

Aruba Wirelessを使用したISE 2.0サードパーティ統合の設定

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[設定](#)

[ネットワーク図](#)

[サードパーティサポートの課題](#)

[セッション](#)

[URLリダイレクト](#)

[CoA](#)

[ISEでのソリューション](#)

[Cisco ISE](#)

[ステップ1: ネットワークデバイスへのArubaワイヤレスコントローラの追加](#)

[ステップ2: 許可プロファイルの設定](#)

[ステップ3: 許可ルール \(Authorization Rule \) の設定](#)

[Aruba AP](#)

[ステップ1: キャプティブポータルの設定](#)

[ステップ2: RADIUS サーバの設定](#)

[ステップ3: SSID 設定](#)

[確認](#)

[ステップ1: EAP-PEAPを使用したSSID mgarcarz_arubawithへの接続](#)

[ステップ2: BYODのためのWebブラウザトラフィックリダイレクション](#)

[ステップ3: ネットワークセットアップアシスタントの実行](#)

[その他のフローおよび CoA サポート](#)

[CoA を含む CWA](#)

[トラブルシューティング](#)

[FQDNではなくIPアドレスを使用するArubaキャプティブポータル](#)

[Aruba キャプティブ ポータルのアクセス ポリシーが正しくない](#)

[Aruba CoA のポート番号](#)

[Aruba デバイスでのリダイレクション](#)

[関連情報](#)

はじめに

このドキュメントでは、Cisco Identity Services Engine(ISE)のサードパーティ統合機能をトラブルシューティングする方法について説明します。

 注：シスコは、他のベンダーのデバイスの設定またはサポートに対して責任を負わないことに注意してください。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Aruba IAPの設定
- ISE上のBYODフロー
- パスワードおよび証明書認証のためのISE設定

使用するコンポーネント

このドキュメントでは、Cisco Identity Services Engine(ISE)のサードパーティ統合機能をトラブルシューティングする方法について説明します。

他のベンダーやフローとの統合のガイドとして使用できます。ISEバージョン2.0はサードパーティの統合をサポートします。

これは、Aruba IAP 204によって管理されるワイヤレスネットワークをISEと統合して個人所有デバイスの持ち込み(BYOD)サービスを実現する方法を示す設定例です。

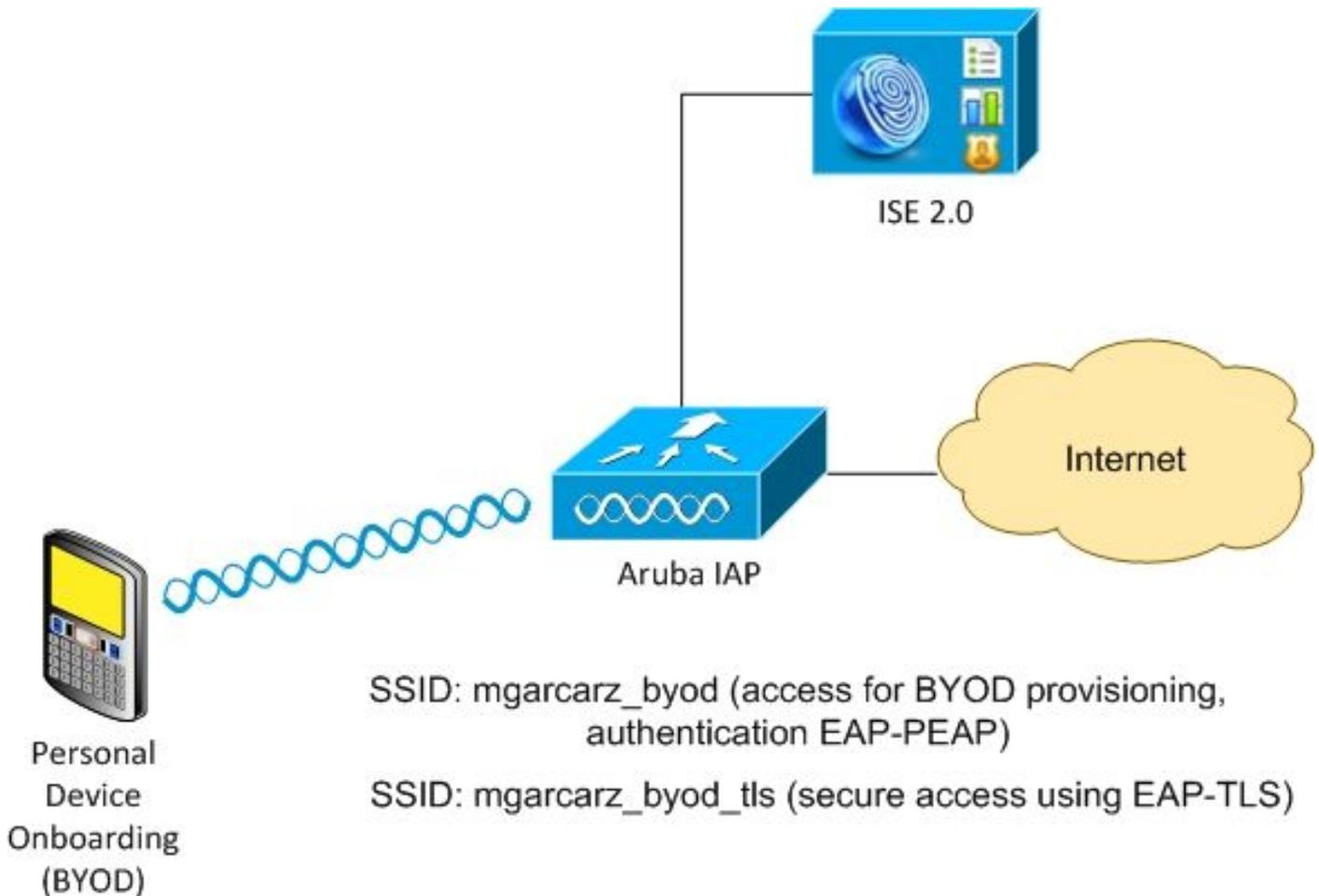
このドキュメントの情報は、次のソフトウェアのバージョンに基づいています。

- Aruba IAP 204 ソフトウェア 6.4.2.3
- Cisco ISE リリース 2.0 以降

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな(デフォルト)設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

ネットワーク図



Aruba AP が管理するワイヤレス ネットワークは 2 つあります。

1 つ目の認証(mgarcarz_byod)は、802.1x Extensible Authentication Protocol-Protected EAP(EAP-PEAP)アクセスに使用されます。

認証が成功した後、ArubaコントローラはユーザをISE BYODポータルにリダイレクトする必要があります。これは、ネイティブサブスクリプトプロビジョニング(NSP)フローです。

ユーザがリダイレクトされ、Network Setup Assistant(NSA)アプリケーションが実行され、証明書がプロビジョニングされてWindowsクライアントにインストールされます。

そのプロセスには SE 内部 CA が使用されます (デフォルト設定) 。

NSAは、Aruba(mgarcarz_byod_tls)によって管理される2つ目のService Set Identifier(SSID)のワイヤレスプロファイルの作成も担当します。これは、802.1x Extensible Authentication Protocol-Transport Layer Security(EAP-TLS)認証に使用されます。

その結果、企業ユーザは個人デバイスのオンボーディングを実行し、企業ネットワークへの安全なアクセスを取得できます。

この例は、さまざまな種類のアクセスに合わせて簡単に変更できます。次に例を示します。

- BYOD サービスを使用する中央 Web 認証 (CWA)
- Posture および BYOD のリダイレクションを使用する 802.1x 認証
- 通常、EAP-PEAP認証にはActive Directory(AD)が使用されます (この記事の内容を短くする

ために、内部ISEユーザが使用されます)

- 通常、証明書プロビジョニングには外部のSimple Certificate Enrollment Protocol(SCEP)サーバが使用されますが、この記事が簡潔にするために、一般にMicrosoft Network Device Enrollment Service(NDES)の内部ISE CAが使用されます。

サードパーティ サポートの課題

ISEゲストフロー(BYOD、CWA、NSP、クライアントプロビジョニングポータル(CPP)など)をサードパーティデバイスで使用する際には課題があります。

セッション

Cisco Network Access Devices(NAD)は、Radius cisco-av-pair called audit-session-idを使用して、認証、許可、アカウントिंग(AAA)サーバにセッションIDを通知します。

この値は、ISEがセッションを追跡し、各フローに適切なサービスを提供するために使用されます。他のベンダーはcisco-avペアをサポートしていません。

ISEは、Access-RequestおよびAccounting Requestで受信したIETF属性に依存する必要があります。

Access-Requestを受信すると、ISEは合成されたCiscoセッションID (Calling-Station-ID、NAS-Port、NAS-IP-Address、および共有秘密から) を作成します。この値はローカルでのみ意味を持ちます (ネットワーク経由では送信されません) 。

その結果、すべてのフロー(BYOD、CWA、NSP、CPP)から正しい属性が付加されることが期待されるため、ISEはシスコセッションIDを再計算してルックアップを実行し、正しいセッションと関連付けて、フローを続行できます。

URL リダイレクト

ISEは、url-redirectおよびurl-redirect-aclと呼ばれるRadius cisco-av-pairを使用して、特定のトラフィックをリダイレクトする必要があることをNADに通知します。

他のベンダーはcisco-avペアをサポートしていません。そのため、通常、これらのデバイスは、ISE上の特定のサービス (認可プロファイル) を指すスタティックリダイレクションURLを使用して設定する必要があります。

ユーザがHTTPセッションを開始すると、これらのNADはURLにリダイレクトされ、ISEが特定のセッションを識別してフローを続行できるように、追加の引数 (IPアドレスやMACアドレスなど) も付加します。

CoA

ISEは、subscriber:command、subscriber:reauthenticate-typeという名前のRadius cisco-av-pairを使用して、特定のセッションに対してNADが実行する必要があるアクションを示します。

他のベンダーはcisco-avペアをサポートしていません。そのため、通常、これらのデバイスは

RFC CoA (3576または5176) と2つの定義済みメッセージのいずれかを使用します。

- 切断要求 (切断パケットとも呼ばれる) – セッションの切断に使用される (頻繁に再接続を強制する)
- coa push : 切断せずにセッション ステータスを透過的に変更するために使用する (たとえば、VPN セッションや、新たに適用された ACL など)

ISE は、cisco-av-pair を使用する Cisco CoA も、CoA RFC 3576 と 5176 もサポートします。

ISE でのソリューション

ISE 2.0では、サードパーティベンダーをサポートするために、特定のベンダーの動作 (セッション、URLリダイレクト、およびCoAのサポート方法) を記述したネットワークデバイスプロファイルの概念が導入されました。

認証プロファイルは特定のタイプのプロファイル (ネットワーク デバイス プロファイル) であり、認証が実行されると、そのプロファイルから ISE の動作が取得されます。

その結果、他のベンダーのデバイスをISEで簡単に管理できます。また、ISE の設定には柔軟性があり、新しいネットワーク デバイス プロファイルを調整したり、作成したりすることもできます。

この記事では、Aruba デバイスのデフォルト プロファイルの使用方法について説明します。

機能の詳細については、以下の情報を参照してください。

[Cisco Identity Services Engine でのネットワーク アクセス デバイス プロファイル](#)

Cisco ISE

ステップ 1 : ネットワークデバイスへのArubaワイヤレスコントローラの追加

[管理 (Administration)] > [ネットワーク リソース (Network Resources)] > [ネットワーク デバイス (Network Devices)] に移動します。選択したベンダーの正しいデバイスプロファイル(この例ではArubaWireless)を選択します。次の図に示すように、共有秘密とCoAポートを必ず設定してください。

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

目的のベンダーに使用できるプロファイルがない場合は、Administration > Network Resources > Network Device Profilesで設定できます。

ステップ 2 : 許可プロファイルの設定

Policy > Policy Elements > Results > Authorization > Authorization Profilesの順に移動し、ステップ1と同じNetwork Device Profileを選択します。ArubaWireless を選択します。設定されているプロファイルは、図に示すように、BYODポータルを使用するAruba-redirect-BYODです。

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

[Web Redirection] 設定の欠落している部分では、認証プロファイルへのスタティックリンクが生成されます。Arubaはゲストポータルへのダイナミックリダイレクションをサポートしていませんが、各認証プロファイルに割り当てられた1つのリンクがAruba上で設定され、次の図に示すように設定されます。

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=10ImawmkIleZQhapEvIXPAoELx>

ステップ 3 : 許可ルール (Authorization Rule) の設定

Policy > Authorization Rulesの順に移動すると、設定が図のように表示されます。

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

まず、ユーザがSSID mgarcarz_arubaに接続し、ISEが認証プロファイルAruba-redirect-BYODを返します。これにより、クライアントはデフォルトのBYODポータルにリダイレクトされます。BYODプロセスが完了すると、クライアントはEAP-TLSで接続し、ネットワークへのフルアクセスが許可されます。

新しいバージョンのISEでは、同じポリシーが次のように表示されます。

Status	Rule Name	Conditions	Results Profiles	Security Groups	Hits	Actions
✓	Authorized	AND example.com:ExternalGroups EQUALS example.com/Builtin/Administrators EndPoints:BYODRegistration EQUALS Yes Network Access:EapAuthentication EQUALS EAP-TLS	PermitAccess	Select from list	0	⚙️
✓	Redirect	Aruba:Aruba-Essid-Name EQUALS mgarcarz_aruba	Aruba_Redirect_BYOD	Select from list	0	⚙️
✓	Default		DenyAccess	Select from list	0	⚙️

Aruba AP

ステップ 1：キャプティブポータルの設定

Aruba 204 上でキャプティブポータルを設定するには、[Security] > [External Captive Portal] に移動し、新規ポータルを追加します。次の図に示すように、適切に設定するためにこの情報を入力します。

- タイプ：Radius認証
- IPまたはホスト名：ISEサーバ
- URL：認可プロファイル設定の下でISE上に作成されるリンクです。特定の認可プロファイルに固有であり、Webリダイレクション設定の下でここで見つけることができます

Native Supplicant Provisioning Value BYOD Portal (default)

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

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

- ポート：図に示すように、選択したポータルがISEでホストされるポート番号（デフォルトでは8443）。

mgarcarz_ise20

Type:	Radius Authentication ▾
IP or hostname:	mgarcarz-ise20.example.
URL:	/portal/g?p=Kjr7eB7RrrLI
Port:	8443
Use https:	Enabled ▾
Captive Portal failure:	Deny internet ▾
Automatic URL Whitelisting:	Disabled ▾
Redirect URL:	<input type="text"/> (optional)

OK Cancel

ステップ 2 : RADIUS サーバの設定

Security > Authentication Serversの順に移動し、CoAポートが図に示すようにISEで設定されているものと同じであることを確認します。

Aruba 204ではデフォルトで5999に設定されていますが、これはRFC 5176に準拠しておらず、ISEでも動作しません。

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"/>	

注 : Arubaバージョン6.5以降では、「キャプティブポータル」チェックボックスも選択します。

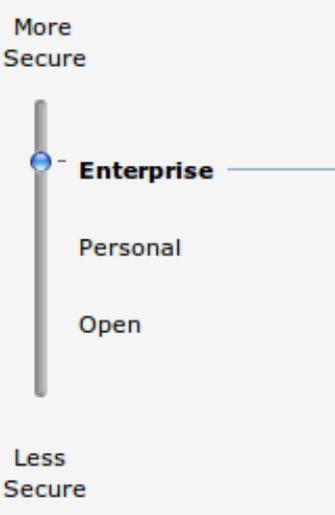
ステップ 3 : SSID 設定

- Securityタブは図に示すとおりです。

Edit mgarcarz_aruba

1 WLAN Settings 2 VLAN 3 Security 4 Access

Security Level



More Secure

Enterprise

Personal

Open

Less Secure

Key management: WPA-2 Enterprise

Termination: Disabled

Authentication server 1: mgarcarz_ise20 [Edit](#)

Authentication server 2: -- Select Server --

Reauth interval: 0 hrs.

Authentication survivability: Disabled

MAC authentication:
 Perform MAC authentication before 802.1X
 MAC authentication fail-thru

Accounting: Use authentication servers

Accounting interval: 0 min.

Blacklisting: Disabled

Fast Roaming

Opportunistic Key Caching(OKC):

802.11r:

802.11k:

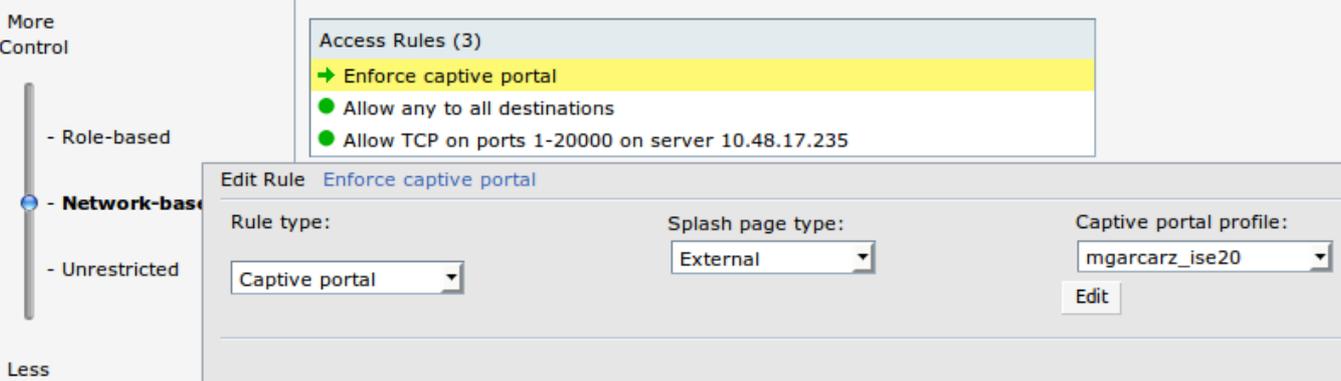
802.11v:

- Accessタブ：Network-based Access Ruleを選択して、SSIDでキャプティブポータルを設定します。

手順1で設定したキャプティブポータルを使用します。Newをクリックし、図に示すように、ルールタイプ：Captive portal、スプラッシュページタイプ：Externalを選択します。

1 WLAN Settings 2 VLAN 3 Security 4 Access

Access Rules



More Control

Less Control

- Role-based

- **Network-based**

- Unrestricted

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

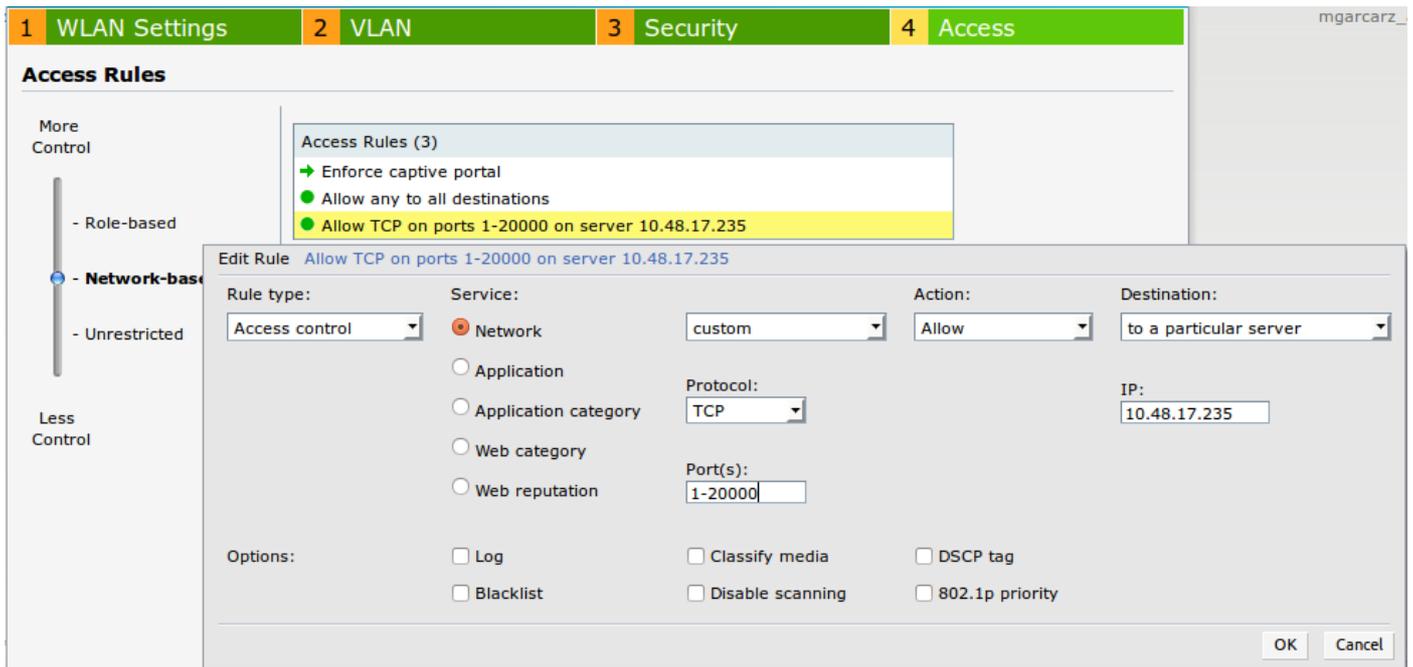
Splash page type: External

Captive portal profile: mgarcarz_ise20

[Edit](#)

さらに、ISEサーバ(1 ~ 20000の範囲のTCPポート)へのすべてのトラフィックを許可します。た

だし、Arubaでデフォルトで設定されているルール「すべての宛先あらゆるトラフィックを許可」は、図に示すように正しく機能していないようです。



確認

ここでは、設定が正常に機能しているかどうかを確認します。

ステップ 1 : EAP-PEAPを使用したSSID mgarcarz_arubaへの接続

ISE 上の最初の認証ログが表示されます。図に示すように、デフォルトの認証ポリシーが使用され、Aruba-redirect-BYOD認証プロファイルが返されました。

The screenshot shows the Cisco Identity Services Engine (ISE) interface. At the top, there are tabs for 'RADIUS Livelog', 'TACACS Livelog', 'Reports', 'Troubleshoot', and 'Adaptive Network Control'. Below this, there are four summary cards: 'Misconfigured Supplicants' (1), 'Misconfigured Network Devices' (0), 'RADIUS Drops' (12), and 'Client Stopped Respond' (0). Below these cards, there is a table showing authentication logs. The table has columns for 'Time', 'Status', 'Det...', 'R.', 'Identity', 'Endpoint ID', 'Authentication Policy', 'Authorization Policy', 'Authorization Profiles', 'Network Device', and 'Event'. The last row shows a successful authentication event for 'ArubaRedirect' with the profile 'Aruba-redirect-BYOD'.

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は、EAP SuccessとともにRadius Access-Acceptメッセージを返します。図に示すように、追加の属性は返されないことに注意してください (no Cisco av-pair url-redirectまたはurl-redirect-act) 。

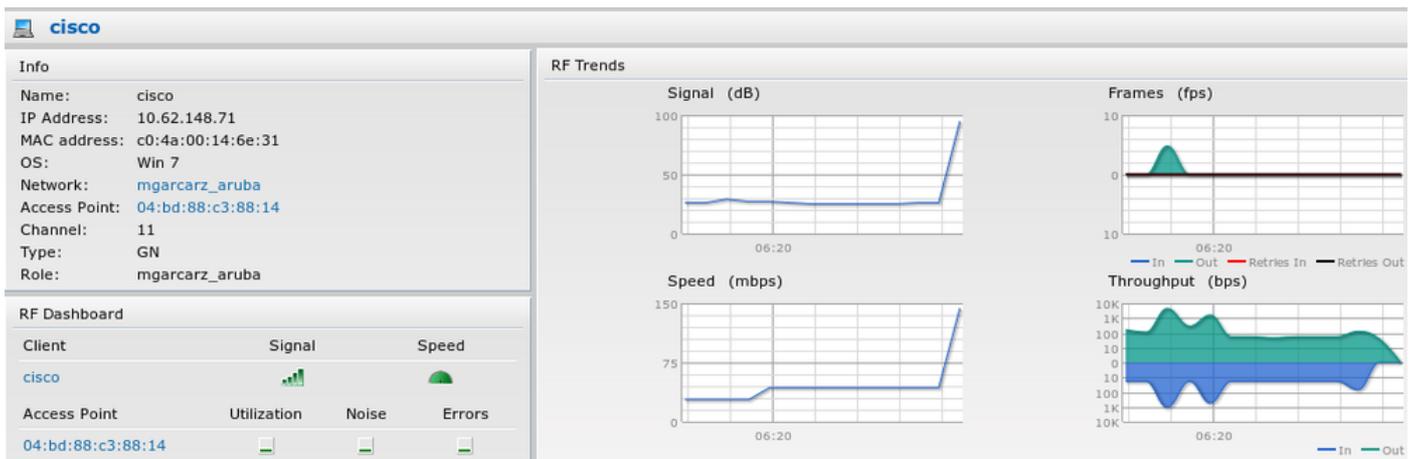
No.	Source	Destination	Protocol	Length	Info	User-Name	Acct-Session-Id
133	10.62.148.118	10.48.17.235	RADIUS	681	Access-Request(1) (id=102, l=639)	cisco	
134	10.48.17.235	10.62.148.118	RADIUS	257	Access-Challenge(11) (id=102, l=215)		
135	10.62.148.118	10.48.17.235	RADIUS	349	Access-Request(1) (id=103, l=307)	cisco	
136	10.48.17.235	10.62.148.118	RADIUS	235	Access-Challenge(11) (id=103, l=193)		
137	10.62.148.118	10.48.17.235	RADIUS	386	Access-Request(1) (id=104, l=344)	cisco	
138	10.48.17.235	10.62.148.118	RADIUS	267	Access-Challenge(11) (id=104, l=225)		
139	10.62.148.118	10.48.17.235	RADIUS	450	Access-Request(1) (id=105, l=408)	cisco	
140	10.48.17.235	10.62.148.118	RADIUS	283	Access-Challenge(11) (id=105, l=241)		
141	10.62.148.118	10.48.17.235	RADIUS	386	Access-Request(1) (id=106, l=344)	cisco	
142	10.48.17.235	10.62.148.118	RADIUS	235	Access-Challenge(11) (id=106, l=193)		
143	10.62.148.118	10.48.17.235	RADIUS	386	Access-Request(1) (id=107, l=344)	cisco	
149	10.48.17.235	10.62.148.118	RADIUS	363	Access-Accept(2) (id=107, l=321)	cisco	
150	10.62.148.118	10.48.17.235	RADIUS	337	Accounting-Request(4) (id=108, l=295)	cisco	04BD8888142-C04A00146E31-42F8
153	10.48.17.235	10.62.148.118	RADIUS	62	Accounting-Response(5) (id=108, l=20)		

```

Packet identifier: 0x6b (107)
Length: 321
Authenticator: 1173a3d3ea3d0798fe30fdaccf644f19
[This is a response to a request in frame 143]
[Time from request: 0.038114000 seconds]
Attribute Value Pairs
  AVP: l=7 t=User-Name(1): cisco
  AVP: l=67 t=State(24): 52656175746853657379696f6e3a30613330313165625862...
  AVP: l=87 t=Class(25): 434143533a30613330313165625862697544413379554e6f...
  AVP: l=6 t=EAP-Message(79) Last Segment[1]
  AVP: l=18 t=Message-Authenticator(80): e0b74092cacf88803dcd37032b761513
  AVP: l=58 t=Vendor-Specific(26) v=Microsoft(311)
  AVP: l=58 t=Vendor-Specific(26) v=Microsoft(311)

```

図に示すように、Arubaはセッションが確立され(EAP-PEAP IDがcisco)、選択されたロールがmgarcarz_arubaであることを報告します。



この役割は、ISE へのリダイレクション (Aruba 上のキャプティブ ポータルの機能) を実行します。

Aruba CLIでは、そのセッションの現在の認証ステータスを確認できます。

```
<#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

現在の権限についてACL ID 138を確認するには、次のようにします。

```
<#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 ... >
```

これは、図に示すように、GUIでそのロールに対して設定した内容と一致します。

Security

Authentication Servers | Users for Internal Server | Roles | Blacklisting | Firewall Settings | Inbound Firewall | Walled Garden

Roles

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

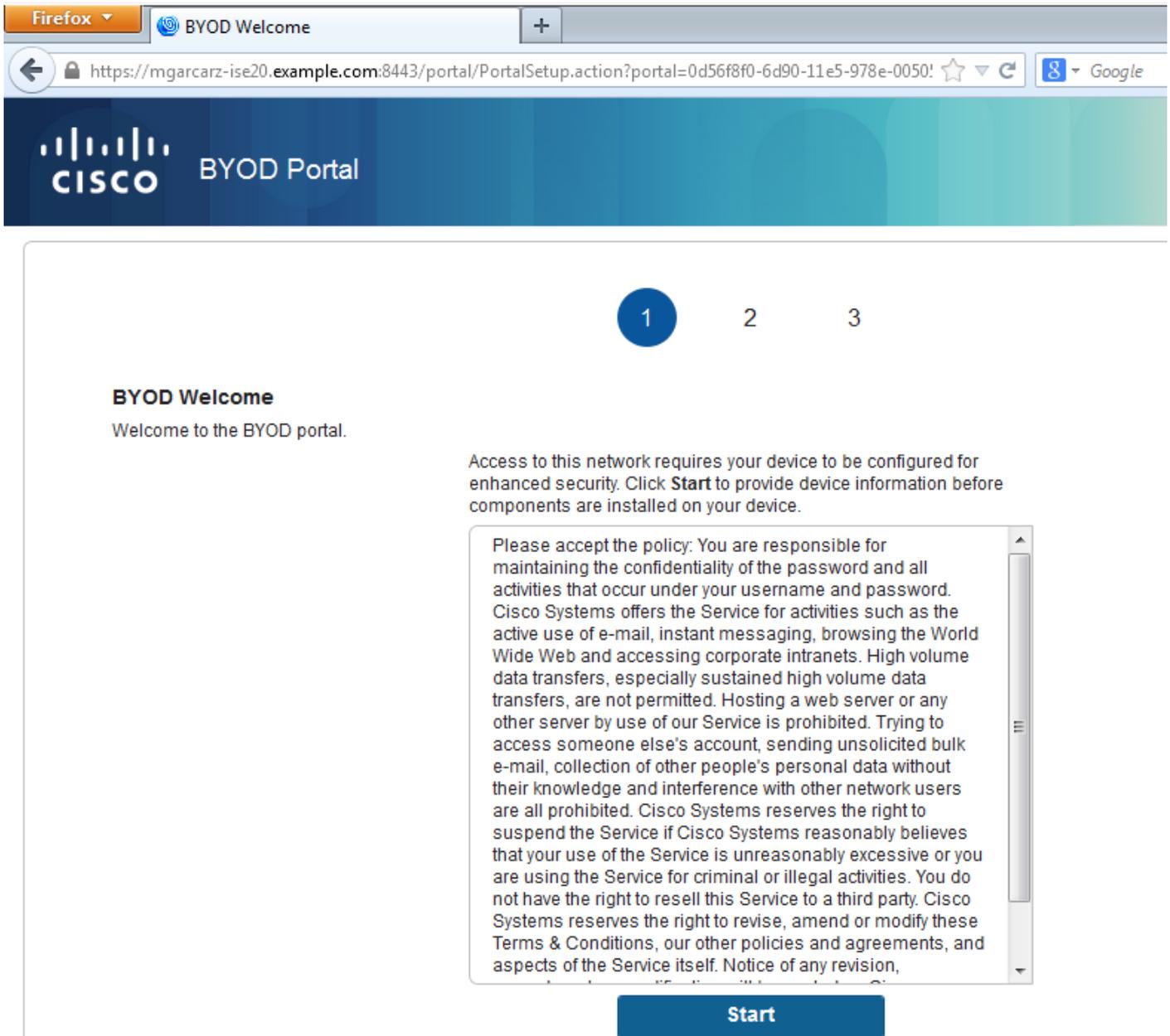
Access Rules for **mgarcarz_aruba**

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

New Delete New Edit Delete ↑ ↓

ステップ 2 : BYODのためのWebブラウザトラフィックリダイレクション

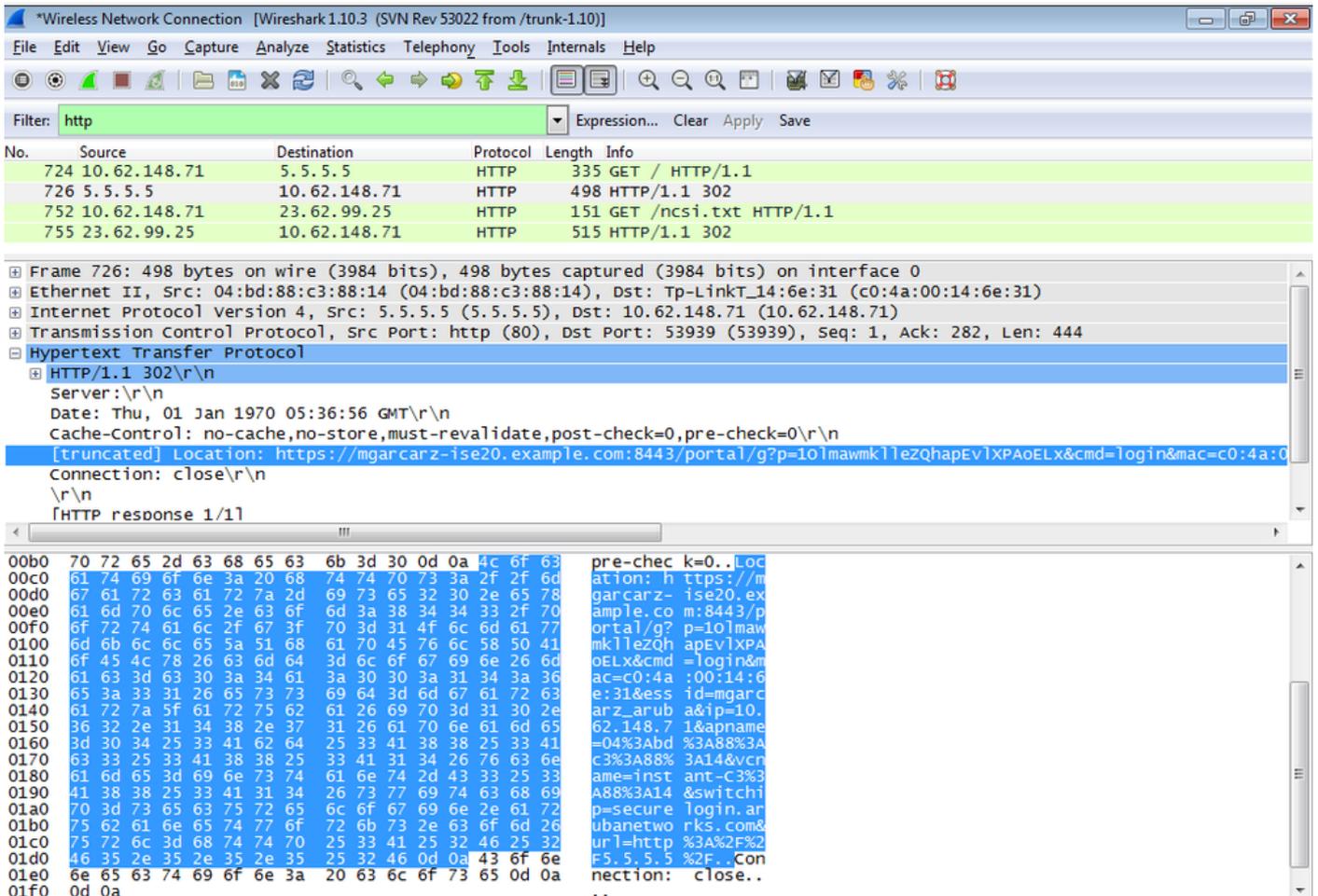
ユーザがWebブラウザを開き、任意のアドレスを入力すると、図に示すようにリダイレクトが発生します。



パケットキャプチャを見ると、Arubaが宛先(5.5.5.5)をスプーフィングし、ISEにHTTPリダイレクションを返すことが確認できます。

これはISEで設定されたスタティックURLと同じであり、Arubaのキャプティブポータルにコピーされることに注意してください。ただし、次の図に示すように、さらに複数の引数が追加されています。

- 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



これらの引数により、ISEはCiscoセッションIDを再作成し、ISE上の対応するセッションを見つけ出し、BYOD (または他の設定済み) フローを続行できます。

シスコデバイスの場合、通常はaudit_session_idが使用されますが、これは他のベンダーではサポートされていません。

ISEのデバッグから、audit-session-id値の生成を確認できます (この値はネットワークを介して送信されることはありません)。

```
<#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
```

次に、BYODにデバイスを登録した後の相関関係を示します (2ページ)。

```
<#root>
```

```
AcsLogs,2015-10-29 23:25:48,538,DEBUG,0x7fc0b39a4700,cntx=0000032947,CallingStationID=c04a00146e31,FramedIPAddress=10.62.148.71,Log_Message=[2015-10-29 23:25:48.533 +01:00 0000011874 88010 INFO
```

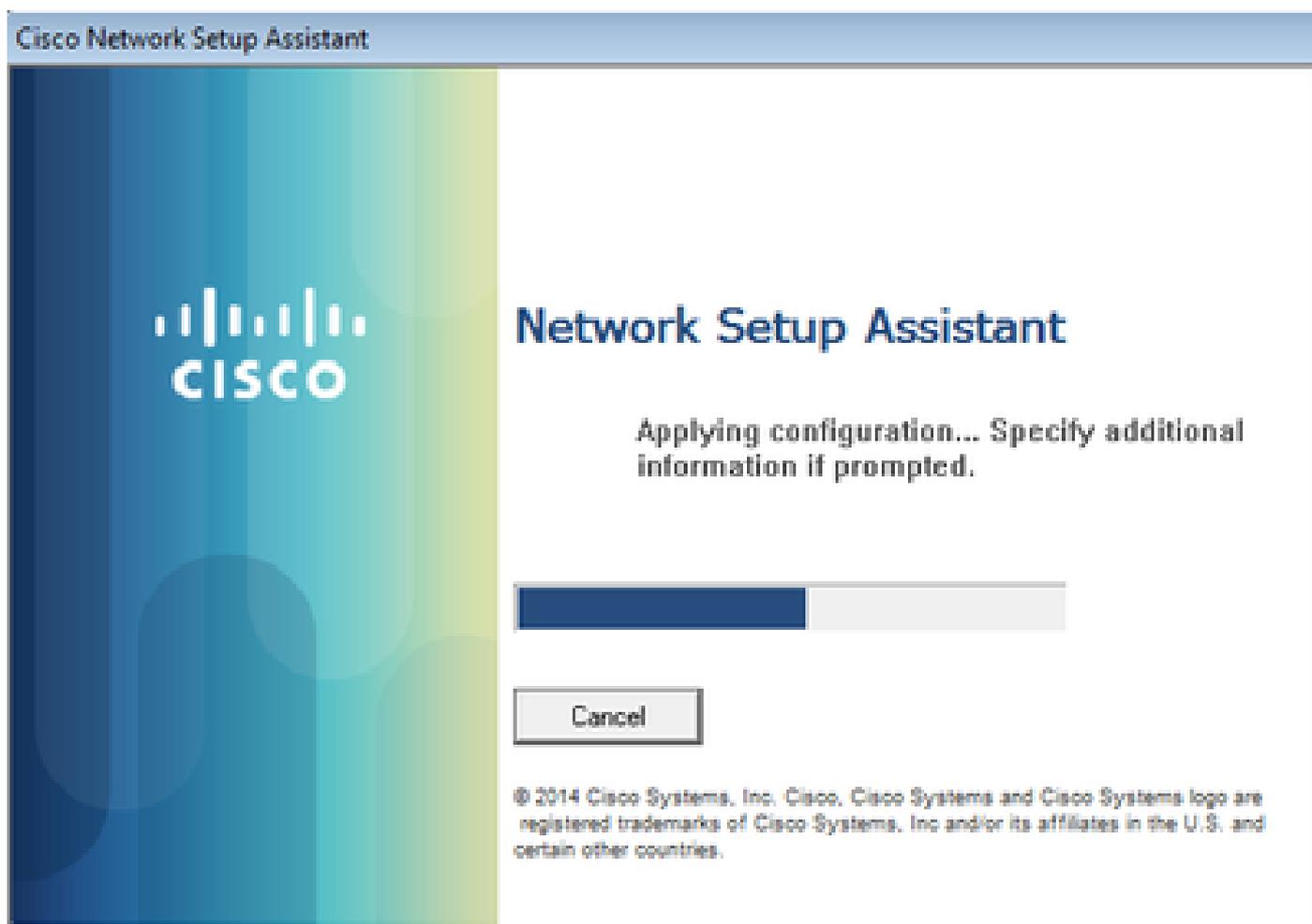
MyDevices: Successfully registered/provisioned the device

(endpoint), ConfigVersionId=145, UserName=cisco, MacAddress=c0:4a:00:14:6e:31, IpAddress=10.62.148.71, AuthenticationIdentityStore=Internal Users, PortalName=BYOD Portal (default), PsnHostName=mgarcarz-ise20.example.com, GuestUserName=cisco, EPMacAddress=C0:4A:00:14:6E:31, EPIIdentityGroup=RegisteredDevices Staticassignment=true, EndPointProfiler=mgarcarz-ise20.example.com, EndPointPolicy=Unknown, NADAddress=10.62.148.118, DeviceName=ttt, DeviceRegistrationStatus=Registered AuditSessionId=0a3011ebXbiuDA3yUNoLUvtCRyuPFxkqYJ7TT06foOZ7G1HXj1M, cisco-av-pair=

audit-session-id=0a3011ebXbiuDA3yUNoLUvtCRyuPFxkqYJ7TT06foOZ7G1HXj1M

後続の要求では、クライアントはBYODページ3にリダイレクトされ、そこでNSAがダウンロードされて実行されます。

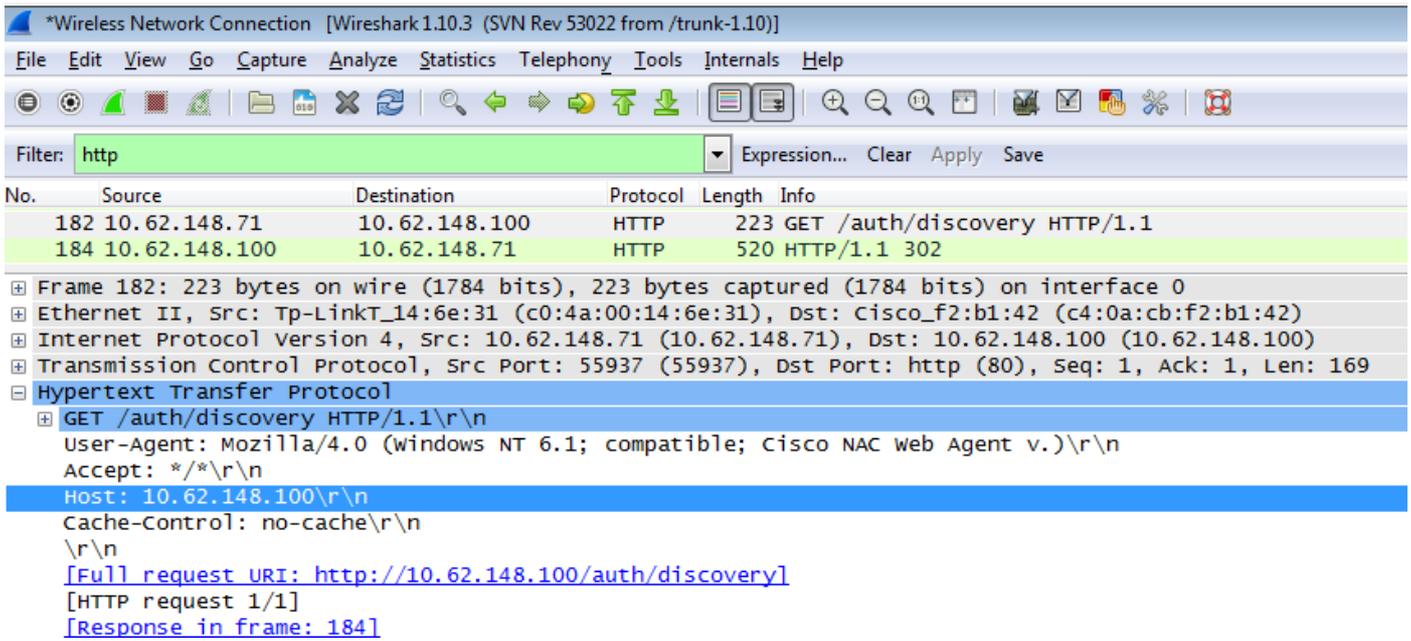
ステップ 3 : ネットワークセットアップアシスタントの実行



NSA には Web ブラウザと同じタスクがあります。まず、ISEのIPアドレスを検出する必要があります。この検出は HTTP リダイレクションによって実行されます。

この時間ユーザは (Webブラウザのように) IPアドレスを入力できないため、そのトラフィックは自動的に生成されます。

図に示すように、デフォルトゲートウェイが使用されます(enroll.cisco.comも使用できます)。



応答はWebブラウザとまったく同じです。

この方法で NSA は、ISE に接続し、xml プロファイルを設定とともに取得し、SCEP 要求を生成し、それを ISE に送信して、署名付き証明書 (ISE の内部 CA による署名) を取得し、ワイヤレス プロファイルを設定し、最終的に設定済み SSID に接続できます。

クライアントからログを収集します(Windowsでは%temp%/spwProfile.log)。分かりやすくするために、一部の出力を省略しています。

<#root>

```
Logging started
SPW Version: 1.0.0.46
System locale is [en]
Loading messages for english...
Initializing profile
SPW is running as High integrity Process - 12288
GetProfilePath: searched path = C:\Users\ADMINI~1.EXA\AppData\Local\Temp\ for file name = spwProfile.xml
GetProfilePath: searched path = C:\Users\ADMINI~1.EXA\AppData\Local\Temp\Low for file name = spwProfile.xml
Profile xml not found Downloading profile configuration...

Downloading profile configuration...

Discovering ISE using default gateway

Identifying wired and wireless network interfaces, total active interfaces: 1
Network interface - mac:C0-4A-00-14-6E-31, name: Wireless Network Connection, type: wireless
Identified default gateway: 10.62.148.100

Identified default gateway: 10.62.148.100, mac address: C0-4A-00-14-6E-31
```

redirect attempt to discover ISE with the response url

DiscoverISE - start

Discovered ISE - : [mgarcarz-ise20.example.com, sessionId: 0a3011ebXbiuDA3yUNoLUvtCRyuPFxkqYJ7TT06fo0Z7

DiscoverISE - end

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

GetProfile - start

GetProfile - end

Successfully retrieved profile xml

using V2 xml version

parsing wireless connection setting

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

set ChallengePwd

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

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

ec 8a 11 78^M

] as rootCA

Installed CA cert for authMode machineOrUser - Success

HttpWrapper::SendScepRequest

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

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

Certificate issued - successfully

ScepWrapper::InstallCert start

ScepWrapper::InstallCert: Reading scep response file

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

ScepWrapper::InstallCert GetCertHash -- return val 1

ScepWrapper::InstallCert end

Configuring wireless profiles...

Configuring ssid [mgarcarz_aruba_tls]

WirelessProfile::SetWirelessProfile - Start

Wireless profile: [mgarcarz_aruba_tls] configured successfully

Connect to SSID

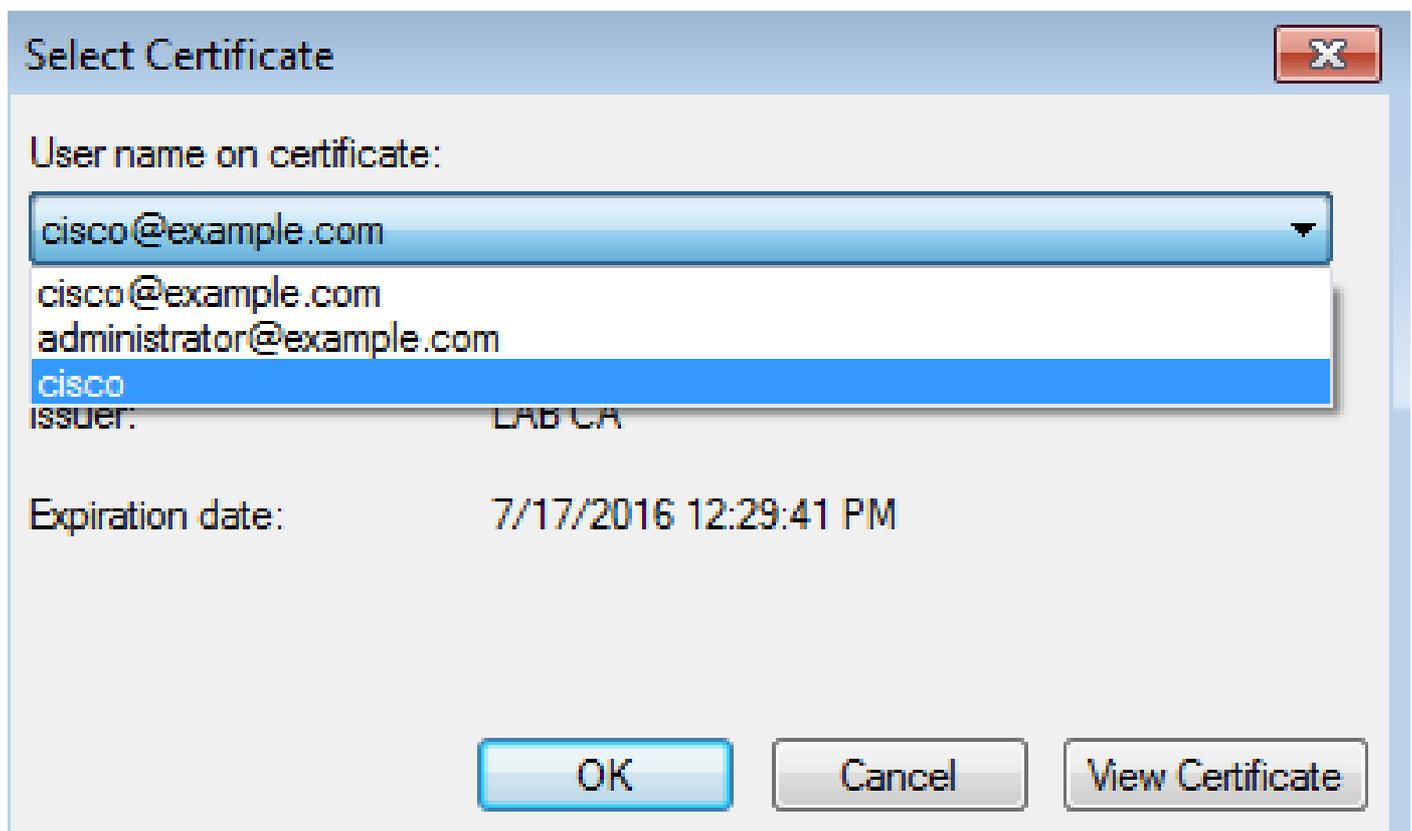
Successfully connected profile: [mgarcarz_aruba_tls]

WirelessProfile::SetWirelessProfile. - End

これらのログは、シスコ デバイスでの BYOD プロセスとまったく同じです。

 注：ここではRadius CoAは不要です。新しく設定された SSID に強制的に再接続するのは、アプリケーション (NSA) の役割です。

この段階で、システムが最終的なSSIDへの関連付けを試行していることをユーザが確認できます。複数のユーザ証明書がある場合は、正しい証明書を選択する必要があります (図を参照)。



接続に成功すると、NSAは次の図のように報告します。



これはISEで確認できます。2番目のログはEAP-TLS認証にヒットし、Basic_Authenticated_Access (EAP-TLS、Employee、およびBYOD Registered true) のすべての条件に一致します。

Cisco Identity Services Engine										
RADIUS Livelog										
Misconfigured Supplicants: 1 Misconfigured Network Devices: 0 RADIUS Drops: 12 Client Stopped Respond: 0										
Time	Status	Det...	R.	Identity	Endpoint ID	Authentication Policy	Authorization Policy	Authorization Profiles	Network Device	Event
2015-10-29 22:23:37...			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...			0	cisco	C0:4A:00:14:6E:31	Default >> Dot1X >> EAP-TLS	Default >> Basic_Authenticated...	PermitAccess	aruba	Authentication succeeded
2015-10-29 22:19:09...			0	cisco	C0:4A:00:14:6E:31	Default >> Dot1X >> Default	Default >> ArubaRedirect	Aruba-redirect-BYOD	aruba	Authentication succeeded

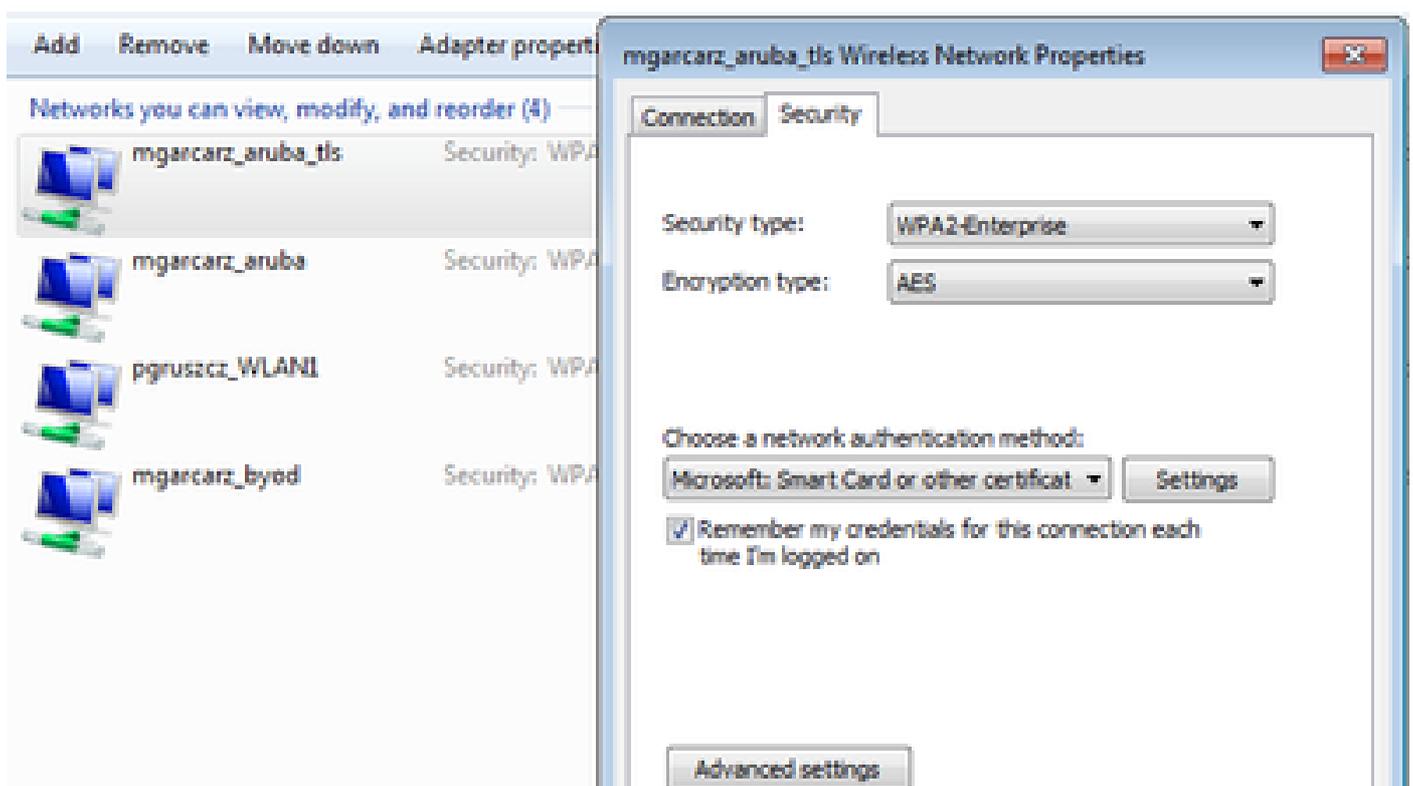
また、エンドポイントIDビューでは、図に示すように、エンドポイントのBYOD登録済みフラグがtrueに設定されていることを確認できます。



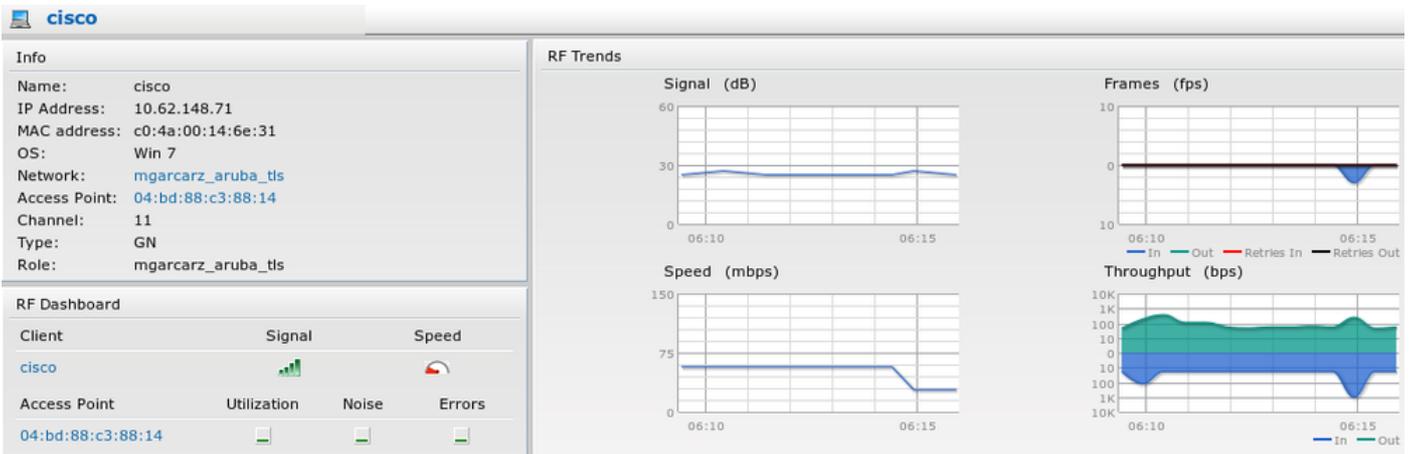
Windows PCでは、新しいワイヤレスプロファイルが優先 (およびEAP-TLS用に設定) として自動的に作成され、次のように表示されます。

Manage wireless networks that use (Wireless Network Connection)

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



この段階で、Arubaはユーザが最終的なSSIDに接続されていることを確認します。



自動的に作成され、ネットワークと同じ名前が付けられたロールは、フルネットワークアクセスを提供します。

Security

Authentication Servers | Users for Internal Server | Roles | Blacklisting | Firewall Settings | Inbound Firewall

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

Buttons: New, Delete, New, Edit, Delete, Up, Down

その他のフローおよび CoA サポート

CoA を含む CWA

BYODフローにはCoAメッセージはありませんが、自己登録ゲストポータルを使用したCWAフローを次に示します。

設定された許可ルールは図に示すとおりです。

<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

ユーザはMAB認証を使用してSSIDに接続し、Webページへの接続を試行すると、自己登録ゲストポータルへのリダイレクトが発生します。このポータルでは、ゲストが新しいアカウントを作成するか、現在のアカウントを使用できます。



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?](#)

ゲストが正常に接続されると、認可状態を変更するためにISEからネットワークデバイスにCoAメッセージが送信されます。



Sponsored Guest Portal

Welcome Message

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

You're very close to gaining network access.

Continue

これは、図に示すように、Operations > Authentificationsの下で確認できます。

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

ISE デバッグ内の CoA メッセージは、次のようになります。

<#root>

```
2015-11-02 18:47:49,553 DEBUG [Thread-137] [] cisco.cpm.prtr.impl.PrRTLoggerImpl -:::-  
DynamicAuthorizationFlow,DEBUG,0x7fc0e9cb2700,cntx=0000000561,sesn=c59aa41a-e029-4ba0-a31b  
-44549024315e,CallingStationID=c04a00157634,[DynamicAuthorizationFlow::createCoACmd]  
Processing incoming attribute vendor , name
```

NAS-IP-Address, value=10.62.148.118

```
.,  
DynamicAuthorizationFlow.cpp:708  
2015-11-02 18:47:49,567 DEBUG [Thread-137] [] cisco.cpm.prvt.impl.PrRTLoggerImpl -:::::-  
DynamicAuthorizationFlow,DEBUG,0x7fc0e9cb2700,cntx=0000000561,sesn=c59aa41a-e029-4ba0-a31b-  
-44549024315e,CallingStationID=c04a00157634,[DynamicAuthorizationFlow::createCoACmd]  
Processing incoming attribute vendor , name
```

Acct-Session-Id, value=04BD88B88144-
C04A00157634-7AD

```
.,DynamicAuthorizationFlow.cpp:708  
2015-11-02 18:47:49,573 DEBUG [Thread-137] [] cisco.cpm.prvt.impl.PrRTLoggerImpl -:::::-  
DynamicAuthorizationFlow,DEBUG,0x7fc0e9cb2700,cntx=0000000561,sesn=c59aa41a-e029-4ba0-a31b-  
-44549024315e,CallingStationID=c04a00157634,[DynamicAuthorizationFlow::createCoACmd]  
Processing incoming attribute vendor , name cisco-av-pair, v  
alue=audit-session-id=0a3011ebisZXypODwqjB6j64GeFiF7RwvyocneEia17ckjtU1HI.,DynamicAuthorizationFlow.cpp  
2015-11-02 18:47:49,584 DEBUG [Thread-137] [] cisco.cpm.prvt.impl.PrRTLoggerImpl -:::::-  
DynamicAuthorizationFlow,DEBUG,0x7fc0e9cb2700,cntx=0000000561,sesn=c59aa41a-e029-4ba0-a31b-  
-44549024315e,CallingStationID=c04a00157634,[DynamicAuthorizationRequestHelper::  
setConnectionParams]
```

defaults from nad profile : NAS=10.62.148.118, port=3799, timeout=5,

retries=2

```
.,DynamicAuthorizationRequestHelper.cpp:59  
2015-11-02 18:47:49,592 DEBUG [Thread-137] [] cisco.cpm.prvt.impl.PrRTLoggerImpl -:::::-  
DynamicAuthorizationFlow,DEBUG,0x7fc0e9cb2700,cntx=0000000561,sesn=c59aa41a-e029-4ba0-a31b-  
-44549024315e,CallingStationID=c04a00157634,[DynamicAuthorizationRequestHelper::set  
ConnectionParams] NAS=10.62.148.118, port=3799, timeout=5, retries=1,  
DynamicAuthorizationRequestHelper.cpp:86  
2015-11-02 18:47:49,615 DEBUG [Thread-137] [] cisco.cpm.prvt.impl.PrRTLoggerImpl -:::::-  
DynamicAuthorizationFlow,DEBUG,0x7fc0e9cb2700,cntx=0000000561,sesn=c59aa41a-e029-4ba0-a31b-  
-44549024315e,CallingStationID=c04a00157634,[DynamicAuthorizationFlow::onLocalHttpEvent]:
```

invoking DynamicAuthorization,DynamicAuthorizationFlow.cpp:246

ArubaからのDisconnect-ACK:

<#root>

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

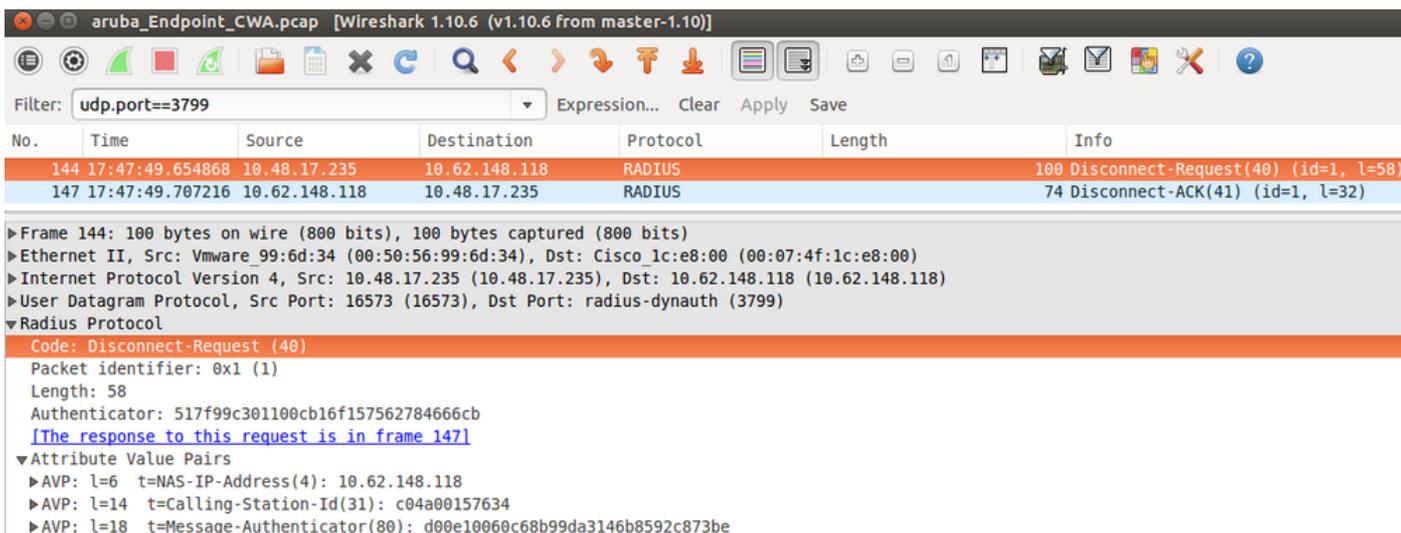
CallingStationID=c04a00157634

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

Packet type 41(DisconnectACK).

```
,  
DynamicAuthorizationFlow.cpp:303
```

CoA Disconnect-Request(40)およびDisconnect-ACK(41)によるパケットキャプチャは次のようになります。



The image shows a Wireshark capture of two RADIUS packets. The first packet (No. 144) is a Disconnect-Request (40) from 10.48.17.235 to 10.62.148.118. The second packet (No. 147) is a Disconnect-ACK (41) from 10.62.148.118 to 10.48.17.235. The details pane for packet 144 shows the RADIUS protocol structure, including the Disconnect-Request code, packet identifier, length, authenticator, and several Attribute Value Pairs (AVPs).

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)

Details for Frame 144:

- Code: Disconnect-Request (40)
- Packet identifier: 0x1 (1)
- Length: 58
- Authenticator: 517f99c301100cb16f157562784666cb
- 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

 注:RFC CoAは、デバイスプロファイルAruba (デフォルト設定) に関連する認証に使用されています。シスコデバイスに関連する認証では、Cisco CoAタイプの再認証でした。

トラブルシューティング

ここでは、設定のトラブルシューティングに使用できる情報を示します。

Aruba キャプティブ ポータルが FQDN ではなく IP アドレスを使用

ArubaのキャプティブポータルがISEのFQDNではなくIPアドレスで設定されている場合、PSN NSAは失敗します。

```
<#root>
```

```
Warning - [HTTPConnection]
```

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

```
CN
```

その理由は、ISEに接続する際の厳密な証明書検証です。IPアドレスを使用してISEに接続する場合 (FQDNではなくIPアドレスを使用したリダイレクトURLの結果)、サブジェクト名= FQDNのISE証明書が表示され、検証が失敗します。

 注:Webブラウザは引き続きBYODポータルを使用します (ユーザによる承認が必要な警告を表示) 。

Aruba キャプティブ ポータルのアクセス ポリシーが正しくない

デフォルトでは、キャプティブポータルで設定されたArubaアクセスポリシーはTCPポート80、443、および8080を許可します。

NSAは、ISEからxmlプロファイルを取得するためにtcpポート8905に接続できません。次のエラーが報告されます。

```
<#root>
```

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

```
[
```

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

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

```
typeHint=SPWConfig&referrer=Windows&mac_address=C0-4A-00-14-6E-31&spw_version=1.0.0.46&session=0a3011ebXbiuDA3yUNoLUvtCRyuPFxkqYJ7TT06fo0Z7G1HXj1M&os=Windows A11]  
- http Error: [2]
```

```
HTTP response code: 0
```

```
]
```

```
GetProfile - end
```

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

Aruba CoA のポート番号

デフォルトでは、ArubaはCoA Air Group CoAポート5999のポート番号を提供します。残念ながら、Aruba 204はそのような要求に応答しませんでした (図を参照) 。

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

パケットキャプチャは次の図のように表示されます。

The screenshot shows a Wireshark capture of a network packet. The filter is set to 'udp.port==5999'. The packet list shows two packets: a RADIUS Disconnect-Request (40 bytes) and an ICMP Destination unreachable (Port unreachable) (128 bytes). The packet details pane shows the RADIUS protocol structure, including the Disconnect-Request code, packet identifier, authenticator, and several Attribute Value Pairs (AVPs) such as NAS-IP-Address, Calling-Station-Id, and Message-Authenticator.

RFC 5176で説明されているように、ここで使用する最適なオプションはCoAポート3977です。

Aruba デバイスでのリダイレクション

Aruba 3600のv6.3では、リダイレクションが他のコントローラとは少し異なる動作をしていることがわかります。パケットキャプチャと説明については、こちらを参照してください。

No.	Time	Source	Destination	Protocol	Length	Info
770	09:29:40.5119116	10.75.94.213	173.194.124.52	HTTP	1373	GET / HTTP/1.1
772	09:29:40.5210658	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 /&arubalp=6b0512fc-f699-45c6-b5cb-e62b3260e5 HTTP/1.1
797	09:29:41.7563066	173.194.124.52	10.75.94.213	HTTP	485	HTTP/1.1 302 Temporarily Moved

<#root>

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

&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/

&aruba1p=6b0512fc-f699-45c6-b5cb-e62b3260e5

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

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

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

関連情報

- [Cisco Identity Services Engine 管理者ガイド リリース 2.0](#)
- [Cisco Identity Services Engine でのネットワーク アクセス デバイス プロファイル](#)
- [テクニカル サポートとドキュメント - Cisco Systems](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。