Konfigurieren der Integration von Drittanbieterlösungen mit ISE 2.0 mit Aruba Wireless

Inhalt

Einleitung

In diesem Dokument wird die Fehlerbehebung bei der Integrationsfunktion von Drittanbietern auf der Cisco Identity Services Engine (ISE) beschrieben.

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

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Aruba IAP-Konfiguration
- BYOD fließt über die ISE
- ISE-Konfiguration für Passwort- und Zertifikatsauthentifizierung

Verwendete Komponenten

In diesem Dokument wird die Fehlerbehebung bei der Integrationsfunktion von Drittanbietern auf der Cisco Identity Services Engine (ISE) beschrieben.

Sie kann als Leitfaden für die Integration mit anderen Anbietern und für Flows verwendet werden. ISE Version 2.0 unterstützt die Integration von Drittanbieterlösungen.

In diesem Konfigurationsbeispiel wird die Integration des vom Aruba IAP 204 verwalteten Wireless-Netzwerks in die ISE für BYOD-Services (Bring Your Own Device) erläutert.

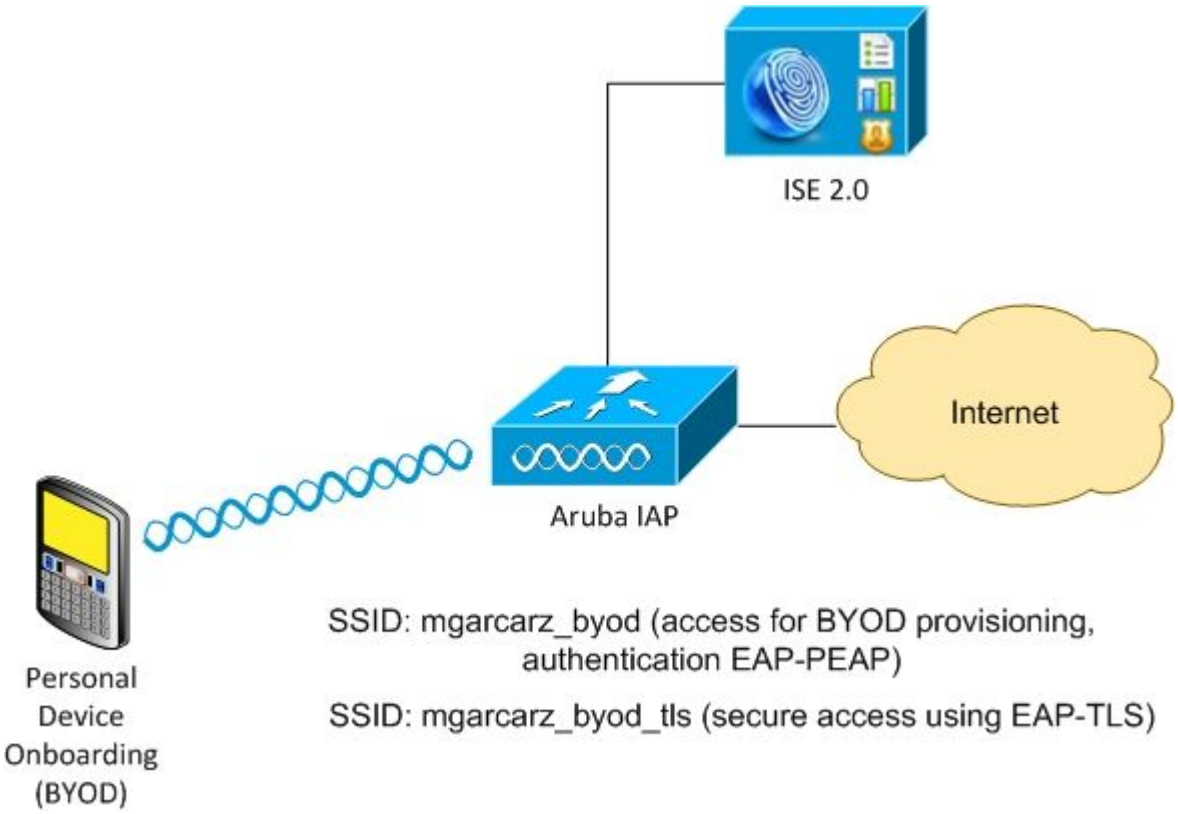
Die Informationen in diesem Dokument basieren auf folgenden Software-Versionen:

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

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

Netzwerkdiagramm



Es gibt zwei Wireless-Netzwerke, die von Aruba AP verwaltet werden.

Das erste Modul (mgarcarz_byod) wird für den EAP-Zugriff (Extensible Authentication Protocol-Protected EAP) nach dem 802.1x-Standard verwendet.

Nach erfolgreicher Authentifizierung muss der Aruba Controller den Benutzer an den ISE BYOD-Portal-Fluss - Native Supplicant Provisioning (NSP) - 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 eine interne ISE-CA verwendet (Standardkonfiguration).

Die NSA ist außerdem für die Erstellung eines Wireless-Profils für die zweite von Aruba verwaltete Service Set Identifier (SSID) (mgarcarz_byod_tls) verantwortlich, die für die 802.1x Extensible Authentication Protocol-Transport Layer Security (EAP-TLS)-Authentifizierung verwendet wird.

So können Benutzer im Unternehmen ihre privaten Geräte integrieren und sicheren Zugriff auf das Unternehmensnetzwerk erhalten.

Dieses Beispiel kann für verschiedene Zugriffsarten leicht geändert werden. Beispiel:

- Zentrale Web-Authentifizierung (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, werden interne ISE-Benutzer verwendet).
- In der Regel wird für die Zertifikatbereitstellung ein externer SCEP-Server (Simple Certificate Enrollment Protocol) verwendet, in der Regel der Microsoft Network Device Enrollment Service (NDES), um diesen Artikel kurz zu halten. Es wird eine interne ISE-Zertifizierungsstelle verwendet.

Herausforderungen bei der Unterstützung von Drittanbietern

Es gibt eine Reihe von Herausforderungen, wenn Sie ISE-Guest-Flows (wie BYOD, CWA, NSP, Client Provisioning Portal (CPP)) mit Drittanbietergeräten nutzen.

Sitzungen

Cisco Network Access Devices (NAD) verwendet Radius cisco-av-pair called audit-session-id, um den AAA-Server (Authentication, Authorization, and Accounting) über die Sitzungs-ID zu informieren.

Dieser Wert wird von der ISE verwendet, um die Sitzungen nachzuverfolgen und die richtigen Services für die einzelnen Datenflüsse bereitzustellen. Andere Anbieter bieten keine Unterstützung für cisco-av pair.

ISE muss sich auf IETF-Attribute verlassen, die in Access-Request und Accounting Request eingegangen sind.

Nachdem Sie die Zugriffsanfrage erhalten haben, erstellt die ISE eine synthetisierte Cisco Session-ID (aus Calling-Station-ID, NAS-Port, NAS-IP-Adresse und Shared Secret). Dieser Wert hat nur eine lokale Bedeutung (wird nicht über das Netzwerk gesendet).

Aus diesem Grund wird von jedem Fluss (BYOD, CWA, NSP, CPP) erwartet, dass richtige 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 Fluss fortzusetzen.

URL-Umleitung

Die ISE verwendet Radius cisco-av-pair called url-redirect and url-redirect-acl, um der NAD mitzuteilen, dass bestimmter Datenverkehr umgeleitet werden muss.

Andere Anbieter bieten keine Unterstützung für cisco-av pair. In der Regel müssen diese Geräte mit einer statischen Umleitungs-URL konfiguriert werden, die auf einen bestimmten Service (Autorisierungsprofil) auf der ISE verweist.

Sobald der Benutzer eine HTTP-Sitzung initiiert hat, leiten diese NADs zur URL um und fügen zusätzliche Argumente (wie IP-Adresse oder MAC-Adresse) an, damit die ISE eine bestimmte Sitzung identifizieren und den Fluss fortsetzen kann.

CoA

Die ISE verwendet Radius cisco-av-pair mit dem Namen Subscriber:command, Subscriber:reAuthenticate-type, um anzugeben, welche Aktionen NAD für eine bestimmte Sitzung ausführen muss.

Andere Anbieter bieten keine Unterstützung für cisco-av pair. In der Regel verwenden diese Geräte RFC-CoA (3576 oder 5176) und eine der beiden definierten Meldungen:

- disconnect-Anfrage (auch als Paket von disconnect bezeichnet) - dass eine zum Trennen der Sitzung verwendet wird (sehr oft, um eine erneute Verbindung zu erzwingen)
- CoA-Push - dieser dient dazu, den Sitzungsstatus transparent und ohne Trennung der Verbindung zu ändern (z. B. VPN-Sitzung und Anwendung einer neuen ACL).

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

Lösung auf der ISE

Zur Unterstützung von Drittanbietern wurde mit ISE 2.0 ein Konzept von Netzwerkgeräteprofilen eingeführt, das beschreibt, wie sich bestimmte Anbieter verhalten - wie Sitzungen, URL-Umleitung und

CoA unterstützt werden.

Autorisierungsprofile sind von einem bestimmten Typ (Netzwerkgeräteprofil) und nach der Authentifizierung wird das ISE-Verhalten von diesem Profil abgeleitet.

Dementsprechend können Geräte anderer Anbieter problemlos über die ISE verwaltet werden. Darüber hinaus ist die Konfiguration auf der ISE flexibel und ermöglicht die Anpassung oder Erstellung neuer Netzwerkgeräteprofile.

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

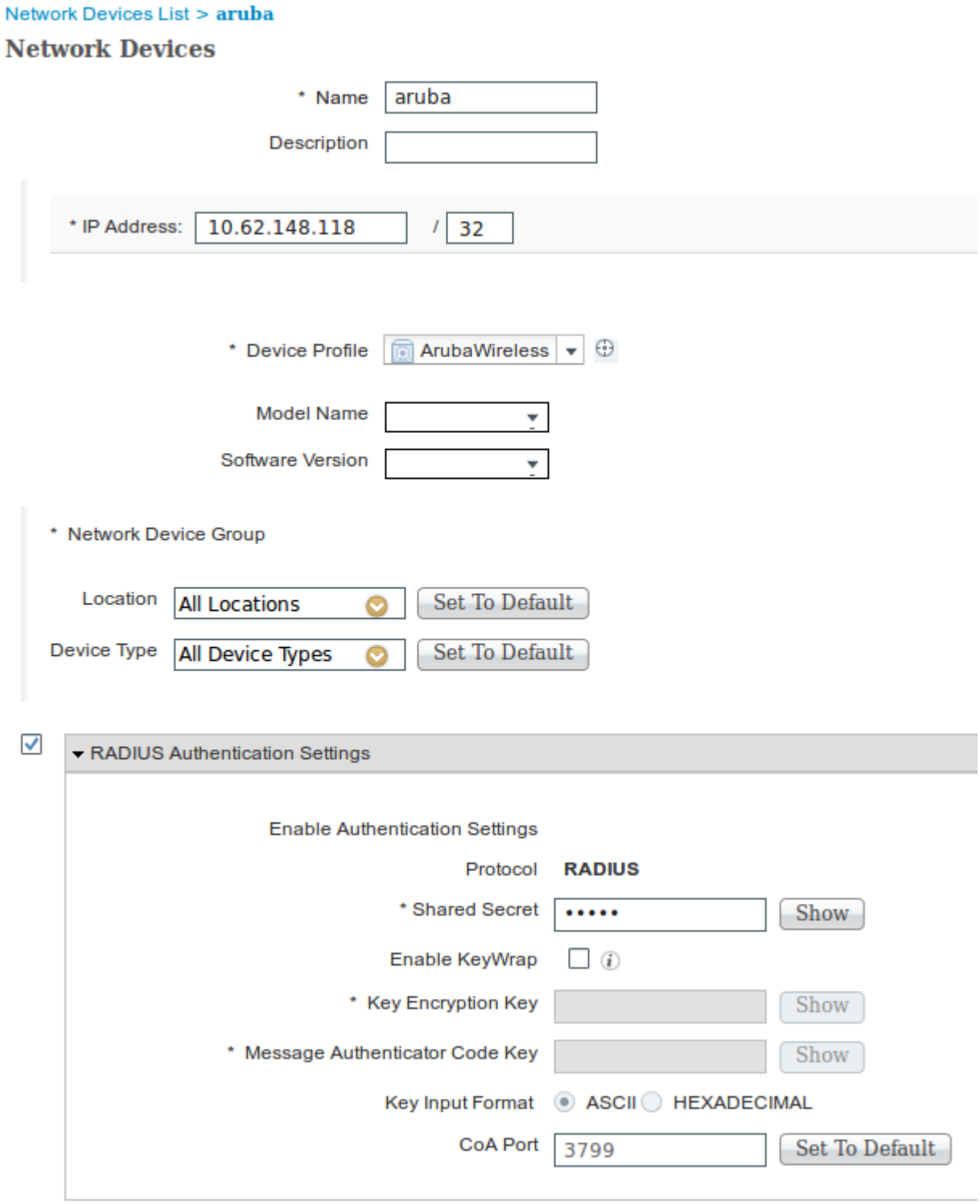
Weitere Informationen zu dieser Funktion:

Netzwerkzugriffs-Geräteprofile mit Cisco Identity Services Engine

Cisco ISE

Schritt 1: Aruba Wireless Controller zu Netzwerkgeräten hinzufügen

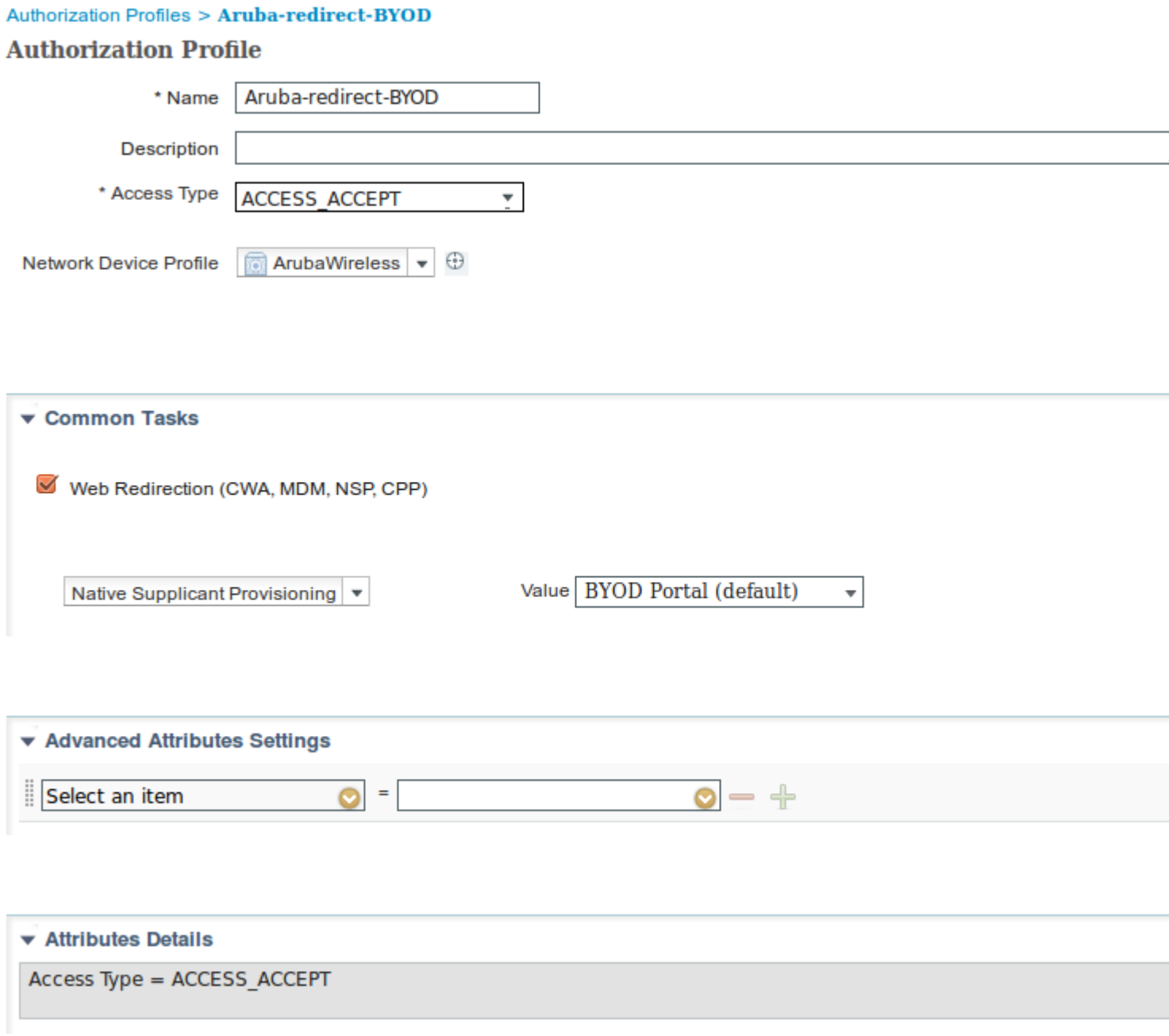
Navigieren Sie zu **Administration > Network Resources > Network Devices (Verwaltung > Netzwerkressourcen > Netzwerkgeräte).** Wählen Sie das richtige Geräteprofil für den ausgewählten Anbieter aus, in diesem Fall: **ArubaWireless.** Stellen Sie sicher, dass Sie den **Shared Secret**- und **CoA-Port**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



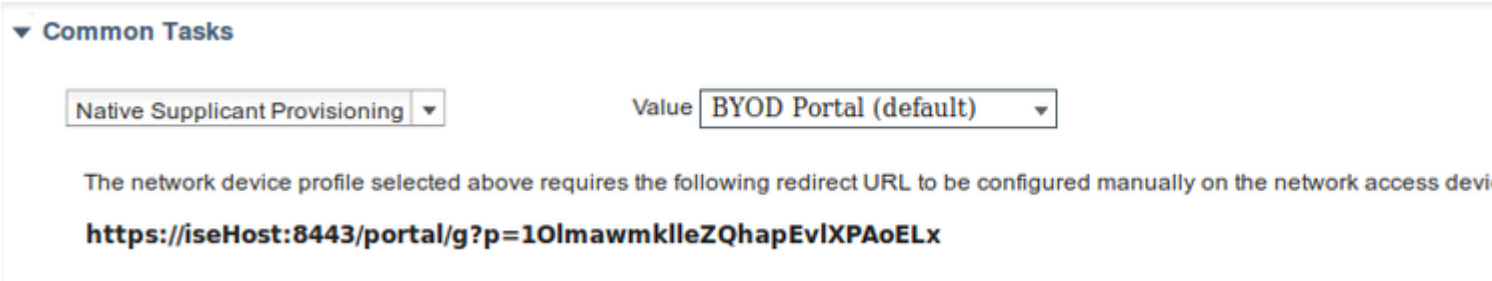
Falls kein Profil für den gewünschten Anbieter verfügbar ist, kann es unter **Administration > Network Resources > Network Device Profiles (Administration > Netzwerkressourcen > Netzwerkgeräteprofile)** konfiguriert werden.

Schritt 2: Autorisierungsprofil konfigurieren

Navigieren Sie zu **Policy > Policy Elements > Results > Authorization > Authorization Profiles,** und wählen Sie das gleiche **Netzwerkgeräteprofil** wie in Schritt 1 aus. **Aruba Wireless**: Das konfigurierte Profil lautet "**Aruba-redirect-BYOD with BYOD Portal"** und ist in den Bildern dargestellt.



Fehlender Teil der Web Redirection-Konfiguration, in der eine statische Verknüpfung mit dem Autorisierungsprofil generiert wird. Obwohl Aruba keine dynamische Umleitung zum Gastportal unterstützt, ist jedem Autorisierungsprofil ein Link zugewiesen, der dann auf Aruba konfiguriert und im Bild dargestellt wird.



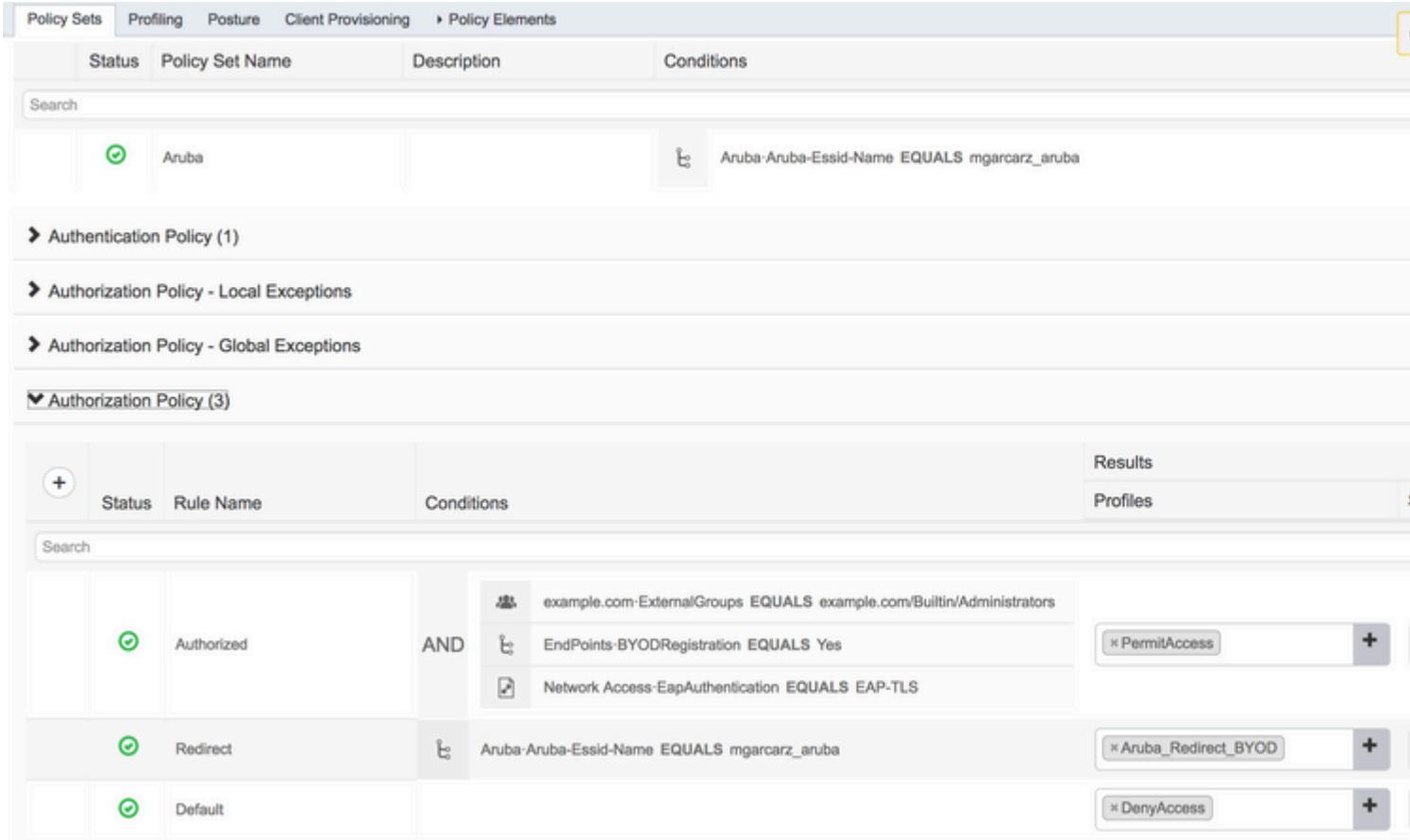
Schritt 3: Konfiguration der Authentifizierungsregeln

Navigieren Sie zu **Policy > Authorization Rules** (Richtlinie > Autorisierungsregeln), und die Konfiguration

wird im Bild angezeigt.

Zunächst stellt der Benutzer eine Verbindung mit der SSID mgracarz_aruba her, und die ISE gibt das Autorisierungsprofil "Aruba-redirect-BYOD" zurück, das den Client zum Standard-BYOD-Portal umleitet. Nach Abschluss des BYOD-Prozesses stellt der Client eine Verbindung mit EAP-TLS her, und der uneingeschränkte Zugriff auf das Netzwerk wird gewährt.

In den neueren Versionen der ISE sieht die gleiche Richtlinie möglicherweise wie folgt aus:

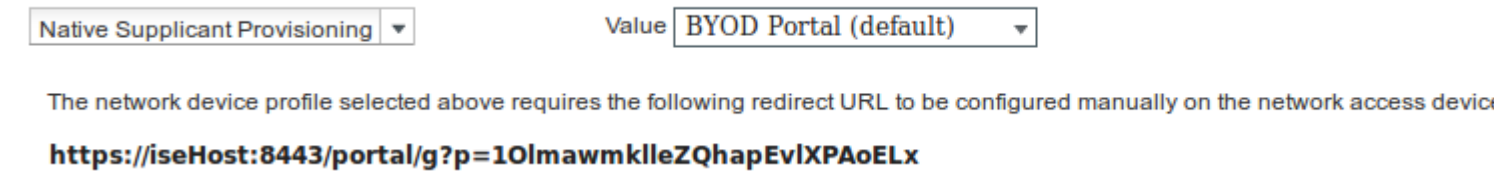


Aruba AP

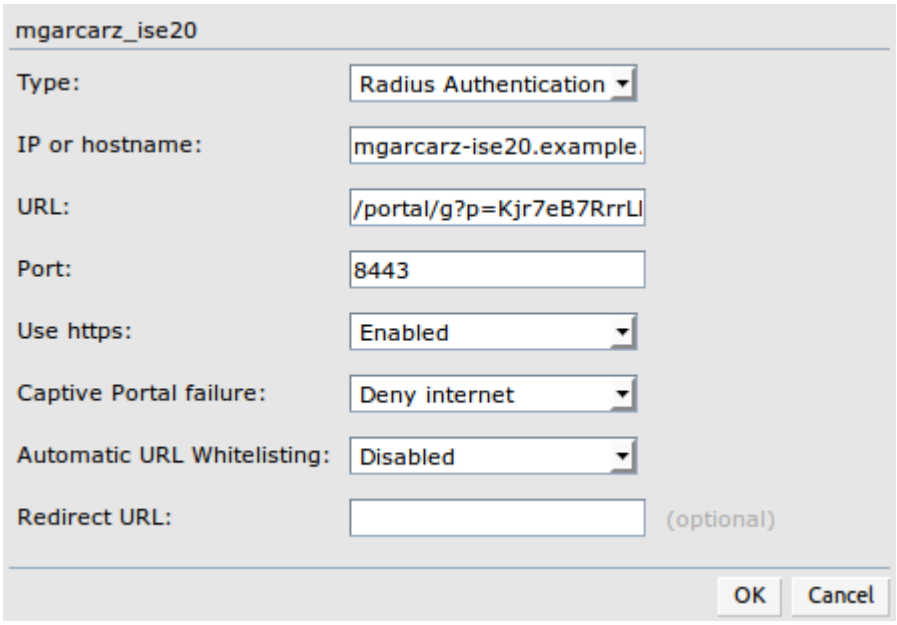
Schritt 1: Captive Portal-Konfiguration

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 zur korrekten Konfiguration ein, wie im Bild dargestellt.

- Typ: RADIUS-Authentifizierung
- IP- oder Hostname: ISE-Server
- URL: Dieser Link wird auf der ISE unter der Konfiguration des Autorisierungsprofils erstellt. Er bezieht sich auf ein bestimmtes Autorisierungsprofil und ist hier unter der Konfiguration der Webumleitung zu finden.



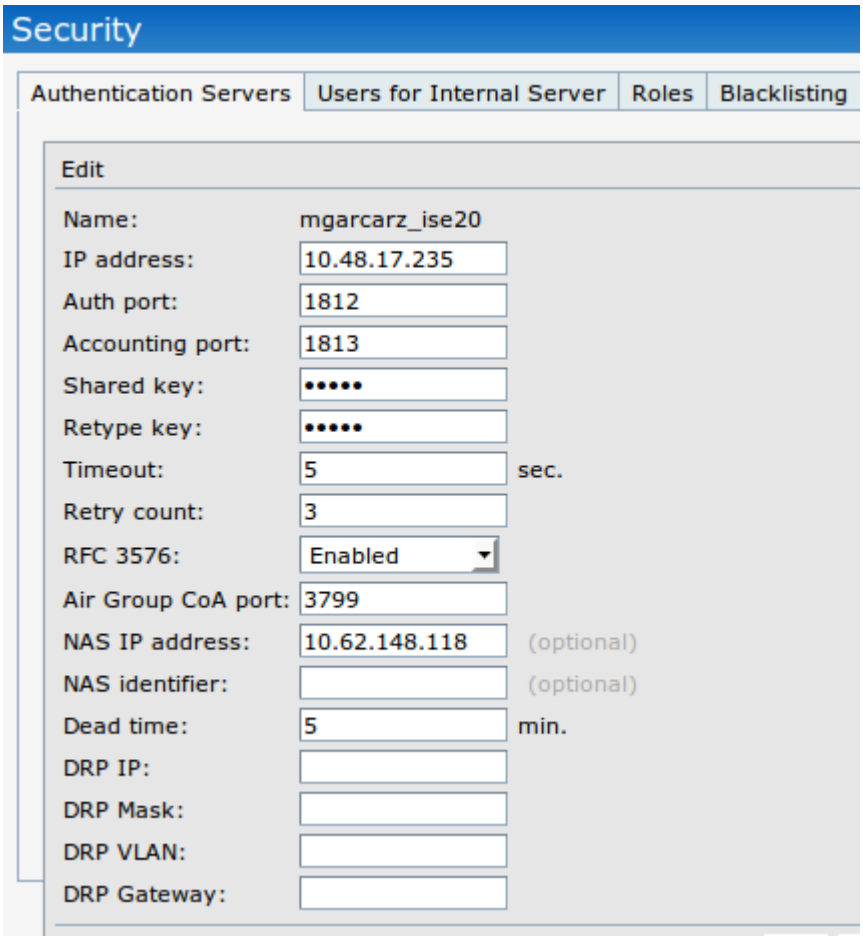
- Port: Die Portnummer, auf der das ausgewählte Portal auf der ISE gehostet wird (standardmäßig 8443), wie im Bild gezeigt.



Schritt 2: Radius-Serverkonfiguration

Navigieren Sie zu **Security > Authentication Servers**, und stellen Sie sicher, dass der CoA-Port mit dem auf der ISE konfigurierten Port identisch ist (siehe Abbildung).

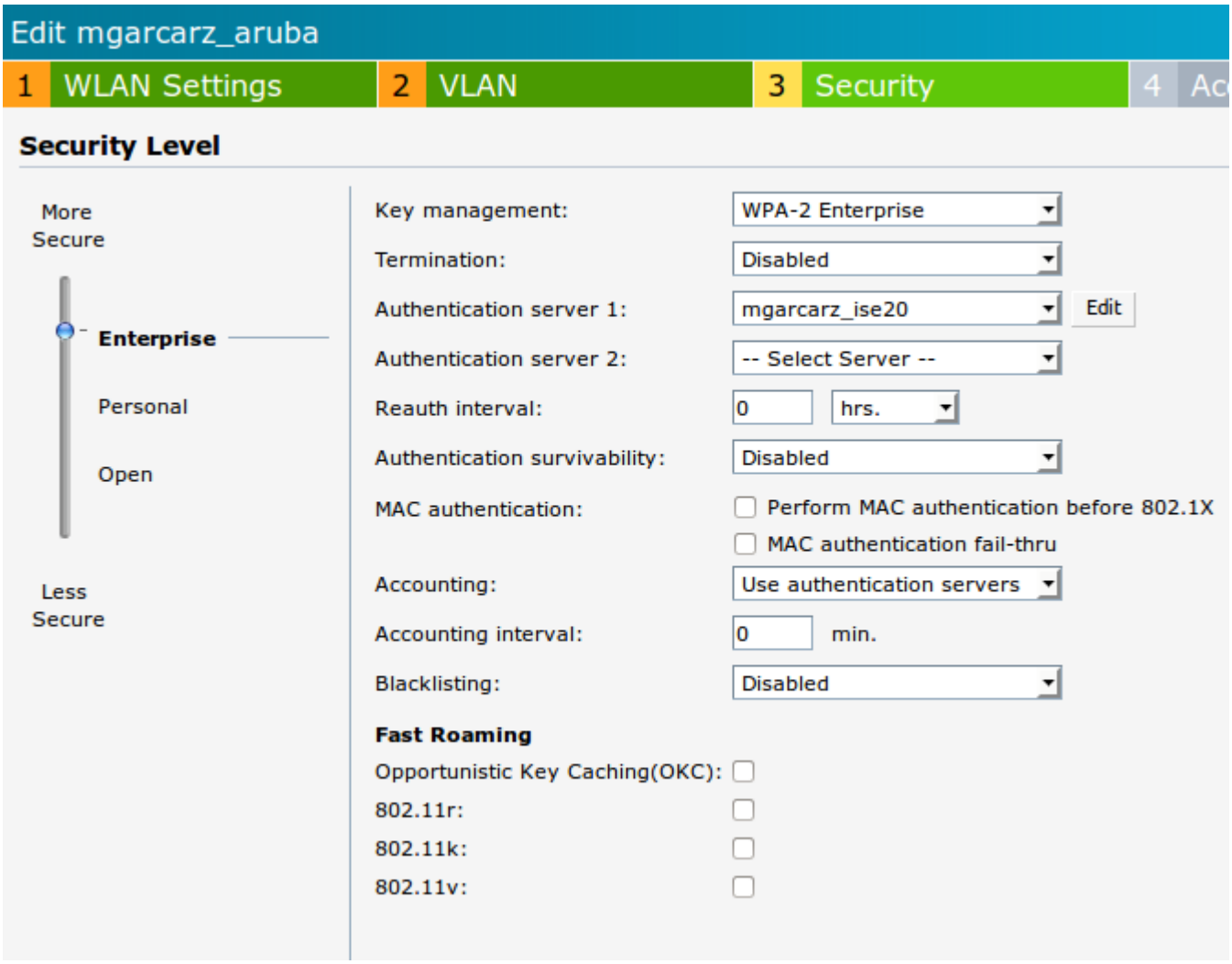
Standardmäßig ist für Aruba 204 "5999" festgelegt, dies ist jedoch nicht mit RFC 5176 kompatibel und funktioniert auch nicht mit der ISE.



Hinweis: Aktivieren Sie in Aruba ab Version 6.5 auch das Kontrollkästchen "Captive Portal".

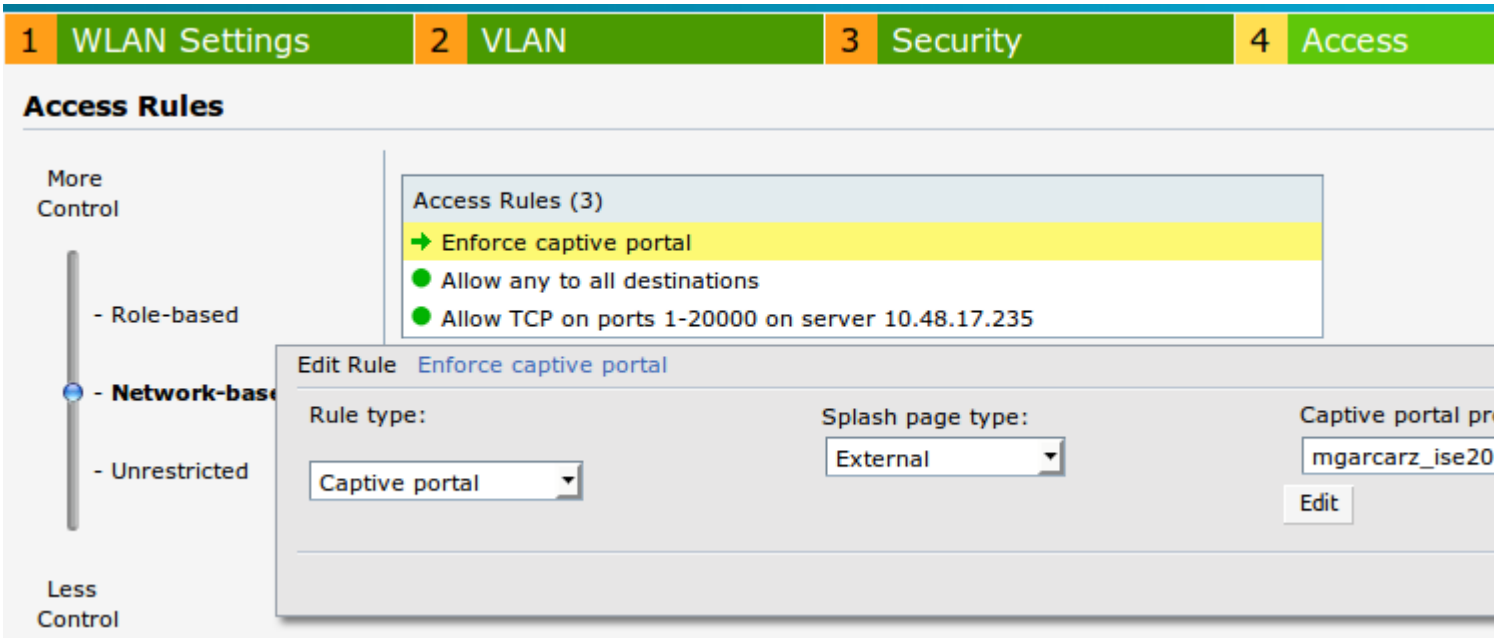
Schritt 3: SSID-Konfiguration

- Die Registerkarte "Sicherheit" ist wie im Bild dargestellt.

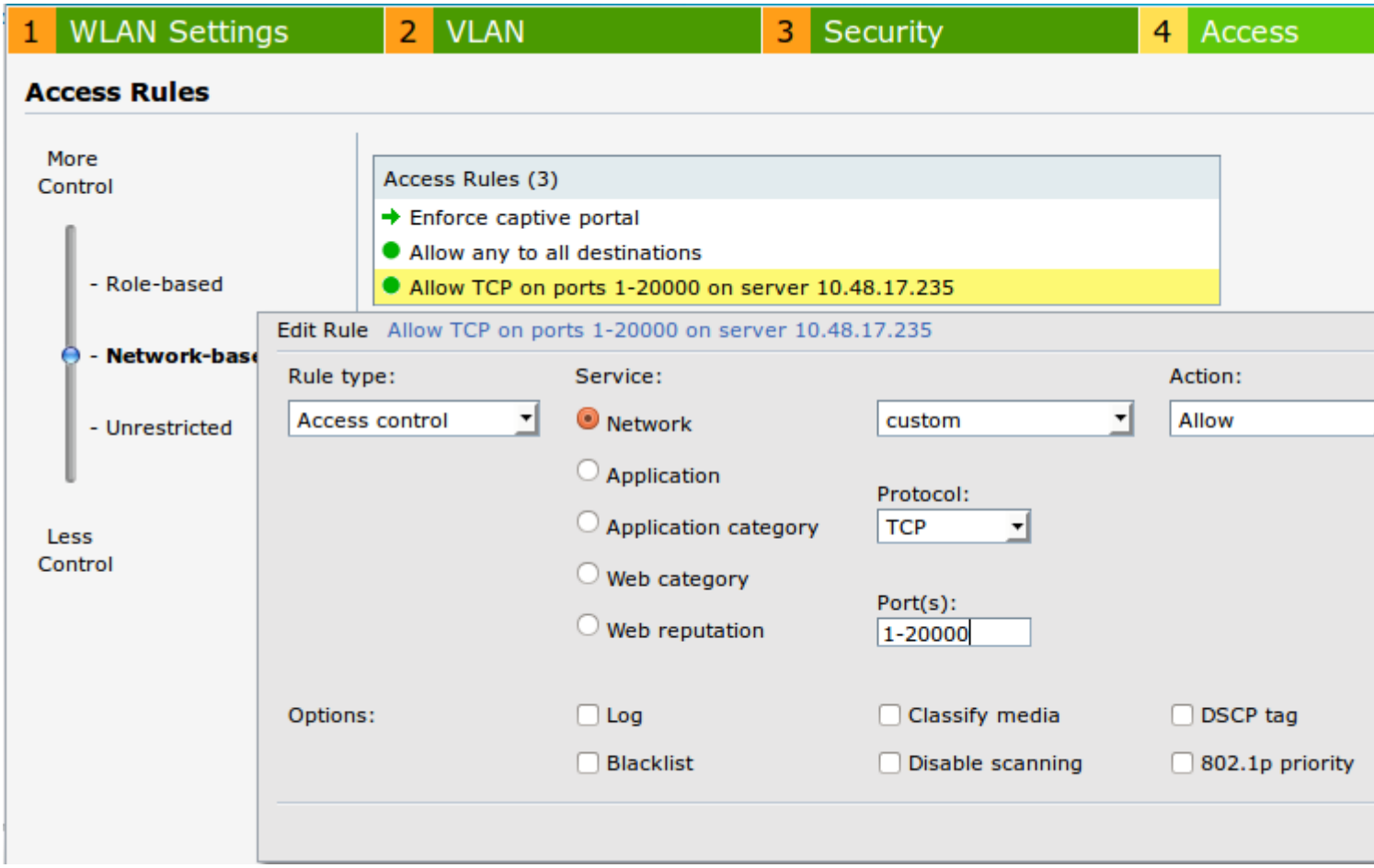


- Registerkarte "Zugriff": Wählen Sie **eine netzwerkbasierte Zugriffsregel** aus, um das Captive Portal auf der SSID zu konfigurieren.

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



Außerdem sollte der gesamte Datenverkehr zum ISE-Server zugelassen werden (TCP-Ports im Bereich 1-20000), während die Regel standardmäßig auf Aruba konfiguriert ist: **Any to all destination** scheint nicht richtig zu funktionieren, wie im Bild gezeigt.

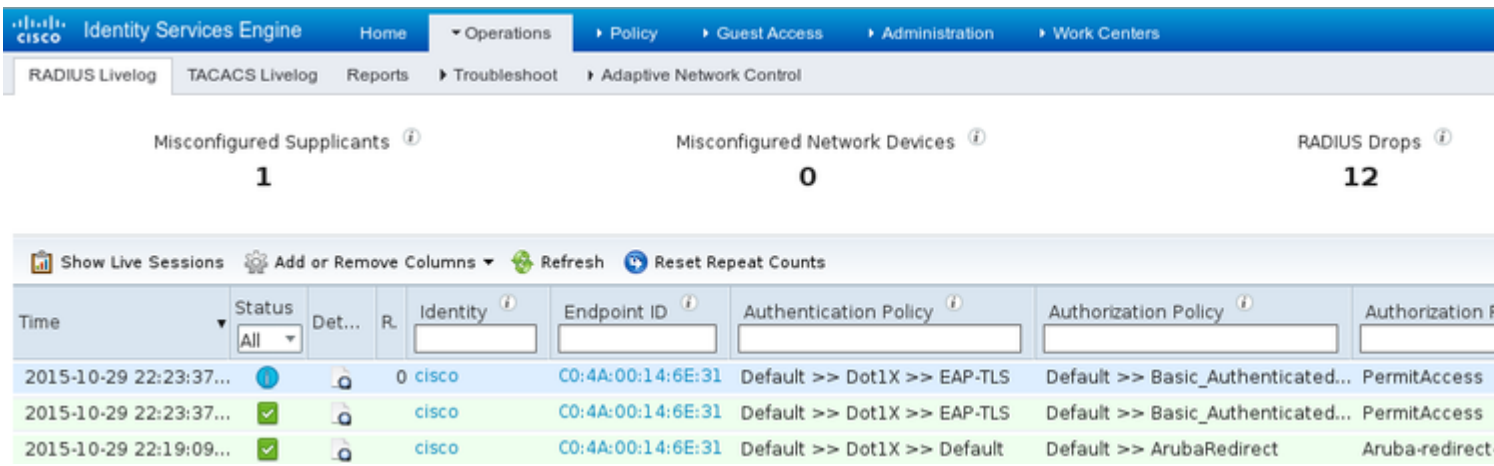


Überprüfung

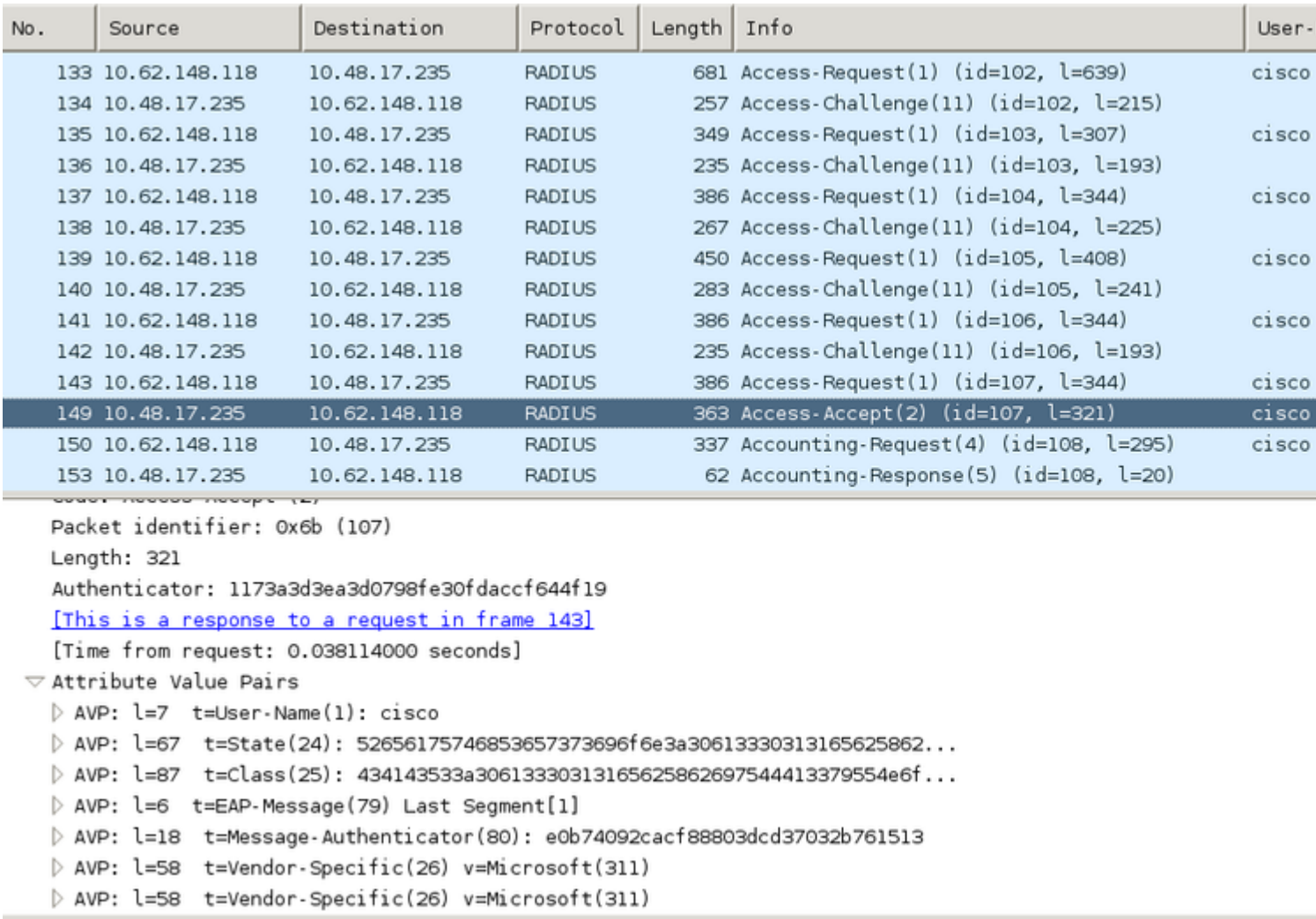
Verwenden Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Schritt 1: Verbindung zur SSID mgarcarz_aruba mit EAP-PEAP

Das erste Authentifizierungsprotokoll auf der ISE wird angezeigt. Es wurde eine Standardauthentifizierungsrichtlinie verwendet. Das Aruba-redirect-BYOD-Autorisierungsprofil wurde zurückgegeben, wie im Bild gezeigt.



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



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 berichtet, dass die Sitzung hergestellt wurde (die EAP-PEAP-Identität lautet **cisco**) und dass die ausgewählte Rolle **mgarcarz_aruba** ist, wie im Bild gezeigt.

Diese Rolle ist für die Umleitung zur ISE (Captive Portal-Funktion auf Aruba) verantwortlich.

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

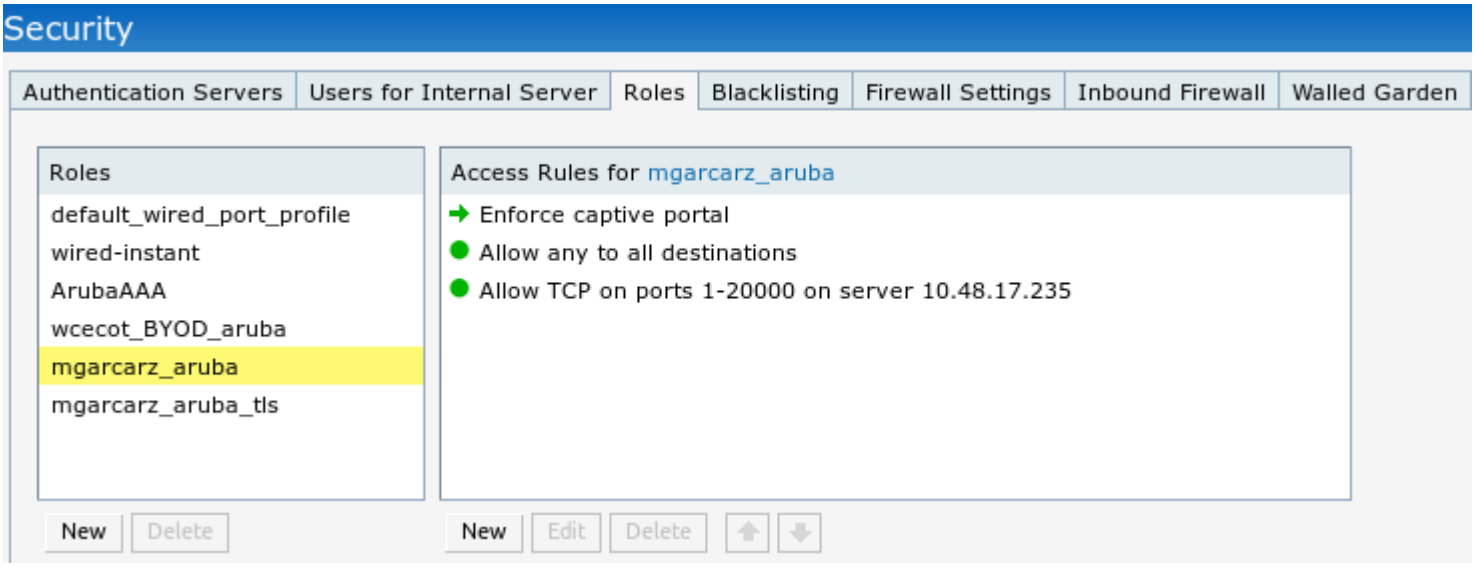
```
<#root>

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#
```

So überprüfen Sie die ACL-ID 138 für die aktuellen Berechtigungen:

```
<#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
```

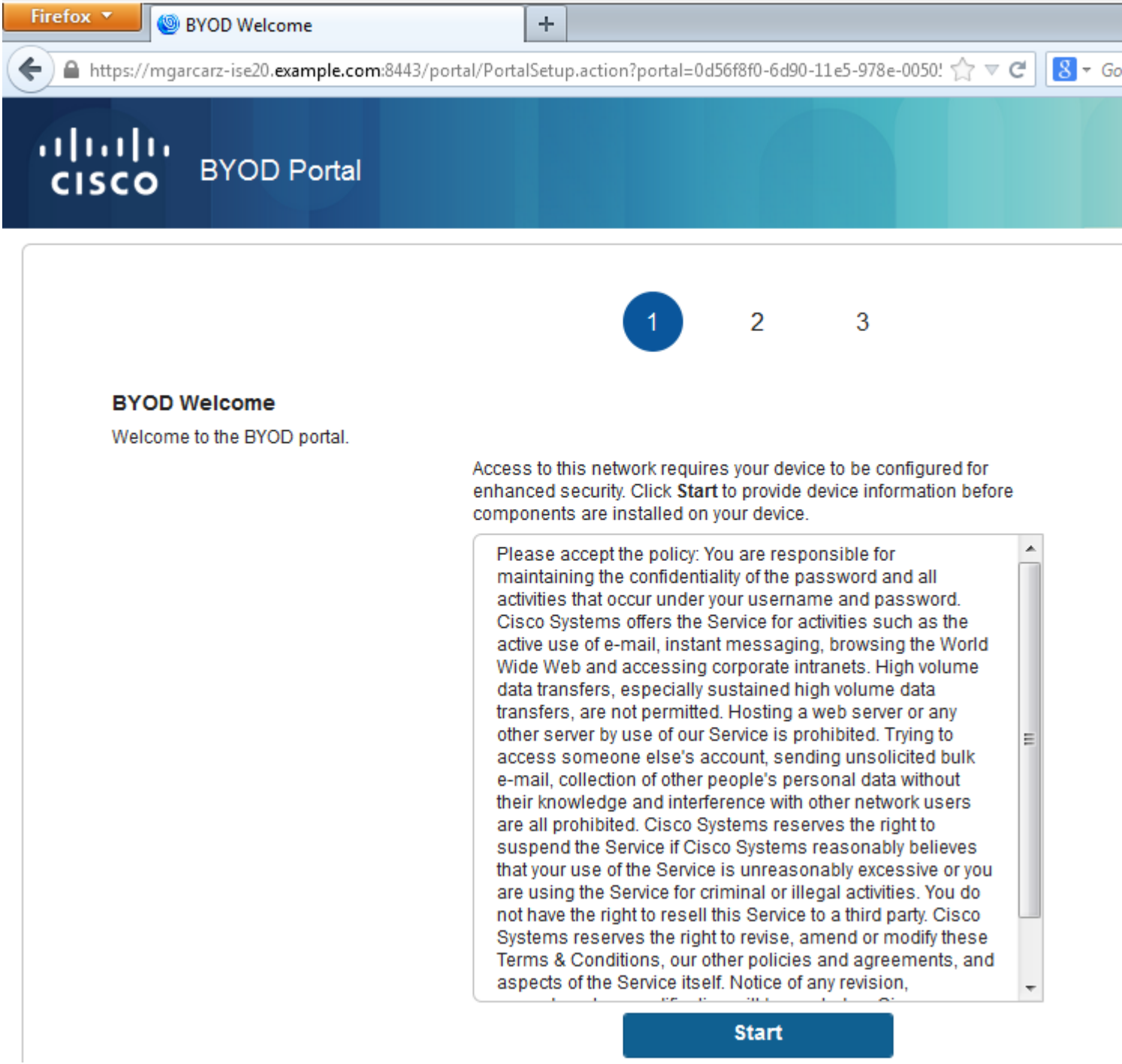
```
 7:  any  10.48.17.235 255.255.255.255  6 0-65535 1-20000  P4  hits 18

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

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



Schritt 2: Umleitung von Webbrowser-Datenverkehr für BYOD

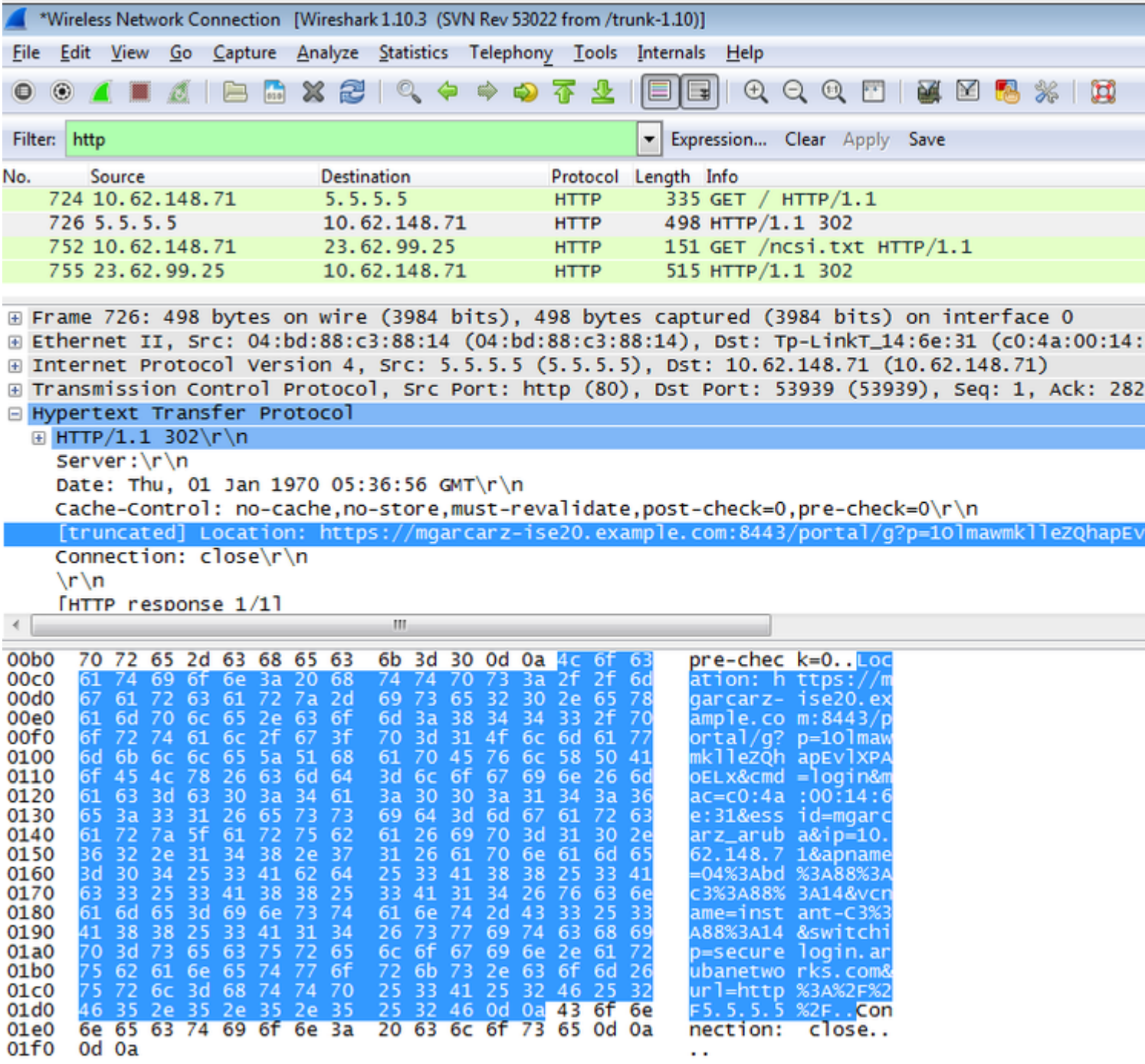
Sobald der Benutzer den Webbrowser öffnet und eine beliebige Adresse eingibt, erfolgt die Umleitung wie im Bild dargestellt.



Wenn Sie sich die Paketerfassungen ansehen, wird bestätigt, dass Aruba das Ziel (5.5.5.5) imitiert und die HTTP-Umleitung an die ISE zurückgibt.

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

- cmd = Anmeldung
- mac = c0:4a:00:14:6e:31
- essid = mgarcarz_aruba
- ip = 10,62.148,7
- apname = 4bd88c38814 (Mac)
- url = http://5.5.5.5



Aufgrund dieser Argumente kann die ISE die Cisco Session-ID neu erstellen, die entsprechende Sitzung auf der ISE ermitteln und mit dem BYOD-Fluss (oder einem anderen konfigurierten Fluss) fortfahren.

Für Cisco Geräte wird normalerweise **audit_session_id** verwendet, was jedoch von anderen Anbietern nicht unterstützt wird.

Um zu bestätigen, dass die ISE-Debugging-Funktion die Generierung des Werts "audit-session-id" anzeigt (der nie über das Netzwerk gesendet wird):

<#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

Und dann, Korrelation dieser nach der Registrierung des Geräts auf BYOD Seite 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, 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

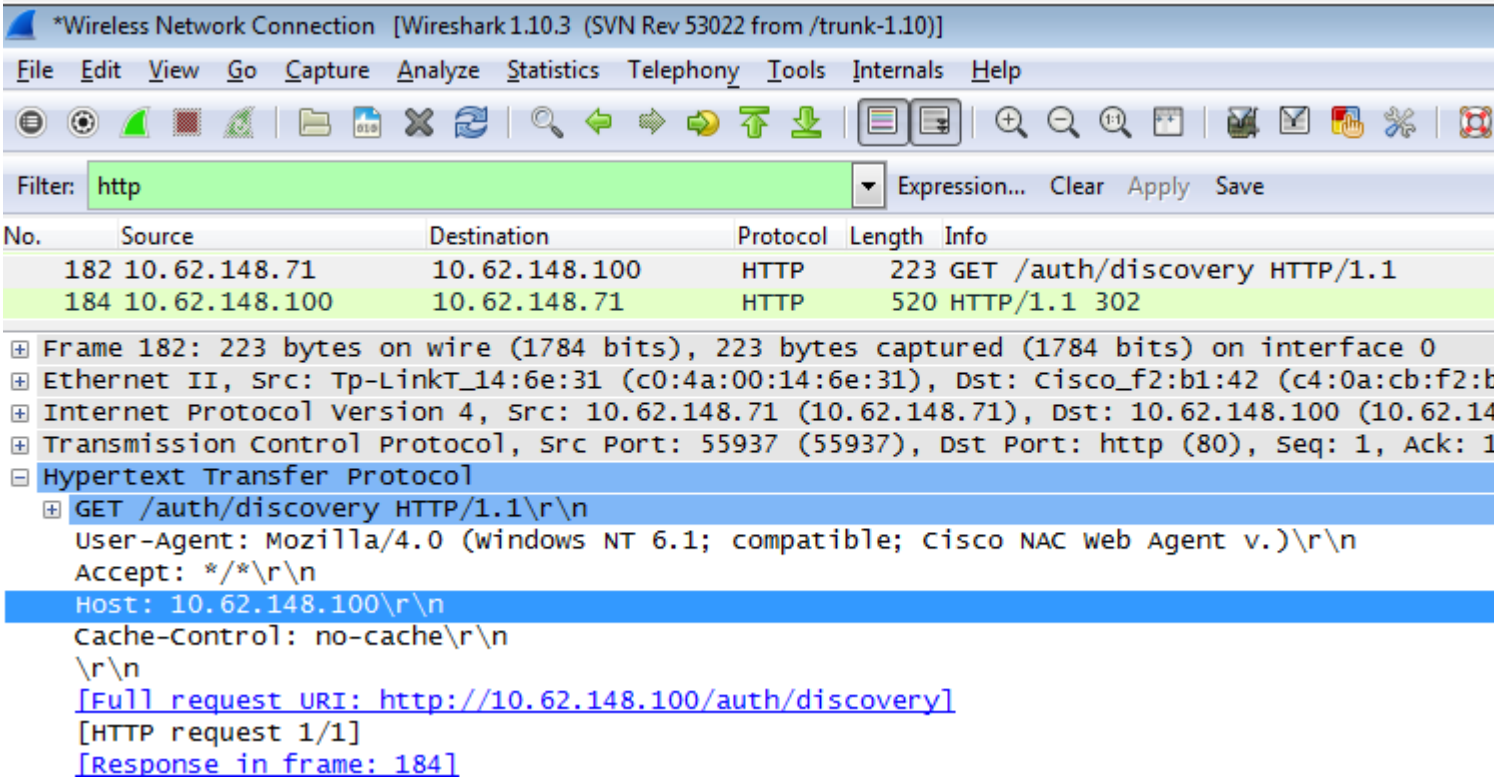
Bei nachfolgenden Anfragen wird der Client auf BYOD-Seite 3. umgeleitet, auf der die NSA heruntergeladen und ausgeführt wird.

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 erfolgt über HTTP Redirection (HTTP-Umleitung).

Da der Benutzer diesmal nicht die Möglichkeit hat, die IP-Adresse einzugeben (wie im Webbrowser), wird dieser Datenverkehr automatisch generiert.

Es wird, wie im Bild dargestellt, das Standard-Gateway verwendet **(**es kann auch **enroll.cisco.com** verwendet werden).



Die Antwort ist genau die gleiche wie für den Webbrowser.

Auf diese Weise kann die NSA eine Verbindung zur ISE herstellen, ein XML-Profil mit Konfiguration abrufen, eine SCEP-Anforderung generieren, diese an die ISE senden, ein signiertes Zertifikat (signiert von der internen ISE-Zertifizierungsstelle) abrufen, ein Wireless-Profil konfigurieren und schließlich eine Verbindung zur konfigurierten SSID herstellen.

Sammeln Sie Protokolle vom Client (unter Windows befinden sich in %**temp%/spwProfile.log**). Einige Ausgaben werden der Übersichtlichkeit halber weggelassen:

<#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: 0a3011ebXbiuDA3yUNoLUvtCRyuPFxkqYJ7TT06foOZ7C
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=S
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

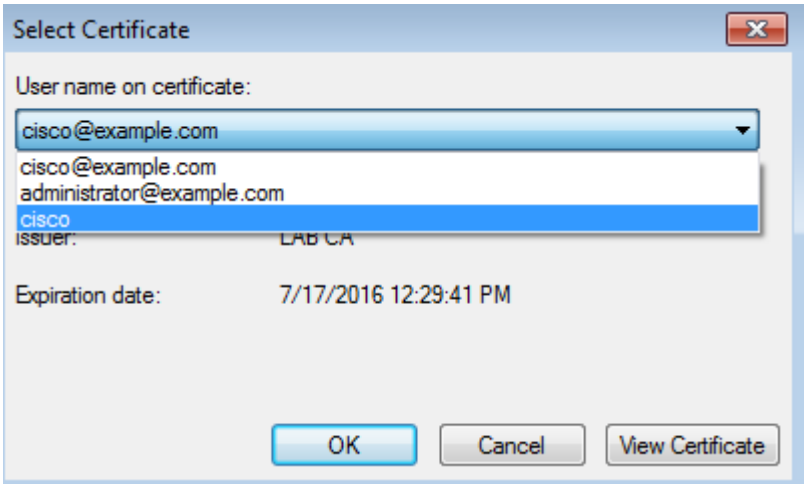
Wireless profile: [mgarcarz_aruba_tls] configured successfully

```
Connect to SSID

Successfully connected profile: [mgarcarz_aruba_tls]

WirelessProfile::SetWirelessProfile. - End
```

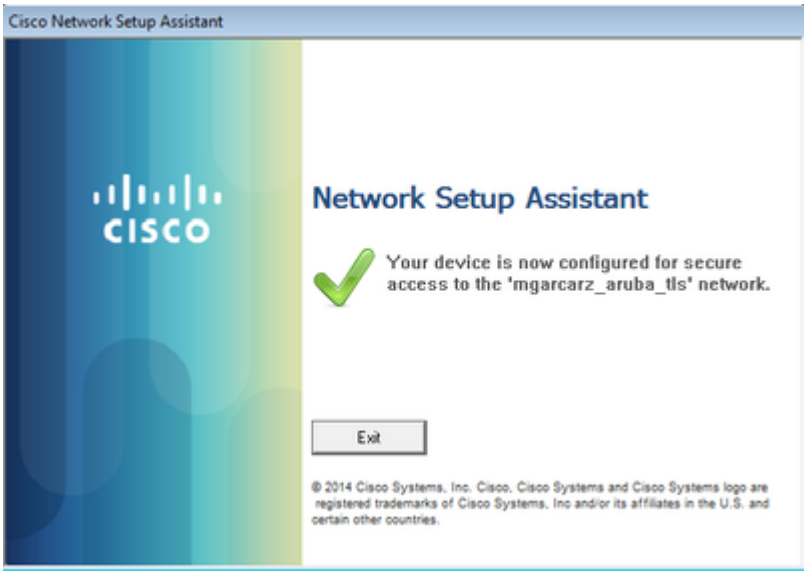
Diese Protokolle entsprechen genau denen für BYOD-Prozesse mit Cisco Geräten.

> **Hinweis**: Radius CoA ist hier nicht erforderlich. Die Anwendung (NSA) erzwingt die erneute Verbindung mit einer neu konfigurierten SSID.

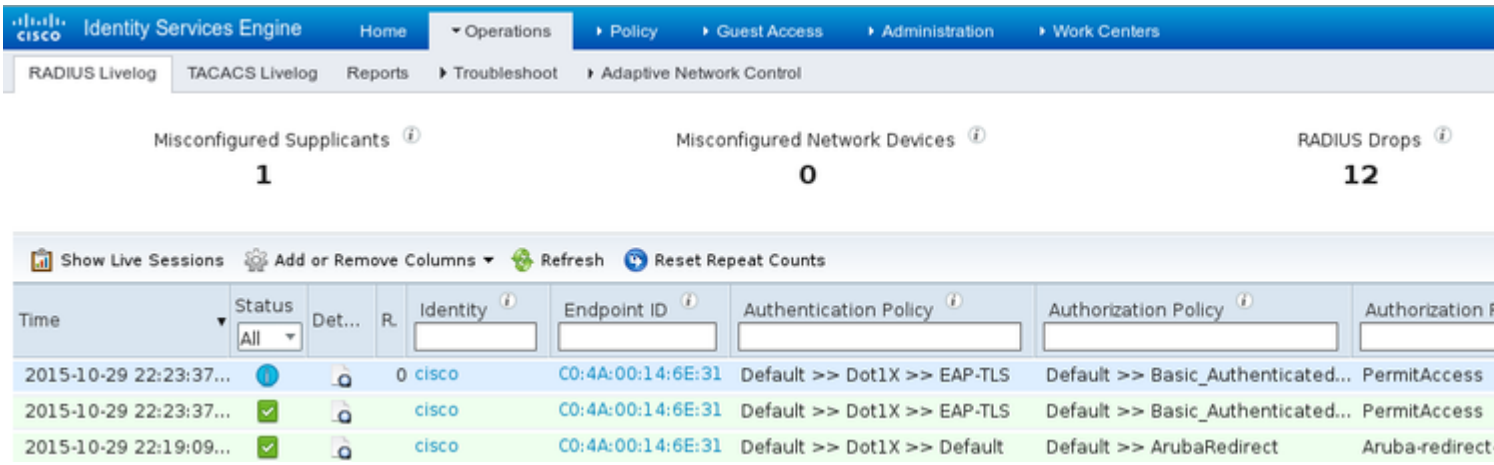
In dieser Phase kann der Benutzer sehen, dass das System versucht, eine Verbindung mit einer endgültigen SSID herzustellen. Wenn Sie über mehr als ein Benutzerzertifikat verfügen, müssen Sie das richtige auswählen (wie dargestellt).



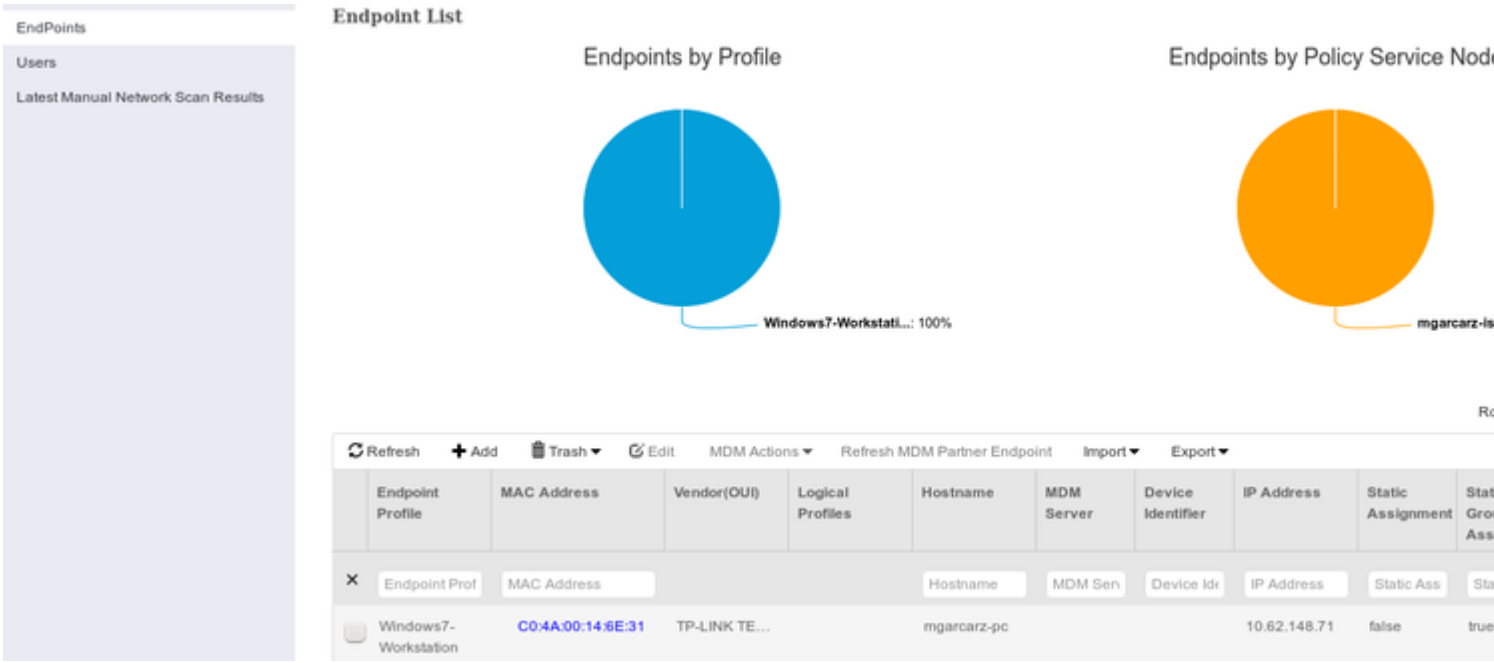
Nach einer erfolgreichen Verbindung meldet die NSA, dass die im Bild dargestellte Situation eintritt.



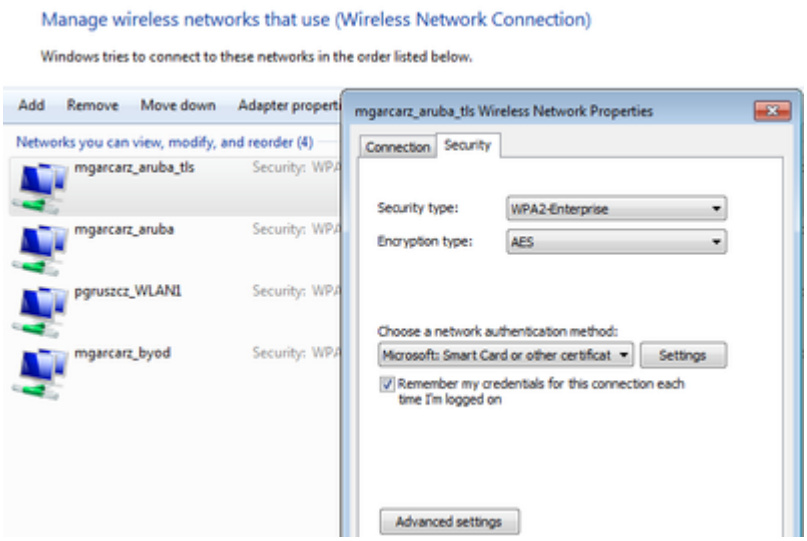
Das kann auf der ISE bestätigt werden - das zweite Protokoll trifft auf die EAP-TLS-Authentifizierung, die allen Bedingungen für Basic_Authenticated_Access (EAP-TLS, Employee und BYOD Registered true) entspricht.



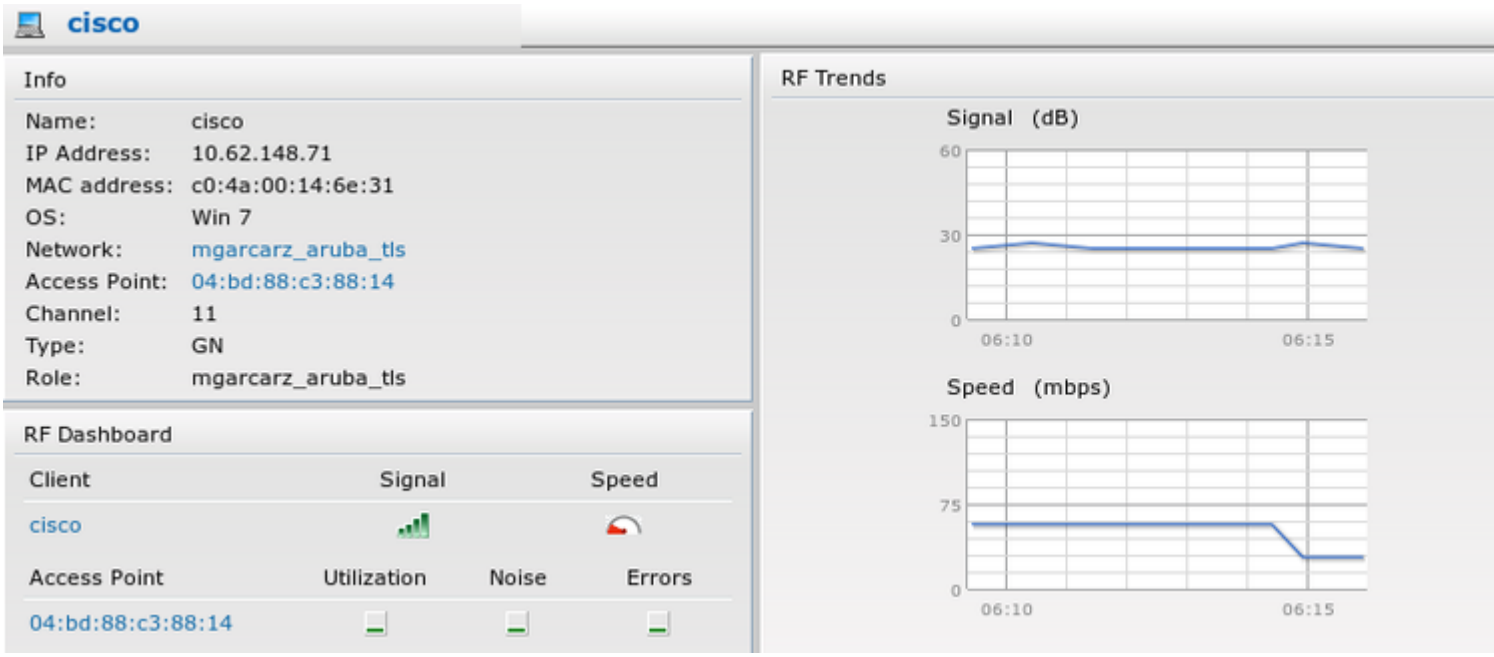
Die Ansicht der Endgeräteidentität kann außerdem bestätigen, dass für das Endgerät das Flag "BYOD Registered" auf "true" gesetzt ist, wie im Bild gezeigt.



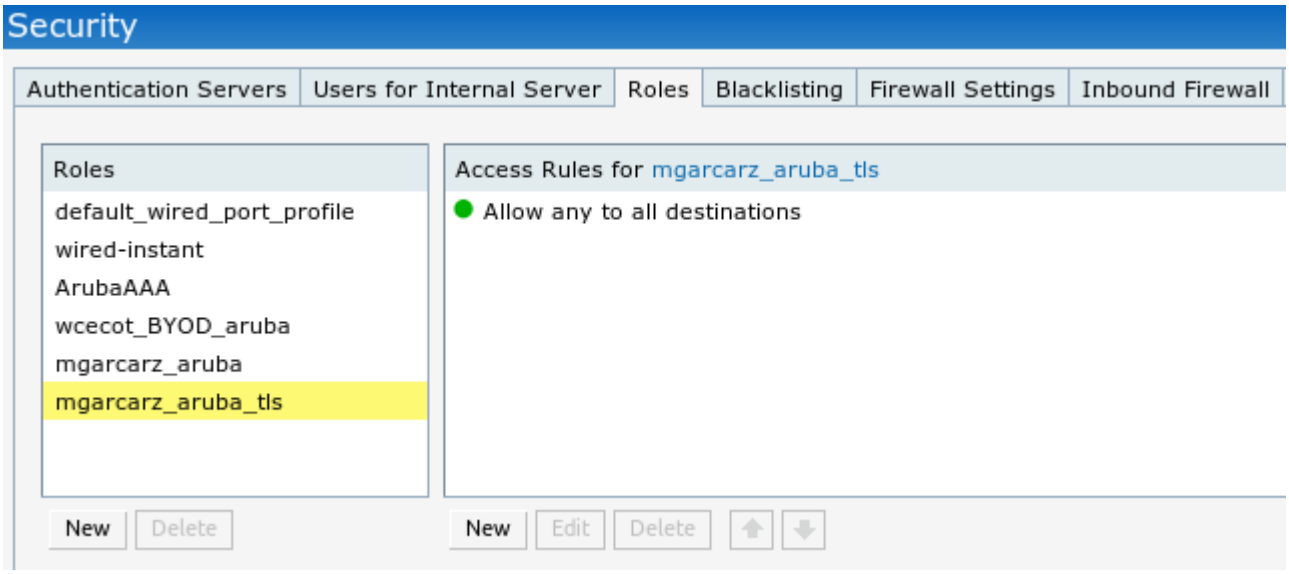
Auf Windows-PCs wurde automatisch ein neues Drahtlosprofil erstellt, wie dies bevorzugt (und für EAP-TLS konfiguriert) und dargestellt wird.



Zu diesem Zeitpunkt bestätigt Aruba, dass der Benutzer mit der endgültigen SSID verbunden ist.



Die Rolle, die automatisch erstellt wird und die den Namen Network trägt, bietet vollständigen Netzwerkzugriff.

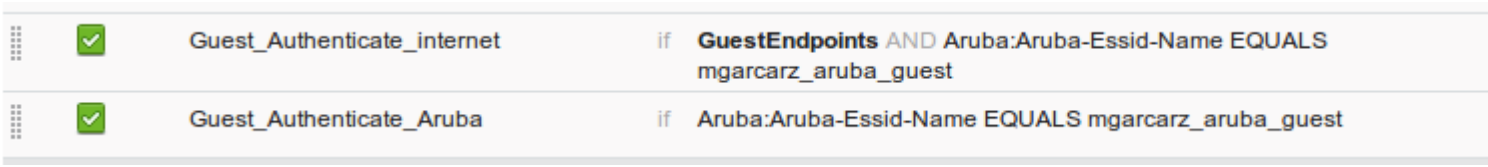


Weitere Flows und CoA-Unterstützung

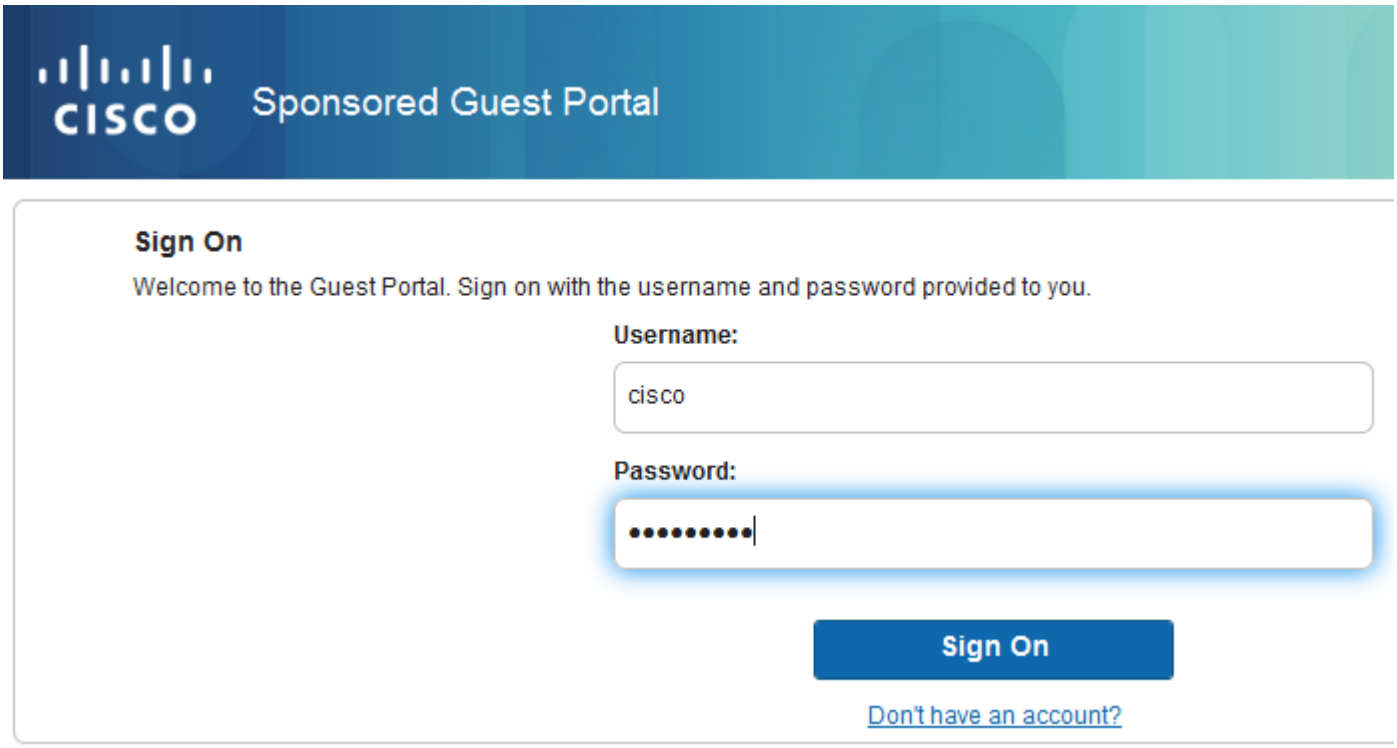
CWA mit CoA

Während im BYOD-Fluss keine CoA-Meldungen vorhanden sind, wird der CWA-Fluss mit dem Portal für selbst registrierte Gäste hier dargestellt:

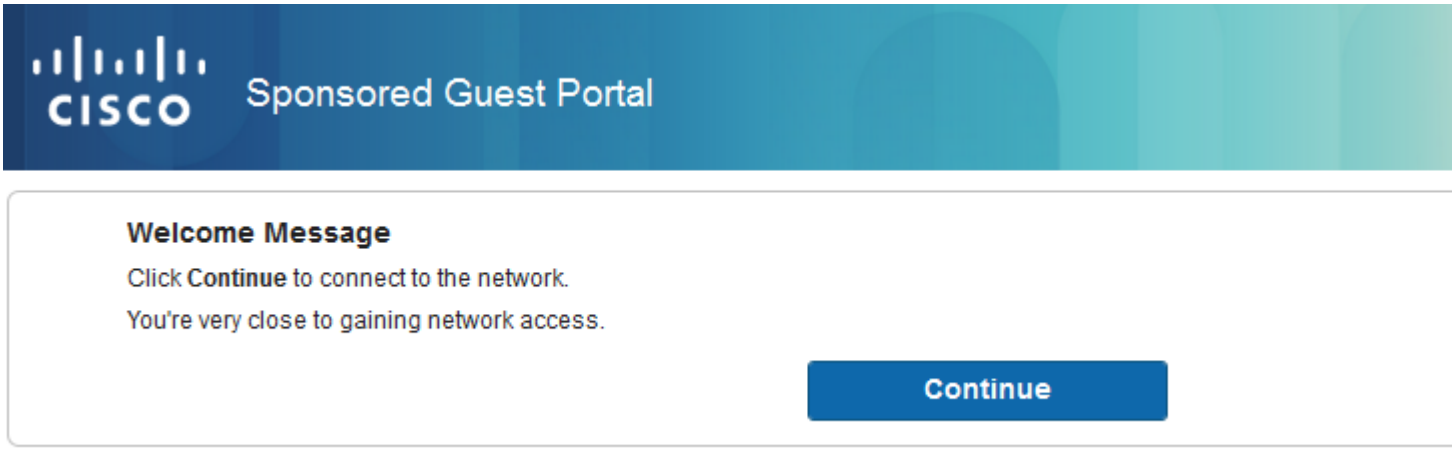
Die konfigurierten Autorisierungsregeln werden im Bild angezeigt.



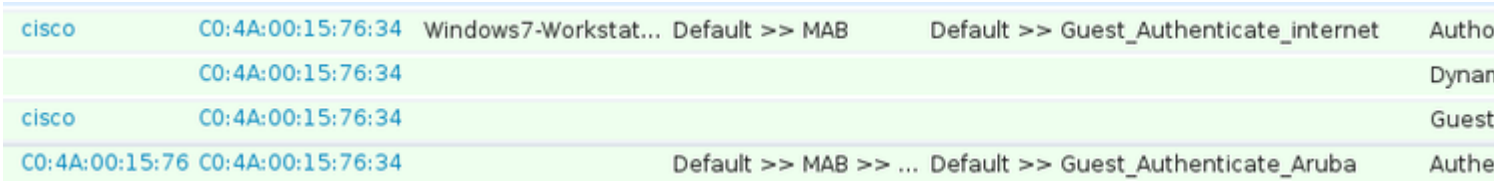
Der Benutzer stellt über MAB-Authentifizierung eine Verbindung zum SSID her. Wenn er versucht, eine Verbindung zu einer Webseite herzustellen, wird eine Umleitung zum Portal für selbst registrierte Gäste durchgeführt, auf dem Guest ein neues Konto erstellen oder das aktuelle Konto verwenden kann.



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



Sie kann unter **Operationen** > **Authentifizierungen** und wie im Bild dargestellt überprüft werden.



CoA-Meldung bei ISE-Debugging:

<#root>

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

NAS-IP-Address, value=10.62.148.118

.,
DynamicAuthorizationFlow.cpp:708
2015-11-02 18:47:49,567 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

**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=0a3011ebisZXypODwqjB6j64GeFiF7RwvyocneEia17ckjtU1HI.,DynamicAuthorizationFlow.cpp:
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:

<#root>

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,

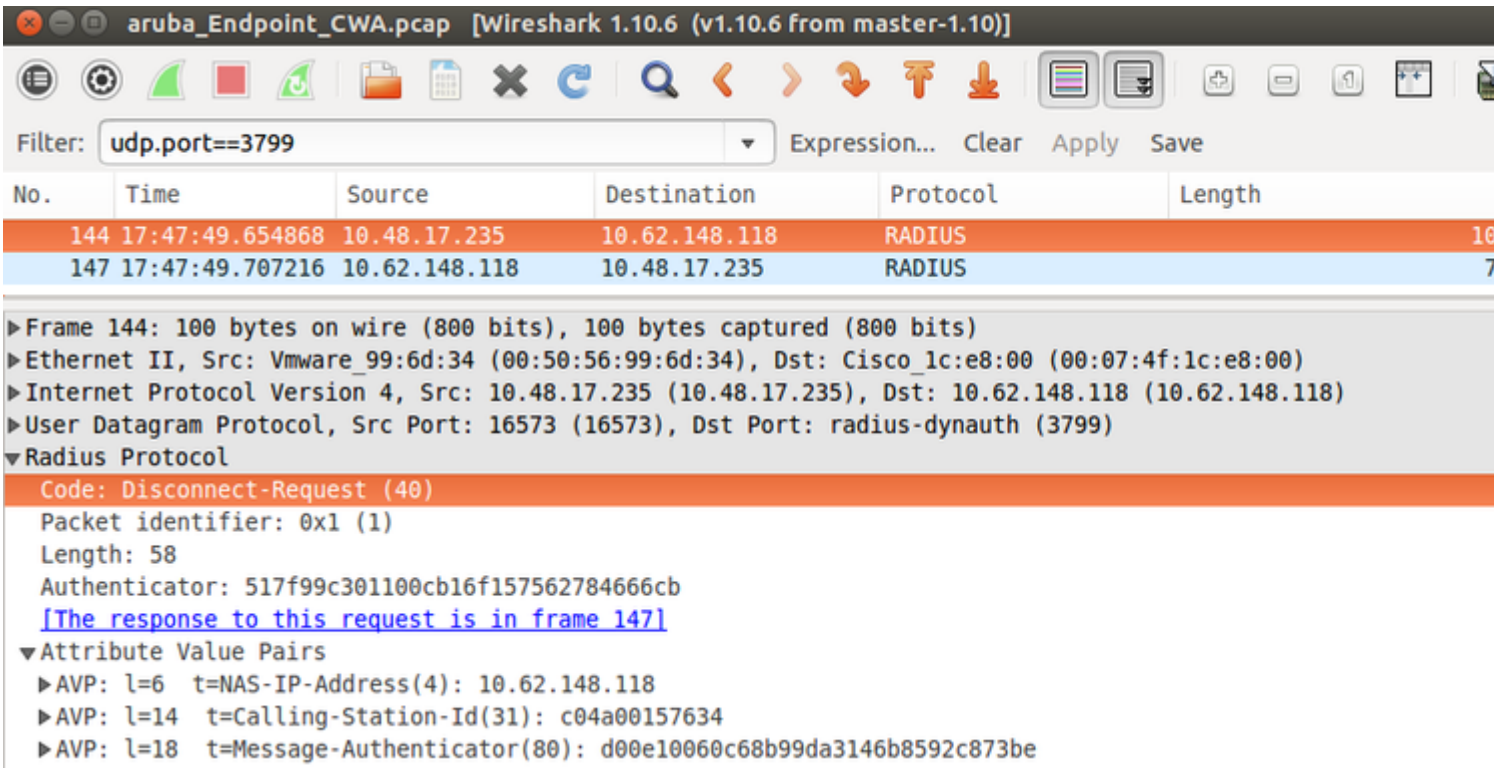
CallingStationID=c04a00157634

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

Packet type 41(DisconnectACK).

,
DynamicAuthorizationFlow.cpp:303

Die Paketerfassung mit CoA-Trennanforderung (40) und Diconnect-ACK (41) erfolgt wie dargestellt.



> **Hinweis**: RFC-CoA wurde für die Authentifizierung im Zusammenhang mit dem Geräteprofil Aruba verwendet (Standardeinstellungen). Für die Authentifizierung in Bezug auf ein Cisco Gerät wäre "Cisco CoA type reAuthenticate" verwendet worden.

Fehlerbehebung

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

Aruba Captive Portal mit IP-Adresse anstelle von FQDN

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

<#root>

```
Warning - [HTTPConnection]
```

Abort the HTTP connection due to invalid certificate

CN

Der Grund dafür ist die strenge Zertifikatsvalidierung bei der Verbindung mit der ISE. Wenn Sie die IP-Adresse für die Verbindung mit der ISE verwenden (als Ergebnis der Umleitungs-URL mit IP-Adresse anstelle von FQDN) und ein ISE-Zertifikat mit dem Antragstellernamen erhalten, schlägt die FQDN-

Validierung fehl.

> **Hinweis:** Webbrowser wird mit BYOD-Portal fortgesetzt (mit einer Warnung, die vom Benutzer genehmigt werden muss).

Aruba Captive Portal: Richtlinie für falschen Zugriff

Standardmäßig ermöglicht die mit Captive Portal konfigurierte Aruba Access-Policy die TCP-Ports 80, 443 und 8080.

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

<#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=0a3011ebXbiuDA3yUNoLUvtCRyuPFxkqYJ7TT06foOZ7G1HXj1M&os=Windows All]
- http Error: [2]

HTTP response code: 0

]
GetProfile - end
Failed to get profile. Error: 2

Aruba CoA-Portnummer

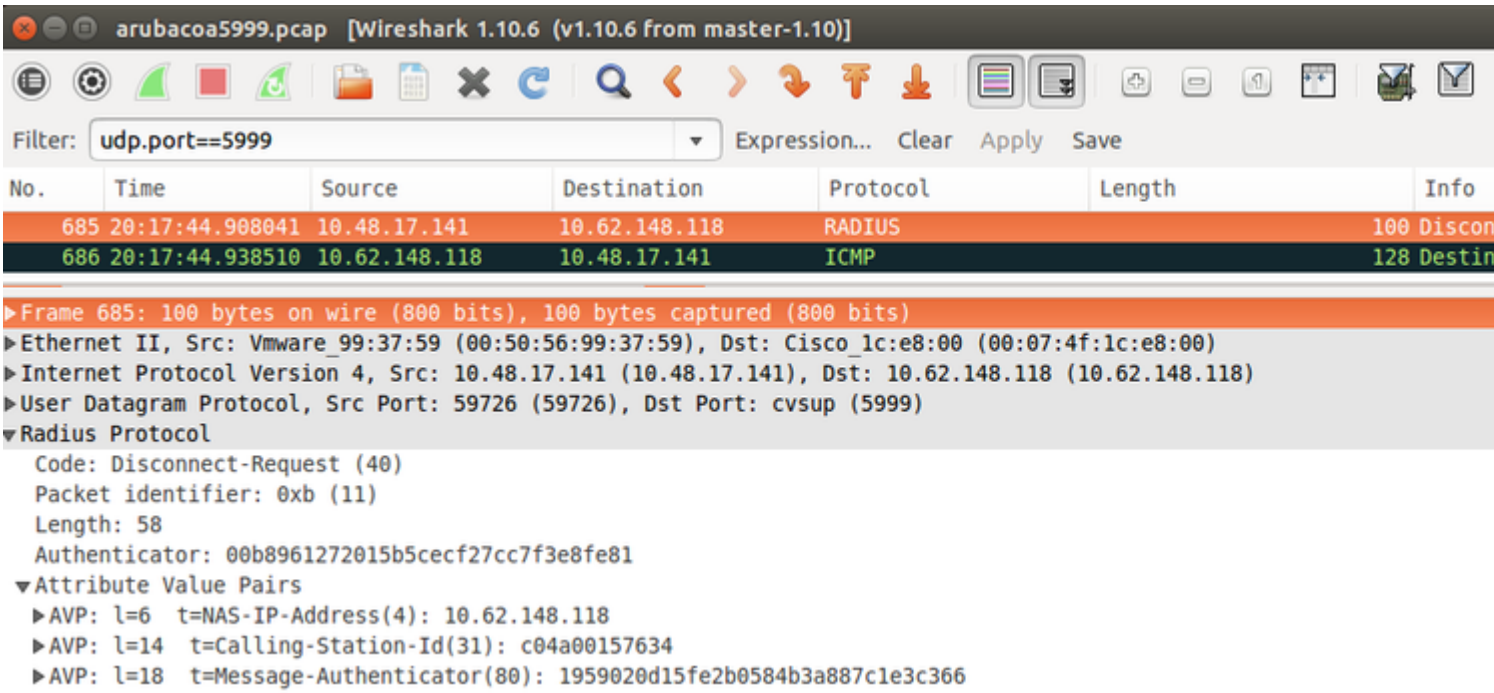
Standardmäßig gibt Aruba die Portnummer für den CoA **Air Group CoA-Port** 5999 an. Leider hat Aruba 204 nicht auf solche Anfragen reagiert (wie gezeigt).

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 erfolgt wie im Bild dargestellt.



Die beste Option zur Verwendung hier ist der CoA-Port 3977, wie in RFC 5176 beschrieben.

Umleitung auf einigen Aruba Geräten

Auf Aruba 3600 mit v6.3 fällt auf, dass die Umleitung etwas anders funktioniert als auf anderen Controllern. Die Paketerfassung und -erklärungen finden Sie hier.

<#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&essid=SC%2DWiFi&apname=LRC-006&apgroup=default&url=http%3A%2F%2Fww
```

Zugehörige Informationen

- Administratorleitfaden für die Cisco Identity Services Engine, Version 2.0
- Netzwerkzugriffs-Geräteprofile mit Cisco Identity Services Engine
- Technischer Support und Dokumentation für Cisco Systeme

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.