Configure ISE 2.0 3rd Party Integration with Aruba Wireless

Contents

Introduction

This document describes how to troubleshoot 3rd Party Integration feature on Cisco Identity Services Engine (ISE).

Note: Be aware that Cisco is not responsible for configuration or support of devices from other vendors.

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Aruba IAP configuration
- BYOD flows on ISE
- ISE configuration for password and certificate authentication

Components Used

This document describes how to troubleshoot 3rd Party Integration feature on Cisco Identity Services Engine (ISE).

It can be used as a guide for integration with other vendors and flows. ISE version 2.0 supports 3rd Party Integration.

This is a configuration example that presents how to integrate wireless network managed by Aruba IAP 204 with ISE for Bring Your Own Device (BYOD) services.

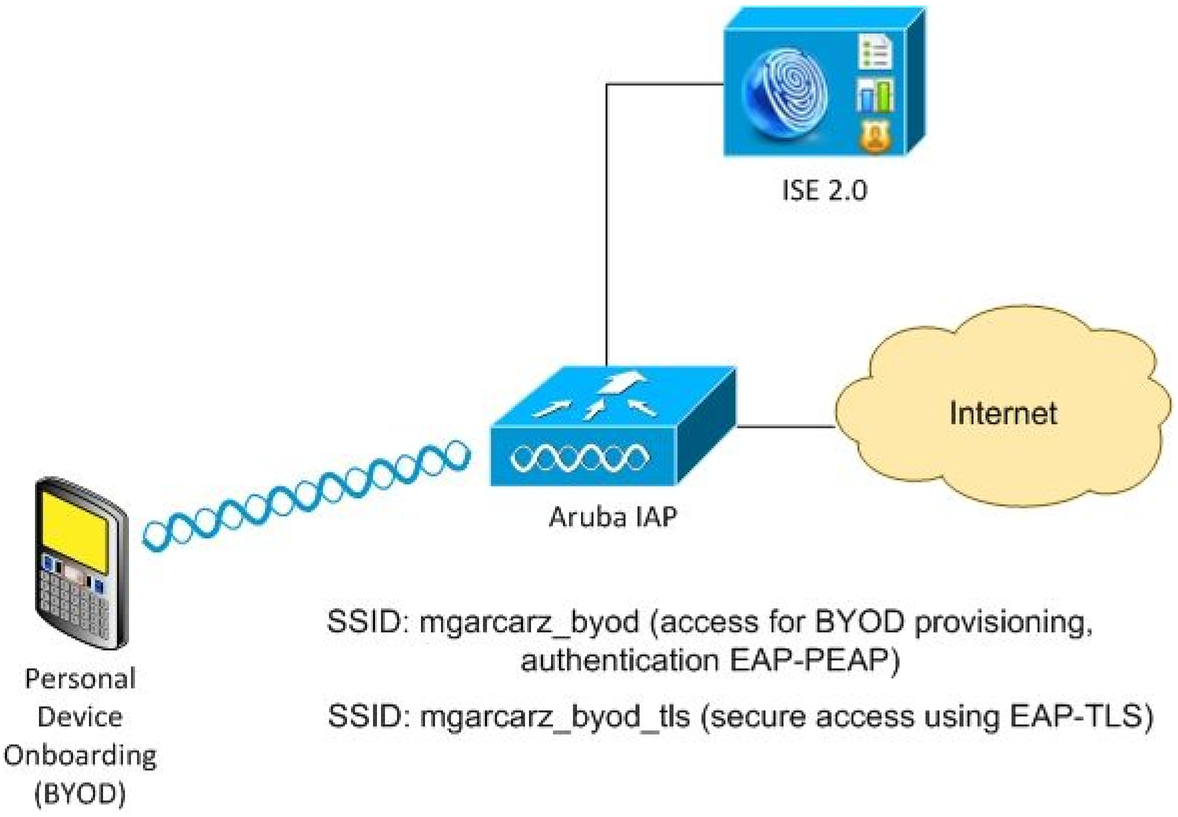
The information in this document is based on these software versions:

- Aruba IAP 204 software 6.4.2.3
- Cisco ISE, Release 2.0 and later

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Configure

Network Diagram


ISE 2.0
Internet
Aruba IAP
Personal Device Onboarding (BYOD)
SSID: mgarcarz_byod (access for BYOD provisioning, authentication EAP-PEAP)
SSID: mgarcarz_byod_tls (secure access using EAP-TLS)

There are two wireless networks managed by Aruba AP.

The first one (mgarcarz_byod) is used for 802.1x Extensible Authentication Protocol-Protected EAP (EAP-PEAP) access.

After a successful authentication, Aruba controller must redirect user to ISE BYOD portal - Native Supplicant Provisioning (NSP) flow.

User is redirected, Network Setup Assistant (NSA) application is executed and certificate is provisioned and installed on Windows client.

ISE internal CA is used for that process (default configuration).

NSA is also responsible for creation of wireless profile for the second Service Set Identifier (SSID) managed by Aruba (mgarcarz_byod_tls) - that one is used for 802.1x Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) authentication.

As a result, corporate user is able to perform onboarding of personal device and get secure access into corporate network.

This example can be easily modified for different types of access, for example:

- Central Web Authentication (CWA) with BYOD service
- 802.1x authentication with Posture and BYOD redirection
- Typically, for EAP-PEAP authentication Active Directory is used (to keep this article short internal ISE users are used)
- Typically, for Certificate Provisioning external Simple Certificate Enrollment Protocol (SCEP) server is used, commonly Microsoft Network Device Enrollment Service (NDES) in order to keep this article short, internal ISE CA is used.

Challenges with 3rd Party Support

There are the challenges when you use ISE Guest flows (like BYOD, CWA, NSP, Client Provisioning Portal (CPP)) with 3rd party devices.

Sessions

Cisco Network Access Devices (NAD) uses Radius cisco-av-pair called audit-session-id in order to inform Authentication, Authorization, and Accounting (AAA) server about session ID.

That value is used by ISE in order to track the sessions and provide the correct services for each flow. Other vendors do not support cisco-av pair.

ISE has to rely on IETF attributes received in Access-Request and Accounting Request.

After you receive Access-Request, ISE builds synthesized Cisco Session ID (from Calling-Station-ID, NAS-Port, NAS-IP-Address and shared secret). That value has a local significance only (not sent via network).

As a result, it's expected from every flow (BYOD, CWA, NSP, CPP) to attach correct attributes - so ISE is able to recalculate Cisco Session ID and perform a lookup in order to correlate it with the correct session and continue the flow.

URL Redirect

ISE uses Radius cisco-av-pair called url-redirect and url-redirect-acl in order to inform NAD that specific traffic must be redirected.

Other vendors do not support cisco-av pair. So typically, those devices must be configured with static redirection URL which points to specific service (Authorization Profile) on ISE.

Once the user initiates HTTP session, those NADs redirect to the URL and also attach additional arguments (like IP address or MAC address) in order to allow ISE identify specific session and continue the flow.

CoA

ISE uses Radius cisco-av-pair called subscriber:command, subscriber:reauthenticate-type in order to indicate what actions must NAD take for a specific session.

Other vendors do not support cisco-av pair. So typically, those devices use RFC CoA (3576 or 5176) and one of the two defined messages:

- disconnect request (called also packet of disconnect) - that one is used to disconnect the session (very often to force reconnection)
- CoA push - that one is used to change session status transparently without disconnection (for example VPN session and new ACL applied)

ISE supports both Cisco CoA with cisco-av-pair and also both RFC CoA 3576/5176.

Solution on ISE

In order to support 3rd party vendors, ISE 2.0 introduced a concept of Network Device Profiles which describes how specific vendor behaves - how Sessions, URL Redirect and CoA is supported.

Authorization Profiles are of specific type (Network Device Profile) and once the authentication occurs ISE behavior is derived from that profile.

As a result, devices from other vendors can be managed easily by ISE. Also configuration on ISE is flexible and allows to tune or create new Network Device Profiles.

This article presents the usage of default profile for Aruba device.

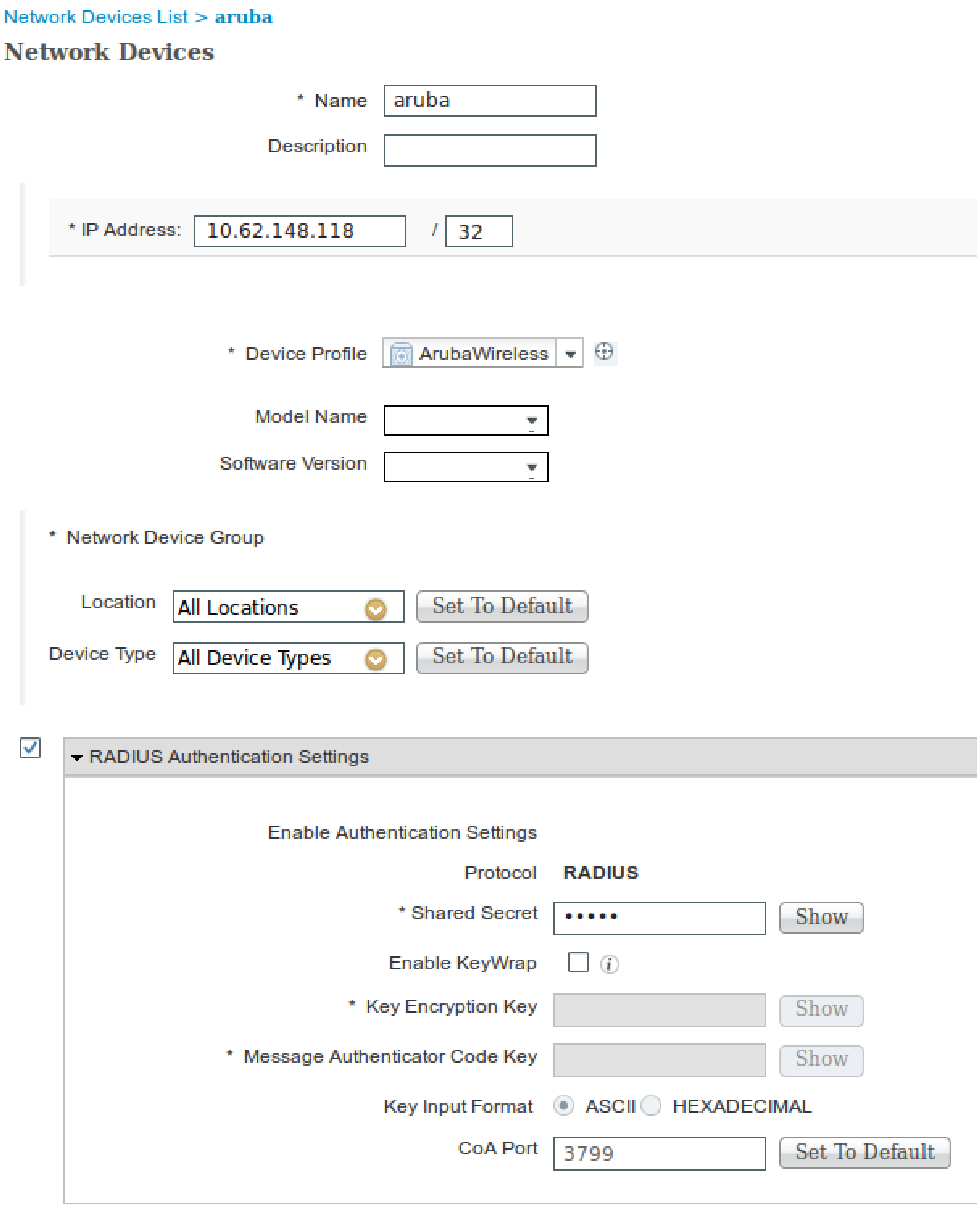
More information on the feature:

Network Access Device Profiles with Cisco Identity Services Engine

Cisco ISE

Step 1. Add Aruba Wireless Controller to Network Devices

Navigate to **Administration > Network Resources > Network Devices.** Choose correct Device Profile for selected vendor, in this case: **ArubaWireless.** Ensure to configure **Shared Secret** and **CoA port** as shown in the images.



Network Devices List > **aruba**

Network Devices

* Name: aruba

Description:

* IP Address: 10.62.148.118 / 32

* Device Profile: ArubaWireless

Model Name:

Software Version:

* Network Device Group

Location: All Locations [Set To Default]

Device Type: All Device Types [Set To Default]

☑ RADIUS Authentication Settings

Enable Authentication Settings

Protocol: **RADIUS**

* Shared Secret: ••••• [Show]

Enable KeyWrap: □

* Key Encryption Key: [Show]

* Message Authenticator Code Key: [Show]

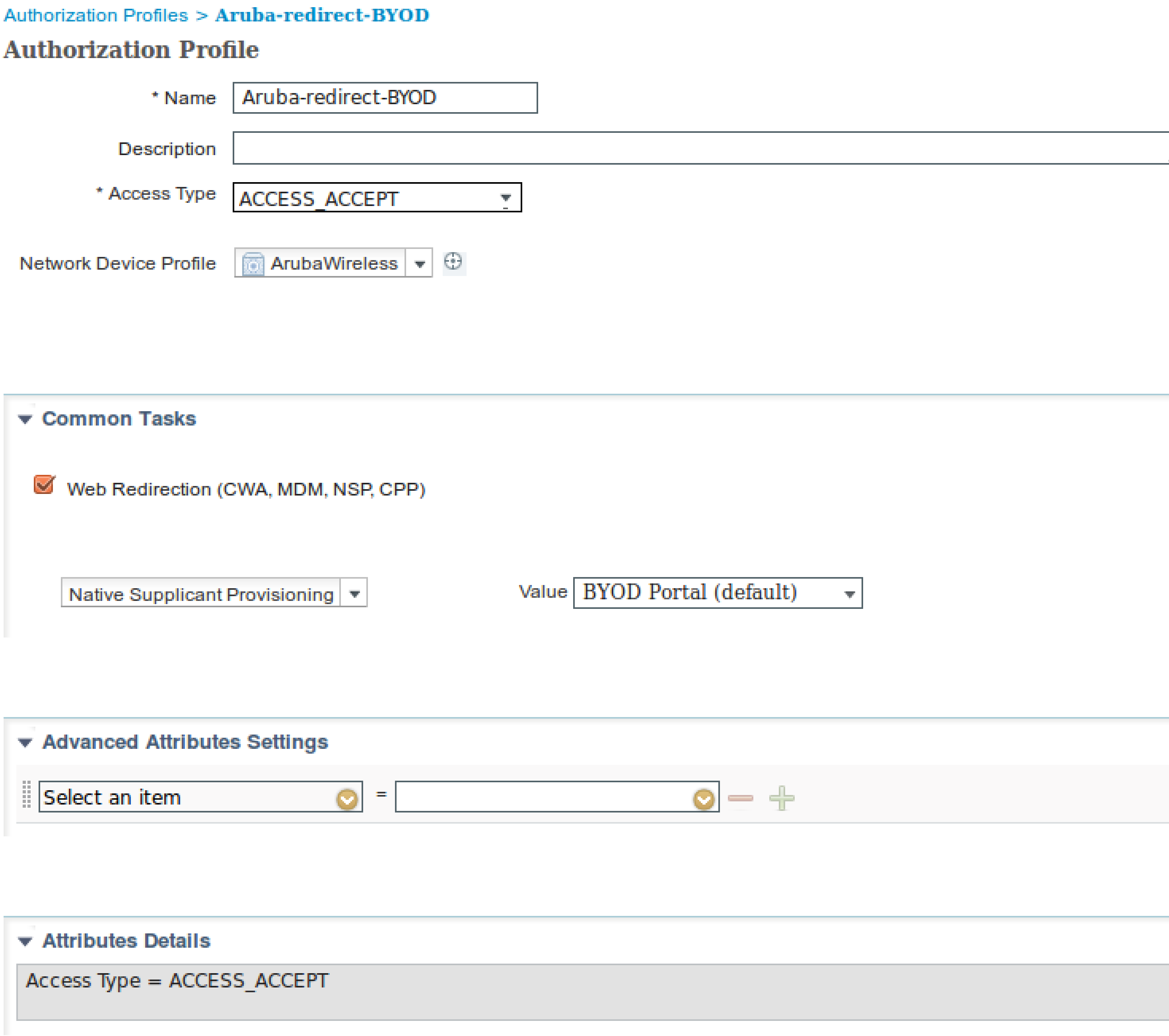
Key Input Format: ● ASCII ○ HEXADECIMAL

CoA Port: 3799 [Set To Default]

In case, there is no available profile for the desired vendor, it can be configured under **Administration > Network Resources > Network Device Profiles**.

Step 2. Configure Authorization Profile

Navigate to **Policy > Policy Elements > Results > Authorization > Authorization Profiles** choose the same **Network Device Profile** as in Step 1. **ArubaWireless**. The profile configured is **Aruba-redirect-BYOD with BYOD Portal** and as shown in the images.



Authorization Profiles > Aruba-redirect-BYOD

Authorization Profile

* Name: Aruba-redirect-BYOD

Description:

* Access Type: ACCESS_ACCEPT

Network Device Profile: ArubaWireless

Common Tasks

☑ Web Redirection (CWA, MDM, NSP, CPP)

Native Supplicant Provisioning — Value: BYOD Portal (default)

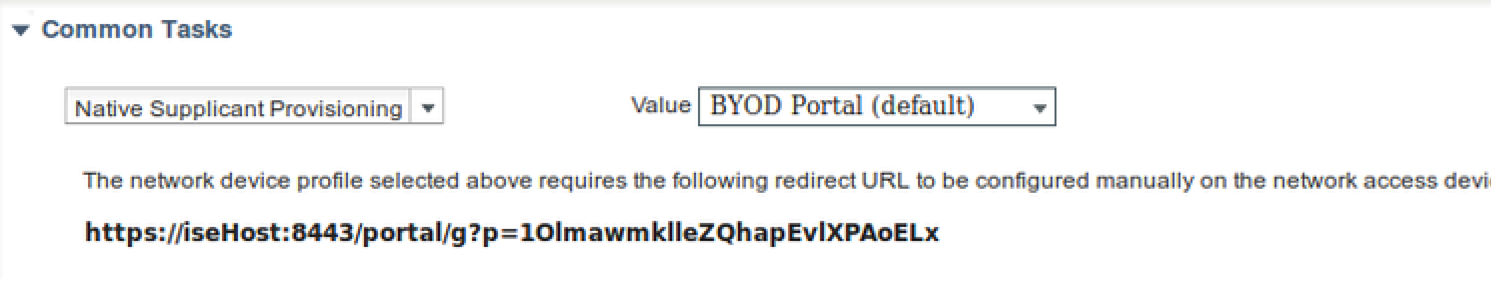
Advanced Attributes Settings

Select an item =

Attributes Details

Access Type = ACCESS_ACCEPT

Missing part of the Web Redirection configuration, where static link to Authorization Profile is generated. While Aruba doesn't support dynamic redirection to guest portal, there is one link assigned to each Authorization profile, which is then configured on Aruba and as shown in the image.



Common Tasks

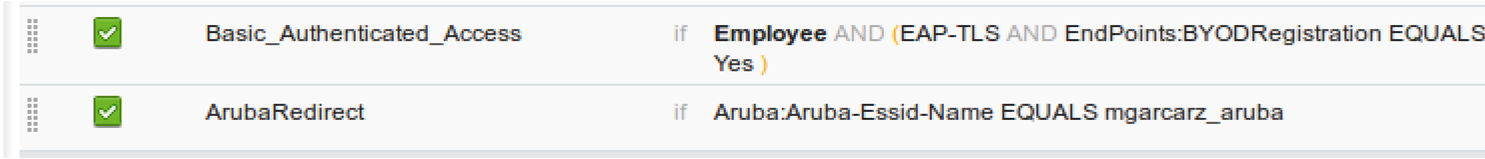
Native Supplicant Provisioning — Value: BYOD Portal (default)

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

https://iseHost:8443/portal/g?p=1OlmawmklleZQhapEvlXPAoELx

Step 3. Configure Authorization Rules

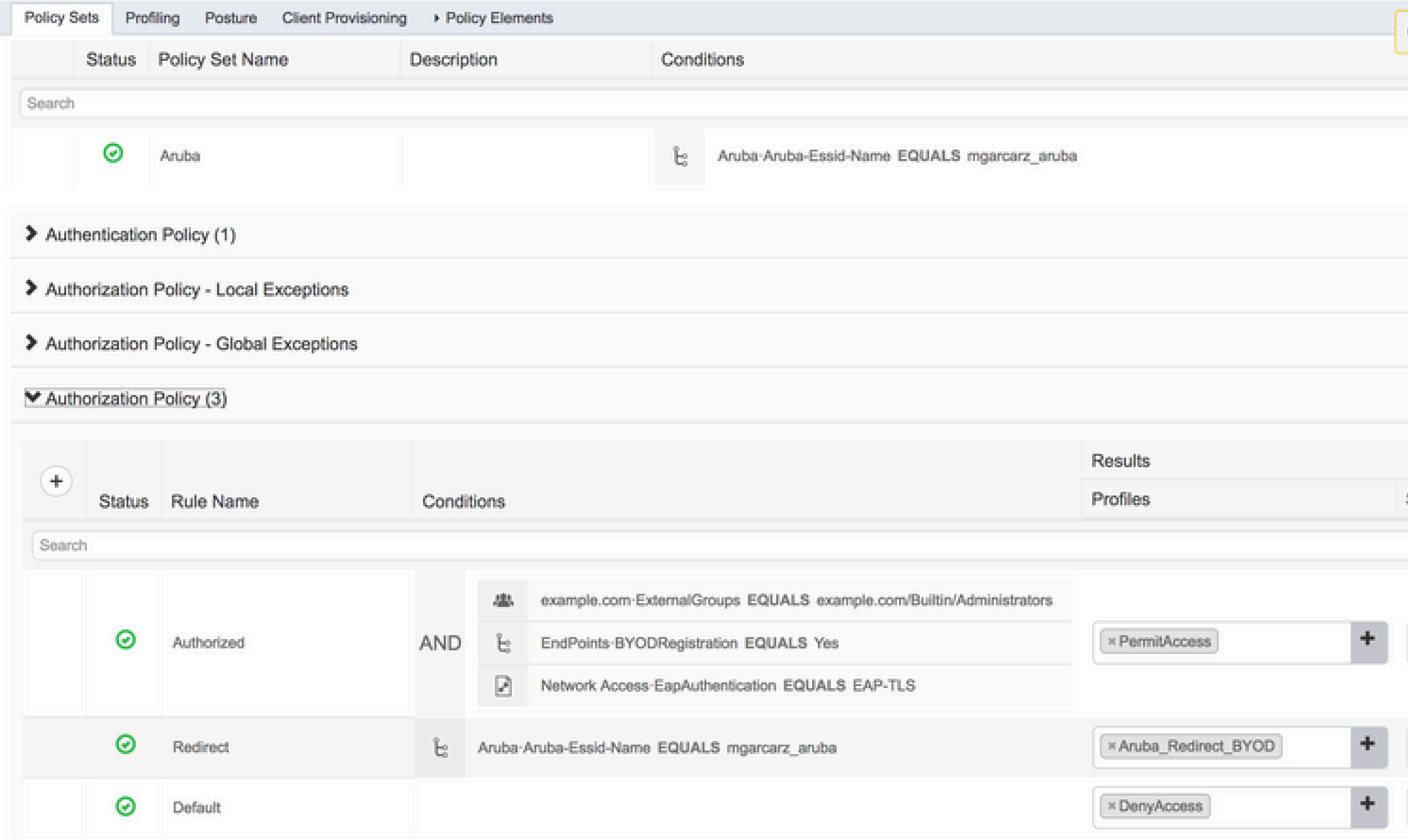
Navigate to **Policy > Authorization Rules** and the configuration is as shown in the image.



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

First, user connects to SSID mgracarz_aruba and ISE returns Authorization Profile Aruba-redirect-BYOD which redirects client to default BYOD portal. After the completion of BYOD process, client connects with EAP-TLS and full access to the network is granted.

In the newer versions of ISE the same Policy might look like the following:


Policy Sets
Profiling
Posture
Client Provisioning
Policy Elements
Search

Status	Policy Set Name	Description	Conditions
✓	Aruba		Aruba·Aruba-Essid-Name EQUALS mgarcarz_aruba

Authentication Policy (1)
Authorization Policy - Local Exceptions
Authorization Policy - Global Exceptions
Authorization Policy (3)

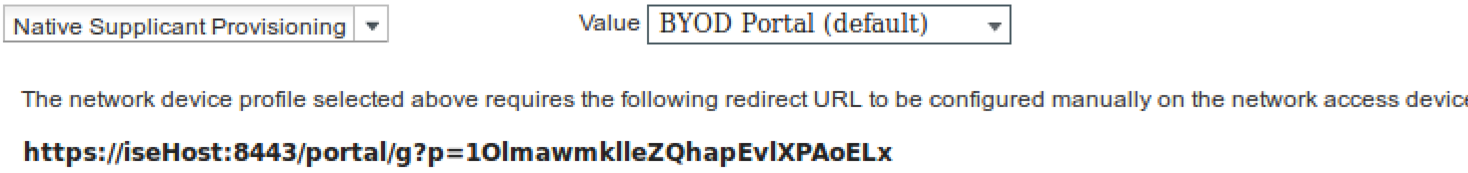
Status	Rule Name	Conditions		Results Profiles
✓	Authorized	AND	example.com·ExternalGroups EQUALS example.com/Builtin/Administrators EndPoints·BYODRegistration EQUALS Yes Network Access·EapAuthentication EQUALS EAP-TLS	PermitAccess
✓	Redirect		Aruba·Aruba-Essid-Name EQUALS mgarcarz_aruba	Aruba_Redirect_BYOD
✓	Default			DenyAccess

Aruba AP

Step 1. Captive Portal Configuration

In order to configure Captive Portal on Aruba 204, navigate to **Security > External Captive Portal** and add new one. Enter this information for proper configuration and as shown in the image.

- Type: Radius Authentication
- IP or hostname: ISE server
- URL: link that is created on ISE under Authorization Profile configuration; it is specific to particular Authorization Profile and can be found here under the Web Redirection configuration

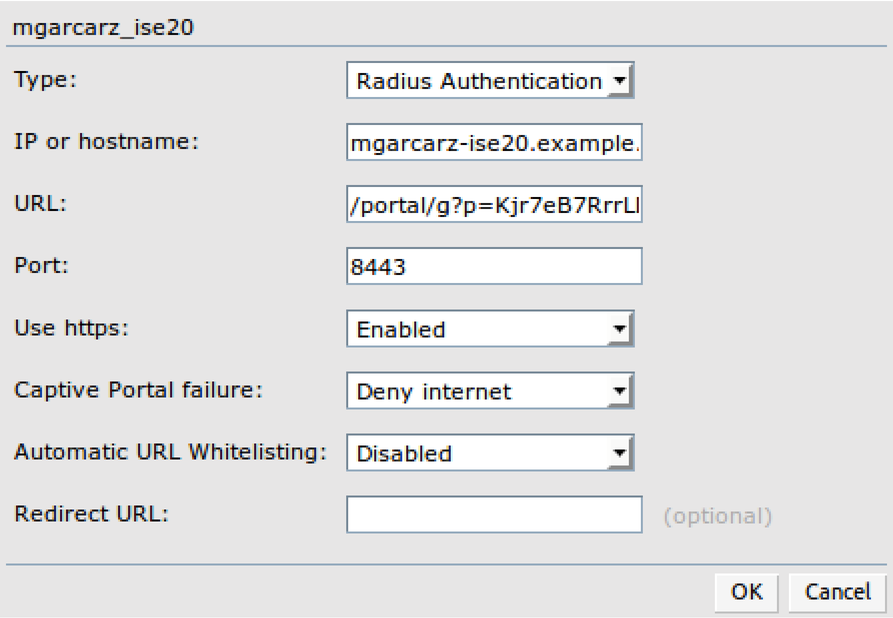

Native Supplicant Provisioning

Value: BYOD Portal (default)

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

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

- Port: port number on which selected portal is hosted on ISE (by default: 8443) as shown in the image.


mgarcarz_ise20

Type: Radius Authentication

IP or hostname: mgarcarz-ise20.example.

URL: /portal/g?p=Kjr7eB7RrrLl

Port: 8443

Use https: Enabled

Captive Portal failure: Deny internet

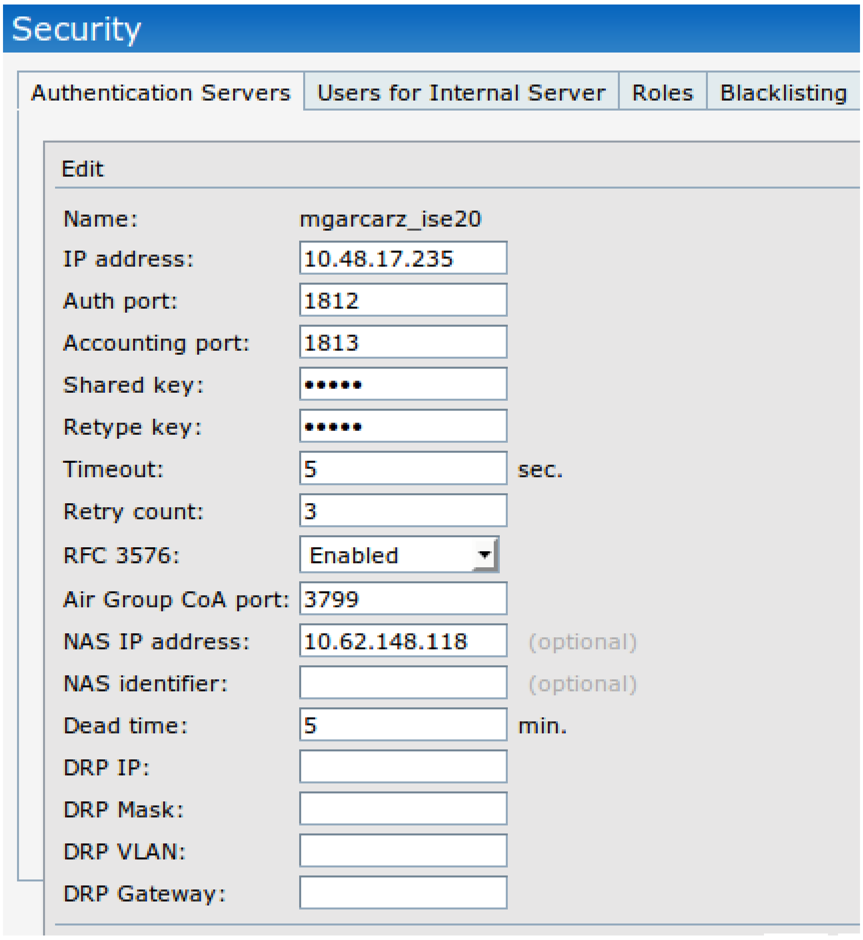
Automatic URL Whitelisting: Disabled

Redirect URL: (optional)

Step 2. Radius Server Configuration

Navigate to **Security** > **Authentication Servers** ensure that CoA port is the same as configured on ISE as shown in the image.

By default, on Aruba 204, it is set to 5999, however, that is not compliant with RFC 5176 and it also does not work with ISE.

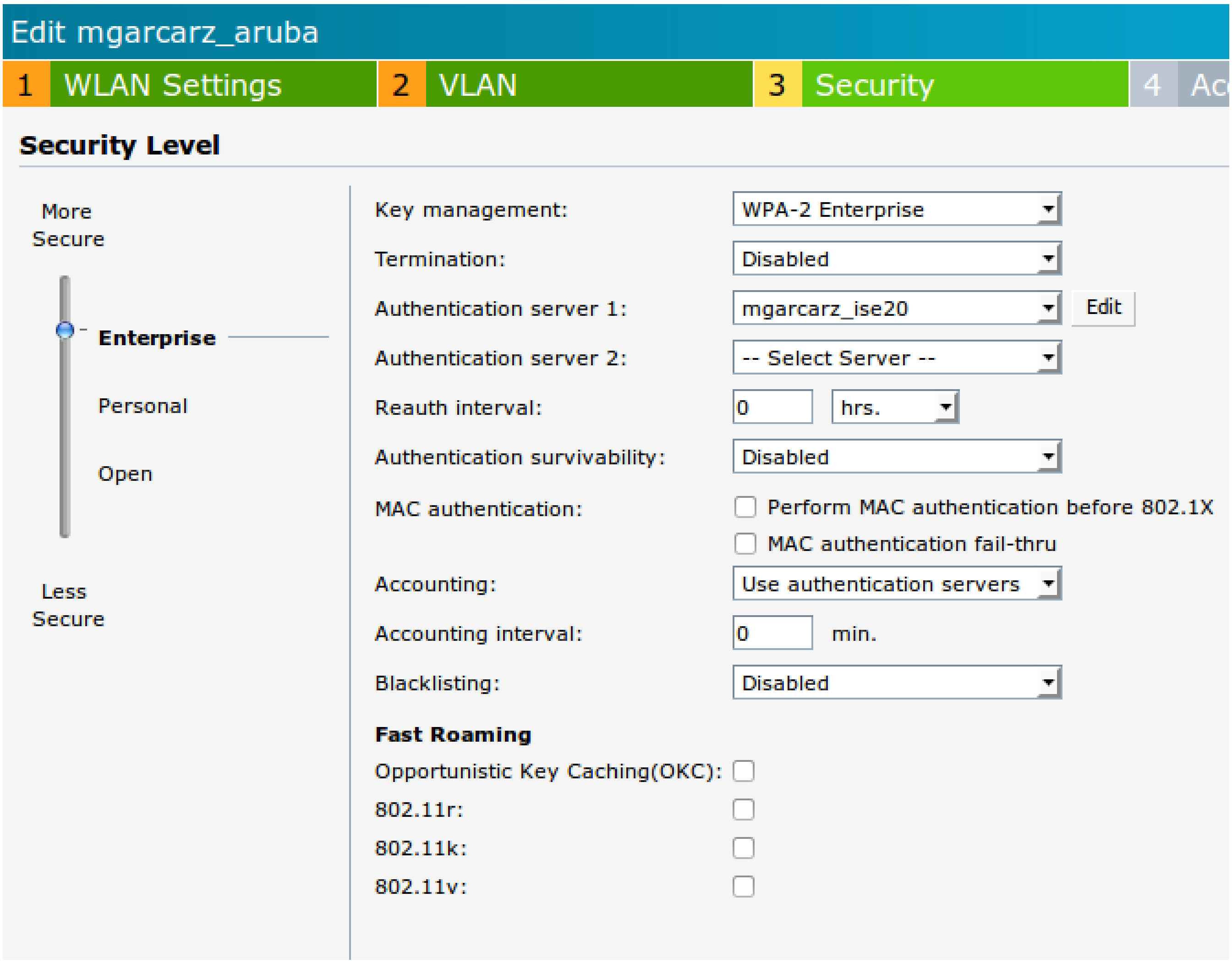


Name:	mgarcarz_ise20	
IP address:	10.48.17.235	
Auth port:	1812	
Accounting port:	1813	
Shared key:	•••••	
Retype key:	•••••	
Timeout:	5	sec.
Retry count:	3	
RFC 3576:	Enabled	
Air Group CoA port:	3799	
NAS IP address:	10.62.148.118	(optional)
NAS identifier:		(optional)
Dead time:	5	min.
DRP IP:		
DRP Mask:		
DRP VLAN:		
DRP Gateway:		

Note: In Aruba version 6.5 and newer select also "Captive Portal" checkbox.

Step 3. SSID Configuration

- Security tab is as shown in the image.



Edit mgarcarz_aruba

Security Level

Key management: WPA-2 Enterprise

Termination: Disabled

Authentication server 1: mgarcarz_ise20

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): □

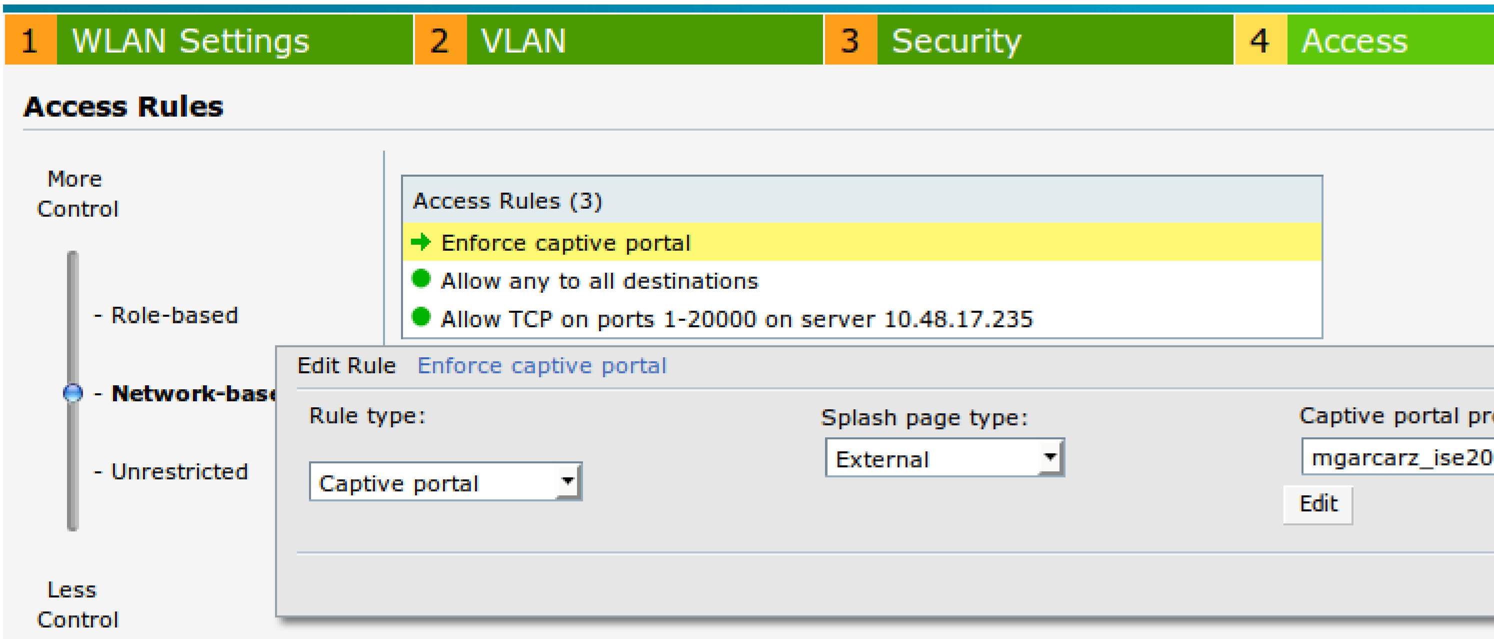
802.11r: □

802.11k: □

802.11v: □

- Access tab: select **Network-based Access Rule** in order to configure captive portal on SSID.

Use captive portal that was configured in Step 1. Click **New**, choose Rule type: **Captive portal**, Splash page type: **External** as shown in the image.



Access Rules

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

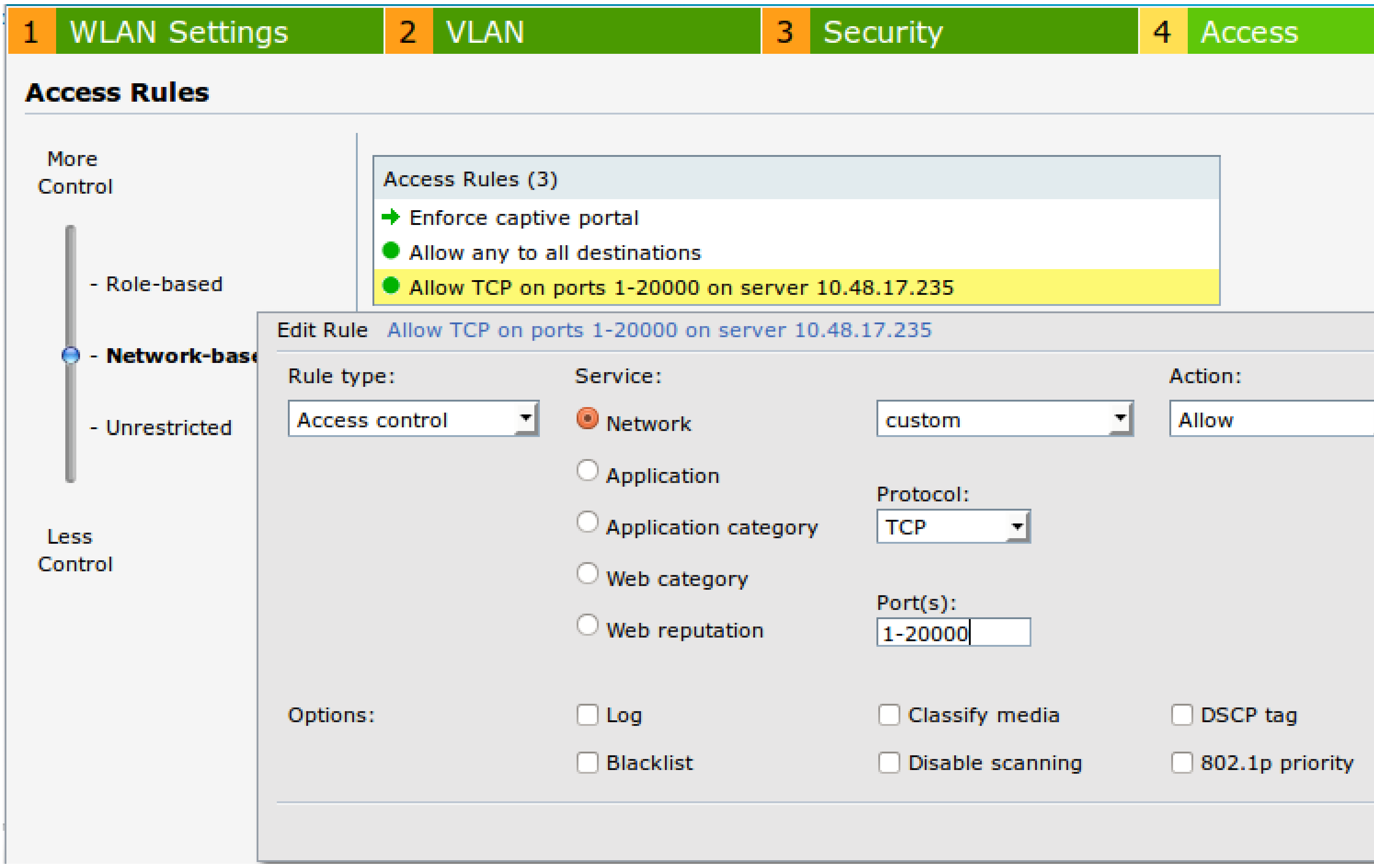
Rule type: Captive portal

Splash page type: External

Captive portal pr mgarcarz_ise20

In addition, allow all traffic to ISE server (TCP ports in range 1-20000), while rule configured by default on

Aruba: **Allow any to all destinations** seems to be not working properly as shown in the image.



Access Rules

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 Allow TCP on ports 1-20000 on server 10.48.17.235

Rule type: Access control

Service: ● Network ○ Application ○ Application category ○ Web category ○ Web reputation

custom

Protocol: TCP

Port(s): 1-20000

Action: Allow

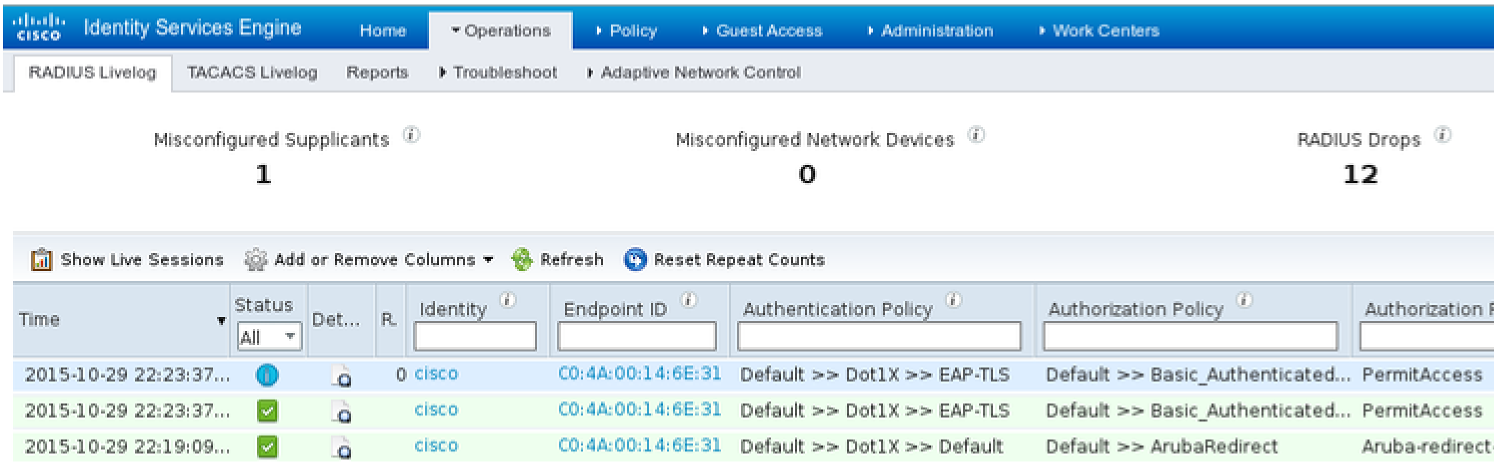
Options: □ Log □ Classify media □ DSCP tag □ Blacklist □ Disable scanning □ 802.1p priority

Verify

Use this section in order to confirm that your configuration works properly.

Step 1. Connection to SSID mgarcarz_aruba with EAP-PEAP

First authentication log on ISE appears. Default authentication policy has been used, Aruba-redirect-BYOD authorization profile has been returned as shown in the image.



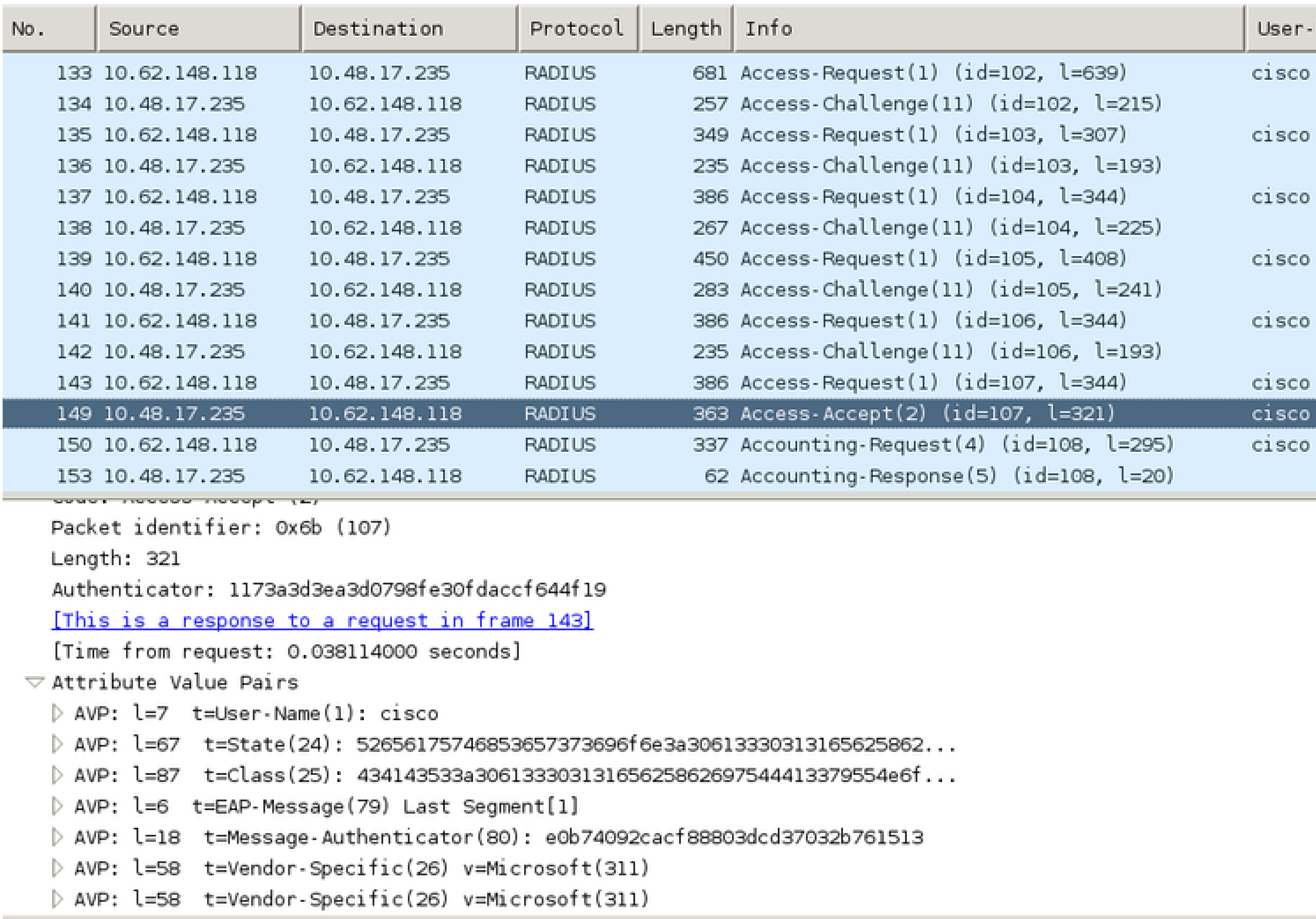
Misconfigured Supplicants 1

Misconfigured Network Devices 0

RADIUS Drops 12

Time	Status	Det...	R.	Identity	Endpoint ID	Authentication Policy	Authorization Policy	Authorization P
	All							
2015-10-29 22:23:37...	●	🔍	0	cisco	C0:4A:00:14:6E:31	Default >> Dot1X >> EAP-TLS	Default >> Basic_Authenticated...	PermitAccess
2015-10-29 22:23:37...	☑	🔍		cisco	C0:4A:00:14:6E:31	Default >> Dot1X >> EAP-TLS	Default >> Basic_Authenticated...	PermitAccess
2015-10-29 22:19:09...	☑	🔍		cisco	C0:4A:00:14:6E:31	Default >> Dot1X >> Default	Default >> ArubaRedirect	Aruba-redirect

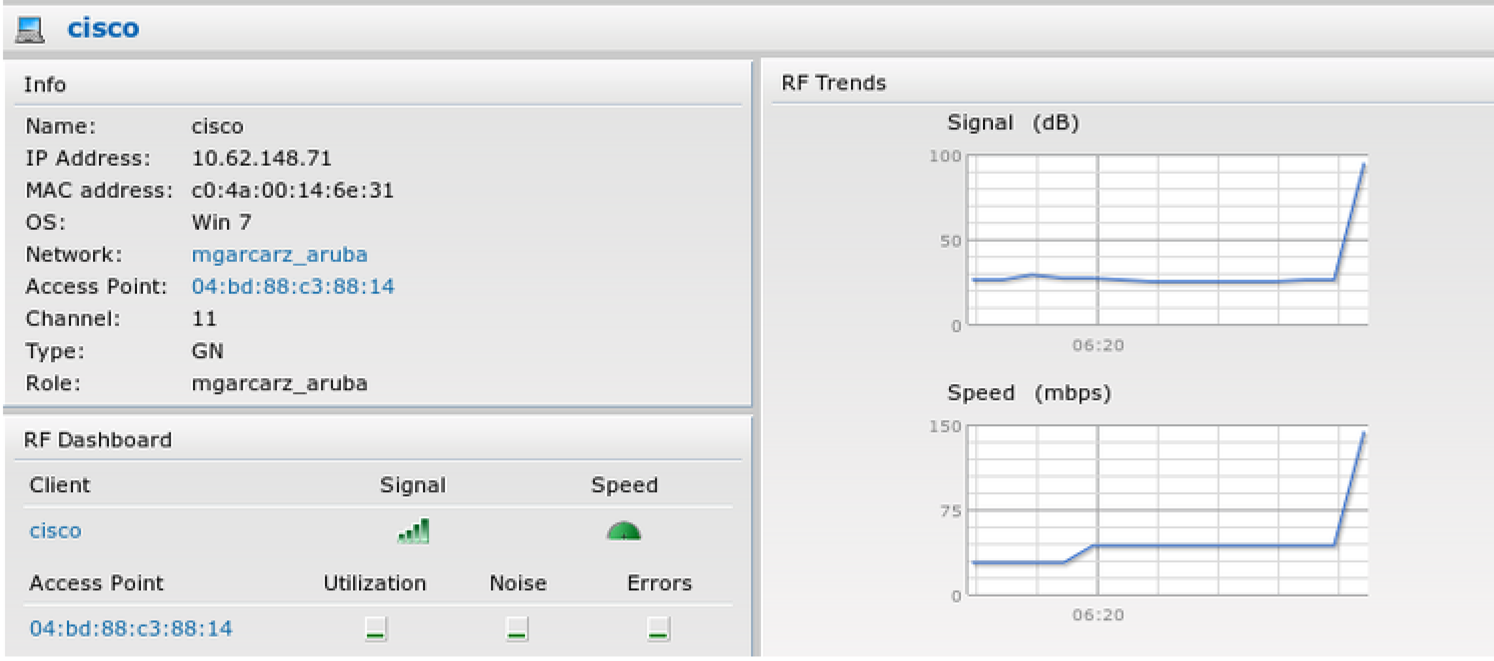
ISE returns Radius Access-Accept message with EAP Success. Note that no additional attributes are returned (no Cisco av-pair url-redirect or url-redirect-acl) as shown in the image.



```
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): 5265617574685365737369666e3a30613330313165625862...
  ▷ AVP: l=87  t=Class(25): 434143533a306133303131656258626975444133795544e6f...
  ▷ 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 reports that the session is established (EAP-PEAP identity is **cisco**) and selected Role is **mgarcarz_aruba** as shown in the image.



cisco

Info

Name: cisco
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
Role: mgarcarz_aruba

RF Dashboard

Client	Signal	Speed
cisco		

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

That role is responsible for the redirection to the ISE (captive portal functionality on Aruba).

In Aruba CLI, it is possible to confirm what is the current authorization status for that session:

<#root>

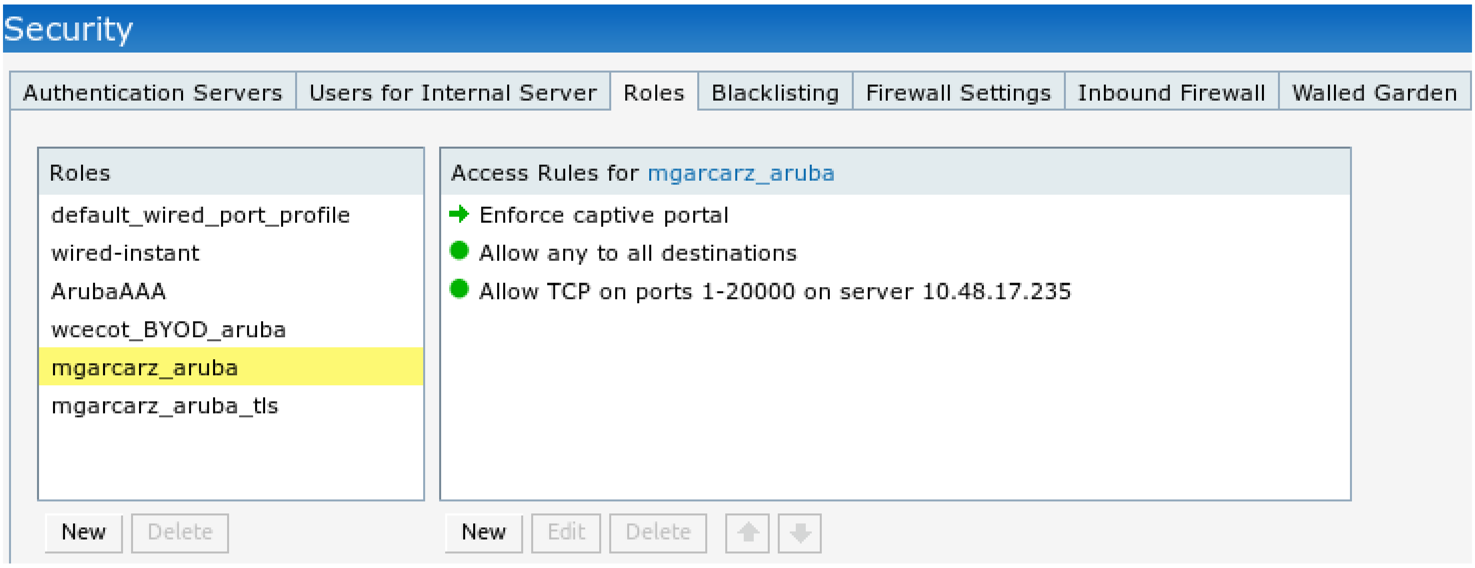
```
04:bd:88:c3:88:14#

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#
```

And in order to check ACL ID 138 for the current permissions:

<#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 ... >
```

That matches with what was configured in GUI for that Role as shown in the image.



Roles

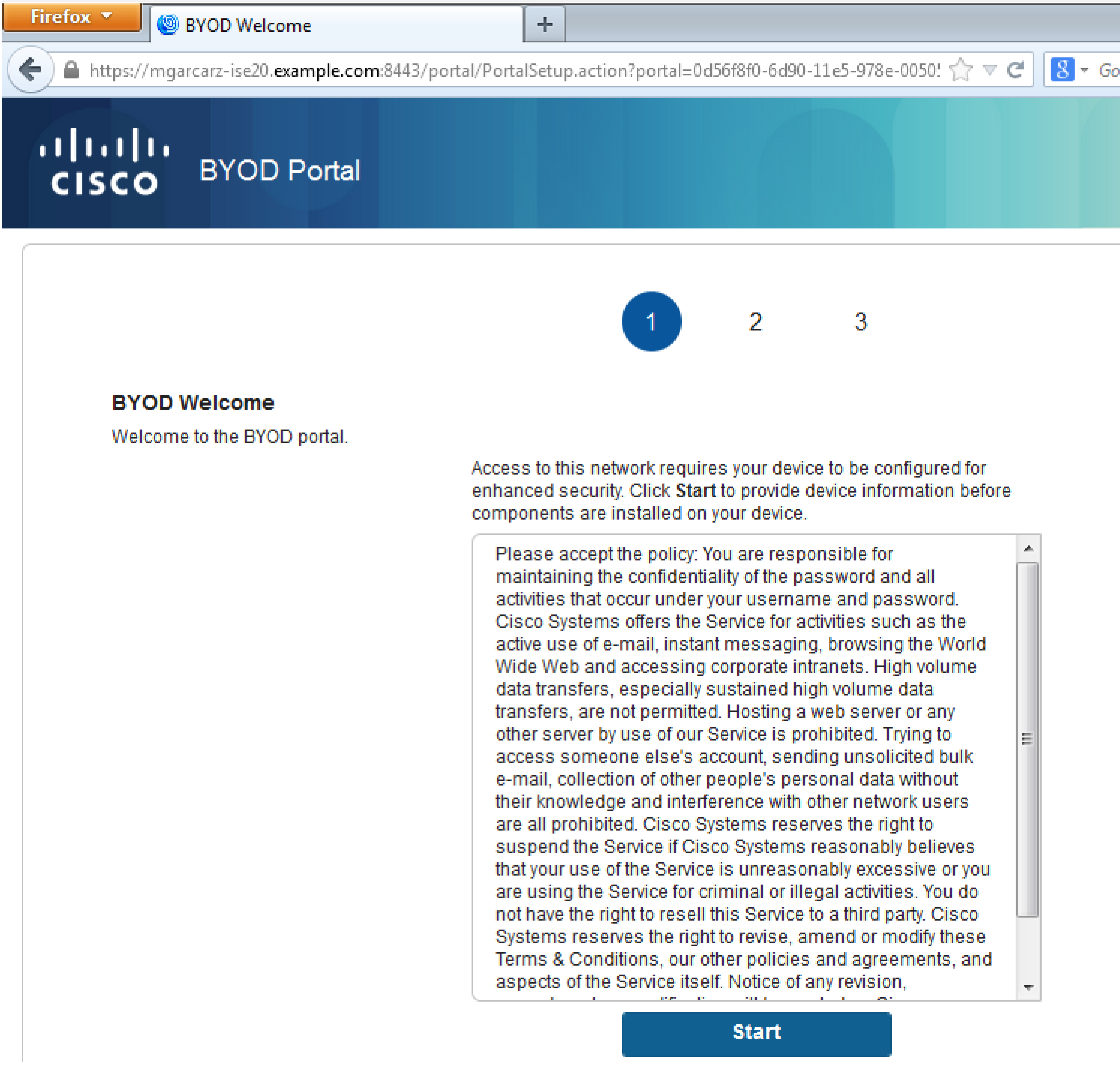
- default_wired_port_profile
- wired-instant
- ArubaAAA
- wcecot_BYOD_aruba
- mgarcarz_aruba
- mgarcarz_aruba_tls

Access Rules for mgarcarz_aruba

- ➔ Enforce captive portal
- ● Allow any to all destinations
- ● Allow TCP on ports 1-20000 on server 10.48.17.235

Step 2. Web Browser Traffic Redirection for BYOD

Once user opens the web browser and types any address, redirection occurs as shown in the image.



https://mgarcarz-ise20.example.com:8443/portal/PortalSetup.action?portal=0d56f8f0-6d90-11e5-978e-0050!

BYOD Welcome

Welcome to the BYOD portal.

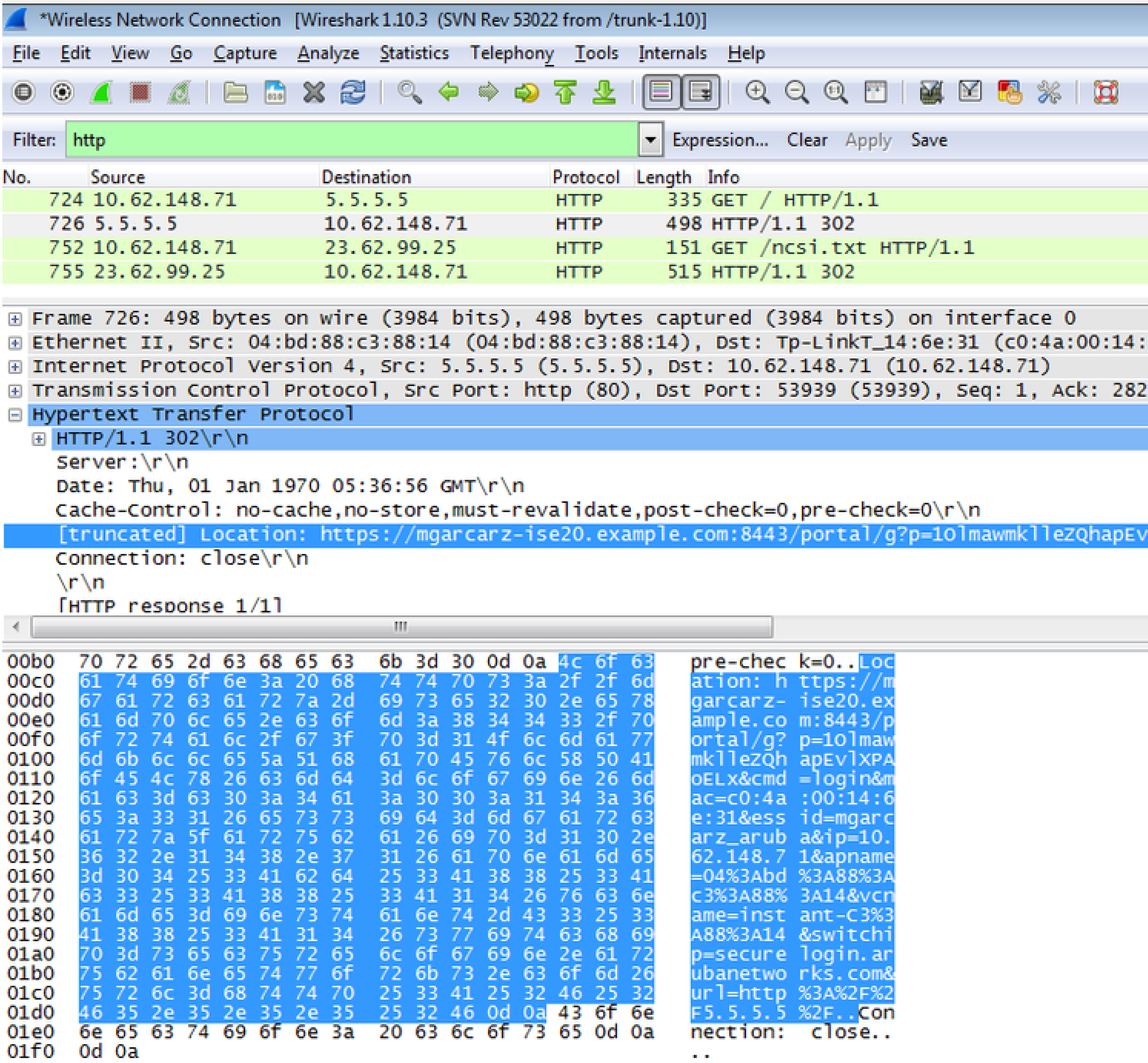
Access to this network requires your device to be configured for enhanced security. Click **Start** to provide device information before components are installed on your device.

Please accept the policy: You are responsible for maintaining the confidentiality of the password and all activities that occur under your username and password. Cisco Systems offers the Service for activities such as the active use of e-mail, instant messaging, browsing the World Wide Web and accessing corporate intranets. High volume data transfers, especially sustained high volume data transfers, are not permitted. Hosting a web server or any other server by use of our Service is prohibited. Trying to access someone else's account, sending unsolicited bulk e-mail, collection of other people's personal data without their knowledge and interference with other network users are all prohibited. Cisco Systems reserves the right to suspend the Service if Cisco Systems reasonably believes that your use of the Service is unreasonably excessive or you are using the Service for criminal or illegal activities. You do not have the right to resell this Service to a third party. Cisco Systems reserves the right to revise, amend or modify these Terms & Conditions, our other policies and agreements, and aspects of the Service itself. Notice of any revision,

Looking at the packet captures, it is confirmed that Aruba spoofs the destination (5.5.5.5) and returns the HTTP redirection to ISE.

Note that it is the same static URL as configured in ISE and copied to Captive Portal on Aruba - but additionally multiple arguments are added as follows and as shown in the image:

- cmd = login
- mac = c0:4a:00:14:6e:31
- essid = mgarcarz_aruba
- ip = 10.62.148.7
- apname = 4bd88c38814 (mac)
- url = http://5.5.5.5


*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:
⊞ 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=1OlmawmklleZQhapEv
    Connection: close\r\n
    \r\n
    [HTTP response 1/1]
```

```
00b0  70 72 65 2d 63 68 65 63  6b 3d 30 0d 0a 4c 6f 63   pre-chec k=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=1Olmaw
0100  6d 6b 6c 6c 65 5a 51 68  61 70 45 76 6c 58 50 41   mklleZQh 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&vcn
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                                              ..
```

Because of these arguments, ISE is able to recreate Cisco Session ID, find out the corresponding session on ISE and continue with BYOD (or any other configured) flow.

For Cisco devices, **audit_session_id** would be normally used but that is not supported by other vendors.

In order to confirm that from ISE debugs, it's possible to see the generation of audit-session-id value (which is never sent over the network):

<#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`

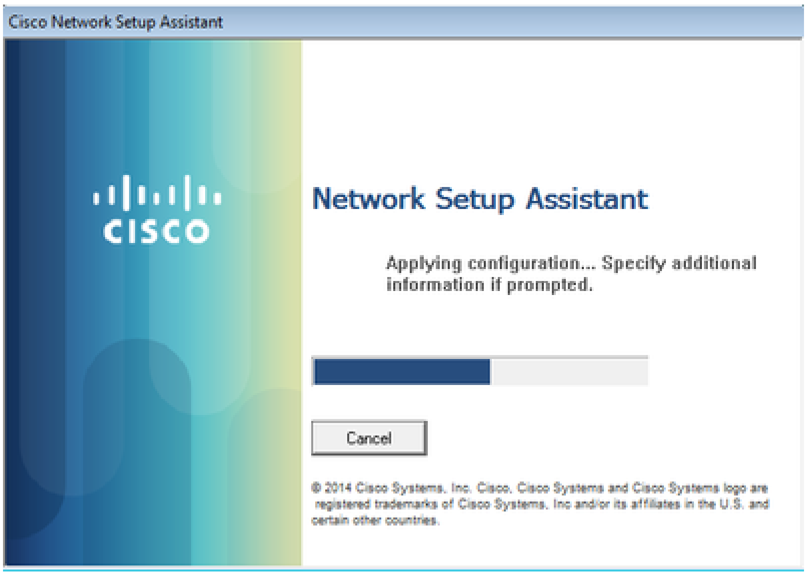
And then, correlation of that after registration of the device on BYOD Page 2:

<#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
```

In subsequent requests, client is redirected to BYOD Page 3. where NSA is downloaded and executed.

Step 3. Network Setup Assistant Execution



Cisco Network Setup Assistant

Network Setup Assistant

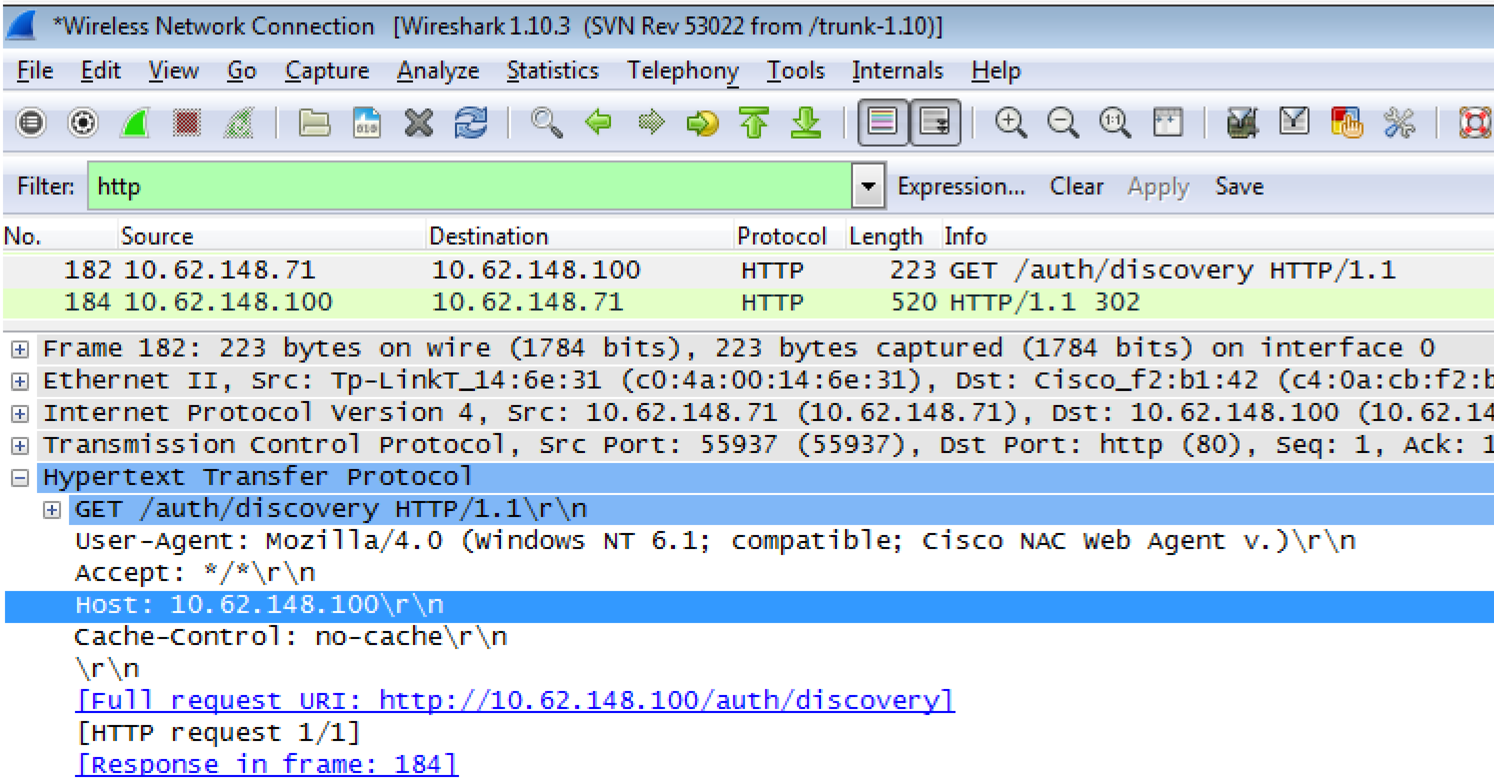
Applying configuration... Specify additional information if prompted.

© 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.

NSA has the same task as web browser. First, it needs to detect what is the IP address of ISE. That is achieved via HTTP redirection.

Because this time user does not have a possibility to type IP address (as in the web browser), that traffic is generated automatically.

Default gateway is used (also **enroll.cisco.com** can be used) as shown in the image.


*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
    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:b
⊞ Internet Protocol Version 4, Src: 10.62.148.71 (10.62.148.71), Dst: 10.62.148.100 (10.62.14
⊞ 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]
```

Response is exactly the same as for the web browser.

This way NSA is able to connect to ISE, get xml profile with configuration, generate SCEP request, send it to ISE, get signed certificate (signed by ISE internal CA), configure wireless profile and finally connect to the configured SSID.

Collect logs from the client (on Windows are in **%temp%/spwProfile.log**). Some outputs are omitted for clarity:

<#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: 0a3011ebXbiuDA3yUNoLUvtCRyuPFxkqYJ7TT06foOZ7G
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
```

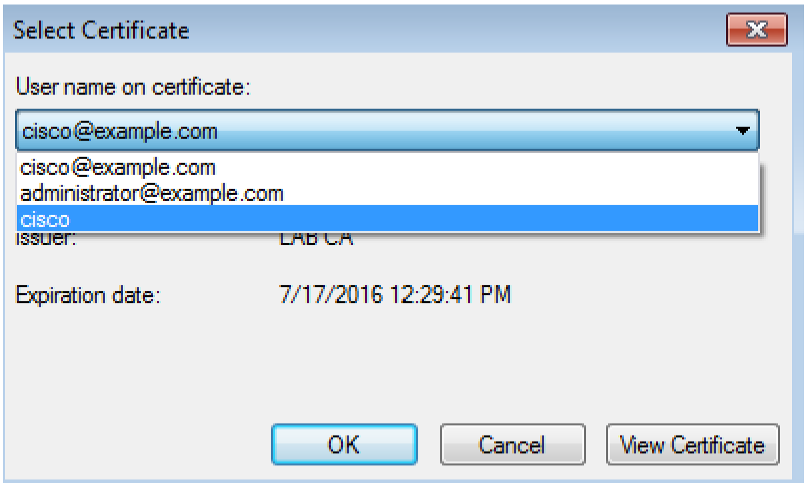
Wireless profile: [mgarcarz_aruba_tls] configured successfully

```
Connect to SSID

Successfully connected profile: [mgarcarz_aruba_tls]

WirelessProfile::SetWirelessProfile. - End
```

Those logs are exactly the same as for BYOD process with Cisco devices.

> **Note**: Radius CoA is not required here. It's the application (NSA) which forces reconnection to a newly configured SSID.

At that stage, user can see that the system tries to associate to a final SSID. If you have more then one user certificate, you must select the correct one (as shown).



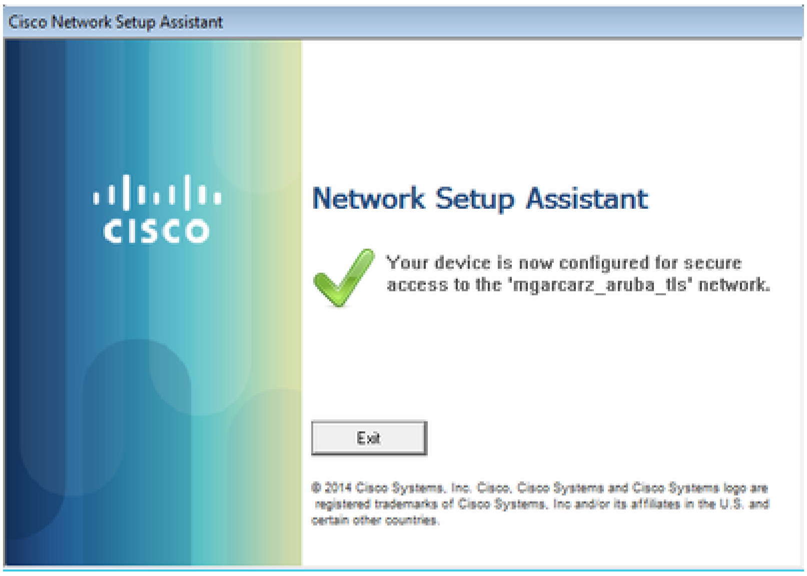
User name on certificate: cisco@example.com

cisco@example.com
administrator@example.com
cisco

Issuer: LAB CA

Expiration date: 7/17/2016 12:29:41 PM

After a successful connection, NSA reports is as shown in the image.

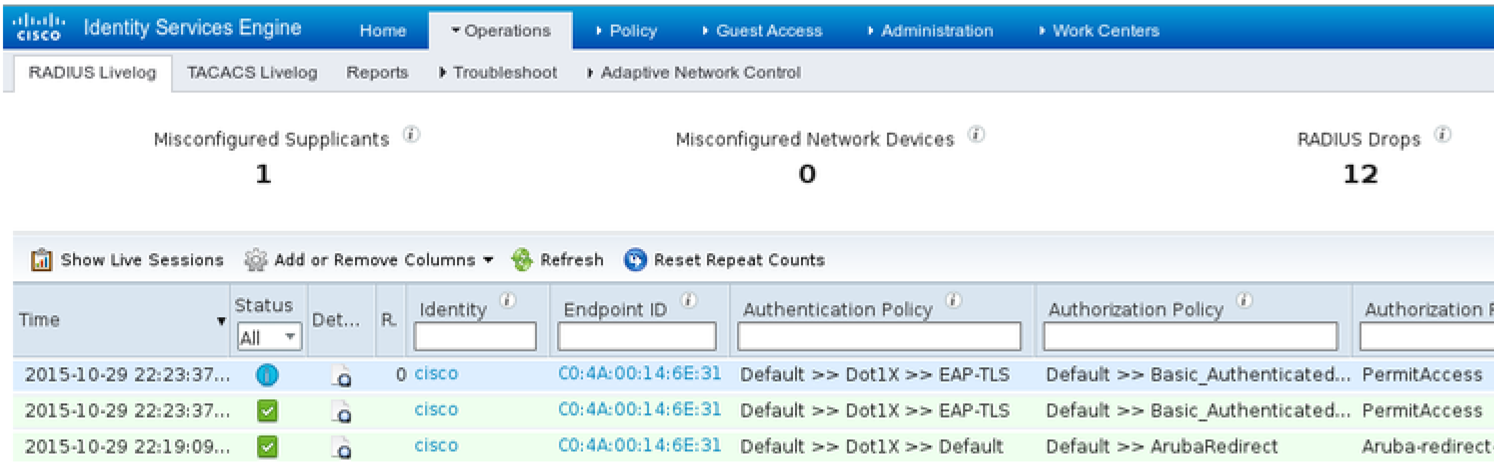


Network Setup Assistant

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

© 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.

That can be confirmed on ISE - the second log hits EAP-TLS authentication, which matches all the conditions for Basic_Authenticated_Access (EAP-TLS, Employee, and BYOD Registered true).



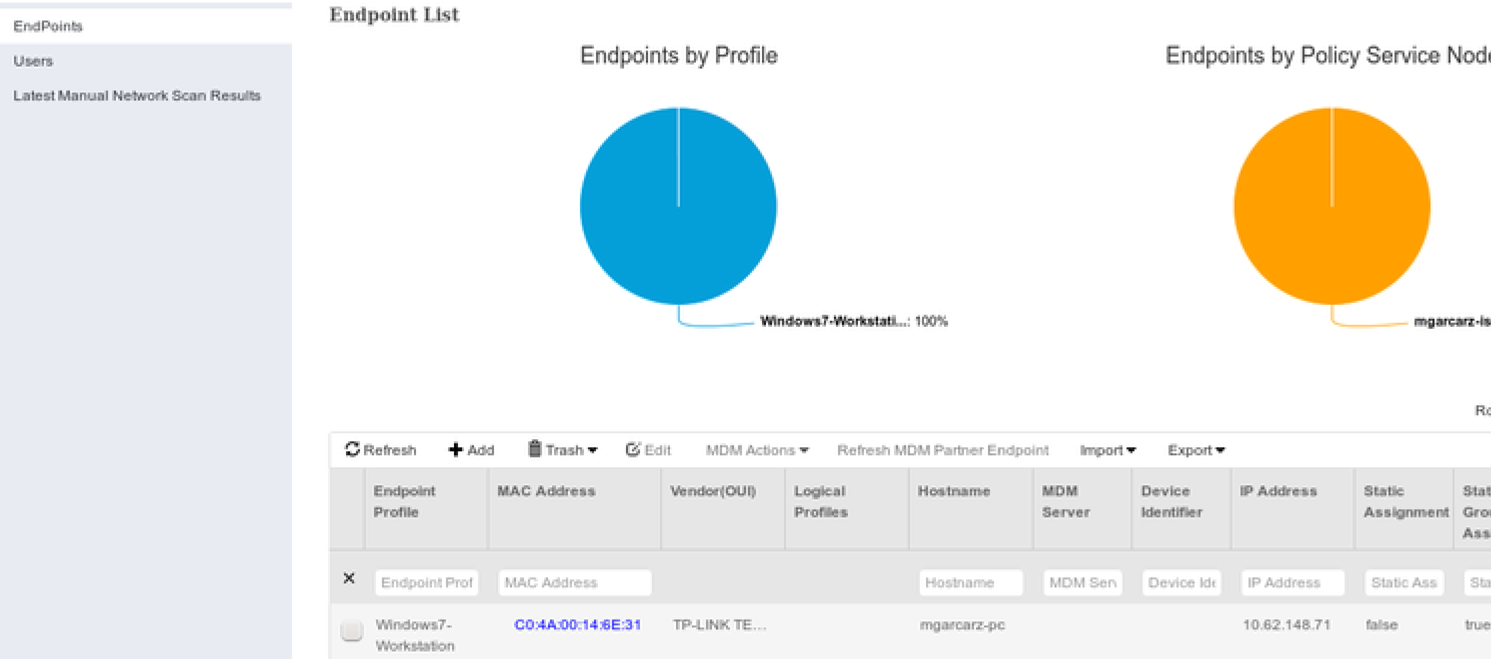
Misconfigured Supplicants 1

Misconfigured Network Devices 0

RADIUS Drops 12

Time	Status	Det...	R.	Identity	Endpoint ID	Authentication Policy	Authorization Policy	Authorization
2015-10-29 22:23:37...	●		0	cisco	C0:4A:00:14:6E:31	Default >> Dot1X >> EAP-TLS	Default >> Basic_Authenticated...	PermitAccess
2015-10-29 22:23:37...	☑			cisco	C0:4A:00:14:6E:31	Default >> Dot1X >> EAP-TLS	Default >> Basic_Authenticated...	PermitAccess
2015-10-29 22:19:09...	☑			cisco	C0:4A:00:14:6E:31	Default >> Dot1X >> Default	Default >> ArubaRedirect	Aruba-redirect

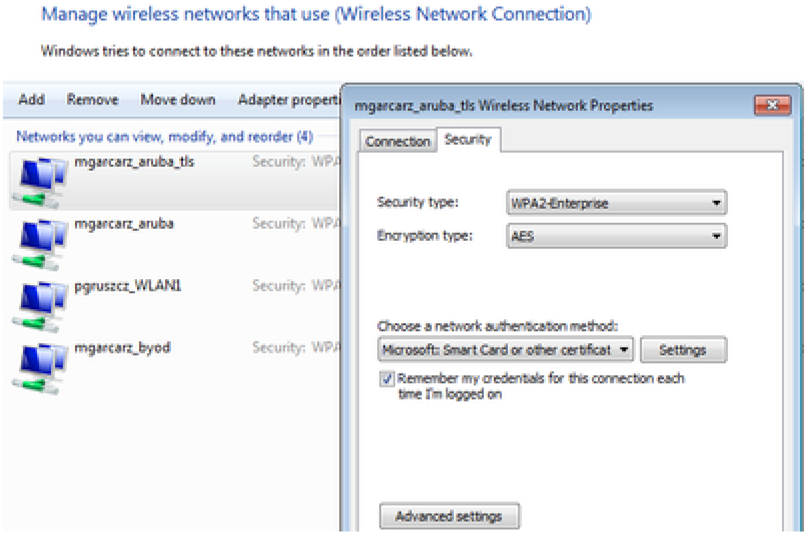
Also, endpoint identity view can confirm that endpoint has BYOD Registered flag set to true as shown in the image.



EndPoints
Users
Latest Manual Network Scan Results
Endpoint List
Endpoints by Profile
Windows7-Workstati...: 100%
Endpoints by Policy Service Nod
mgarcarz-is
Refresh
Add
Trash
Edit
MDM Actions
Refresh MDM Partner Endpoint
Import
Export

Endpoint Profile	MAC Address	Vendor(OUI)	Logical Profiles	Hostname	MDM Server	Device Identifier	IP Address	Static Assignment	Stat Gro Ass
Windows7-Workstation	C0:4A:00:14:6E:31	TP-LINK TE...		mgarcarz-pc			10.62.148.71	false	true

On Windows PC, new wireless profile has been created automatically as preferred (and configured for EAP-TLS) and as shown.



Manage wireless networks that use (Wireless Network Connection)

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

Add
Remove
Move down
Adapter properti
Networks you can view, modify, and reorder (4)
mgarcarz_aruba_tls Security: WPA
mgarcarz_aruba Security: WPA
pgruszcz_WLAN1 Security: WPA
mgarcarz_byod Security: WPA
Connection
Security
Settings
Advanced settings

mgarcarz_aruba_tls Wireless Network Properties

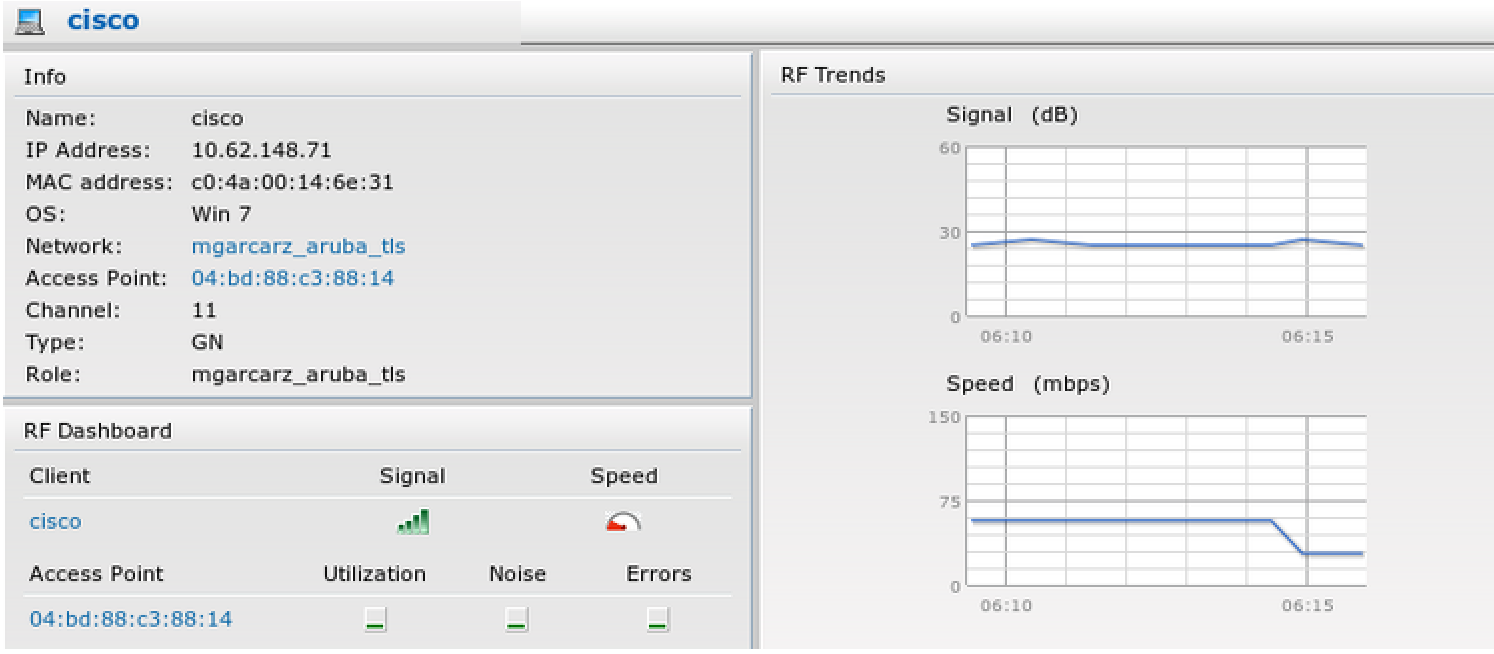
Security type: WPA2-Enterprise

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

At that stage, Aruba confirms that the user is connected to the final SSID.



cisco

Info

Name:	cisco
IP Address:	10.62.148.71
MAC address:	c0:4a:00:14:6e:31
OS:	Win 7
Network:	mgarcarz_aruba_tls
Access Point:	04:bd:88:c3:88:14
Channel:	11
Type:	GN
Role:	mgarcarz_aruba_tls

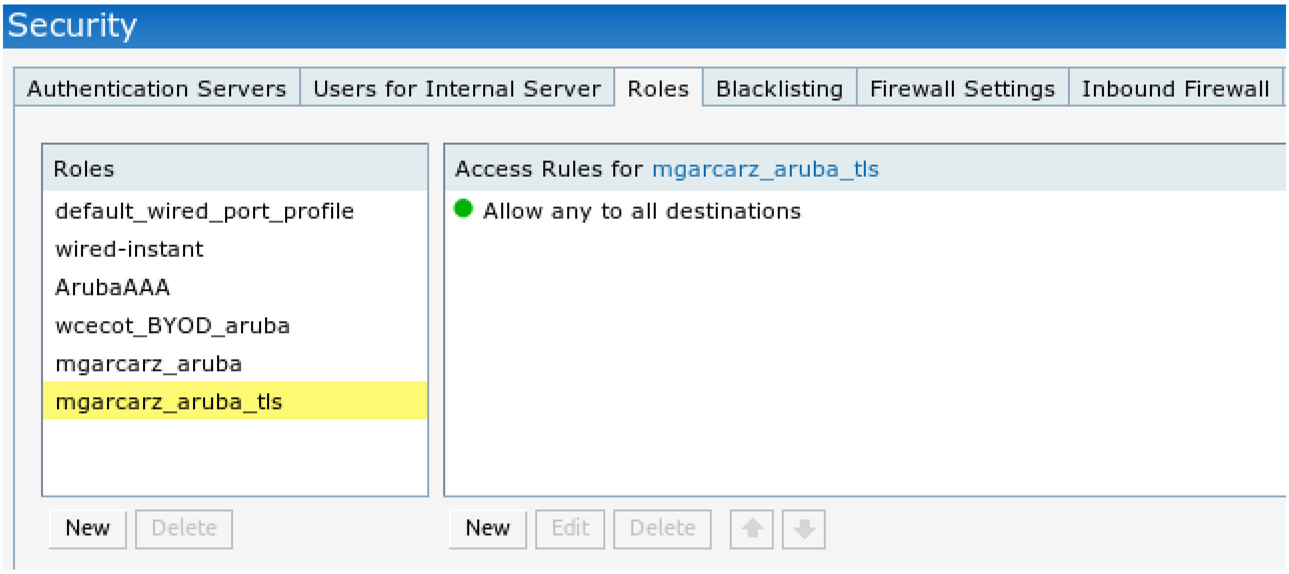
RF Dashboard

Client	Signal	Speed
cisco		

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

RF Trends

The role which is created automatically and named the same as Network provides full network access.



Security

Roles

default_wired_port_profile

wired-instant

ArubaAAA

wcecot_BYOD_aruba

mgarcarz_aruba

mgarcarz_aruba_tls

Access Rules for mgarcarz_aruba_tls

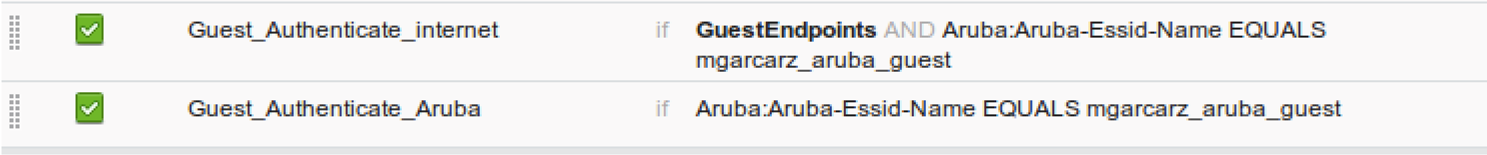
● Allow any to all destinations

Other Flows and CoA Support

CWA with CoA

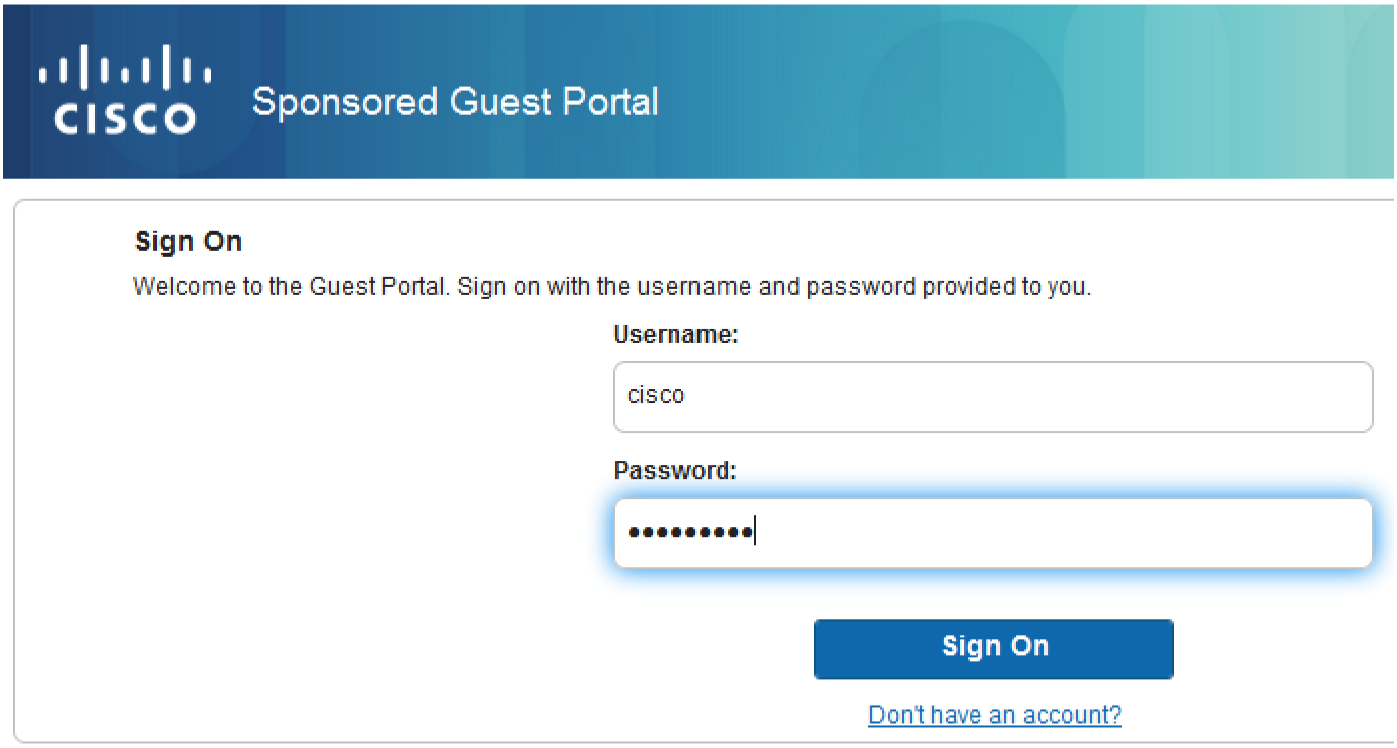
While in BYOD flow there are no CoA messages, CWA flow with Self Registered Guest Portal is demonstrated here:

The Authorization Rules configured are as shown in the image.



	☑	Guest_Authenticate_internet	if	**GuestEndpoints** AND Aruba:Aruba-Essid-Name EQUALS mgarcarz_aruba_guest
	☑	Guest_Authenticate_Aruba	if	Aruba:Aruba-Essid-Name EQUALS mgarcarz_aruba_guest

User connects to the SSID with MAB authentication and once when it tries to connect to some web page, redirection to Self Registered Guest Portal happens, where Guest can create new account or use current one.



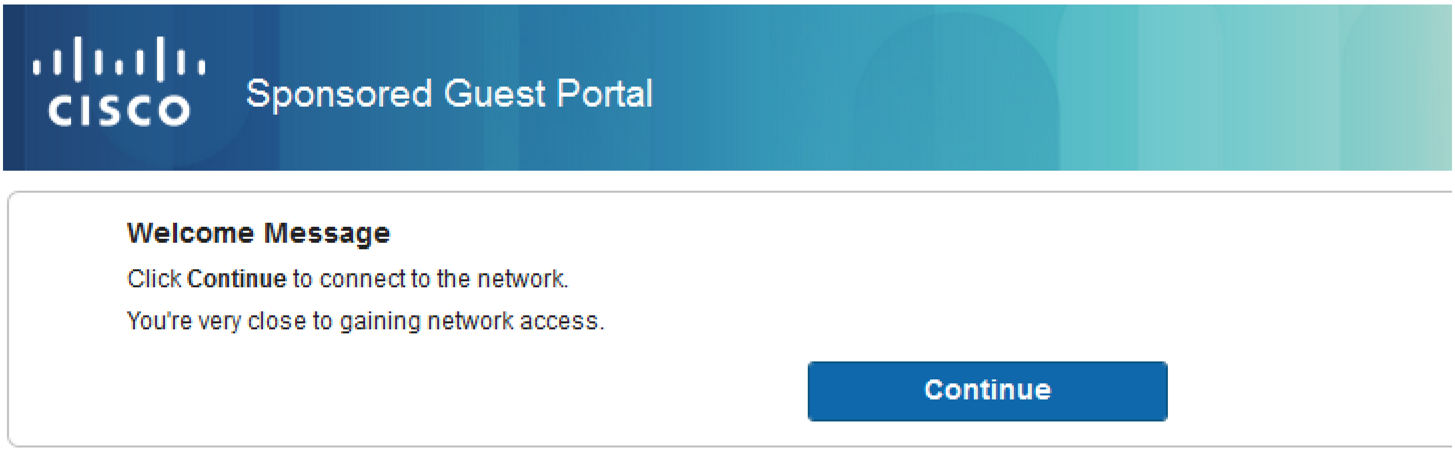
Sign On

Welcome to the Guest Portal. Sign on with the username and password provided to you.

Username: cisco

Password: ••••••••••

After the guest is successfully connected, CoA message is sent from ISE to Network Device in order to change authorization state.

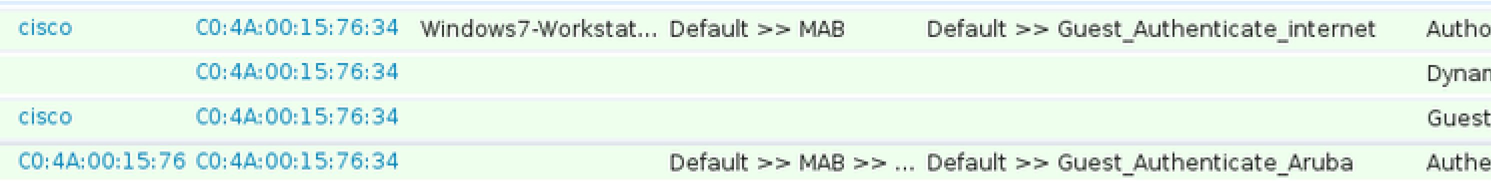


Welcome Message

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

You're very close to gaining network access.

It can be verified under **Operations** > **Authenitcations** and as shown in the image.



cisco	C0:4A:00:15:76:34	Windows7-Workstat...	Default >> MAB	Default >> Guest_Authenticate_internet	Autho
	C0:4A:00:15:76:34				Dyna
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 message in ISE debugs:

<#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
```

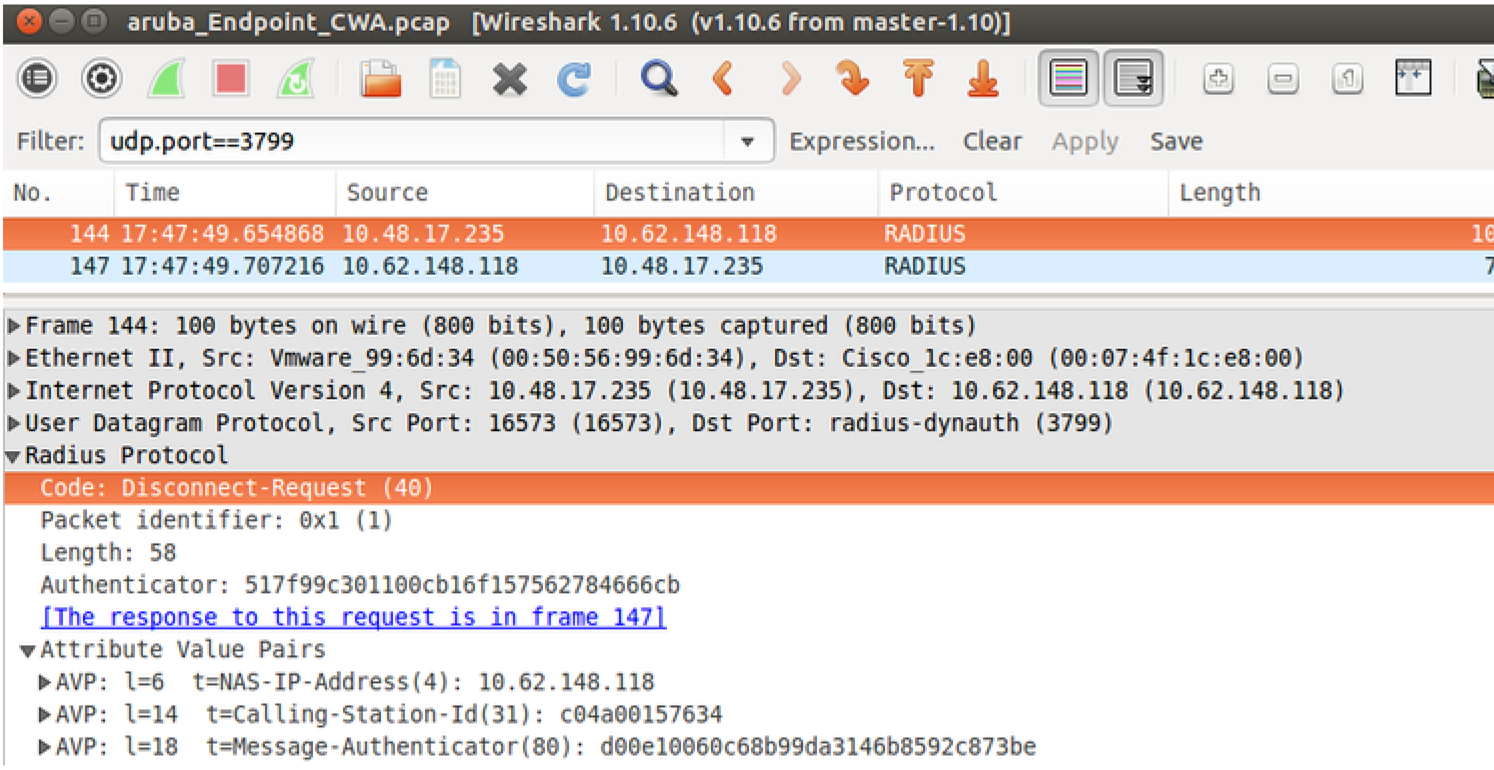
and Disconnect-ACK that comes from Aruba:

<#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
```

Packet captures with CoA Diconnect-Request (40) and Diconnect-ACK (41) is as shown.


aruba_Endpoint_CWA.pcap [Wireshark 1.10.6 (v1.10.6 from master-1.10)]
Filter:
Expression...
Clear
Apply
Save

Filter: udp.port==3799

```
No.   Time             Source         Destination    Protocol   Length
  144 17:47:49.654868  10.48.17.235   10.62.148.118  RADIUS     10
  147 17:47:49.707216  10.62.148.118  10.48.17.235   RADIUS     7
```

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

Note: RFC CoA has been used for authentication related to Device Profile Aruba (default settings). For authentication related to Cisco device, it would have been Cisco CoA type reauthenticate.

Troubleshoot

This section provides information you can use in order to troubleshoot your configuration.

Aruba Captive Portal with IP Address Instead of FQDN

If Captive Portal on Aruba is configured with IP address instead of FQDN of ISE, PSN NSA fails:

<#root>

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


CN
```

The reason for that is strict certificate validation when you connect to ISE. When you use IP address in order to connect to ISE (as a result of redirection URL with IP address instead of FQDN) and are presented with

ISE certificate with Subject Name = FQDN validation fails.

> **Note**: Web browser continues with BYOD portal (with warning which needs to be approved by user).

Aruba Captive Portal Incorrect Access Policy

By default, Aruba Access-Policy configured with Captive Portal allows for tcp ports 80, 443 and 8080.

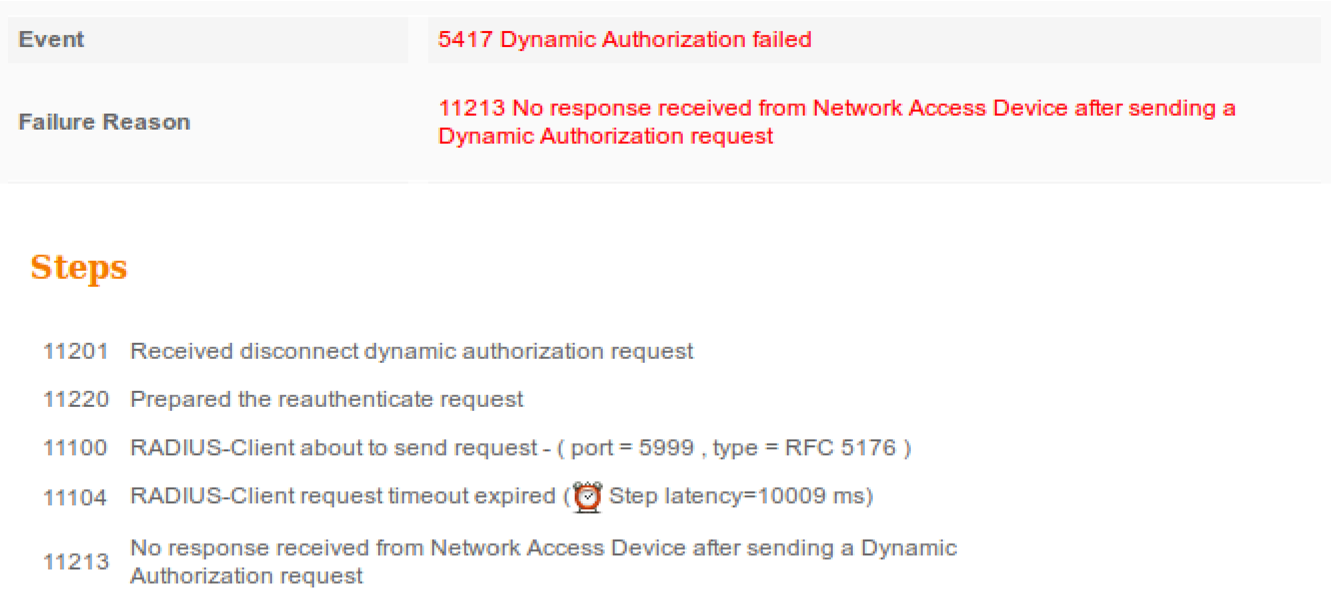
NSA is not able to connect to tcp port 8905 in order to get xml profile from ISE. This error is reported:

<#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 Port Number

By default, Aruba provides port number for CoA **Air Group CoA port** 5999. Unfortunately, Aruba 204 did not respond to such requests (as shown).

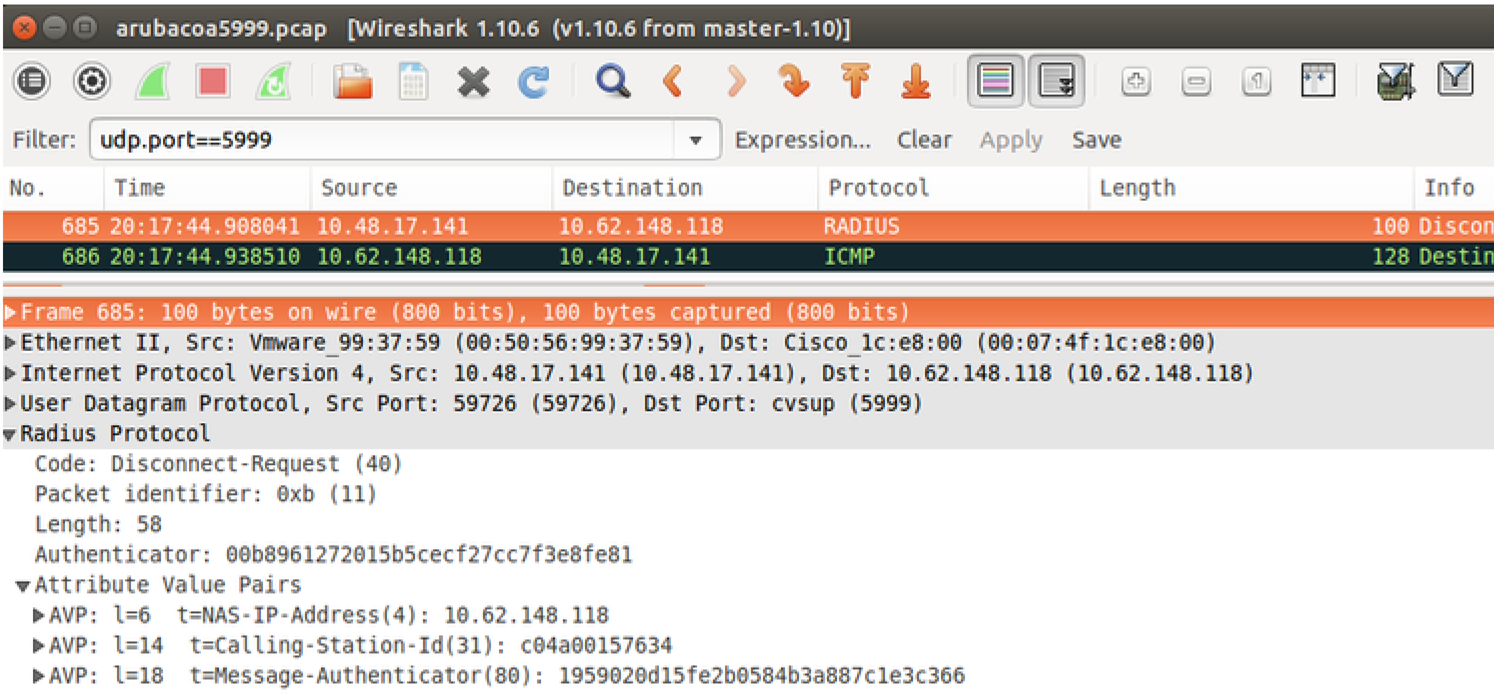


Event	5417 Dynamic Authorization failed
Failure Reason	11213 No response received from Network Access Device after sending a Dynamic Authorization request

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 capture is as shown in the image.

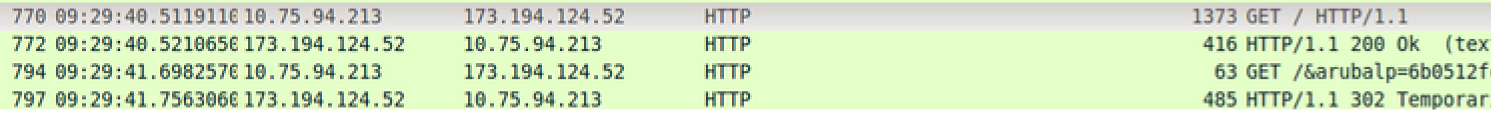

arubacoa5999.pcap [Wireshark 1.10.6 (v1.10.6 from master-1.10)]
Filter:
Expression...
Clear
Apply
Save

```
Filter: udp.port==5999

No.   Time             Source         Destination    Protocol   Length   Info
  685 20:17:44.908041 10.48.17.141   10.62.148.118  RADIUS              100 Discon
  686 20:17:44.938510 10.62.148.118  10.48.17.141   ICMP                128 Destin

▶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
```

The best option to use here can be CoA port 3977 as described in RFC 5176.

Redirection on Some Aruba Devices

On Aruba 3600 with v6.3 it is noticed that the redirection works slightly different then on other controllers. Packet capture and explanation can be found here.



```
770 09:29:40.5119110 10.75.94.213    173.194.124.52  HTTP   1373 GET / HTTP/1.1
772 09:29:40.5210650 173.194.124.52  10.75.94.213    HTTP    416 HTTP/1.1 200 Ok  (tex
794 09:29:41.6982570 10.75.94.213    173.194.124.52  HTTP     63 GET /&arubalp=6b0512f
797 09:29:41.7563060 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&essid=SC%2DWiFi&apname=LRC-006&apgroup=default&url=http%3A%2F%2Fw

Related Information

- Cisco Identity Services Engine Administrator Guide, Release 2.0
- Network Access Device Profiles with Cisco Identity Services Engine

- Technical Support & Documentation - Cisco Systems