Stratégies ISE basées sur des exemples de configuration SSID

Contenu

Introduction

Ce document décrit comment configurer des stratégies d'autorisation dans le Logiciel Cisco Identity Services Engine (ISE) pour distinguer les différents identifiants d'ensemble de services (SSID). Il est très commun pour qu'une organisation ait le multiple SSID dans leur réseau Sans fil pour différents buts. Un des buts les plus communs est d'avoir un SSID entreprise pour les employés et un invité SSID pour des visiteurs à l'organisation.

Ce guide assume cela :

1. Le contrôleur LAN Sans fil (WLC) est installé et fonctionne pour tout le SSID impliqué.
2. L'authentification travaille à tout le SSID impliqué contre ISE.

D'autres documents dans cette gamme

- Authentification Web centrale avec un exemple de configuration de commutateur et de Cisco Identity Services Engine
- Authentification Web centrale exemple sur WLC et ISE configuration
- L'invité ISE explique l'exemple de configuration d'authentification RADIUS/802.1x
- Posture intégrée VPN utilisant l'iPEP ISE et ASA

Conditions préalables

Conditions requises

Aucune spécification déterminée n'est requise pour ce document.

Composants utilisés

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

- Version Sans fil 7.3.101.0 de contrôleur LAN
- Version 1.1.2.145 de Cisco Identity Services Engine

Les versions antérieures ont également chacun des deux caractéristiques.

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous à Conventions relatives aux conseils techniques Cisco.

Configurez

Cette section vous fournit des informations pour configurer les fonctionnalités décrites dans ce document.

Note: Utilisez l'outil Command Lookup Tool (clients enregistrés seulement) pour obtenir plus d'informations sur les commandes utilisées dans cette section.

Configurations

Ce document utilise les configurations suivantes :

- Méthode 1 : Airespace-WLAN-id
- Méthode 2 : APPELER-STATION-ID

Seulement une méthode de configuration devrait être utilisée à la fois. Si les deux configurations sont mises en application simultanément, la quantité a traité par des augmentations ISE et les affects ordonnent la lisibilité. Ce document passe en revue les avantages et les inconvénients de chaque méthode de configuration.

Méthode 1 : Airespace-WLAN-id

Chaque réseau local sans fil (WLAN) créé sur le WLC a un ID de WLAN. L'ID de WLAN est affiché à la page récapitulative WLAN.

Quand un client se connecte au SSID, la demande RADIUS à ISE contient l'attribut d'Airespace-WLAN-ID. Cet attribut simple est utilisé pour prendre des décisions politiques dans ISE. Un inconvénient à cet attribut est si l'ID de WLAN ne s'assortit pas sur un SSID propagé à travers de plusieurs contrôleurs. Si ceci décrit votre déploiement, continuez à la méthode 2.

Dans ce cas, l'Airespace-WLAN-id est utilisé comme condition. Il peut être utilisé comme état simple (par lui-même) ou en état composé (en même temps qu'un autre attribut) pour réaliser l'effet désiré. Ce document couvre les deux cas d'utilisation. Avec les deux SSID ci-dessus, ces deux règles peuvent être créées.

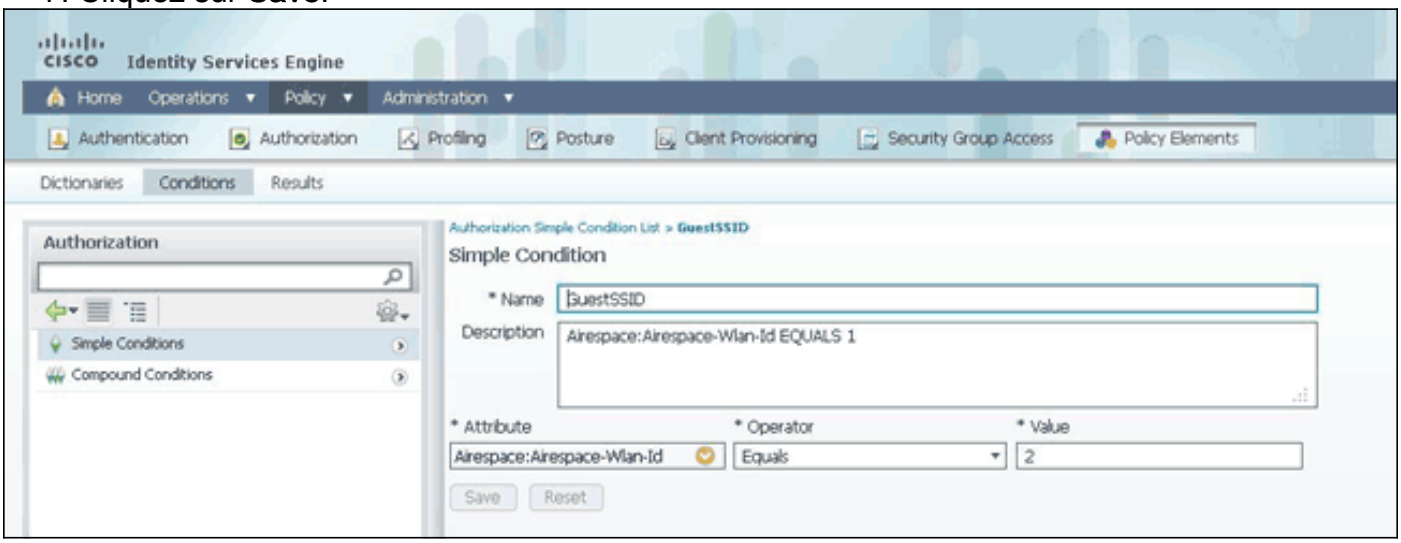
A) Les utilisateurs d'invité doivent ouvrir une session à l'invité SSID.

B) Les utilisateurs en entreprise doivent être dans le groupe « utilisateurs de Répertoire actif (AD) de domaine » et doivent ouvrir une session au SSID entreprise.

Ordonnez A

Ordonnez A a juste une condition requise, ainsi vous pouvez établir un état simple (basé sur les valeurs ci-dessus) :

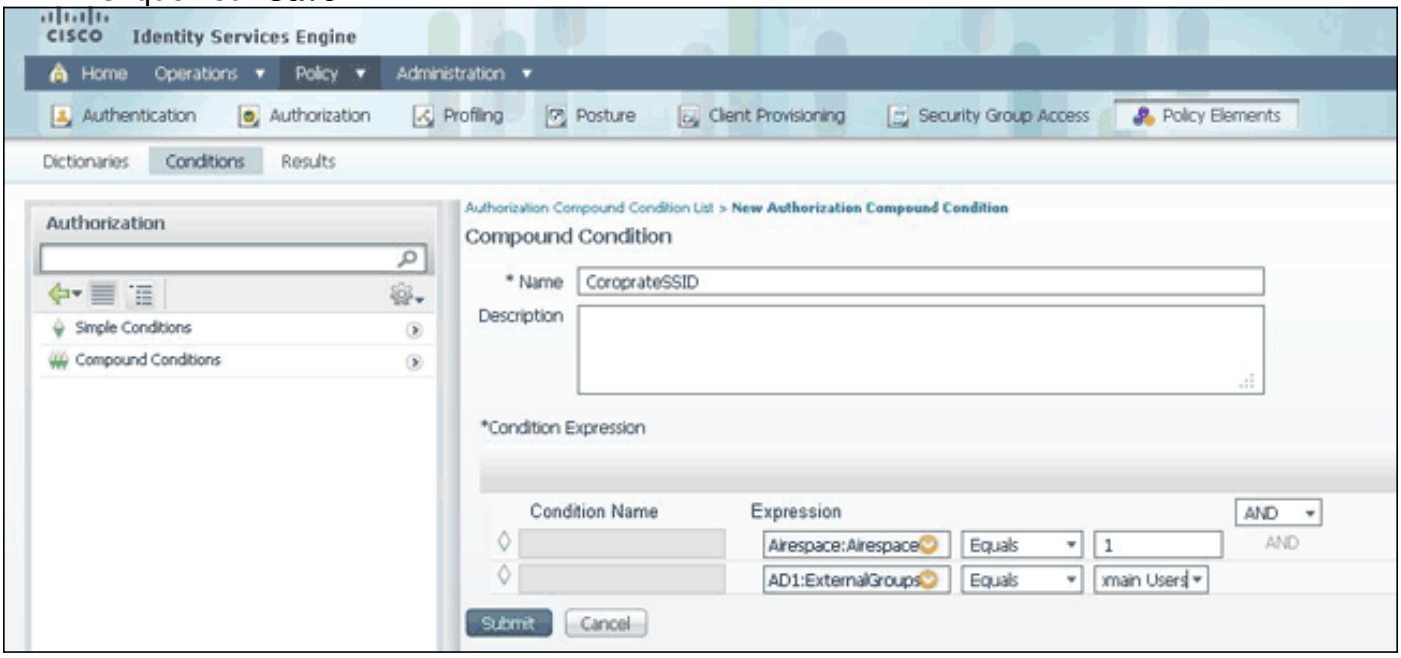
1. Dans ISE, allez à la **stratégie > aux éléments > aux états > à l'autorisation de stratégie > des états simples** et créez un nouvel état.
2. Dans la zone d'identification, écrivez un nom de condition
3. Dans le champ description, écrivez une description (facultative).
4. De la liste déroulante d'attribut, choisissez **Airespace > Airespace-Wlan-Id--[1]**.
5. De la liste déroulante d'opérateur, choisissez les **égaux.**
6. De la liste déroulante de valeur, choisissez **2.**
7. Cliquez sur **Save**.



Règle B

La règle B a deux conditions requises, ainsi vous pouvez établir un état composé (basé sur les valeurs ci-dessus) :

1. Dans ISE, allez à la **stratégie > aux éléments > aux états > à l'autorisation de stratégie > des états composés** et créez un nouvel état.
2. Dans la zone d'identification, écrivez un nom de condition.
3. Dans le champ description, écrivez une description (facultative).
4. Choisissez **créent le nouvel état (option anticipée)**.
5. De la liste déroulante d'attribut, choisissez **Airespace > Airespace-Wlan-Id--[1]**.
6. De la liste déroulante d'opérateur, choisissez les **égaux.**
7. De la liste déroulante de valeur, choisissez **1.**
8. Cliquez sur l'équipement vers la droite et choisissez **ajoutent l'attribut/valeur**.
9. De la liste déroulante d'attribut, choisissez **AD1 > les groupes externes**.
10. De la liste déroulante d'opérateur, choisissez les **égaux.**
11. De la liste déroulante de valeur, sélectionnez le groupe requis. Dans cet exemple, il est placé aux utilisateurs de domaine.
12. Cliquez sur **Save**.



Note: Dans tout ce document nous utilisons des profils simples d'autorisation configurés sous la stratégie > les éléments de stratégie > les résultats > l'autorisation > les profils d'autorisation. Ils sont placés pour permettre Access, mais peuvent être adaptés pour adapter les besoins de votre déploiement.

Maintenant que nous avons les conditions, nous pouvons nous appliquer les à une stratégie d'autorisation. Allez à la **stratégie > à l'autorisation**. Déterminez où insérer la règle dans la liste ou éditer votre règle existante.

Règle d'invité

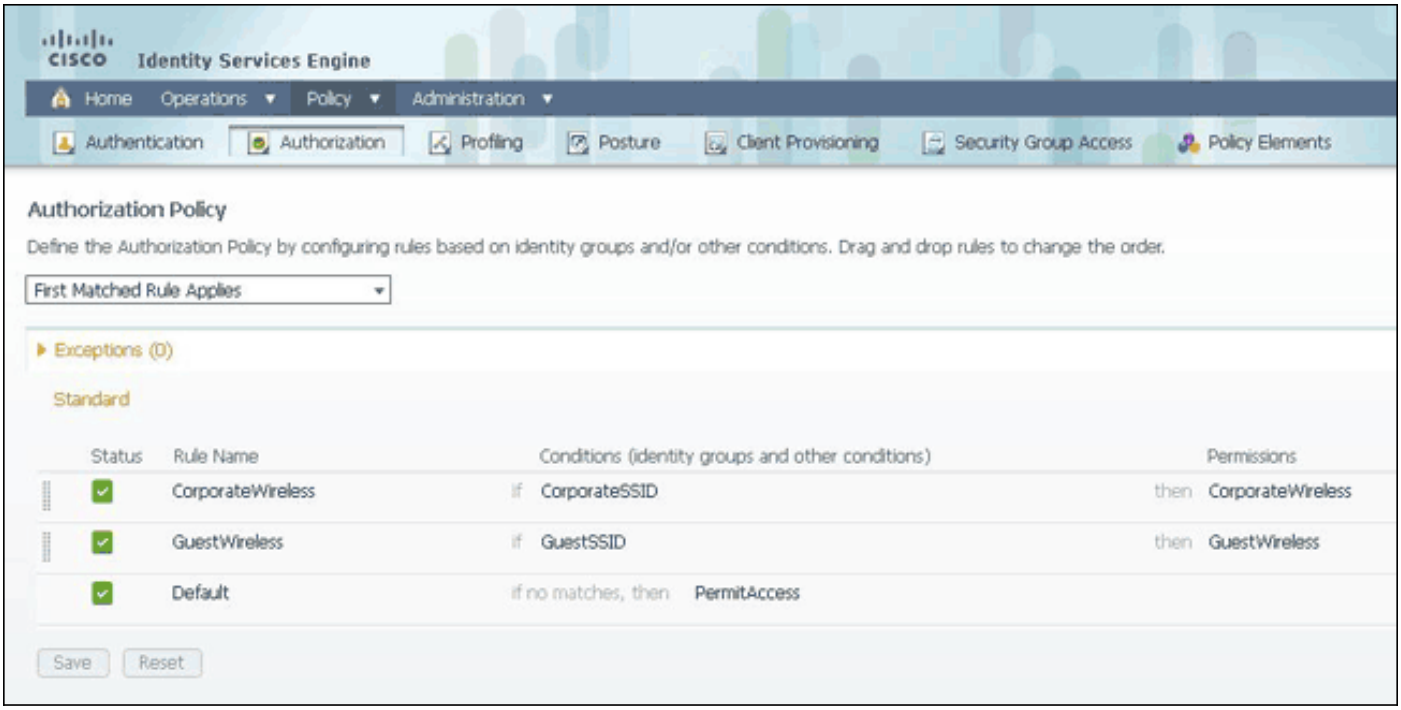
1. Cliquez sur vers le bas la flèche à la droite d'une règle existante et choisissez l'**insertion une nouvelle règle**.
2. En écrivez un nom pour votre règle d'invité et laissez les groupes d'identité mettent en place le positionnement à.
3. Dans des conditions, cliquez sur le plus et cliquez sur l'**état existant choisi de la bibliothèque**.

4. Sous le nom de condition, choisissez l'**état simple > le GuestSSID**.
5. Sous des autorisations, choisissez le profil approprié d'autorisation pour vos utilisateurs d'invité.
6. Cliquez sur **Done**.

Règle entreprise

1. Cliquez sur vers le bas la flèche à la droite d'une règle existante et choisissez l'**insertion une nouvelle règle**.
2. En écrivez un nom pour votre règle entreprise et laissez les groupes d'identité mettent en place le positionnement à.
3. Dans des conditions, cliquez sur le plus et cliquez sur l'**état existant choisi de la bibliothèque**.
4. Sous le nom de condition, choisissez l'**état composé > le CorporateSSID**.
5. Sous des autorisations, choisissez le profil approprié d'autorisation pour vos utilisateurs en entreprise.
6. Cliquez sur **Done**.

Note: Jusqu'à ce que vous cliquiez sur la sauvegarde au bas de la liste de stratégie, aucune modification apportée sur cet écran ne sera appliquée à votre déploiement.



Méthode 2 : APPELER-STATION-ID

Le WLC peut être configuré pour envoyer le nom SSID dans l'attribut d'Appeler-Station-ID de RADIUS, qui consécutivement peut être utilisé comme condition sur ISE. L'avantage de cet attribut est qu'il peut l'utiliser indépendamment de ce que l'ID de WLAN est placé à sur le WLC. Par défaut, le WLC n'envoie pas le SSID dans l'attribut d'Appeler-Station-ID. Pour activer cette caractéristique sur le WLC, aller à la **Sécurité > à l'AAA > Radius > Authentication** et placer le type d'ID de station d'appel à l'adresse MAC AP : SSID. Ceci place le format du l'Appeler-Station-ID à *<MAC d'AP que l'utilisateur connecte le to> : <SSID Name>*.

Vous pouvez voir quel nom SSID va être envoyé de la page récapitulative WLAN.

Puisque l'attribut d'Appeler-Station-id contient également l'adresse MAC d'AP, une expression régulière (EXPRESSION RÉGULIÈRE) est utilisée pour apparier le nom SSID dans la stratégie ISE. L'opérateur « Matches" dans la configuration de condition peut lire une EXPRESSION RÉGULIÈRE du champ de valeur.

Exemples d'EXPRESSION RÉGULIÈRE

« Débuts avec » — par exemple, utilisez la valeur d'EXPRESSION RÉGULIÈRE du **^ (point culminant). *** — cette condition est configurée en tant que CERTIFICAT : Point culminant de l'organisation MATCHES " » (toute correspondance dans une condition qui commence par « le point culminant »).

« Finit avec » — par exemple, utilisez la valeur d'EXPRESSION RÉGULIÈRE de. *** (mktg) $** — cette condition est configurée en tant que CERTIFICAT : Mktg de l'organisation MATCHES " » (toute correspondance dans une condition qui finit avec « le mktg »).

« Contient » — par exemple, utilisez la valeur d'EXPRESSION RÉGULIÈRE de .*(1234).* — cette condition est configuré en tant que CERTIFICAT : L'organisation APPARIE '1234' (toute correspondance dans une condition qui contient "1234", tel qu'Eng1234, 1234Dev, et Corp1234Mktg).

« Ne commence pas » — par exemple, utilisez la valeur d'EXPRESSION RÉGULIÈRE du **^ (? ! LDAP). *** — cette condition est configurée en tant que CERTIFICAT : LDAP de l'organisation MATCHES " » (toute correspondance avec une condition qui ne commence pas par « le LDAP », comme l'usLDAP ou le CorpLDAPmktg).

L'Appeler-Station-ID finit avec le nom SSID, ainsi l'EXPRESSION RÉGULIÈRE à l'utiliser dans cet exemple est**. * (: <SSID NAME>) $**. Maintenez ceci dans l'esprit comme vous passez par la configuration.

Avec les deux SSID ci-dessus, vous pouvez créer deux règles avec ces conditions requises :

A) Les utilisateurs d'invité doivent ouvrir une session à l'invité SSID.

B) Les utilisateurs en entreprise doivent être dans le groupe « utilisateurs d'AD de domaine » et doivent ouvrir une session au SSID entreprise.

Ordonnez A

Ordonnez A a juste une condition requise, ainsi vous pouvez établir un état simple (basé sur les valeurs ci-dessus) :

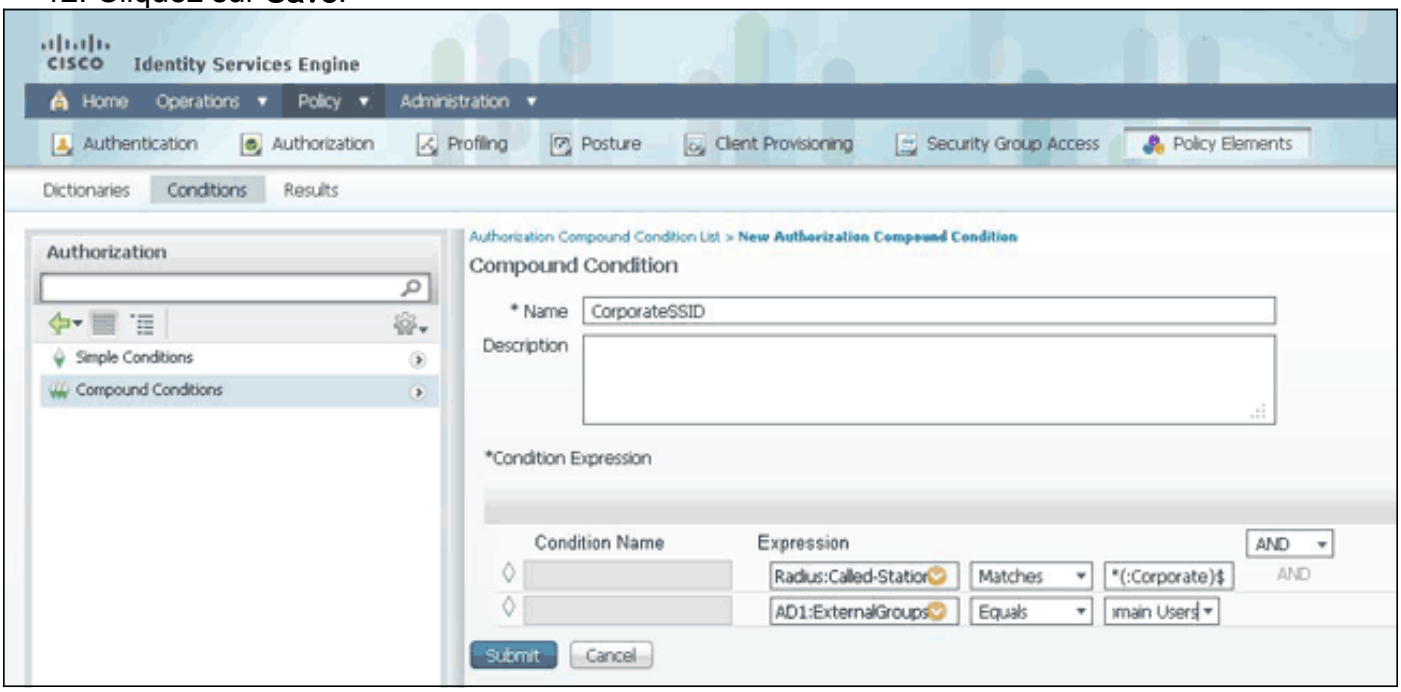
1. Dans ISE, allez à la **stratégie > aux éléments > aux états > à l'autorisation de stratégie > des états simples** et créez un nouvel état.
2. Dans la zone d'identification, écrivez un nom de condition.
3. Dans le champ description, écrivez une description (facultative).
4. De la liste déroulante d'attribut, choisissez **Radius - > Called-Station-ID--[30]**.
5. De la liste déroulante d'opérateur, choisissez les **correspondances.**
6. De la liste déroulante de valeur, choisissez. *** (: Invité) $**. Ce distingue les majuscules et minuscules.
7. Cliquez sur **Save**.

Règle B

La règle B a deux conditions requises, ainsi vous pouvez établir un état composé (basé sur les valeurs ci-dessus) :

1. Dans ISE, allez à la **stratégie > aux éléments > aux états > à l'autorisation de stratégie > des états composés** et créez un nouvel état.
2. Dans la zone d'identification, écrivez un nom de condition.
3. Dans le champ description, écrivez une description (facultative).
4. Choisissez **créent le nouvel état (option anticipée)**.
5. De la liste déroulante d'attribut, choisissez **Radius - > Called-Station-Id--[30]**.
6. De la liste déroulante d'opérateur, choisissez les **correspondances.**
7. De la liste déroulante de valeur, choisissez**. * (:) $ entreprise**. Ce distingue les majuscules et minuscules.
8. Cliquez sur l'équipement vers la droite et choisissez **ajoutent l'attribut/valeur**.
9. De la liste déroulante d'attribut, choisissez **AD1 > les groupes externes**.
10. De la liste déroulante d'opérateur, choisissez les **égaux.**

11. De la liste déroulante de valeur, sélectionnez le groupe requis. Dans cet exemple, il est placé aux utilisateurs de domaine.
12. Cliquez sur **Save**.



Note: Dans tout ce document, nous utilisons des profils simples d'autorisation configurés sous la stratégie > les éléments de stratégie > les résultats > l'autorisation > les profils d'autorisation. Ils sont placés pour permettre Access, mais peuvent être adaptés pour adapter les besoins de votre déploiement.

Maintenant que les conditions sont configurées, appliquez-vous les à une stratégie d'autorisation. Allez à la **stratégie > à l'autorisation**. Insérez la règle dans la liste dans la localisation adaptée ou éditez une règle existante.

Règle d'invité

1. Cliquez sur vers le bas la flèche à la droite d'une règle existante et choisissez l'**insertion une nouvelle règle**.
2. En écrivez un nom pour votre règle d'invité et laissez les groupes d'identité mettent en place le positionnement à.
3. Dans des conditions, cliquez sur le plus et cliquez sur l'**état existant choisi de la bibliothèque**.
4. Sous le nom de condition, choisissez l'**état simple > le GuestSSID**
5. Sous des autorisations, choisissez le profil approprié d'autorisation pour vos utilisateurs d'invité.
6. Cliquez sur **Done**.

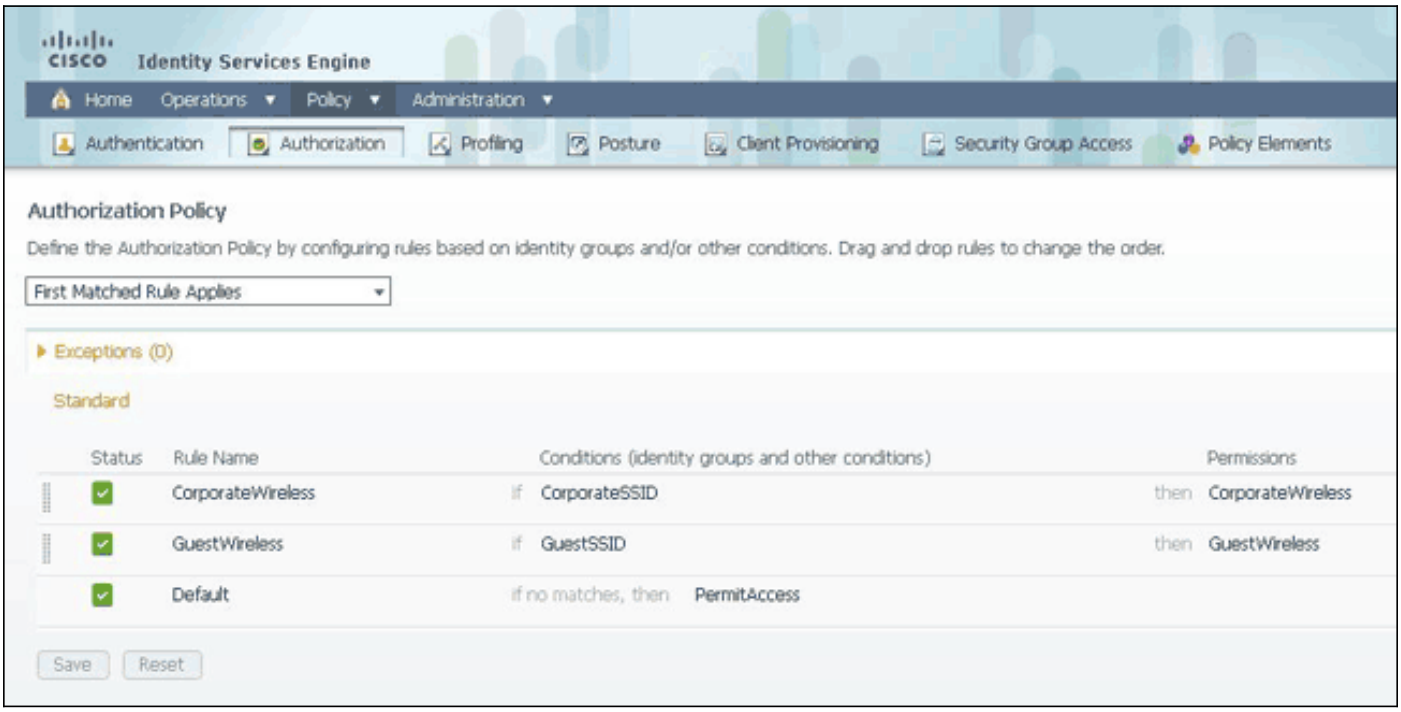
Règle entreprise

1. Cliquez sur vers le bas la flèche à la droite d'une règle existante et choisissez l'**insertion une nouvelle règle**.
2. En écrivez un nom pour votre règle entreprise et laissez les groupes d'identité mettent en place le positionnement à.
3. Dans des conditions, cliquez sur le plus et cliquez sur l'**état existant choisi de la bibliothèque**.
4. Sous le nom de condition, choisissez l'**état composé > le CorporateSSID**.
5. Sous des autorisations, choisissez le profil approprié d'autorisation pour vos utilisateurs en

entreprise.

6. Cliquez sur **Done**.
7. **Sauvegarde de** clic au bas de la liste de stratégie.

Note: Jusqu'à ce que vous cliquiez sur la sauvegarde au bas de la liste de stratégie, aucune modification apportée sur cet écran ne sera appliquée à votre déploiement.



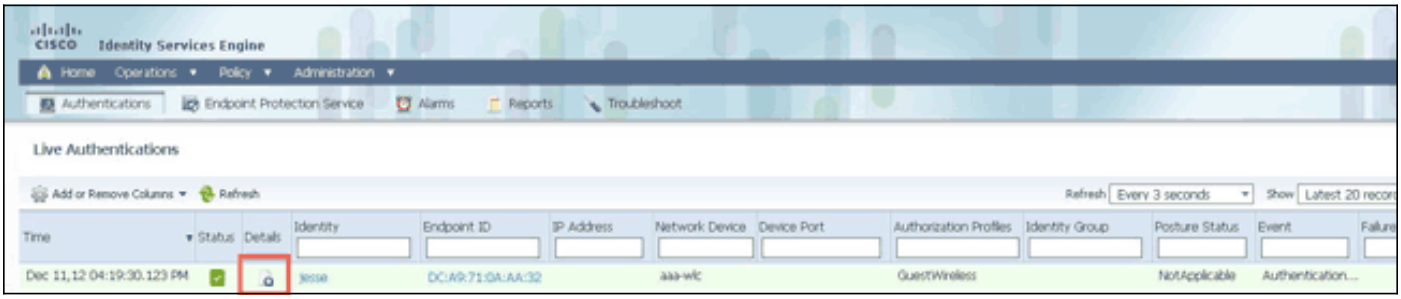
Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

Dépannez

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

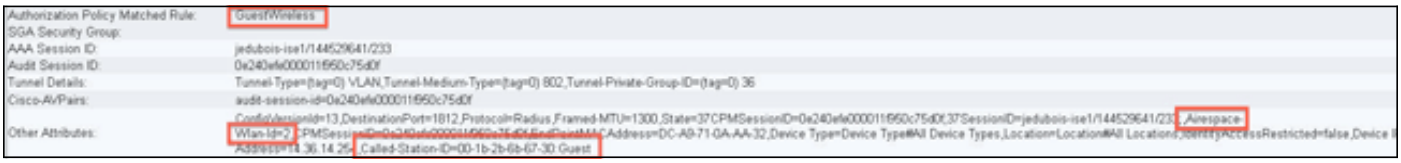
Pour découvrir si la stratégie était créée correctement et s'assurer ISE reçoit les attributs appropriés, passez en revue l'état détaillé d'authentification pour passé ou l'authentification défaillante pour l'utilisateur. Choisissez les **exécutions > les authentifications** et puis cliquez sur l'icône de **détails** pour une authentification.



D'abord, vérifiez le résumé d'authentification. Ceci affiche les fondements de l'authentification ce qui incluent ce que le profil d'autorisation a été fourni à l'utilisateur.

Authentication Summary	
Logged At:	December 11,2012 4:19:30.123 PM
RADIUS Status:	Authentication succeeded
NAS Failure:	
Username:	jesse
MAC/IP Address:	DC:A9:71:0A:AA:32
Network Device:	aaa-wlc : 14.36.14.254 :
Allowed Protocol:	Default Network Access
Identity Store:	AD1
Authorization Profiles:	GuestWireless
SGA Security Group:	
Authentication Protocol :	PEAP(EAP-MSCHAPv2)

Si la stratégie est incorrecte, les détails d'authentification afficheront quel Airespace-WLAN-id et quel Appeler-Station-id a été envoyé du WLC. Ajustez vos règles en conséquence. La règle appariée par stratégie d'autorisation confirme si l'authentification apparie votre règle destinée.



Ces règles misconfigured généralement. Pour indiquer la question de configuration, appariez la règle contre ce qui est vu dans les détails d'authentification. Si vous ne voyez pas les attributs dans les autres attributs mettent en place, assurez-vous que le WLC est correctement configuré.

Informations connexes

- Support et documentation techniques - Cisco Systems