

Konfigurieren der ISE 2.0-Drittanbieterintegration mit Aruba Wireless

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Herausforderungen durch Unterstützung von Drittanbietern](#)

[Sitzungen](#)

[URL-Umleitung](#)

[CoA](#)

[Lösung auf ISE](#)

[Cisco ISE](#)

[Schritt 1: Aruba Wireless Controller zu Netzwerkgeräten hinzufügen](#)

[Schritt 2: Autorisierungsprofil konfigurieren](#)

[Schritt 3: Autorisierungsregeln konfigurieren](#)

[Aruba AP](#)

[Schritt 1: Captive Portal-Konfiguration](#)

[Schritt 2: Radius-Serverkonfiguration](#)

[Schritt 3: SSID-Konfiguration](#)

[Überprüfen](#)

[Schritt 1: Verbindung mit SSID mgarcarz_aruba mit EAP-PEAP](#)

[Schritt 2: Umleitung des Web-Browser-Datenverkehrs für BYOD](#)

[Schritt 3: Ausführung des Network Setup Assistant](#)

[Weitere Datenflüsse und CoA-Unterstützung](#)

[CWA mit CoA](#)

[Fehlerbehebung](#)

[Captive Portal von Aruba mit IP-Adresse statt FQDN](#)

[Aruba Captive Portal: Falsche Zugriffsrichtlinie](#)

[Aruba CoA-Portnummer](#)

[Umleitung auf einigen Aruba Geräten](#)

[Zugehörige Informationen](#)

Einführung

In diesem Dokument wird die Fehlerbehebung für die Integration von Drittanbieterlösungen in die Cisco Identity Services Engine (ISE) beschrieben. Sie kann als Leitfaden für die Integration mit anderen Anbietern und Datenflüssen verwendet werden. ISE Version 2.0 unterstützt die Integration von Drittanbieterlösungen. Dies ist ein Konfigurationsbeispiel, in dem die Integration eines von Aruba IAP 204 verwalteten Wireless-Netzwerks mit ISE for Bring Your Own Device

(BYOD)-Services erläutert wird.

Hinweis: Beachten Sie, dass Cisco nicht für die Konfiguration oder den Support von Geräten anderer Anbieter verantwortlich ist.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Aruba IAP-Konfiguration
- BYOD-Datenflüsse auf der ISE
- ISE-Konfiguration für Kennwort- und Zertifikatsauthentifizierung

Verwendete Komponenten

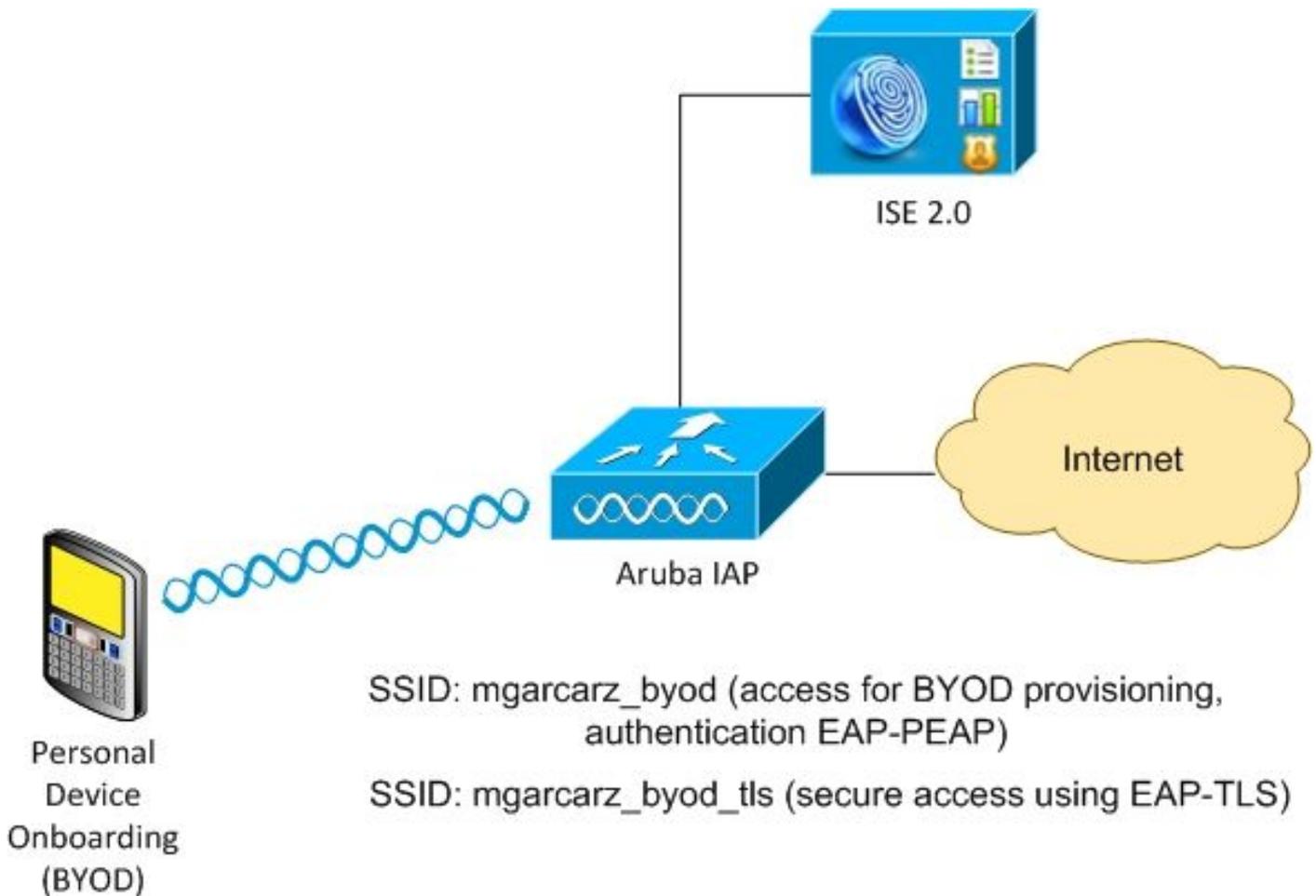
Die Informationen in diesem Dokument basieren auf den folgenden Softwareversionen:

- Aruba IAP 204 Software 6.4.2.3
- Cisco ISE, Version 2.0 und höher

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Konfigurieren

Netzwerkdiagramm



Es gibt zwei Wireless-Netzwerke, die vom Aruba AP verwaltet werden. Der erste (mgarcarz_byod) wird für den 802.1x Extensible Authentication Protocol-Protected EAP (EAP-PEAP)-Zugriff verwendet. Nach erfolgreicher Authentifizierung muss der Aruba Controller den Benutzer zum ISE BYOD-Portal - Native Supplicant Provisioning (NSP) Flow umleiten. Der Benutzer wird umgeleitet, die Anwendung Network Setup Assistant (NSA) wird ausgeführt, und das Zertifikat wird bereitgestellt und auf dem Windows-Client installiert. Für diesen Prozess wird die interne ISE-CA verwendet (Standardkonfiguration). Die NSA ist auch für die Erstellung eines Wireless-Profiles für den zweiten Service Set Identifier (SSID) verantwortlich, der von Aruba (mgarcarz_byod_tls) verwaltet wird. Dieser wird für die 802.1x Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)-Authentifizierung verwendet.

So können Benutzer privater Geräte integrieren und sicheren Zugriff auf das Unternehmensnetzwerk erhalten.

Dieses Beispiel kann problemlos für verschiedene Zugriffstypen geändert werden, z. B.:

- Central Web Authentication (CWA) mit BYOD-Service
- 802.1x-Authentifizierung mit Status und BYOD-Umleitung
- In der Regel wird für die EAP-PEAP-Authentifizierung Active Directory verwendet (um diesen Artikel kurz zu halten, interne ISE-Benutzer werden verwendet).
- In der Regel wird für die Zertifikatsbereitstellung ein externer SCEP-Server (Simple Certificate Enrollment Protocol) verwendet. In der Regel wird der Microsoft Network Device Enrollment Service (NDES) verwendet, um diesen Artikel kurz zu halten, die interne ISE-Zertifizierungsstelle.

Herausforderungen durch Unterstützung von Drittanbietern

Welche Herausforderungen ergeben sich bei der Verwendung von ISE-Gastdatenströmen (wie BYOD, CWA, NSP, Client Provisioning Portal (CPP)) mit Geräten von Drittanbietern?

Sitzungen

Cisco Network Access Devices (NAD) verwendet Radius cisco-av-pair, die als Audit-Session-ID bezeichnet wird, um den Authentication, Authorization, and Accounting (AAA)-Server über die Sitzungs-ID zu informieren. Dieser Wert wird von der ISE verwendet, um die Sitzungen nachzuverfolgen und die richtigen Services für jeden Datenfluss bereitzustellen. Andere Anbieter bieten keine Unterstützung für Cisco-av-Paare. Daher muss sich die ISE auf IETF-Attribute verlassen, die in Access-Request und Accounting-Request empfangen wurden.

Nachdem Sie Access-Request erhalten haben, erstellt die ISE synthetisierte Cisco Session-ID (von der Calling Station-ID, vom NAS-Port, von der NAS-IP-Adresse und vom gemeinsam genutzten geheimen Schlüssel). Dieser Wert hat nur eine lokale Bedeutung (nicht über das Netzwerk gesendet). Daher wird von jedem Datenfluss (BYOD, CWA, NSP, CPP) erwartet, dass korrekte Attribute hinzugefügt werden. Die ISE kann daher die Cisco Session-ID neu berechnen und eine Suche durchführen, um sie mit der richtigen Sitzung zu korrelieren und den Datenfluss fortzusetzen.

URL-Umleitung

Die ISE verwendet Radius cisco-av-pair, auch Url-Redirect und url-redirect-acl genannt, um die NAD darüber zu informieren, dass bestimmter Datenverkehr umgeleitet werden muss.

Andere Anbieter bieten keine Unterstützung für Cisco-av-Paare. Daher müssen diese Geräte in der Regel mit einer statischen Umleitungs-URL konfiguriert werden, die auf einen bestimmten Service (Authorization Profile) der ISE verweist. Sobald der Benutzer eine HTTP-Sitzung initiiert hat, werden diese NADs an die URL umgeleitet und außerdem zusätzliche Argumente (wie IP-Adresse oder MAC-Adresse) hinzugefügt, um die ISE die Identifizierung einer bestimmten Sitzung und die Fortsetzung des Datenflusses zu ermöglichen.

CoA

Die ISE verwendet Radius cisco-av-pair namens "Subscriber:Command", "Subscriber:reauthentication-type", um anzugeben, welche Aktionen NAD für eine bestimmte Sitzung ausführen muss. Andere Anbieter bieten keine Unterstützung für Cisco-av-Paare. In der Regel verwenden diese Geräte RFC CoA (3576 oder 5176) und eine der beiden definierten Meldungen:

- Disconnect-Anfrage (auch als "Packet of Disconnect" bezeichnet) - dass man die Sitzung trennt (sehr oft, um eine erneute Verbindung zu erzwingen)
- CoA-Push: Diese Push-Funktion dient zum transparenten Ändern des Sitzungsstatus ohne Verbindungstrennung (z. B. VPN-Sitzung und neue Zugriffskontrolllisten).

Die ISE unterstützt sowohl Cisco CoA mit cisco-av-pair als auch RFC CoA 3576/5176.

Lösung auf ISE

Zur Unterstützung von Drittanbietern führte die ISE 2.0 ein Konzept von Netzwerkgeräteprofilen ein, in dem das Verhalten bestimmter Anbieter beschrieben wird: Unterstützung von Sitzungen,

URL-Umleitung und CoA.

Autorisierungsprofile haben einen bestimmten Typ (Netzwerkgeräteprofil), und sobald die Authentifizierung erfolgt, wird das ISE-Verhalten von diesem Profil abgeleitet. So können Geräte anderer Anbieter problemlos über die ISE verwaltet werden. Die Konfiguration auf der ISE ist flexibel und ermöglicht die Anpassung oder Erstellung neuer Netzwerkgeräteprofile.

In diesem Artikel wird die Verwendung des Standardprofils für das Aruba Gerät dargestellt.

Weitere Informationen zur Funktion:

[Geräteprofile für den Netzwerkzugriff mit der Cisco Identity Services Engine](#)

Cisco ISE

Schritt 1: Aruba Wireless Controller zu Netzwerkgeräten hinzufügen

Navigieren Sie zu **Administration > Network Resources > Network Devices (Verwaltung > Netzwerkressourcen > Netzwerkgeräte)**. Wählen Sie das richtige Geräteprofil für den ausgewählten Anbieter aus. In diesem Fall: **ArubaWireless**. Stellen Sie sicher, dass Sie den **Shared Secret-** und **CoA-Port** wie in den Bildern gezeigt konfigurieren.

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

Falls kein Profil für den gewünschten Anbieter verfügbar ist, kann es unter **Administration > Network Resources > Network Device Profiles** konfiguriert werden.

Schritt 2: Autorisierungsprofil konfigurieren

Navigieren Sie zu **Richtlinien > Richtlinienelemente > Ergebnisse > Autorisierung > Autorisierungsprofile**, und wählen Sie das gleiche **Netzwerkgeräteprofil** aus wie in Schritt

1. **ArubaWireless**. Das konfigurierte Profil lautet **Aruba-redirect-BYOD** mit **BYOD-Portal** und wie in den Bildern gezeigt.

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

Fehlender Teil der Webumleitungskonfiguration, in der eine statische Verbindung zum Autorisierungsprofil generiert wird. Aruba unterstützt zwar keine dynamische Umleitung zum Gastportal, aber jedem Autorisierungsprofil wird ein Link zugewiesen, der auf Aruba konfiguriert und im Bild dargestellt wird.

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=10ImawmkleZQhapEvIXPAoELx>

Schritt 3: Autorisierungsregeln konfigurieren

Navigieren Sie zu **Richtlinien > Autorisierungsregeln**, und die Konfiguration wird wie im Bild gezeigt angezeigt.

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

Zunächst stellt der Benutzer eine Verbindung zu SSID mgarcarz_aruba her, und die ISE gibt das Authorization Profile Aruba-redirect-BYOD zurück, das den Client zum standardmäßigen BYOD-Portal umleitet. Nach Abschluss des BYOD-Prozesses stellt der Client eine Verbindung mit EAP-TLS her, und es wird der vollständige Zugriff auf das Netzwerk gewährt.

Aruba AP

Schritt 1: Captive Portal-Konfiguration

Um Captive Portal auf Aruba 204 zu konfigurieren, navigieren Sie zu **Security > External Captive Portal** und fügen Sie ein neues hinzu. Geben Sie diese Informationen für die korrekte Konfiguration und wie im Bild gezeigt ein.

- Typ: Radius-Authentifizierung
- IP- oder Hostname: ISE-Server
- URL: Link, der auf der ISE unter "Authorization Profile Configuration" (Konfiguration des Autorisierungsprofils) erstellt wird; Sie ist spezifisch für ein bestimmtes Autorisierungsprofil und kann hier unter der Web Redirection-Konfiguration gefunden werden.

Native Supplicant Provisioning Value

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

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

- Port: Portnummer, auf der das ausgewählte Portal auf der ISE gehostet wird (standardmäßig: 8443), wie im Bild gezeigt.

mgarcarz_ise20

Type:

IP or hostname:

URL:

Port:

Use https:

Captive Portal failure:

Automatic URL Whitelisting:

Redirect URL: (optional)

Schritt 2: Radius-Serverkonfiguration

Navigieren Sie zu **Security > Authentication Servers (Sicherheit > Authentifizierungsserver)**, um sicherzustellen, dass der CoA-Port mit dem auf der ISE konfigurierten Port identisch ist, wie im Bild gezeigt. (auf Aruba 204 ist er standardmäßig auf 5999 festgelegt, dies entspricht jedoch nicht dem RFC 5176 und funktioniert auch nicht mit der 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"/>

Schritt 3: SSID-Konfiguration

- Die Registerkarte Sicherheit wird im Bild angezeigt.

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:

- Registerkarte Zugriff: Wählen Sie **Network-Based Access Rule (Netzwerkbasierte Zugriffsregel)**, um das Captive Portal auf der SSID zu konfigurieren.

Verwenden Sie das Captive Portal, das in Schritt 1 konfiguriert wurde. Klicken Sie auf **Neu**, wählen Sie Regeltyp: **Captive Portal**, Splash page type: **Extern** wie im Bild dargestellt.

Access Rules

More Control

Network-based

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

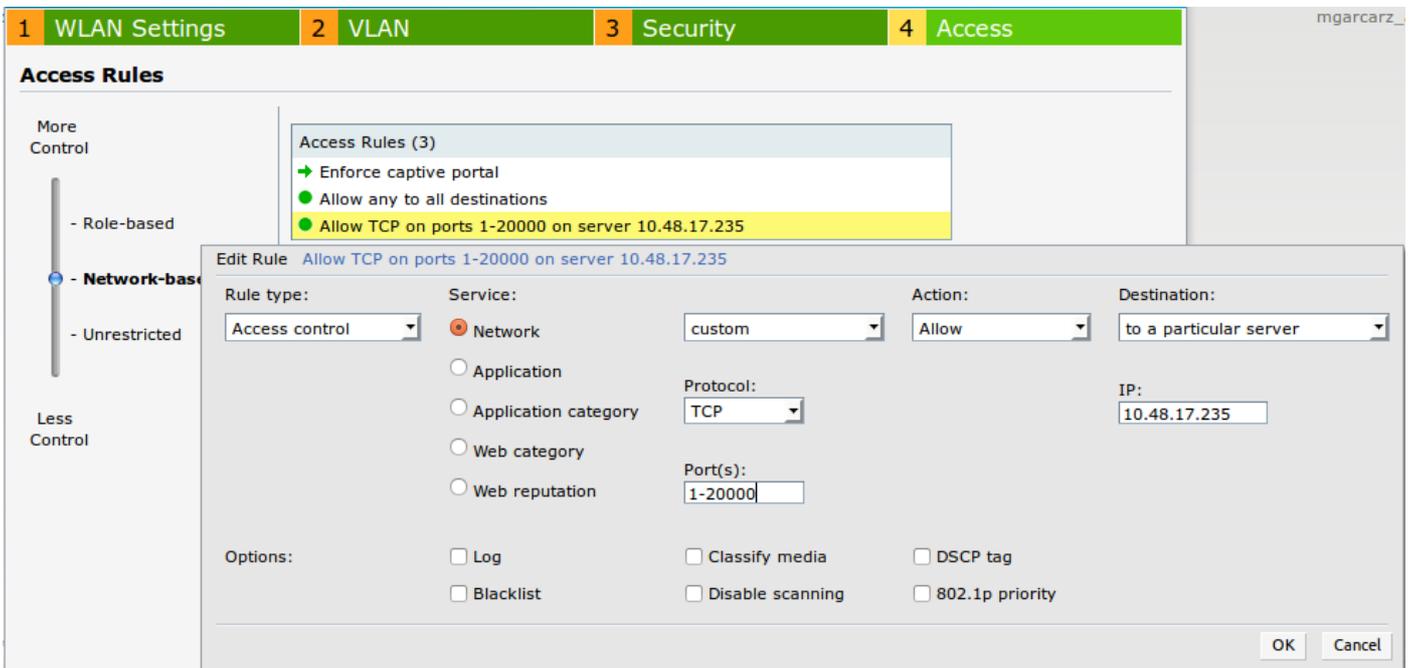
Edit Rule Enforce captive portal

Rule type: Captive portal

Splash page type: External

Captive portal profile: mgarcarz_ise20 Edit

Darüber hinaus sollte der gesamte Datenverkehr zum ISE-Server zugelassen werden (TCP-Ports im Bereich 1-2000), während die Regel auf Aruba standardmäßig konfiguriert ist: **Lassen Sie alle Ziele** scheint nicht richtig funktionieren, wie im Bild gezeigt.



Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Schritt 1: Verbindung mit SSID mgarcarz_aruba mit EAP-PEAP

Das erste Authentifizierungsprotokoll auf der ISE wird angezeigt. Es wurden Standard-Authentifizierungsrichtlinien verwendet, das Autorisierungsprofil Aruba-redirect-BYOD wurde wie im Bild gezeigt zurückgegeben.

Time	Status	Det...	R.	Identity	Endpoint ID	Authentication Policy	Authorization Policy	Authorization Profiles	Network Device	Event
2015-10-29 22:23:37...				0 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

ISE gibt RADIUS Access-Accept-Nachricht mit EAP Success zurück. Beachten Sie, dass keine weiteren Attribute zurückgegeben werden (keine Cisco av-pair url-redirect oder url-redirect-acl), wie im Bild gezeigt.

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	04BD88888142-C04A00146E31-42F8
153	10.48.17.235	10.62.148.118	RADIUS	62	Accounting-Response(5) (id=108, l=20)		

```

Packet identifier: 0xb (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 berichtet, dass die Sitzung eingerichtet ist (EAP-PEAP-Identität ist **cisco**) und dass die ausgewählte Rolle **mgarcarz_aruba** ist, wie im Bild gezeigt.



Diese Rolle ist für die Umleitung zur ISE (Captive Portal Funktionalität auf Aruba) zuständig.

In der Aruba CLI kann der aktuelle Autorisierungsstatus für diese Sitzung bestätigt werden:

```

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#

```

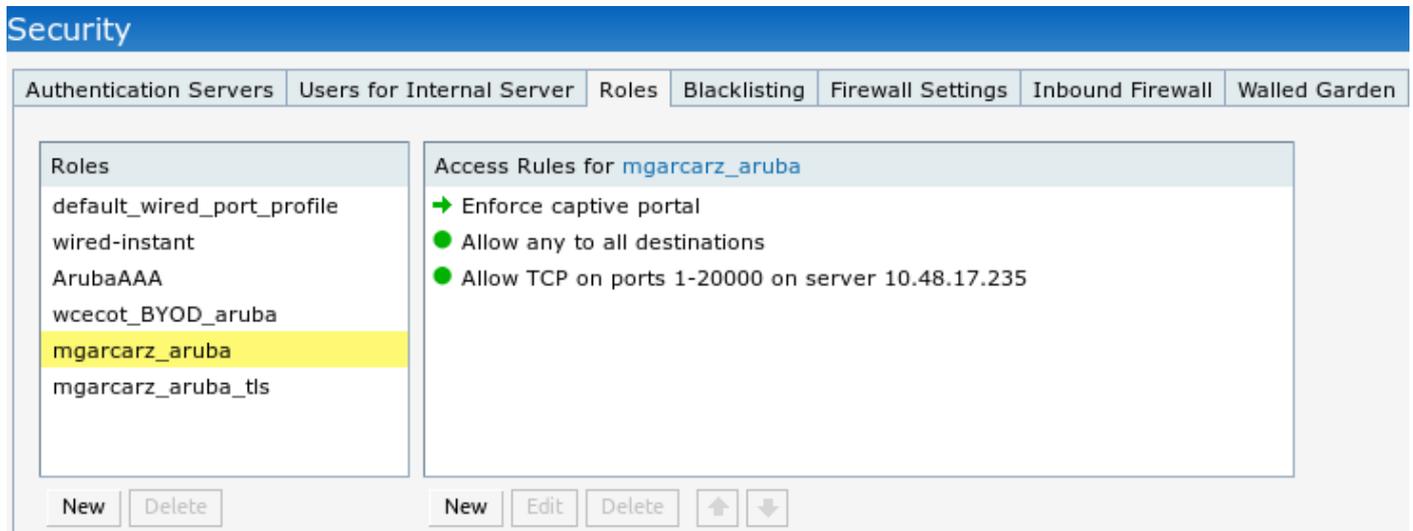
Um die ACL-ID 138 auf die aktuellen Berechtigungen zu überprüfen, gehen Sie folgendermaßen vor:

```

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 ... >

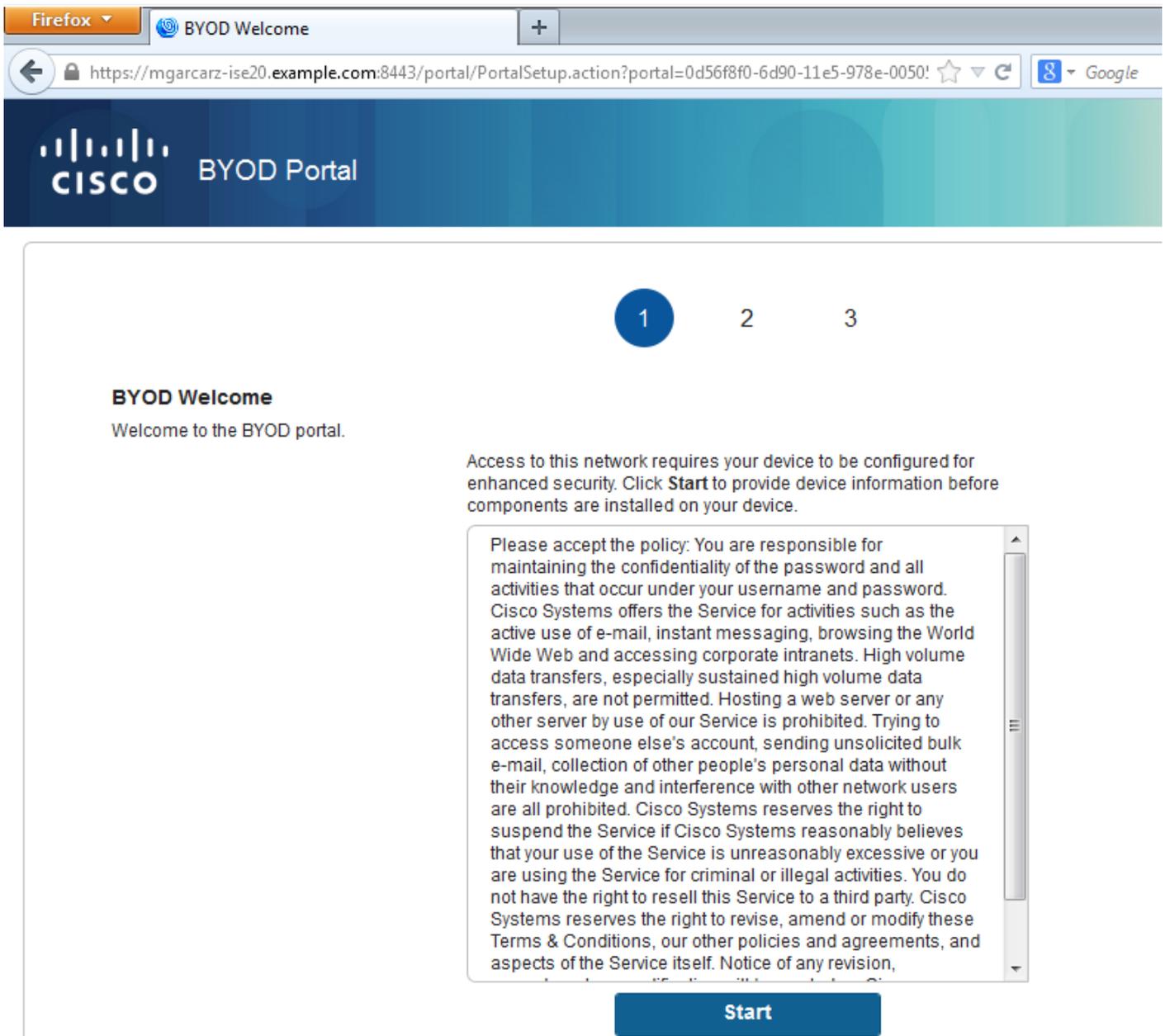
```

Dies entspricht der Konfiguration in der GUI für diese Rolle, wie im Bild gezeigt.



Schritt 2: Umleitung des Web-Browser-Datenverkehrs für BYOD

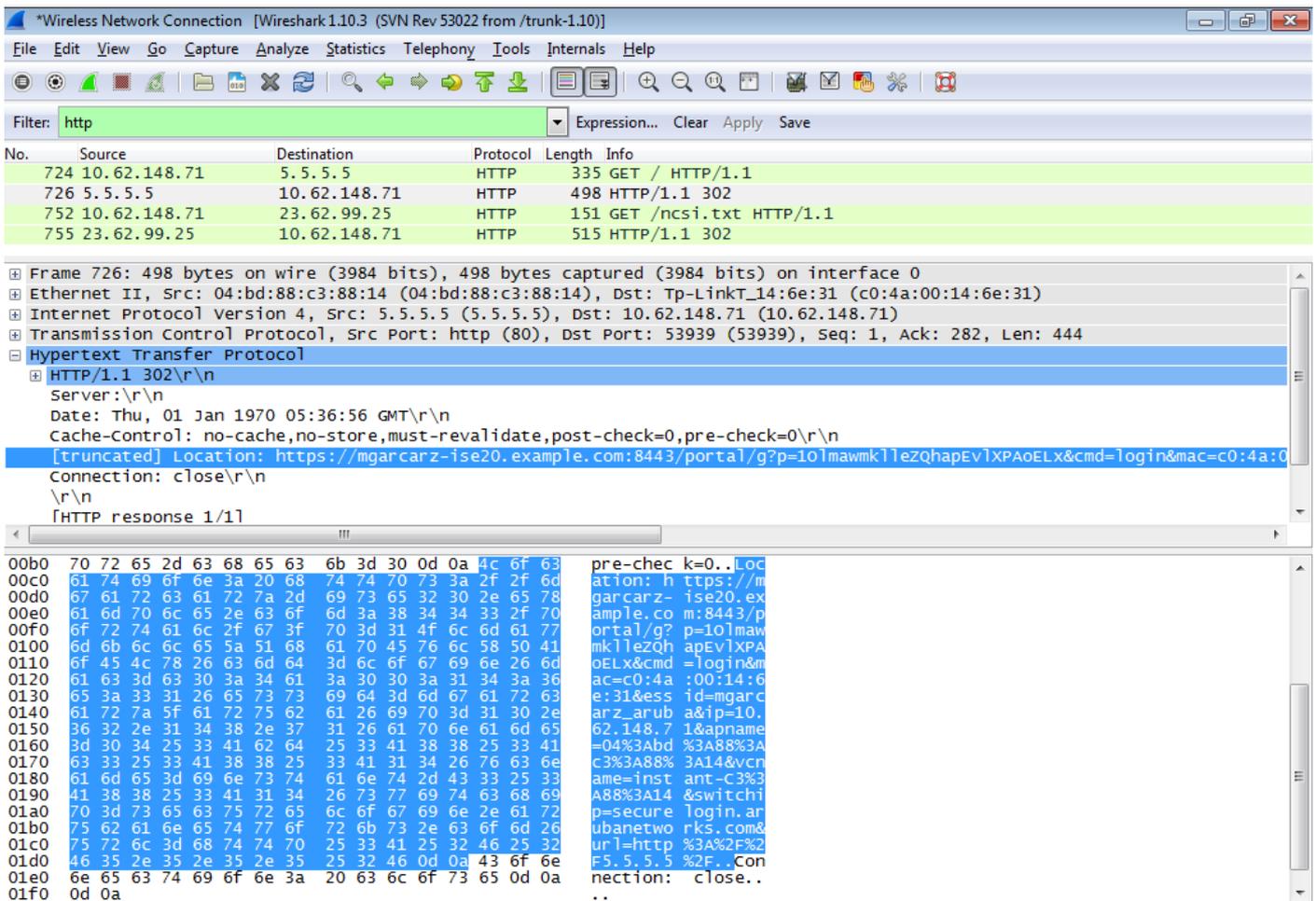
Sobald der Benutzer den Webbrowser öffnet und eine beliebige Adresse eingibt, erfolgt die Umleitung wie im Bild gezeigt.



Wenn man sich die Paketerfassungen anschaut, wird bestätigt, dass Aruba das Ziel (5.5.5.5) spuckt und die HTTP-Umleitung an die ISE zurückgibt.

Beachten Sie, dass es sich um dieselbe statische URL handelt, die in der ISE konfiguriert und auf Aruba in das Captive Portal kopiert wurde. Es werden jedoch zusätzlich mehrere Argumente wie folgt und wie im Bild gezeigt hinzugefügt:

- cmd = Anmeldung
- MAC = c0:4a:00:14:6e:31
- essig = mgarcarz_aruba
- ip = 10,62,148,7
- apname = 4bd88c38814 (mac)
- url = <http://5.5.5.5>



Aus diesen Gründen kann die ISE die Cisco Session ID neu erstellen, die entsprechende Sitzung auf der ISE ermitteln und den BYOD-Fluss (oder einen anderen konfigurierten) fortsetzen. Für Cisco Geräte wird `audit_session_id` normalerweise verwendet, dies wird jedoch von anderen Anbietern nicht unterstützt.

Um zu bestätigen, dass aus ISE-Debuggen der Wert für die Audit-Session-ID (der nie über das Netzwerk gesendet wird) angezeigt wird:

```
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:
```

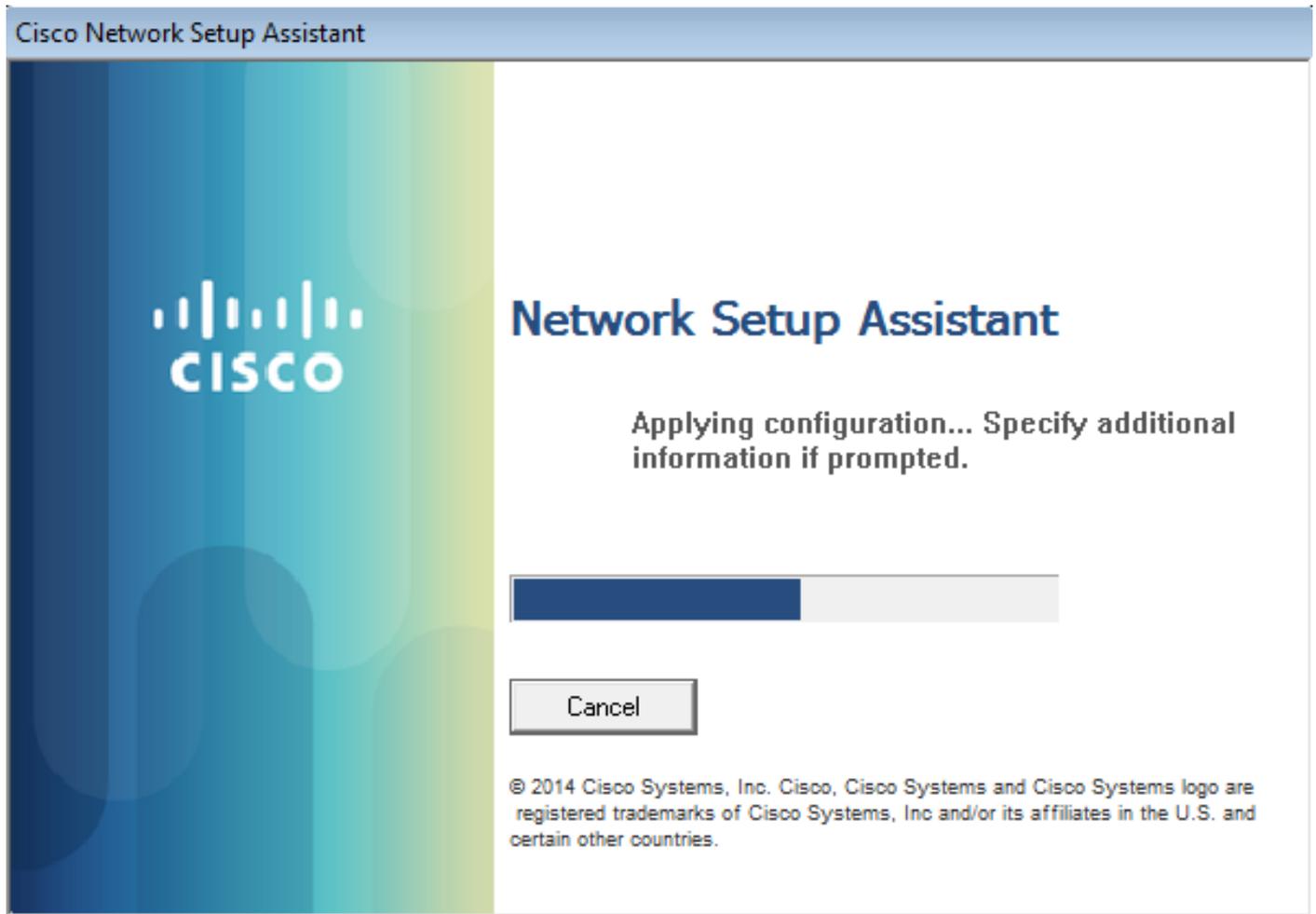
```
audit-session-id=0a3011ebXbiuDA3yUNoLUvtCRyuPFxkqYJ7TT06foOZ7G1HXj1M
```

Die Korrelation dieser Daten nach der Registrierung des Geräts auf BYOD Seite 2:

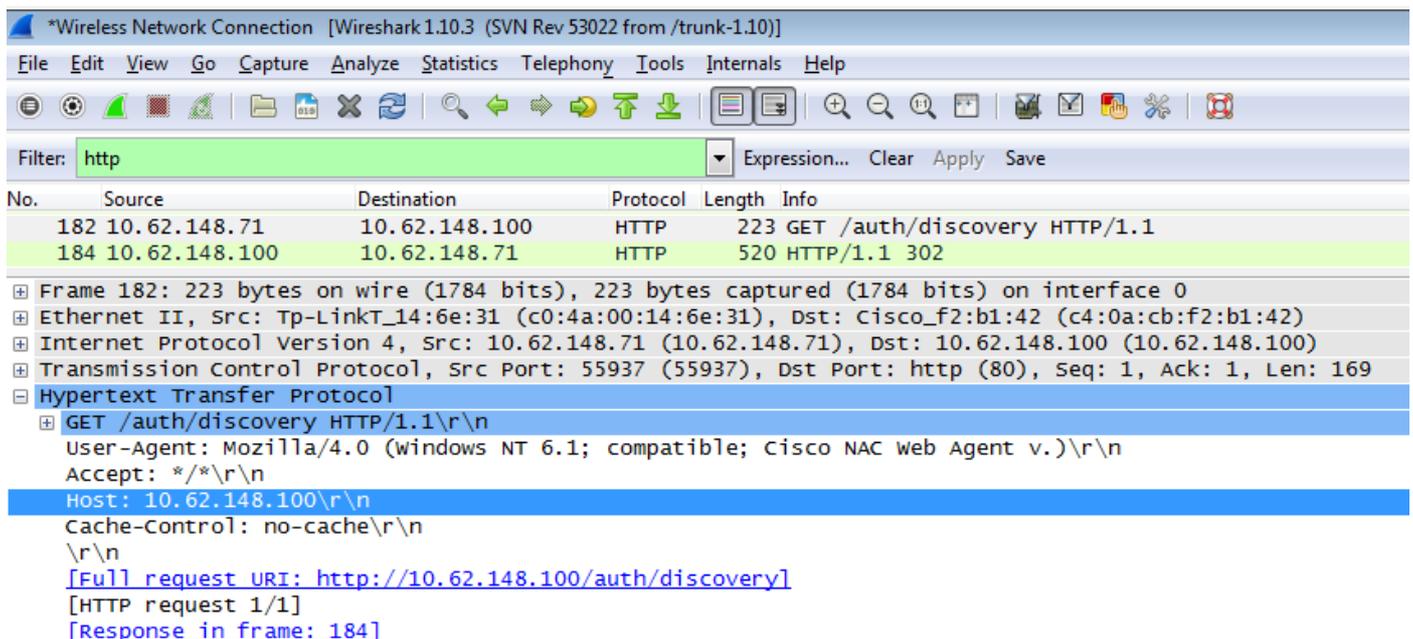
```
AcsLogs,2015-10-29 23:25:48,538,DEBUG,0x7fc0b39a4700,cntx=0000032947,CallingStationID=c04a00146e31,FramedIPAddress=10.62.148.71,Log_Message=[2015-10-29 23:25:48.533 +01:00 0000011874 88010 INFO MyDevices: Successfully registered/provisioned the device (endpoint), ConfigVersionId=145, UserName=cisco, 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, EPIdentityGroup=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
```

Bei nachfolgenden Anfragen wird der Client an BYOD Seite 3 umgeleitet. wo NSA heruntergeladen und ausgeführt wird.

Schritt 3: Ausführung des Network Setup Assistant



Die NSA hat die gleiche Aufgabe wie der Webbrowser. Zunächst muss die IP-Adresse der ISE ermittelt werden. Dies wird durch HTTP-Umleitung erreicht. Da dieser Benutzer jedoch nicht die Möglichkeit hat, IP-Adresse einzugeben (wie im Webbrowser), wird dieser Datenverkehr automatisch generiert. Das Standard-Gateway wird verwendet (auch **enroll.cisco.com** kann verwendet werden), wie im Bild gezeigt.



Die Antwort entspricht genau der des Webbrowsers. Auf diese Weise kann die NSA eine

Verbindung zur ISE herstellen, ein XML-Profil mit Konfiguration abrufen, SCEP-Anfragen generieren, an die ISE senden, ein signiertes Zertifikat (signiert von der internen ISE-CA) erhalten, das Wireless-Profil konfigurieren und schließlich eine Verbindung zum konfigurierten SSID herstellen. Protokollierung vom Client abrufen (unter Windows ist in %temp%/spwProfile.log). Aus Gründen der Klarheit werden einige Ausgaben weggelassen:

```
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 result: 0
GetProfilePath: searched path = C:\Users\ADMINI~1.EXA\AppData\Local\Temp\Low for file name =
spwProfile.xml result: 0
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:
0a3011ebXbiuDA3yUNoLUvtCRyuPFxkqYJ7TT06foOZ7G1HXj1M]
DiscoverISE - end
Successfully Discovered ISE: mgarcarz-ise20.example.com, session id:
0a3011ebXbiuDA3yUNoLUvtCRyuPFxkqYJ7TT06foOZ7G1HXj1M, macAddress: C0-4A-00-14-6E-31

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:MAC]
set ChallengePwd

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

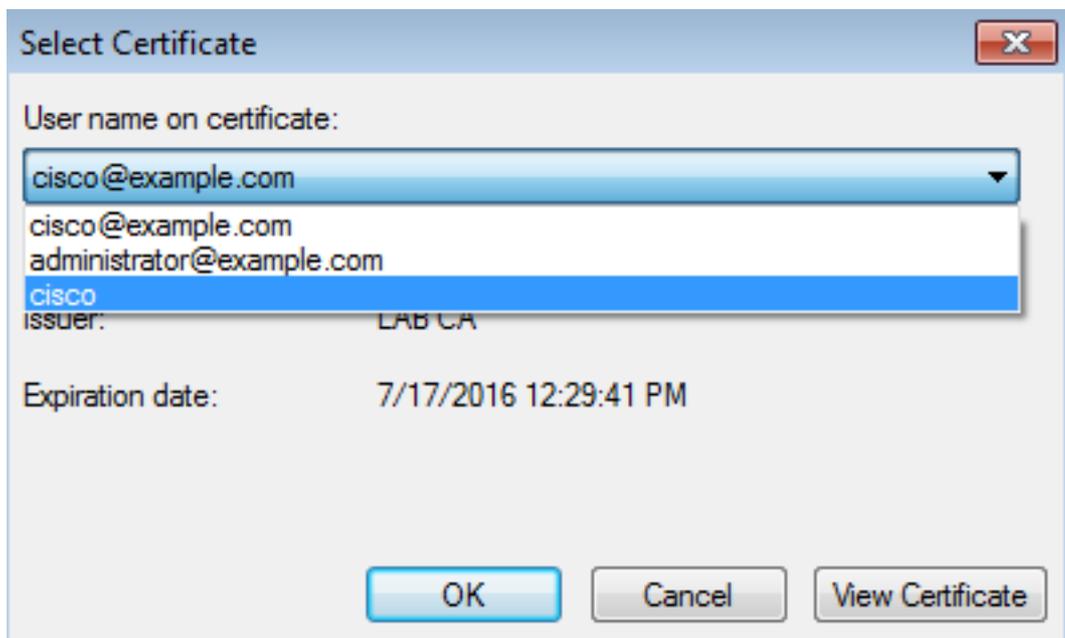
Configuring wireless profiles...
Configuring ssid [mgarcarz_aruba_tls]
WirelessProfile::SetWirelessProfile - Start
```

```
Wireless profile: [mgarcarz_aruba_tls] configured successfully
Connect to SSID
Successfully connected profile: [mgarcarz_aruba_tls]
WirelessProfile::SetWirelessProfile. - End
```

Diese Protokolle entsprechen genau den BYOD-Prozessen bei Cisco Geräten.

Hinweis: Radius CoA ist hier nicht erforderlich. Die Anwendung (NSA) erzwingt die Neuverbindung zu einer neu konfigurierten SSID.

In dieser Phase kann der Benutzer sehen, dass das System versucht, eine Verbindung zu einer endgültigen SSID herzustellen. Wenn Sie über mehr als ein Benutzerzertifikat verfügen, müssen Sie das entsprechende Benutzerzertifikat wie im Bild gezeigt auswählen.



Nach erfolgreicher Verbindung werden die NSA-Berichte wie im Bild gezeigt angezeigt.



Network Setup Assistant



Your device is now configured for secure access to the 'mgarcarz_aruba_tls' network.

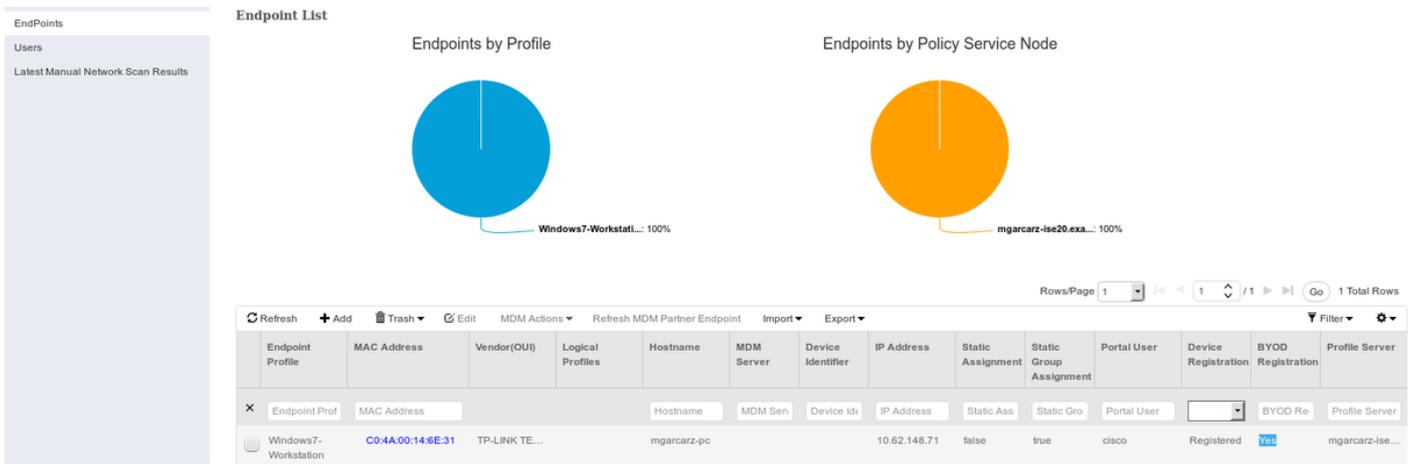
Exit

© 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.

Dies kann auf der ISE bestätigt werden. Das zweite Protokoll trifft auf die EAP-TLS-Authentifizierung, die alle Bedingungen für Basic_Authenticated_Access (EAP-TLS, Employee und BYOD Registered true) erfüllt, wie im Bild gezeigt.

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	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

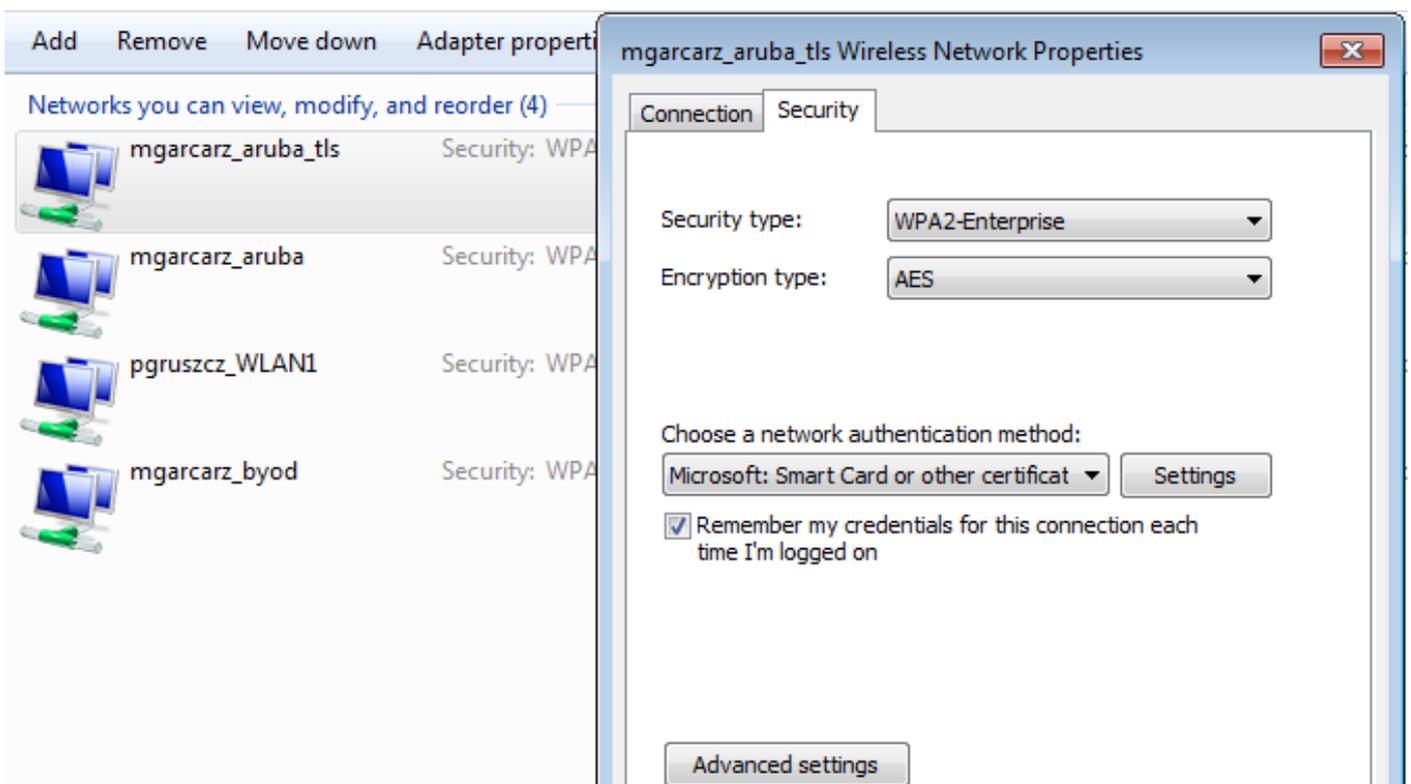
Die Ansicht der Endgeräteidentität kann auch bestätigen, dass das Flag BYOD Registered auf true festgelegt ist, wie im Bild gezeigt.



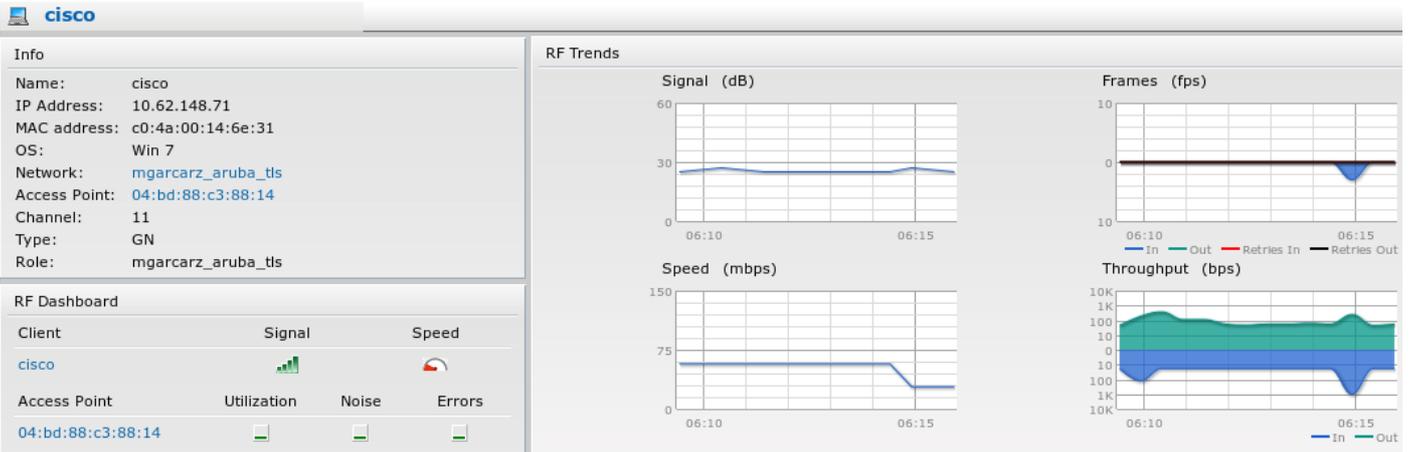
Auf dem Windows-PC wurde automatisch ein neues Wireless-Profil erstellt (und für EAP-TLS konfiguriert), wie im Bild gezeigt.

Manage wireless networks that use (Wireless Network Connection)

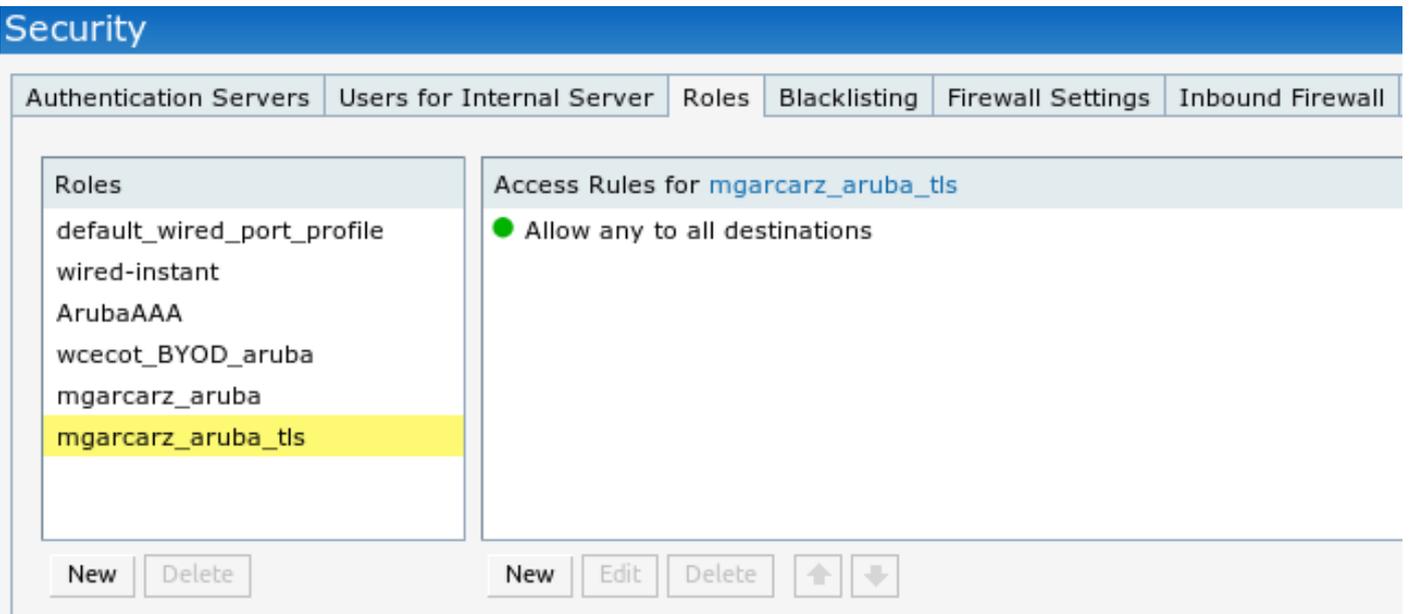
Windows tries to connect to these networks in the order listed below.



In dieser Phase bestätigt Aruba, dass der Benutzer mit der endgültigen SSID verbunden ist, wie im Bild gezeigt.



Die Rolle, die automatisch erstellt wird und die gleiche Bezeichnung wie das Netzwerk trägt, bietet vollständigen Netzwerkzugriff, wie im Bild gezeigt.



Weitere Datenflüsse und CoA-Unterstützung

CWA mit CoA

Während im BYOD-Fluss keine CoA-Meldungen vorhanden sind, wird der CWA-Fluss mit dem selbst registrierten Gastportal hier gezeigt:

Die konfigurierten Autorisierungsregeln sind im Bild dargestellt.

<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

Der Benutzer stellt über MAB-Authentifizierung eine Verbindung zum SSID her. Wenn er versucht, eine Verbindung zu einer Webseite herzustellen, wird eine Umleitung zum selbst registrierten Gastportal durchgeführt, in dem der Gast wie im Bild gezeigt ein neues Konto erstellen oder ein aktuelles Konto verwenden kann.



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?](#)

Nachdem der Gast erfolgreich verbunden wurde, wird eine CoA-Nachricht von der ISE an das Netzwerkgerät gesendet, um den Autorisierungsstatus wie im Bild gezeigt zu ändern.



Sponsored Guest Portal

Welcome Message

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

You're very close to gaining network access.

Continue

Sie kann unter **Operations > Authentifications (Vorgänge > Autorisierungen)** und wie im Bild gezeigt überprüft werden.

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

CoA-Nachricht in ISE-Debuggen:

```
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.prrt.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=0a3011ebisZXypODwqjB6j64GeFiF7RwvyocneEial7ckjtU1HI.,DynamicAuthorizationFlow.cpp:708
2015-11-02 18:47:49,584 DEBUG [Thread-137][] cisco.cpm.prrt.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.prrt.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.prrt.impl.PrRTLoggerImpl -:::--
DynamicAuthorizationFlow,DEBUG,0x7fc0e9cb2700,cntx=0000000561,sesn=c59aa41a-e029-4ba0-a31b-44549024315e,CallingStationID=c04a00157634,[DynamicAuthorizationFlow::onLocalHttpEvent]:
invoking DynamicAuthorization,DynamicAuthorizationFlow.cpp:246

```

und Disconnect-ACK von Aruba:

```

2015-11-02 18:47:49,737 DEBUG [Thread-147][] cisco.cpm.prrt.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

```

Die Paketerfassung mit CoA Diconnect-Request (40) und Diconnect-ACK (41) ist im Bild dargestellt.

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_Ic: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

Hinweis: RFC CoA wurde für die Authentifizierung im Zusammenhang mit dem Geräteprofil Aruba (Standardeinstellungen) verwendet. Für die Authentifizierung in Bezug auf Cisco Geräte wäre eine erneute Authentifizierung des Cisco CoA-Typs gewesen.

Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration

verwenden können.

Captive Portal von Aruba mit IP-Adresse statt FQDN

Wenn das Captive Portal auf Aruba mit einer IP-Adresse anstelle eines FQDN der ISE konfiguriert ist, schlägt die PSN NSA fehl:

```
Warning - [HTTPConnection] Abort the HTTP connection due to invalid certificate  
CN
```

Der Grund hierfür ist eine strikte Zertifikatsvalidierung, wenn Sie eine Verbindung zur ISE herstellen. Wenn Sie die IP-Adresse verwenden, um eine Verbindung zur ISE herzustellen (als Ergebnis einer Umleitungs-URL mit IP-Adresse anstatt FQDN) und ein ISE-Zertifikat mit dem Betreffnamen = FQDN-Validierung angezeigt wird, schlägt fehl.

Hinweis: Webbrowser setzt BYOD-Portal fort (mit Warnung, die vom Benutzer genehmigt werden muss).

Aruba Captive Portal: Falsche Zugriffsrichtlinie

Standardmäßig ist für die Aruba Access-Policy, die mit Captive Portal konfiguriert ist, die TCP-Ports 80, 443 und 8080 zulässig.

Die NSA kann keine Verbindung mit dem TCP-Port 8905 herstellen, um ein XML-Profil von der ISE zu erhalten. Dieser Fehler wird gemeldet:

```
Failed to get spw profile url using - url  
[https://mgarcarz-ise20.example.com:8905/auth/provisioning/evaluate?  
typeHint=SPWConfig&referrer=Windows&mac_address=C0-4A-00-14-6E-31&spw_version=  
1.0.0.46&session=0a3011ebXbiuDA3yUNoLUvtCRyuPFxkqYJ7TT06foOZ7G1HXj1M&os=Windows All]  
- http Error: [2] HTTP response code: 0]  
GetProfile - end  
Failed to get profile. Error: 2
```

Aruba CoA-Portnummer

Standardmäßig stellt Aruba die Portnummer für den CoA **Air Group CoA-Port** 5999 bereit. Leider antwortete Aruba 204 nicht auf solche Anfragen, wie im Bild gezeigt.

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

Die Paketerfassung wird im Bild gezeigt.

arubacoa5999.pcap [Wireshark 1.10.6 (v1.10.6 from master-1.10)]

Filter: `udp.port==5999` Expression... Clear Apply Save

No.	Time	Source	Destination	Protocol	Length	Info
685	20:17:44.908041	10.48.17.141	10.62.148.118	RADIUS	100	Disconnect-Request(40) (id=11, l=58)
686	20:17:44.938510	10.62.148.118	10.48.17.141	ICMP	128	Destination unreachable (Port unreachable)

▶ Frame 685: 100 bytes on wire (800 bits), 100 bytes captured (800 bits)

▶ Ethernet II, Src: Vmware_99:37:59 (00:50:56:99:37:59), Dst: Cisco_1c:e8:00 (00:07:4f:1c:e8:00)

▶ Internet Protocol Version 4, Src: 10.48.17.141 (10.48.17.141), Dst: 10.62.148.118 (10.62.148.118)

▶ User Datagram Protocol, Src Port: 59726 (59726), Dst Port: cvsup (5999)

▼ RADIUS Protocol

- Code: Disconnect-Request (40)
- Packet identifier: 0xb (11)
- Length: 58
- Authenticator: 00b8961272015b5cecf27cc7f3e8fe81
- ▼ 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): 1959020d15fe2b0584b3a887c1e3c366

Die beste Option für diese Option ist der CoA-Port 3977, wie in RFC 5176 beschrieben.

Umleitung auf einigen Aruba Geräten

Bei Aruba 3600 mit v6.3 ist festzustellen, dass die Umleitung etwas anders funktioniert als bei anderen Controllern. Die Paketerfassung und -erklärungen finden Sie hier und wie im Bild gezeigt.

770	09:29:40.5119116	10.75.94.213	173.194.124.52	HTTP	1373	GET / HTTP/1.1
772	09:29:40.5218656	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

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?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%2Egoogle%2Ecom%2F
```

Zugehörige Informationen

- [Administratoranleitung für Cisco Identity Services Engine, Version 2.0](#)
- [Geräteprofile für den Netzwerkzugriff mit der Cisco Identity Services Engine](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)