# Exemple de configuration de point névralgique de version 1.3 ISE

## Contenu



## Introduction

La version 1.3 du Logiciel Cisco Identity Services Engine (ISE) a un nouveau type d'invité Hotspot appelé par portail. Ce type de portail te permet pour permettre d'accéder l'accès invité au réseau et ne force pas l'utilisateur pour ne fournir aucune qualification. Ce document décrit comment configurer et dépanner cette fonctionnalité.

## Conditions préalables

### Conditions requises

Cisco recommande que vous ayez l'expérience avec la configuration ISE et la connaissance de base de ces thèmes :

- Déploiements ISE et écoulements d'invité
- Configuration des contrôleurs LAN Sans fil (WLCs)

### Composants utilisés

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

- Microsoft Windows 7
- Version 7.6 et ultérieures de Cisco WLC
- Logiciel ISE, version 1.3 et ultérieures

# Topologie et écoulement

Ce scénario est pour les utilisateurs d'invité qui reçoivent la Politique d'Utilisation Acceptable (AUP) et seulement puis soit donné l'accès à Internet (ou tout autre accès limité).

**Étape 1.** Associés d'utilisateur d'invité à l'Identifiant SSID (Service Set Identifier) : Point névralgique. C'est un réseau ouvert avec le filtrage MAC avec ISE pour l'authentification. Cette authentification apparie la deuxième règle d'autorisation sur l'ISE et le point névralgique de redirect to de profil d'autorisation. ISE renvoie un RAYON Access-reçoit avec deux Cisco-poids du commerce-paires :

- URL-réorienter-acl (que le trafic devrait être réorienté, et le nom de la liste de contrôle d'accès (ACL) défini localement sur le WLC)
- URL-réorientez (où réorienter ce trafic à ISE)

**Étape 2.** Un utilisateur d'invité est réorienté à l'ISE, reçoit l'AUP, et fournit sur option un code d'accès secret.

**Étape 3.** ISE envoie une modification de RAYON d'Admin-remise de l'autorisation (CoA) au WLC. Le WLC authentifie à nouveau l'utilisateur quand il envoie l'Access-demande de RAYON. ISE répond avec l'ACL du l'Access-recevoir et d'Airespace défini localement sur le WLC, qui fournit l'accès à Internet seulement.

> **Note**: L'Admin-remise CoA est spécifique pour la fonctionnalité de point névralgique et est décrite dans l'ID de bogue Cisco CSCus46754. Le comportement pour la version 1.2 ISE avec un portail d'invité était différent ; un CoA authentifient à nouveau ou Terminate a été envoyée.

**Étape 4.** Un utilisateur d'invité désire l'accès au réseau. L'administrateur réseau est certain que l'utilisateur ait reçu l'AUP. L'utilisateur d'invité peut être réorienté à l'URL d'original, à un URL statique-configuré, ou à une page de succès. Toutes les pages affichées par ISE peuvent être personnalisées.

L'intégration avec un contrôle facultatif de posture est présentée dans la dernière section.

# Configurez

## WLC

1. Ajoutez le nouveau serveur de RAYON pour l'authentification et la comptabilité. Naviguez vers la **Sécurité > l'AAA > Radius > Authentication** afin d'activer CoA de RAYON (RFC 3576).

Il y a une configuration semblable pour la comptabilité. On lui informe également configurer le WLC pour envoyer le SSID dans l'attribut d'ID de station appelée, qui permet à l'ISE pour configurer des règles flexibles basées sur le SSID :

2. Sous les WLAN tabulez, créez le point névralgique Sans fil du RÉSEAU LOCAL (WLAN) et configurez l'interface appropriée. Placez la Sécurité Layer2 à **aucun** avec le filtrage MAC. Dans des serveurs de Sécurité/Authentification, autorisation et comptabilité (AAA), sélectionnez l'adresse IP ISE pour l'authentification et la comptabilité (la comptabilité est facultative). Sur l'onglet Avancé, le **dépassement d'AAA d'**enable et a placé l'état de Contrôle d'admission au réseau (NAC) au RAYON NAC (support CoA).

3. Naviguez vers la **Sécurité > les listes de contrôle d'accès > les listes de contrôle d'accès** et créez deux Listes d'accès :

   HotspotRedirect, qui permet le trafic qui ne devrait pas être réorienté et réoriente tout autre traficInternet, qui est refusé pour des réseaux d'entreprise et permis pour tous les autres

   Voici un exemple d'ACL de HotspotRedirect (le besoin d'exclure le trafic à/de ISE de la redirection) :

## ISE

1. Naviguez vers l'**accès invité > configurent > des portails d'invité**, et créent un nouveau type portail, portail d'invité de point névralgique :

2. Choisissez le nom portail qui sera mis en référence dans le profil d'autorisation. Afin de personnaliser le portail des configurations portailes de comportement et d'écoulement, de l'AUP d'enable, et d'un code secret (facultatif) :

   Plusieurs plus d'options peuvent être activées sous la personnalisation de page du portail ; toutes les pages présentées peuvent être personnalisées.

3. Naviguez vers la **stratégie > les résultats > l'autorisation > le profil d'autorisation** afin de configurer des profils d'autorisation.

   Point névralgique (avec la redirection à nom portail et à ACL HotspotRedirect de point névralgique) :

Internet (avec l'Internet d'égaux d'ACL d'Airespace) :

4. Afin de vérifier les règles d'autorisation, naviguez vers la **stratégie > l'autorisation**. Dans la version 1.3 ISE par défaut pour l'accès défectueux de dérivation d'authentification MAC (MAB) (adresse MAC non trouvée), l'authentification est continuée (non rejeté). C'est très utile pour des portails d'invité parce qu'il n'y a aucun besoin de changer n'importe quoi dans les règles d'authentification par défaut.

   Pour la première authentification de MAB, la deuxième règle est appariée (le point final n'est pas encore dans tout groupe d'identité). Alors l'utilisateur est réorienté à un webportal (point névralgique), reçoit l'AUP, et tape sur option le code d'accès secret correct. ISE envoie un CoA de RAYON et le WLC exécute la ré-authentification. Pour la deuxième authentification, la première règle est appariée avec le profil PermitInternet d'autorisation et renvoie le nom d'ACL qui est appliqué sur le WLC (cette fois, le point final est déjà dans le groupe de GuestEndpoints).

   Par défaut, des invités qui reçoivent l'AUP sont mis dans le groupe d'identité de GuestEndpoints. Le groupe d'identité qui est assigné pour ces points finaux est configuré sous la configuration portaile d'invité, qui peut être différente pour chaque portail.

5. Ajoutez le WLC comme périphérique d'accès au réseau de la **gestion > des ressources de réseau > des périphériques de réseau**.

# Vérifiez

Utilisez cette section pour confirmer que votre configuration fonctionne correctement.

1. Après que les utilisateurs d'invité s'associent avec le point névralgique SSID et tapent un URL, ils sont réorientés à l'AUP :

2. Si le code d'accès était configuré sous le portail d'invité, alors on l'exige. Si l'utilisateur fournit un code incorrect, des affichages d'une erreur :

3. Voici l'écran qui affiche si le code correct est écrit :

4. Une fois que le code correct est écrit, le WLC exécute la ré-authentification et présente l'ACL

d'Internet relié à la session.

## Posture supplémentaire

S'il y a un besoin de permettre d'accéder aux utilisateurs d'invité, mais seulement quand ils satisfont une stratégie spécifique (posture) comme les mises à jour fraîches d'antivirus et les mises à jour de Microsoft Windows, alors elle peut être accomplie avec ces règles :

La règle de point névralgique ne fournira pas l'accès à Internet, mais exécute à la place la redirection à un service de posture. Alors l'agent de Web peut être poussé à la station (le ravitaillement de client ordonne) et exécuter des contrôles de stratégie (règles de posture). La conformité d'état est envoyée par l'agent de Web à ISE. Après que la station soit conforme, ISE envoie un autre CoA authentifie à nouveau, qui déclenche une mise à jour d'autorisation sur le WLC. Alors la règle de HotSpot_Compliant est produite et l'accès à Internet est fourni.

La configuration de posture avec le NAC ou l'agent de Web est très semblable comme dans la version 1.2 ISE et est hors de place pour ce document (voyez le pour en savoir plus de section Informations connexes).

## Dépannez

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

ISE devrait présenter :

Voici l'écoulement :

- L'utilisateur d'invité rencontre la deuxième règle d'autorisation et est réorienté au point névralgique (« authentification réussie »).
- Après que l'utilisateur reçoive l'AUP, ISE envoie l'Admin-remise CoA, qui est confirmée par le WLC (« autorisation dynamique réussie »).
- Le WLC exécute la ré-authentification, et le nom d'ACL est retourné (« réservé Autoriser réussi »).

Ceci peut être également vérifié si vous naviguez vers des **exécutions > des états > ISE signale > accès invité signale > état d'acceptation AUP** :

## Informations connexes

- Services de posture sur le guide de configuration de Cisco ISE
- Guide d'administrateurs de Cisco ISE 1.3
- Authentification Web centrale exemple sur WLC et ISE configuration
- Authentification Web centrale avec FlexConnect aps sur un WLC avec l'exemple de configuration ISE

- Support et documentation techniques - Cisco Systems