ISE-beleid op basis van SSID-configuratievoorbeelden

Inhoud

Inleiding

Dit document beschrijft hoe u het autorisatiebeleid in Cisco Identity Services Engine (ISE) kunt configureren om onderscheid te maken tussen verschillende Service set identificatoren (SSID's). Het is heel gebruikelijk dat een organisatie meerdere SSID's in hun draadloze netwerk heeft voor verschillende doeleinden. Een van de meest algemene doelstellingen is om een SSID van de onderneming voor werknemers en een gast SSID voor bezoekers aan de organisatie te hebben.

In deze handleiding wordt uitgegaan van:

1. De Wireless LAN Controller is ingesteld en werkt voor alle betrokken SSID's.
2. Verificatie werkt bij alle SSID's die betrokken zijn tegen ISE.

Overige documenten in deze serie

- Central-webverificatie met een Configuratievoorbeeld van Switch- en Identity Services Engine
- Central-webverificatie in het configuratievoorbeeld van WLC en ISE
- ISE Guest Account voor RADIUS/802.1x-verificatievoorbeeld
- VPN Inline Posture met iPEP ISE en ASA

Voorwaarden

Vereisten

Er zijn geen specifieke vereisten van toepassing op dit document.

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Draadloze LAN-controller release 7.3.10.0
- Identity Services Engine release 1.1.2.14.5

Eerdere versies hebben ook beide functies.

De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden beschreven, hadden een opgeschoonde (standaard)configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Configureren

Deze sectie bevat informatie over het configureren van de functies die in dit document worden beschreven.

Opmerking: Gebruik het Opname Gereedschap (alleen geregistreerde klanten) om meer informatie te verkrijgen over de opdrachten die in deze sectie worden gebruikt.

Configuraties

Dit document gebruikt deze configuraties:

- Methode 1: Airespace-Wlan-ID
- Methode 2: Uitgeroepen station-ID

Er mag slechts één configuratiemethode tegelijk worden gebruikt. Als beide configuraties tegelijkertijd worden geïmplementeerd, wordt het door ISE verwerkte bedrag verhoogd en beïnvloedt het de leesbaarheid van de regels. Dit document beschrijft de voor- en nadelen van elke configuratiemethode.

Methode 1: Airespace-Wlan-ID

Elk Wireless Local Area Network (WLAN) dat op de WLC is gemaakt, heeft een WLAN-id. De WLAN-id wordt op de WLAN-overzichtspagina weergegeven.

Wanneer een client verbinding maakt met SSID, bevat het RADIUS-verzoek aan ISE de Airespace-WLAN-ID-eigenschap. Deze simpele eigenschap wordt gebruikt om beleidsbeslissingen in ISE te nemen. Eén nadeel voor deze eigenschap is als de WLAN-id niet

overeenkomt met een SSID dat wordt verspreid over meerdere controllers. Als dit uw plaatsing beschrijft, blijf methode 2.

In dit geval wordt Airespace-Wlan-ID als toestand gebruikt. Het kan als een eenvoudige conditie (op zichzelf) of in een samengestelde conditie (in combinatie met een andere eigenschap) worden gebruikt om het gewenste resultaat te bereiken. Dit document heeft betrekking op beide gebruiksgevallen. Met de twee bovenstaande SSID's kunnen deze twee regels worden gemaakt.

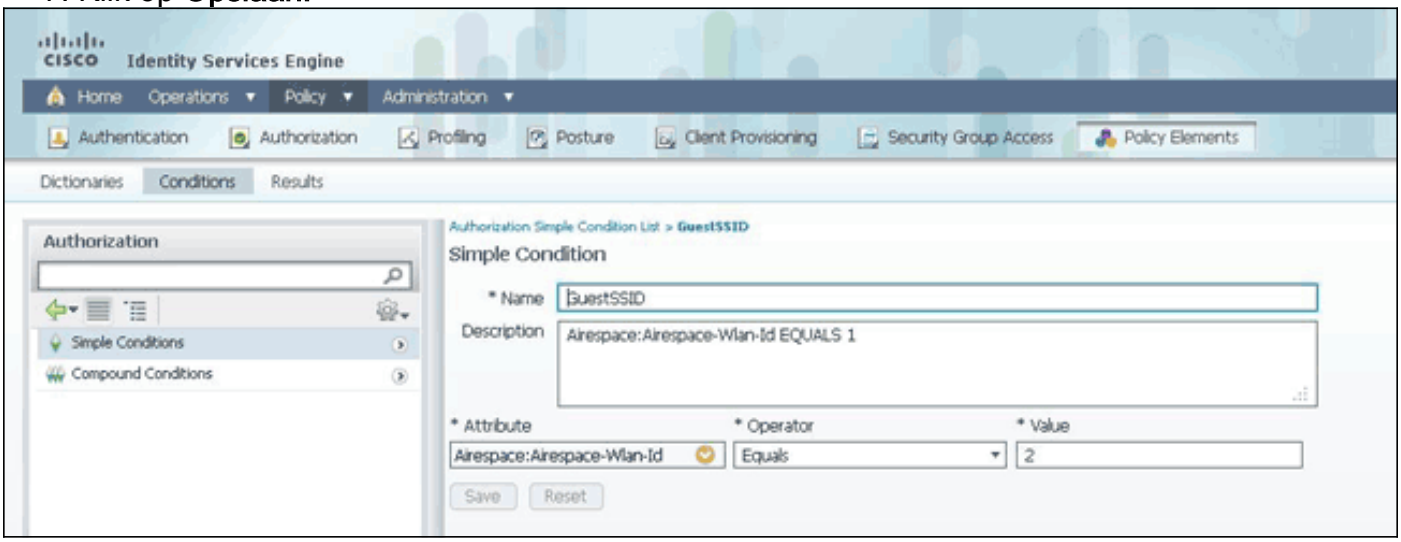
A) De gebruikers van de gast moeten inloggen bij de Guest SSID.

B) Bedrijven moeten in de Active Directory (AD) groep "Domain Gebruikers" zijn en moeten zich bij de Corporate SSID aanmelden.

Regel A

Regel A heeft slechts één vereiste, zodat je een eenvoudige voorwaarde kunt maken (op basis van de bovenstaande waarden):

1. In ISE, ga naar **Policy > Policy Elementen > Voorwaarden > Vergunning > Eenvoudige Voorwaarden** en maak een nieuwe voorwaarde.
2. Voer in het veld Naam een naam in
3. Typ in het veld Description een omschrijving (optioneel).
4. Kies in de vervolgkeuzelijst Kenmerken de optie **Asperace > Airespace-WLAN-ID—[1]**.
5. Selecteer in de vervolgkeuzelijst Exploitant de optie **Gelijk.**
6. Kies in de vervolgkeuzelijst Waarde **2**.
7. Klik op **Opslaan.**

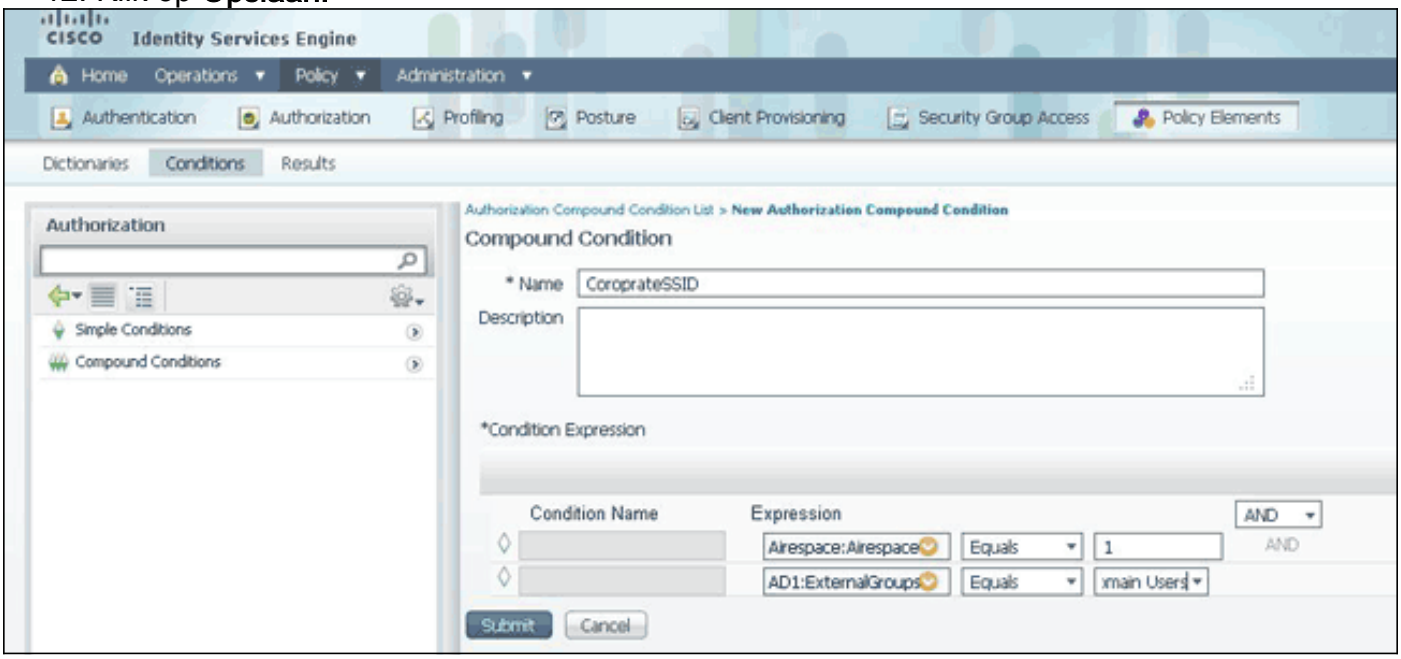


Artikel B

Regel B bevat twee vereisten, zodat u een samengestelde toestand kunt bouwen (op basis van de bovenstaande waarden):

1. In ISE, ga naar **Policy > Policy Elementen > Voorwaarden > Vergunning > Samengestelde Voorwaarden** en creëren een nieuwe voorwaarde.
2. Voer in het veld Naam een naam in.
3. Typ in het veld Description een omschrijving (optioneel).
4. Kies **Nieuwe conditionering maken (geavanceerde optie)**.
5. Kies in de vervolgkeuzelijst Kenmerken de optie **Asperace > Airespace-WLAN-ID—[1]**.

6. Selecteer in de vervolgkeuzelijst Exploitant de optie **Gelijk.**
7. Kies in de vervolgkeuzelijst Waarde **1**.
8. Klik op het tandwiel rechts en kies **Toevoegen kenmerk/waarde**.
9. Kies in de vervolgkeuzelijst Eigenschappen de optie **AD1 > Externe groepen**.
10. Selecteer in de vervolgkeuzelijst Exploitant de optie **Gelijk.**
11. Selecteer de gewenste groep in de vervolgkeuzelijst Waarde. In dit voorbeeld wordt deze ingesteld op Domain Gebruikers.
12. Klik op **Opslaan.**



N.B.: In dit document gebruiken we eenvoudige autorisatieprofielen die zijn geconfigureerd onder Beleidselementen > Resultaten > autorisatie > autorisatieprofielen. Ze zijn ingesteld om toegang te verlenen, maar kunnen worden aangepast aan de behoeften van uw inzet.

Nu we de voorwaarden hebben, kunnen we ze toepassen op een vergunningsbeleid. Ga naar **beleid > autorisatie**. Bepaal waar u de regel in de lijst wilt invoeren of bewerk de bestaande regel.

Guest Rule

1. Klik op de pijl omlaag rechts van een bestaande regel en kies **Invoegen van een nieuwe regel**.
2. Voer een naam in voor de gastregel en laat het veld Identiteitsgroepen ingesteld op AnyRes.
3. Klik onder Voorwaarden op het plus en klik op **Bestaande conditionering uit bibliotheek selecteren**.
4. Kies onder de naam Voorwaarde **eenvoudige conditionering > GuestSSID**.
5. Kies onder Toegangsrechten het juiste licentieprofiel voor uw Gastgebruikers.
6. Klik op **Klaar.**

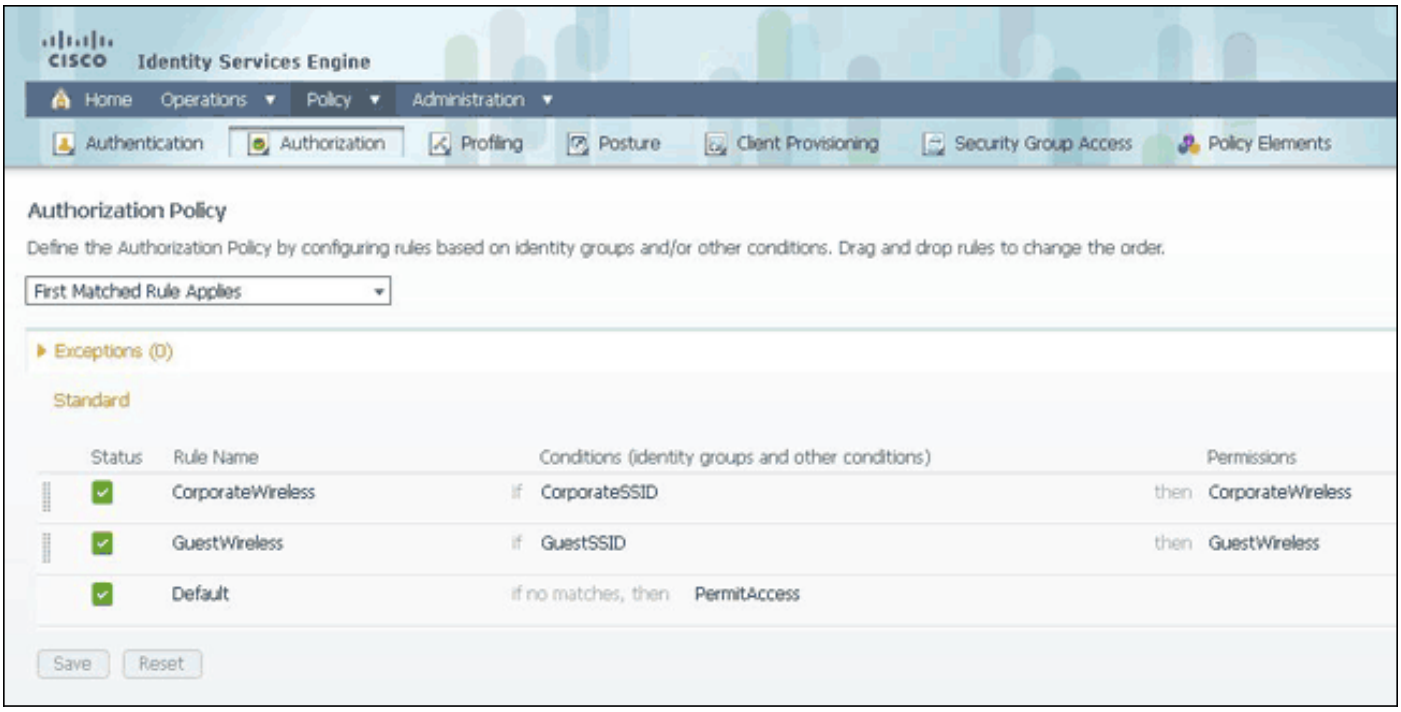
Corporate Rule

1. Klik op de pijl omlaag rechts van een bestaande regel en kies **Invoegen van een nieuwe regel**.
2. Voer een naam in voor de bedrijfsregel en laat het veld Identiteitsgroepen ingesteld op AnyAny.
3. Klik onder Voorwaarden op het plus en klik op **Bestaande conditionering uit bibliotheek**

selecteren.

4. Kies onder de naam Voorwaarde een **optie Samengestelde conditionering > CorporateSSID**.
5. Kies onder Toegangsrechten het juiste licentieprofiel voor uw zakelijke gebruikers.
6. Klik op **Klaar.**

Opmerking: Totdat u op Opslaan onder in de Beleidslijst klikt, worden er geen wijzigingen op dit scherm aangebracht op uw implementatie.



Methode 2: Uitgeroepen station-ID

De WLC kan worden geconfigureerd om de naam van SSID in de eigenschap RADIUS CD-ROM te verzenden, die op zijn beurt kan worden gebruikt als voorwaarde op ISE. Het voordeel van deze eigenschap is dat het kan worden gebruikt ongeacht wat de WLAN-ID op de WLC heeft ingesteld. Standaard stuurt de WLC de SSID niet in de eigenschap CD-ROM. Ga naar **Security > AAA > RADIUS > Verificatie** om deze optie in te schakelen op het WLC-**type** en stel de Call Station ID in op AP MAC-adres:SSID. Dit stelt het formaat van de geroepen-Station-ID in op *<MAC van de AP waarop de gebruiker een verbinding maakt met>:<SSID Name>*.

U kunt zien wat de naam van SSID van de WLAN samenvattende pagina wordt verzonden.

Aangezien de eigenschap geroepen-Station-ID ook het MAC-adres van de AP bevat, wordt een Reguliere expressie (REGEX) gebruikt om de naam van SSID in het ISE-beleid aan te passen. De operator 'Matches' in de conditie configuratie kan een REGEX van het veld Waarde lezen.

REGEX voorbeelden

'Begint met '-bijvoorbeeld, gebruik de REGEX waarde van **^ (Acme).***-deze conditie is ingesteld als CERTIFICAAT:Organisatie KOMT overeen met 'Acme' (elke match met een conditie die begint met 'Acme').

'Eind met—gebruik bijvoorbeeld de REGEX-waarde van **.*(mktg)$**—deze voorwaarde is ingesteld als CERTIFICAAT:Organisatie past 'mktg' toe (elke overeenkomst met een voorwaarde die eindigt met 'mktg').

'Bevat', bijvoorbeeld, gebruik de REGEX-waarde van **.*(1234).***-deze conditie is ingesteld als CERTIFICAAT:Organisatie KOMT '1234' (elke match met een voorwaarde die "1234" bevat, zoals Eng1234, 1234Dev, en p1234MKG).

'Begin niet met '-bijvoorbeeld, gebruik de REGEX waarde van **^(?!LDAP).***- deze conditie is ingesteld als CERTIFICAAT:Organisatie KOMT aan 'LDAP' (elke match met een toestand die niet begint met 'LDAP', zoals onsLDAP of CorpLDAPmktg).

De geroepen-Station-ID eindigt met de naam van SSID, zodat de REGEX die in dit voorbeeld moet worden gebruikt **.* (:<SSID NAME>)$**. Houd dit in gedachten als je door de configuratie gaat.

Met de twee bovenstaande SSID's kunt u twee regels maken met deze vereisten:

A) De gebruikers van de gast moeten inloggen bij de Guest SSID.

B) Bedrijven moeten in de AD groep "Gebruikers van het Domein" zijn en moeten inloggen bij de Corporate SSID.

Regel A

Regel A heeft slechts één vereiste, zodat je een eenvoudige voorwaarde kunt maken (op basis van de bovenstaande waarden):

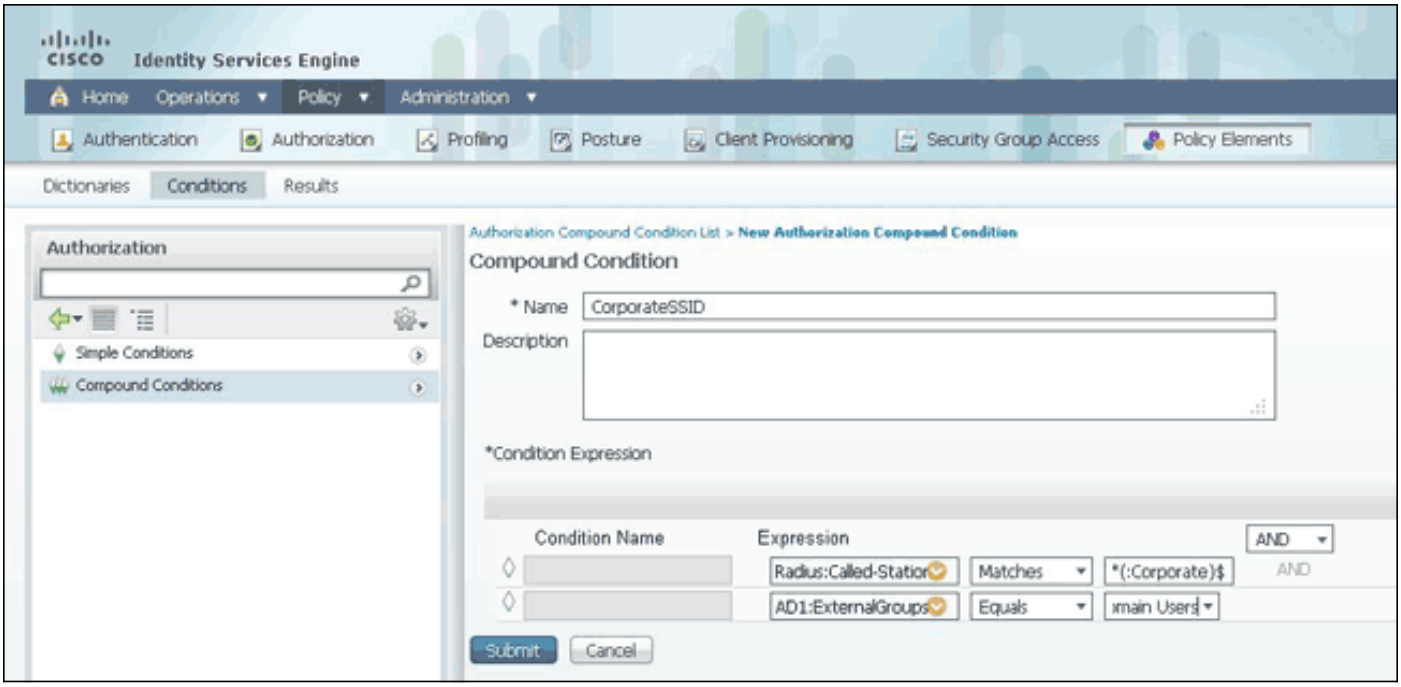
1. In ISE, ga naar **Policy > Policy Elementen > Voorwaarden > Vergunning > Eenvoudige Voorwaarden** en maak een nieuwe voorwaarde.
2. Voer in het veld Naam een naam in.
3. Typ in het veld Description een omschrijving (optioneel).
4. Kies in de vervolgkeuzelijst Kenmerken de optie **Straal -> Uitgeroepen station-ID—[30]**.
5. Kies in de vervolgkeuzelijst Exploitant **overeenkomsten.**
6. Kies **.* (:Guest)$** in de vervolgkeuzelijst Waarde. Dit is hoofdlettergevoelig.

7. Klik op **Opslaan**.

Artikel B

Regel B bevat twee vereisten, zodat u een samengestelde toestand kunt bouwen (op basis van de bovenstaande waarden):

1. In ISE, ga naar **Policy > Policy Elementen > Voorwaarden > Vergunning > Samengestelde Voorwaarden** en creëren een nieuwe voorwaarde.
2. Voer in het veld Naam een naam in.
3. Typ in het veld Description een omschrijving (optioneel).
4. Kies **Nieuwe conditionering maken (geavanceerde optie)**.
5. Kies in de vervolgkeuzelijst Kenmerken de optie **Straal -> Uitgeroepen station-ID—[30]**.
6. Kies in de vervolgkeuzelijst Exploitant **overeenkomsten.**
7. Kies in de vervolgkeuzelijst Waarde **.* (:Corporate)$**. Dit is hoofdlettergevoelig.
8. Klik op het tandwiel rechts en kies **Toevoegen kenmerk/waarde**.
9. Kies in de vervolgkeuzelijst Eigenschappen de optie **AD1 > Externe groepen**.
10. Selecteer in de vervolgkeuzelijst Exploitant de optie **Gelijk.**
11. Selecteer de gewenste groep in de vervolgkeuzelijst Waarde. In dit voorbeeld wordt deze ingesteld op Domain Gebruikers.
12. Klik op **Opslaan.**



N.B.: In dit document gebruiken we eenvoudige autorisatie profielen die zijn geconfigureerd onder Policy > Policy Elementen > Resultaten > autorisatie > autorisatieprofielen. Ze zijn ingesteld om toegang te verlenen, maar kunnen worden aangepast aan de behoeften van uw inzet.

Nu de voorwaarden zijn ingesteld, moet u deze toepassen op een vergunningsbeleid. Ga naar **beleid > autorisatie**. Plaats de regel in de lijst op de juiste locatie of bewerk een bestaande regel.

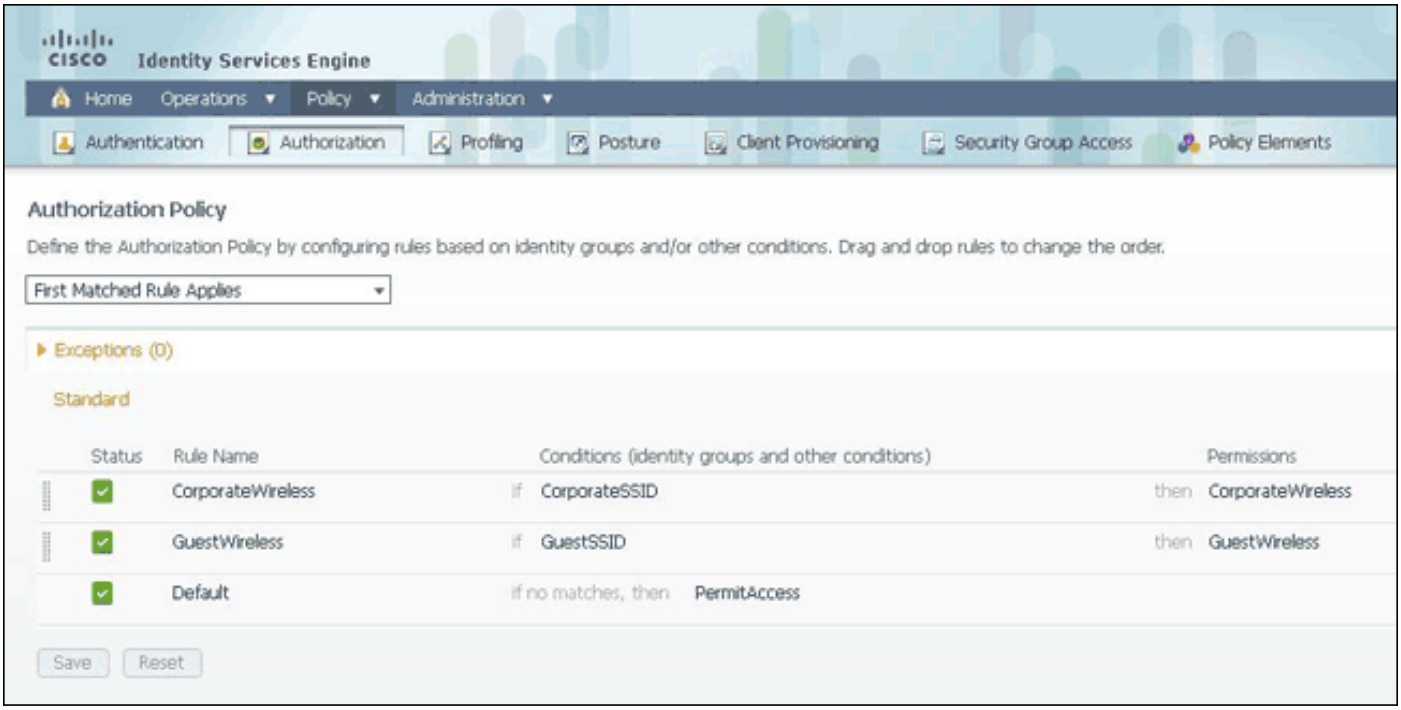
Guest Rule

1. Klik op de pijl omlaag rechts van een bestaande regel en kies **Invoegen van een nieuwe regel**.
2. Voer een naam in voor de gastregel en laat het veld Identiteitsgroepen ingesteld op AnyRes.
3. Klik onder Voorwaarden op het plus en klik op **Bestaande conditionering uit bibliotheek selecteren**.
4. Kies onder de naam conditioner **eenvoudige conditionering > GuestSSID**
5. Kies onder Toegangsrechten het juiste licentieprofiel voor uw Gastgebruikers.
6. Klik op **Klaar**.

Corporate Rule

1. Klik op de pijl omlaag rechts van een bestaande regel en kies **Invoegen van een nieuwe regel**.
2. Voer een naam in voor de bedrijfsregel en laat het veld Identiteitsgroepen ingesteld op AnyAny.
3. Klik onder Voorwaarden op het plus en klik op **Bestaande conditionering uit bibliotheek selecteren**.
4. Kies onder de naam Voorwaarde een **optie Samengestelde conditionering > CorporateSSID**.
5. Kies onder Toegangsrechten het juiste licentieprofiel voor uw zakelijke gebruikers.
6. Klik op **Klaar.**
7. Klik onder in de Beleidslijst op **Opslaan**.

Opmerking: Totdat u op Opslaan onder in de Beleidslijst klikt, worden er geen wijzigingen op dit scherm aangebracht op uw implementatie.



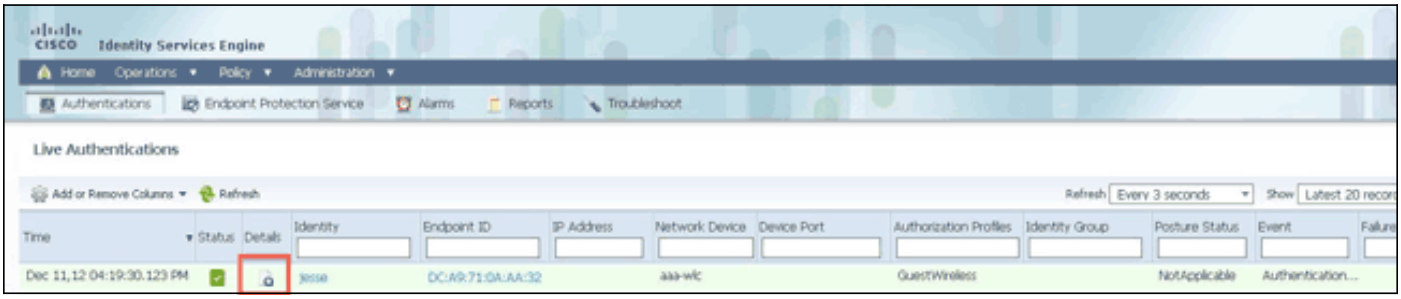
Verifiëren

Er is momenteel geen verificatieprocedure beschikbaar voor deze configuratie.

Problemen oplossen

Deze sectie bevat informatie waarmee u problemen met de configuratie kunt oplossen.

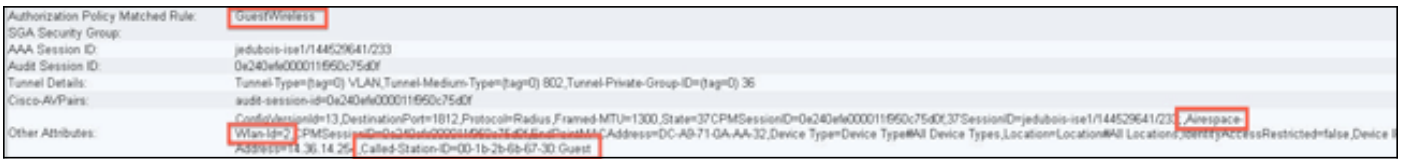
Om te weten te komen of het beleid goed is opgezet en om er zeker van te zijn dat ISE de juiste eigenschappen ontvangt, dient u het gedetailleerde verslag over de echtheidscontrole te bekijken voor ofwel een geslaagd ofwel mislukte authenticatie voor de gebruiker. Kies **Transacties > Authenticaties** en klik vervolgens op het **Details** pictogram voor een authenticatie.



Controleer eerst de verificatiesamenvatting. Dit toont de basisbeginselen van de echtheidscontrole, waaronder het vergunningsprofiel dat aan de gebruiker is verstrekt.

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)

Als het beleid niet correct is, zal de Verificatiedetails tonen wat Airespace-WLAN-ID en wat de geroepen-ID van de WLC werd verzonden. Pas uw regels dienovereenkomstig aan. De regel van het machtigingsbeleid aangepast bevestigt of de echtheidscontrole al dan niet overeenkomt met uw beoogde regel.



Deze regels zijn vaak verkeerd ingesteld. Om de configuratie kwestie te onthullen, stem de regel tegen wat in de authenticatiedetails wordt gezien. Als u de eigenschappen in het veld Andere eigenschappen niet ziet, zorg er dan voor dat de WLC correct is geconfigureerd.

Gerelateerde informatie

- Technische ondersteuning en documentatie – Cisco Systems