Exemple de configuration de l'authentification Web centralisée sur le WLC et ISE

Contenu

[Introduction](#)
[Conditions préalables](#)
[Conditions requises](#)
[Components Used](#)
[Configuration](#)
[Configuration WLC](#)
[Configuration ISE](#)
[Créer le profil d'autorisation](#)
[Créer une règle d'authentification](#)
[Créer une stratégie d'autorisation](#)
[Activer le renouvellement IP (facultatif - non recommandé)](#)
[Scénario Anchor-Foreign](#)
[Vérification](#)
[Dépannage](#)
[Considérations spéciales pour les scénarios d'ancrage](#)

Introduction

Ce document décrit un exemple de configuration qui est utilisé afin de terminer l'authentification Web centrale (CWA) sur le contrôleur de réseau local sans fil (WLC).

Il est remplacé par le guide de déploiement invité plus complet disponible ici : https://communities.cisco.com/docs/DOC-77590

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Components Used

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

- Le logiciel **Cisco ® Identity Services Engine (ISE)** version 3.0
- Logiciel Cisco WLC version 8.3.150.0

Configuration

La première méthode d'authentification Web est l'authentification Web locale. Dans ce cas, le WLC redirige le trafic HTTP vers un serveur interne ou externe où l'utilisateur est invité à s'authentifier. Le WLC récupère ensuite les informations d'identification (renvoyées via une requête HTTP GET dans le cas d'un serveur externe) et effectue une authentification RADIUS. Dans le cas d'un utilisateur invité, un serveur externe tel que Identity Services Engine (ISE) est requis car le portail fournit des fonctionnalités telles que l'enregistrement des périphériques et l'auto-approvisionnement. Le flux comprend les étapes suivantes :

1. L'utilisateur s'associe au SSID (Service Set Identifier) d'authentification Web.

2. L'utilisateur ouvre le navigateur.

3. Le WLC redirige vers le portail invité (tel qu'ISE) dès qu'une URL est entrée.

4. L'utilisateur s'authentifie sur le portail.

5. Le portail invité redirige vers le WLC avec les informations d'identification entrées.

6. Le WLC authentifie l'utilisateur invité via RADIUS.

7. Le WLC redirige vers l'URL d'origine.

Ce flux comprend plusieurs redirections. La nouvelle approche consiste à utiliser le CWA. Le flux comprend les étapes suivantes :

1. L'utilisateur s'associe au SSID d'authentification Web, qui est en fait ouvert. Aucune sécurité de couche 2 et de couche 3, seul le filtrage Mac est activé.

2. L'utilisateur ouvre le navigateur.

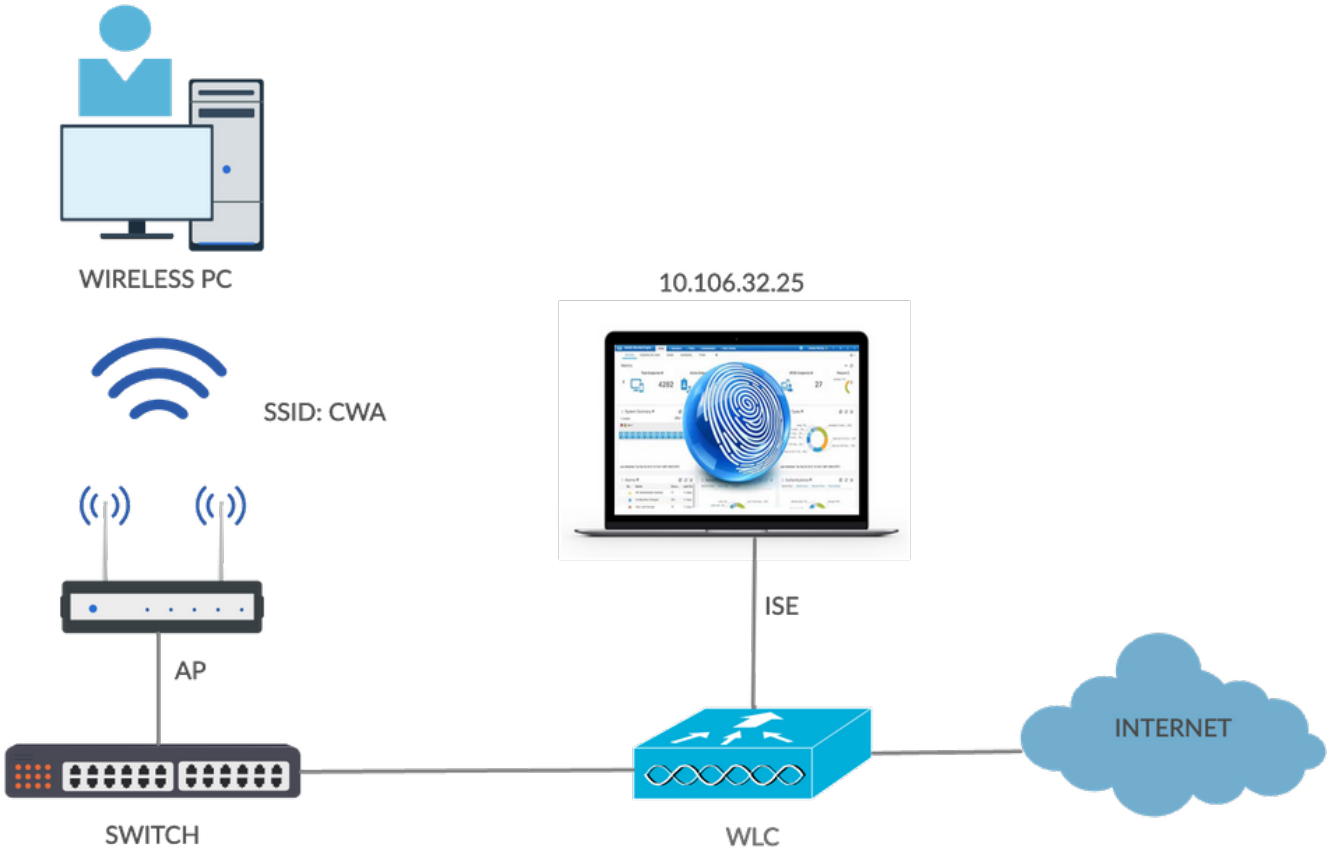
3. Le WLC redirige vers le portail invité.

4. L'utilisateur s'authentifie sur le portail.

5. L'ISE envoie un changement d'autorisation RADIUS (CoA - port UDP 1700) pour indiquer au contrôleur que l'utilisateur est valide, et finit par appliquer des attributs RADIUS tels que la liste de contrôle d'accès (ACL).

6. L'utilisateur est invité à réessayer l'URL d'origine.

La configuration utilisée est la suivante :

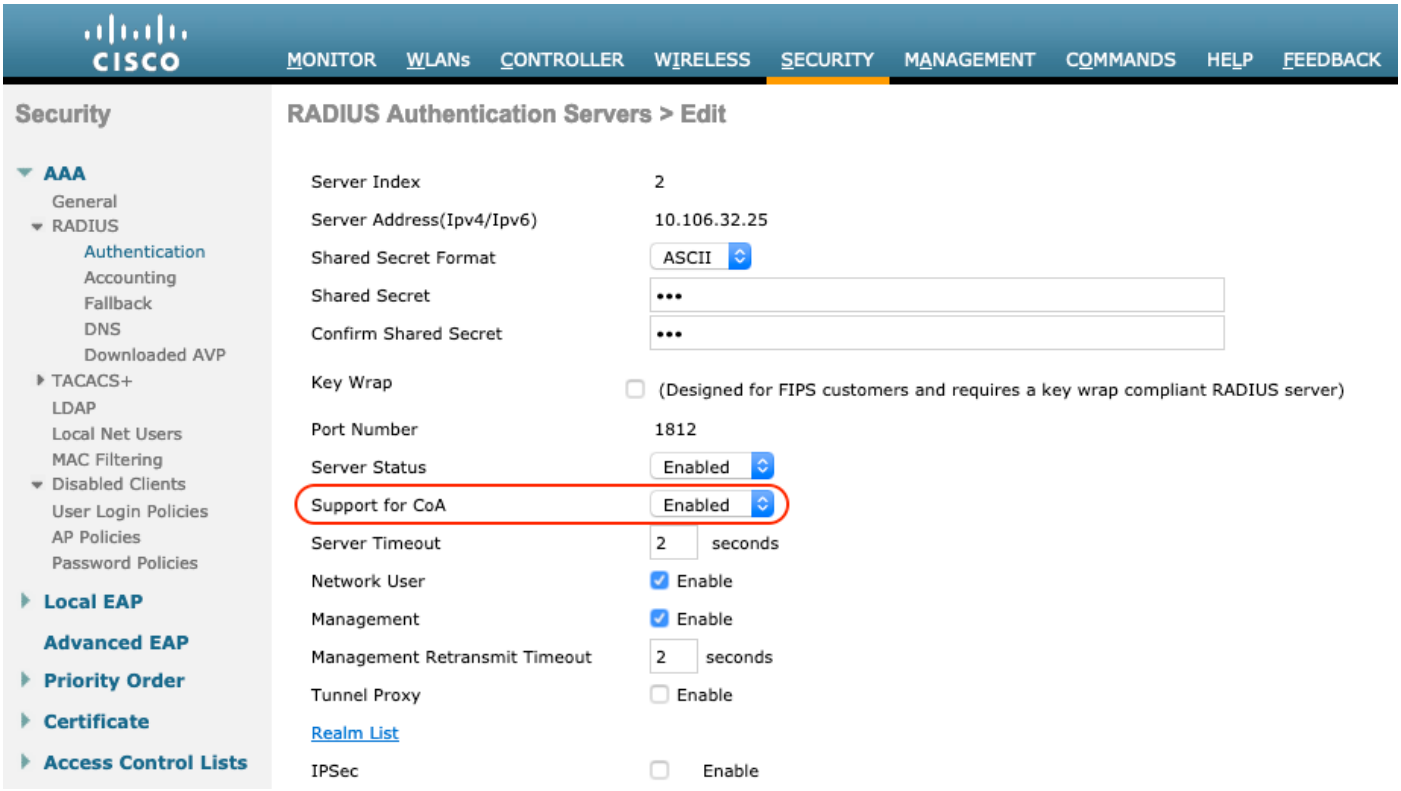


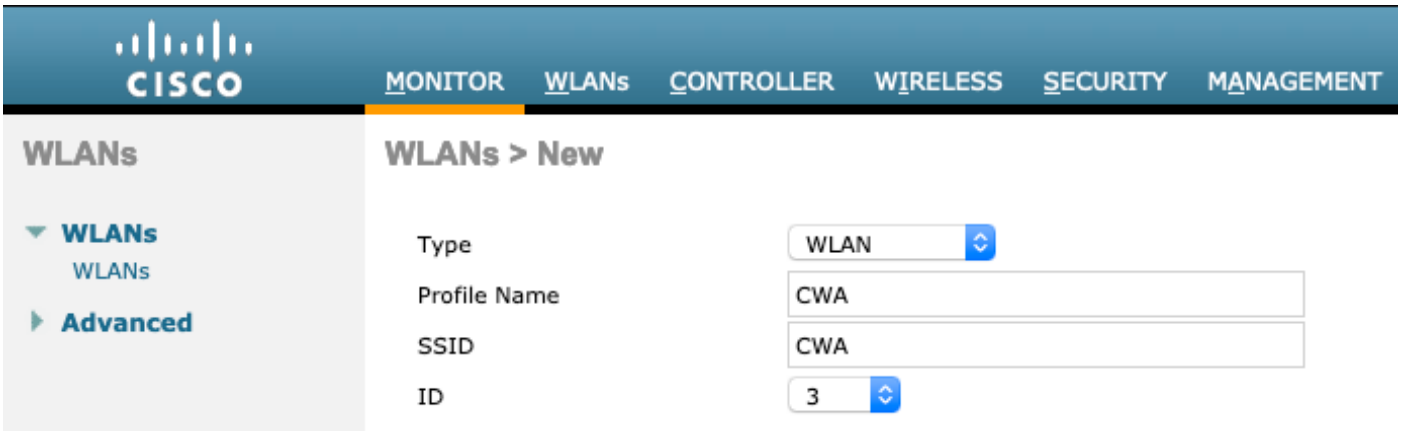
Configuration WLC

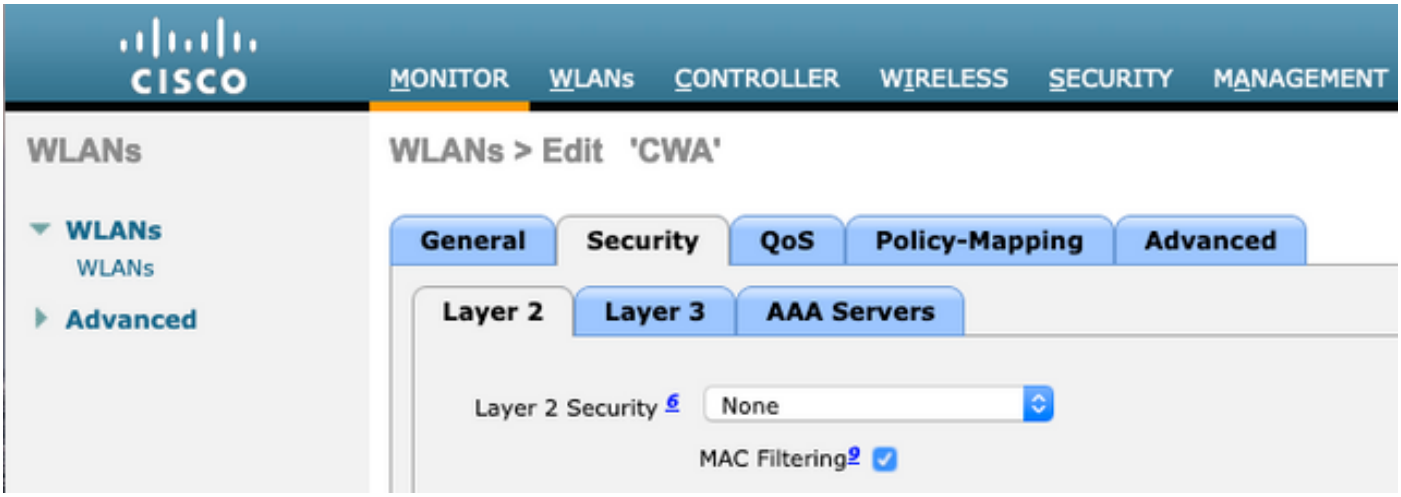
La configuration du WLC est assez simple. Une **astuce** est utilisée (comme sur les commutateurs) afin d'obtenir l'URL d'authentification dynamique de l'ISE (puisqu'il utilise la modification d'autorisation (CoA), une session doit être créée et l'ID de session fait partie de l'URL). Le SSID est configuré afin d'utiliser le filtrage MAC. L'ISE est configuré afin de renvoyer un access-accept même si l'adresse MAC est introuvable afin d'envoyer l'URL de redirection pour tous les utilisateurs.

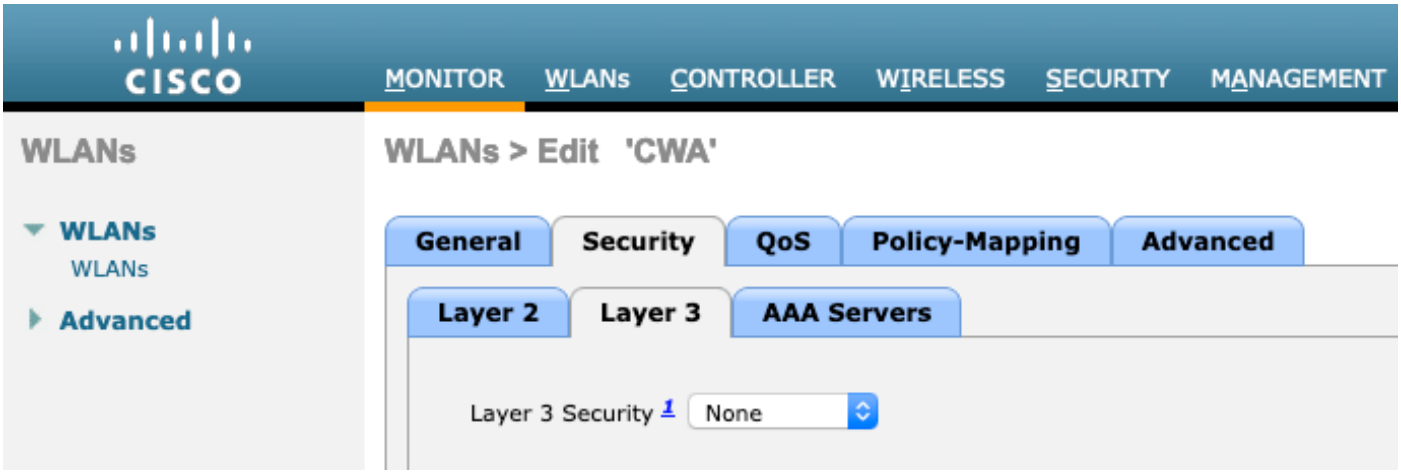
En outre, la substitution NAC (Network Admission Control) et AAA (Authentication, Authorization and Accounting) ISE doit être activée. Le NAC ISE permet à l'ISE d'envoyer une requête CoA qui indique que l'utilisateur est maintenant authentifié et qu'il peut accéder au réseau. Il est également utilisé pour l'évaluation de la posture, auquel cas l'ISE modifie le profil utilisateur en fonction du résultat de la posture.

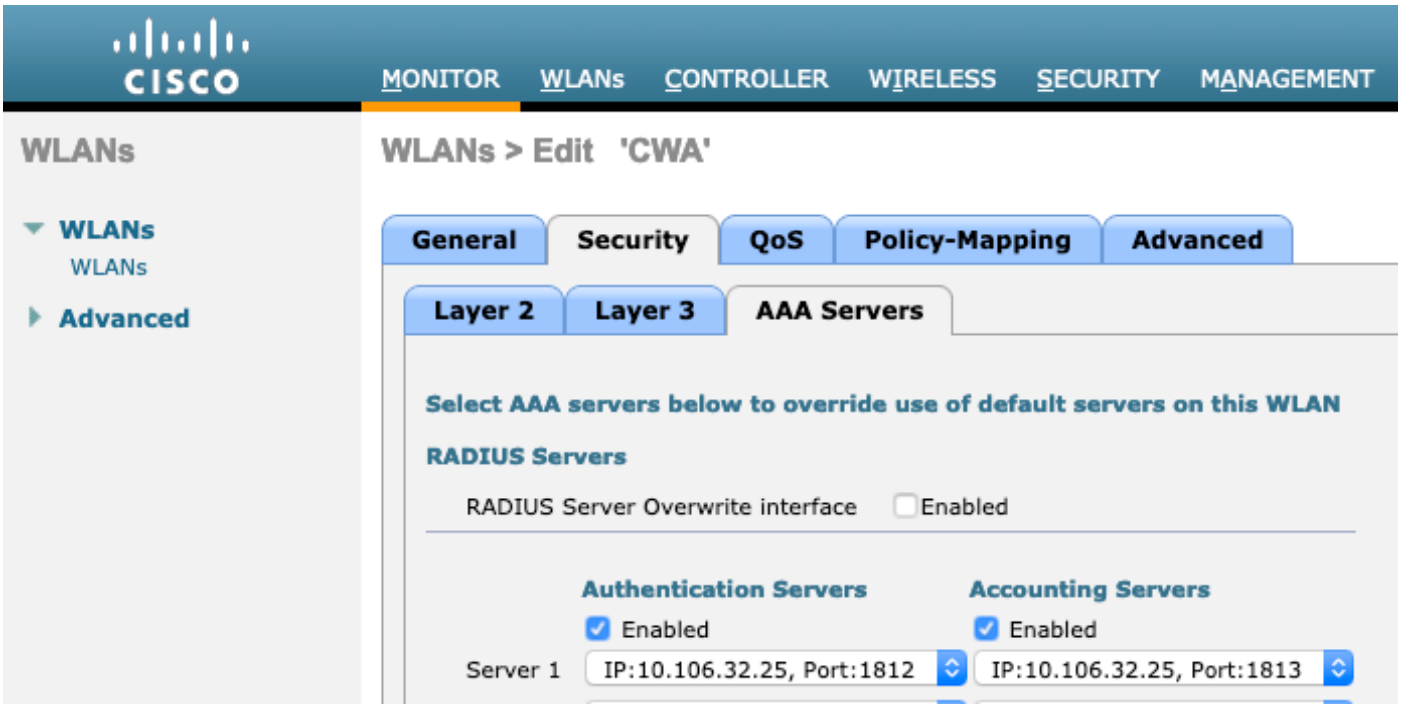
Assurez-vous que le serveur RADIUS a **pris en charge CoA** activé, qui est par défaut activé.

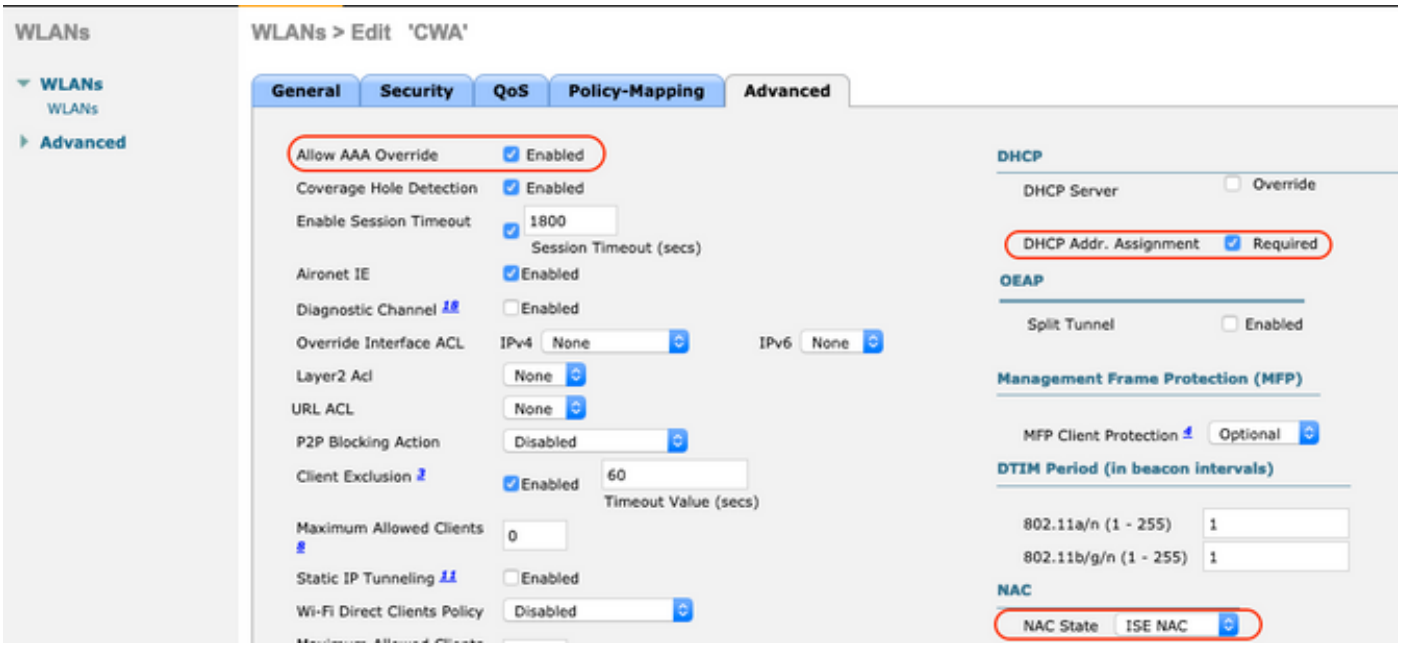

MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK
Security
RADIUS Authentication Servers > Edit
AAA
General
RADIUS
Authentication
Accounting
Fallback
DNS
Downloaded AVP
TACACS+
LDAP
Local Net Users
MAC Filtering
Disabled Clients
User Login Policies
AP Policies
Password Policies
Local EAP
Advanced EAP
Priority Order
Certificate
Access Control Lists
Server Index 2
Server Address(Ipv4/Ipv6) 10.106.32.25
Shared Secret Format ASCII
Shared Secret
Confirm Shared Secret
Key Wrap (Designed for FIPS customers and requires a key wrap compliant RADIUS server)
Port Number 1812
Server Status Enabled
Support for CoA Enabled
Server Timeout 2 seconds
Network User Enable
Management Enable
Management Retransmit Timeout 2 seconds
Tunnel Proxy Enable
Realm List
IPSec Enable


MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT
WLANs
WLANs > New
WLANs
WLANs
Advanced
Type WLAN
Profile Name CWA
SSID CWA
ID 3


MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT
WLANs
WLANs > Edit 'CWA'
WLANs
WLANs
Advanced
General
Security
QoS
Policy-Mapping
Advanced
Layer 2
Layer 3
AAA Servers
Layer 2 Security 6 None
MAC Filtering 9



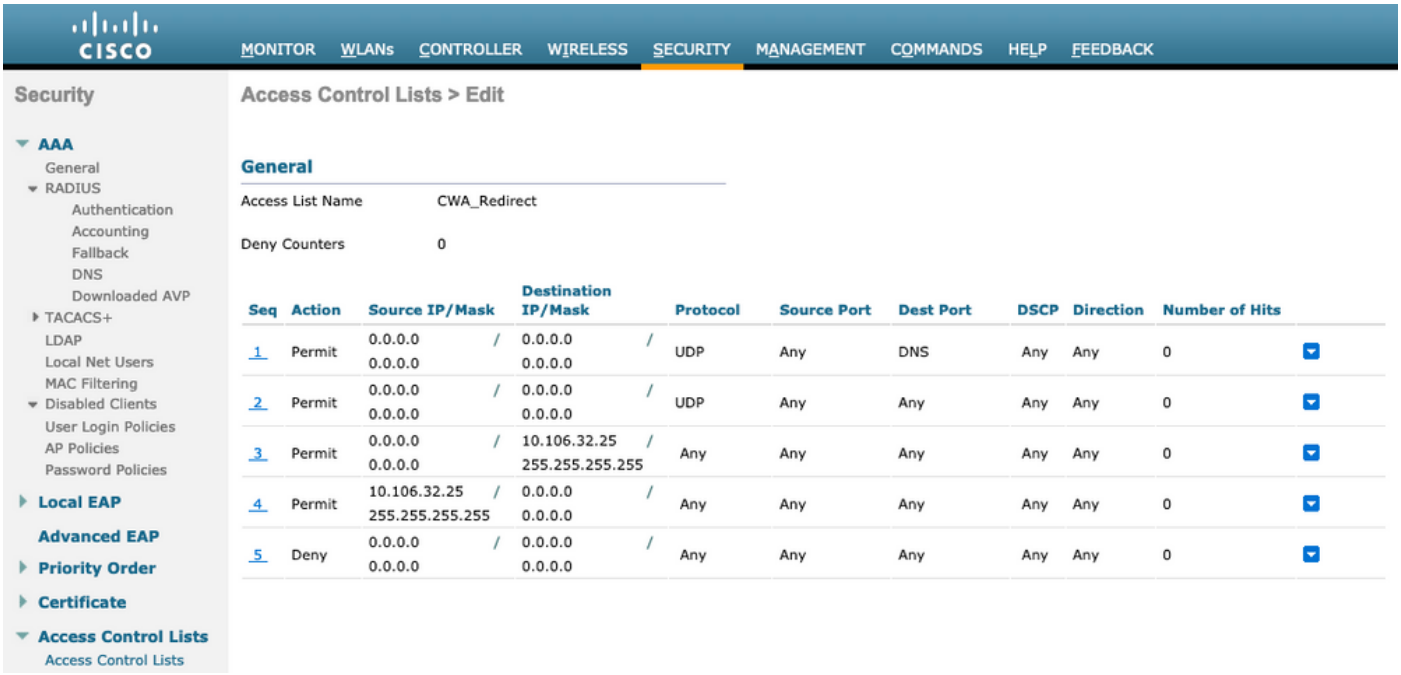




La dernière étape consiste à créer une liste de contrôle d'accès de redirection. Cette liste de contrôle d'accès est référencée dans l'acceptation d'accès de l'ISE et définit le trafic qui doit être redirigé (refusé par la liste de contrôle d'accès) et le trafic qui ne doit pas être redirigé (autorisé par la liste de contrôle d'accès). Ici, vous empêchez simplement le trafic de redirection vers l'ISE.

Vous pouvez être plus spécifique et empêcher uniquement le trafic en provenance/à destination de l'ISE sur le port 8443 (portail invité), mais toujours rediriger si un utilisateur tente d'accéder à l'ISE sur le port 80/443.

> **Note**: Les versions antérieures du logiciel WLC, telles que 7.2 ou 7.3, ne vous demandaient pas de spécifier DNS (Domain Name System), mais les versions ultérieures de code vous obligent à autoriser le trafic DNS sur cette liste de contrôle d'accès de redirection.



La configuration est maintenant terminée sur le WLC.

Configuration ISE

Créer le profil d'autorisation

Sur ISE, le profil d'autorisation doit être créé. Ensuite, les stratégies d'authentification et d'autorisation sont configurées. Le WLC doit déjà être configuré en tant que périphérique réseau.

Dans le profil d'autorisation, saisissez le nom de la liste de contrôle d'accès créée précédemment sur le WLC.

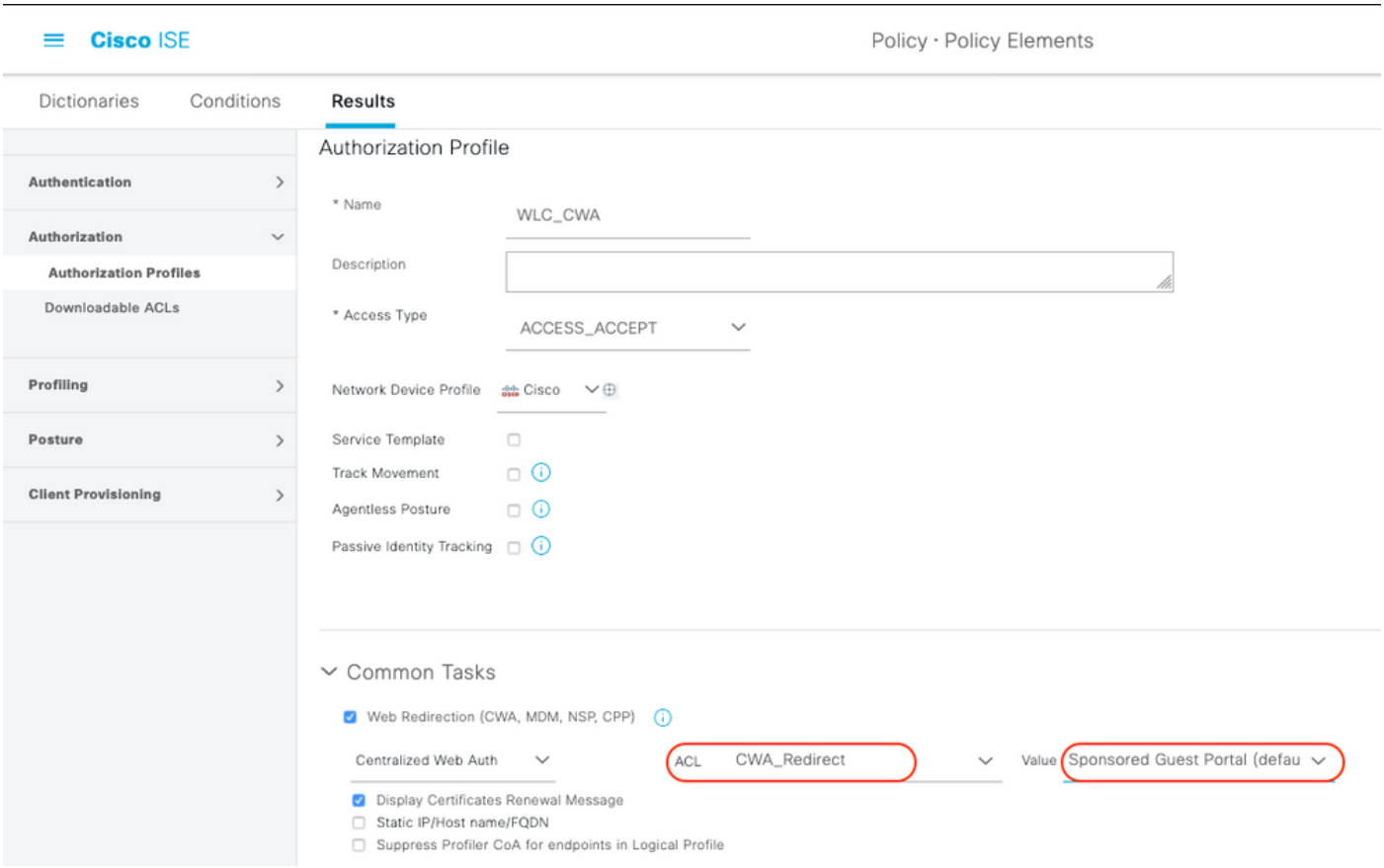
1. Cliquez sur **Stratégie**, puis sur **Eléments de stratégie**.
2. Cliquez sur **Résultats**.
3. Développez **Autorisation**, puis cliquez sur **Profil d'autorisation**.
4. Cliquez sur le bouton **Ajouter** afin de créer un nouveau profil d'autorisation pour le webauth central.
5. Dans le champ **Nom**, saisissez un nom pour le profil. Cet exemple utilise **WLC_CWA**.

6. Choisissez **ACCESS_ACCEPT** dans la liste déroulante Type d'accès.

7. Cochez la case **Redirection Web**, puis sélectionnez **Authentification Web centralisée** dans la liste déroulante.

8. Dans le champ ACL, saisissez le nom de la liste de contrôle d'accès sur le commutateur qui définit le trafic à rediriger. Cet exemple utilise **CWA_Redirect**.

9. Dans le champ Valeur, vous pouvez choisir **Sponsored Guest Portal** ou **Self-Registered Guest Portal** dans la liste déroulante. Dans le portail invité sponsorisé, les sponsors créent des comptes invités et les invités accèdent au réseau à l'aide de leur nom d'utilisateur et de leur mot de passe assignés alors qu'ils se trouvent dans le portail invité auto-inscription, les invités sont autorisés à créer leurs propres comptes et à accéder au réseau à l'aide de leur nom d'utilisateur et de leur mot de passe assignés. Cet exemple utilise **Sponsored Guest Portal.**



Créer une règle d'authentification

Assurez-vous que l'ISE accepte toutes les authentifications MAC du WLC et assurez-vous qu'il poursuivra l'authentification même si l'utilisateur est introuvable.

Sous **Stratégie > Jeux de stratégies > Jeu de stratégies par défaut**, cliquez sur **Authentification**.

L'image suivante montre un exemple de configuration de la règle de stratégie d'authentification. Dans cet exemple, une règle est configurée qui se déclenche lorsque MAB est détecté.

1. Entrez un nom pour votre règle d'authentification. Cet exemple utilise **MAB**, qui existe déjà par défaut sur ISE.

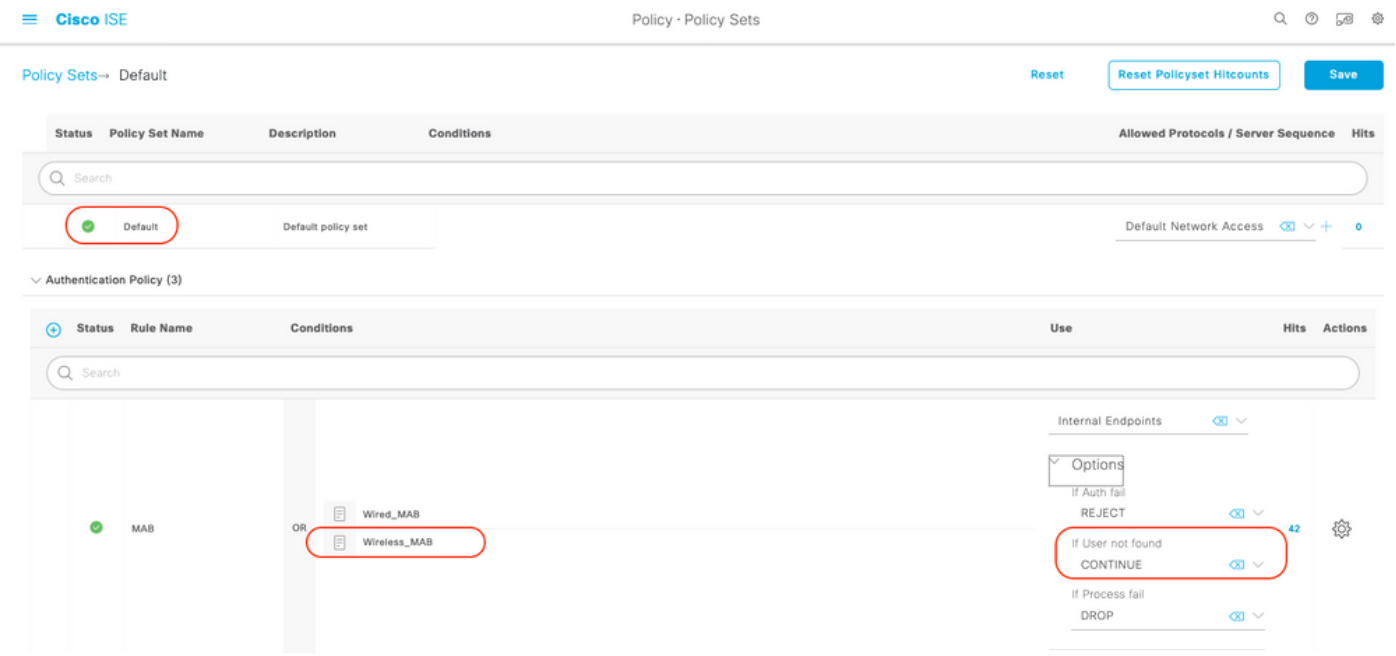
2. Sélectionnez l'icône plus (+) dans le champ de condition.

3. Àpartir de **Conditions Studio,** faites glisser **Wireless_MAB** dans la fenêtre de l'éditeur et **enregistrez**

4. Utiliser **des terminaux internes**.

5. Cliquez sur Options et choisissez **Continuer** dans la liste déroulante Si l'utilisateur est introuvable

   Note: La règle d'authentification MAB est déjà créée par défaut sur ISE.



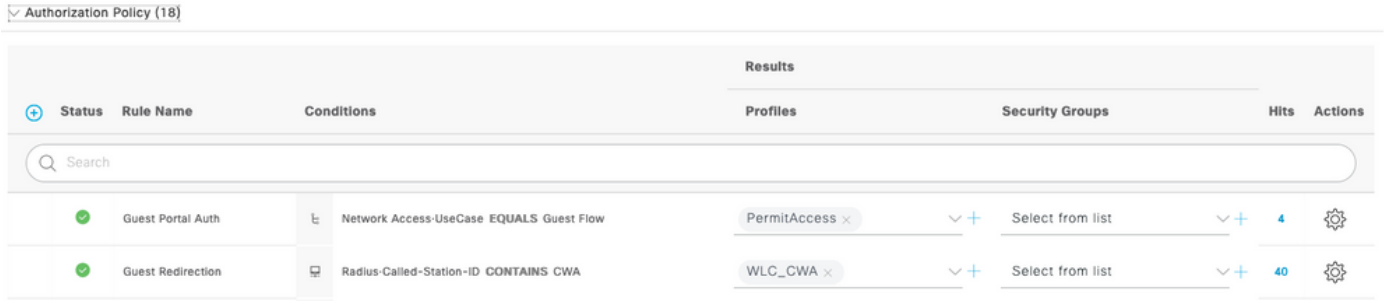
Créer une stratégie d'autorisation

Configurez la stratégie d'autorisation. Il est important de comprendre qu'il existe deux authentifications/autorisations :

- La première est lorsque l'utilisateur s'associe au SSID (« CWA » dans ce cas) et que le profil CWA est renvoyé.
  Dans cet exemple, **Airespace-Wlan-Id est utilisé comme condition.** Lorsqu'un client se connecte au SSID, la demande d'accès RADIUS à ISE contient l'attribut Airespace-WLAN-ID. Cet attribut est utilisé pour prendre des décisions de stratégie dans ISE. Ainsi, lorsqu'un client inconnu se connecte à SSID CWA, ISE envoie un access-accept avec l'URL de redirection (portail Web) et la liste de contrôle d'accès. L'utilisation de la règle Airespace-Wlan-Id garantit que la page du portail est présentée aux utilisateurs qui se connectent uniquement au SSID CWA.

- La seconde est lorsque l'utilisateur s'authentifie sur le portail Web. Celle-ci correspond à la règle par défaut (utilisateurs internes) de cette configuration (elle peut être configurée pour répondre à vos besoins). Il est important que la partie autorisation ne corresponde plus au profil CWA. Sinon, il y aura une boucle de redirection. L'attribut **Network Access : UseCase**

Equals Guest Flow peut être utilisé afin de correspondre à cette deuxième authentification. Voici le résultat :



Complétez ces étapes afin de créer les règles d'autorisation comme indiqué dans les images précédentes :

1. Créez une nouvelle règle et entrez un nom. Cet exemple utilise la **redirection invité**.

2. Cliquez sur l'icône représentant un crayon dans le champ de condition, puis créez une nouvelle condition.

3. Sous **Éditeur**, cliquez sur pour ajouter un attribut.

4. Choisissez **Radius** et développez-le.

5. Cliquez sur **Radius · Called-Station-ID**, puis sélectionnez l'opérateur **CONTAINS**.

6. Entrez le **CWA** dans le champ de droite, dans cet exemple 1.

7. Sur la page General Authorization, sélectionnez **WLC_CWA** (Authorization Profile) sous **Results.**

   Cette étape permet à ISE de continuer même si l'utilisateur (ou l'adresse MAC) n'est pas connu lorsqu'il est connecté au SSID **CWA** et de le présenter avec le portail de connexion.

8. Cliquez sur le bouton **Actions** situé à la fin de la règle **Redirection invité**, puis choisissez d'insérer une nouvelle règle au-dessus de celle-ci.

   Note: Il est très important que cette nouvelle règle soit antérieure à la règle **Guest Redirection**.

9. Entrez un nom pour la nouvelle règle. Cet exemple utilise l'**authentification du portail invité**.

10. Dans le champ Condition, cliquez sur l'icône représentant un crayon, puis choisissez de créer une nouvelle condition.

11. Choisissez **Accès réseau**, puis cliquez sur **UseCase**.

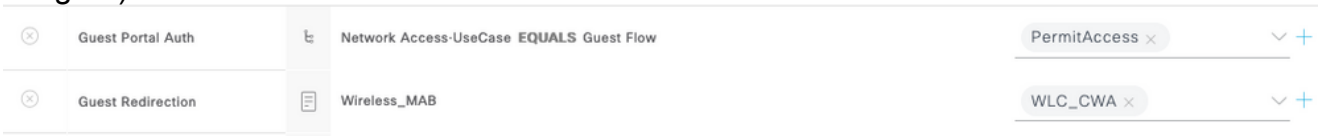
12. Choisissez **Equals** comme opérateur.

13. Choisissez **GuestFlow** comme opérande de droite.

14. Sur la page d'autorisation, cliquez sur l'option de la liste déroulante Résultats

    Vous pouvez choisir une option de profil d'autorisation **PermitAccess** par défaut ou créer un profil personnalisé afin de renvoyer le ou les VLAN que vous souhaitez. Notez qu'en plus de **If GuestFlow**, vous pouvez ajouter d'autres conditions afin de retourner divers profils d'authentification basés sur le groupe d'utilisateurs. Comme indiqué à l'étape 7, cette règle **Guest Portal Auth** correspond à la deuxième authentification d'adresse MAC initiée après la connexion réussie du portail et après l'envoi par ISE d'une CoA afin de réauthentifier le client. La différence avec cette deuxième authentification est que, au lieu de venir à ISE avec simplement son adresse MAC, ISE se souvient du nom d'utilisateur donné dans le portail. Vous pouvez faire en sorte que cette règle d'autorisation tienne compte des informations d'identification entrées quelques millisecondes auparavant dans le portail invité.

Note: Dans un environnement multicontrôleur, l'ID de réseau local sans fil doit être identique sur tous les WLC. Si vous ne voulez pas utiliser l'attribut Airespace-Wlan-Id comme condition, il est préférable de faire correspondre les requêtes Wireless_MAB (condition intégrée).



Activer le renouvellement IP (facultatif - non recommandé)

Si vous affectez un VLAN, la dernière étape consiste pour le PC client à renouveler son adresse IP. Cette étape est réalisée par le portail invité pour les clients Windows. Si vous n'avez pas défini de VLAN pour la **2e** règle **AUTH** précédemment, vous pouvez ignorer cette étape. Il ne s'agit pas d'une conception recommandée car le fait de modifier le VLAN client après qu'il ait déjà une adresse IP perturbera la connectivité, certains clients pourraient y réagir à tort et nécessite des privilèges Windows élevés pour fonctionner correctement.

Si vous avez attribué un VLAN, procédez comme suit afin d'activer le renouvellement IP :

1. Cliquez sur **Centres de travail > Accès invité**, puis sur **Portails et composants.**

2. Cliquez sur **Portails invités**.

3. Cliquez sur **Sponsored Guest Portal** (utilisé dans cet exemple), puis développez **VLAN DHCP Release Page Settings**.

4. Cochez la case **VLAN DHCP Release**.

   Note: La prise en charge de la version DHCP du VLAN est disponible uniquement pour les périphériques Windows. Il n'est pas disponible pour les appareils mobiles. Si le périphérique enregistré est mobile et que l'option de libération DHCP VLAN est activée, l'invité est invité à renouveler manuellement son adresse IP. Pour les utilisateurs de périphériques mobiles, nous vous recommandons d'utiliser des listes de contrôle d'accès (ACL) sur le WLC, plutôt

que d'utiliser des VLAN.

Scénario Anchor-Foreign

Cette configuration peut également fonctionner avec la fonction d'ancrage automatique des WLC. Le seul hic est que puisque cette méthode d'authentification Web est la couche 2, vous devez être conscient que ce sera le WLC étranger qui fait tout le fonctionnement de RADIUS. Seul le WLC étranger contacte l'ISE, et la liste de contrôle d'accès de redirection doit être également présente sur le WLC étranger. Le nom de la liste de contrôle d'accès doit exister au niveau de l'étranger (n'a pas besoin d'entrées de liste de contrôle d'accès). Le WLC étranger enverra le nom de la liste de contrôle d'accès à l'ancrage et il sera l'ancrage qui appliquera la redirection (et aura donc besoin du contenu ALC approprié).

Comme dans d'autres scénarios, le WLC étranger montre rapidement que le client est dans l'état **RUN**, ce qui n'est pas entièrement vrai. Cela signifie simplement que le trafic est envoyé à l'ancre à partir de là. L'état réel du client peut être vu sur l'ancre où il doit afficher **CENTRAL_WEBAUTH_REQD**.

Voici le flux dans une configuration **ancre-étranger** :

1. Le client se connecte au SSID sur le WLC étranger. Le WLC étranger contacte le serveur ISE pour MAB. ISE envoie access-accept avec l'URL de redirection et redirige l'ACL vers l'étranger.
2. Maintenant, le client est ancré au WLC d'ancrage où il obtient une adresse IP et est placé dans CENTRAL_WEBAUTH_REQD.
3. Lorsque le client tente d'accéder à un site Web, le WLC d'ancrage redirige le client vers la page du portail ISE. La page de connexion s'affiche pour le client.
4. Après une connexion réussie, ISE envoie une CoA au WLC étranger.
5. Le WLC étranger contacte le WLC d'ancrage pour lui indiquer de mettre le client dans l'état EXÉCUTÉ.
6. Tout le trafic client est transféré de l'étranger à l'ancre et sort du WLC d'ancrage.

Les ports de pare-feu requis pour permettre la communication entre le WLC et ISE sont les suivants :

- UDP : 1645, 1812 (authentification RADIUS)
- UDP : 1646, 1813 (comptabilité RADIUS)
- UDP : 1700 (RADIUS CoA)
- TCP : 8443 Guest Portal ou 8905 si vous avez Posturing.

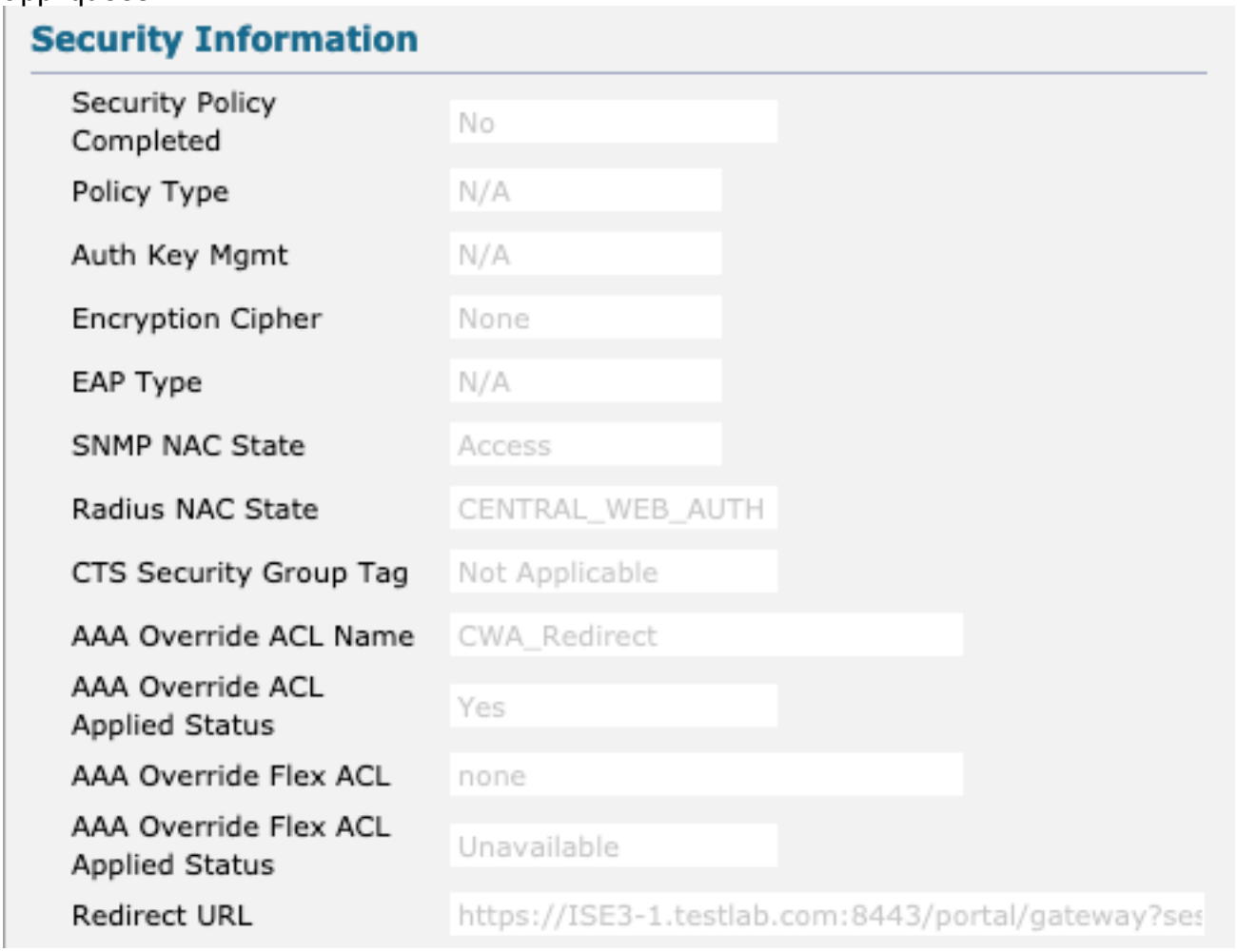
Note: La configuration d'ancrage étranger avec l'authentification Web centrale (CWA) ne fonctionne que dans les versions 7.3 ou ultérieures.

Note: En raison de l'ID de bogue Cisco CSCul83594, vous ne pouvez pas exécuter la comptabilité à la fois sur ancor et à l'étranger, car cela rend le profilage inexact en raison d'un manque potentiel de liaison IP/MAC. Il crée également de nombreux problèmes avec l'ID de session pour les portails invités. Si vous souhaitez configurer la comptabilité, configurez-la sur le contrôleur étranger. Notez que ce ne devrait plus être le cas pour le démarrage du logiciel WLC 8.6 où l'ID de session sera partagé entre l'ancre et les contrôleurs étrangers et la comptabilité sera alors possible d'activer sur les deux.

Vérification

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

1. Une fois que l'utilisateur est associé au SSID, le WLC contacte l'ISE (lorsque le filtrage MAC est configuré). ISE a été configuré pour renvoyer l'accès accepté avec l'URL de redirection et la liste de contrôle d'accès. Il s'agit de la première authentification. Les détails du client dans le WLC montrent que l'URL de redirection et la liste de contrôle d'accès sont appliquées.

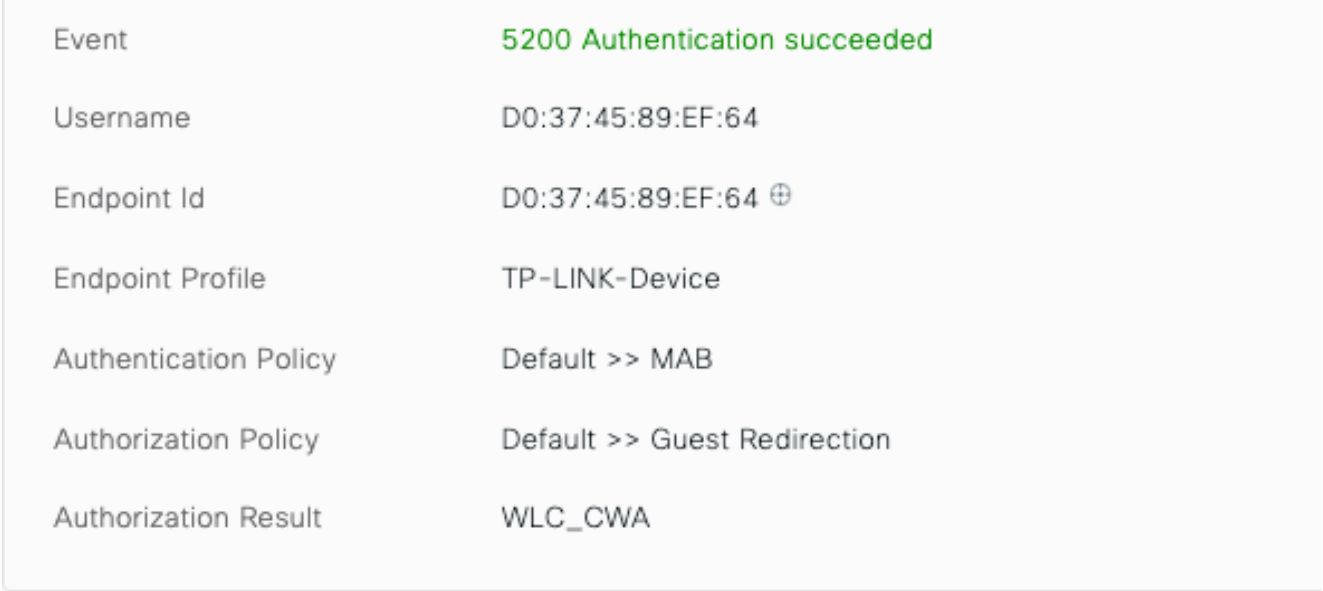


Dans le client WLC et AAA all debug, vous pouvez voir l'accès accepté avec l'URL de redirection et l'ACL envoyées à partir de l'ISE.

```
*radiusTransportThread: d0:37:45:89:ef:64 Access-Accept received from RADIUS server
10.106.32.25 (qid:4) with port:1812, pktId:24 for mobile d0:37:45:89:ef:64 receiveId = 0
*radiusTransportThread: AuthorizationResponse: 0x166ab570


*radiusTransportThread: structureSize.............................425

*radiusTransportThread: resultCode.................................0

*radiusTransportThread: protocolUsed...............................0x00000001

*radiusTransportThread: proxyState.................................D0:37:45:89:EF:64-
00:00

*radiusTransportThread: Packet contains 4 AVPs:

*radiusTransportThread: AVP[01] User-Name.............................D0-37-45-89-EF-64
```

```
(17 bytes)

*radiusTransportThread: AVP[02]
Class.................................CACS:0a6a207a0000000a5fe8f217:ISE3-1/397801666/90
(49 bytes)

*radiusTransportThread: AVP[03] Cisco / Url-Redirect-Acl.................CWA_Redirect (12
bytes)

*radiusTransportThread: AVP[04] Cisco / Url-Redirect.....................DATA (175 bytes)

*radiusTransportThread: d0:37:45:89:ef:64 processing avps[0]: attribute 1
*radiusTransportThread: d0:37:45:89:ef:64 username = D0-37-45-89-EF-64

!
*apfReceiveTask: d0:37:45:89:ef:64 Redirect URL received for client from RADIUS. Client
will be moved to WebAuth_Reqd state to facilitate redirection. Skip web-auth Flag = 0
```

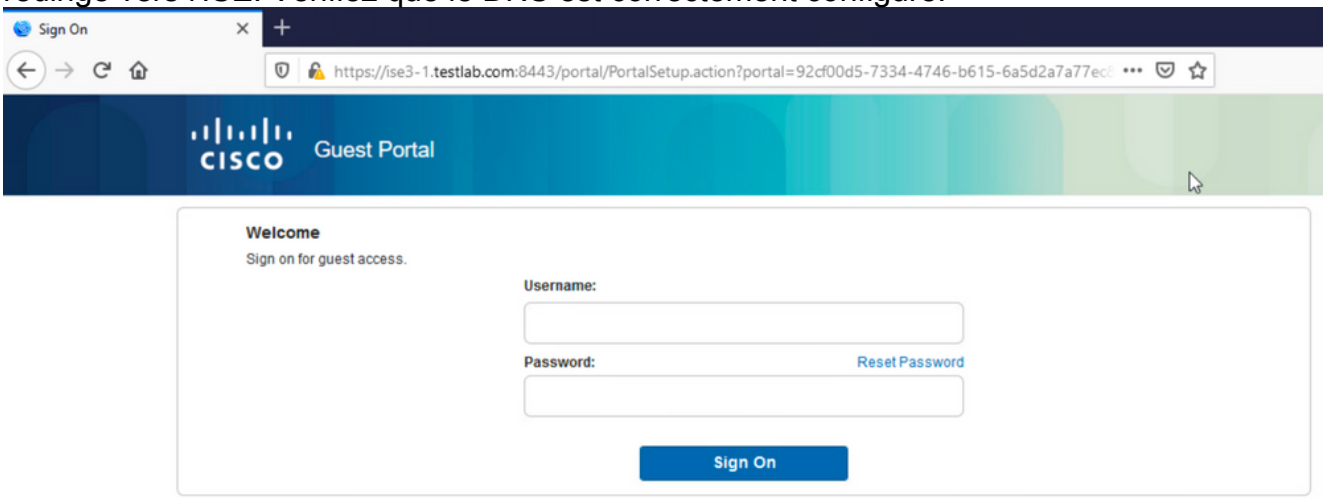
La même chose peut également être vérifiée dans ISE. Accédez à **Opérations > Livelogs Radius**. Cliquez sur le détail de cette adresse MAC.Vous pouvez voir que pour la première authentification (filtrage MAC), ISE renvoie le profil AuthZ **WLC_CWA** lorsqu'il atteint la règle d'authentification **MAB** et la stratégie d'authentification **Redirection invité**.



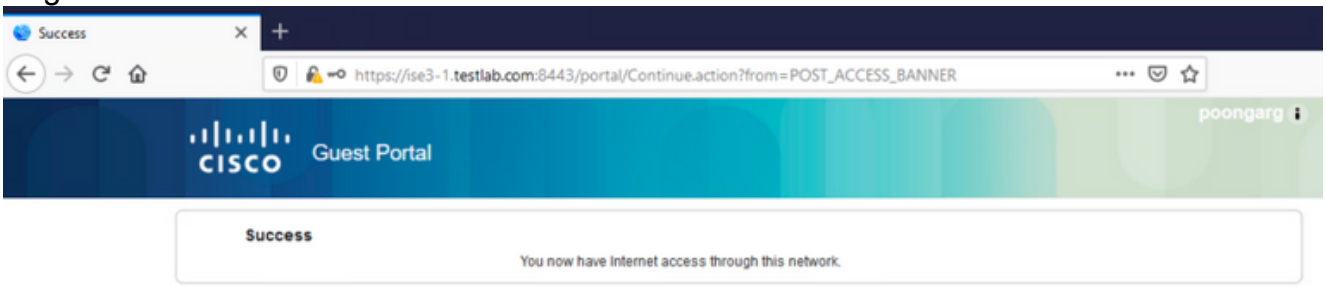
Result

UserName	D0:37:45:89:EF:64
User-Name	D0-37-45-89-EF-64
Class	CACS:0a6a207a0000000a5fe8f217:ISE3-1/397801666/92
cisco-av-pair	url-redirect-acl=CWA_Redirect
cisco-av-pair	url-redirect=https://ISE3-1.testlab.com:8443/portal /gateway?sessionId=0a6a207a0000000a5fe8f217& portal=92cf00d5-7334-4746-b615-6a5d2a7a77ec& action=cwa&token=6dae36954f937ed307a42c8562f3413a
cisco-av-pair	profile-name=TP-LINK-Device
DoNotSuppress	true
LicenseTypes	Essential license consumed.

2. Àce stade, le client obtient une adresse IP. Le client est maintenant dans l'état **CENTRAL_WEB_AUTH**. Lorsqu'une adresse est ouverte sur le client, le navigateur est redirigé vers l'ISE. Vérifiez que le DNS est correctement configuré.

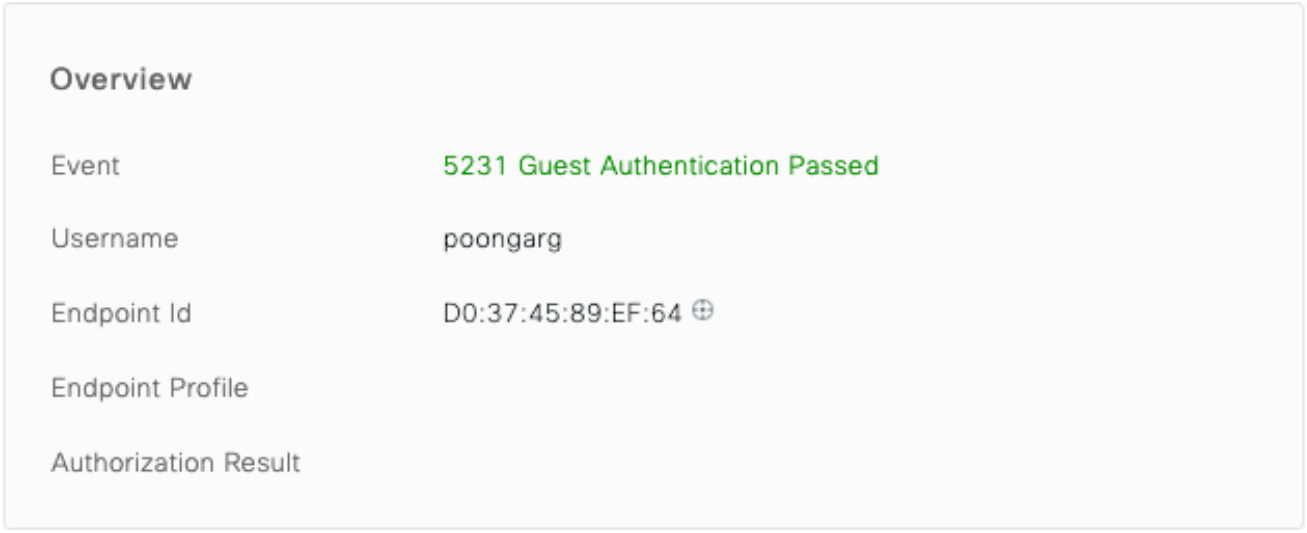


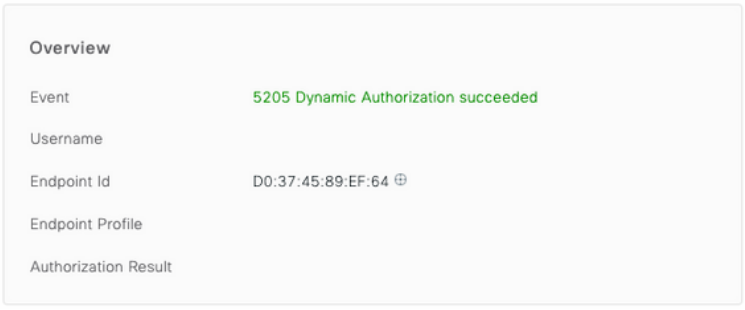
3. Une fois les informations d'identification correctes entrées, l'accès au réseau est accordé. Il s'agit de la deuxième authentification.

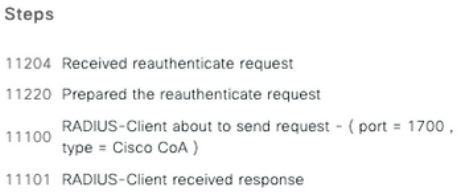


Dec 27, 2020 09:55:46.58...		poongarg	D0:37:45:89:EF:64	Default	Default >> Guest Portal Auth	PermitAccess		Authorize-Only succeeded
Dec 27, 2020 09:55:46.56...			D0:37:45:89:EF:64					Dynamic Authorization succeeded
Dec 27, 2020 09:55:42.60...		poongarg	D0:37:45:89:EF:64				10.106.32.254	Guest Authentication Passed
Dec 27, 2020 09:54:55.55...		D0:37:4...	D0:37:45:89:EF:64	Default >> MAB	Default >> Guest Redirection	WLC_CWA		Authentication succeeded

Lorsque les informations d'identification sont entrées, ISE authentifie le client et envoie la CoA.



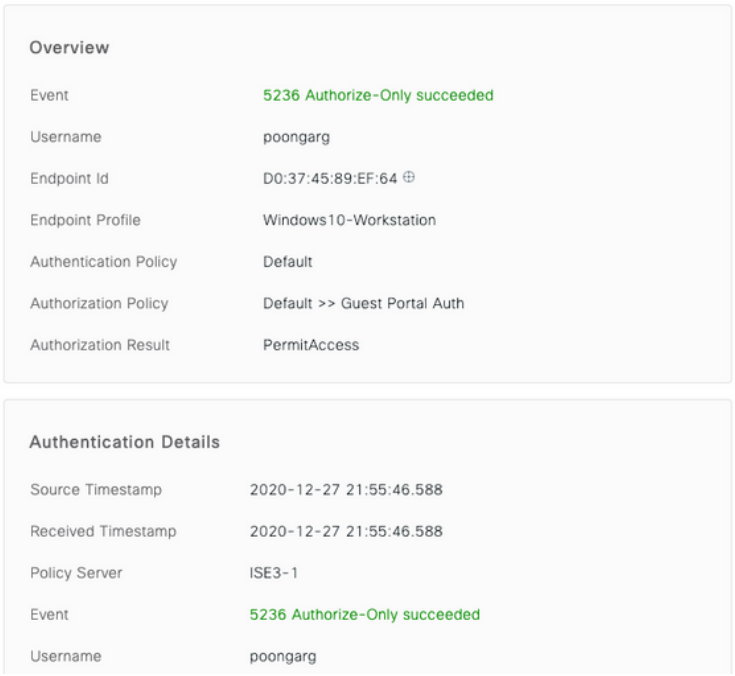




Sur le WLC, ceci peut être vu dans AAA tous les débogages.

```
*radiusCoASupportTransportThread: audit session ID recieved in CoA =
0a6a207a0000000b5fe90410
*radiusCoASupportTransportThread: Received a 'CoA-Request' from 10.106.32.25 port 23974

*radiusCoASupportTransportThread: CoA - Received IP Address : 10.106.32.122, Vlan ID:
(received 0)
*radiusCoASupportTransportThread: d0:37:45:89:ef:64 Calling-Station-Id --->
d0:37:45:89:ef:64
*radiusCoASupportTransportThread: Handling a valid 'CoA-Request' regarding station
d0:37:45:89:ef:64
*radiusCoASupportTransportThread: Sending Radius CoA Response packet on srcPort: 1700,
dpPort: 2, tx Port: 23974
*radiusCoASupportTransportThread: Sent a 'CoA-Ack' to 10.106.32.25 (port:23974)
```

Après cela, le client est réauthentifié et l'accès au réseau lui est accordé.



4. Sur le contrôleur, l'état Policy Manager et l'état RADIUS NAC passent de **CENTRAL_WEB_AUTH** à **RUN**. **Note**: Dans la version 7.2 ou antérieure, l'état **CENTRAL_WEB_AUTH** était appelé **POSTURE_REQD.**

Notez que le type de CoA retourné par ISE a évolué d'une version à l'autre. ISE 3.0 demandera au WLC de commencer la réauthentification en utilisant la dernière méthode, à savoir MAB dans ce cas. Le WLC réauthentifie l'utilisateur lorsqu'il envoie la requête d'accès RADIUS avec l'attribut Authorize-Only.

Exemple de requête CoA ISE 3.0 :

```
▼ AVP: t=Vendor-Specific(26) l=41 vnd=ciscoSystems(9)
    Type: 26
    Length: 41
    Vendor ID: ciscoSystems (9)
  ▼ VSA: t=Cisco-AVPair(1) l=35 val=subscriber:command=reauthenticate
      Type: 1
      Length: 35
      Cisco-AVPair: subscriber:command=reauthenticate
▼ AVP: t=Vendor-Specific(26) l=43 vnd=ciscoSystems(9)
    Type: 26
    Length: 43
    Vendor ID: ciscoSystems (9)
  ▼ VSA: t=Cisco-AVPair(1) l=37 val=subscriber:reauthenticate-type=last
      Type: 1
      Length: 37
      Cisco-AVPair: subscriber:reauthenticate-type=last
```

Le WLC n'enverra alors pas de trame de dissociation au client et réexécutera une authentification RADIUS et appliquera le nouveau résultat de manière transparente au client. Depuis la version 8.3, le WLC prend en charge la définition d'une clé pré-partagée WPA sur un SSID CWA. L'expérience utilisateur reste la même que dans les scénarios non PSK classiques, le WLC n'enverra pas de trame dissociée au client et appliquera simplement le nouveau résultat d'autorisation. Cependant, une « réponse d'association » est toujours envoyée au client bien qu'aucune « demande d'association » n'ait jamais été reçue du client, ce qui peut sembler curieux lors de l'analyse des traces de renifleur.

Dépannage

Complétez ces étapes afin de dépanner ou d'isoler un problème CWA :

1. Entrez la commande **debug client <mac address of client>** sur le contrôleur et le moniteur afin de déterminer si le client atteint l'état **CENTRAL_WEBAUTH_REQD**. Un problème courant est observé lorsque l'ISE retourne une liste de contrôle d'accès de redirection qui n'existe pas (ou n'est pas correctement saisie) sur le WLC. Si c'est le cas, le client est déauthentifié une fois que l'état **CENTRAL_WEBAUTH_REQD** est atteint, ce qui entraîne le redémarrage du processus.

2. Si l'état client correct est atteint, naviguez jusqu'à **monitor > clients** sur l'interface utilisateur graphique Web du WLC et vérifiez que la liste de contrôle d'accès et l'URL de redirection correctes sont appliquées au client.

3. Vérifiez que le DNS correct est utilisé. Le client doit être en mesure de résoudre les sites Web Internet et le nom d'hôte ISE. Vous pouvez le vérifier via nslookup.

4. Vérifiez que toutes les étapes d'authentification se produisent sur ISE :

   L'authentification MAC doit avoir lieu en premier, auquel les attributs CWA sont renvoyés.

   L'authentification de connexion au portail se produit.

   L'autorisation dynamique se produit.

   L'authentification finale est une authentification MAC qui affiche le nom d'utilisateur du portail sur l'ISE, auquel les résultats d'autorisation finale sont renvoyés (par exemple le VLAN final et la liste de contrôle d'accès).

Considérations spéciales pour les scénarios d'ancrage

Considérez ces ID de bogue Cisco qui limitent l'efficacité du processus CWA dans un scénario de mobilité (en particulier lorsque la comptabilité est configurée) :

- CSCuo56780 - *Vulnérabilité de refus de service RADIUS ISE*

- CSCul83594 - *L'ID de session n'est pas synchronisé sur la mobilité, si le réseau est ouvert*