

Configurazione dell'integrazione di ISE 2.0 con Aruba Wireless

Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete](#)

[Sfide con il supporto di terze parti](#)

[Sessioni](#)

[Reindirizzamento URL](#)

[CoA](#)

[Soluzione ISE](#)

[Cisco ISE](#)

[Passaggio 1. Aggiunta di Aruba Wireless Controller ai dispositivi di rete](#)

[Passaggio 2. Configura profilo di autorizzazione](#)

[Passaggio 3. Configurazione delle regole di autorizzazione](#)

[Aruba AP](#)

[Passaggio 1. Configurazione Captive Portal](#)

[Passaggio 2. Configurazione server Radius](#)

[Passaggio 3. Configurazione SSID](#)

[Verifica](#)

[Passaggio 1. Connessione a SSID mgarcarz_arubacon EAP-PEAP](#)

[Passaggio 2. Web Browser Traffic Redirection per BYOD](#)

[Passaggio 3. Esecuzione dell'Assistente installazione rete](#)

[Altri flussi e supporto CoA](#)

[CWA con CoA](#)

[Risoluzione dei problemi](#)

[Aruba Captive Portal con IPAddress anziché FQDN](#)

[Criteri di accesso non corretti per Aruba Captive Portal](#)

[Numero porta CoA Aruba](#)

[Reindirizzamento su alcuni dispositivi Aruba](#)

[Informazioni correlate](#)

Introduzione

Questo documento descrive come risolvere i problemi relativi alla funzionalità di integrazione con terze parti su Cisco Identity Services Engine (ISE).



Nota: Cisco non è responsabile della configurazione o del supporto di dispositivi di altri fornitori.

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Configurazione di Aruba IAP
- Il BYOD fluisce su ISE
- Configurazione ISE per l'autenticazione di password e certificati

Componenti usati

Questo documento descrive come risolvere i problemi relativi alla funzionalità di integrazione con terze parti su Cisco Identity Services Engine (ISE).

Può essere utilizzato come guida per l'integrazione con altri fornitori e flussi. ISE versione 2.0 supporta l'integrazione con soluzioni di terze parti.

Questo è un esempio di configurazione che illustra come integrare una rete wireless gestita da Aruba IAP 204 con ISE per i servizi BYOD (Bring Your Own Device).

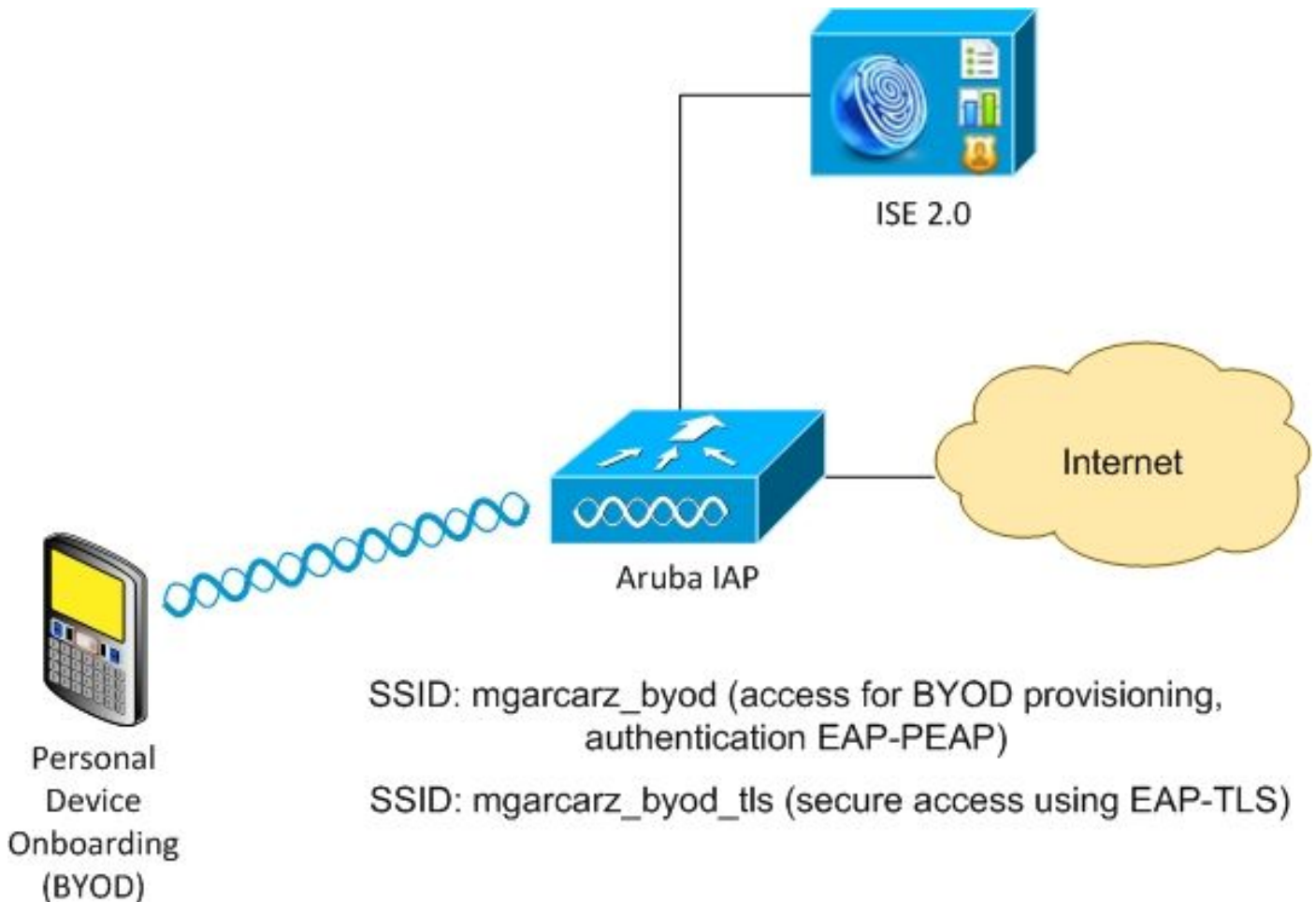
Le informazioni fornite in questo documento si basano sulle seguenti versioni software:

- Software Aruba IAP 204 6.4.2.3
- Cisco ISE versione 2.0 e successive

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Configurazione

Esempio di rete



Ci sono due reti wireless gestite da Aruba AP.

Il primo (mgarcarz_byod) viene usato per l'accesso 802.1x EAP (Extensible Authentication Protocol-Protected EAP).

Dopo un'autenticazione riuscita, il controller Aruba deve reindirizzare l'utente al flusso NSP (Native Supplicant Provisioning) del portale BYOD ISE.

L'utente viene reindirizzato, viene eseguita l'applicazione NSA (Network Setup Assistant) e il certificato viene fornito e installato nel client Windows.

Per questo processo viene utilizzata la CA interna ISE (configurazione predefinita).

L'NSA è anche responsabile della creazione del profilo wireless per il secondo SSID (Service Set Identifier) gestito da Aruba (mgarcarz_byod_tls), utilizzato per l'autenticazione 802.1x Extensible Authentication Protocol-Transport Layer Security (EAP-TLS).

Di conseguenza, l'utente aziendale è in grado di eseguire l'onboarding dei dispositivi personali e ottenere un accesso sicuro alla rete aziendale.

Questo esempio può essere facilmente modificato per diversi tipi di accesso, ad esempio:

- Autenticazione Web centrale (CWA) con servizio BYOD
- Autenticazione 802.1x con reindirizzamento Posture e BYOD
- In genere, per l'autenticazione EAP-PEAP viene utilizzato Active Directory (per evitare che in

questo articolo vengano utilizzati utenti ISE interni)

- In genere, per il provisioning dei certificati viene utilizzato un server SCEP (Simple Certificate Enrollment Protocol) esterno, in genere il servizio NDES (Microsoft Network Device Enrollment Service), in modo da ridurre la lunghezza dell'articolo, viene utilizzato un'autorità di certificazione ISE interna.

Sfide con il supporto di terze parti

L'utilizzo di flussi ISE Guest (come BYOD, CWA, NSP, Client Provisioning Portal (CPP)) con dispositivi di terze parti comporta alcune difficoltà.

Sessioni

NAD (Network Access Devices) di Cisco utilizza Radius cisco-av-pair chiamata audit-session-id per informare il server di autenticazione, autorizzazione e accounting (AAA) sull'ID sessione.

Questo valore viene usato da ISE per tenere traccia delle sessioni e fornire i servizi corretti per ogni flusso. Altri fornitori non supportano la coppia cisco-av.

ISE deve basarsi sugli attributi IETF ricevuti in Access-Request e Accounting Request.

Dopo aver ricevuto Access-Request, ISE crea un ID sessione Cisco sintetizzato (da Calling-Station-ID, NAS-Port, NAS-IP-Address e shared secret). Questo valore ha solo un significato locale (non viene inviato tramite la rete).

Di conseguenza, è previsto che ogni flusso (BYOD, CWA, NSP, CPP) associ gli attributi corretti, quindi ISE è in grado di ricalcolare l'ID sessione Cisco e di eseguire una ricerca per correlarlo alla sessione corretta e continuare il flusso.

Reindirizzamento URL

ISE utilizza Radius cisco-av-pair chiamato url-redirect e url-redirect-acl per informare NAD che il traffico specifico deve essere reindirizzato.

Altri fornitori non supportano la coppia cisco-av. Di norma, quindi, i dispositivi devono essere configurati con un URL di reindirizzamento statico che punti a un servizio specifico (Profilo di autorizzazione) sull'ISE.

Una volta avviata la sessione HTTP, gli NAD reindirizzano all'URL e aggiungono altri argomenti (ad esempio l'indirizzo IP o l'indirizzo MAC) per consentire all'ISE di identificare una sessione specifica e continuare il flusso.

CoA

ISE utilizza Radius cisco-av-pair chiamato subscriber:command, subscriber:reauthenticate-type per indicare le azioni da eseguire e da eseguire per una sessione specifica.

Altri fornitori non supportano la coppia cisco-av. Pertanto, in genere questi dispositivi utilizzano la

RFC CoA (3576 o 5176) e uno dei due messaggi definiti:

- richiesta disconnect (chiamata anche pacchetto di disconnessione) - viene utilizzata per disconnettere la sessione (molto spesso per forzare la riconnessione)
- Push CoA: utilizzato per modificare lo stato della sessione in modo trasparente senza disconnessione (ad esempio, sessione VPN e nuovo ACL applicato)

ISE supporta sia Cisco CoA con cisco-av-pair sia la RFC CoA 3576/5176.

Soluzione ISE

Per supportare i fornitori terzi, ISE 2.0 ha introdotto un concetto di profili di dispositivi di rete che descrive il comportamento di un fornitore specifico - il supporto di Sessioni, Reindirizzamento URL e CoA.

I profili di autorizzazione sono di tipo specifico (Profilo dispositivo di rete) e una volta eseguita l'autenticazione, il comportamento ISE viene derivato da tale profilo.

Di conseguenza, i dispositivi di altri fornitori possono essere gestiti facilmente da ISE. Anche la configurazione su ISE è flessibile e consente di regolare o creare nuovi profili per dispositivi di rete.

In questo articolo viene illustrato l'utilizzo del profilo predefinito per il dispositivo Aruba.

Ulteriori informazioni sulla funzione:

[Profili dei dispositivi di accesso alla rete con Cisco Identity Services Engine](#)

Cisco ISE

Passaggio 1. Aggiunta di Aruba Wireless Controller ai dispositivi di rete



Selezionare Amministrazione > Risorse di rete > Dispositivi di rete. Selezionare il profilo di dispositivo corretto per il fornitore selezionato, in questo caso ArubaWireless. Assicurarsi di configurare il segreto condiviso e la porta CoA come mostrato nelle immagini.

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

Se non è disponibile alcun profilo per il fornitore desiderato, è possibile configurarlo in Amministrazione > Risorse di rete > Profili dispositivi di rete.

Passaggio 2. Configura profilo di autorizzazione

Selezionare Criterio > Elementi criterio > Risultati > Autorizzazione > Profili autorizzazione e scegliere lo stesso profilo dispositivo di rete come nel passo 1. ArubaWireless. Il profilo configurato è Aruba-redirect-BYOD con BYOD Portal e come mostrato nelle immagini.

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 mancante della configurazione del reindirizzamento Web, in cui viene generato il collegamento statico al profilo di autorizzazione. Anche se Aruba non supporta il reindirizzamento dinamico al portale guest, è disponibile un collegamento assegnato a ogni profilo di autorizzazione, che viene quindi configurato su Aruba e mostrato nell'immagine.

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>

Passaggio 3. Configurazione delle regole di autorizzazione

Passare a Criterio > Regole di autorizzazione e la configurazione è come mostrato nell'immagine.

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

In primo luogo, l'utente si connette a SSID mgarcarz_aruba e ISE restituisce il profilo di autorizzazione Aruba-redirect-BYOD che reindirizza il client al portale BYOD predefinito. Al termine del processo BYOD, il client si connette con EAP-TLS e viene concesso l'accesso completo alla rete.

Nelle versioni più recenti di ISE, la stessa policy potrebbe avere il seguente aspetto:

Aruba AP

Passaggio 1. Configurazione Captive Portal

Per configurare Captive Portal su Aruba 2004, selezionare Security > External Captive Portal e aggiungerne uno nuovo. Immettere queste informazioni per la configurazione corretta e come mostrato nell'immagine.

- Tipo: autenticazione Radius
- IP o nome host: server ISE
- URL: collegamento creato su ISE in Configurazione profilo di autorizzazione. È specifico di un particolare profilo di autorizzazione e si trova qui nella configurazione di Web Redirection.

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: numero della porta su cui è ospitato il portale selezionato su ISE (per impostazione predefinita: 8443), come mostrato nell'immagine.

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)

Passaggio 2. Configurazione server Radius

Selezionare Sicurezza > Authentication Server (Server di autenticazione) per verificare che la porta CoA sia la stessa configurata sull'ISE, come mostrato nell'immagine.

Per impostazione predefinita, su Aruba 204 è impostato su 5999, ma non è conforme alla RFC 5176 e non funziona 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: in Aruba versione 6.5 e successive selezionare anche la casella di controllo "Captive Portal".

Passaggio 3. Configurazione SSID

- La scheda Protezione è come illustrato nell'immagine.

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:

- Scheda Accesso: selezionare Regola di accesso basata sulla rete per configurare il portale vincolato su SSID.

Utilizzare il portale captive configurato nel passaggio 1. Fare clic su Nuovo, scegliere Tipo di regola: Portale vincolato, Tipo di pagina schizzo: Esterno come mostrato nell'immagine.

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

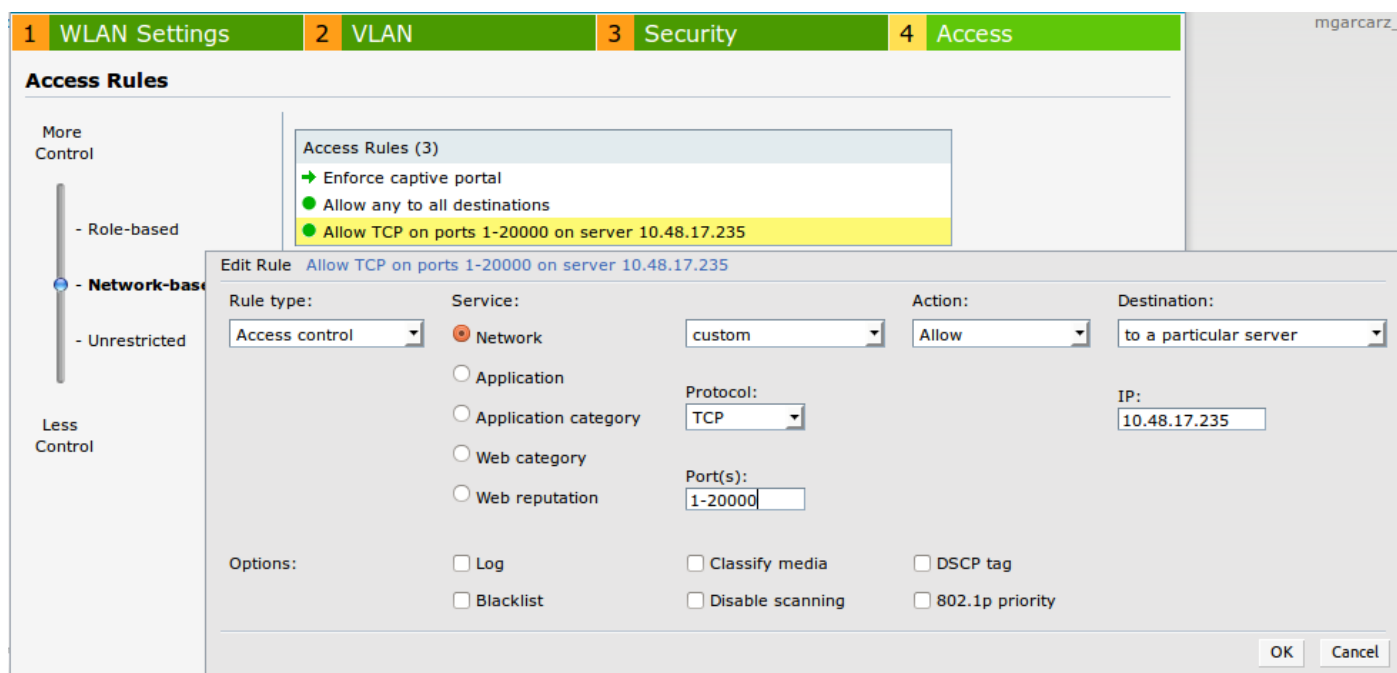
Splash page type: External

Captive portal profile: mgarcarz_ise20

Edit

Inoltre, consentire tutto il traffico verso il server ISE (porte TCP nell'intervallo 1-2000), mentre la

regola configurata per impostazione predefinita su Aruba: Allow any to all destination sembra non funzionare correttamente, come mostrato nell'immagine.



Verifica

Fare riferimento a questa sezione per verificare che la configurazione funzioni correttamente.

Passaggio 1. Connessione a SSID mgarcarz_aruba con EAP-PEAP

Appare il primo accesso di autenticazione ad ISE. È stato utilizzato il criterio di autenticazione predefinito. Il profilo di autorizzazione Aruba-redirect-BYOD è stato restituito come mostrato nell'immagine.

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Home', 'Operations', 'Policy', 'Guest Access', 'Administration', and 'Work Centers'. Below the navigation bar, there are several status indicators: 'Misconfigured Supplicants: 1', 'Misconfigured Network Devices: 0', 'RADIUS Drops: 12', and 'Client Stopped Respond: 0'. The main content area displays a table of live sessions with the following columns: Time, Status, Det..., R., Identity, Endpoint ID, Authentication Policy, Authorization Policy, Authorization Profiles, Network Device, and Event. The table contains three rows of session data.

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...				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 restituisce il messaggio Radius Access-Accept con EAP Success. Notare che non vengono restituiti attributi aggiuntivi (nessun url-redirect o url-redirect-acl a coppia av Cisco) come mostrato nell'immagine.

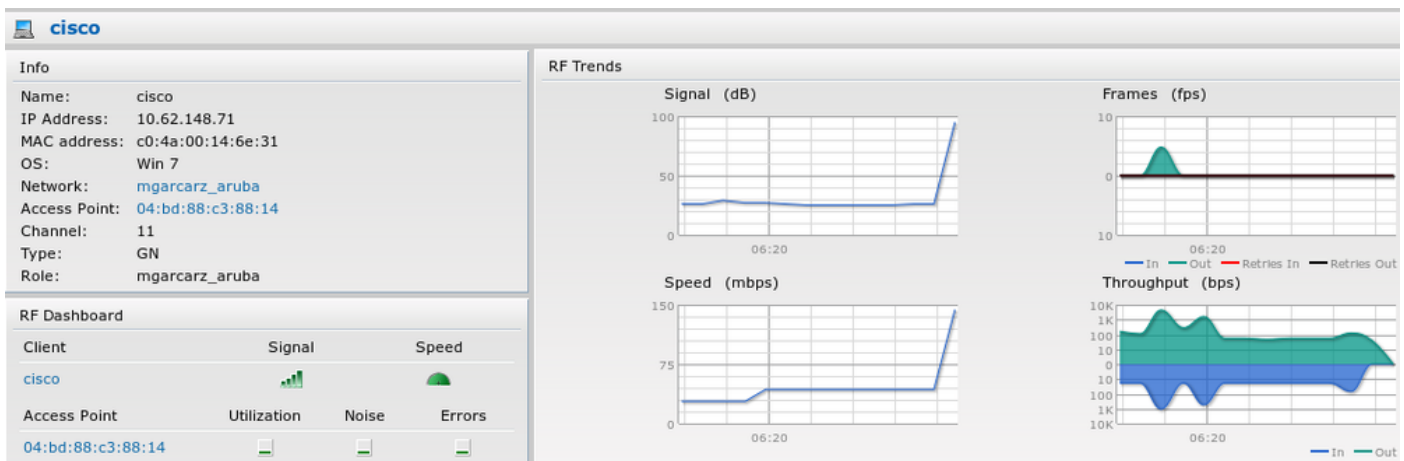
No.	Source	Destination	Protocol	Length	Info	User-Name	Acct-Session-Id
133	10.62.148.118	10.48.17.235	RADIUS	681	Access-Request(1) (id=102, l=639)	cisco	
134	10.48.17.235	10.62.148.118	RADIUS	257	Access-Challenge(11) (id=102, l=215)		
135	10.62.148.118	10.48.17.235	RADIUS	349	Access-Request(1) (id=103, 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 segnala che la sessione è stabilita (l'identità EAP-PEAP è cisco) e il ruolo selezionato è mgarcarz_aruba, come mostrato nell'immagine.



Questo ruolo è responsabile del reindirizzamento all'ISE (Captive Portal Feature su Aruba).

Nella CLI di Aruba, è possibile confermare lo stato di autorizzazione corrente per quella sessione:

```

<#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 per verificare se l'ID ACL 138 contiene le autorizzazioni correnti:

```
<#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

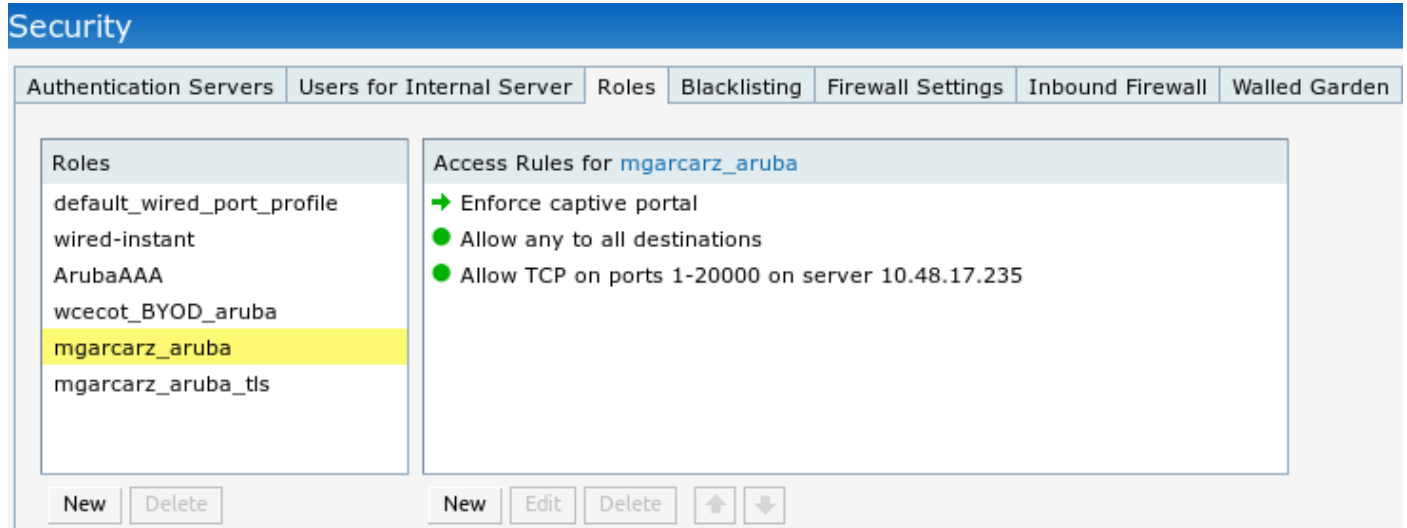
5: any mgarcarz-ise20.example.com 6 0-65535 443-443 Pd4

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
```

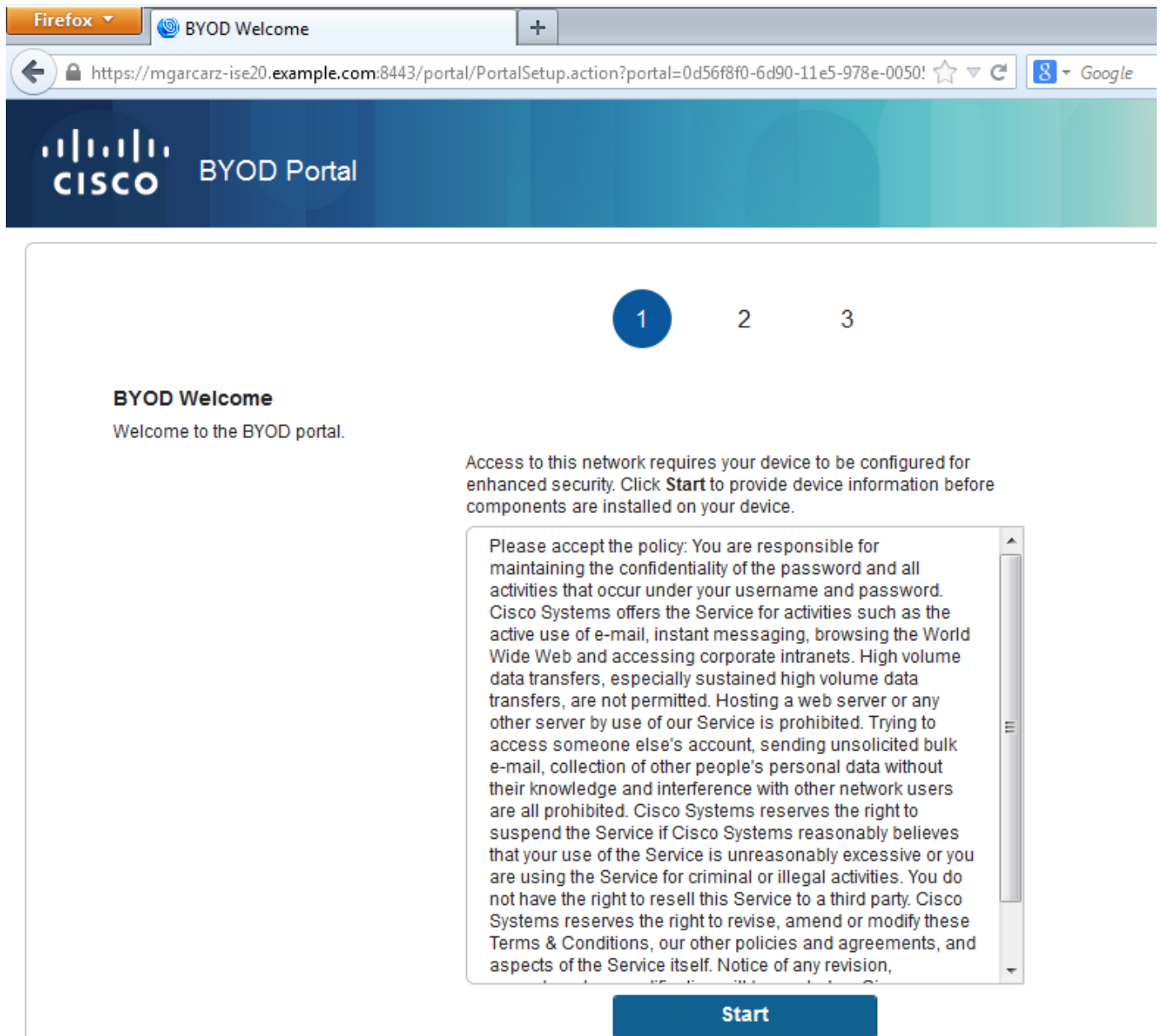
```
<....some output removed for clarity ... >
```

che corrisponde a quanto configurato nella GUI per il ruolo specifico, come mostrato nell'immagine.



Passaggio 2. Web Browser Traffic Redirection per BYOD

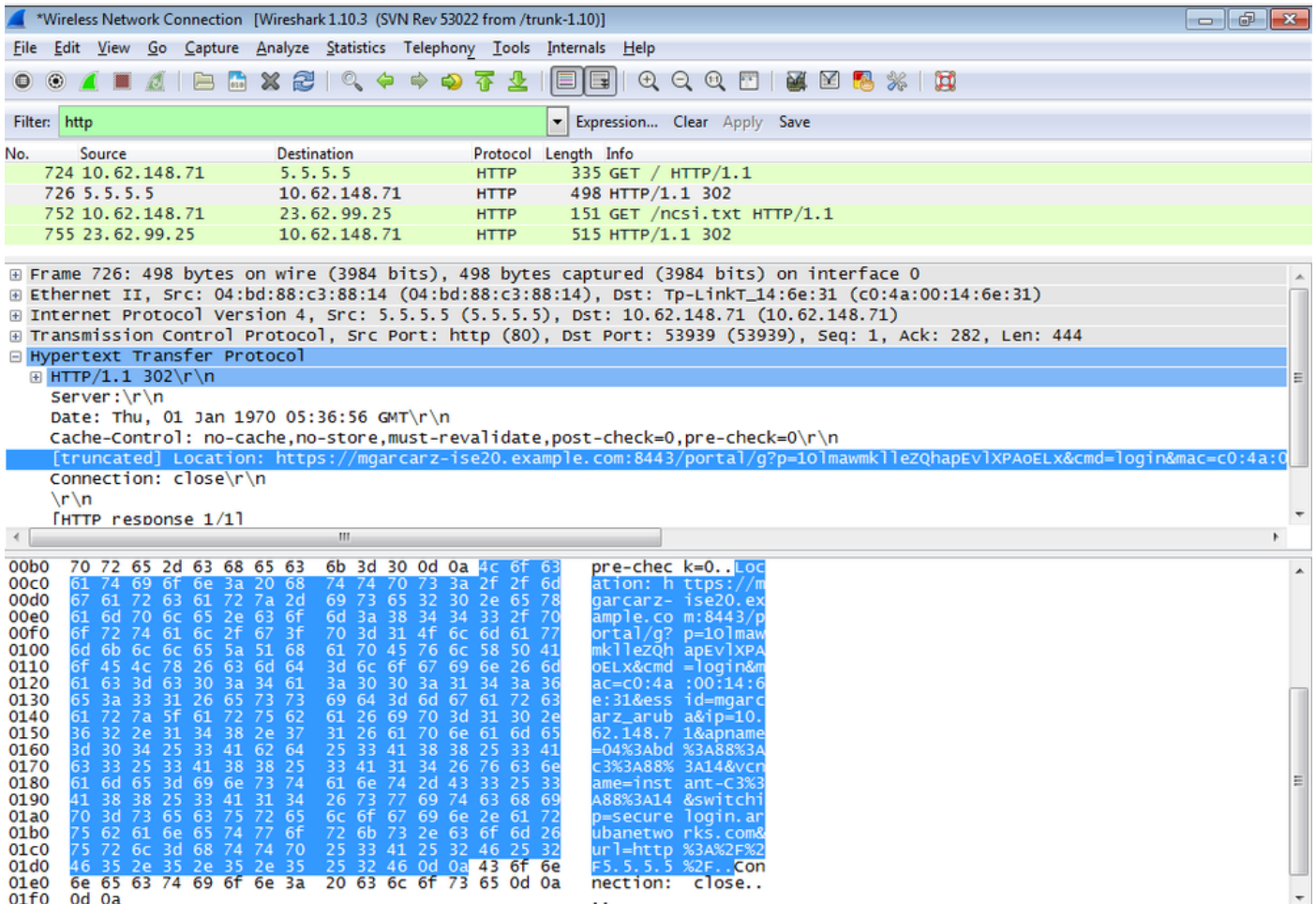
Una volta che l'utente apre il browser Web e digita qualsiasi indirizzo, viene eseguito il reindirizzamento, come mostrato nell'immagine.



Osservando le acquisizioni del pacchetto, si conferma che Aruba falsifica la destinazione (5.5.5.5) e restituisce il reindirizzamento HTTP ad ISE.

Si noti che si tratta dello stesso URL statico configurato in ISE e copiato su Captive Portal su Aruba - ma in aggiunta, vengono aggiunti più argomenti come segue e come mostrato nell'immagine:

- 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>



A causa di questi argomenti, ISE è in grado di ricreare l'ID sessione Cisco, individuare la sessione corrispondente sull'ISE e continuare con il flusso BYOD (o qualsiasi altro flusso configurato).

Per i dispositivi Cisco, audit_session_id viene normalmente utilizzato, ma questa opzione non è supportata da altri fornitori.

Per avere la conferma che dai debug ISE, è possibile vedere la generazione del valore audit-session-id (che non viene mai inviato sulla rete):

<#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 poi, la correlazione di questo dopo la registrazione del dispositivo su BYOD Pagina 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
```

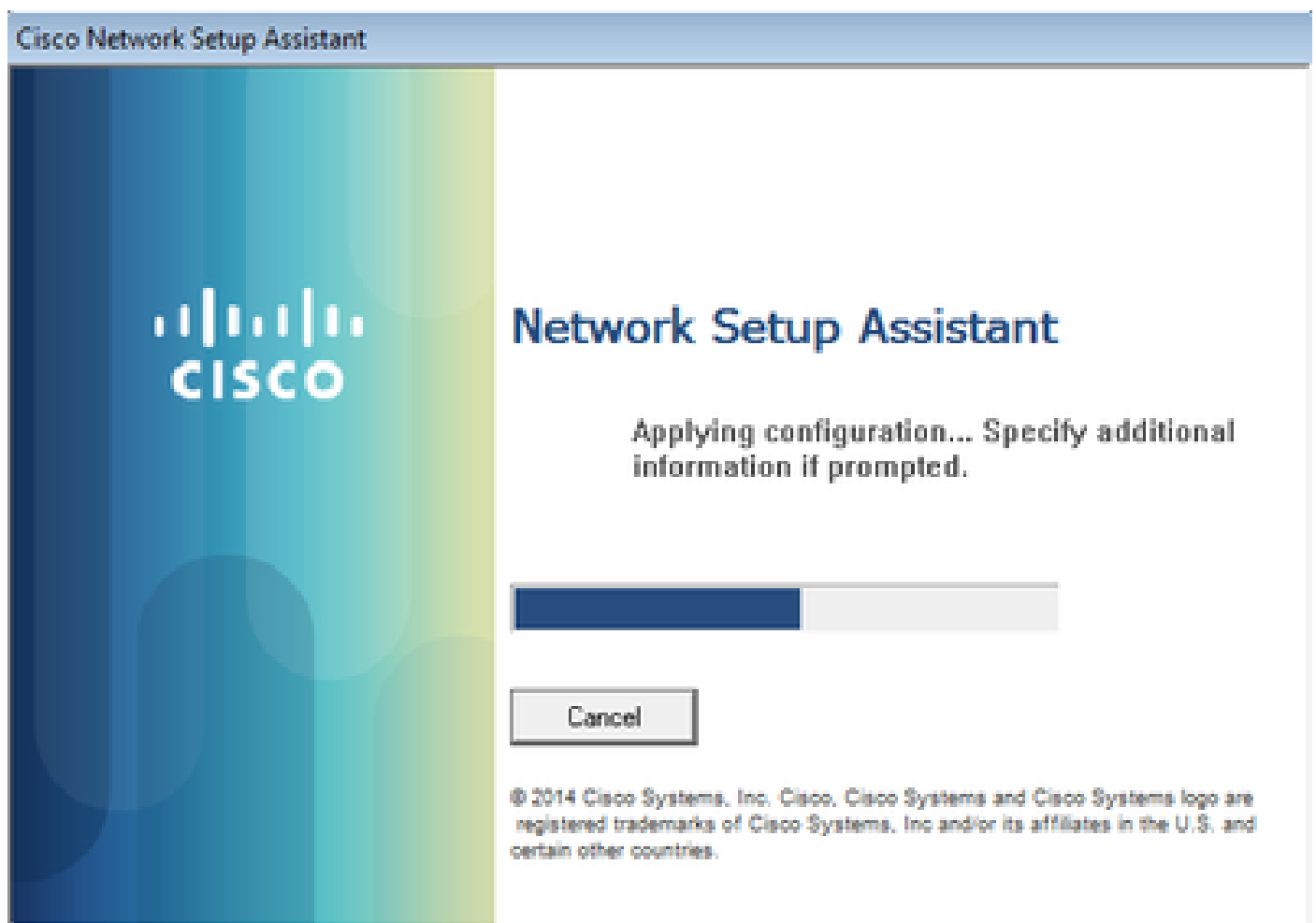
MyDevices: Successfully registered/provisioned the device

(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

Nelle richieste successive, il client viene reindirizzato a BYOD Page 3. dove NSA viene scaricato ed eseguito.

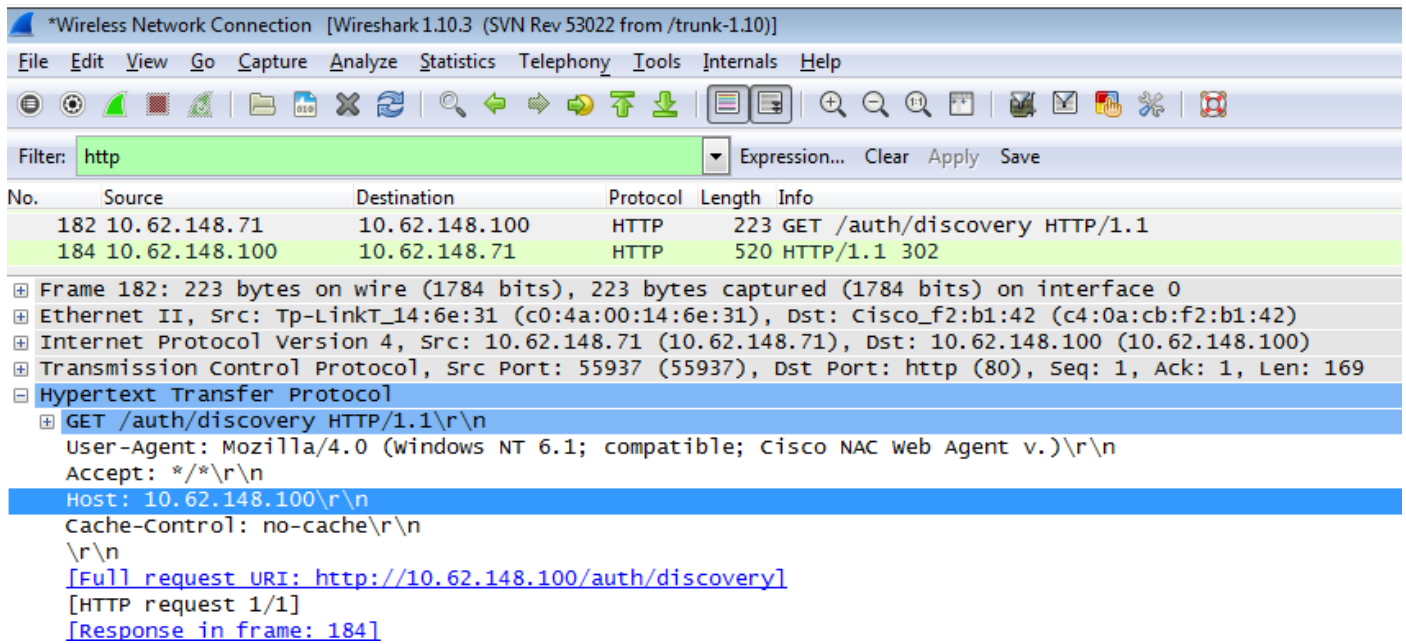
Passaggio 3. Esecuzione dell'Assistente installazione rete



L'NSA svolge la stessa attività del browser Web. Innanzitutto, deve rilevare l'indirizzo IP di ISE. Questa operazione viene eseguita tramite il reindirizzamento HTTP.

Poiché questa volta l'utente non ha la possibilità di digitare l'indirizzo IP (come nel browser Web), il traffico viene generato automaticamente.

Viene usato il gateway predefinito (è possibile usare anche enroll.cisco.com), come mostrato nell'immagine.



La risposta è esattamente la stessa del browser Web.

In questo modo NSA è in grado di connettersi ad ISE, ottenere il profilo xml con la configurazione, generare la richiesta SCEP, inviarla ad ISE, ottenere il certificato firmato (firmato dalla CA interna di ISE), configurare il profilo wireless e infine connettersi all'SSID configurato.

Raccogli registri dal client (in Windows sono in %temp%/spwProfile.log). Alcuni output sono omessi per motivi di chiarezza:

```
<#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

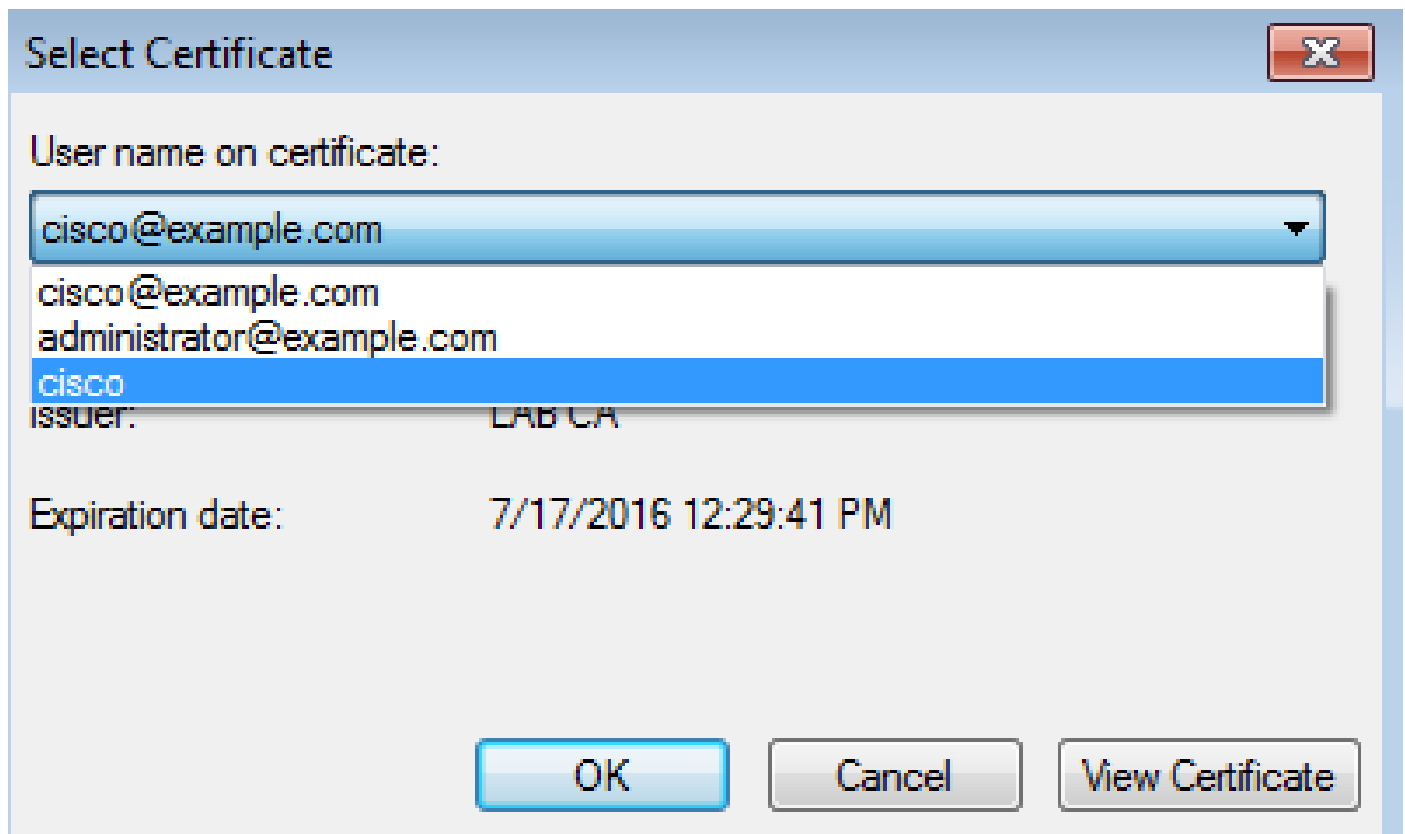
Successfully connected profile: [mgarcarz_aruba_tls]

WirelessProfile::SetWirelessProfile. - End

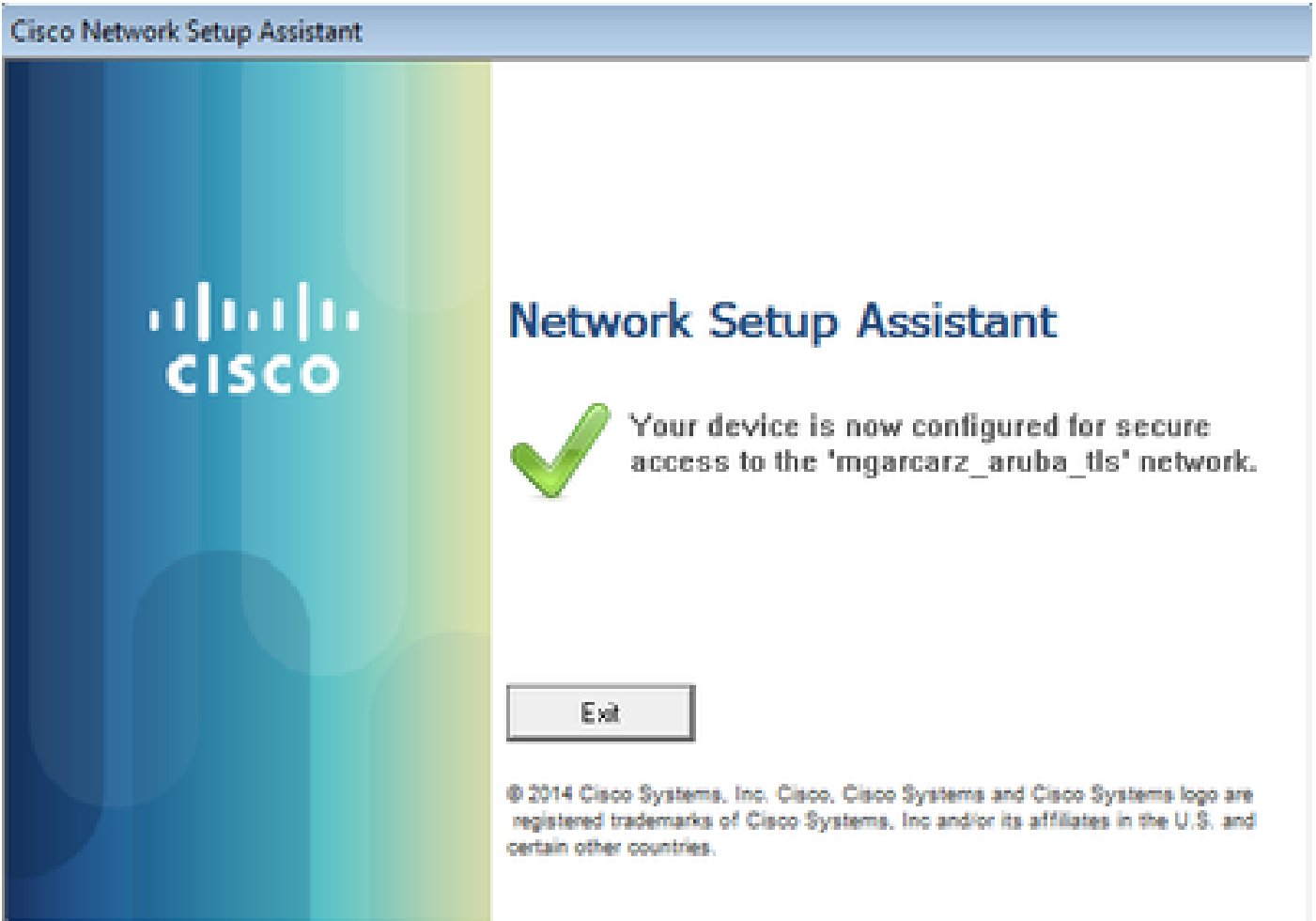
Questi log sono esattamente gli stessi utilizzati per il processo BYOD con i dispositivi Cisco.

 Nota: Radius CoA non è richiesto. È l'applicazione (NSA) che forza la riconnessione a un SSID appena configurato.

In questa fase, l'utente può vedere che il sistema tenta di associarsi a un SSID finale. Se si dispone di più certificati utente, è necessario selezionare quello corretto, come illustrato.



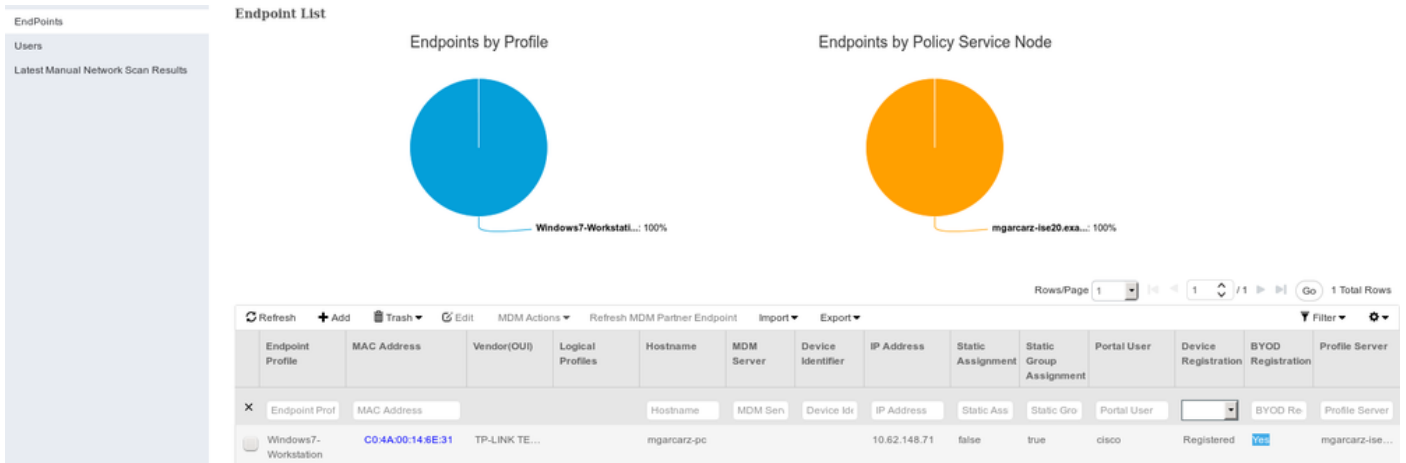
Una volta stabilita la connessione, l'NSA segnala come mostrato nell'immagine.



Ciò può essere confermato con ISE - il secondo log accede all'autenticazione EAP-TLS, che soddisfa tutte le condizioni per Basic_Authenticated_Access (EAP-TLS, Employee, e 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...				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

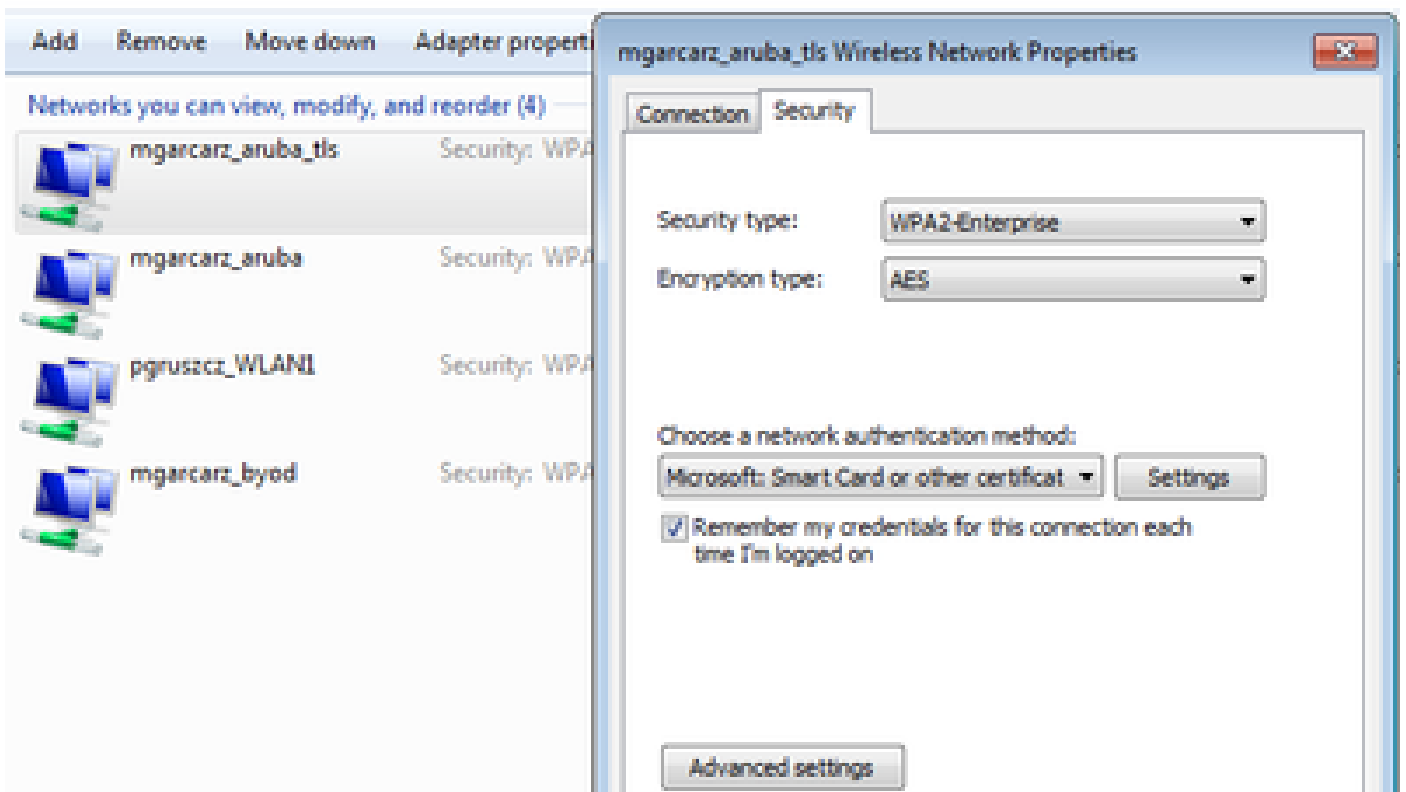
Inoltre, la vista Identità endpoint può confermare che il flag BYOD Registered sull'endpoint è impostato su true, come mostrato nell'immagine.



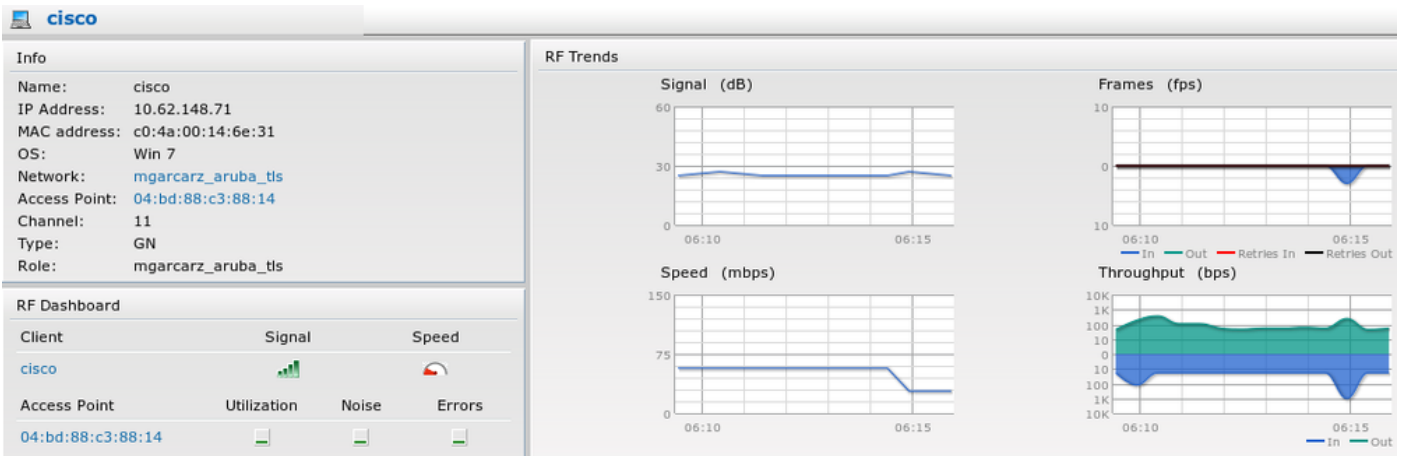
Sul PC Windows, il nuovo profilo wireless è stato creato automaticamente come preferito (e configurato per EAP-TLS) e come mostrato.

Manage wireless networks that use (Wireless Network Connection)

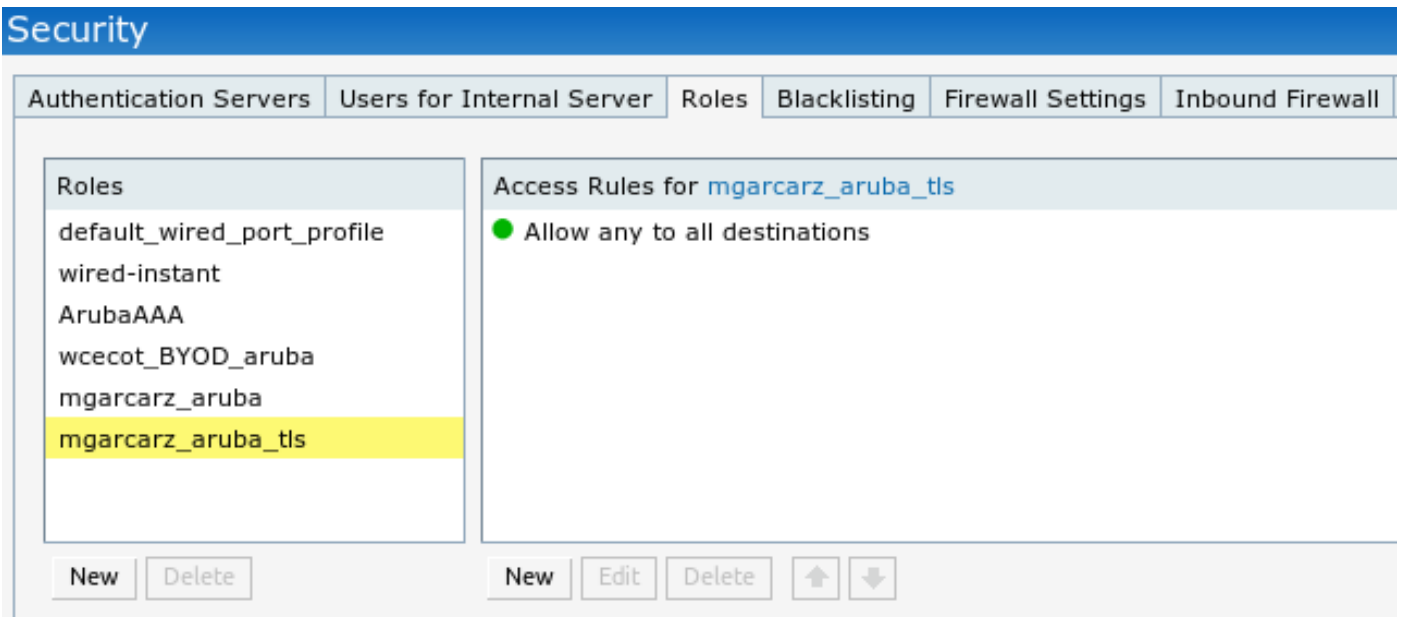
Windows tries to connect to these networks in the order listed below.



In questa fase, Aruba conferma che l'utente è connesso all'SSID finale.



Il ruolo creato automaticamente e denominato come Rete fornisce accesso completo alla rete.



Altri flussi e supporto CoA

CWA con CoA

Mentre in BYOD flow non ci sono messaggi CoA, CWA flow con Self Registered Guest Portal è dimostrato qui:

Le regole di autorizzazione configurate sono quelle illustrate nell'immagine.

<input checked="" type="checkbox"/>	Guest_Authenticate_internet	if GuestEndpoints 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

L'utente si connette all'SSID con l'autenticazione MAB e, una volta che tenta di connettersi ad una pagina Web, viene eseguito il reindirizzamento al portale Guest con registrazione automatica, in cui il guest può creare un nuovo account o utilizzare quello corrente.



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 volta stabilita la connessione, il messaggio CoA viene inviato da ISE al dispositivo di rete per modificare lo stato di autorizzazione.



Sponsored Guest Portal

Welcome Message

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

You're very close to gaining network access.

Continue

È possibile verificarlo in Operazioni > Autenticazioni e come mostrato nell'immagine.

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

Messaggio CoA nei debug 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 provenienti 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
```

Il pacchetto viene acquisito con CoA Disconnect-Request (40) e Disconnect-ACK (41) come mostrato.

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

Filter: `udp.port==3799` Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
144	17:47:49.654868	10.48.17.235	10.62.148.118	RADIUS	100	Disconnect-Request(40) (id=1, l=58)
147	17:47:49.707216	10.62.148.118	10.48.17.235	RADIUS	74	Disconnect-ACK(41) (id=1, l=32)

▶ Frame 144: 100 bytes on wire (800 bits), 100 bytes captured (800 bits)
▶ Ethernet II, Src: Vmware_99:6d:34 (00:50:56:99:6d:34), Dst: Cisco_1c:e8:00 (00:07:4f:1c:e8:00)
▶ Internet Protocol Version 4, Src: 10.48.17.235 (10.48.17.235), Dst: 10.62.148.118 (10.62.148.118)
▶ User Datagram Protocol, Src Port: 16573 (16573), Dst Port: radius-dynauth (3799)
▼ Radius Protocol
Code: Disconnect-Request (40)
Packet identifier: 0x1 (1)
Length: 58
Authenticator: 517f99c301100cb16f157562784666cb
[\[The response to this request is in frame 147\]](#)
▼ Attribute Value Pairs
▶ AVP: l=6 t=NAS-IP-Address(4): 10.62.148.118
▶ AVP: l=14 t=Calling-Station-Id(31): c04a00157634
▶ AVP: l=18 t=Message-Authenticator(80): d00e10060c68b99da3146b8592c873be

Nota: la RFC CoA è stata utilizzata per l'autenticazione relativa al profilo del dispositivo Aruba (impostazioni predefinite). Per l'autenticazione relativa al dispositivo Cisco, sarebbe stato necessario eseguire nuovamente l'autenticazione del tipo Cisco CoA.

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Aruba Captive Portal con indirizzo IP anziché FQDN

Se Captive Portal su Aruba è configurato con un indirizzo IP anziché con un FQDN di ISE, PSN NSA avrà esito negativo:


```
<#root>
```

```
Warning - [HTTPConnection]
```

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

```
CN
```

La ragione di ciò è una rigorosa convalida del certificato quando ci si connette ad ISE. Quando si utilizza l'indirizzo IP per la connessione ad ISE (come risultato del reindirizzamento dell'URL con indirizzo IP anziché FQDN) e viene visualizzato un certificato ISE con Subject Name = La convalida del nome FQDN non riesce.

 Nota: il browser Web continua con il portale BYOD (con avviso che deve essere approvato dall'utente).

Criteri di accesso non corretti per Aruba Captive Portal

Per impostazione predefinita, Aruba Access-Policy configurato con Captive Portal supporta le porte tcp 80, 443 e 8080.

NSA non è in grado di connettersi alla porta tcp 8905 per ottenere il profilo xml da ISE. Questo errore viene segnalato:

```
<#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
```

Numero porta CoA Aruba

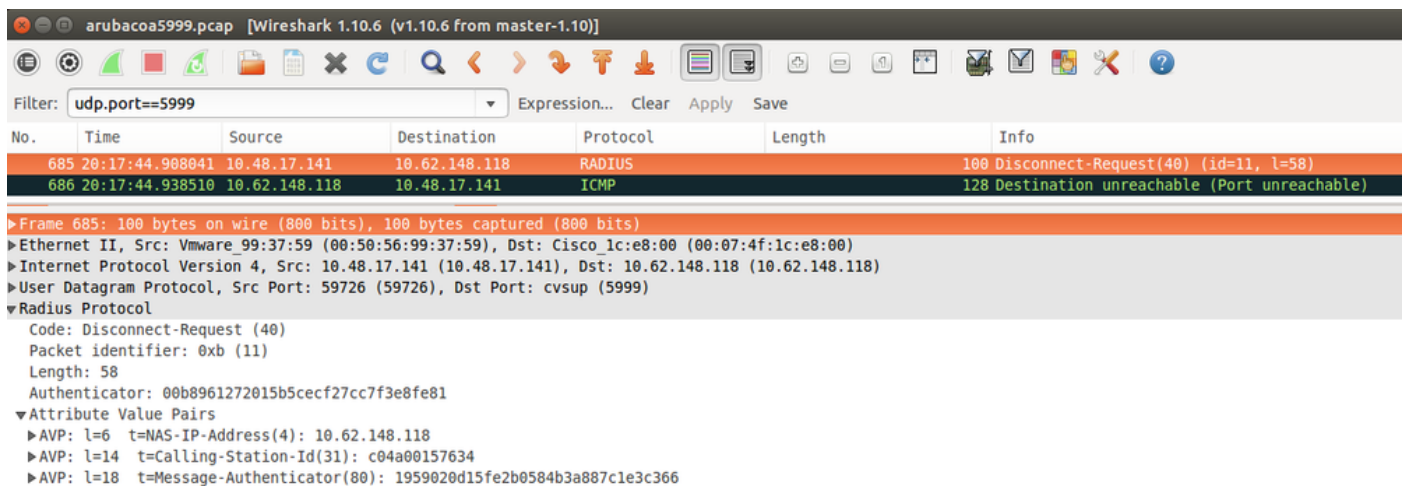
Per impostazione predefinita, Aruba fornisce il numero di porta per la porta 5999 del gruppo CoA. Sfortunatamente, Aruba 204 non ha risposto a tali richieste (come mostrato).

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

L'acquisizione del pacchetto è come mostrato nell'immagine.



L'opzione migliore da utilizzare in questo caso è la porta CoA 3977, come descritto nella RFC 5176.

Reindirizzamento su alcuni dispositivi Aruba

Su Aruba 3600 con v6.3 si nota che il reindirizzamento funziona in modo leggermente diverso rispetto agli altri controller. L'acquisizione e la spiegazione dei pacchetti sono disponibili qui.

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/

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

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

https://10.75.89.197:8443/porta1/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%2Fwww

Informazioni correlate

- [Guida per l'amministratore di Cisco Identity Services Engine, versione 2.0](#)
- [Profili dei dispositivi di accesso alla rete con Cisco Identity Services Engine](#)
- [Documentazione e supporto tecnico – Cisco Systems](#)

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).