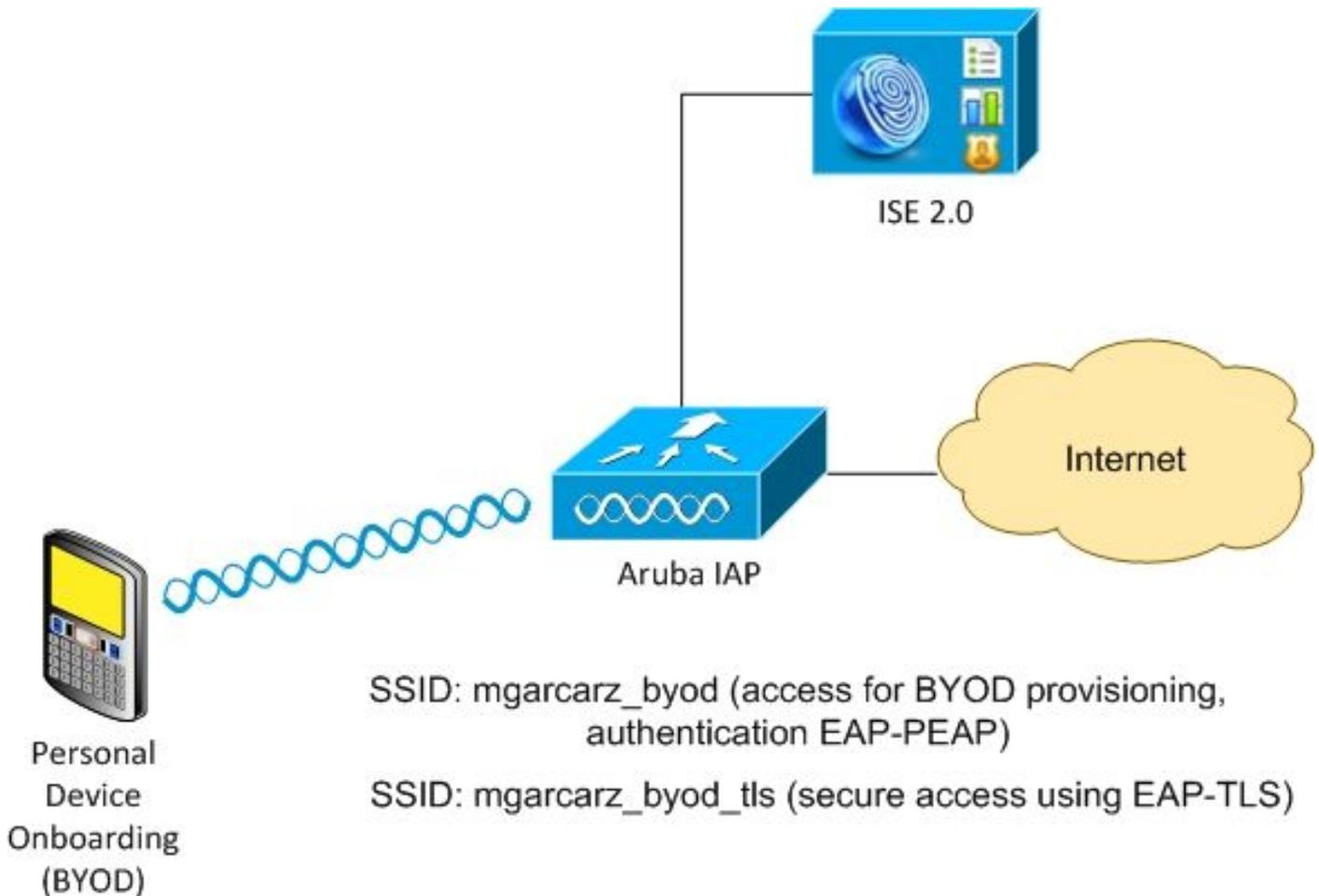
As informações neste documento são baseadas nestas versões de software:

- Software Aruba IAP 204 6.4.2.3
- Cisco ISE, versão 2.0 e posterior

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

## Configurar

### Diagrama de Rede



Há duas redes sem fio gerenciadas pelo AP Aruba.

O primeiro (mgarcarz\_byod) é usado para acesso EAP Protegido por Protocolo de Autenticação Extensível 802.1x (EAP-PEAP).

Após uma autenticação bem-sucedida, o controlador Aruba deve redirecionar o usuário para o portal de BYOD do ISE - fluxo de NSP (Provisionamento de solicitante nativo).

O usuário é redirecionado, o aplicativo Network Setup Assistant (NSA) é executado e o certificado é provisionado e instalado no cliente Windows.

A CA interna do ISE é usada para esse processo (configuração padrão).

A NSA também é responsável pela criação do perfil sem fio para o segundo Service Set Identifier (SSID) gerenciado pela Aruba (mgarcarz\_byod\_tls) - que é usado para autenticação 802.1x Extensible Authentication Protocol-Transport Layer Security (EAP-TLS).

Como resultado, o usuário corporativo pode executar a integração de dispositivos pessoais e obter acesso seguro à rede corporativa.

Este exemplo pode ser facilmente modificado para diferentes tipos de acesso, por exemplo:

- Autenticação da Web Central (CWA) com serviço BYOD
- Autenticação 802.1x com postura e redirecionamento de BYOD
- Geralmente, para autenticação EAP-PEAP, o Active Directory é usado (para manter este

artigo com abreviações, os usuários internos do ISE são usados)

- Normalmente, para o Provisionamento de Certificado é usado o servidor externo do Protocolo de Registro de Certificado Simples (SCEP), geralmente o Serviço de Registro de Dispositivo de Rede (NDES) da Microsoft para manter este artigo curto, é usada a CA interna do ISE.

## Desafios com suporte de terceiros

Há desafios quando você usa fluxos de convidados do ISE (como BYOD, CWA, NSP, Client Provisioning Portal (CPP)) com dispositivos de terceiros.

## SESSÕES

O Cisco Network Access Devices (NAD) usa o Radius cisco-av-pair chamado audit-session-id para informar o servidor de Autenticação, Autorização e Contabilidade (AAA) sobre a ID de sessão.

Esse valor é usado pelo ISE para rastrear as sessões e fornecer os serviços corretos para cada fluxo. Outros fornecedores não oferecem suporte ao par cisco-av.

O ISE precisa confiar nos atributos IETF recebidos na solicitação de acesso e na solicitação de contabilidade.

Depois que você recebe a solicitação de acesso, o ISE cria o ID de sessão sintetizado da Cisco (a partir de ID de estação de chamada, porta NAS, endereço IP NAS e segredo compartilhado). Esse valor tem significado local apenas (não enviado via rede).

Como resultado, espera-se que de cada fluxo (BYOD, CWA, NSP, CPP) anexe atributos corretos, para que o ISE possa recalcular a ID de sessão da Cisco e realizar uma pesquisa para correlacioná-la com a sessão correta e continuar o fluxo.

## Redirecionamento de URL

O ISE usa o par Radius cisco-av chamado url-redirect e url-redirect-acl para informar ao NAD que o tráfego específico deve ser redirecionado.

Outros fornecedores não oferecem suporte ao par cisco-av. Normalmente, esses dispositivos devem ser configurados com URL de redirecionamento estático que aponta para um serviço específico (perfil de autorização) no ISE.

Quando o usuário inicia a sessão HTTP, esses NADs redirecionam para o URL e também anexam argumentos adicionais (como endereço IP ou endereço MAC) para permitir que o ISE identifique uma sessão específica e continue o fluxo.

## CoA

O ISE usa Radius cisco-av-pair chamado subscriber:command, subscriber:reauthenticate-type para indicar quais ações o NAD deve executar para uma sessão específica.

Outros fornecedores não oferecem suporte ao par cisco-av. Normalmente, esses dispositivos usam RFC CoA (3576 ou 5176) e uma das duas mensagens definidas:

- solicitação de desconexão (também chamada de pacote de desconexão) - que é usada para desconectar a sessão (frequentemente para forçar a reconexão)
- Envio de CoA - que é usado para alterar o status da sessão de forma transparente, sem desconexão (por exemplo, sessão VPN e nova ACL aplicada)

O ISE suporta o Cisco CoA com o cisco-av-pair e também o RFC CoA 3576/5176.

## Solução no ISE

Para oferecer suporte a fornecedores terceirizados, o ISE 2.0 introduziu um conceito de perfis de dispositivo de rede que descreve como um fornecedor específico se comporta - como as sessões, o redirecionamento de URL e o CoA são suportados.

Os perfis de autorização são de um tipo específico (Network Device Profile) e, uma vez que a autenticação ocorre, o comportamento do ISE é derivado desse perfil.

Como resultado, os dispositivos de outros fornecedores podem ser gerenciados facilmente pelo ISE. Além disso, a configuração no ISE é flexível e permite ajustar ou criar novos perfis de dispositivo de rede.

Este artigo apresenta o uso do perfil padrão para o dispositivo Aruba.

Mais informações sobre o recurso:

[Perfis de dispositivo de acesso à rede com o Cisco Identity Services Engine](#)

## Cisco ISE

Etapa 1. Adicionar o controlador sem fio Aruba aos dispositivos de rede

Navegue até Administração > Recursos de rede > Dispositivos de rede. Escolha o perfil de dispositivo correto para o fornecedor selecionado, neste caso: ArubaWireless. Certifique-se de configurar Shared Secret e CoA port como mostrado nas imagens.

## 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

Caso não haja nenhum perfil disponível para o fornecedor desejado, ele pode ser configurado em Administração > Recursos de rede > Perfis de dispositivo de rede.

Etapa 2. Configurar perfil de autorização

Navegue até Policy > Policy Elements > Results > Authorization > Authorization Profiles e escolha o mesmo Network Device Profile da Etapa 1. ArubaWireless. O perfil configurado é Aruba-redirect-BYOD com o BYOD Portal e como mostrado nas imagens.

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

Parte ausente da configuração de Redirecionamento da Web, onde o link estático para o Perfil de Autorização é gerado. Embora o Aruba não suporte redirecionamento dinâmico para o portal do convidado, há um link atribuído a cada perfil de autorização, que é então configurado no Aruba e como mostrado na imagem.

#### 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>**

### Etapa 3. Configurar regras de autorização

Navegue para Política > Regras de autorização e a configuração é como mostrado na imagem.

✓	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

Primeiro, o usuário se conecta ao SSID mgarcarz\_aruba e o ISE retorna o perfil de autorização Aruba-redirect-BYOD, que redireciona o cliente para o portal BYOD padrão. Após a conclusão do processo de BYOD, o cliente se conecta com EAP-TLS e o acesso total à rede é concedido.

Nas versões mais recentes do ISE, a mesma política pode ser semelhante a esta:

Status	Policy Set Name	Description	Conditions	Results	Profiles	Security Groups	Hits	Actions																																
✓	Aruba		Aruba:Aruba-Essid-Name EQUALS mgarcarz_aruba		Default Network Access		0																																	
<p>Authentication Policy (1)</p> <p>Authorization Policy - Local Exceptions</p> <p>Authorization Policy - Global Exceptions</p> <p>Authorization Policy (3)</p> <table border="1"> <thead> <tr> <th>Status</th> <th>Rule Name</th> <th>Conditions</th> <th>Results</th> <th>Profiles</th> <th>Security Groups</th> <th>Hits</th> <th>Actions</th> </tr> </thead> <tbody> <tr> <td>✓</td> <td>Authorized</td> <td>AND example.com:ExternalGroups EQUALS example.com:BuiltIn/Administrators EndPoints:BYODRegistration EQUALS Yes Network Access:EapAuthentication EQUALS EAP-TLS</td> <td>PermitAccess</td> <td></td> <td>Select from list</td> <td>0</td> <td></td> </tr> <tr> <td>✓</td> <td>Redirect</td> <td>Aruba:Aruba-Essid-Name EQUALS mgarcarz_aruba</td> <td>Aruba_Redirect_BYOD</td> <td></td> <td>Select from list</td> <td>0</td> <td></td> </tr> <tr> <td>✓</td> <td>Default</td> <td></td> <td>DenyAccess</td> <td></td> <td>Select from list</td> <td>0</td> <td></td> </tr> </tbody> </table>									Status	Rule Name	Conditions	Results	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	
Status	Rule Name	Conditions	Results	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																																		

## AP Aruba

### Etapa 1. Configuração do portal cativo

Para configurar o Captive Portal no Aruba 204, navegue para Security > External Captive Portal e adicione um novo. Insira essas informações para obter a configuração apropriada e conforme mostrado na imagem.

- Tipo: Autenticação Radius
- IP ou nome do host: servidor ISE
- URL: link criado no ISE na configuração do perfil de autorização; é específico para um perfil de autorização específico e pode ser encontrado aqui na configuração do redirecionamento da Web

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=10ImawmkIleZQhapEvIXPAoELx**

- Porta: número da porta na qual o portal selecionado está hospedado no ISE (por padrão: 8443), conforme mostrado na imagem.

mgarcarz\_ise20

---

Type:

IP or hostname:

URL:

Port:

Use https:

Captive Portal failure:

Automatic URL Whitelisting:

Redirect URL:  (optional)

---

## Etapa 2. Configuração de servidor RADIUS

Navegue até Segurança > Servidores de autenticação para garantir que a porta de CoA seja a mesma configurada no ISE, como mostrado na imagem.

Por padrão, no Aruba 204, é definido como 5999, no entanto, não está em conformidade com o RFC 5176 e também não funciona com o 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"/>	

Observação: no Aruba versão 6.5 e mais recente, marque também a caixa de seleção "Captive Portal".

## Etapa 3. Configuração de SSID

- A guia Segurança é como mostrado na imagem.

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:

- Guia Acesso: selecione Regra de acesso baseada em rede para configurar o portal cativo no SSID.

Use o portal cativo configurado na Etapa 1. Clique em Novo, escolha Tipo de regra: Portal cativo, Tipo de página de abertura: Externo, conforme mostrado na imagem.

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

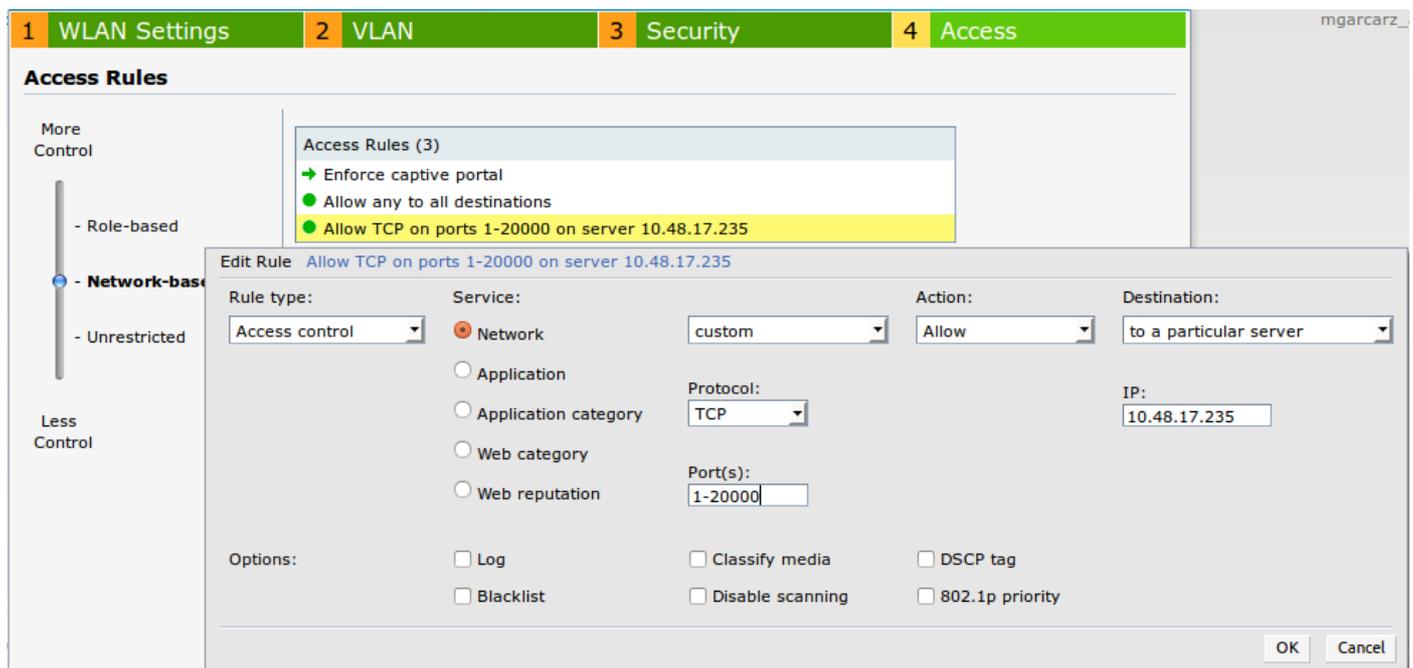
Rule type: Captive portal

Splash page type: External

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

Além disso, permitir todo o tráfego para o servidor ISE (portas TCP no intervalo de 1 a 20000),

enquanto a regra configurada por padrão no Aruba: Permitir qualquer um para todos os destinos parece não estar funcionando corretamente como mostrado na imagem.



## Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

Etapa 1. Conexão ao SSID mgarcarz\_aruba com EAP-PEAP

O primeiro log de autenticação no ISE é exibido. A política de autenticação padrão foi usada, o perfil de autorização Aruba-redirect-BYOD foi retornado conforme mostrado na imagem.

The image shows the Cisco Identity Services Engine (ISE) interface. At the top, there are tabs for 'RADIUS Livelog', 'TACACS Livelog', 'Reports', 'Troubleshoot', and 'Adaptive Network Control'. Below the tabs, there are four summary cards: 'Misconfigured Supplicants' (1), 'Misconfigured Network Devices' (0), 'RADIUS Drops' (12), and 'Client Stopped Respond' (0). Below the summary cards, there is a table of authentication logs. The table has columns for Time, Status, Det..., R., Identity, Endpoint ID, Authentication Policy, Authorization Policy, Authorization Profiles, Network Device, and Event. The logs show three entries: 1. Time: 2015-10-29 22:23:37..., Status: All, Identity: 0 cisco, Endpoint ID: C0:4A:00:14:6E:31, Authentication Policy: Default >> Dot1X >> EAP-TLS, Authorization Policy: Default >> Basic\_Authenticated..., Authorization Profiles: PermitAccess, Network Device: aruba, Event: Session State is Started. 2. Time: 2015-10-29 22:23:37..., Status: All, Identity: cisco, Endpoint ID: C0:4A:00:14:6E:31, Authentication Policy: Default >> Dot1X >> EAP-TLS, Authorization Policy: Default >> Basic\_Authenticated..., Authorization Profiles: PermitAccess, Network Device: aruba, Event: Authentication succeeded. 3. Time: 2015-10-29 22:19:09..., Status: All, Identity: cisco, Endpoint ID: C0:4A:00:14:6E:31, Authentication Policy: Default >> Dot1X >> Default, Authorization Policy: Default >> ArubaRedirect, Authorization Profiles: Aruba-redirect-BYOD, Network Device: aruba, Event: Authentication succeeded.

O ISE retorna a mensagem Radius Access-Accept com EAP Success. Observe que nenhum atributo adicional é retornado (nenhum url-redirect de par Cisco av ou url-redirect-acl) como mostrado na imagem.

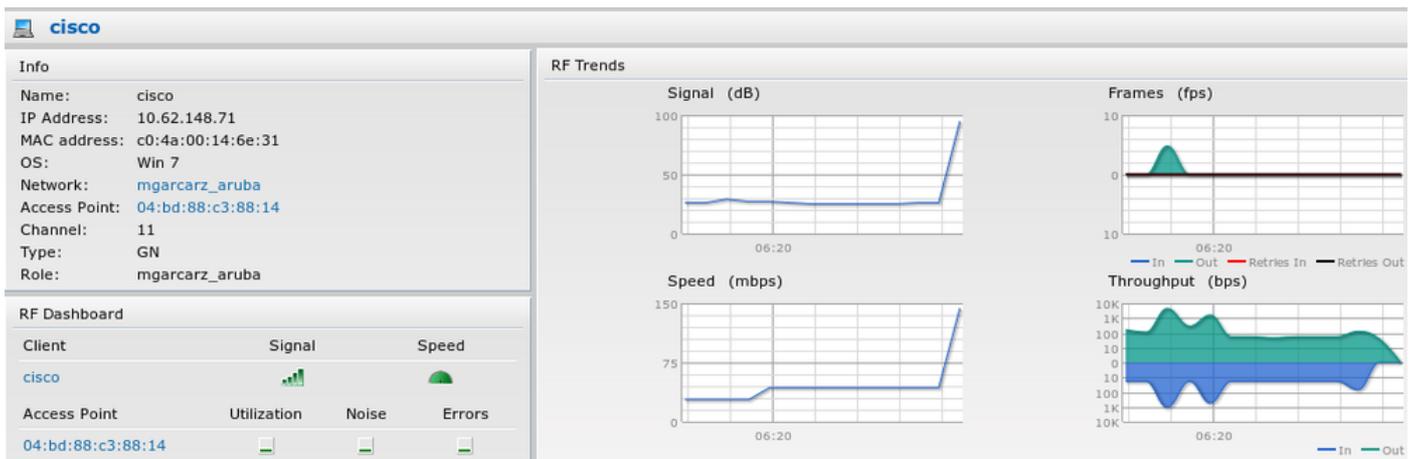
No.	Source	Destination	Protocol	Length	Info	User-Name	Acct-Session-Id
133	10.62.148.118	10.48.17.235	RADIUS	681	Access-Request(1) (id=102, l=639)	cisco	
134	10.48.17.235	10.62.148.118	RADIUS	257	Access-Challenge(11) (id=102, l=215)		
135	10.62.148.118	10.48.17.235	RADIUS	349	Access-Request(1) (id=103,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

```

A Aruba relata que a sessão foi estabelecida (a identidade EAP-PEAP é cisco) e a função selecionada é mgarcarz\_aruba, como mostrado na imagem.



Essa função é responsável pelo redirecionamento para o ISE (funcionalidade de portal cativo no Aruba).

Na CLI do Aruba, é possível confirmar qual é o status de autorização atual para essa sessão:

```
<#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

E para verificar a ID de ACL 138 para as permissões atuais:

```
<#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

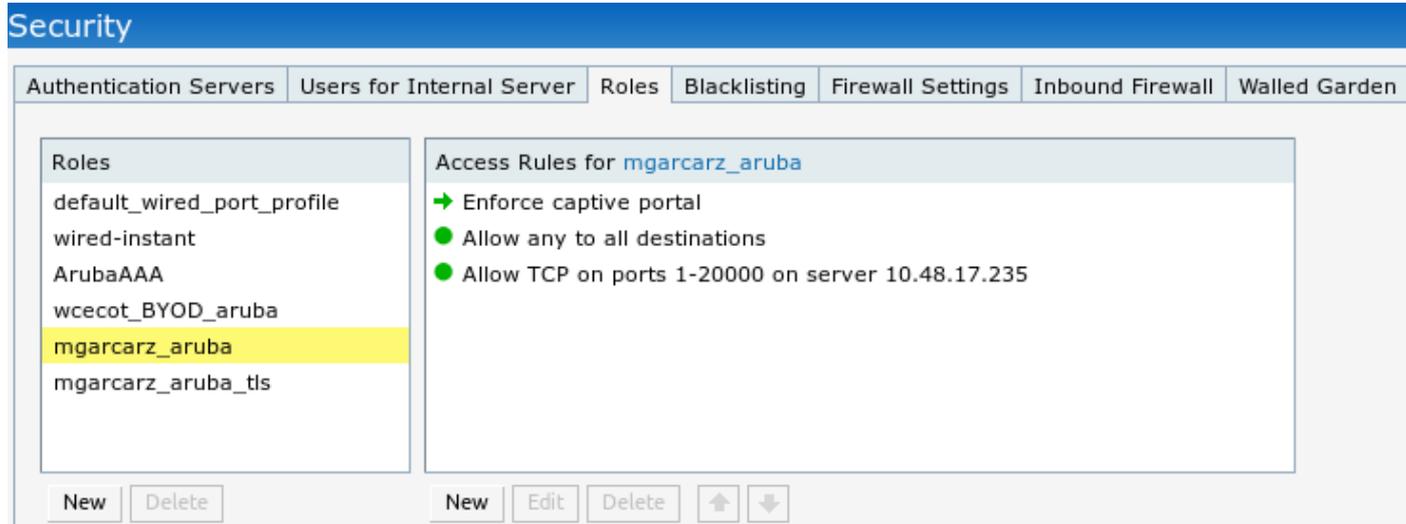
5: any mgarcarz-ise20.example.com 6 0-65535 443-443 Pd4

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
```

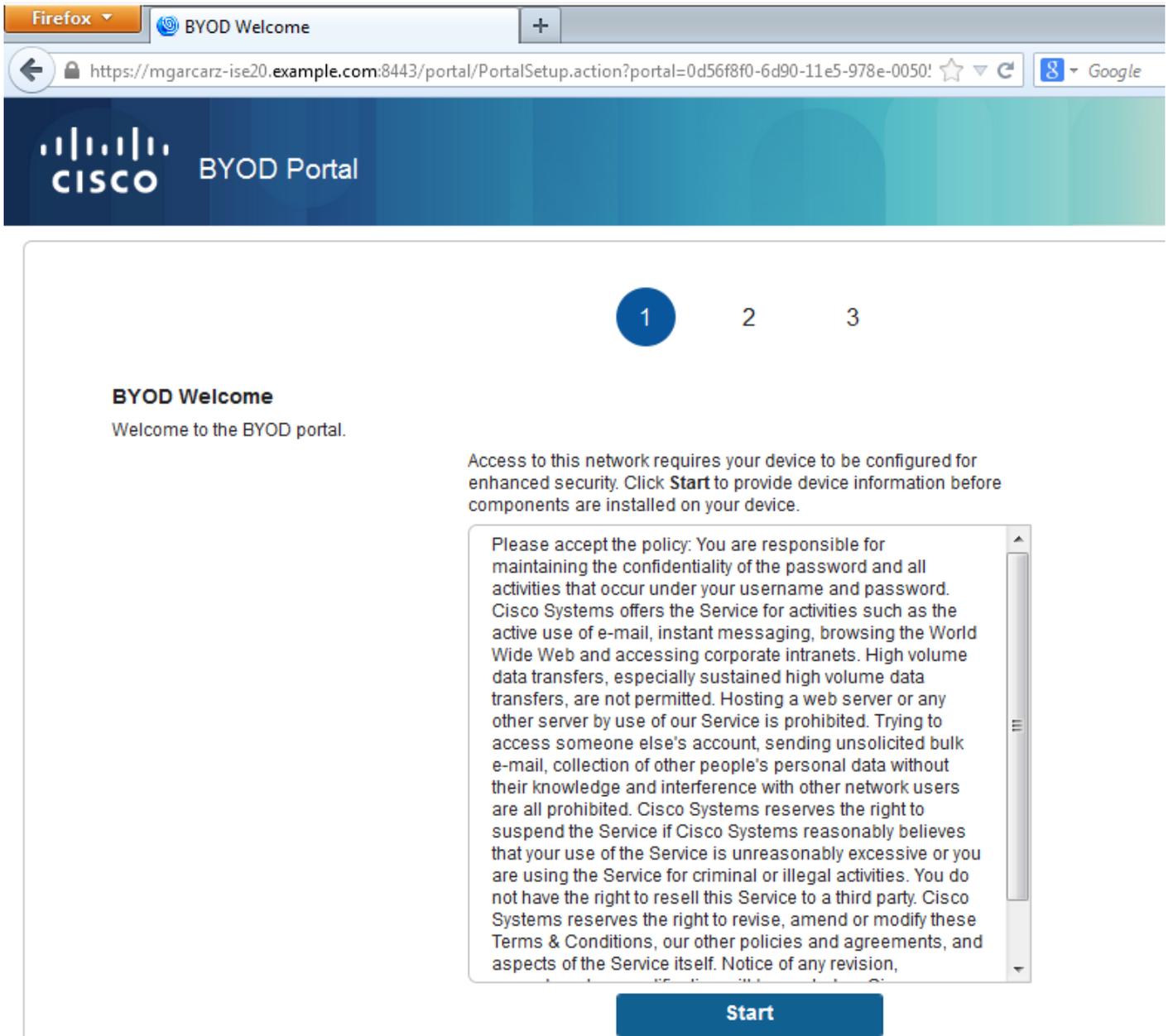
```
<....some output removed for clarity ... >
```

Corresponde ao que foi configurado na GUI para essa função, conforme mostrado na imagem.



## Etapa 2. Redirecionamento de tráfego do navegador da Web para BYOD

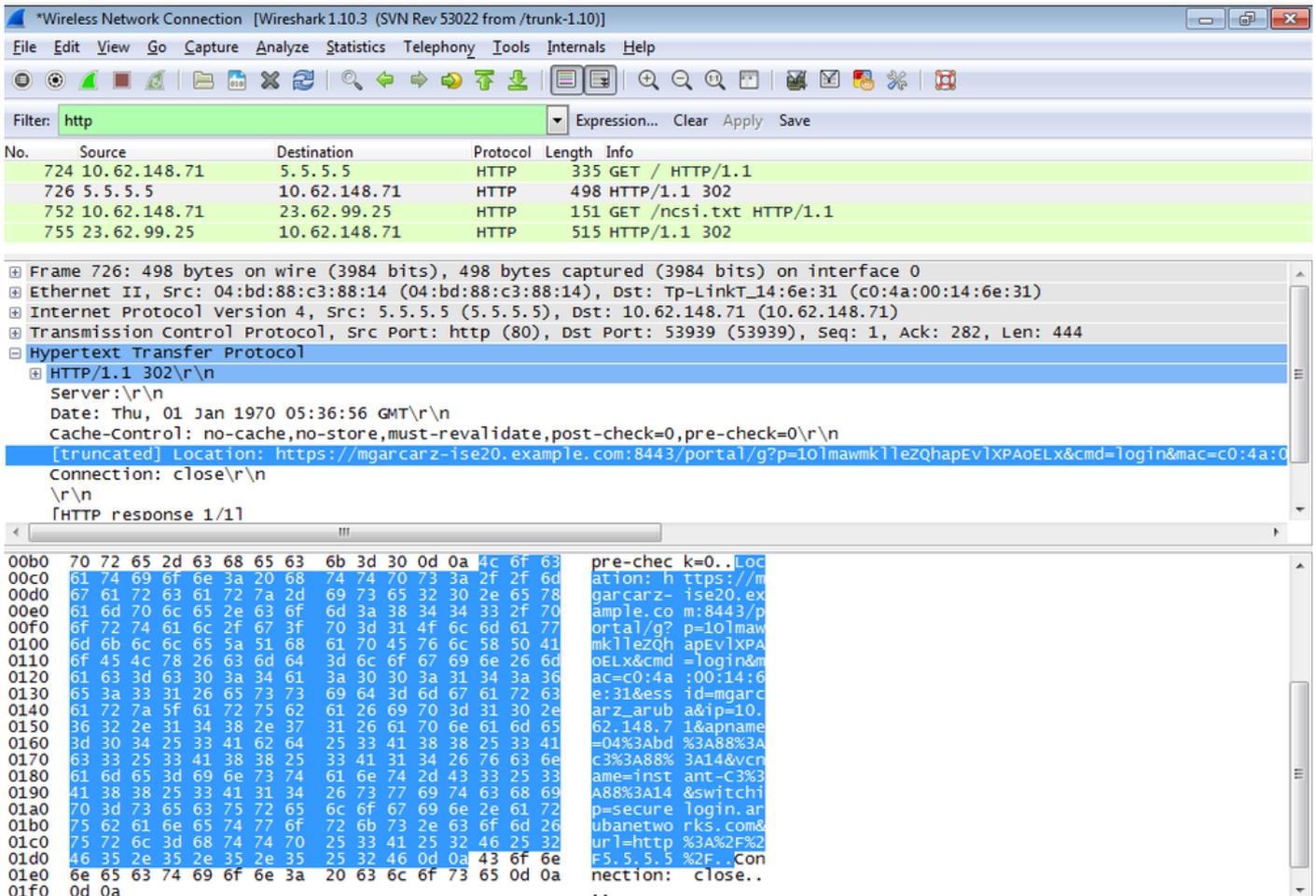
Quando o usuário abre o navegador da Web e digita qualquer endereço, o redirecionamento ocorre como mostrado na imagem.



Observando as capturas de pacotes, confirma-se que Aruba falsifica o destino (5.5.5.5) e retorna o redirecionamento HTTP para o ISE.

Observe que é a mesma URL estática configurada no ISE e copiada para o portal cativo no Aruba, mas, além disso, vários argumentos são adicionados da seguinte forma e como mostrado na imagem:

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



Por causa desses argumentos, o ISE é capaz de recriar a ID de sessão da Cisco, descobrir a sessão correspondente no ISE e continuar com o fluxo de BYOD (ou qualquer outro configurado).

Para dispositivos Cisco, `audit_session_id` seria normalmente usado, mas não é suportado por outros fornecedores.

Para confirmar isso nas depurações do ISE, é possível ver a geração do valor `audit-session-id` (que nunca é enviado pela rede):

```
<#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
```

E depois, correlação disso após o registro do dispositivo no 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
```

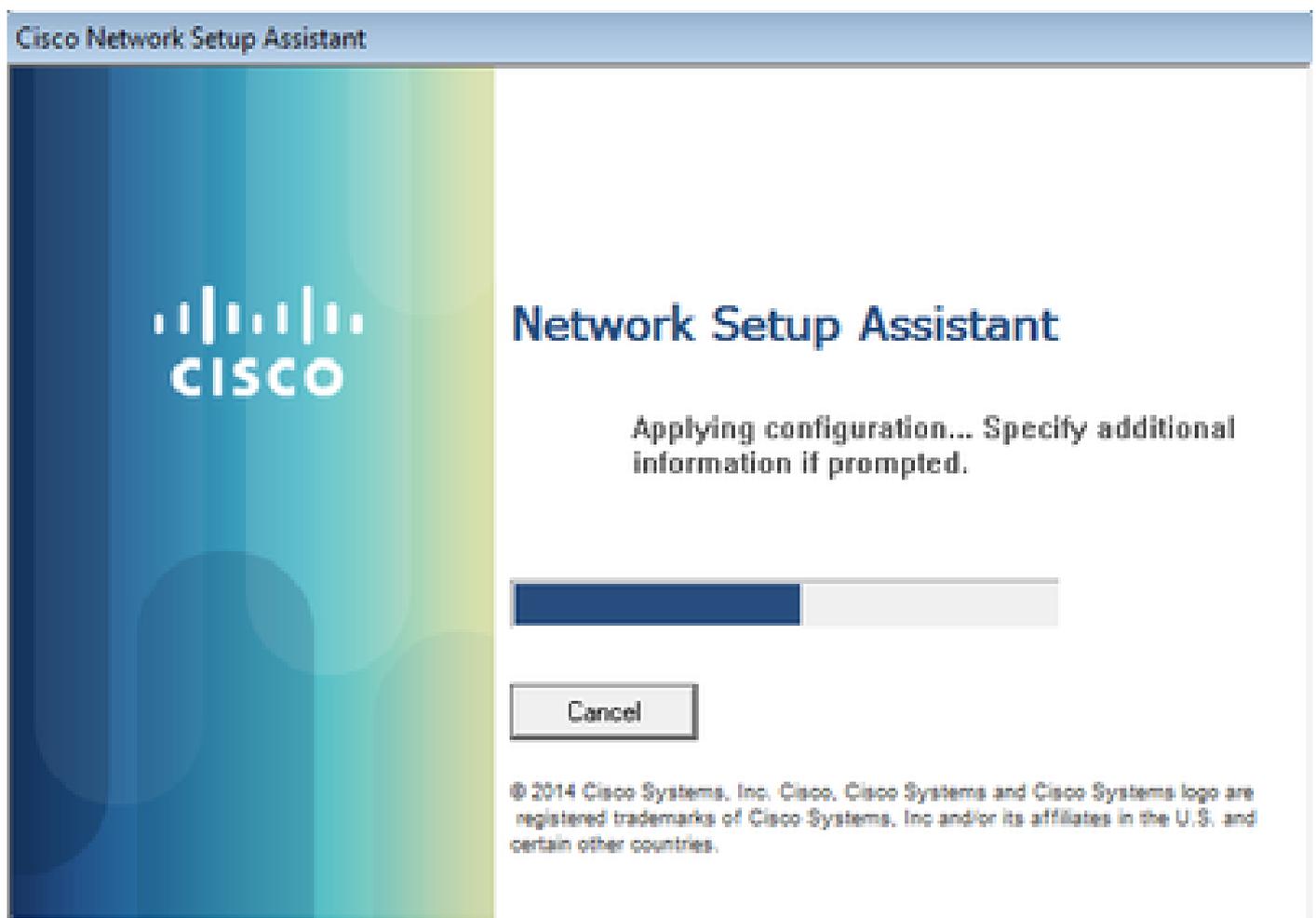
MyDevices: Successfully registered/provisioned the device

(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

Em solicitações subsequentes, o cliente é redirecionado para a página 3 do BYOD, onde a NSA é baixada e executada.

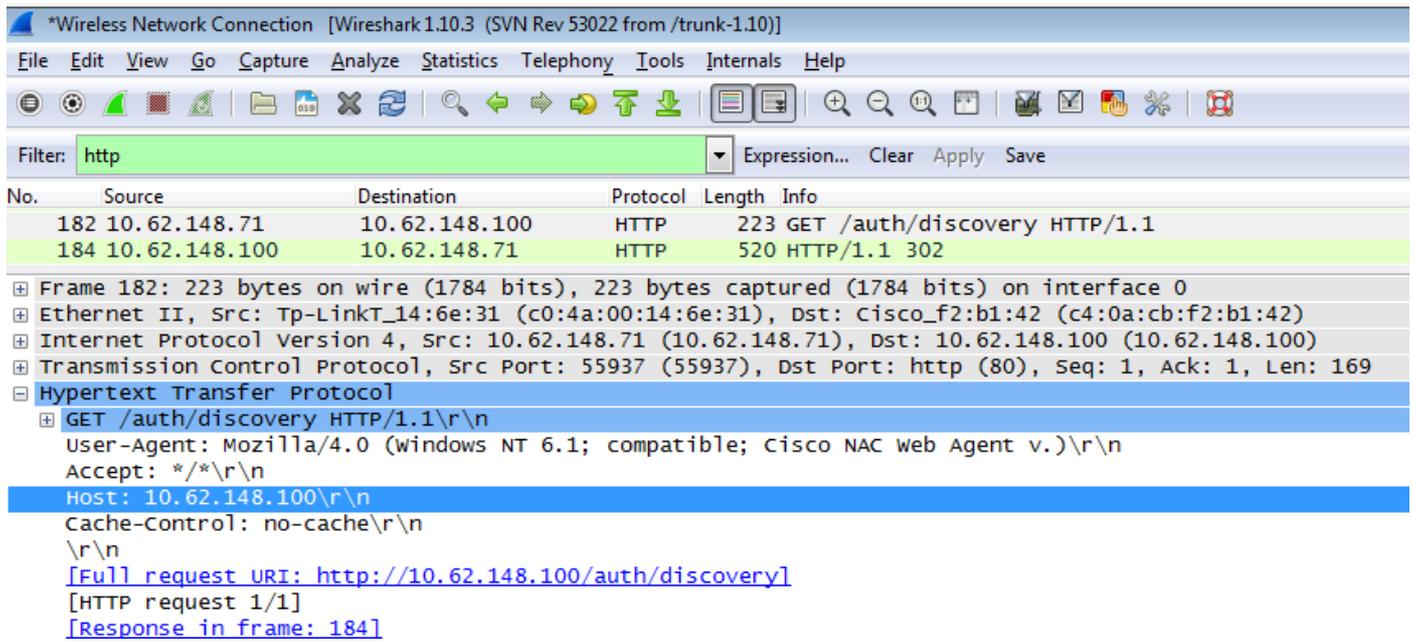
### Etapa 3. Execução do Assistente de configuração de rede



A NSA tem a mesma tarefa que o navegador da Web. Primeiro, ele precisa detectar qual é o endereço IP do ISE. Isso é obtido através do redirecionamento HTTP.

Como dessa vez o usuário não tem a possibilidade de digitar o endereço IP (como no navegador da Web), esse tráfego é gerado automaticamente.

O gateway padrão é usado (também é possível usar enroll.cisco.com) como mostrado na imagem.



A resposta é exatamente igual à do navegador da Web.

Dessa forma, o NSA pode se conectar ao ISE, obter o perfil xml com a configuração, gerar a solicitação SCEP, enviá-la ao ISE, obter o certificado assinado (assinado pela CA interna do ISE), configurar o perfil sem fio e, finalmente, se conectar ao SSID configurado.

Coletar logs do cliente (no Windows, está em %temp%/spwProfile.log). Algumas saídas são omitidas por questões de clareza:

```
<#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: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

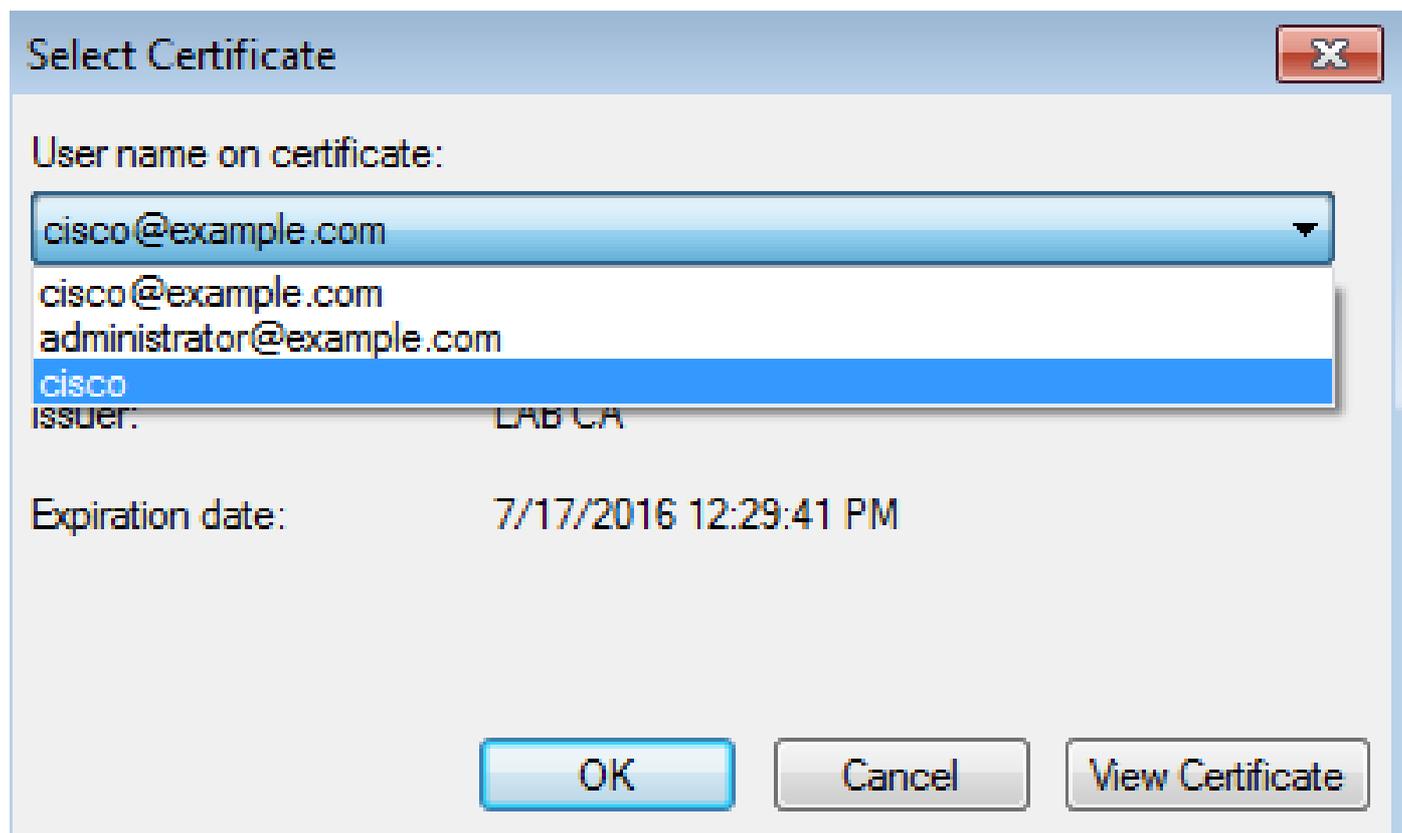
Successfully connected profile: [mgarcarz\_aruba\_tls]

WirelessProfile::SetWirelessProfile. - End

Esses registros são exatamente os mesmos do processo de BYOD com dispositivos da Cisco.

 Observação: Radius CoA não é necessário aqui. É o aplicativo (NSA) que força a reconexão a um SSID recém-configurado.

Nesse estágio, o usuário pode ver que o sistema tenta associar-se a um SSID final. Se você tiver mais de um certificado de usuário, deverá selecionar o correto (como mostrado).



Após uma conexão bem-sucedida, os relatórios de NSA são mostrados na imagem.



## Network Setup Assistant



Your device is now configured for secure access to the 'mgarcarz\_aruba\_tls' network.

Exit

© 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.

Isso pode ser confirmado no ISE - o segundo registro alcança a autenticação EAP-TLS, que corresponde a todas as condições para Basic\_Authenticated\_Access (EAP-TLS, Employee, and BYOD Registered true).

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

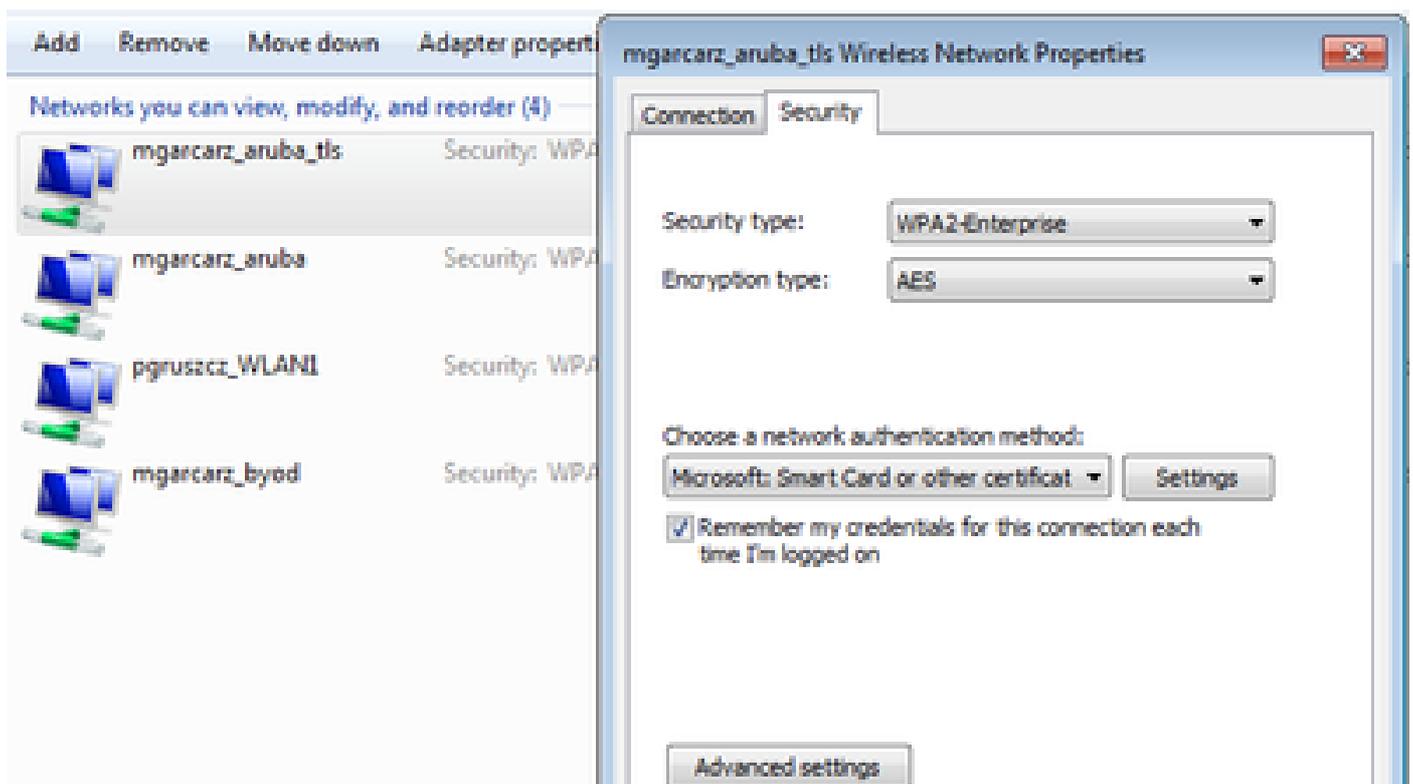
Além disso, a exibição da identidade do endpoint pode confirmar se o endpoint tem o sinalizador BYOD Registered definido como verdadeiro, como mostrado na imagem.



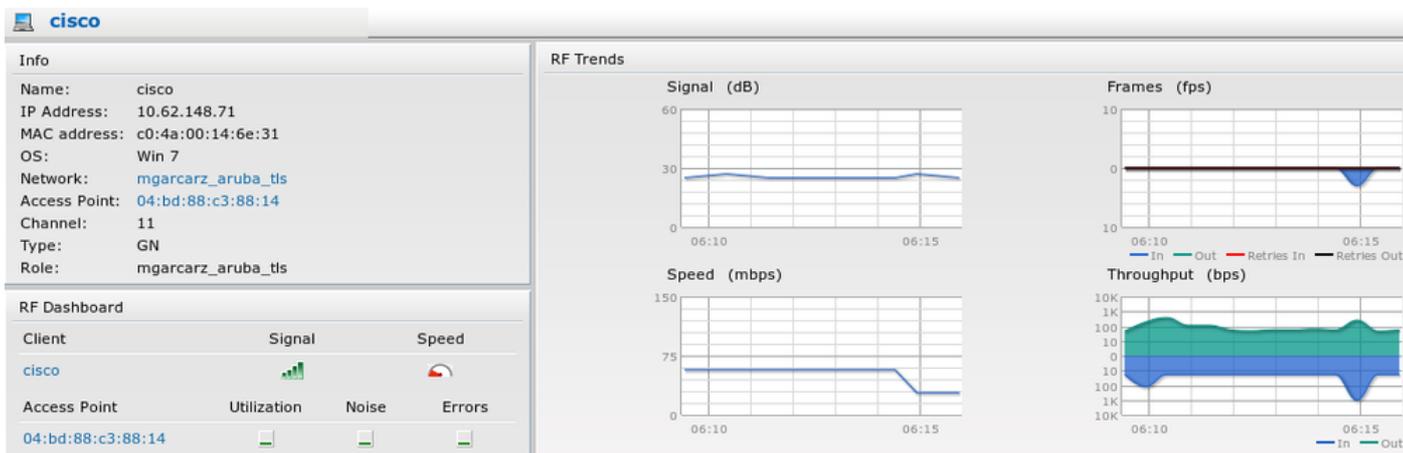
No Windows PC, um novo perfil sem fio foi criado automaticamente como preferencial (e configurado para EAP-TLS) e como mostrado.

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

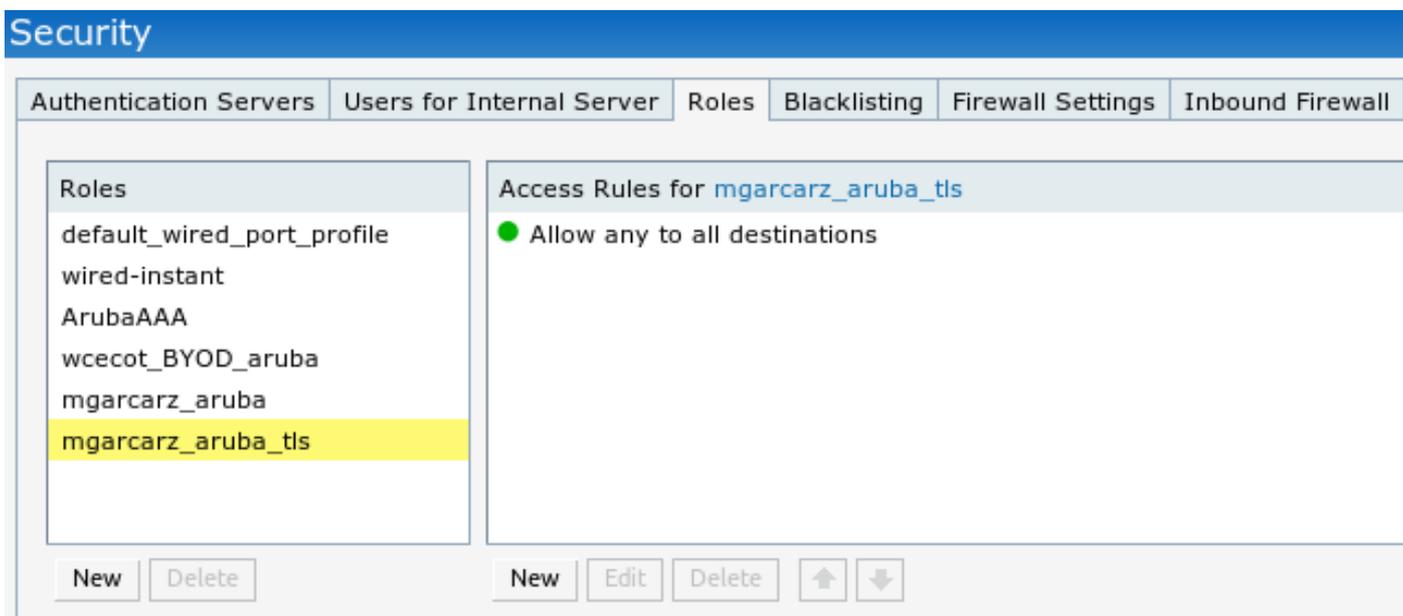
Windows tries to connect to these networks in the order listed below.



Nesse estágio, a Aruba confirma que o usuário está conectado ao SSID final.



A função que é criada automaticamente e nomeada como Rede fornece acesso total à rede.



## Outros fluxos e suporte a CoA

### CWA com CoA

Durante o fluxo de BYOD, não há mensagens de CoA, o fluxo de CWA com o portal de convidados registrados automaticamente é demonstrado aqui:

As regras de autorização configuradas são as mostradas na imagem.

<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

O usuário se conecta ao SSID com autenticação MAB e, uma vez que ele tenta se conectar a alguma página da Web, ocorre o redirecionamento para o Portal de convidado registrado automaticamente, onde o convidado pode criar uma nova conta ou usar a atual.



## 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?](#)

Depois que o convidado é conectado com êxito, a mensagem de CoA é enviada do ISE para o dispositivo de rede para alterar o estado de autorização.



## Sponsored Guest Portal

### Welcome Message

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

You're very close to gaining network access.

Continue

Ele pode ser verificado em Operations > Authentication e como mostrado na imagem.

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

Mensagem de CoA em depurações do 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

e Disconnect-ACK que vem da 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,
```

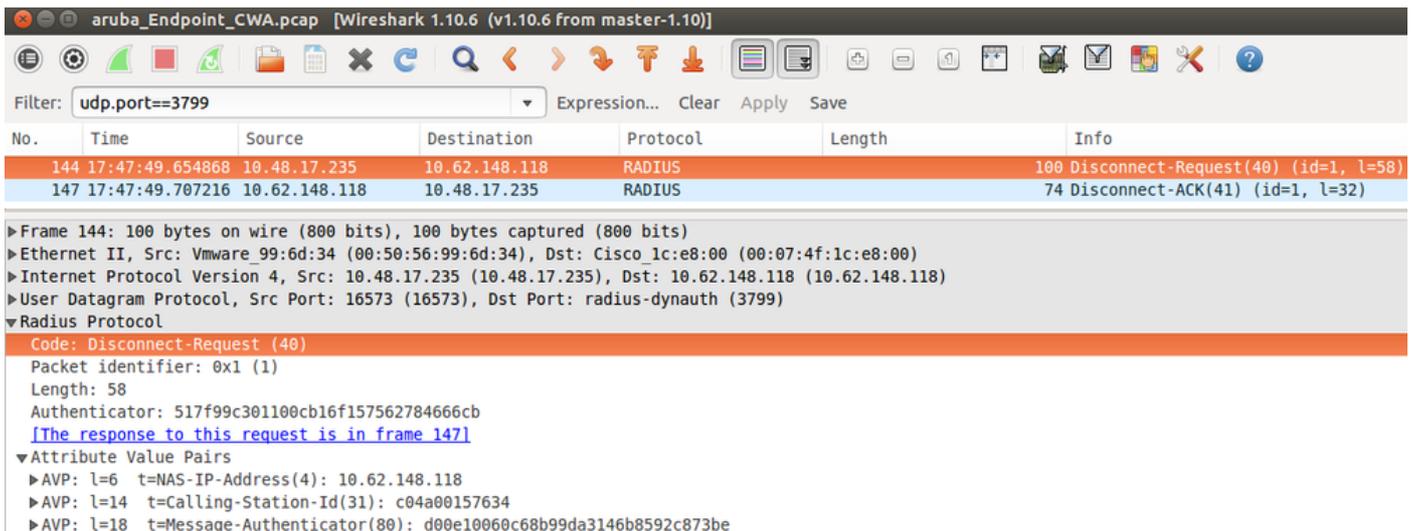
CallingStationID=c04a00157634

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

Packet type 41(DisconnectACK).

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

Capturas de pacotes com CoA Disconnect-Request (40) e Disconnect-ACK (41) é como mostrado.



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)

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

 Observação: o RFC CoA foi usado para autenticação relacionada ao perfil de dispositivo Aruba (configurações padrão). Para autenticação relacionada ao dispositivo Cisco, teria sido o tipo de CoA da Cisco reautenticar.

## Troubleshooting

Esta seção disponibiliza informações para a solução de problemas de configuração.

### Aruba Captive Portal com endereço IP em vez de FQDN

Se o portal cativo no Aruba estiver configurado com o endereço IP em vez do FQDN do ISE, o PSN NSA falhará:

```
<#root>
```

```
Warning - [HTTPConnection]
```

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

```
CN
```

O motivo disso é a validação de certificado estrita quando você se conecta ao ISE. Quando você usa um endereço IP para se conectar ao ISE (como resultado do URL de redirecionamento com endereço IP em vez de FQDN) e é apresentado um certificado ISE com Nome do assunto = Falha na validação do FQDN.

 Observação: o navegador da Web continua com o portal BYOD (com aviso que precisa ser aprovado pelo usuário).

## Política de acesso incorreta do Aruba Captive Portal

Por padrão, a Aruba Access-Policy configurada com o Captive Portal permite as portas tcp 80, 443 e 8080.

O NSA não pode se conectar à porta tcp 8905 para obter o perfil xml do ISE. Este erro é relatado:

```
<#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 da porta de CoA da Aruba

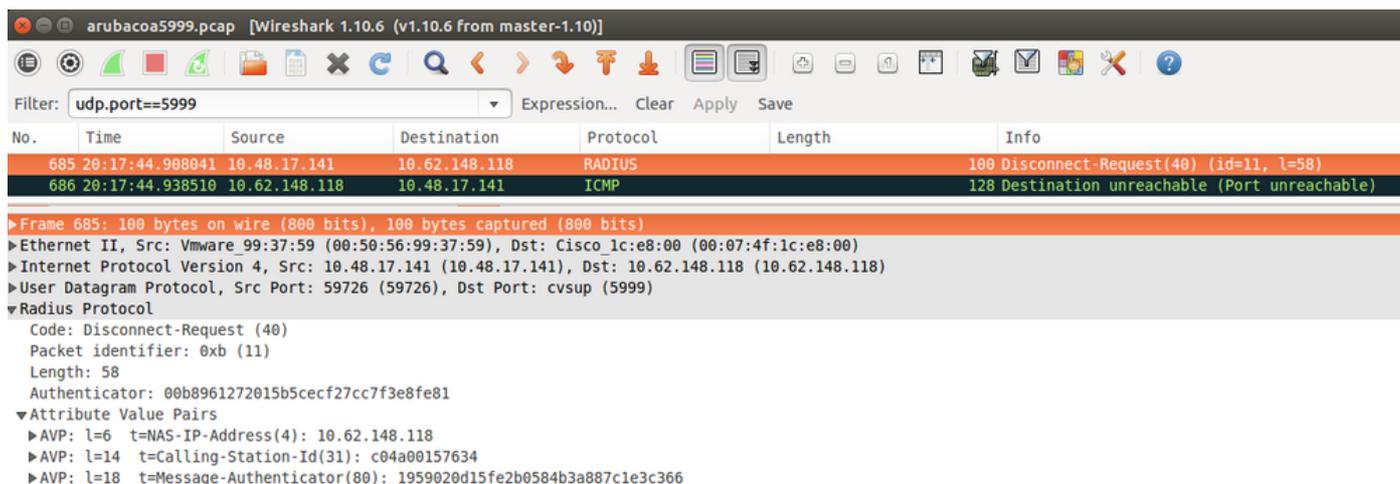
Por padrão, a Aruba fornece o número da porta para a porta 5999 do CoA Air Group CoA. Infelizmente, o Aruba 204 não respondeu a tais solicitações (como mostrado).

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

A captura de pacotes é como mostrado na imagem.



A melhor opção a ser usada aqui pode ser a porta 3977 de CoA, conforme descrito no RFC 5176.

## Redirecionamento em alguns dispositivos Aruba

No Aruba 3600 com v6.3, percebe-se que o redirecionamento funciona ligeiramente diferente de outros controladores. Captura e explicação de pacotes podem ser encontradas aqui.

No.	Time	Source	Destination	Protocol	Length	Info
776	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

## Informações Relacionadas

- [Guia do Administrador do Cisco Identity Services Engine, Versão 2.0](#)
- [Perfis de dispositivo de acesso à rede com o Cisco Identity Services Engine](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)

## Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.