Directivas ISE basadas en los ejemplos de configuración SSID

Contenido

Introducción

Este documento describe cómo configurar las directivas de la autorización en Cisco Identity Services Engine (ISE) para distinguir entre diversos identificadores del conjunto de servicio (SSID). Es muy común para que una organización tenga SSID múltiples en su red inalámbrica para los diversos propósitos. Uno de los propósitos mas comunes es tener un SSID corporativo para los empleados y un invitado SSID para los visitantes a la organización.

Esta guía asume eso:

1. El regulador del Wireless LAN (WLC) se configura y trabaja para todos los SSID implicados.
2. La autenticación trabaja en todos los SSID implicados contra el ISE.

Otros documentos en esta serie

- Autenticación Web central con un ejemplo de configuración del Switch y del Identity Services Engine
- Autenticación Web central en el ejemplo de configuración del WLC y ISE
- El invitado ISE explica el ejemplo de la configuración de autenticación RADIUS/802.1x
- Postura en línea VPN usando el iPEP ISE y ASA

prerrequisitos

Requisitos

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Versión 7.3.101.0 del regulador del Wireless LAN
- Versión 1.1.2.145 del Identity Services Engine

Las versiones anteriores también tienen ambas características.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones sobre documentos.

Configurar

En esta sección encontrará la información para configurar las funciones descritas en este documento.

Note: Utilice la herramienta Command Lookup Tool (clientes registrados solamente) para obtener más información sobre los comandos utilizados en esta sección.

Configuraciones

En este documento, se utilizan estas configuraciones:

- Método 1: Airespace-WLAN-identificación
- Método 2: LLAMAR-ESTACIÓN-ID

Solamente un método de configuración debe ser en un momento usado. Si ambas configuraciones se implementan simultáneamente, la cantidad procesó por los aumentos ISE y afecta a la legibilidad de la regla. Este documentos revisa las ventajas y desventajas de cada método de configuración.

Método 1: Airespace-WLAN-identificación

Cada Wireless Local Area Network (red inalámbrica (WLAN)) creado en el WLC tiene un ID DE WLAN. El ID DE WLAN se visualiza en la página de resumen de la red inalámbrica (WLAN).

Cuando un cliente conecta con el SSID, el pedido de RADIUS al ISE contiene el atributo Airespace-RED INALÁMBRICA (WLAN)-ID. Este atributo simple se utiliza para tomar las decisiones de políticas en el ISE. Una desventaja a este atributo es si el ID DE WLAN no hace juego en un SSID separado a través de los controladores múltiples. Si esto describe su despliegue, continúe al método 2.

En este caso, la Airespace-WLAN-identificación se utiliza como condición. Puede ser utilizada como condición simple (en sí mismo) o en condiciones compuestas (conjuntamente con otro atributo) para alcanzar el resultado deseado. Este documentos abarca ambos casos del uso. Con los dos SSID arriba, estas dos reglas pueden ser creadas.

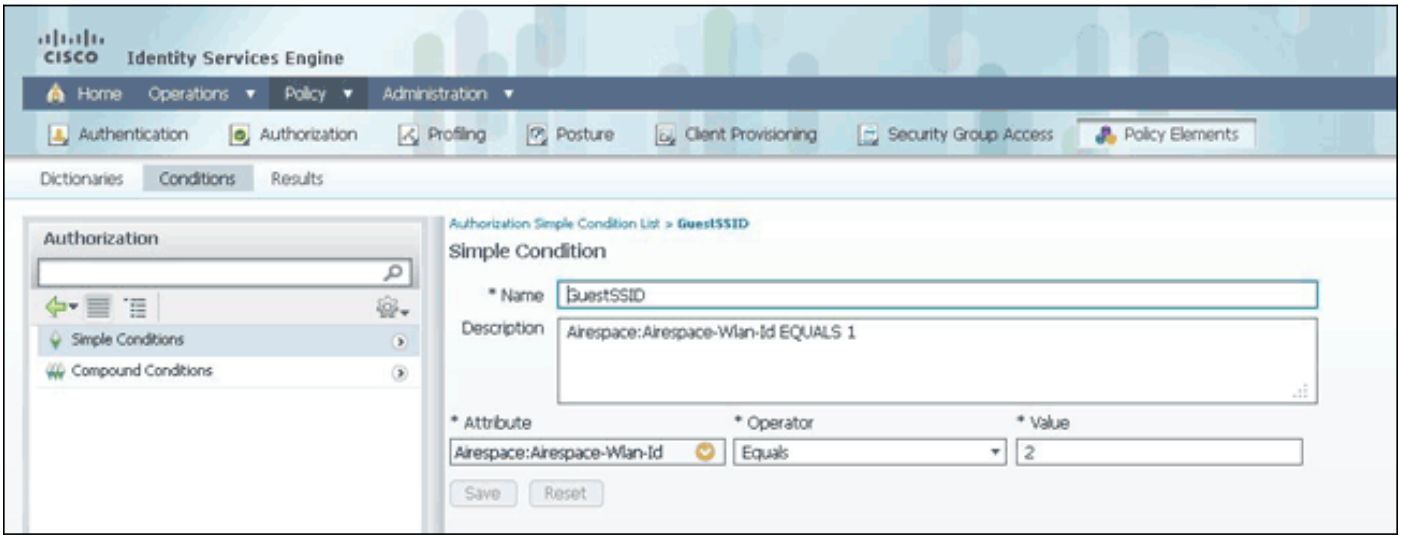
A) Los Usuarios invitados deben iniciar sesión al invitado SSID.

B) Los usuarios corporativos deben estar en el grupo “Domain User” del Active Directory (AD) y deben iniciar sesión al SSID corporativo.

Gobierne A

Gobierne A tiene apenas un requisito, así que usted puede construir una condición simple (basada en los valores antedichos):

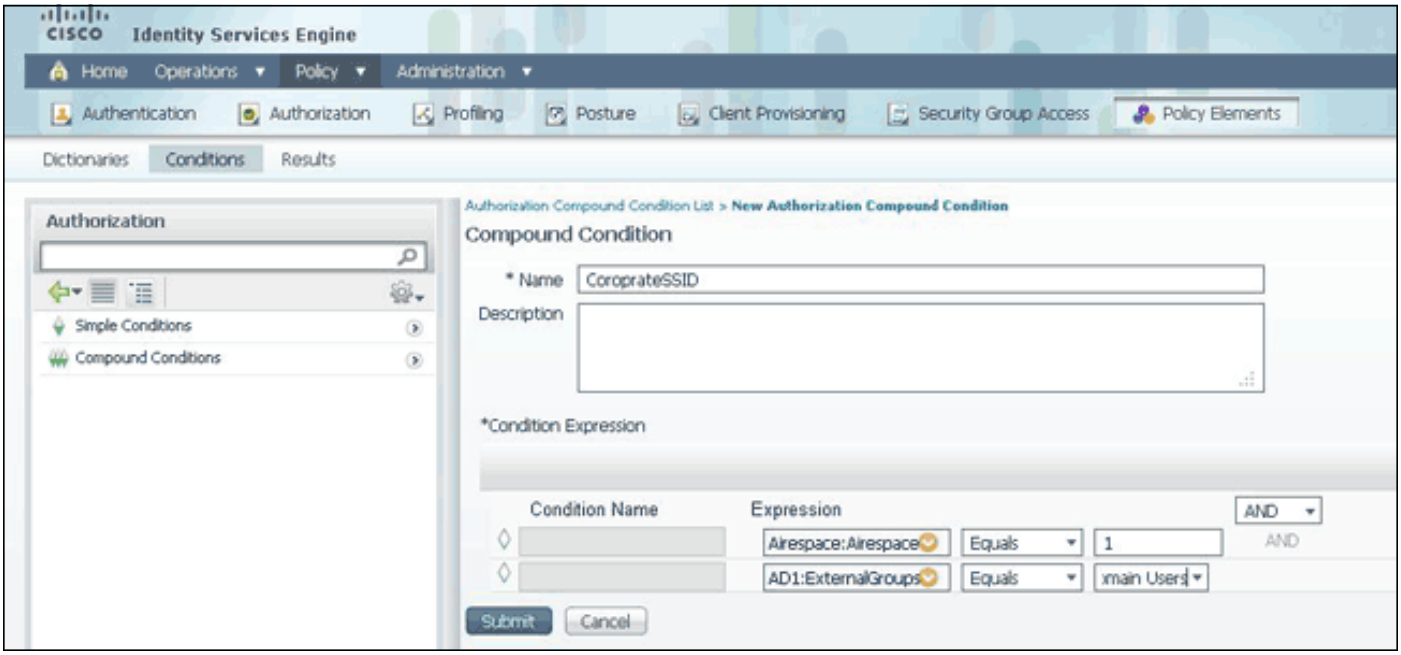
1. En el ISE, van a la **directiva > a los elementos > a las condiciones > a la autorización de la directiva > las condiciones simples** y crean una nueva condición.
2. En el campo de nombre, ingrese un nombre de condición
3. En el campo Description (Descripción), ingrese una descripción (opcional).
4. De la lista desplegable del atributo, elija el **Airespace > Airespace-Wlan-Id--[1]**.
5. De la lista desplegable del operador, elija los **iguales.**
6. De la lista desplegable de valores, elija **2.**
7. Click **Save**.



Gobierne B

La regla B tiene dos requisitos, así que usted puede construir una condición compuesta (basada en los valores antedichos):

1. En el ISE, van a la **directiva > a los elementos > a las condiciones > a la autorización de la directiva > las condiciones compuestas** y crean una nueva condición.
2. En el campo de nombre, ingrese un nombre de condición.
3. En el campo Description (Descripción), ingrese una descripción (opcional).
4. Elija **crean la nueva condición (opción anticipada)**.
5. De la lista desplegable del atributo, elija el **Airespace > Airespace-Wlan-Id--[1]**.
6. De la lista desplegable del operador, elija los **iguales.**
7. De la lista desplegable de valores, elija **1.**
8. Haga clic el engranaje a la derecha y elija **agregan el atributo/el valor**.
9. De la lista desplegable del atributo, elija **AD1 > los grupos externos**.
10. De la lista desplegable del operador, elija los **iguales.**
11. De la lista desplegable de valores, seleccione al grupo requerido. En este ejemplo, se fija a los Domain User.
12. Click **Save**.



Note: En este documento utilizamos los perfiles simples de la autorización configurados bajo la directiva > los elementos de la directiva > los resultados > la autorización > perfiles de la autorización. Se fijan para permitir el acceso, pero pueden ser adaptados para caber las necesidades de su despliegue.

Ahora que tenemos las condiciones, podemos aplicarlas a una directiva de la autorización. Vaya a la **directiva > a la autorización**. Determine donde insertar la regla en la lista o editar su regla existente.

Regla del invitado

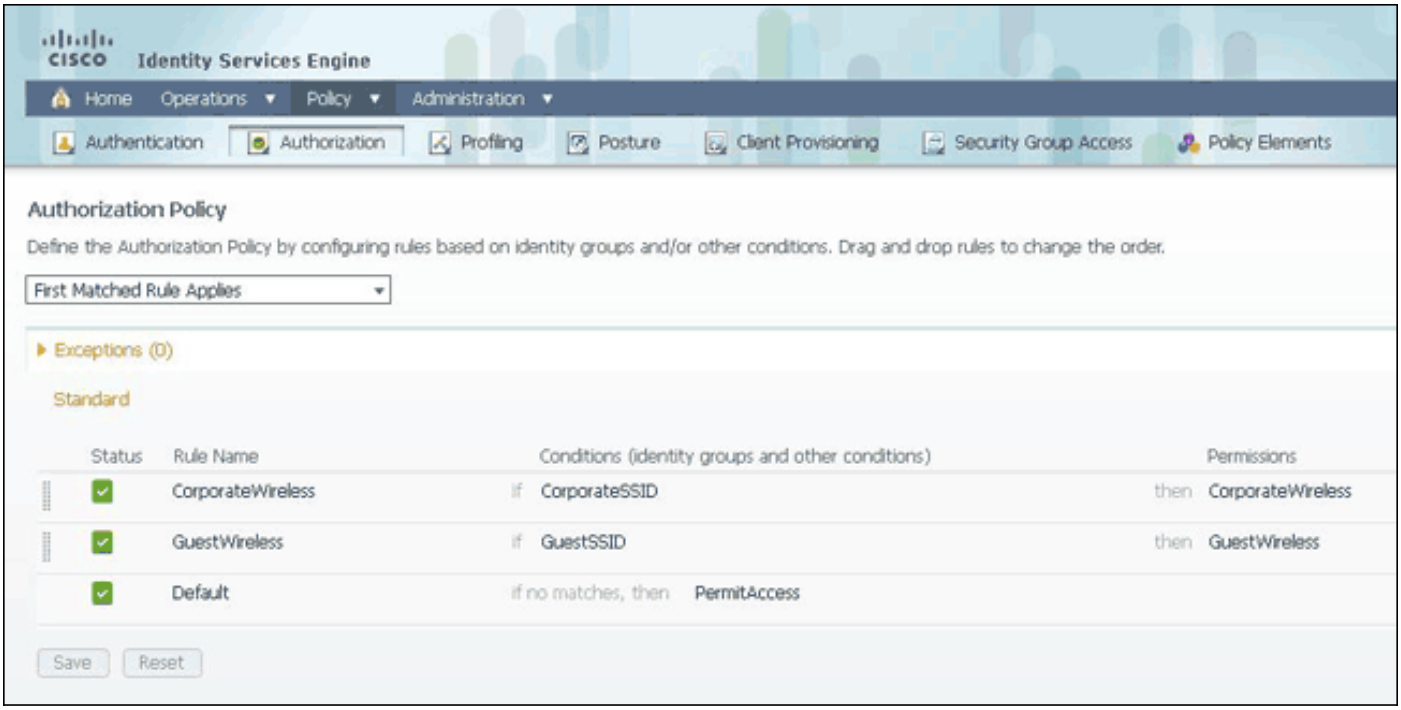
1. Haga clic la flecha hacia abajo a la derecha de una regla existente y elija el **separador de millares una nueva regla**.
2. Ingrese un nombre para su regla del invitado y salga los grupos de la identidad del campo

definido a ningunos.
3. Bajo condiciones, haga clic el más y haga clic la **condición existente selecta de la biblioteca**.
4. Bajo nombre de condición, elija la **condición simple > GuestSSID**.
5. Bajo los permisos, elija el perfil apropiado de la autorización para sus Usuarios invitados.
6. Haga clic en Done (Listo).

Regla corporativa

1. Haga clic la flecha hacia abajo a la derecha de una regla existente y elija el **separador de millares una nueva regla**.
2. Ingrese un nombre para su regla corporativa y salga los grupos de la identidad del campo definido a ningunos.
3. Bajo condiciones, haga clic el más y haga clic la **condición existente selecta de la biblioteca**.
4. Bajo nombre de condición, elija la **condición compuesta > CorporateSSID**.
5. Bajo los permisos, elija el perfil apropiado de la autorización para sus usuarios corporativos.
6. Haga clic en Done (Listo).

Note: Hasta que usted haga clic la salvaguardia en la parte inferior de la lista de la directiva, no se aplicará ningunos cambios realizados en esta pantalla a su despliegue.



Método 2: LLAMAR-ESTACIÓN-ID

El WLC se puede configurar para enviar el nombre SSID en el atributo RADIUS LLAMAR-ESTACIÓN-ID, que a su vez se puede utilizar como condición en el ISE. La ventaja de este atributo es que puede ser utilizado sin importar lo que se fija el ID DE WLAN en al WLC. Por abandono, el WLC no envía el SSID en el atributo Llamar-Estación-ID. Para habilitar esta característica en el WLC, ir a la **Seguridad >AAA > RADIUS > autenticación** y fijar el tipo del ID de la estación de la llamada a la dirección MAC AP: SSID. Esto fija el formato del Llamar-Estación-ID a *<MAC del AP que el usuario está conectando el to>: Name> <SSID*.

Usted puede ver qué nombre SSID va a ser enviado de la página de resumen de la red inalámbrica (WLAN).

Puesto que el atributo Llamar-Estación-identificación también contiene la dirección MAC del AP, una expresión normal (REGEX) se utiliza para hacer juego el nombre SSID en la directiva ISE. Coincidencias del operador las “en la configuración de la condición pueden leer un REGEX del campo de valor.

Ejemplos REGEX

“Comienza con” — por ejemplo, utilice el valor REGEX del **^ (cumbre). *** — esta condición se configura como CERTIFICADO: La cumbre de las COINCIDENCIAS de la organización” (ningunos hacen juego con una condición que comience con “la cumbre”).

“Termina con” — por ejemplo, utilice el valor REGEX de. *** (mktg) $** — esta condición se configura como CERTIFICADO: El mktg de las COINCIDENCIAS de la organización” (ningunos hacen juego con una condición esa los extremos con “el mktg”).

“Contiene” — por ejemplo, utilice el valor REGEX de .*(1234).* — esta condición se configura como CERTIFICADO: La organización HACE JUEGO '1234' (cualquier coincidencia con una condición que contiene el "1234", tal como Eng1234, 1234Dev, y Corp1234Mktg).

¡“No comienza con” — por ejemplo, utilice el valor REGEX del **^ (?! LDAP). *** — esta condición se configura como CERTIFICADO: El LDAP de las COINCIDENCIAS de la organización” (ningunos hacen juego con una condición que no comience con “el LDAP”, por ejemplo el usLDAP o CorpLDAPmktg).

El Llamar-Estación-ID termina con el nombre SSID, así que el REGEX a utilizar en este ejemplo es**. * (: NAME>) <SSID $**. Tenga esto presente como usted pasa con la configuración.

Con los dos SSID arriba, usted puede crear dos reglas con estos requisitos:

A) Los Usuarios invitados deben iniciar sesión al invitado SSID.

B) Los usuarios corporativos deben estar en el grupo “Domain User” AD y deben iniciar sesión al SSID corporativo.

Gobierne A

Gobierne A tiene apenas un requisito, así que usted puede construir una condición simple (basada en los valores antedichos):

1. En el ISE, van a la **directiva > a los elementos > a las condiciones > a la autorización de la directiva > las condiciones simples** y crean una nueva condición.
2. En el campo de nombre, ingrese un nombre de condición.
3. En el campo Description (Descripción), ingrese una descripción (opcional).
4. De la lista desplegable del atributo, elija el **radio - > Called-Station-ID--[30]**.
5. De la lista desplegable del operador, elija las **coincidencias.**
6. De la lista desplegable de valores, elija. *** (: Invitado) $**. Esto es con diferenciación entre mayúsculas y minúsculas.
7. Click **Save**.

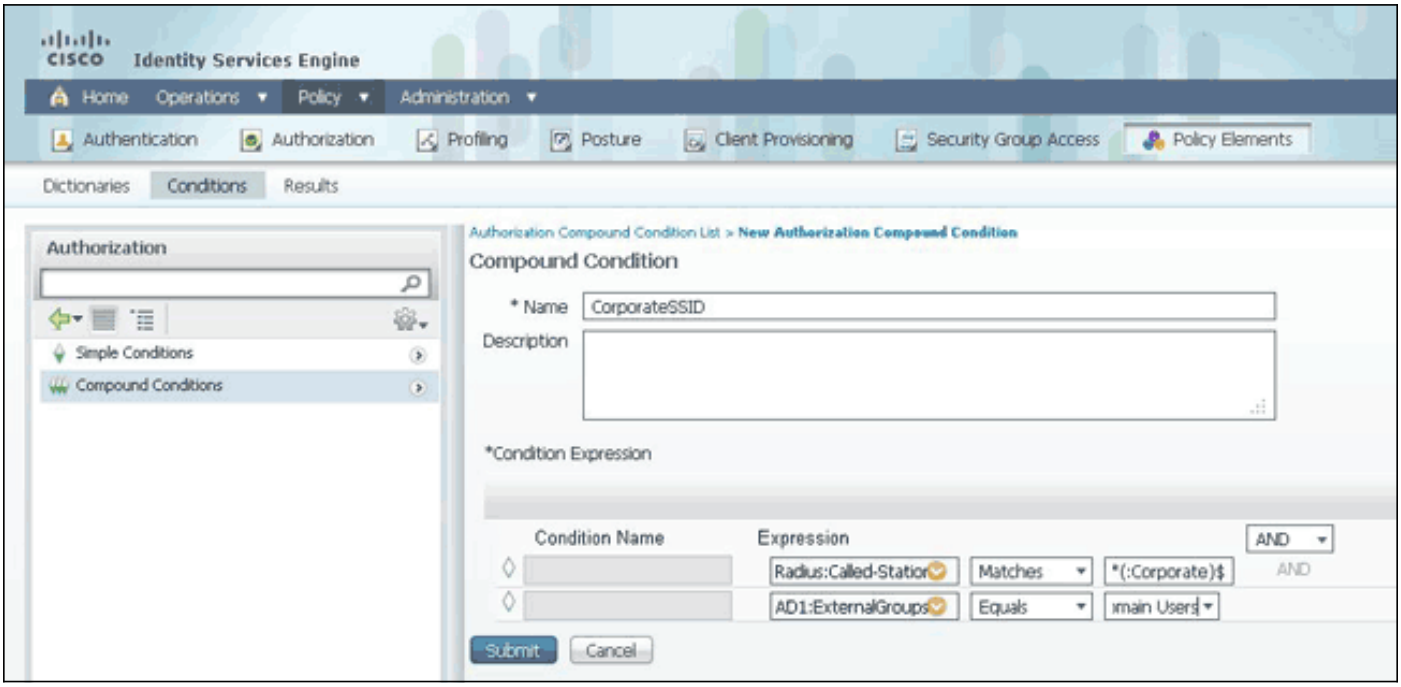
Regla B

La regla B tiene dos requisitos, así que usted puede construir una condición compuesta (basada en los valores antedichos):

1. En el ISE, van a la **directiva > a los elementos > a las condiciones > a la autorización de la directiva > las condiciones compuestas** y crean una nueva condición.
2. En el campo de nombre, ingrese un nombre de condición.
3. En el campo Description (Descripción), ingrese una descripción (opcional).
4. Elija **crean la nueva condición (opción anticipada)**.
5. De la lista desplegable del atributo, elija el **radio - > Called-Station-Id--[30]**.
6. De la lista desplegable del operador, elija las **coincidencias.**
7. De la lista desplegable de valores, elija**. * (:) $ corporativo**. Esto es con diferenciación entre mayúsculas y minúsculas.
8. Haga clic el engranaje a la derecha y elija **agregan el atributo/el valor**.
9. De la lista desplegable del atributo, elija **AD1 > los grupos externos**.
10. De la lista desplegable del operador, elija los **iguales.**
11. De la lista desplegable de valores, seleccione al grupo requerido. En este ejemplo, se fija a

los Domain User.

12. Click **Save**.



Note: En este documento, utilizamos los perfiles simples de la autorización configurados bajo la directiva > los elementos de la directiva > los resultados > la autorización > perfiles de la autorización. Se fijan para permitir el acceso, pero pueden ser adaptados para caber las necesidades de su despliegue.

Ahora que se configuran las condiciones, apliqúelas a una directiva de la autorización. Vaya a la **directiva > a la autorización**. Inserte la regla en la lista en la ubicación apropiada o edite una regla existente.

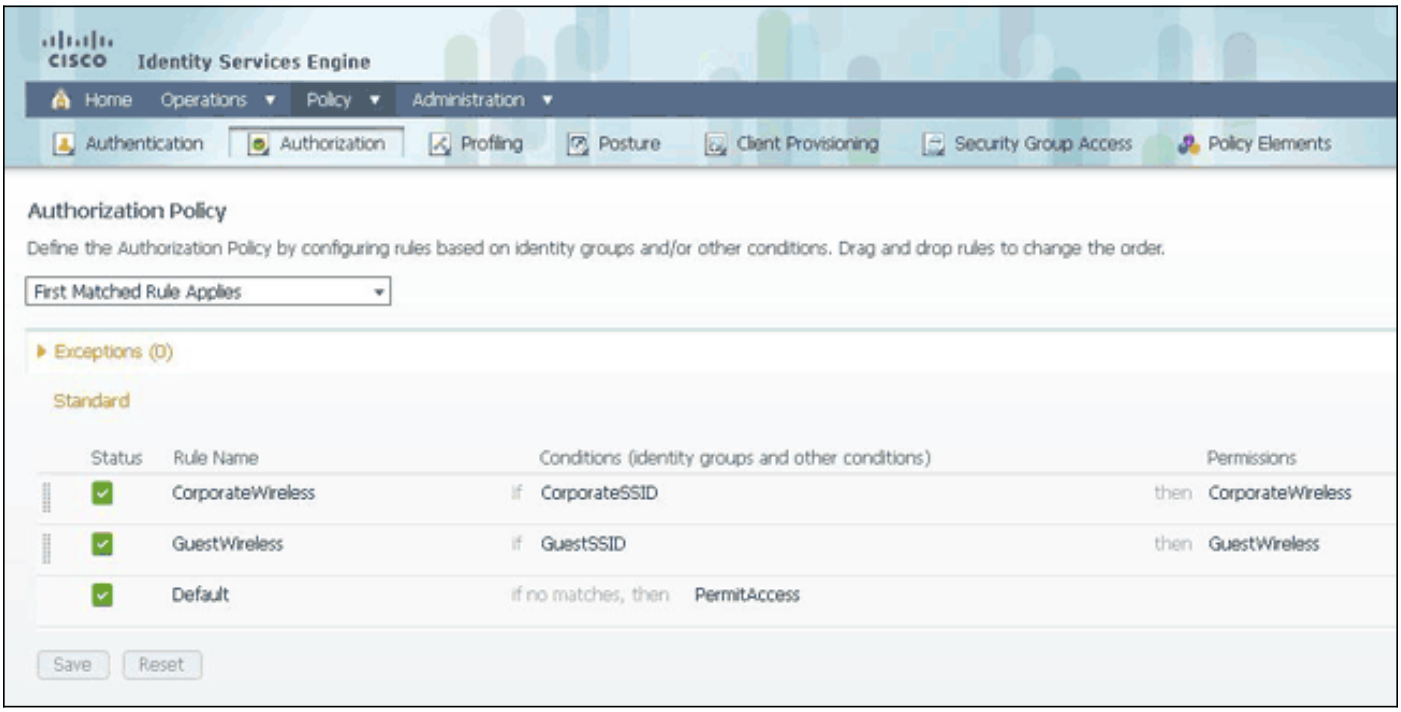
Regla del invitado

1. Haga clic la flecha hacia abajo a la derecha de una regla existente y elija el **separador de millares una nueva regla**.
2. Ingrese un nombre para su regla del invitado y salga los grupos de la identidad del campo definido a ningunos.
3. Bajo condiciones, haga clic el más y haga clic la **condición existente selecta de la biblioteca**.
4. Bajo nombre de condición, elija la **condición simple > GuestSSID**
5. Bajo los permisos, elija el perfil apropiado de la autorización para sus Usuarios invitados.
6. Haga clic en Done (Listo).

Regla corporativa

1. Haga clic la flecha hacia abajo a la derecha de una regla existente y elija el **separador de millares una nueva regla**.
2. Ingrese un nombre para su regla corporativa y salga los grupos de la identidad del campo definido a ningunos.
3. Bajo condiciones, haga clic el más y haga clic la **condición existente selecta de la biblioteca**.
4. Bajo nombre de condición, elija la **condición compuesta > CorporateSSID**.
5. Bajo los permisos, elija el perfil apropiado de la autorización para sus usuarios corporativos.
6. Haga clic en Done (Listo).
7. Haga clic la **salvaguardia** en la parte inferior de la lista de la directiva.

Note: Hasta que usted haga clic la salvaguardia en la parte inferior de la lista de la directiva, no se aplicará ningunos cambios realizados en esta pantalla a su despliegue.



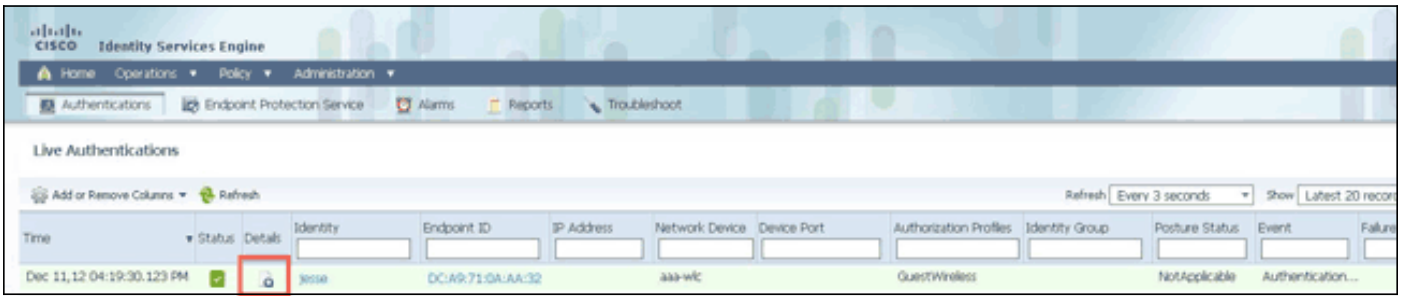
Verificación

Actualmente, no hay un procedimiento de verificación disponible para esta configuración.

Troubleshooting

En esta sección encontrará información que puede utilizar para solucionar problemas de configuración.

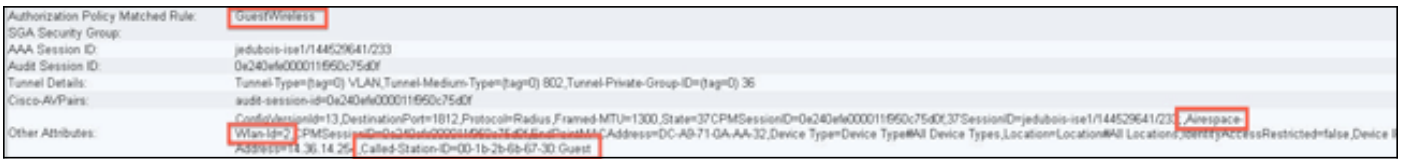
Para descubrir si la directiva fue creada correctamente y aseegurarse el ISE está recibiendo los atributos apropiados, revise el informe detallado de la autenticación para haber pasado o la autenticación fallida para el usuario. Elija las **operaciones > las autenticaciones** y después haga clic el icono de los **detalles** para una autenticación.



Primero, marque el resumen de la autenticación. Esto muestra los fundamentos de la autenticación cuál incluye lo que fue proporcionado el perfil de la autorización al usuario.

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 directiva es incorrecta, los detalles de la autenticación mostrarán qué Airespace-WLAN-identificación y qué Llamar-Estación-identificación fue enviada del WLC. Ajuste sus reglas por consiguiente. La regla correspondida con directiva de la autorización confirma independientemente de si la autenticación está correspondiendo con su regla prevista.



Estas reglas se configuran mal comúnmente. Para revelar el problema de configuración, haga juego la regla contra qué se ve en los detalles de la autenticación. Si usted no ve que los atributos en los otros atributos colocan, aseegurese el WLC se configura correctamente.

Información Relacionada

- Soporte Técnico y Documentación - Cisco Systems