

Configureren ISE 2.0 integratie van derden met Aruba Wireless

Inhoud

[Inleiding](#)

[Voorwaarden](#)

[Vereisten](#)

[Gebruikte componenten](#)

[Configureren](#)

[Netwerkdigram](#)

[Uitdagingen met ondersteuning van derden](#)

[Sessies](#)

[URL-omleiding](#)

[RvA](#)

[Oplossing op ISE](#)

[Cisco ISE-software](#)

[Stap 1. Aruba draadloze controller toevoegen aan netwerkapparaten](#)

[Stap 2. Autorisatieprofiel configureren](#)

[Stap 3. Autorisatieregels configureren](#)

[Aruba AP](#)

[Stap 1. Configuratie Captive Portal](#)

[Stap 2. Configuratie van RADIUS-server](#)

[Stap 3. SSID-configuratie](#)

[Verifiëren](#)

[Stap 1. Verbinding met SID mgarcarz arubamet EAP-PEAP](#)

[Stap 2. Web Browser Traffic Redirection voor BYOD](#)

[Stap 3. Uitvoeren van Network Setup Assistant](#)

[Ondersteuning van andere stromen en CoA](#)

[CWA met CoA](#)

[Problemen oplossen](#)

[Aruba Captive Portal met IPAddress in plaats van FQDN](#)

[Aruba Captive Portal Onjuist toegangsbeleid](#)

[Aruba CoA poortnummer](#)

[Omleiding op sommige Aruba-apparaten](#)

[Gerelateerde informatie](#)

Inleiding

Dit document beschrijft hoe u problemen kunt oplossen bij integratie van derden via Cisco Identity Services Engine (ISE).

Opmerking: houd er rekening mee dat Cisco niet verantwoordelijk is voor de configuratie of ondersteuning van apparaten van andere leveranciers.

Voorwaarden

Vereisten

Cisco raadt kennis van de volgende onderwerpen aan:

- Configuratie Aruba IAP
- BYOD stroomt op ISE
- ISE-configuratie voor wachtwoord- en certificaatverificatie

Gebruikte componenten

Dit document beschrijft hoe u problemen kunt oplossen bij integratie van derden via Cisco Identity Services Engine (ISE).

Het kan worden gebruikt als een gids voor integratie met andere leveranciers en stromen. ISE versie 2.0 ondersteunt integratie van derden.

Dit is een configuratievoorbeeld dat laat zien hoe u een draadloos netwerk kunt integreren dat wordt beheerd door Aruba IAP 204 met ISE voor Bring Your Own Device (BYOD)-services.

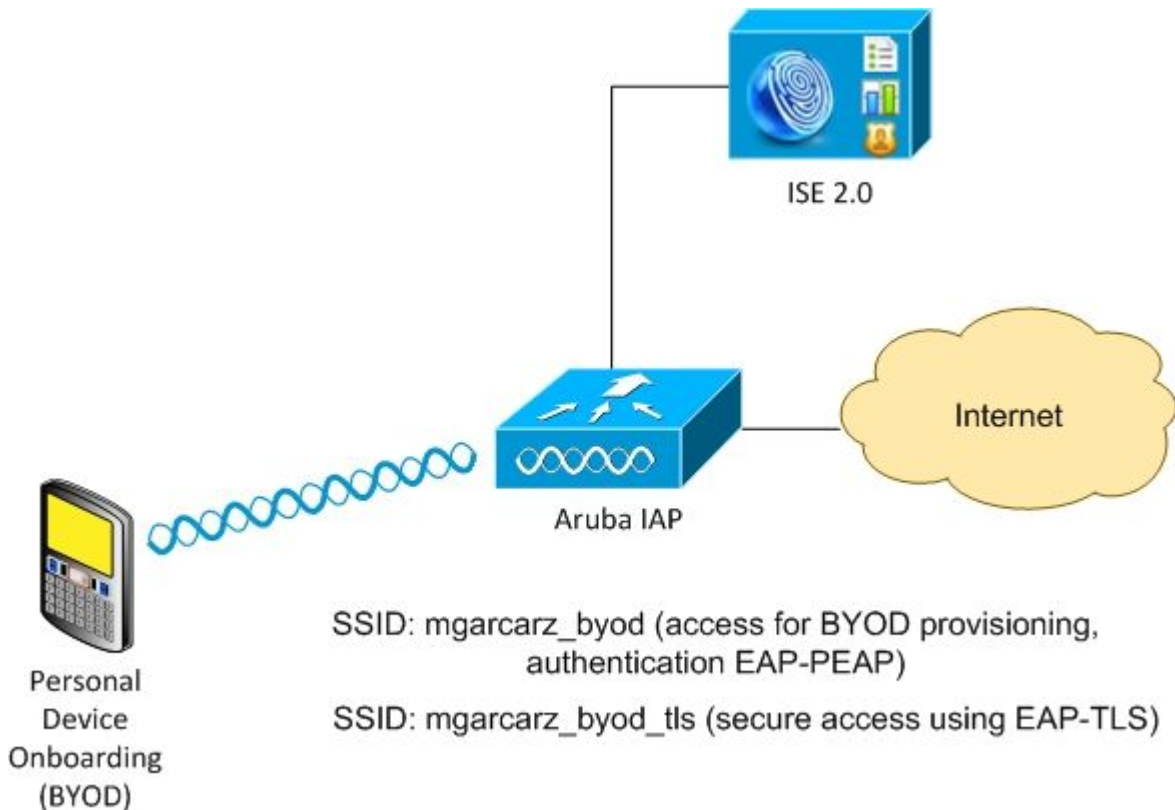
De informatie in dit document is gebaseerd op de volgende softwareversies:

- Aruba IAP 204-software 6.4.2.3
- Cisco ISE, release 2.0 en hoger

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u zorgen dat u de potentiële impact van elke opdracht begrijpt.

Configureren

Netwerkdigram



Er zijn twee draadloze netwerken beheerd door Aruba AP.

De eerste (mgarcarz_byod) wordt gebruikt voor 802.1x Extensible Verification Protocol-Protected EAP (EAP-PEAP)-toegang.

Na een succesvolle verificatie moet Aruba-controller de gebruiker omleiden naar ISE BYOD portal - Native Supplicant Provisioning (NSP) flow.

De gebruiker wordt omgeleid, de toepassing Network Setup Assistant (NSA) wordt uitgevoerd en het certificaat wordt geleverd en geïnstalleerd op de Windows-client.

ISE interne CA wordt gebruikt voor dat proces (standaardconfiguratie).

NSA is ook verantwoordelijk voor het maken van een draadloos profiel voor de tweede Service Set Identifier (SSID) die wordt beheerd door Aruba (mgarcarz_byod_tls) - die wordt gebruikt voor 802.1x Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)-verificatie.

Als gevolg daarvan kan een bedrijfsgebruiker onboarding uitvoeren van een persoonlijk apparaat en beveiligde toegang tot het bedrijfsnetwerk verkrijgen.

Dit voorbeeld kan gemakkelijk voor verschillende soorten toegang worden gewijzigd, bijvoorbeeld:

- Central Web Verification (CWA) met BYOD-service
- 802.1x verificatie met postuur- en BYOD-omleiding
- Doorgaans wordt voor EAP-PEAP-verificatie Active Directory gebruikt (om dit artikel kort te houden worden interne ISE-gebruikers gebruikt)
- Typisch, voor de externe Eenvoudige server van het Protocol van de Inschrijving van het Certificaat van de Provisioning van het Certificaat (SCEP) wordt gebruikt, algemeen de Dienst van de Inschrijving van het Apparaat van het Netwerk van Microsoft (NDES) om dit artikel kort te houden, wordt interne CA gebruikt.

Uitdagingen met ondersteuning van derden

Er zijn de uitdagingen wanneer u ISE Guest flows (zoals BYOD, CWA, NSP, Client Provisioning Portal (CPP)) gebruikt met apparaten van derden.

Sessies

Cisco Network Access Devices (NAD) maakt gebruik van Radius cisco-av-paar dat audit-sessie-id wordt genoemd om verificatie-, autorisatie- en accounting (AAA) server te informeren over sessie-ID.

Die waarde wordt door ISE gebruikt om de sessies te volgen en de juiste diensten voor elke stroom te leveren. Andere leveranciers ondersteunen geen cisco-av-paar.

ISE moet zich baseren op IETF-attributen die worden ontvangen in Access-request en accounting request.

Nadat u een toegangs aanvraag hebt ontvangen, maakt ISE een gesynthetiseerde Cisco Session ID (van Calling-Station-ID, NAS-poort, NAS-IP-adres en gedeeld geheim). Die waarde heeft alleen een lokale betekenis (niet verzonden via het netwerk).

Dientengevolge, heeft het van elke stroom (BYOD, CWA, NSP, CPP) verwacht om correcte attributen vast te maken - zodat is ISE in staat om Cisco Session ID opnieuw te berekenen en een raadpleging uit te voeren om het met de juiste sessie te correleren en de stroom voort te zetten.

URL-omleiding

ISE maakt gebruik van Radius cisco-av-pair genaamd url-redirect en url-redirect-acl om te informeren over en aan te geven dat specifiek verkeer moet worden omgeleid.

Andere leveranciers ondersteunen geen cisco-av-paar. Deze apparaten moeten dus doorgaans worden geconfigureerd met statische omleiding-URL die verwijst naar specifieke service (autorisatieprofiel) op ISE.

Zodra de gebruiker HTTP-sessie start, verwijzen die NAD's naar de URL en voegen ook extra argumenten toe (zoals IP-adres of MAC-adres) om ISE toe te staan specifieke sessie te identificeren en de stroom voort te zetten.

RvA

ISE maakt gebruik van Radius cisco-av-paar, Subscriber:Command:Subscriber:Reauthenticate-type om aan te geven welke handelingen moeten en moeten worden uitgevoerd voor een bepaalde sessie.

Andere leveranciers ondersteunen geen cisco-av-paar. Deze apparaten gebruiken doorgaans RFC CoA (3576 of 5176) en een van de twee gedefinieerde berichten:

- verzoek om verbinding verbreken (ook wel pakketverbinding verbreken genoemd) - dat wordt gebruikt om de sessie los te koppelen (zeer vaak om herverbinding af te dwingen)
- CoA-push - die wordt gebruikt om de sessiestatus transparant te wijzigen zonder de verbinding te verbreken (bijvoorbeeld VPN-sessie en nieuwe ACL toegepast)

ISE ondersteunt zowel Cisco CoA met cisco-av-paar als ook RFC CoA 3576/5176.

Oplossing op ISE

Om leveranciers van derden te ondersteunen, introduceerde ISE 2.0 een concept van Network Device

Profiles, waarin beschreven wordt hoe bepaalde leveranciers zich gedragen - hoe Sessies, URL Redirect en CoA worden ondersteund.

Autorisatieprofielen zijn van een specifiek type (Network Device Profile) en zodra de verificatie plaatsvindt, wordt het ISE-gedrag afgeleid van dat profiel.

Hierdoor kunnen apparaten van andere leveranciers eenvoudig door ISE worden beheerd. Ook de configuratie op ISE is flexibel en maakt het mogelijk om nieuwe netwerkapparaatprofielen te maken of af te stemmen.

In dit artikel wordt het gebruik van standaardprofiel voor Aruba-apparaten gepresenteerd.

Meer informatie over deze functie:

[Profielen voor netwerktoegangsapparaat met Cisco Identity Services Engine](#)

Cisco ISE-software

Stap 1. Aruba draadloze controller toevoegen aan netwerkapparaten

Ga naar **Beheer > Netwerkbronnen > Netwerkapparaten**. Kies correct apparaatprofiel voor geselecteerde verkoper, in dit geval: **ArubaWireless**. Zorg ervoor dat u de **gedeelde geheim-** en **CoA-poort** configureert zoals in de afbeeldingen wordt getoond.

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

Als er geen profiel beschikbaar is voor de gewenste leverancier, kan dit worden geconfigureerd onder **Beheer > Netwerkbronnen > Netwerkapparaatprofielen**.

Stap 2. Autorisatieprofiel configureren

Ga naar **Beleid > Beleidselementen > Resultaten > Autorisatie > Autorisatieprofielen** en kies hetzelfde profiel voor netwerkkapparaten als in Stap 1. **ArubaDraadloos**. Het gevormde profiel is **Aruba-redirect-BYOD met BYOD Portal** en zoals getoond in de beelden.

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

Ontbrekend deel van de configuratie van de omleiding van het web, waar een statische link naar het autorisatieprofiel wordt gegenereerd. Hoewel Aruba geen dynamische omleiding naar het gastenportaal ondersteunt, is er één link toegewezen aan elk Autorisatieprofiel, dat dan op Aruba wordt geconfigureerd en zoals in de afbeelding wordt getoond.

Common Tasks

Value

The network device profile selected above requires the following redirect URL to be configured manually on the network access device

https://iseHost:8443/portal/g?p=10lmawmkllZQhapEvIXPAoELx

Stap 3. Autorisatieregels configureren

Navigeer naar **Policy > Autorisatieregels** en de configuratie wordt weergegeven zoals in de afbeelding.

<input checked="" type="checkbox"/>	Basic_Authenticated_Access	if Employee AND (EAP-TLS AND EndPoints:BYODRegistration EQUALS Yes)
<input checked="" type="checkbox"/>	ArubaRedirect	if Aruba:Aruba-Essid-Name EQUALS mgarcarz_aruba

Ten eerste, gebruiker verbindt met SSID mgarcarz_aruba en ISE retourneert autorisatieprofiel Aruba-redirect-BYOD die client omleidt naar standaard BYOD portal. Nadat het BYOD-proces is voltooid, maakt de client verbinding met EAP-TLS en wordt volledige toegang tot het netwerk verleend.

In de nieuwere versies van ISE kan hetzelfde beleid er als volgt uitzien:

The screenshot shows the ISE Policy Elements configuration page. It features a table with columns for Status, Policy Set Name, Description, and Conditions. Below the table, there are expandable sections for Authentication Policy, Authorization Policy - Local Exceptions, Authorization Policy - Global Exceptions, and Authorization Policy (3). The expanded section shows three rules:

Status	Rule Name	Conditions	Results
<input checked="" type="checkbox"/>	Authorized	AND example.com:ExternalGroups EQUALS example.com/Builtin/Administrators EndPoints:BYODRegistration EQUALS Yes Network Access-EapAuthentication EQUALS EAP-TLS	PermitAccess
<input checked="" type="checkbox"/>	Redirect	Aruba:Aruba-Essid-Name EQUALS mgarcarz_aruba	Aruba_Redirect_BYOD
<input checked="" type="checkbox"/>	Default		DenyAccess

Aruba AP

Stap 1. Configuratie Captive Portal

Om Captive Portal op Aruba 204 te configureren, navigeer naar **Security > Externe Captive Portal** en voeg er een nieuwe toe. Voer deze informatie in voor een juiste configuratie en zoals in het beeld wordt getoond.

- Type: Radius-verificatie
- IP of hostnaam: ISE-server
- URL: link die op ISE is gemaakt onder Autorisatieprofielconfiguratie; het is specifiek voor een bepaald autorisatieprofiel en kan hier worden gevonden onder de configuratie van de webomleiding

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:

https://iseHost:8443/portal/g?p=10lmawmkleZQhapEvIXPAoELx

- Port: poortnummer waarop de geselecteerde portal wordt gehost op ISE (standaard: 8443) zoals weergegeven in de afbeelding.

The screenshot shows a configuration dialog box for a RADIUS server profile named 'mgarcarz_ise20'. The fields are as follows:

Type:	Radius Authentication ▼
IP or hostname:	mgarcarz-ise20.example.
URL:	/portal/g?p=Kjr7eB7RrrLl
Port:	8443
Use https:	Enabled ▼
Captive Portal failure:	Deny internet ▼
Automatic URL Whitelisting:	Disabled ▼
Redirect URL:	(optional)

Buttons: OK, Cancel

Stap 2. Configuratie van RADIUS-server

Navigeren naar **Security > Verificatieservers** zorgt ervoor dat de CoA-poort hetzelfde is als die op ISE is geconfigureerd zoals in het afbeelding.

Standaard is het op Aruba 204 ingesteld op 5999, dat echter niet voldoet aan RFC 5176 en ook niet werkt met 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="text" value="*****"/>	
Retype key:	<input type="text" 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"/>	

Opmerking: In Aruba versie 6.5 en nieuwer selecteer ook "Captive Portal" checkbox.

Stap 3. SSID-configuratie

- Het tabblad Beveiliging is zoals in de afbeelding.

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:

- Tabblad Toegang: selecteer **Netwerkgebaseerde toegangsregel** om een toegangsporthaal op een SSID te configureren.

Gebruik een intern portal dat in stap 1 is geconfigureerd. Klik op **Nieuw**, kies Regel type: **Captive portal**, Splash pagina type: **Extern** zoals in de afbeelding.

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 pr: mgarcarz_ise20 [Edit](#)

Laat bovendien al het verkeer naar ISE-server toe (TCP-poorten in bereik 1-20000), terwijl regel standaard ingesteld op Aruba: **Toestaan om het even welke bestemming** lijkt niet goed te werken zoals in de afbeelding.

The screenshot shows the Cisco ISE configuration interface. At the top, there are four tabs: 1 WLAN Settings, 2 VLAN, 3 Security, and 4 Access. The 'Access Rules' section is active, showing a list of three rules. The third rule, 'Allow TCP on ports 1-20000 on server 10.48.17.235', is highlighted in yellow. An 'Edit Rule' dialog box is open for this rule, showing the following configuration: Rule type: Access control; Service: Network (selected); Action: Allow; Protocol: TCP; Port(s): 1-20000. There are also checkboxes for Log, Blacklist, Classify media, Disable scanning, DSCP tag, and 802.1p priority.

Verifiëren

Gebruik deze sectie om te controleren of uw configuratie goed werkt.

Stap 1. Verbinding met SID mgarcarz_aruba met EAP-PEAP

Er wordt eerst een verificatielogboek weergegeven op ISE. Standaardverificatiebeleid is gebruikt, het autorisatieprofiel van Aruba-redirect-BYOD is getourneerd zoals in de afbeelding.

The screenshot shows the Cisco ISE Identity Services Engine interface. The top navigation bar includes Home, Operations, Policy, Guest Access, Administration, and Work Centers. The main content area shows 'Misconfigured Supplicants: 1', 'Misconfigured Network Devices: 0', and 'RADIUS Drops: 12'. Below this is a table of live sessions with columns for Time, Status, Det..., R., Identity, Endpoint ID, Authentication Policy, Authorization Policy, and Authorization F.

Time	Status	Det...	R.	Identity	Endpoint ID	Authentication Policy	Authorization Policy	Authorization F
2015-10-29 22:23:37...			0	cisco	CO:4A:00:14:6E:31	Default >> Dot1X >> EAP-TLS	Default >> Basic_Authenticated...	PermitAccess
2015-10-29 22:23:37...				cisco	CO:4A:00:14:6E:31	Default >> Dot1X >> EAP-TLS	Default >> Basic_Authenticated...	PermitAccess
2015-10-29 22:19:09...				cisco	CO:4A:00:14:6E:31	Default >> Dot1X >> Default	Default >> ArubaRedirect	Aruba-redirect

ISE retourneert Radius Access-Accept bericht met EAP Success. Merk op dat er geen extra eigenschappen worden teruggegeven (geen Cisco av-paar url-redirect of url-redirect-acl) zoals in de afbeelding.

No.	Source	Destination	Protocol	Length	Info	User-
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
153	10.48.17.235	10.62.148.118	RADIUS	62	Accounting-Response(5) (id=108, l=20)	

Packet identifier: 0x6b (107)

Length: 321

Authenticator: 1173a3d3ea3d0798fe30fdaccf644f19

[\[This is a response to a request in frame 143\]](#)

[Time from request: 0.038114000 seconds]

Attribute Value Pairs

▷ AVP: l=7 t=User-Name(1): cisco

▷ AVP: l=67 t=State(24): 52656175746853657373696f6e3a30613330313165625862...

▷ AVP: l=87 t=Class(25): 434143533a30613330313165625862697544413379554e6f...

▷ AVP: l=6 t=EAP-Message(79) Last Segment[1]

▷ AVP: l=18 t=Message-Authenticator(80): e0b74092cacf88803dcd37032b761513

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

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

Aruba meldt dat de sessie is ingesteld (EAP-PEAP-identiteit is **cisco**) en geselecteerde Rol is **mgarcarz_aruba** zoals in de afbeelding.

The screenshot shows a Cisco network management interface. On the left, there is a 'Info' section for a client named 'cisco' with IP address 10.62.148.71, MAC address c0:4a:00:14:6e:31, OS Win 7, Network mgarcarz_aruba, Access Point 04:bd:88:c3:88:14, Channel 11, Type GN, and Role mgarcarz_aruba. Below this is an 'RF Dashboard' with a table showing Signal and Speed for the client and Utilization, Noise, and Errors for the Access Point. On the right, there are two line graphs: 'Signal (dB)' and 'Speed (mbps)', both showing a sharp increase at 06:20.

Client	Signal	Speed
cisco		

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

Die rol is verantwoordelijk voor de omleiding naar de ISE (captive portal functionaliteit op Aruba).

In de CLI van Aruba is het mogelijk om te bevestigen wat de huidige status van autorisatie voor die sessie is:

```
<#root>
```

```
04:bd:88:c3:88:14#
```

```
show datapath user
```

```
Datapath User Table Entries
```

```
-----  
Flags: P - Permanent, W - WEP, T- TKIP, A - AESCCM  
R - ProxyARP to User, N - VPN, L - local, I - Intercept, D - Deny local routing  
FM(Forward Mode): S - Split, B - Bridge, N - N/A
```

IP	MAC	ACLs	Contract	Location	Age	Sessions	Flags	Vlan	FM
10.62.148.118	04:BD:88:C3:88:14	105/0	0/0	0	1	0/65535	P	1	N
10.62.148.71	C0:4A:00:14:6E:31	138/0	0/0	0	0	6/65535		1	B
0.0.0.0	C0:4A:00:14:6E:31	138/0	0/0	0	0	0/65535	P	1	B
172.31.98.1	04:BD:88:C3:88:14	105/0	0/0	0	1	0/65535	P	3333	B
0.0.0.0	04:BD:88:C3:88:14	105/0	0/0	0	0	0/65535	P	1	N

```
04:bd:88:c3:88:14#
```

En om ACL-id 138 te controleren op de huidige machtigingen:

```
<#root>
```

```
04:bd:88:c3:88:14#
```

```
show datapath acl 138
```

```
Datapath ACL 138 Entries
```

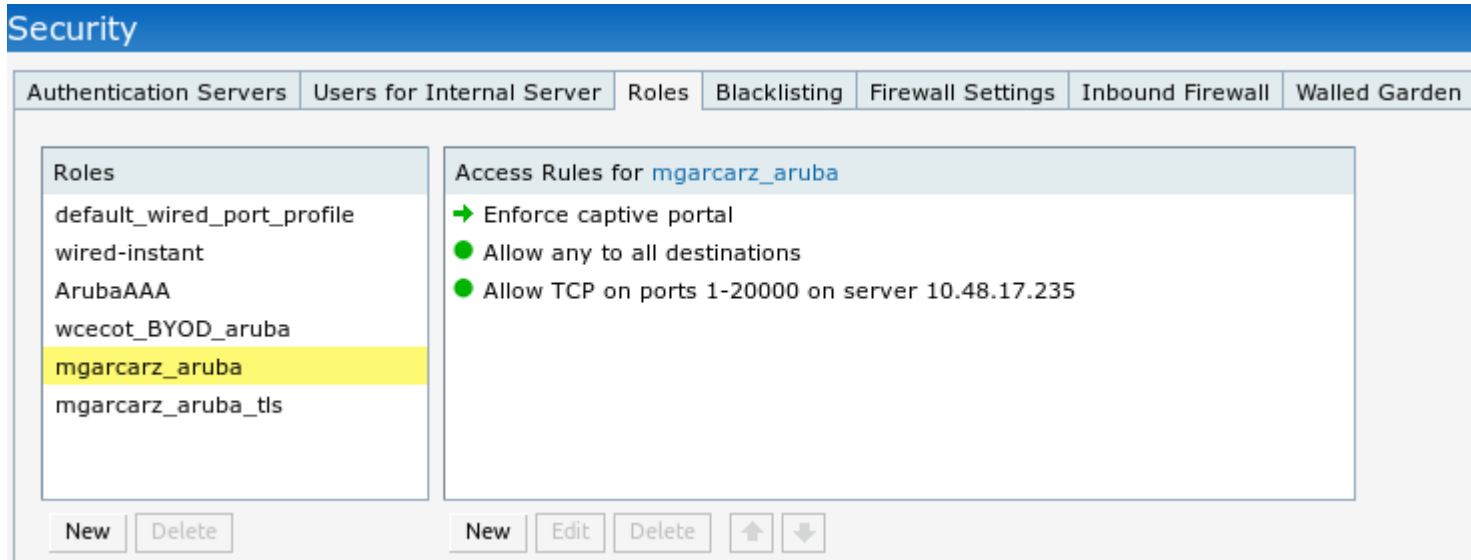
```
-----  
Flags: P - permit, L - log, E - established, M/e - MAC/etype filter  
S - SNAT, D - DNAT, R - redirect, r - reverse redirect m - Mirror  
I - Invert SA, i - Invert DA, H - high prio, O - set prio, C - Classify Media  
A - Disable Scanning, B - black list, T - set TOS, 4 - IPv4, 6 - IPv6  
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

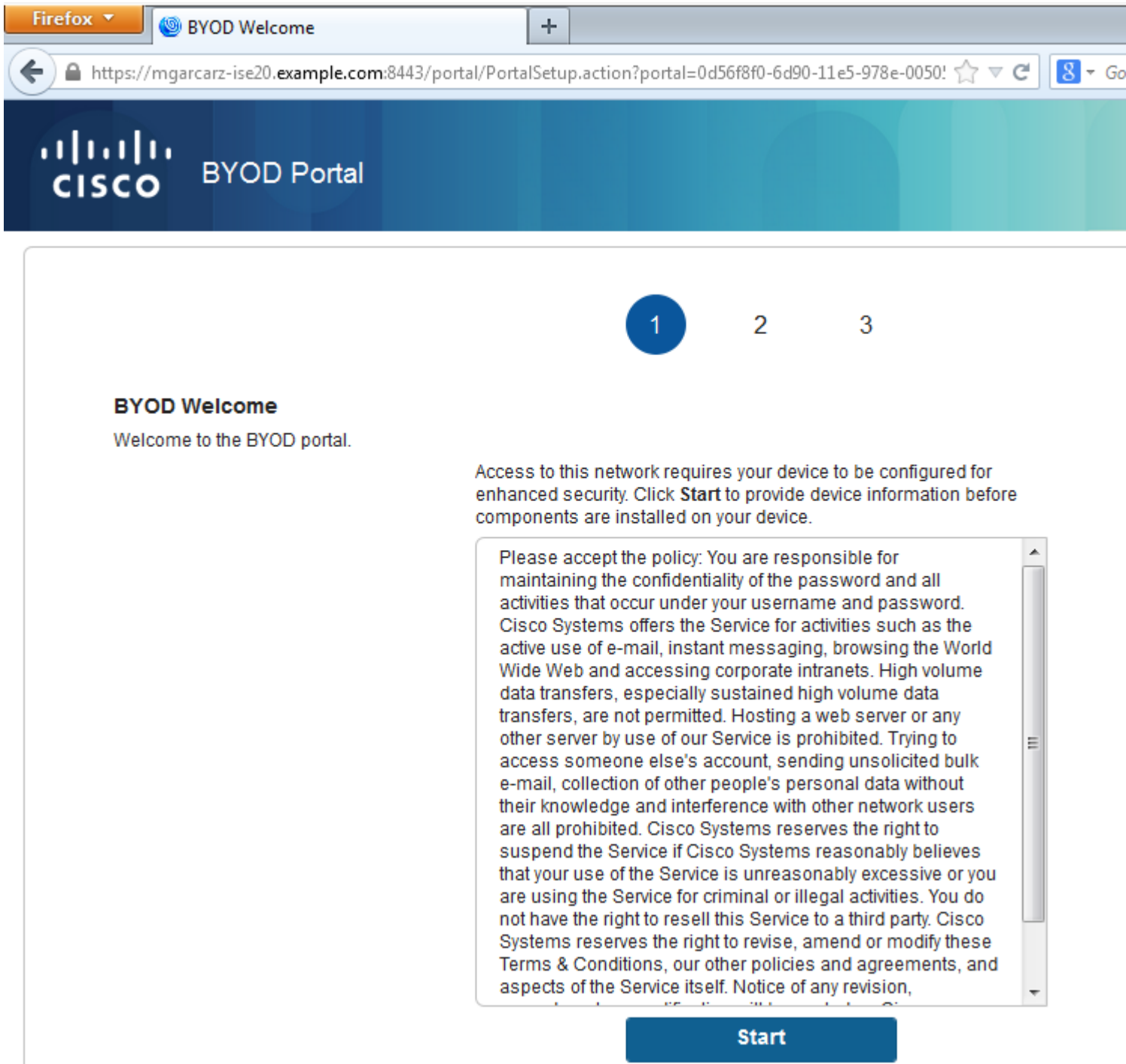
<...some output removed for clarity ... >

Dat komt overeen met wat in GUI voor die rol is geconfigureerd zoals in de afbeelding.



Stap 2. Web Browser Traffic Redirection voor BYOD

Zodra de gebruiker de webbrowser opent en elk adres typt, vindt omleiding plaats zoals in de afbeelding.



Als we kijken naar het pakketbestand, zien we dat Aruba de bestemming spooft (5.5.5.5) en de HTTP-omleiding terugstuurt naar ISE.

Merk op dat het dezelfde statische URL is als geconfigureerd in ISE en gekopieerd naar Captive Portal op Aruba - maar daarnaast worden meerdere argumenten als volgt toegevoegd en zoals getoond in het beeld:

- cmd = aanmelding
- mac = c0:4a:00:14:6e:31
- essid = mgarcarz_aruba
- ip = 10.62.148,7
- apname = 4bd88c38814 (mac)
- url = <http://5.5.5.5>

*Wireless Network Connection [Wireshark 1.10.3 (SVN Rev 53022 from /trunk-1.10)]

File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help

Filter: http Expression... Clear Apply Save

No.	Source	Destination	Protocol	Length	Info
724	10.62.148.71	5.5.5.5	HTTP	335	GET / HTTP/1.1
726	5.5.5.5	10.62.148.71	HTTP	498	HTTP/1.1 302
752	10.62.148.71	23.62.99.25	HTTP	151	GET /ncsi.txt HTTP/1.1
755	23.62.99.25	10.62.148.71	HTTP	515	HTTP/1.1 302

Frame 726: 498 bytes on wire (3984 bits), 498 bytes captured (3984 bits) on interface 0

Ethernet II, Src: 04:bd:88:c3:88:14 (04:bd:88:c3:88:14), Dst: Tp-LinkT_14:6e:31 (c0:4a:00:14:6e:31)

Internet Protocol Version 4, Src: 5.5.5.5 (5.5.5.5), Dst: 10.62.148.71 (10.62.148.71)

Transmission Control Protocol, Src Port: http (80), Dst Port: 53939 (53939), Seq: 1, Ack: 282

Hypertext Transfer Protocol

HTTP/1.1 302\r\n

Server:\r\n

Date: Thu, 01 Jan 1970 05:36:56 GMT\r\n

Cache-Control: no-cache,no-store,must-revalidate,post-check=0,pre-check=0\r\n

[truncated] Location: https://mgarcarz-ise20.example.com:8443/portal/g?p=101mawmk1lezQhapEVLXPApEVLXPApEVLX&cmd=login&mac=c0:4a:00:14:6e:31&ssid=mgarcarz_aruba&ip=10.62.148.71&apname=04%3Abd%3A88%3Ac3%3A88%3A14&vcrname=instant-C3%3A88%3A14&switchip=securelogin.arubanetworks.com&url=http%3A%2F%2F5.5.5.5%2F..Connection: close..

```

00b0 70 72 65 2d 63 68 65 63 6b 3d 30 0d 0a 4c 6f 63 pre-heck=0..Loc
00c0 61 74 69 6f 6e 3a 20 68 74 74 70 73 3a 2f 2f 6d ation: h ttps://m
00d0 67 61 72 63 61 72 7a 2d 69 73 65 32 30 2e 65 78 garcarz- ise20.ex
00e0 61 6d 70 6c 65 2e 63 6f 6d 3a 38 34 34 33 2f 70 ample.co m:8443/p
00f0 6f 72 74 61 6c 2f 67 3f 70 3d 31 4f 6c 6d 61 77 ortal/g? p=101maw
0100 6d 6b 6c 6c 65 5a 51 68 61 70 45 76 6c 58 50 41 mk1lezQh apEVLXPA
0110 6f 45 4c 78 26 63 6d 64 3d 6c 6f 67 69 6e 26 6d oELx&cmd =login&m
0120 61 63 3d 63 30 3a 34 61 3a 30 30 3a 31 34 3a 36 ac=c0:4a :00:14:6
0130 65 3a 33 31 26 65 73 73 69 64 3d 6d 67 61 72 63 e:31&ess id=mgarc
0140 61 72 7a 5f 61 72 75 62 61 26 69 70 3d 31 30 2e arz_arub a&ip=10.
0150 36 32 2e 31 34 38 2e 37 31 26 61 70 6e 61 6d 65 62.148.7 1&apname
0160 3d 30 34 25 33 41 62 64 25 33 41 38 38 25 33 41 =04%3Abd %3A88%3A
0170 63 33 25 33 41 38 38 25 33 41 31 34 26 76 63 6e c3%3A88% 3A14&vcr
0180 61 6d 65 3d 69 6e 73 74 61 6e 74 2d 43 33 25 33 ame=inst ant-C3%3
0190 41 38 38 25 33 41 31 34 26 73 77 69 74 63 68 69 A88%3A14 &switchi
01a0 70 3d 73 65 63 75 72 65 6c 6f 67 69 6e 2e 61 72 p=secure login.ar
01b0 75 62 61 6e 65 74 77 6f 72 6b 73 2e 63 6f 6d 26 ubanetwo rks.com&
01c0 75 72 6c 3d 68 74 74 70 25 33 41 25 32 46 25 32 url=http %3A%2F%2
01d0 46 35 2e 35 2e 35 2e 35 25 32 46 0d 0a 43 6f 6e F5.5.5.5 %2F..Con
01e0 6e 65 63 74 69 6f 6e 3a 20 63 6c 6f 73 65 0d 0a nection: close..
01f0 0d 0a ..

```

Wegens deze argumenten, kan ISE Cisco Session ID opnieuw genereren, de corresponderende sessie over ISE achterhalen en doorgaan met BYOD (of een andere geconfigureerde) flow.

Voor Cisco-apparaten wordt **audit_sessie_id** normaal gebruikt, maar dat wordt niet ondersteund door andere leveranciers.

Om te bevestigen dat van ISE debugs, is het mogelijk om de generatie van controle-sessie-id waarde (die nooit over het netwerk wordt verzonden) te zien:

<#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

```

En dan, correlatie van dat na registratie van het apparaat op BYOD pagina 2:

<#root>

```
AcLogs,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
```

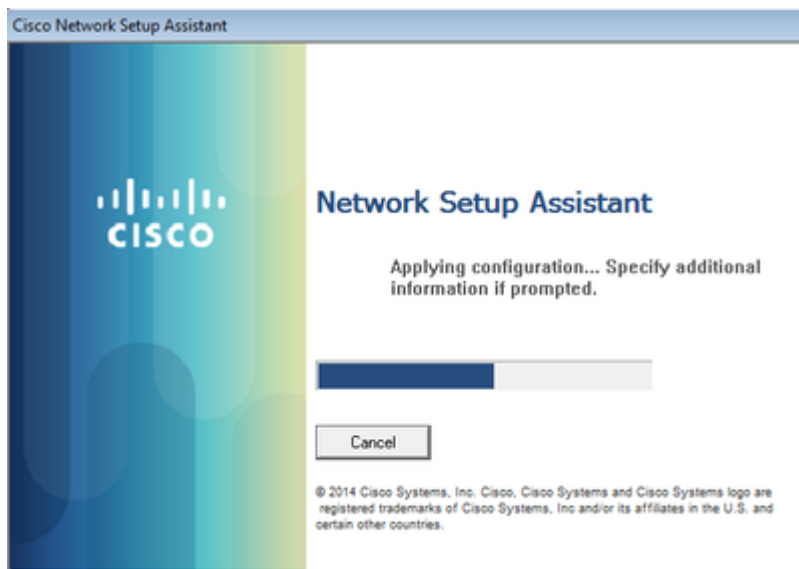
MyDevices: Successfully registered/provisioned the device

```
(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

In latere verzoeken wordt de client doorgestuurd naar BYOD Page 3. waar NSA wordt gedownload en uitgevoerd.

Stap 3. Uitvoeren van Network Setup Assistant



NSA heeft dezelfde taak als webbrowser. Ten eerste moet het weten wat het IP-adres van ISE is. Dat wordt bereikt via HTTP-omleiding.

Omdat de gebruiker dit keer geen mogelijkheid heeft om IP-adres in te voeren (zoals in de webbrowser), wordt dat verkeer automatisch gegenereerd.

Standaard gateway wordt gebruikt (ook **enroll.cisco.com** kan worden gebruikt) zoals in de afbeelding.

Filter: http

No.	Source	Destination	Protocol	Length	Info
182	10.62.148.71	10.62.148.100	HTTP	223	GET /auth/discovery HTTP/1.1
184	10.62.148.100	10.62.148.71	HTTP	520	HTTP/1.1 302

Frame 182: 223 bytes on wire (1784 bits), 223 bytes captured (1784 bits) on interface 0
 Ethernet II, Src: Tp-LinkT_14:6e:31 (c0:4a:00:14:6e:31), Dst: Cisco_f2:b1:42 (c4:0a:cb:f2:b1:42)
 Internet Protocol Version 4, Src: 10.62.148.71 (10.62.148.71), Dst: 10.62.148.100 (10.62.148.100)
 Transmission Control Protocol, Src Port: 55937 (55937), Dst Port: http (80), Seq: 1, Ack: 1
 Hypertext Transfer Protocol
 GET /auth/discovery HTTP/1.1\r\n
 User-Agent: Mozilla/4.0 (windows NT 6.1; compatible; Cisco NAC web Agent v.)\r\n
 Accept: */*\r\n
 Host: 10.62.148.100\r\n
 Cache-Control: no-cache\r\n
 \r\n
 [Full request URI: http://10.62.148.100/auth/discovery]
 [HTTP request 1/1]
 [Response in frame: 184]

De reactie is precies hetzelfde als voor de webbrowser.

Op deze manier kan NSA verbinding maken met ISE, xml-profiel met configuratie genereren, SCEP-verzoek genereren, naar ISE sturen, ondertekend certificaat verkrijgen (ondertekend door ISE interne CA), draadloos profiel configureren en uiteindelijk verbinding maken met de geconfigureerde SSID.

Logbestanden verzamelen vanaf de client (op Windows is in `%temp%/spwProfile.log`). Sommige outputs worden voor de duidelijkheid weggelaten:

```
<#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: 0a3011ebXbiuDA3yUNoLUvtCRyuPFxkqYJ7TT06fo0Z70

DiscoverISE - end

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

GetProfile - start

GetProfile - end

Successfully retrieved profile xml

using V2 xml version

parsing wireless connection setting

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

set ChallengePwd

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

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

ec 8a 11 78^M

] as rootCA

Installed CA cert for authMode machineOrUser - Success

HttpWrapper::SendScepRequest

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

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

Certificate issued - successfully

ScepWrapper::InstallCert start

ScepWrapper::InstallCert: Reading scep response file

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

ScepWrapper::InstallCert GetCertHash -- return val 1

ScepWrapper::InstallCert end

Configuring wireless profiles...

Configuring ssid [mgarcarz_aruba_tls]

WirelessProfile::SetWirelessProfile - Start

Wireless profile: [mgarcarz_aruba_tls] configured successfully

Connect to SSID

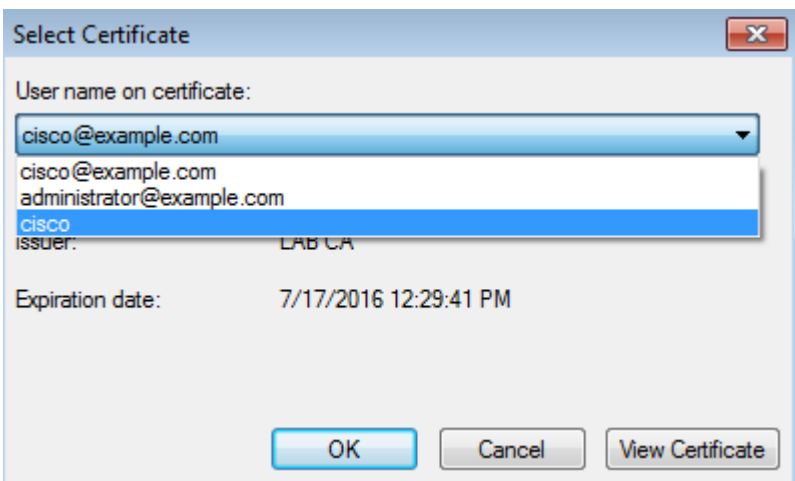
Successfully connected profile: [mgarcarz_aruba_tls]

WirelessProfile::SetWirelessProfile. - End

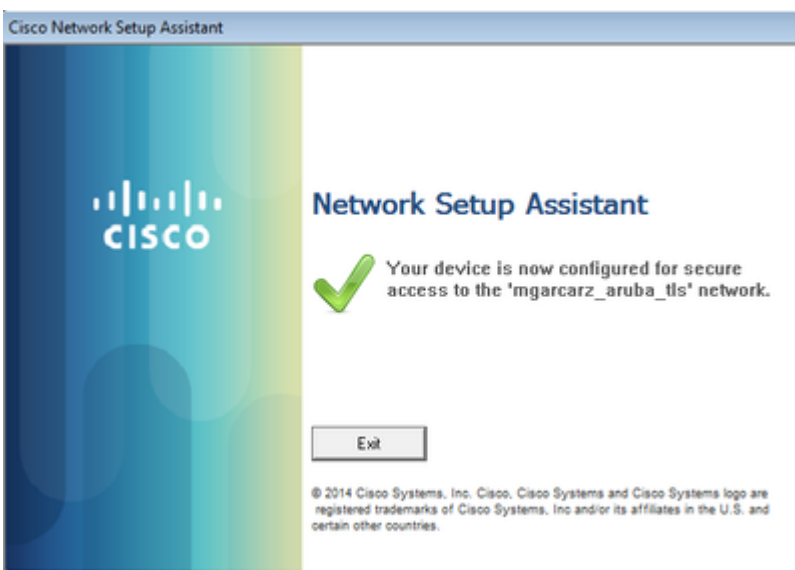
Deze logs zijn precies hetzelfde als bij het BYOD-proces met Cisco-apparaten.

Opmerking: Radius CoA is hier niet vereist. Het is de toepassing (NSA) die de verbinding met een nieuw geconfigureerde SSID afdwingt.

In dat stadium, kan de gebruiker zien dat het systeem probeert om aan definitieve SSID te associëren. Als u meer dan één gebruikerscertificaat hebt, moet u het juiste certificaat selecteren (zoals aangegeven op de afbeelding).



Na een succesvolle verbinding, NSA rapporten is zoals getoond in het beeld.



Dat kan worden bevestigd op ISE - het tweede log raakt EAP-TLS-verificatie, die voldoet aan alle voorwaarden voor Basic_Authenticated_Access (EAP-TLS, Werknemer en BYOD Registered true).

Identity Services Engine Home Operations Policy Guest Access Administration Work Centers

RADIUS Livelog TACACS Livelog Reports Troubleshoot Adaptive Network Control

Misconfigured Supplicants **1** Misconfigured Network Devices **0** RADIUS Drops **12**

Show Live Sessions Add or Remove Columns Refresh Reset Repeat Counts


Time	Status	Det...	R.	Identity	Endpoint ID	Authentication Policy	Authorization Policy	Authorization F
2015-10-29 22:23:37...			0	cisco	CO:4A:00:14:6E:31	Default >> Dot1X >> EAP-TLS	Default >> Basic_Authenticated...	PermitAccess
2015-10-29 22:23:37...				cisco	CO:4A:00:14:6E:31	Default >> Dot1X >> EAP-TLS	Default >> Basic_Authenticated...	PermitAccess
2015-10-29 22:19:09...				cisco	CO:4A:00:14:6E:31	Default >> Dot1X >> Default	Default >> ArubaRedirect	Aruba-redirect

Ook, kan de mening van de endpointidentiteit bevestigen dat het eindpunt BYOD Geregistreerde vlag heeft die aan waar zoals aangetoond in het beeld wordt geplaatst.

EndPoints Users Latest Manual Network Scan Results


Endpoint List

Endpoints by Profile



Windows7-Workstatl...: 100%

Endpoints by Policy Service Node



mgarcarz-is...

Endpoint Profile	MAC Address	Vendor(OUI)	Logical Profiles	Hostname	MDM Server	Device Identifier	IP Address	Static Assignment	Stat Gro	Ass
Windows7-Workstation	CO:4A:00:14:6E:31	TP-LINK TE...		mgarcarz-pc			10.62.148.71	false	true	

Op Windows PC is automatisch een nieuw draadloos profiel gemaakt, zoals de voorkeur (en geconfigureerd voor EAP-TLS) en zoals getoond.

Manage wireless networks that use (Wireless Network Connection)

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

Network Name	Security
mgarcarz_aruba_tls	WPA2-Enterprise
mgarcarz_aruba	WPA2-Enterprise
pgruszc_WLAN1	WPA2-Enterprise
mgarcarz_byod	WPA2-Enterprise

mgarcarz_aruba_tls Wireless Network Properties

Connection Security

Security type: WPA2-Enterprise

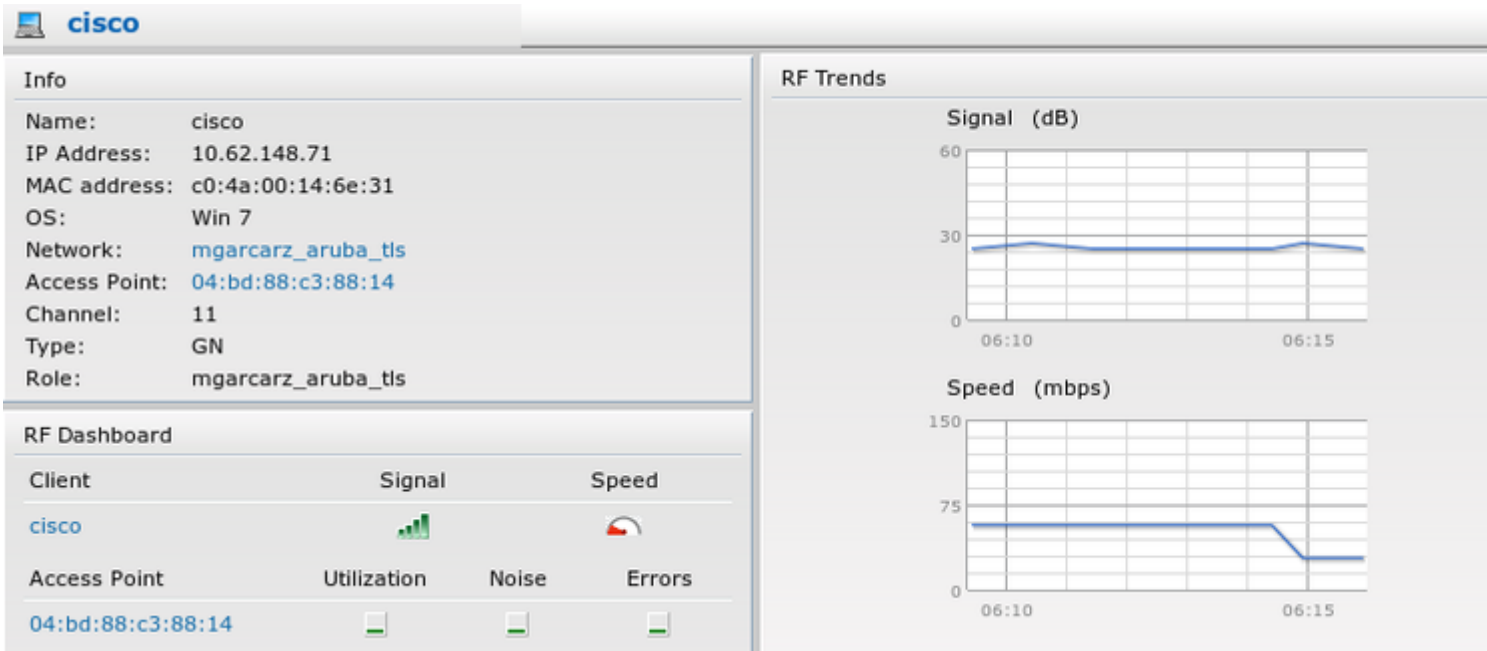
Encryption type: AES

Choose a network authentication method: Microsoft: Smart Card or other certificat

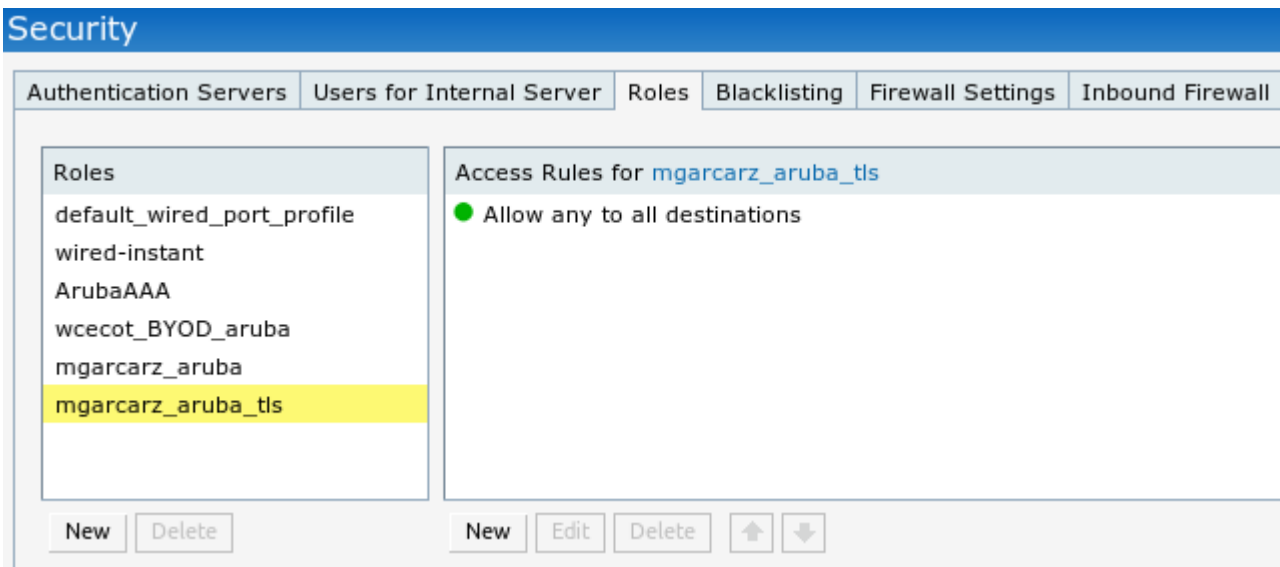
Remember my credentials for this connection each time I'm logged on

Advanced settings

In dat stadium bevestigt Aruba dat de gebruiker is verbonden met de uiteindelijke SSID.



De rol die automatisch wordt gemaakt en dezelfde naam krijgt als Network biedt volledige netwerktoegang.



Ondersteuning van andere stromen en CoA

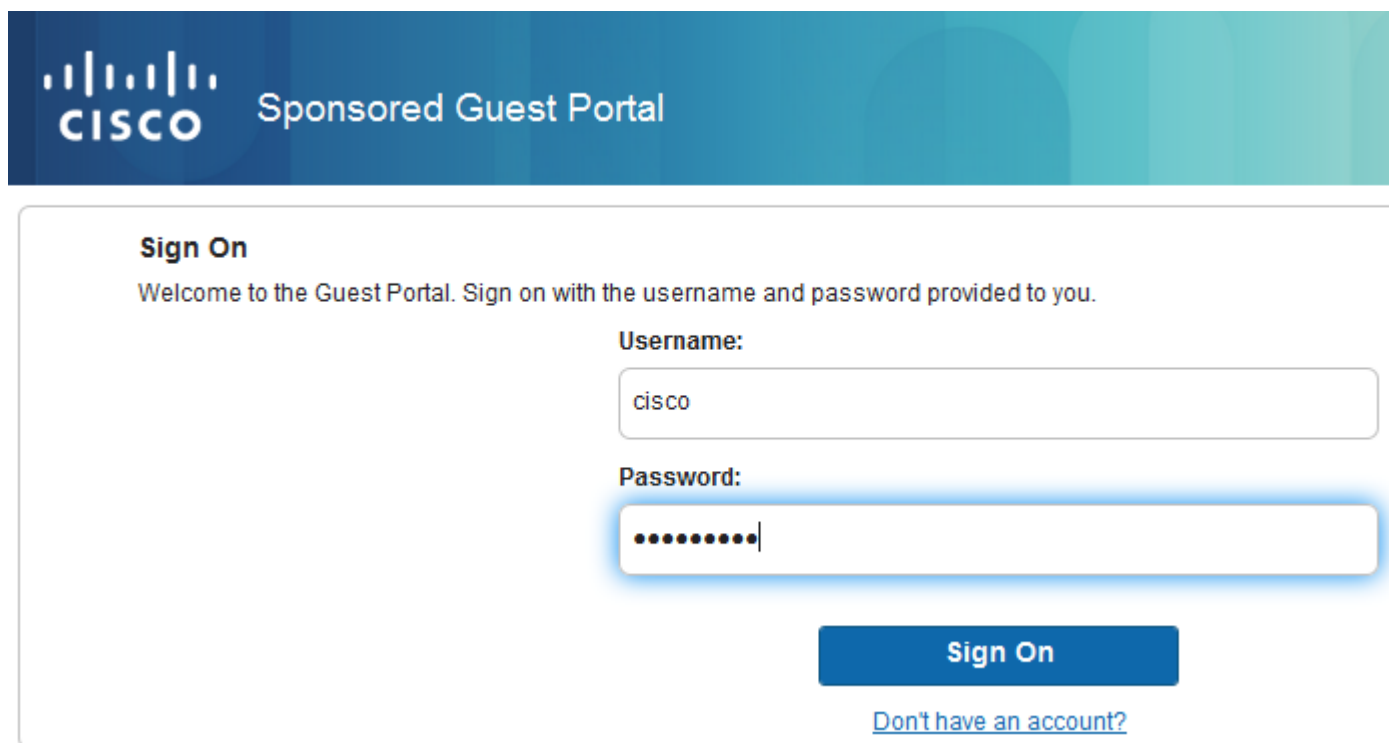
CWA met CoA

Terwijl in BYOD flow er geen CoA-berichten zijn, wordt CWA flow met Self Registered Guest Portal hier gedemonstreerd:

De ingestelde autorisatieregels zijn zoals in de afbeelding.

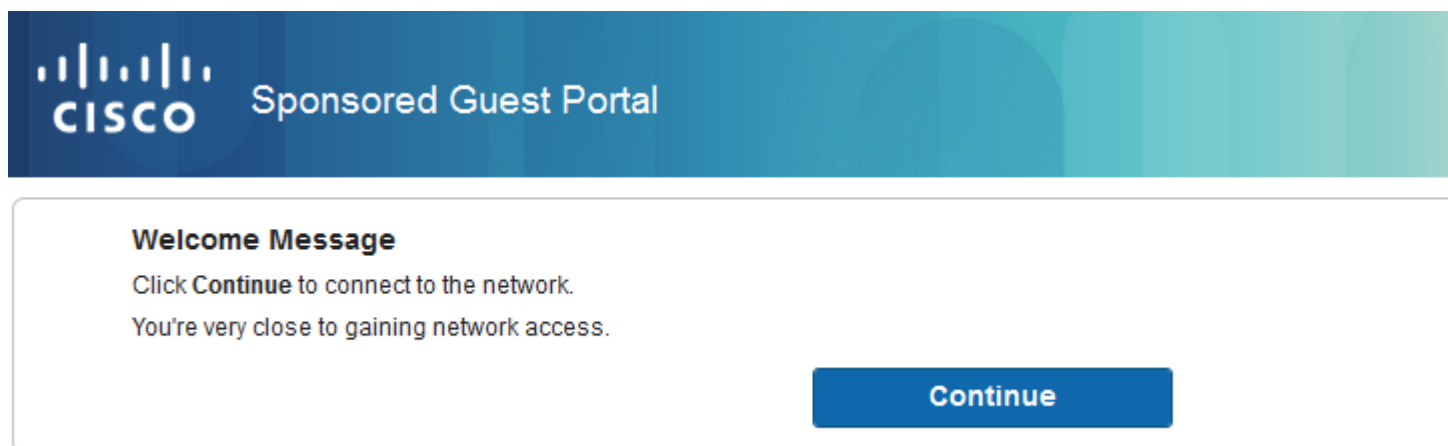
<input checked="" type="checkbox"/>	Guest_Authenticate_internet	if GuestEndpoints AND Aruba:Aruba-Essid-Name EQUALS mgarcarz_aruba_guest
<input checked="" type="checkbox"/>	Guest_Authenticate_Aruba	if Aruba:Aruba-Essid-Name EQUALS mgarcarz_aruba_guest

Gebruiker maakt verbinding met de SSID met MAB-verificatie en zodra het probeert verbinding te maken met een webpagina, wordt omleiding naar Self Registered Guest Portal gedaan, waar Gast een nieuw account kan maken of een huidig account kan gebruiken.



The screenshot shows the 'Sign On' section of the Cisco Sponsored Guest Portal. It features the Cisco logo and the text 'Sponsored Guest Portal'. Below the header, there is a 'Sign On' heading and a welcome message: 'Welcome to the Guest Portal. Sign on with the username and password provided to you.' There are two input fields: 'Username:' with the value 'cisco' and 'Password:' with masked characters. A blue 'Sign On' button is positioned below the password field, and a link for 'Don't have an account?' is located below the button.

Nadat de gast met succes is verbonden, wordt er een CoA-bericht van ISE naar het netwerkapparaat verzonden om de autorisatiestatus te wijzigen.



The screenshot shows the 'Welcome Message' section of the Cisco Sponsored Guest Portal. It features the Cisco logo and the text 'Sponsored Guest Portal'. Below the header, there is a 'Welcome Message' heading and the text: 'Click Continue to connect to the network. You're very close to gaining network access.' A blue 'Continue' button is positioned at the bottom right of the message area.

Het kan worden geverifieerd onder **Operations > Authentications** en zoals getoond in de afbeelding.

cisco	C0:4A:00:15:76:34	Windows7-Workstat...	Default >> MAB	Default >> Guest_Authenticate_internet	Autho
	C0:4A:00:15:76:34				Dynan
cisco	C0:4A:00:15:76:34				Guest
C0:4A:00:15:76	C0:4A:00:15:76:34		Default >> MAB >> ...	Default >> Guest_Authenticate_Aruba	Authe

CoA-bericht in ISE-debug:

<#root>


```
2015-11-02 18:47:49,553 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
```

```
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
```

en Disconnect-ACK die afkomstig is van Aruba:

```
<#root>
```

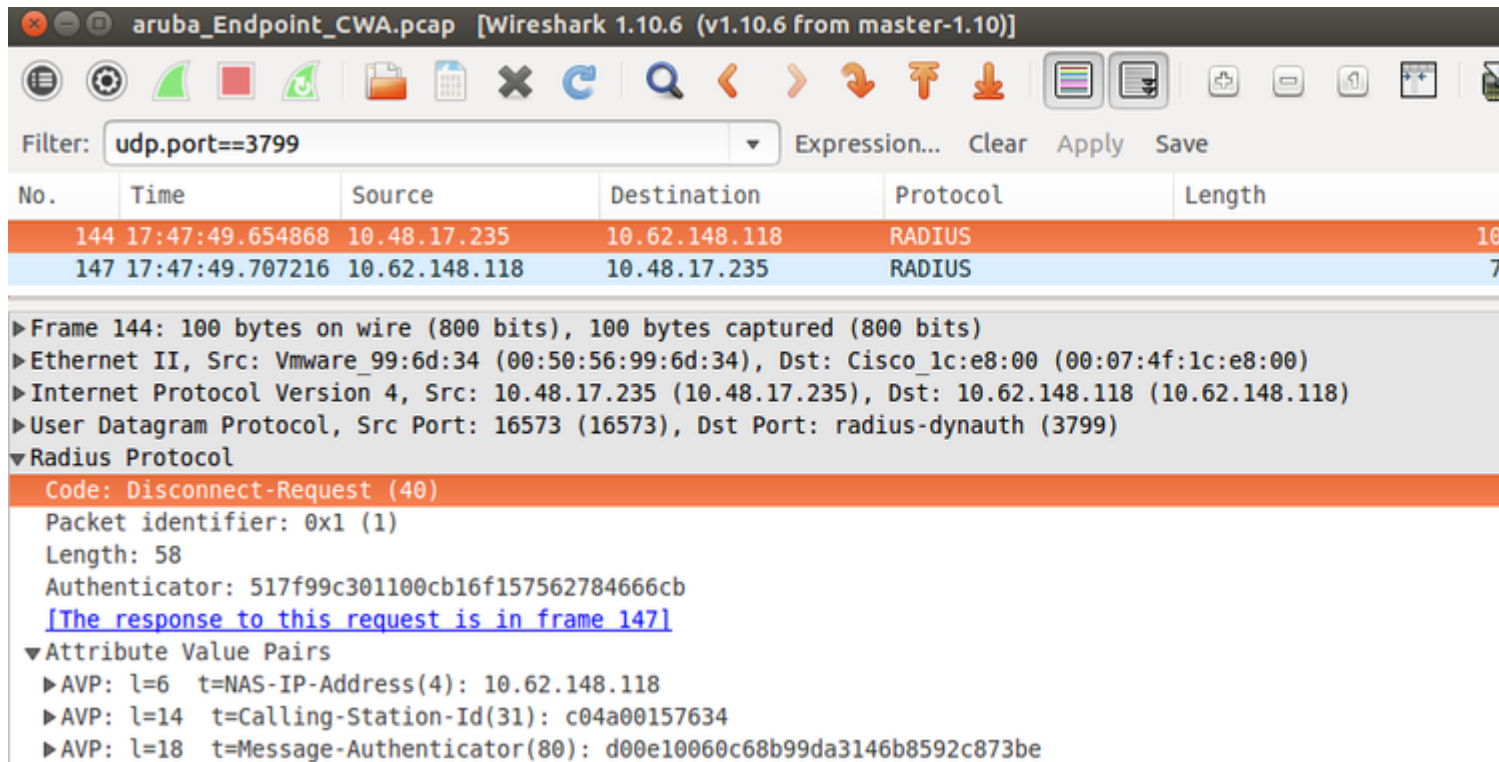
```
2015-11-02 18:47:49,737 DEBUG [Thread-147][] cisco.cpm.prvt.impl.PrRTLoggerImpl -:::::-
DynamicAuthorizationFlow,DEBUG,0x7fc0e9eb4700,cntx=0000000561,sesn=c59aa41a-e029-4ba0-a31b
-44549024315e,
```

```
CallingStationID=c04a00157634
```

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

```
Packet type 41(DisconnectACK).
```

Packet Capture met CoA, Diconnect-request (40) en Diconnect-ACK (41) wordt uitgevoerd zoals aangegeven op de afbeelding.



Opmerking: RFC CoA is gebruikt voor verificatie met betrekking tot Apparaatprofiel Aruba (standaardinstellingen). Voor verificatie met betrekking tot Cisco-apparaat zou het Cisco CoA-type opnieuw zijn geverifieerd.

Problemen oplossen

Deze sectie bevat informatie die u kunt gebruiken om problemen met de configuratie te troubleshooten.

Aruba Captive Portal met IP-adres in plaats van FQDN

Als Captive Portal op Aruba is geconfigureerd met IP-adres in plaats van FQDN van ISE, faalt PSN NSA:

```
<#root>
```

```
Warning - [HTTPConnection]
```

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

```
CN
```

De reden hiervoor is een strikte certificatsvalidatie wanneer u verbinding maakt met ISE. Wanneer u IP-adres gebruikt om verbinding te maken met ISE (als gevolg van een omleiding van URL met IP-adres in plaats van FQDN) en u een ISE-certificaat krijgt met onderwerpnaam = FQDN-validatie mislukt.

Opmerking: webbrowser gaat verder met BYOD portal (met waarschuwing die moet worden goedgekeurd door de gebruiker).

Aruba Captive Portal Onjuist toegangsbeleid

Standaard is Aruba Access-Policy geconfigureerd met Captive Portal voor TCP-poorten 80, 443 en 8080.

NSA kan geen verbinding maken met TCP-poort 8905 om een xml-profiel te verkrijgen van ISE. Deze fout wordt gerapporteerd:

```
<#root>
```

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

```
[
```

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

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

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

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

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

```
HTTP response code: 0
```

```
]
```

```
GetProfile - end
```

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

Aruba CoA poortnummer

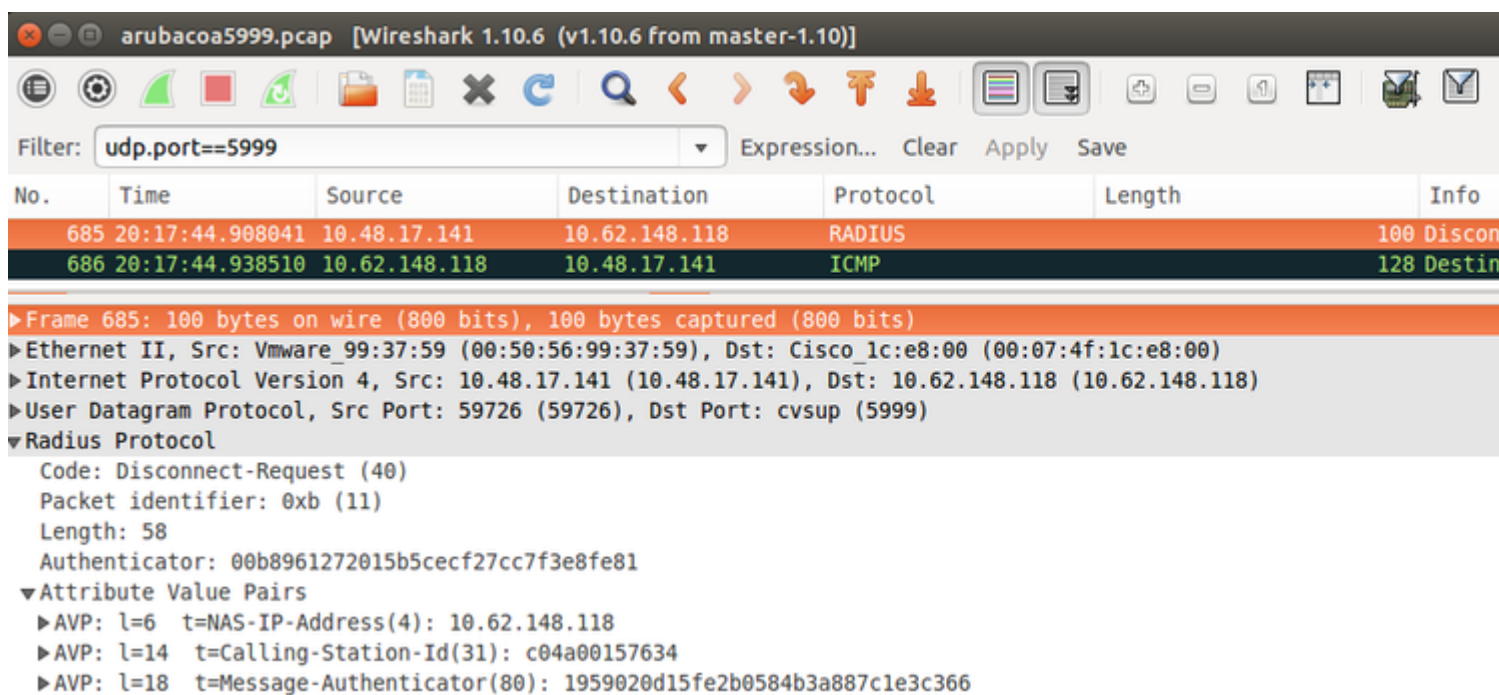
Aruba levert standaard het poortnummer voor CoA **Air Group CoA poort 5999**. Helaas reageerde Aruba 204 niet op dergelijke verzoeken (zoals getoond).

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

Packet-opname is zoals in de afbeelding.



De beste optie om hier te gebruiken kan CoA poort 3977 zijn zoals beschreven in RFC 5176.

Omleiding op sommige Aruba-apparaten

Op Aruba 3600 met v6.3 valt op dat de omleiding iets anders werkt dan op andere controllers. Packet Capture en uitleg zijn hier te vinden.

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 (tex
794	09:29:41.6982576	10.75.94.213	173.194.124.52	HTTP	63	GET /&arubalp=6b0512f
797	09:29:41.7563066	173.194.124.52	10.75.94.213	HTTP	485	HTTP/1.1 302 Temporar

<#root>

packet 1: PC is sending GET request to google.com
packet 2: Aruba is returning HTTP 200 OK with following content:
<meta http-equiv='refresh' content='1; url=http://www.google.com/

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

'>\n

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

http://www.google.com/

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

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

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

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

Gerelateerde informatie

- [Beheerdershandleiding voor Cisco Identity Services Engine, release 2.0](#)
- [Profielen voor netwerktoegangsapparaat met Cisco Identity Services Engine](#)
- [Technische ondersteuning en documentatie â€™ Cisco Systems](#)

Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document ([link](#)) te raadplegen.