Configuration de l'intégration tierce ISE 2.0 avec Aruba Wireless

Table des matières

Introduction

Ce document décrit comment dépanner la fonctionnalité d'intégration tierce sur Cisco Identity Services Engine (ISE).

Remarque : sachez que Cisco n'est pas responsable de la configuration ou de l'assistance des périphériques d'autres fournisseurs.

Conditions préalables

Exigences

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Configuration Aruba IAP
- Flux BYOD sur ISE
- Configuration ISE pour l'authentification par mot de passe et certificat

Composants utilisés

Ce document décrit comment dépanner la fonctionnalité d'intégration tierce sur Cisco Identity Services Engine (ISE).

Il peut être utilisé comme guide pour l'intégration avec d'autres fournisseurs et flux. ISE version 2.0 prend en charge l'intégration tierce.

Il s'agit d'un exemple de configuration qui présente comment intégrer un réseau sans fil géré par Aruba IAP 204 avec ISE pour les services BYOD (Bring Your Own Device).

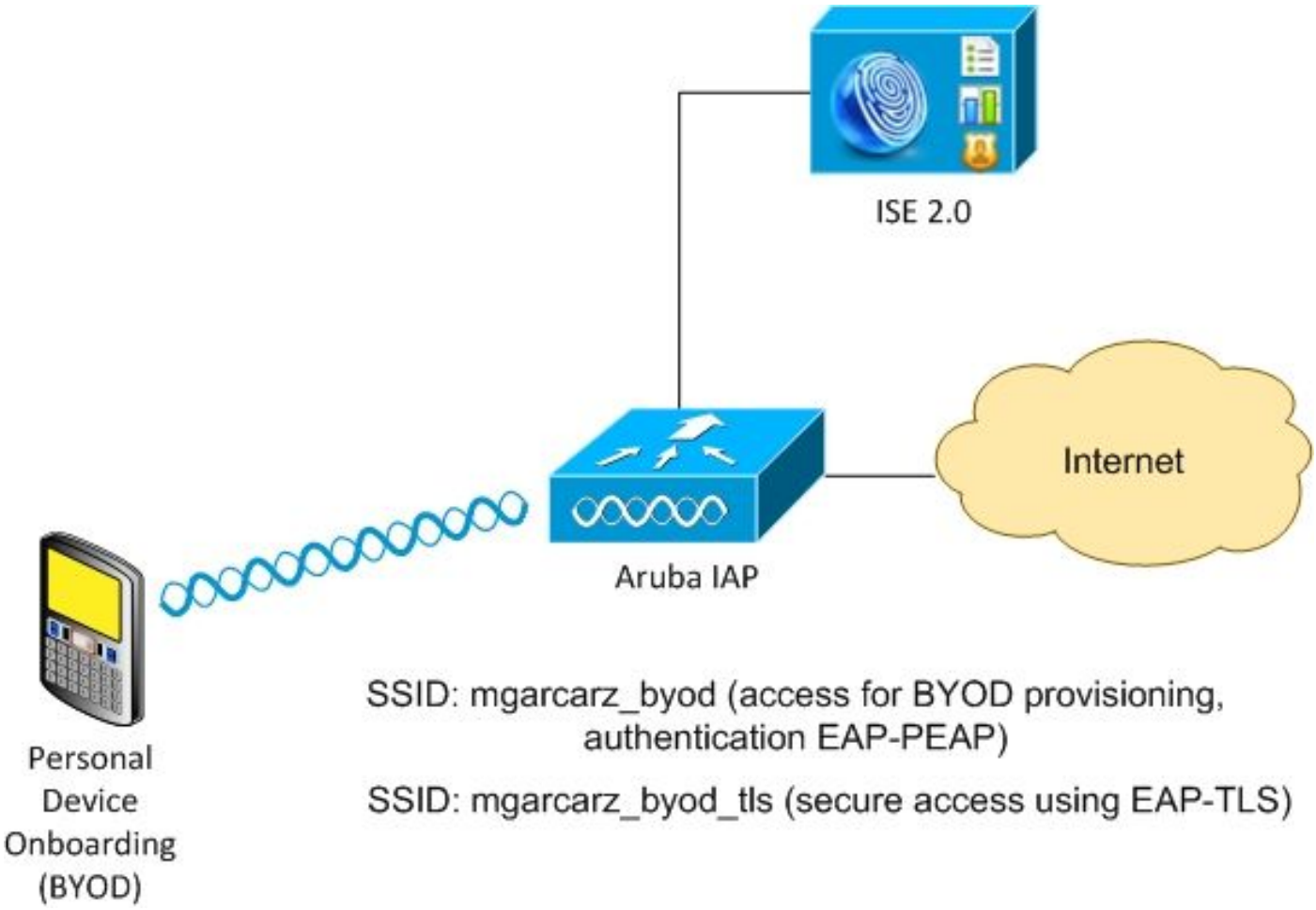
Les informations contenues dans ce document sont basées sur les versions de logiciel suivantes :

- Logiciel Aruba IAP 204 6.4.2.3
- Cisco ISE, version 2.0 et ultérieure

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. Si votre réseau est en ligne, assurez-vous de bien comprendre l’incidence possible des commandes.

Configurer

Diagramme du réseau



Il existe deux réseaux sans fil gérés par Aruba AP.

Le premier (mgarcarz_byod) est utilisé pour l'accès EAP-PEAP (Extensible Authentication Protocol-Protected EAP) 802.1x.

Après une authentification réussie, le contrôleur Aruba doit rediriger l'utilisateur vers le flux NSP (Native Supplicant Provisioning) du portail ISE BYOD.

L'utilisateur est redirigé, l'application Network Setup Assistant (NSA) est exécutée et le certificat est provisionné et installé sur le client Windows.

L'autorité de certification interne ISE est utilisée pour ce processus (configuration par défaut).

NSA est également responsable de la création du profil sans fil pour le deuxième SSID (Service Set Identifier) géré par Aruba (mgarcarz_byod_tls), qui est utilisé pour l'authentification EAP-TLS (Extensible Authentication Protocol-Transport Layer Security) 802.1x.

Par conséquent, l'utilisateur de l'entreprise peut intégrer son périphérique personnel et obtenir un accès sécurisé au réseau de l'entreprise.

Cet exemple peut être facilement modifié pour différents types d'accès, par exemple :

- Authentification Web centralisée (CWA) avec service BYOD
- authentification 802.1x avec posture et redirection BYOD
- Généralement, pour l'authentification EAP-PEAP, Active Directory est utilisé (pour que cet

article soit court, des utilisateurs ISE internes sont utilisés)
- Généralement, pour le serveur SCEP (Simple Certificate Enrollment Protocol) externe de mise en service de certificats, généralement le service NDES (Network Device Enrollment Service) de Microsoft, afin de garder cet article court, l'autorité de certification ISE interne est utilisée.

Défis liés à l'assistance tierce

L'utilisation de flux d'invité ISE (tels que BYOD, CWA, NSP, Client Provisioning Portal (CPP)) avec des périphériques tiers pose des problèmes.

Sessions

Cisco Network Access Devices (NAD) utilise Radius cisco-av-pair appelé audit-session-id afin d'informer le serveur AAA (Authentication, Authorization, and Accounting) de l'ID de session.

Cette valeur est utilisée par ISE afin de suivre les sessions et de fournir les services corrects pour chaque flux. Les autres fournisseurs ne prennent pas en charge la paire cisco-av.

ISE doit s'appuyer sur les attributs IETF reçus dans la demande d'accès et la demande de comptabilisation.

Après réception de la demande d'accès, ISE crée un ID de session Cisco synthétisé (à partir de Calling-Station-ID, NAS-Port, NAS-IP-Address et shared secret). Cette valeur a une signification locale uniquement (non envoyée via le réseau).

Par conséquent, il est prévu que chaque flux (BYOD, CWA, NSP, CPP) associe les attributs corrects. ISE peut ainsi recalculer l'ID de session Cisco et effectuer une recherche afin de le mettre en corrélation avec la session correcte et de poursuivre le flux.

Redirection d'URL

ISE utilise Radius cisco-av-pair appelé url-redirect et url-redirect-acl afin d'informer NAD que le trafic spécifique doit être redirigé.

Les autres fournisseurs ne prennent pas en charge la paire cisco-av. En général, ces périphériques doivent donc être configurés avec une URL de redirection statique qui pointe vers un service spécifique (profil d'autorisation) sur ISE.

Une fois que l'utilisateur a initié une session HTTP, ces NAD redirigent vers l'URL et joignent également des arguments supplémentaires (comme l'adresse IP ou l'adresse MAC) afin de permettre à ISE d'identifier une session spécifique et de poursuivre le flux.

CoA

ISE utilise Radius cisco-av-pair appelé subscriber:command, subscriber:reauthenticate-type afin d'indiquer les actions que NAD doit entreprendre pour une session spécifique.

Les autres fournisseurs ne prennent pas en charge la paire cisco-av. En général, ces périphériques utilisent RFC CoA (3576 ou 5176) et l'un des deux messages définis :

- demande de déconnexion (également appelée paquet de déconnexion) : celle-ci est utilisée pour déconnecter la session (très souvent pour forcer la reconnexion)
- Push CoA : utilisé pour modifier l'état de la session de manière transparente sans déconnexion (par exemple, session VPN et nouvelle liste de contrôle d'accès appliquée)

ISE prend en charge Cisco CoA avec paire cisco-av, ainsi que RFC CoA 3576/5176.

Solution sur ISE

Afin de prendre en charge les fournisseurs tiers, ISE 2.0 a introduit un concept de profils de périphériques réseau qui décrit le comportement spécifique des fournisseurs - la prise en charge des sessions, de la redirection d'URL et de la CoA.

Les profils d'autorisation sont de type spécifique (profil de périphérique réseau) et, une fois l'authentification effectuée, le comportement ISE est dérivé de ce profil.

Par conséquent, les périphériques d'autres fournisseurs peuvent être gérés facilement par ISE. La configuration sur ISE est également flexible et permet d'ajuster ou de créer de nouveaux profils de périphériques réseau.

Cet article présente l'utilisation du profil par défaut pour le périphérique Aruba.

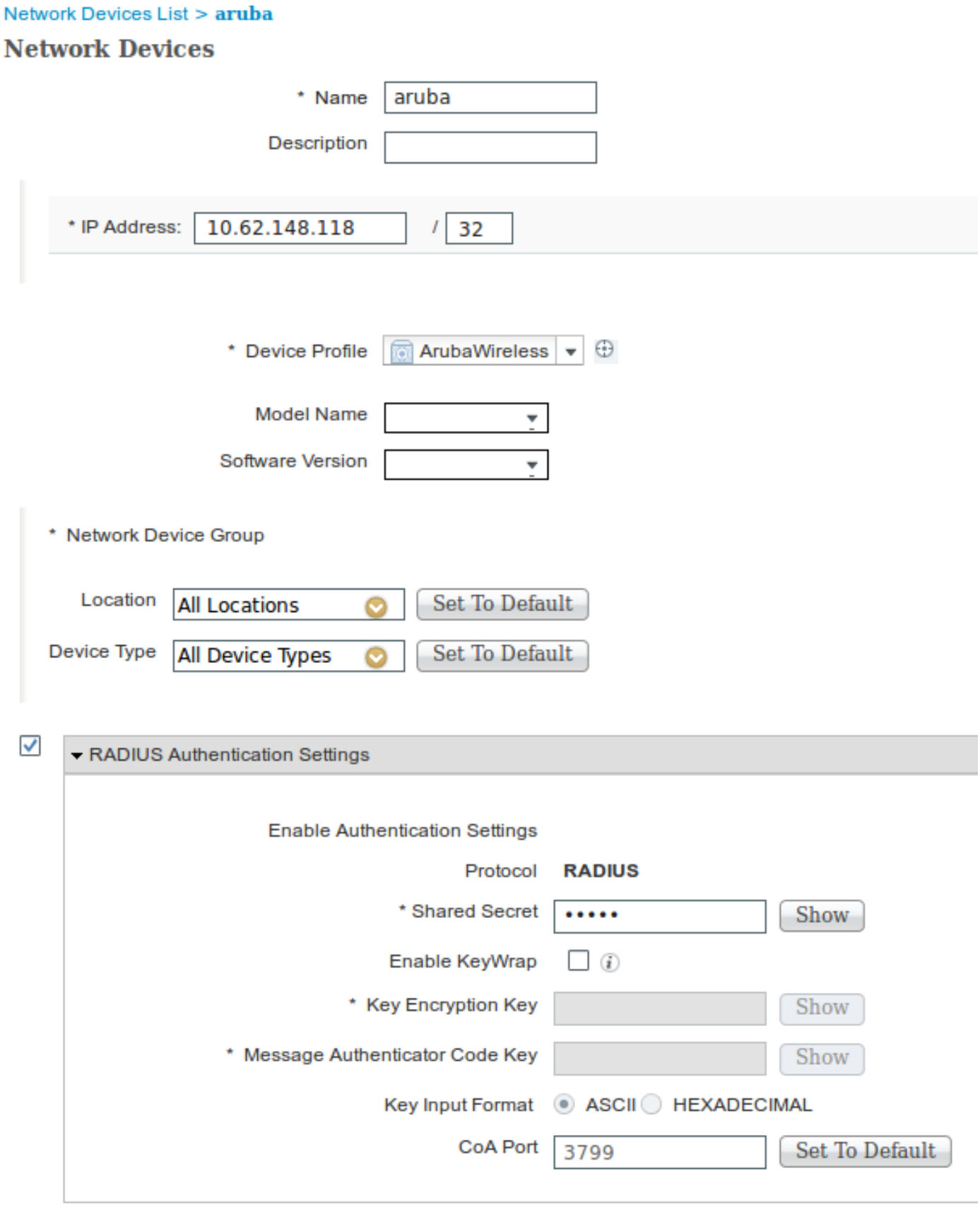
Plus d'informations sur la fonctionnalité :

Profils de périphériques d'accès réseau avec Cisco Identity Services Engine

Cisco ISE

Étape 1. Ajout d'un contrôleur sans fil Aruba aux périphériques réseau

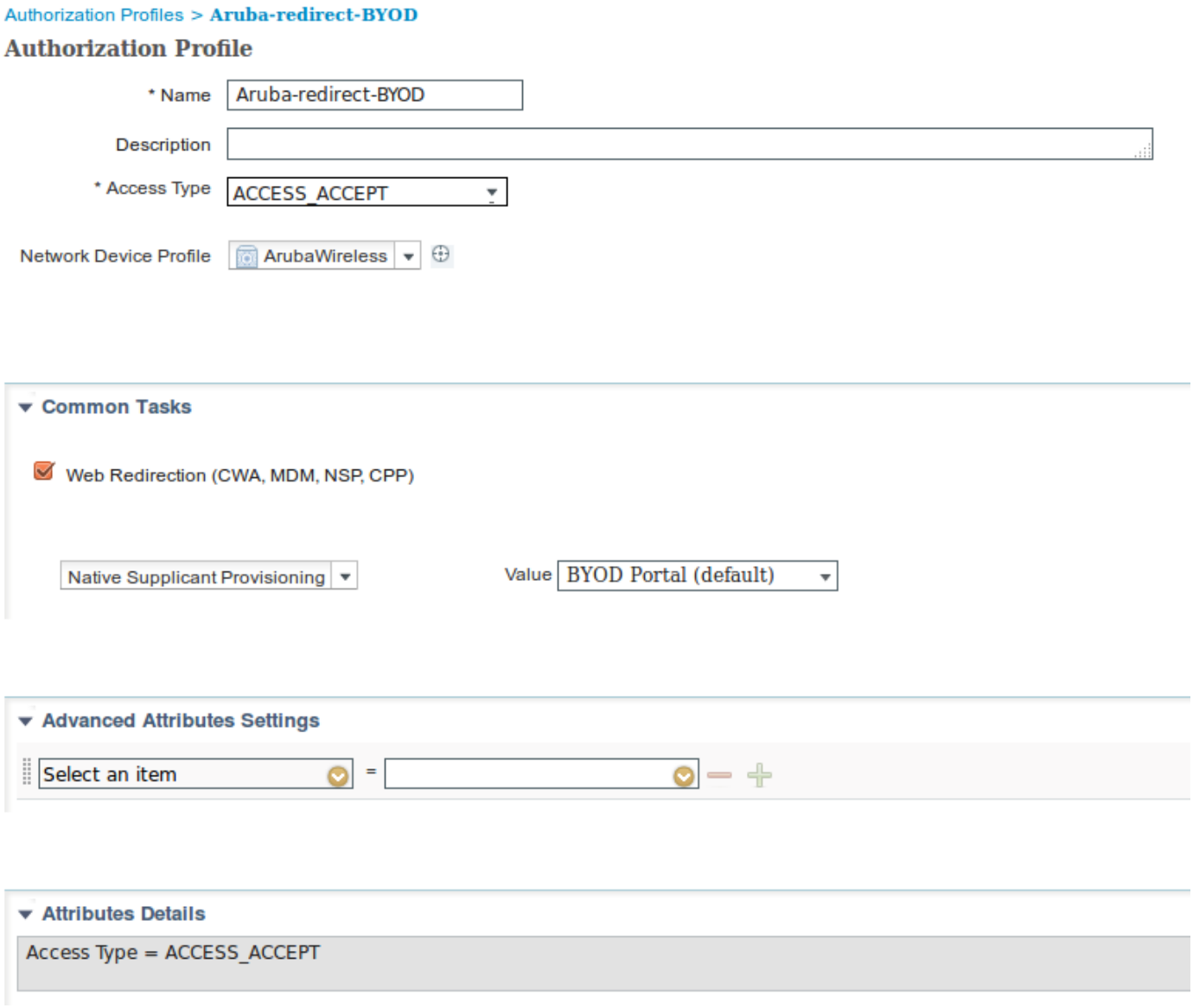
Accédez à Administration > Network Resources > Network Devices. Choisissez le profil de périphérique correct pour le fournisseur sélectionné, dans ce cas : ArubaWireless. Assurez-vous de configurer le secret partagé et le port CoA, comme indiqué dans les images.



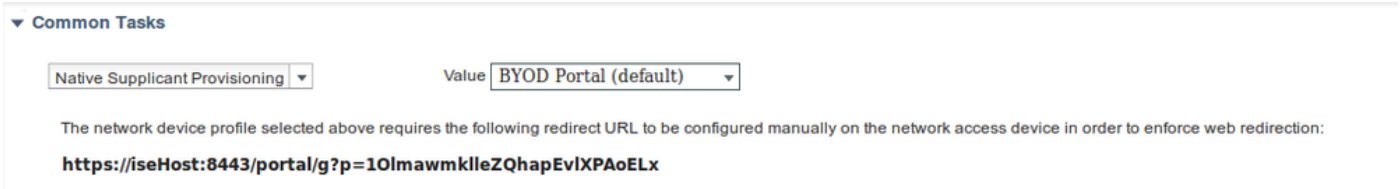
Si aucun profil n'est disponible pour le fournisseur souhaité, vous pouvez le configurer sous Administration > Network Resources > Network Device Profiles.

Étape 2. Configurer le profil d'autorisation

Accédez à Policy > Policy Elements > Results > Authorization > Authorization Profiles et sélectionnez le même profil de périphérique réseau qu'à l'étape 1. ArubaSans fil. Le profil configuré est Aruba-redirect-BYOD with BYOD Portal et comme illustré dans les images.

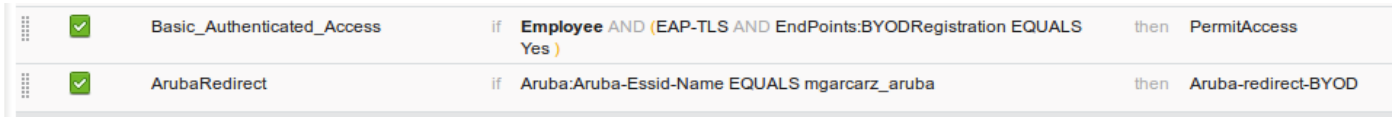


Partie manquante de la configuration de redirection Web, où le lien statique vers le profil d'autorisation est généré. Bien qu'Aruba ne prenne pas en charge la redirection dynamique vers le portail invité, un lien est attribué à chaque profil d'autorisation, qui est ensuite configuré sur Aruba et comme illustré dans l'image.



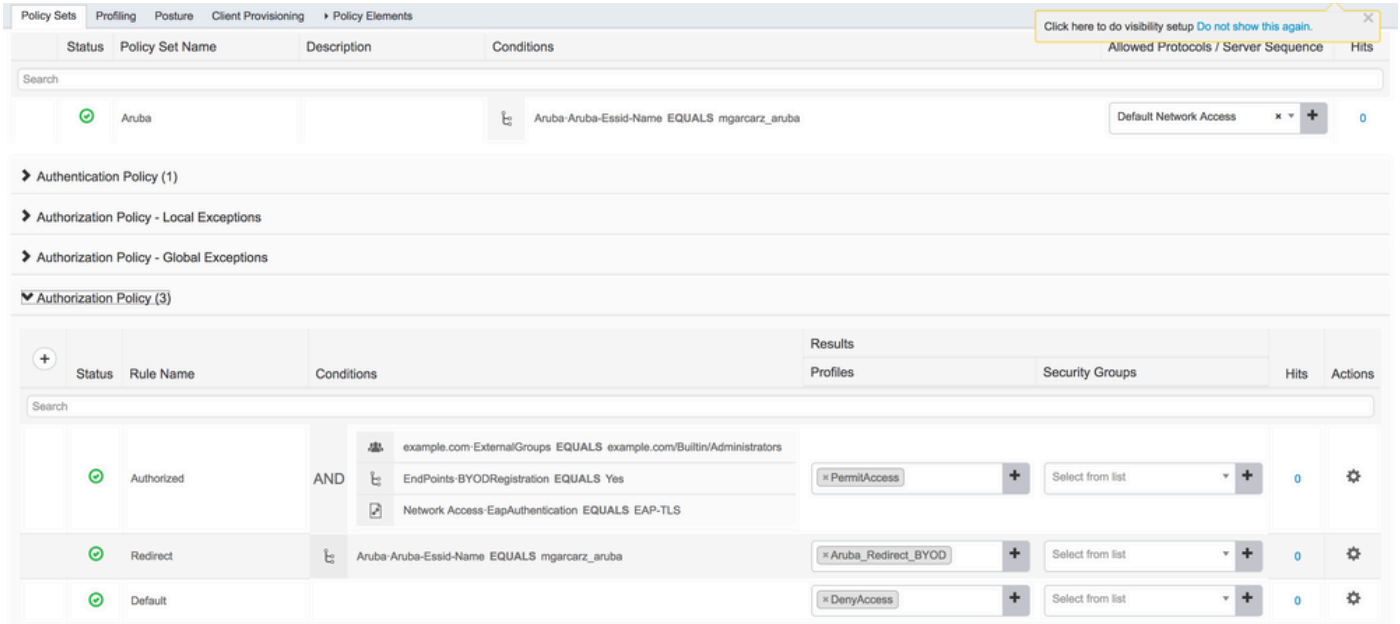
Étape 3. Configurer les règles d'autorisation

Accédez à Policy > Authorization Rules et la configuration est comme indiqué dans l'image.



Tout d'abord, l'utilisateur se connecte au SSID mgracarz_aruba et ISE renvoie le profil d'autorisation Aruba-redirect-BYOD qui redirige le client vers le portail BYOD par défaut. Une fois le processus BYOD terminé, le client se connecte à EAP-TLS et l'accès complet au réseau lui est accordé.

Dans les versions plus récentes d'ISE, la même stratégie peut ressembler à ce qui suit :

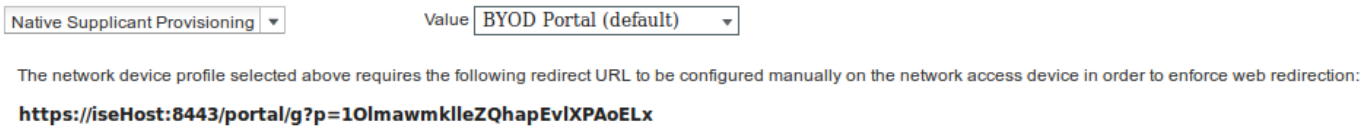


Point d'accès Aruba

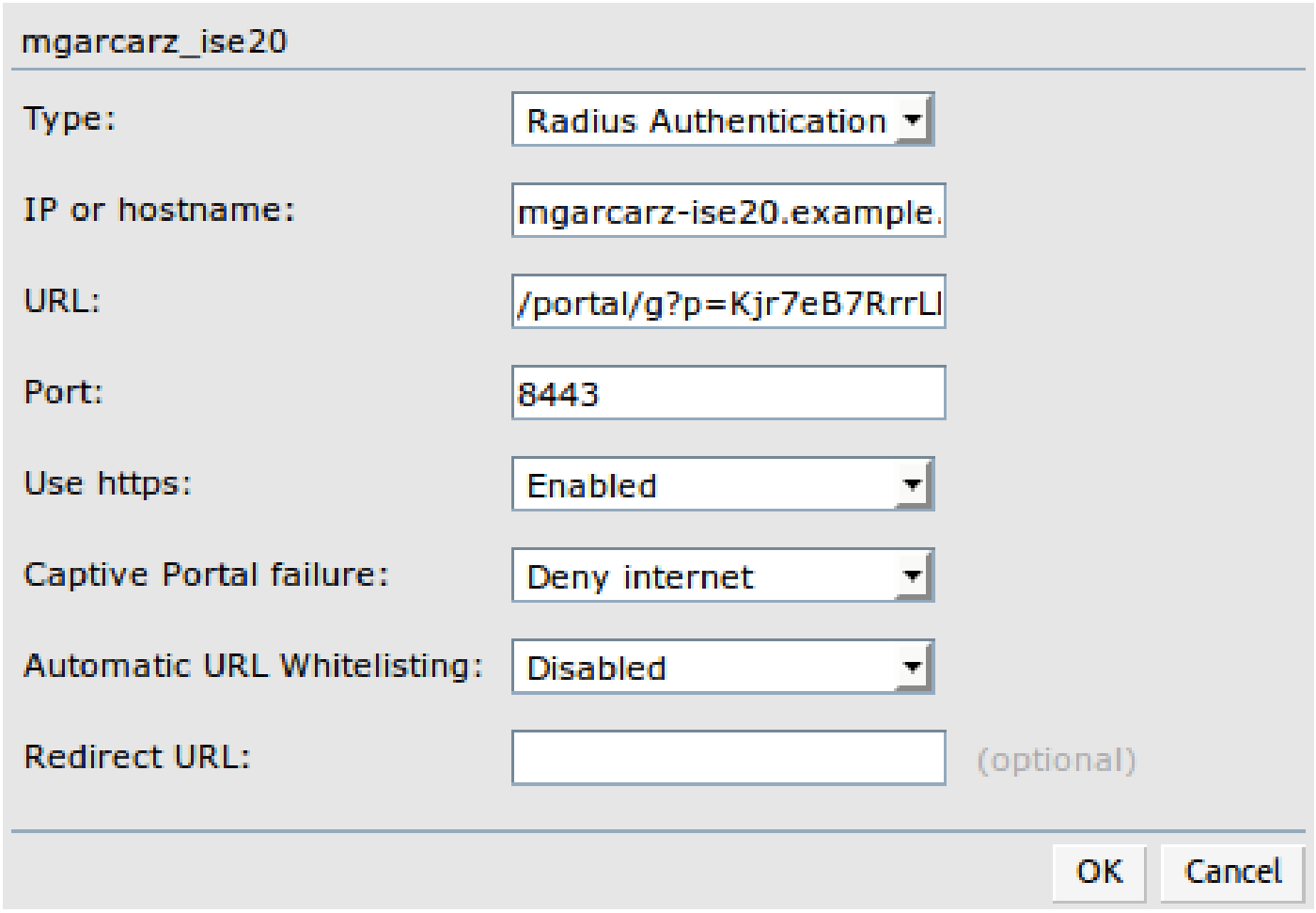
Étape 1. Configuration du portail captif

Afin de configurer le portail captif sur Aruba 204, naviguez vers Security > External Captive Portal et ajoutez un nouveau. Entrez ces informations pour une configuration correcte et comme indiqué dans l'image.

- Type : Authentification Radius
- IP ou nom d'hôte : serveur ISE
- URL : lien créé sur ISE dans la configuration du profil d'autorisation ; il est spécifique à un profil d'autorisation particulier et peut être trouvé ici dans la configuration de redirection Web



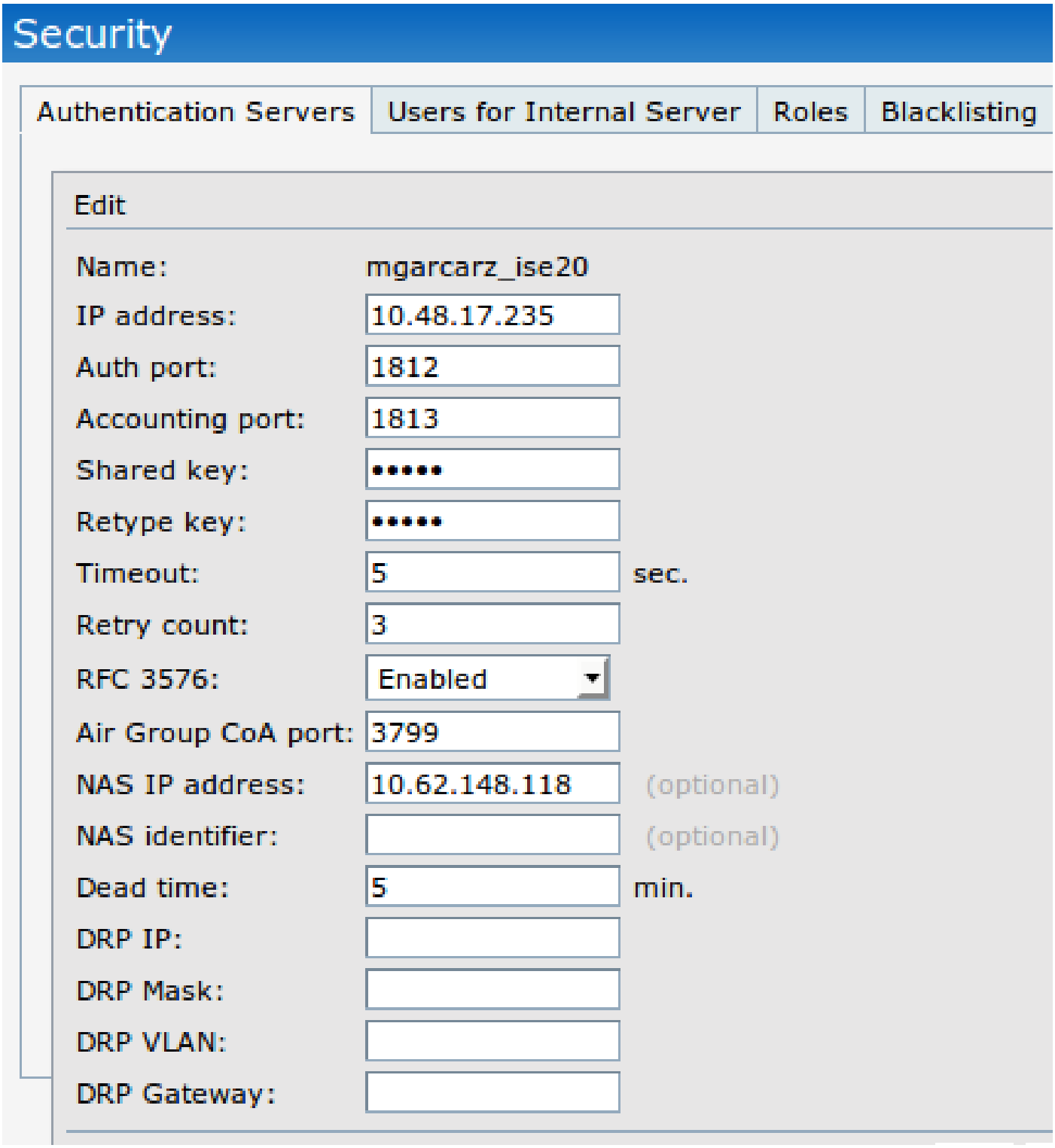
- Port : numéro de port sur lequel le portail sélectionné est hébergé sur ISE (par défaut : 8443), comme illustré dans l'image.



Étape 2. Configuration du serveur RADIUS

Naviguez jusqu'à Security > Authentication Servers pour vous assurer que le port CoA est le même que celui configuré sur ISE comme indiqué dans l'image.

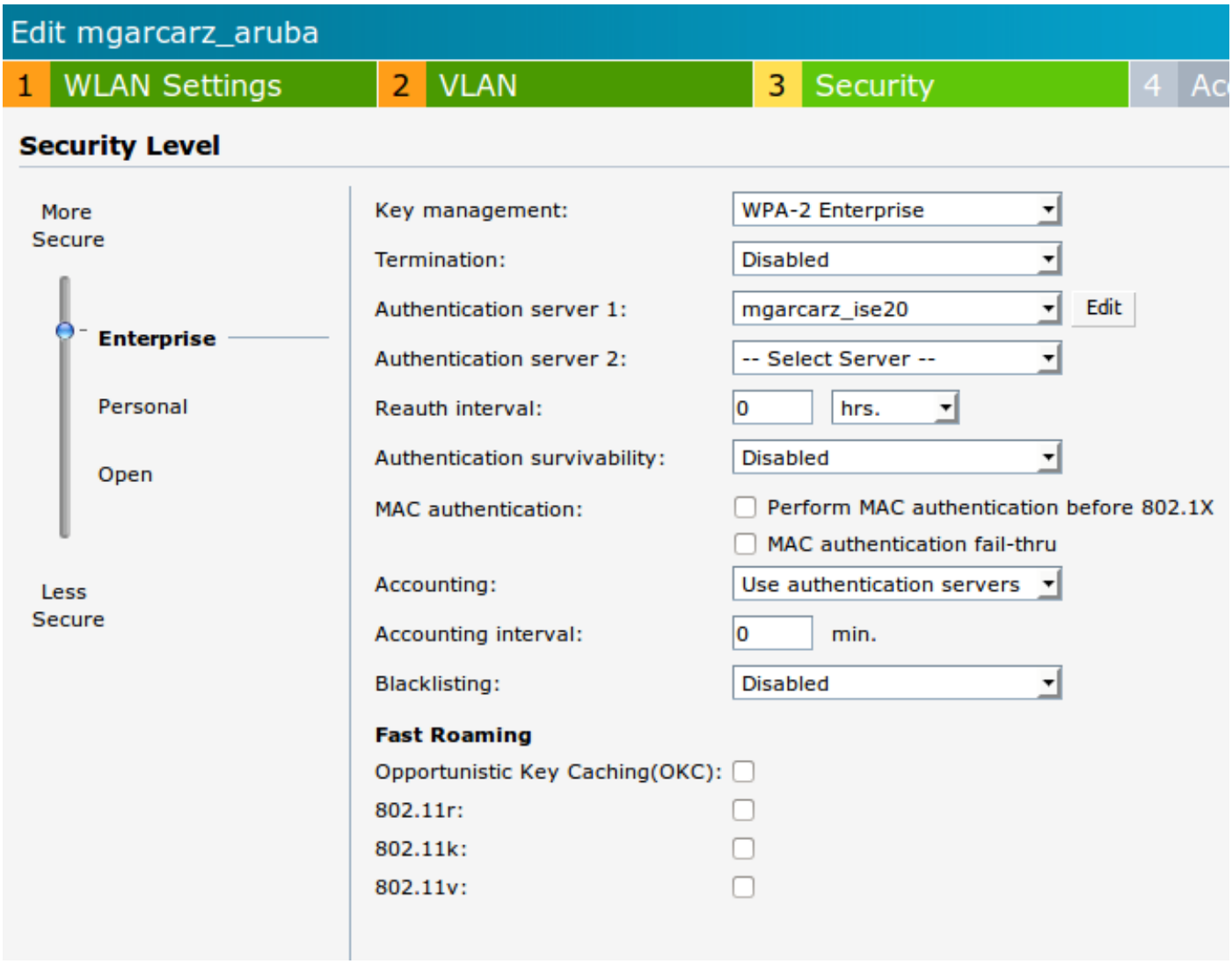
Par défaut, sur Aruba 204, il est défini sur 5999, mais il n'est pas conforme à la RFC 5176 et ne fonctionne pas non plus avec ISE.



Remarque : dans Aruba version 6.5 et plus récente, cochez également la case « Portail captif ».

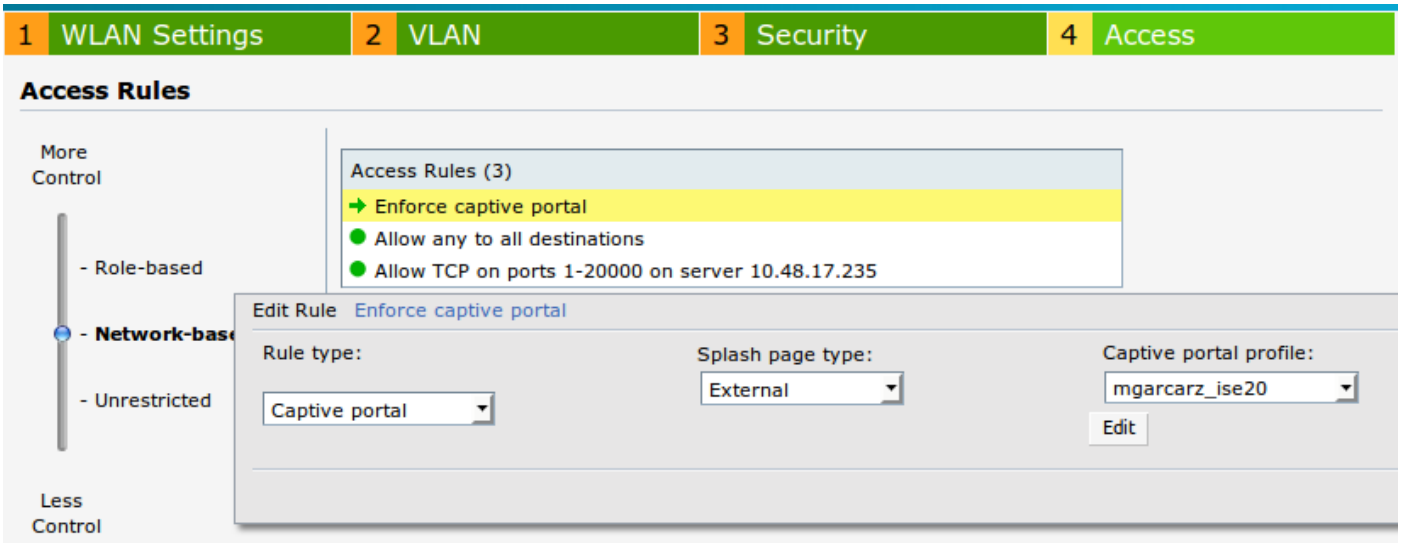
Étape 3. Configuration SSID

- L'onglet Sécurité est tel qu'illustré dans l'image.



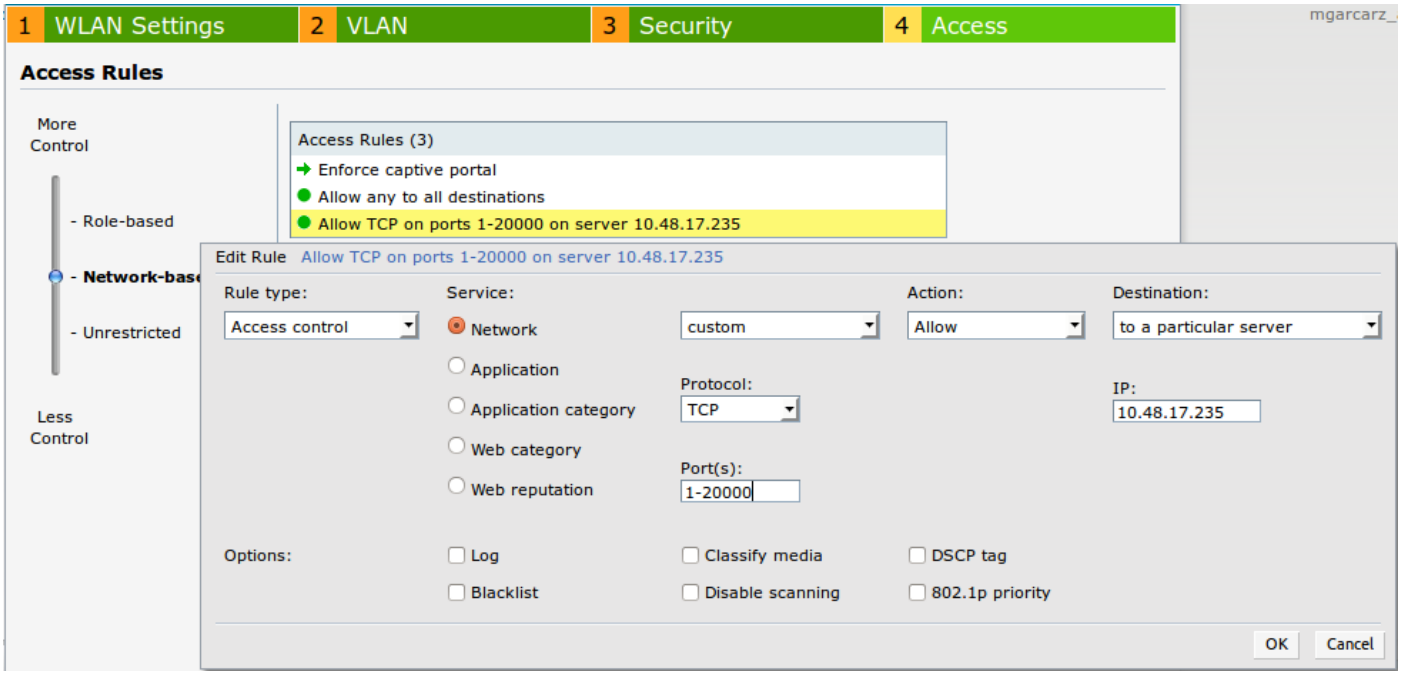
- Onglet Access : sélectionnez Network-based Access Rule afin de configurer le portail captif sur SSID.

Utilisez le portail captif configuré à l'étape 1. Cliquez sur New, choisissez Rule type : Captive portal, Splash page type : External comme indiqué dans l'image.



En outre, autoriser tout le trafic vers le serveur ISE (ports TCP dans la plage 1-20000), tandis que

la règle configurée par défaut sur Aruba : Allow any to all destinations semble ne pas fonctionner correctement comme indiqué dans l'image.

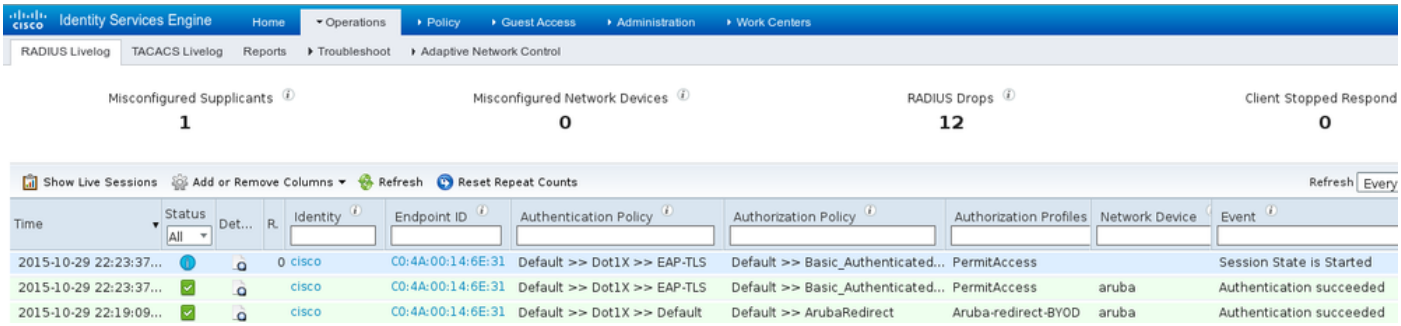


Vérifier

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

Étape 1. Connexion au SSID mgarcarz_aruba avec EAP-PEAP

La première connexion d'authentification sur ISE apparaît. La stratégie d'authentification par défaut a été utilisée, le profil d'autorisation Aruba-redirect-BYOD a été renvoyé comme indiqué dans l'image.

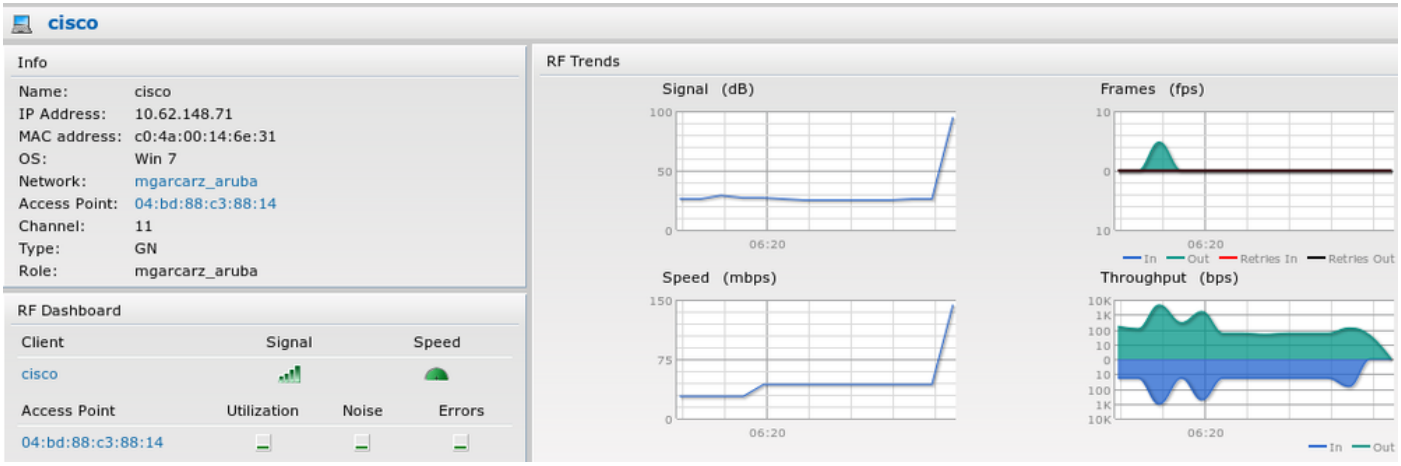


ISE renvoie un message d'acceptation d'accès Radius avec succès EAP. Notez qu'aucun attribut supplémentaire n'est renvoyé (pas de paire av Cisco url-redirect ou url-redirect-acl) comme indiqué dans l'image.

No.	Source	Destination	Protocol	Length	Info	User-Name	Acct-Session-Id
133	10.62.148.118	10.48.17.235	RADIUS	681	Access-Request(1) (id=102, l=639)	cisco	
134	10.48.17.235	10.62.148.118	RADIUS	257	Access-Challenge(11) (id=102, l=215)		
135	10.62.148.118	10.48.17.235	RADIUS	349	Access-Request(1) (id=103, l=307)	cisco	
136	10.48.17.235	10.62.148.118	RADIUS	235	Access-Challenge(11) (id=103, l=193)		
137	10.62.148.118	10.48.17.235	RADIUS	386	Access-Request(1) (id=104, l=344)	cisco	
138	10.48.17.235	10.62.148.118	RADIUS	267	Access-Challenge(11) (id=104, l=225)		
139	10.62.148.118	10.48.17.235	RADIUS	450	Access-Request(1) (id=105, l=408)	cisco	
140	10.48.17.235	10.62.148.118	RADIUS	283	Access-Challenge(11) (id=105, l=241)		
141	10.62.148.118	10.48.17.235	RADIUS	386	Access-Request(1) (id=106, l=344)	cisco	
142	10.48.17.235	10.62.148.118	RADIUS	235	Access-Challenge(11) (id=106, l=193)		
143	10.62.148.118	10.48.17.235	RADIUS	386	Access-Request(1) (id=107, l=344)	cisco	
149	10.48.17.235	10.62.148.118	RADIUS	363	Access-Accept(2) (id=107, l=321)	cisco	
150	10.62.148.118	10.48.17.235	RADIUS	337	Accounting-Request(4) (id=108, l=295)	cisco	04BD88888142-C04A00146E31-42F8
153	10.48.17.235	10.62.148.118	RADIUS	62	Accounting-Response(5) (id=108, l=20)		

```
Packet identifier: 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 indique que la session est établie (l'identité EAP-PEAP est cisco) et que le rôle sélectionné est mgarcarz_aruba, comme indiqué dans l'image.



Ce rôle est responsable de la redirection vers la fonctionnalité ISE (portail captif sur Aruba).

Dans l'interface de ligne de commande d'Aruba, il est possible de confirmer l'état d'autorisation actuel de cette 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#
```

Et afin de vérifier l'ID ACL 138 pour les autorisations actuelles :

<#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

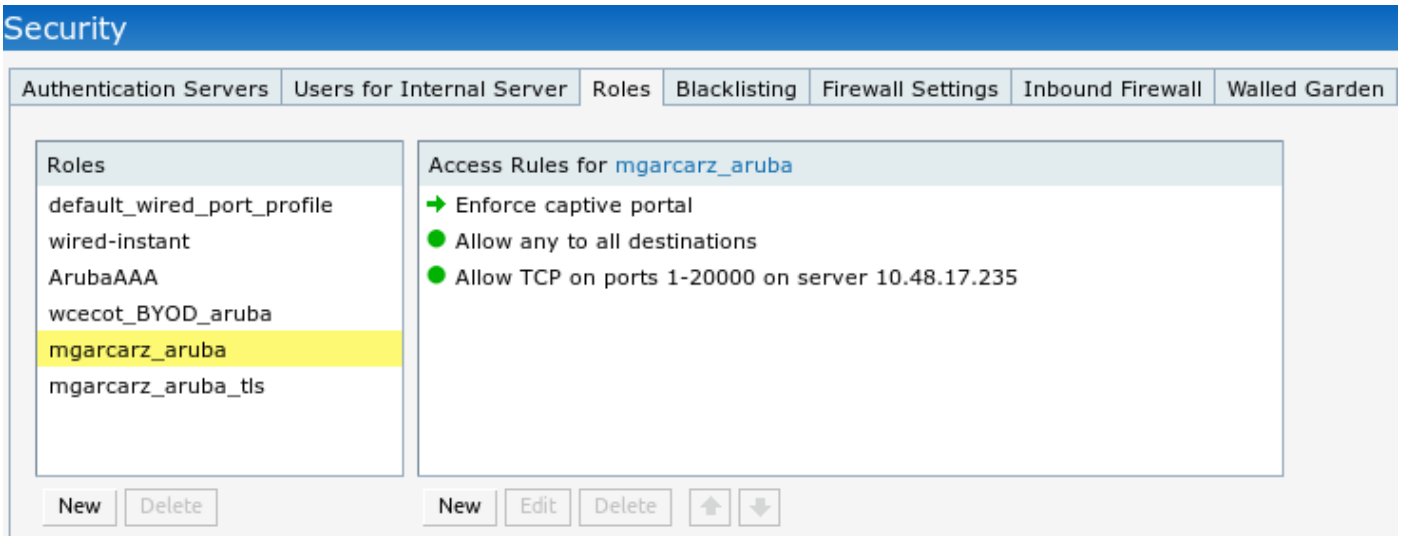
5: any mgarcarz-ise20.example.com 6 0-65535 443-443 Pd4

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

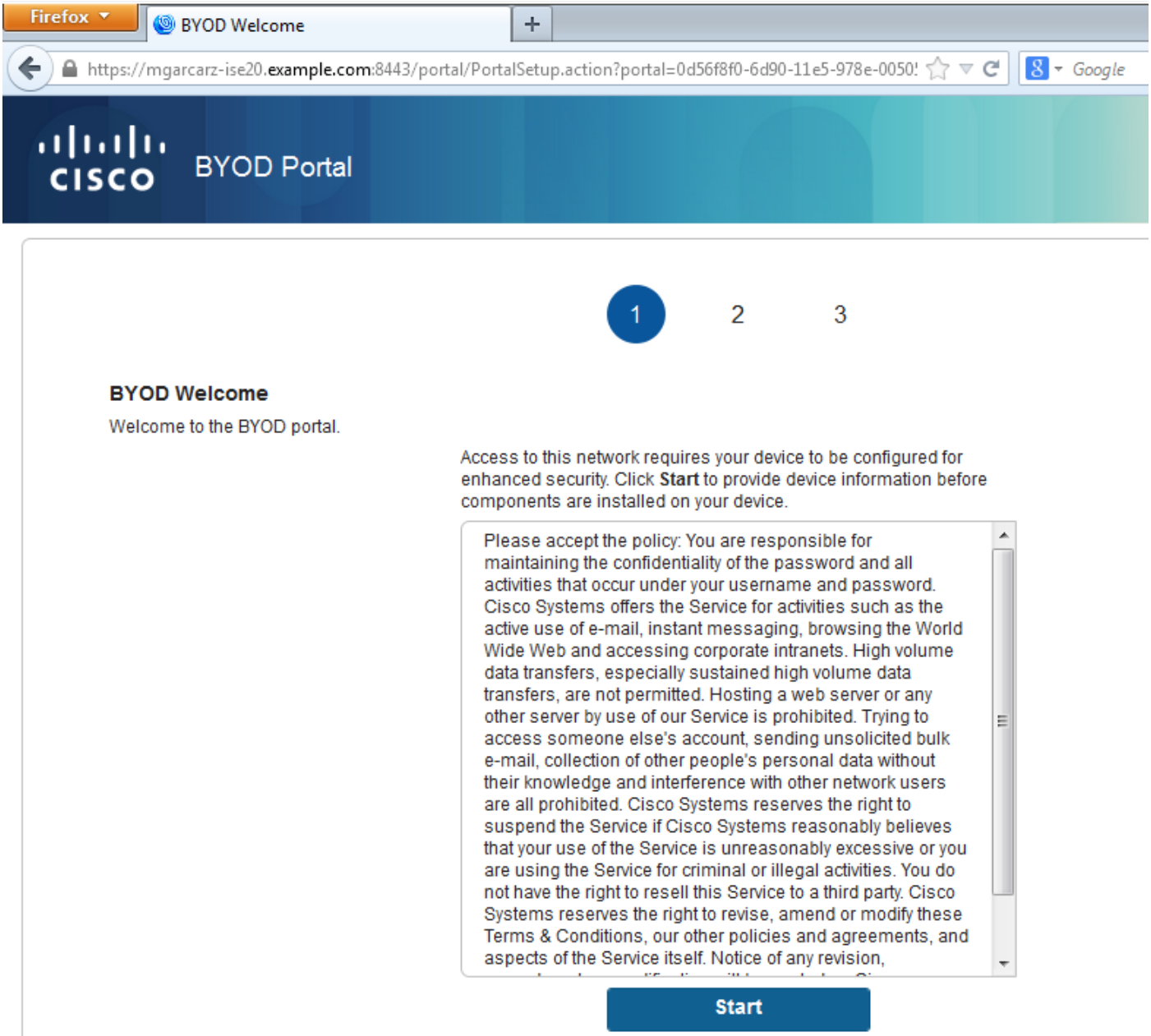
```
<....some output removed for clarity ... >
```

Cela correspond à ce qui a été configuré dans l'interface utilisateur graphique pour ce rôle, comme illustré dans l'image.



Étape 2. Redirection du trafic du navigateur Web pour le BYOD

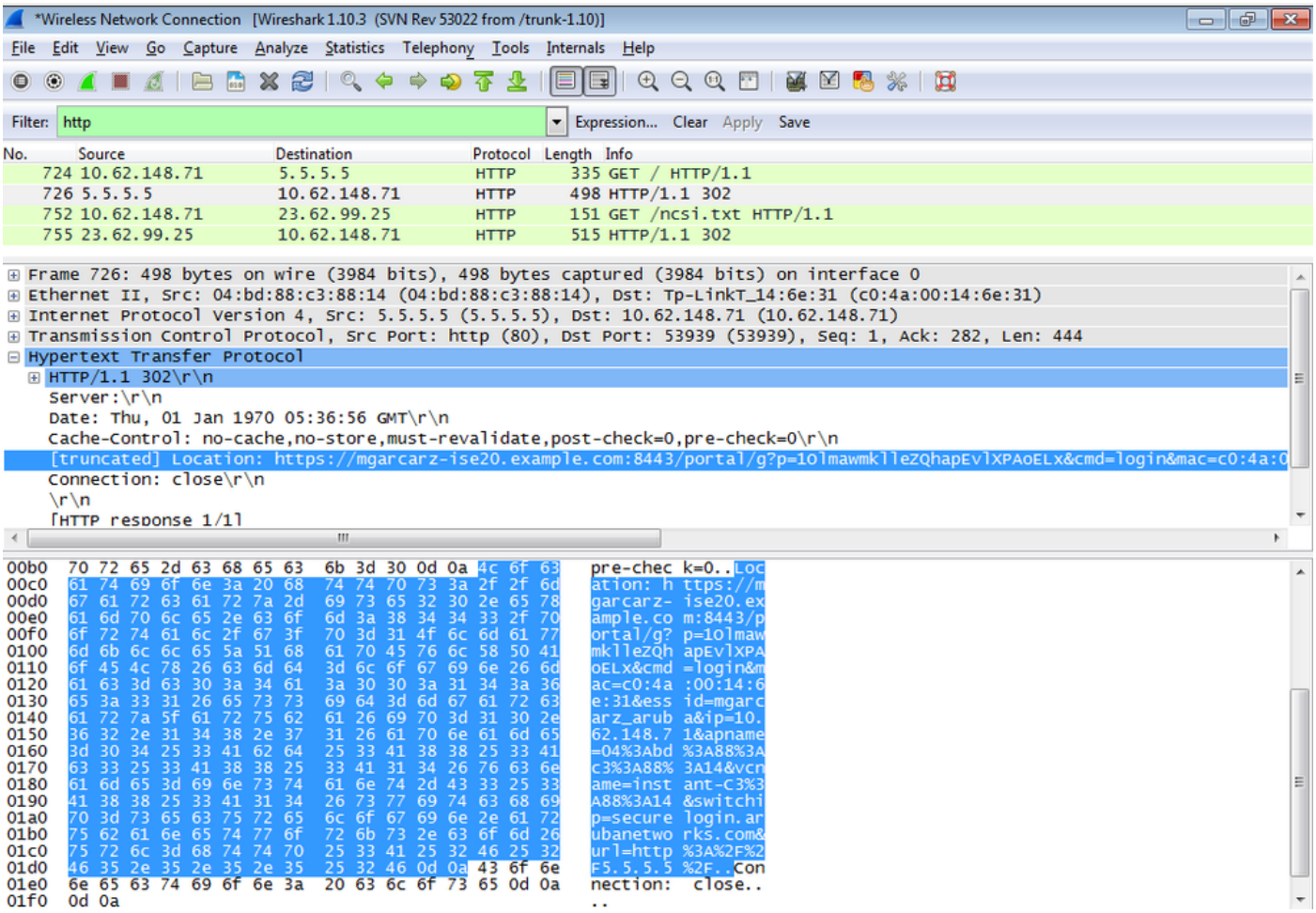
Une fois que l'utilisateur a ouvert le navigateur Web et saisi une adresse, la redirection s'effectue comme indiqué dans l'image.



En examinant les captures de paquets, il est confirmé qu'Aruba usurpe la destination (5.5.5.5) et renvoie la redirection HTTP vers ISE.

Notez qu'il s'agit de la même URL statique que celle configurée dans ISE et copiée sur Captive Portal sur Aruba, mais que plusieurs arguments supplémentaires sont ajoutés comme suit et comme illustré dans l'image :

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



Grâce à ces arguments, ISE peut recréer l'ID de session Cisco, trouver la session correspondante sur ISE et continuer avec le flux BYOD (ou tout autre flux configuré).

Pour les périphériques Cisco, audit_session_id serait normalement utilisé, mais cela n'est pas pris en charge par d'autres fournisseurs.

Afin de confirmer qu'à partir des débogages ISE, il est possible de voir la génération de la valeur audit-session-id (qui n'est jamais envoyée sur le réseau) :

<#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

Et ensuite, corrélation de cela après l'enregistrement de l'appareil sur le 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
```

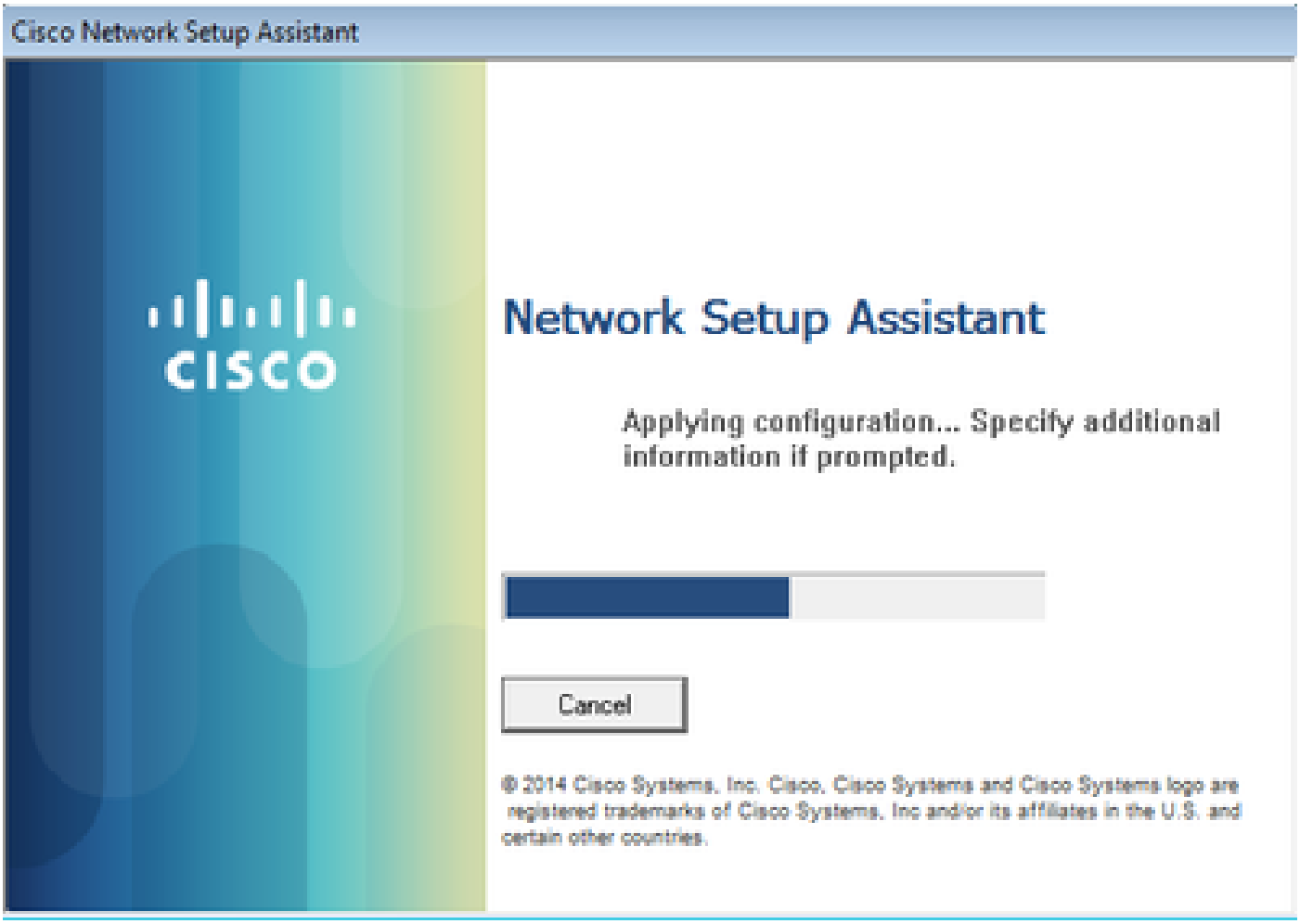
MyDevices: Successfully registered/provisioned the device

```
(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

Dans les demandes suivantes, le client est redirigé vers la page 3 du BYOD, où NSA est téléchargé et exécuté.

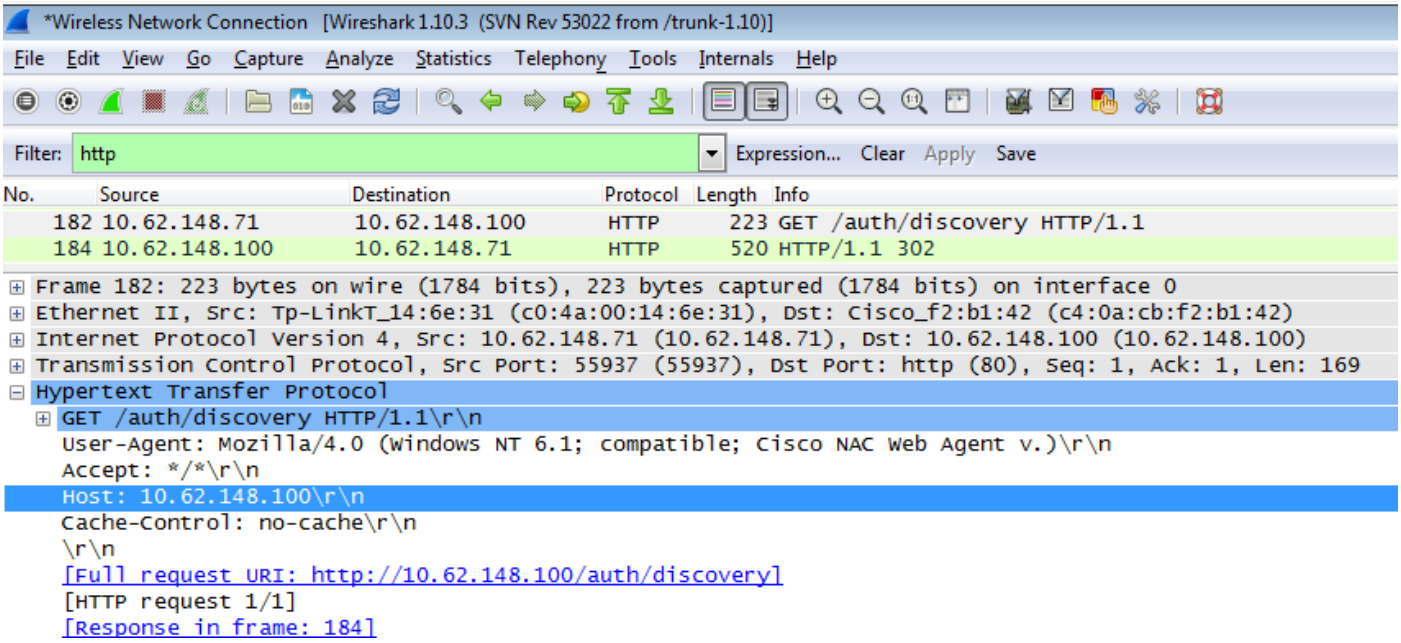
Étape 3. Exécution de Network Setup Assistant



NSA a la même tâche que le navigateur Web. Tout d'abord, il doit détecter l'adresse IP d'ISE. Cela est possible via la redirection HTTP.

Étant donné que cette fois l'utilisateur n'a pas la possibilité de taper une adresse IP (comme dans le navigateur Web), ce trafic est généré automatiquement.

La passerelle par défaut est utilisée (également enroll.cisco.com peut être utilisé) comme indiqué dans l'image.



La réponse est exactement la même que pour le navigateur Web.

De cette façon, NSA peut se connecter à ISE, obtenir un profil xml avec configuration, générer une requête SCEP, l'envoyer à ISE, obtenir un certificat signé (signé par l'autorité de certification interne ISE), configurer le profil sans fil et enfin se connecter au SSID configuré.

Collecter les journaux du client (sous Windows, ils se trouvent dans %temp%/spwProfile.log). Certains résultats sont omis pour des raisons de clarté :

<#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: 0a3011ebXbiuDA3yUNoLUvtCRyuPFxkqYJ7TT06foOZ7
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=
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

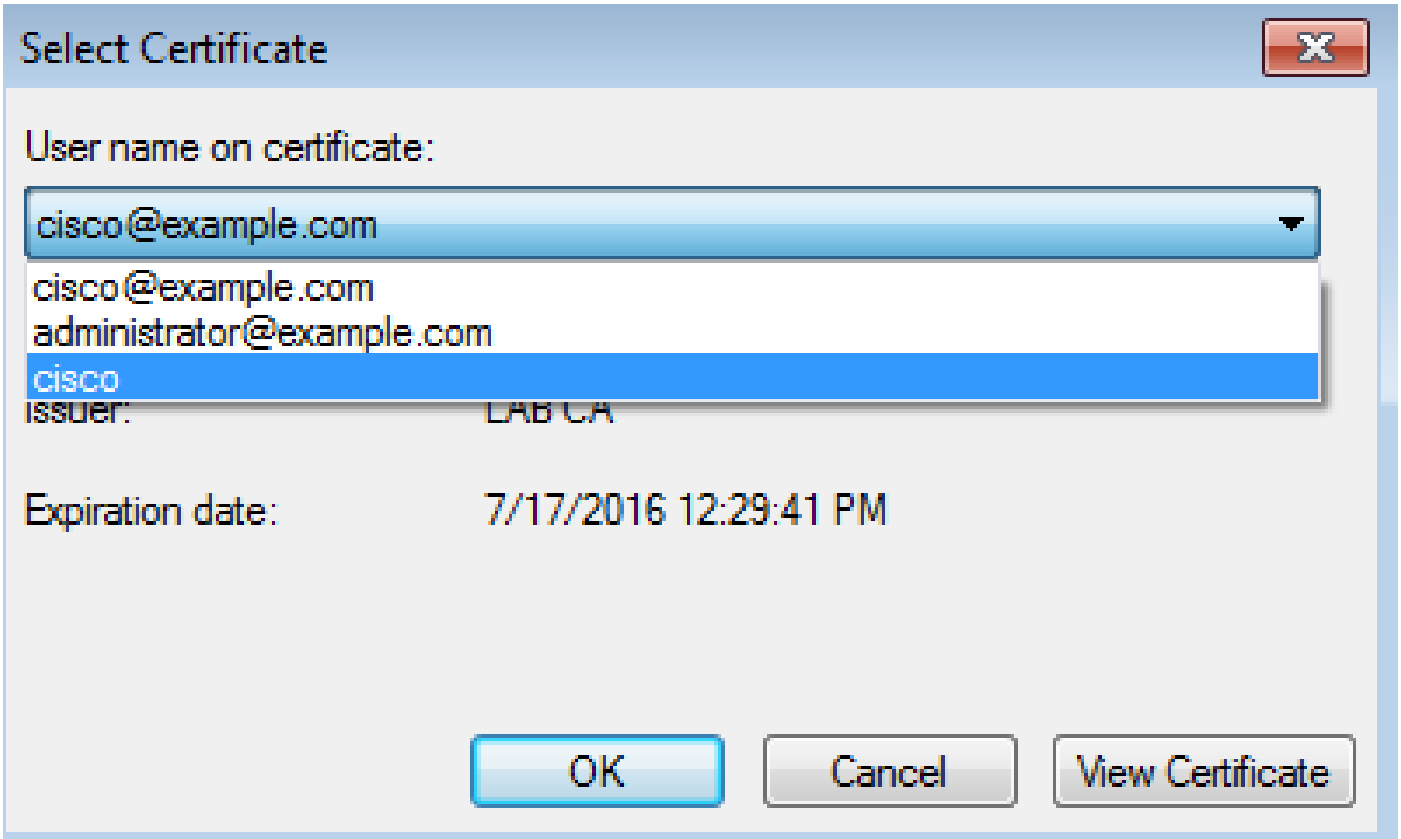
Wireless profile: [mgarcarz_aruba_tls] configured successfully

```
Connect to SSID

Successfully connected profile: [mgarcarz_aruba_tls]

WirelessProfile::SetWirelessProfile. - End
```

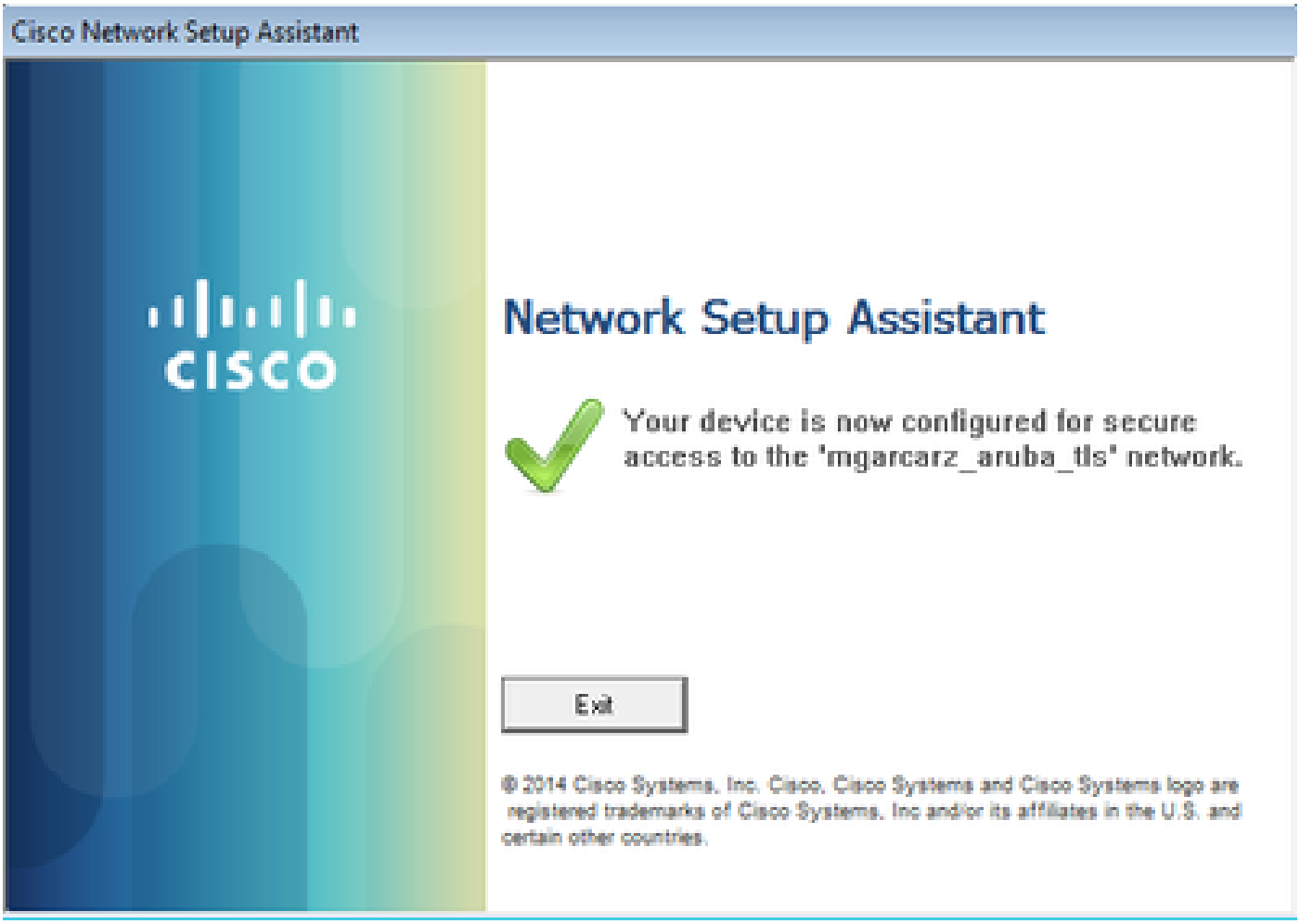
Ces journaux sont exactement les mêmes que pour le processus BYOD avec les périphériques Cisco.

Remarque : Radius CoA n'est pas requis ici. C'est l'application (NSA) qui force la reconnexion à un SSID nouvellement configuré.

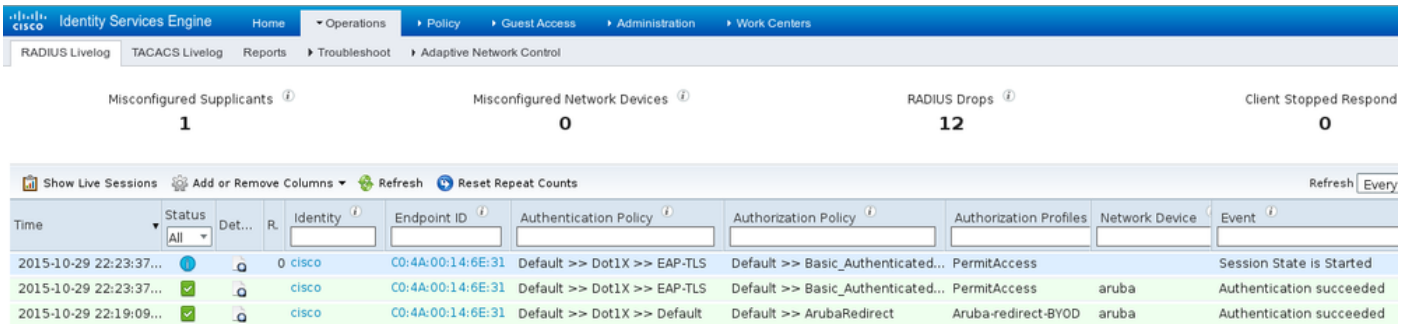
À ce stade, l'utilisateur peut voir que le système tente de s'associer à un SSID final. Si vous disposez de plusieurs certificats utilisateur, vous devez sélectionner le certificat correct (comme illustré).



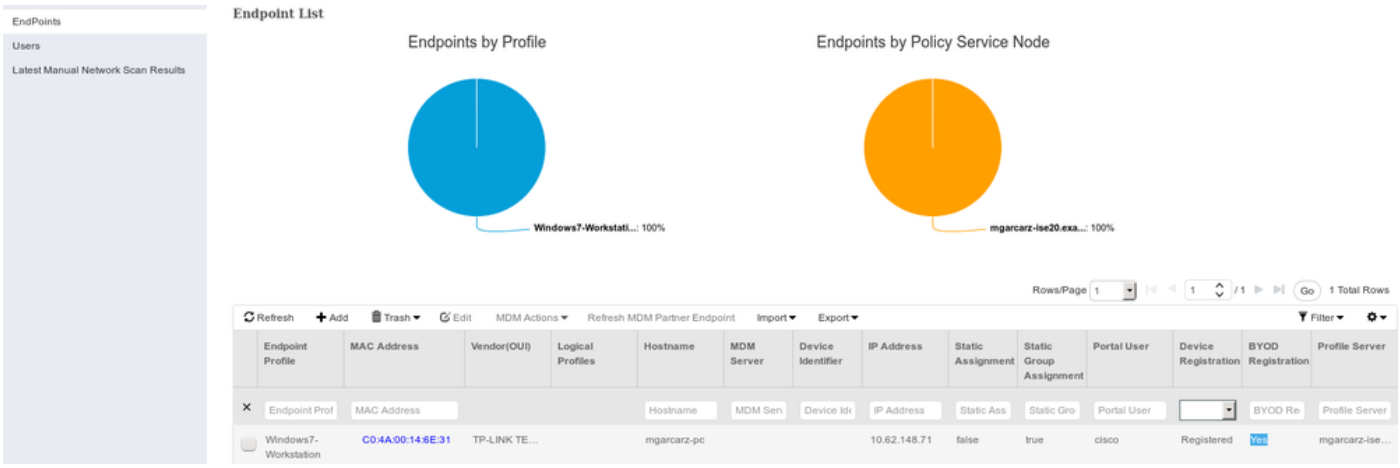
Une fois la connexion établie, les rapports NSA sont tels qu'ils apparaissent dans l'image.



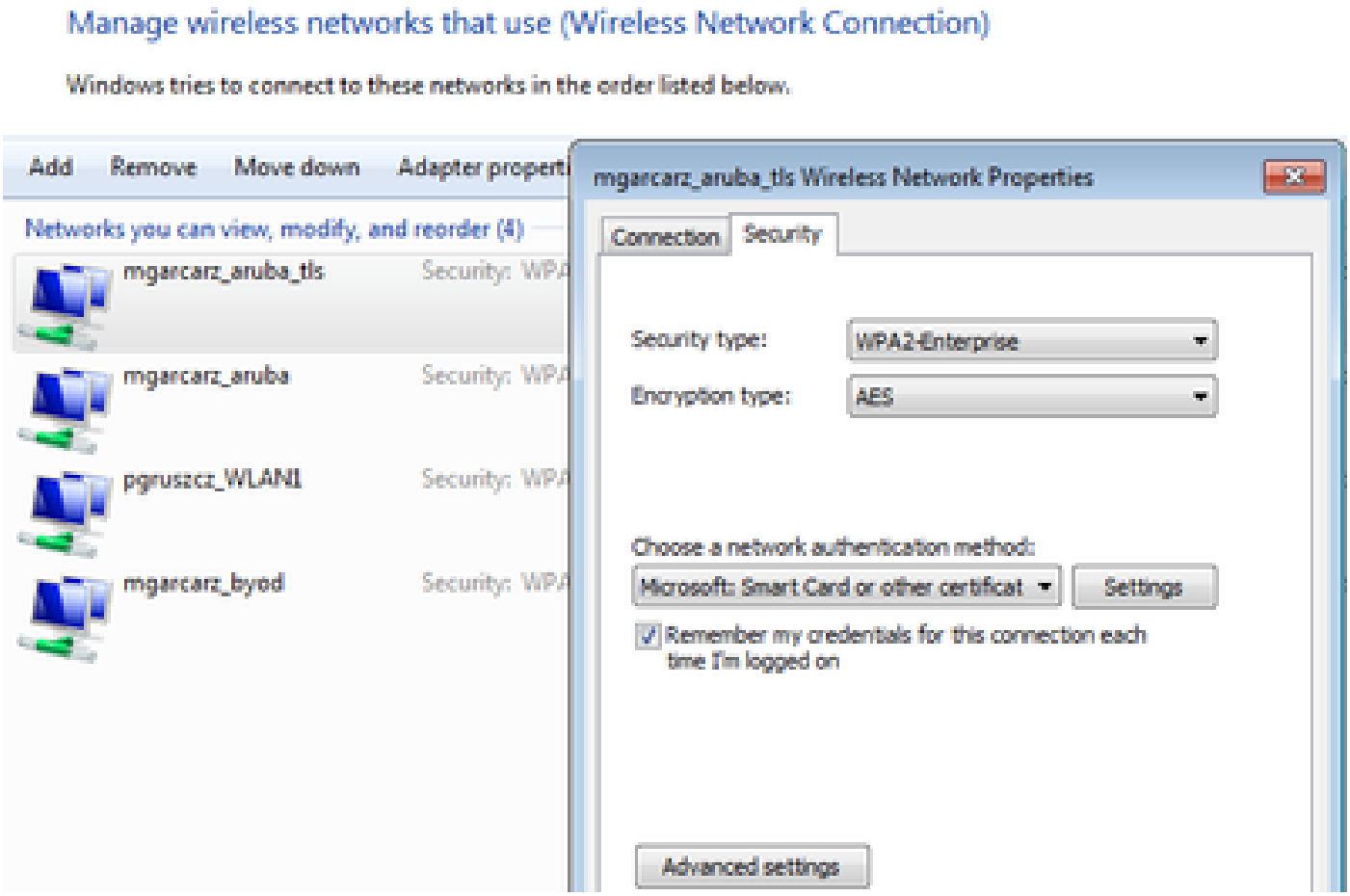
Cela peut être confirmé sur ISE : le deuxième journal atteint l'authentification EAP-TLS, qui correspond à toutes les conditions pour Basic_Authenticated_Access (EAP-TLS, Employee et BYOD Registered true).



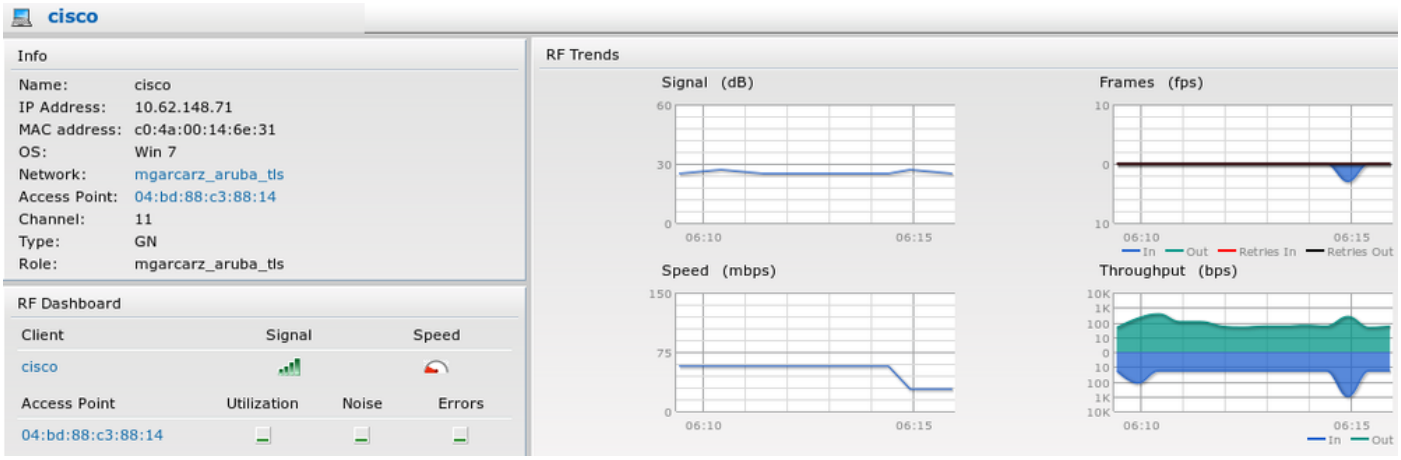
En outre, l'affichage de l'identité du point de terminaison peut confirmer que l'indicateur BYOD Registered du point de terminaison a la valeur true, comme illustré dans l'image.



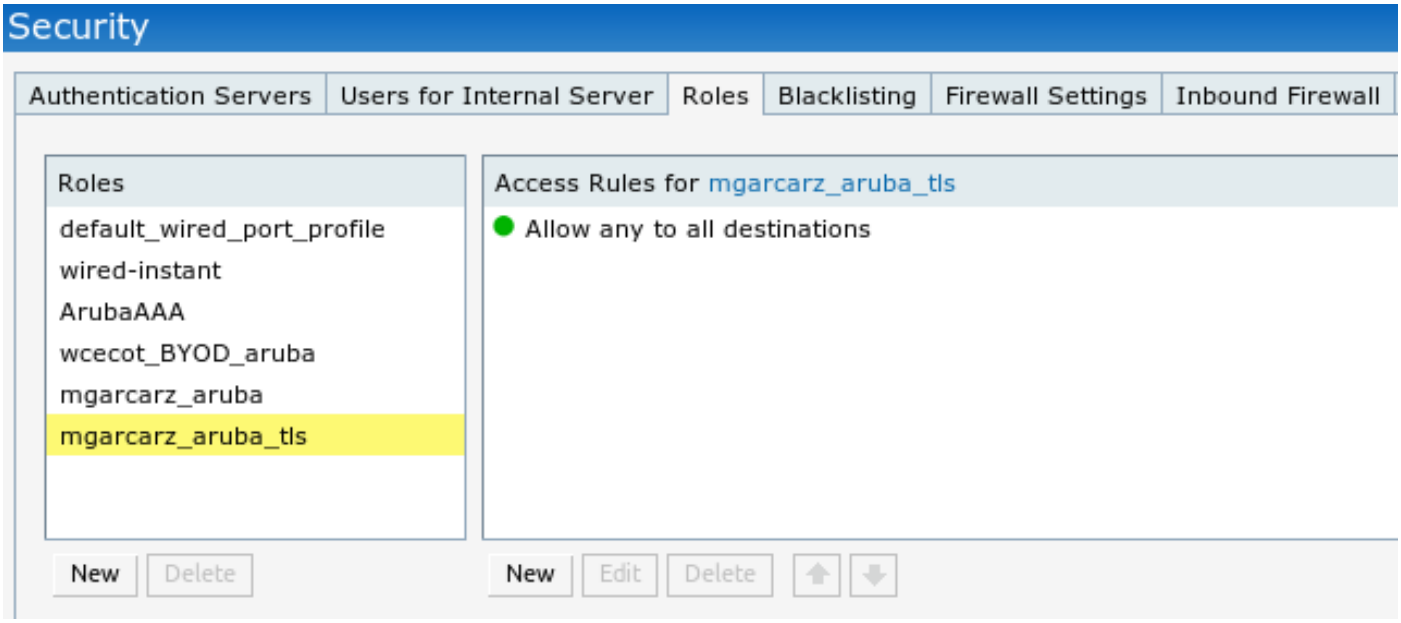
Sur le PC Windows, un nouveau profil sans fil a été créé automatiquement comme favori (et configuré pour EAP-TLS) et comme illustré.



À ce stade, Aruba confirme que l'utilisateur est connecté au SSID final.



Le rôle qui est créé automatiquement et nommé de la même manière que Réseau fournit un accès réseau complet.

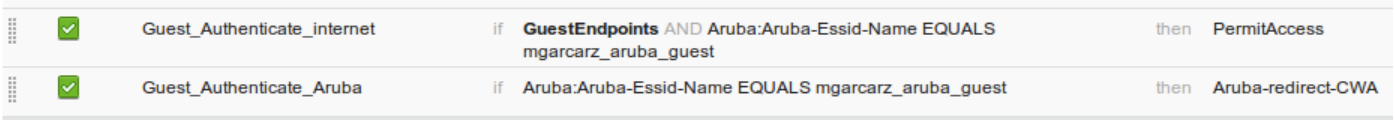


Autres flux et assistance CoA

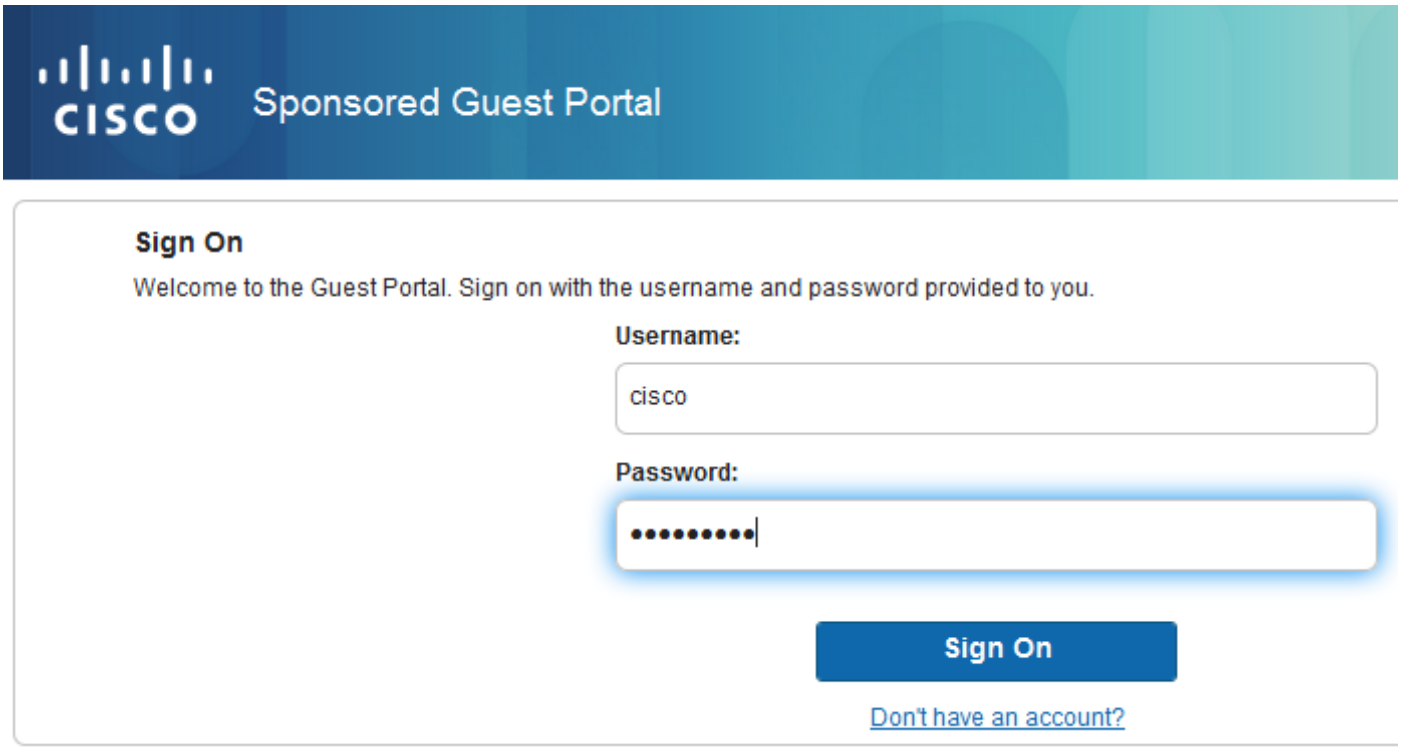
CWA avec CoA

Alors que dans le flux BYOD, il n'y a pas de messages CoA, le flux CWA avec le portail d'invité auto-enregistré est présenté ici :

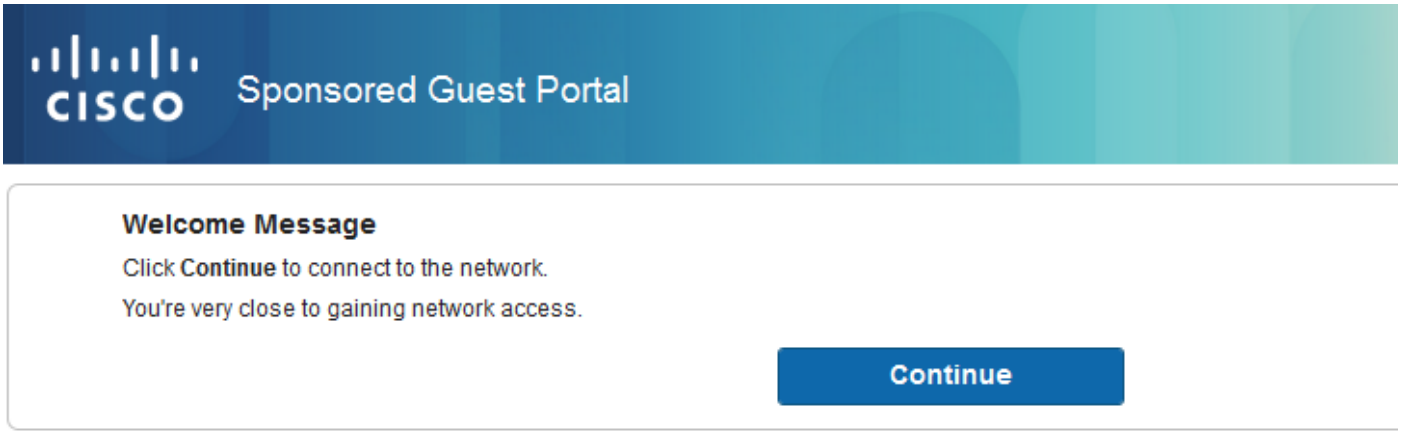
Les règles d'autorisation configurées sont comme indiqué dans l'image.



L'utilisateur se connecte au SSID avec l'authentification MAB et une fois qu'il tente de se connecter à une page Web, la redirection vers le portail d'invité auto-enregistré se produit, où l'invité peut créer un nouveau compte ou utiliser le compte actuel.



Une fois que l'invité est correctement connecté, un message CoA est envoyé d'ISE au périphérique réseau afin de modifier l'état d'autorisation.



Il peut être vérifié sous Opérations > Authentifications et comme montré dans l'image.

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

Message CoA dans les débogages ISE :

<#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

et Disconnect-ACK d'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,

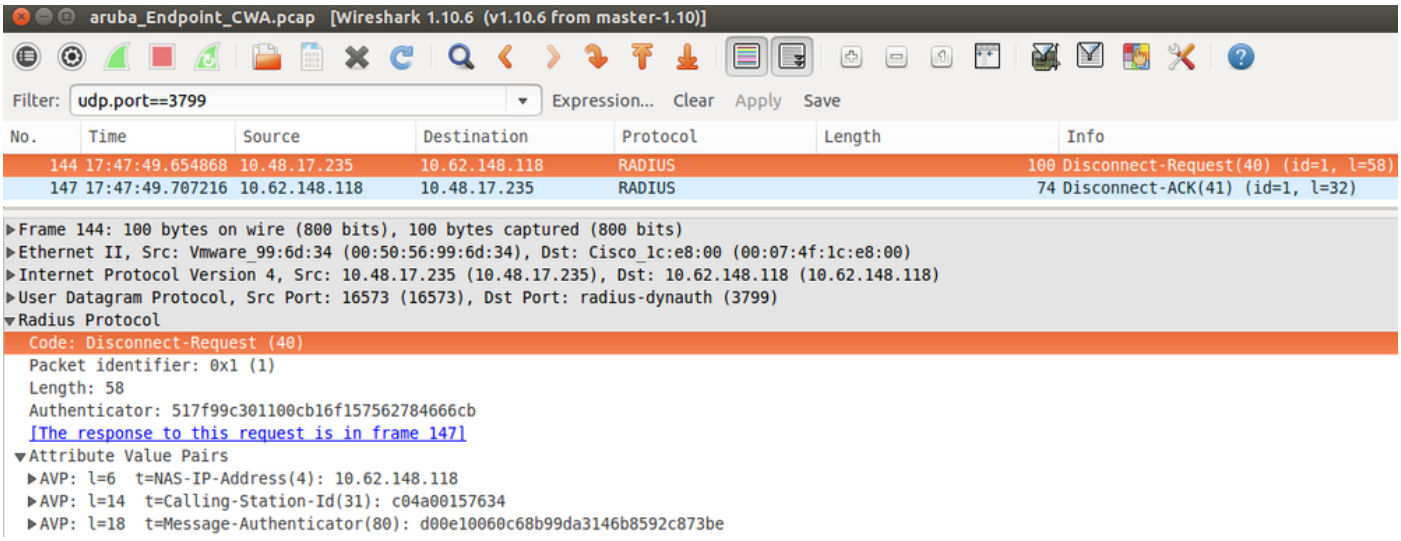
CallingStationID=c04a00157634

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

Packet type 41(DisconnectACK).

,
DynamicAuthorizationFlow.cpp:303

Les captures de paquets avec CoA Disonnect-Request (40) et Diconnect-ACK (41) se présentent comme illustré.



Remarque : RFC CoA a été utilisé pour l'authentification liée au profil de périphérique Aruba (paramètres par défaut). Pour l'authentification liée au périphérique Cisco, il aurait été de type Cisco CoA réauthentifier.

Dépannage

Cette section fournit des informations que vous pouvez utiliser pour dépanner votre configuration.

Portail captif Aruba avec adresse IP au lieu du nom de domaine complet

Si Captive Portal sur Aruba est configuré avec une adresse IP au lieu du nom de domaine complet d'ISE, PSN NSA échoue :

<#root>

```
Warning - [HTTPConnection]
```

Abort the HTTP connection due to invalid certificate

CN

La raison en est une validation stricte des certificats lorsque vous vous connectez à ISE. Lorsque vous utilisez l'adresse IP afin de vous connecter à ISE (à la suite de l'URL de redirection avec l'adresse IP au lieu de FQDN) et sont présentés avec le certificat ISE avec le nom du sujet = la validation FQDN échoue.

Remarque : le navigateur Web continue avec le portail BYOD (avec un avertissement qui

doit être approuvé par l'utilisateur).

Aruba Captive Portal - Politique d'accès incorrecte

Par défaut, la politique d'accès Aruba configurée avec Captive Portal autorise les ports TCP 80, 443 et 8080.

NSA ne peut pas se connecter au port TCP 8905 pour obtenir le profil xml d'ISE. Cette erreur est signalée :

<#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=0a3O11ebXbiuDA3yUNoLUvtCRyuPFxkqYJ7TT06foOZ7G1HXj1M&os=Windows All]
- http Error: [2]

HTTP response code: 0

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

Numéro de port Aruba CoA

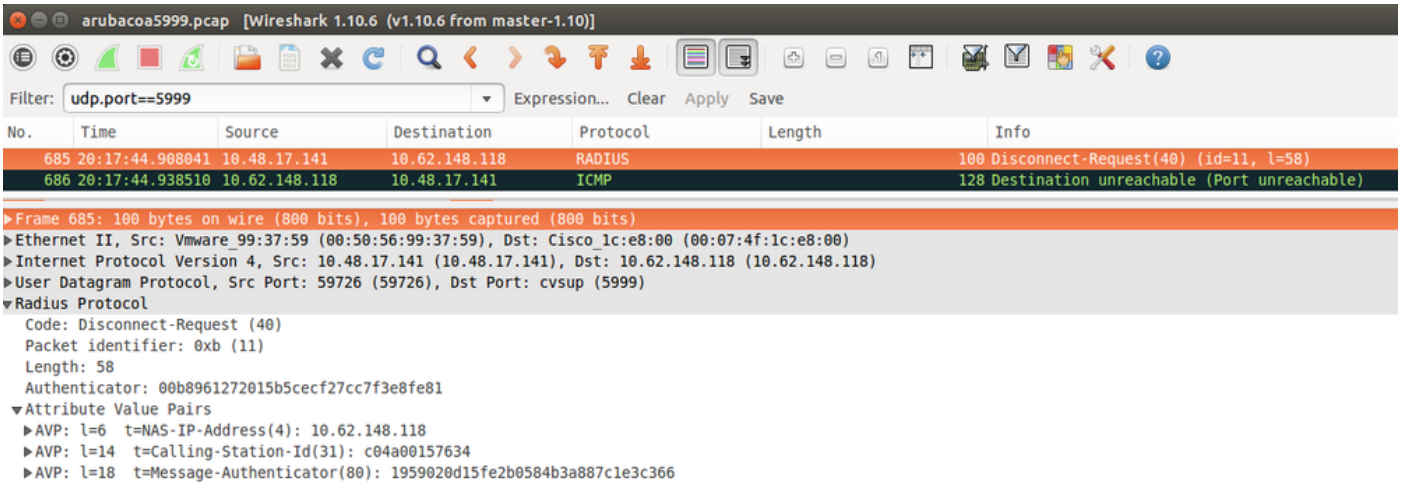
Par défaut, Aruba fournit un numéro de port pour le port 5999 CoA Air Group CoA. Malheureusement, Aruba 204 n'a pas répondu à ces demandes (comme indiqué).

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

La capture de paquets se déroule comme illustré dans l'image.



La meilleure option à utiliser ici peut être le port CoA 3977, comme décrit dans la RFC 5176.

Redirection sur certains périphériques Aruba

Sur Aruba 3600 avec v6.3, on remarque que la redirection fonctionne légèrement différemment que sur les autres contrôleurs. La capture des paquets et l'explication sont disponibles ici.

<#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

Informations connexes

- Guide de l'administrateur de Cisco Identity Services Engine, version 2.0
- Profils de périphériques d'accès réseau avec Cisco Identity Services Engine
- Assistance et documentation techniques - Cisco Systems

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.