

نيوكت ٤٦٣٣ أ ي ل ع ة م ئ ا ق ل ا ISE ت ا س ا ي س SSID

المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [الاصطلاحات](#)
- [التكوين](#)
- [التكوينات](#)
- [التحقق من الصحة](#)
- [استكشاف الأخطاء وإصلاحها](#)
- [معلومات ذات صلة](#)

المقدمة

يصف هذا المستند كيفية تكوين سياسات التفويض في ISE (Cisco Identity Services Engine) للتمييز بين معرفات مجموعات الخدمات المختلفة (SSIDs). من الشائع جداً أن يكون في المؤسسة عدة SSIDs في شبكتهم اللاسلكية لأغراض مختلفة. أحد أكثر الأغراض شيوعاً هو وجود SSID للشركة للموظفين و SSID ضيف للزائرين في المؤسسة.

يفترض هذا الدليل ما يلي:

1. يتم إعداد وحدة التحكم في الشبكة المحلية اللاسلكية (WLC) وهي تعمل لجميع SSIDs المعنية.
 2. تعمل المصادقة على جميع SSIDs المعنية مقابل ISE.
- مستندات أخرى في هذه السلسلة

- [المصادقة المركزية للويب مع محول ومثال تكوين محرك خدمات الهوية](#)
- [مثال على تكوين مصادقة الويب المركزية على شبكة LAN اللاسلكية \(WLC\) ومحرك خدمات كشف الهوية \(ISE\)](#)
- [حسابات ضيف ISE لمثال تكوين مصادقة RADIUS/802.1x](#)
- [VPN Inline Posture \(وضعية الشبكة الخاصة الظاهرية \(VPN\) باستخدام ISE iPEP و ASA\)](#)

المتطلبات الأساسية

المتطلبات

لا توجد متطلبات خاصة لهذا المستند.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات البرامج والمكونات المادية التالية:

- وحدة تحكم الشبكة المحلية (LAN) اللاسلكية الإصدار 7.3.101.0
- Identity Services Engine الإصدار 1.1.2.145
- تتضمن الإصدارات السابقة أيضا كل من هذه الميزات.

تم إنشاء المعلومات الواردة في هذا المستند من الأجهزة الموجودة في بيئة معملية خاصة. بدأت جميع الأجهزة المستخدمة في هذا المستند بتكوين ممسوح (افتراضي). إذا كانت شبكتك مباشرة، فتأكد من فهمك للتأثير المحتمل لأي أمر.

[الاصطلاحات](#)

راجع [اصطلاحات تلميحات Cisco التقنية للحصول على مزيد من المعلومات حول اصطلاحات المستندات.](#)

[التكوين](#)

في هذا القسم، تُقدّم لك معلومات تكوين الميزات الموضحة في هذا المستند.

ملاحظة: أستخدم [أداة بحث الأوامر](#) (للعلماء [المسجلين](#) فقط) للحصول على مزيد من المعلومات حول الأوامر المستخدمة في هذا القسم.

[التكوينات](#)

يستخدم هذا المستند التكوينات التالية:

• الطريقة 1: Airespace-WLAN-id

• الطريقة 2: Call-Station-ID

يجب استخدام طريقة تكوين واحدة فقط في كل مرة. وإذا تم تنفيذ كلا التكوينين في نفس الوقت، فإن المبلغ الذي تتم معالجته بواسطة معيار ISE يزيد ويؤثر على إمكانية قراءة القاعدة. يراجع هذا وثيقة المزاي والعيوب من كل تشكيل طريقة.

[الطريقة 1: Airespace-WLAN-id](#)

تحتوي كل شبكة محلية لاسلكية (WLAN) تم إنشاؤها على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) على معرف شبكة محلية لاسلكية (WLAN). يتم عرض معرف WLAN في صفحة ملخص WLAN.

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN	Corporate	Corporate	Enabled	[WPA2][Auth(802.1X)]
2	WLAN	Guest	Guest	Enabled	MAC Filtering

عندما يتصل عميل ب SSID، يحتوي طلب RADIUS إلى ISE على سمة Airespace-WLAN-ID. يتم استخدام هذه السمة البسيطة لاتخاذ قرارات النهج في ISE. يتمثل أحد عيوب هذه السمة في حالة عدم تطابق معرف الشبكة المحلية اللاسلكية (WLAN) مع توزيع SSID عبر وحدات تحكم متعددة. إذا كان هذا يصف عملية النشر الخاصة بك، فتابع إلى الأسلوب 2.

في هذه الحالة، استعملت Airespace-wlan-id كشرط. يمكن استخدامه كشرط بسيط (بحد ذاته) أو في حالة مركبة (بالاشتراك مع سمة أخرى) لتحقيق النتيجة المطلوبة. يغطي هذا المستند كلا من حالات الاستخدام. يمكن إنشاء هاتين القاعدتين مع وجود نوعي SSIDs أعلاه.

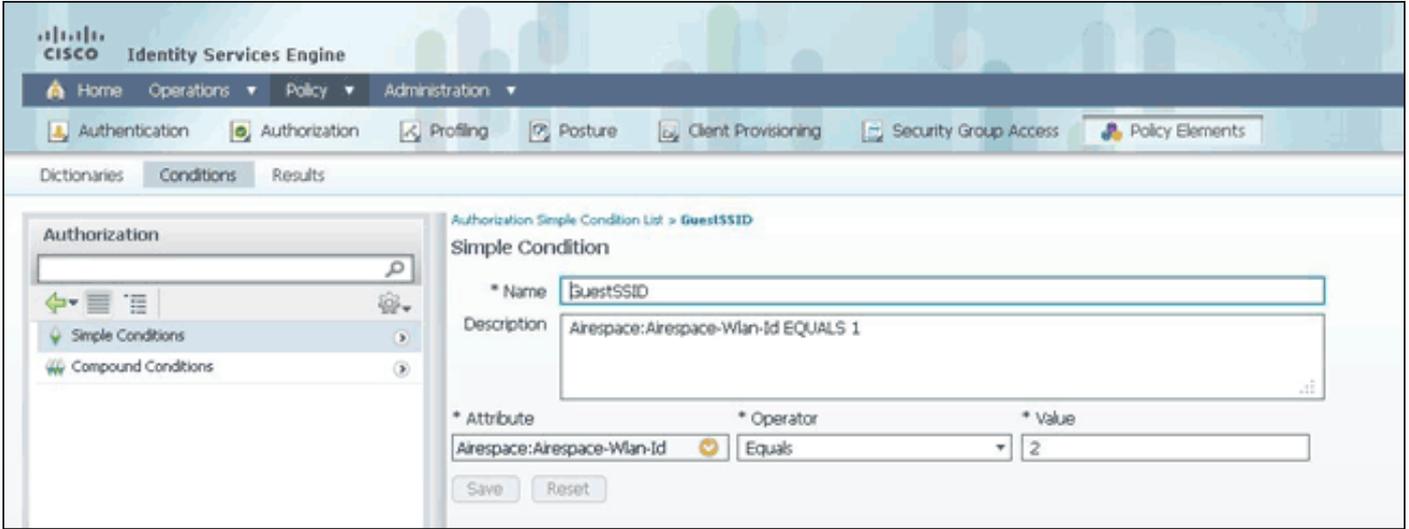
أ) يجب على المستخدمين الضيوف تسجيل الدخول إلى SSID للضيف.

ب) يجب أن يكون المستخدمون المشتركون ضمن مجموعة "مستخدمي المجال" في خدمة (Active Directory (AD ويجب عليهم تسجيل الدخول إلى SSID الخاصة بالشركة.

القاعدة ألف

القاعدة أ لها متطلب واحد فقط، لذلك يمكنك بناء شرط بسيط (بناء على القيم أعلاه):

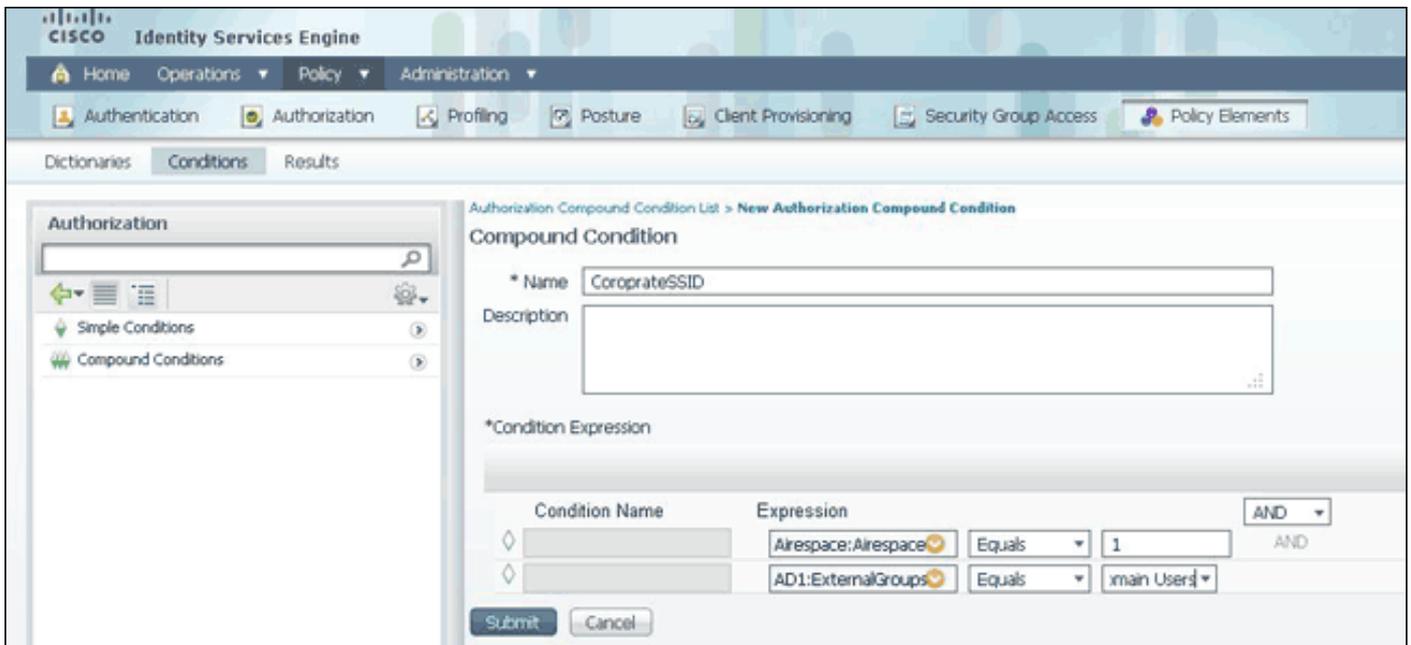
1. في ISE، انتقل إلى السياسة < عناصر السياسة < الشروط < التخويل < الشروط البسيطة وقم بإنشاء شرط جديد.
2. في حقل الاسم، أدخل اسم الشرط.
3. دخلت في الوصف مجال، وصف (إختياري).
4. من القائمة المنسدلة سم، اختر 1 [Airespace > Airespace-WLAN-ID].
5. من القائمة المنسدلة المشغل، اختر يساوي.
6. من القائمة المنسدلة "القيمة"، اختر 2.
7. طقطقة حفظ.



القاعدة باء

القاعدة ب لها متطلبان، بحيث يمكنك بناء حالة مركبة (بناء على القيم أعلاه):

1. في ISE، انتقل إلى السياسة < عناصر السياسة < الشروط < التخويل < الشروط المركبة وقم بإنشاء شرط جديد.
2. دخلت في الإسم مجال، شرط إسم.
3. دخلت في الوصف مجال، وصف (إختياري).
4. اختر إنشاء شرط جديد (خيار متقدم).
5. من القائمة المنسدلة سم، اختر 1 [Airespace > Airespace-WLAN-ID].
6. من القائمة المنسدلة المشغل، اختر يساوي.
7. من القائمة المنسدلة "القيمة"، اختر 1.
8. انقر على العتاد إلى اليمين واختر إضافة سم/قيمة.
9. من القائمة المنسدلة سم، اختر AD1 < مجموعات خارجية.
10. من القائمة المنسدلة المشغل، اختر يساوي.
11. من القائمة المنسدلة "القيمة"، حدد المجموعة المطلوبة. في هذا المثال، يتم تعيينها على مستخدمي المجال.
12. طقطقة حفظ.



ملاحظة: في هذا المستند، نستخدم توصيفات تخويل بسيطة مكونة في إطار السياسة < عناصر السياسة > النتائج < التخويل > توصيفات التخويل. وهي مصممة للسماح بالوصول، ولكن يمكن تكييفها لتلائم إحتياجات عملية النشر لديك.

الآن بعد أن أصبحت لدينا الشروط، يمكننا تطبيقها على نهج التخويل. انتقل إلى السياسة < التخويل. حدد مكان إدراج القاعدة في القائمة أو تحرير القاعدة الموجودة.

قاعدة الضيف

1. انقر فوق السهم لأسفل على يمين القاعدة الموجودة واختر إدراج قاعدة جديدة.
2. أدخل اسما لقاعدة الضيف الخاصة بك واترك حقل مجموعات الهوية معين إلى أي.
3. تحت الشروط، انقر فوق علامة الجمع وانقر فوق تحديد شرط موجود من المكتبة.
4. تحت اسم الشرط، اختر شرط بسيط < GuestSSID.
5. تحت الأذونات، اختر ملف تعريف التخويل المناسب للمستخدمين الضيوف.
6. طقطقة تم.

قاعدة الشركة

1. انقر فوق السهم لأسفل على يمين القاعدة الموجودة واختر إدراج قاعدة جديدة.
2. أدخل اسما لقاعدة الشركة وترك حقل مجموعات الهوية معين إلى أي.
3. تحت الشروط، انقر فوق علامة الجمع وانقر فوق تحديد شرط موجود من المكتبة.
4. تحت اسم الشرط، اختر شرط مركب < CorporateSSID.
5. بموجب أذن، اختر ملف تعريف التخويل المناسب لمستخدميك في الشركة.
6. طقطقة تم.

ملاحظة: لن يتم تطبيق أي تغييرات يتم إجراؤها على هذه الشاشة على عملية النشر الخاصة بك حتى تنقر فوق "حفظ" في أسفل قائمة النهج.

Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.

First Matched Rule Applies

Exceptions (0)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
On	CorporateWireless	if CorporateSSID	then CorporateWireless
On	GuestWireless	if GuestSSID	then GuestWireless
On	Default	if no matches, then	PermitAccess

Save Reset

الطريقة 2: Call-Station-ID

يمكن تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لإرسال اسم SSID في سمة Call-Station-ID، والتي يمكن استخدامها بدورها كشرط في ISE. ميزة هذه السمة هي أنه يمكن استخدامها بغض النظر عما تم تعيين معرف WLAN عليه على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). لا تقوم عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) بإرسال SSID في سمة Call-Station-ID بشكل افتراضي. لتمكين هذه الميزة على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، انتقل إلى الأمان < RADIUS > AAA < المصادقة ووضبط نوع معرف محطة الاتصال على عنوان AP MAC:SSID. يعمل هذا على تعيين تنسيق معرف المحطة المستدعى إلى < Mac نقطة الوصول التي يتصل بها المستخدم>: < اسم SSID>.

RADIUS Authentication Servers

Call Station ID Type: AP MAC Address:SSID

Use AES Key Wrap: (Designed for FIPS customers and requires a key wrap compliant RADIUS server)

MAC Delimiter: Hyphen

Network User	Management	Server Index	Server Address	Port	IPsec	Admin Status

يمكنك مشاهدة اسم SSID الذي سيتم إرساله من صفحة ملخص WLAN.

WLANs

Current Filters: None [Change Filter] [Clear Filter] Create New Go

WLAN ID	Type	Profile Name	WLAN SSID	Admin Status	Security Policies
1	WLAN	Corporate	Corporate	Enabled	[WPA2][Auth(802.1X)]
2	WLAN	Guest	Guest	Enabled	MAC Filtering

ونظرا لأن سمة Call-Station-ID تحتوي أيضا على عنوان MAC لنقطة الوصول، يتم استخدام تعبير عادي (REGEX) لمطابقة اسم SSID في نهج ISE. يمكن للعامل 'Match' في تكوين الشرط قراءة REGEX من حقل القيمة.

'يبدأ ب-' على سبيل المثال، أستخدم قيمة regex الخاصة ب ^ (ACME).*- يتم تكوين هذا الشرط ك CERTIFICATE:Organization تطابق المؤسسة 'ACME' (أي تطابق مع شرط يبدأ ب "ACME").

'end ب-' على سبيل المثال، أستخدم قيمة REGEX من *(mktg)\$— يتم تكوين هذا الشرط ك CERTIFICATE:Organization تطابق 'mktg' (أي تطابق مع شرط ينتهي ب "mktg").

'contains'— على سبيل المثال، أستخدم قيمة regex الخاصة ب *(1234).*- تم تكوين هذا الشرط ك CERTIFICATE:Organization تطابق '1234' (أي تطابق مع شرط يحتوي على "1234"، مثل Eng1234 و 1234Dev و Corp1234MKTG).

'لا يبدأ ب-' على سبيل المثال، أستخدم قيمة REGEX الخاصة ب ^ (LDAP!?!)*.*- تم تكوين هذا الشرط ك CERTIFICATE:Organization تطابق 'LDAP' (أي تطابق مع شرط لا يبدأ ب "LDAP"، مثل USldap أو CorpLDAPmktg).

ينتهي Call-Station-ID باسم SSID، لذلك فإن regex المطلوب إستخدامه في هذا المثال هو: (<Name>\$). تذكر هذا دائما عند الانتقال من خلال التكوين.

مع وجود نوعي SSID أعلاه، يمكنك إنشاء قاعدتين مع هذه المتطلبات:

(أ) يجب على المستخدمين الضيوف تسجيل الدخول إلى SSID للضيف.

(ب) يجب أن يكون المستخدمون من الشركات في المجموعة AD "مستخدمو المجال" ويجب أن يسجلوا الدخول إلى SSID للشركة.

القاعدة ألف

القاعدة أ لها متطلب واحد فقط، لذلك يمكنك بناء شرط بسيط (بناء على القيم أعلاه):

1. في ISE، انتقل إلى السياسة < عناصر السياسة < الشروط < التخويل < الشروط البسيطة وقم بإنشاء شرط جديد.
2. دخلت في الإسم مجال، شرط إسم.
3. دخلت في الوصف مجال، وصف (إختياري).
4. من القائمة المنسدلة "سمات"، أختار [RADIUS -> Call-Station-ID—30].
5. من القائمة المنسدلة المشغل، أختار تطابقت.
6. من القائمة المنسدلة القيمة، أختار *(Guest:\$). هذا حساس لحالة الأحرف.
7. طقطقة حفظ.

The screenshot shows the Cisco Identity Services Engine (ISE) web interface. The top navigation bar includes 'Home', 'Operations', 'Policy', and 'Administration'. Below this, there are tabs for 'Authentication', 'Authorization', 'Profiling', 'Posture', 'Client Provisioning', 'Security Group Access', and 'Policy Elements'. The main content area is titled 'Authorization Simple Condition List > New Authorization Simple Condition'. The form fields are: Name: GuestSSID, Description: (empty), Attribute: Radius:Called-Station-ID, Operator: Matches, and Value: *(Guest)\$.

القاعدة ب لها متطلبان، بحيث يمكنك بناء حالة مركبة (بناء على القيم أعلاه):

1. في ISE، انتقل إلى السياسة < عناصر السياسة < الشروط < التخويل < الشروط المركبة وقم بإنشاء شرط جديد.
2. دخلت في الإسم مجال، شرط إسم.
3. دخلت في الوصف مجال، وصف (إختياري).
4. أختار إنشاء شرط جديد (خيار متقدم).
5. من القائمة المنسدلة "سمات"، أختار [RADIUS -> Call-Station-ID—30].
6. من القائمة المنسدلة المشغل، أختار تطابقات.
7. من القائمة المنسدلة القيمة، أختار *(الشركة)\$\$. هذا حساس لحالة الأحرف.
8. انقر على العتاد إلى اليمين واختر إضافة سمة/قيمة.
9. من القائمة المنسدلة سمة، أختار AD1 < مجموعات خارجية.
10. من القائمة المنسدلة المشغل، أختار يساوي.
11. من القائمة المنسدلة "القيمة"، حدد المجموعة المطلوبة. في هذا المثال، يتم تعيينها على مستخدمى المجال.
12. طقطقة حفظ.

ملاحظة: في هذا المستند كله، نستخدم توصيفات تفويض بسيطة تم تكوينها في إطار السياسة < عناصر السياسة < النتائج < التخويل < توصيفات التخويل. وهي مصممة للسماح بالوصول، ولكن يمكن تكييفها لتلائم احتياجات عملية النشر لديك.

الآن بعد تكوين الشروط، قم بتطبيقها على نهج التخويل. انتقل إلى السياسة < التخويل. قم بإدراج القاعدة في القائمة في الموقع المناسب أو تحرير قاعدة موجودة.

قاعدة الضيف

1. انقر فوق السهم لأسفل على يمين القاعدة الموجودة واختر إدراج قاعدة جديدة.
2. أدخل اسما لقاعدة الضيف الخاصة بك واترك حقل مجموعات الهوية معين إلى أي.
3. تحت الشروط، انقر فوق علامة الجمع وانقر فوق تحديد شرط موجود من المكتبة.
4. تحت اسم الشرط، أختار شرط بسيط < GuestSSID.
5. تحت الأدونات، أختار ملف تعريف التخويل المناسب للمستخدمين الضيوف.
6. طقطقة تم.

قاعدة الشركة

1. انقر فوق السهم لأسفل على يمين القاعدة الموجودة واختر إدراج قاعدة جديدة.
 2. أدخل اسما لقاعدة الشركة وترك حقل مجموعات الهوية معين إلى أي.
 3. تحت الشروط، انقر فوق علامة الجمع وانقر فوق تحديد شرط موجود من المكتبة.
 4. تحت اسم الشرط، اختر شرط مركب < CorporateSSID.
 5. بموجب أذون، اختر ملف تعريف التحويل المناسب لمستخدميك في الشركة.
 6. طقطقة تم.
 7. انقر فوق حفظ في أسفل قائمة النهج.
- ملاحظة: لن يتم تطبيق أي تغييرات يتم إجراؤها على هذه الشاشة على عملية النشر الخاصة بك حتى تنقر فوق "حفظ" في أسفل قائمة النهج.

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
On	CorporateWireless	if CorporateSSID	then CorporateWireless
On	GuestWireless	if GuestSSID	then GuestWireless
On	Default	if no matches, then	PermitAccess

التحقق من الصحة

لا يوجد حالياً إجراء للتحقق من صحة هذا التكوين.

استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

لمعرفة ما إذا تم إنشاء النهج بشكل صحيح والتأكد من أن ISE يتلقى السمات المناسبة، راجع تقرير المصادقة التفصيلي لمصادقة تم تمريرها أو فشلت للمستخدم. اختر عمليات < مصادقة ثم انقر على رمز التفاصيل لمصادقة ما.

Time	Status	Identity	Endpoint ID	IP Address	Network Device	Device Port	Authorization Profiles	Identity Group	Posture Status	Event	Failure
Dec 11, 12 04:19:30.123 PM	On	jesse	DC:A9:71:5A:AA:32	aaa-wlc	aaa-wlc	GuestWireless	NotApplicable	Authentication...			

تحقق أولاً من ملخص المصادقة. وهذا يوضح أساسيات المصادقة التي تتضمن ما تم توفيره من ملف تعريف التحويل للمستخدم.

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)

إذا كان النهج غير صحيح، فستظهر تفاصيل المصادقة معرف Airespace-WLAN ومعرف المتصل-Station الذي تم إرساله من عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). عدل القواعد وفقاً لذلك. تؤكد "قاعدة نهج التحويل المطابقة" ما إذا كانت المصادقة مطابقة للقاعدة المقصودة أم لا.

Authorization Policy Matched Rule:	GuestWireless
SGA Security Group:	
AAA Session ID:	jedubois-ise1/144529641/233
Audit Session ID:	0e240ef6000011950c75d0f
Tunnel Details:	Tunnel-Types=(tag=0) VLAN,Tunnel-Medium-Types=(tag=0) 802,Tunnel-Private-Group-ID=(tag=0) 35
Cisco-AirPair:	audit-session-id=0e240ef6000011950c75d0f
Other Attributes:	ConfigId=13, DestinationPort=1812, Protocol=Radius, Framed-MTU=1300, State=37, CPMSessionID=0e240ef6000011950c75d0f, SessionID=jedubois-ise1/144529641/233, Airespace=Wan12, PMSessionID=0e240ef6000011950c75d0f, DeviceMACAddress=DC-A9-71-0A-AA-32, DeviceType=DeviceType#N1, DeviceTypes=Location#All, Location=Jedubois, AccessRestricted=false, DeviceAddress=14.36.14.254, Called-Station-ID=00-1b-2b-6b-67-30, Guest

عادة ما تكون هذه القواعد سيئة التكوين. للكشف عن مشكلة التكوين، قم بمطابقة القاعدة مقابل ما يظهر في تفاصيل المصادقة. إذا لم ترى السمات في حقل سمات أخرى، تأكد من تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) بشكل صحيح.

معلومات ذات صلة

• [الدعم التقني والمستندات - Cisco Systems](#)

ةمچرتل هذه لوج

ةللأل تاي نقتل نم ةومچم مادختساب دن تسمل اذه Cisco تچرت
ملاعلاء انءمچ يف نيمدختسمل معدى وتحم مي دقتل ةيرشبل او
امك ةقيد نوك تنل ةللأل ةمچرت لصف انءمچم لىچرئى. ةصاغل متهتبل ب
Cisco يلخت. فرتحم مچرت مامدقئى تلى ةيفارتحال ةمچرتل عم لالحل وه
ىلإ أمئاد عوچرلاب ي صؤتو تامچرتل هذه ةقदन ةتئىل وئىسم Cisco
Systems (رفوتم طبارل) ي لصلأل يزلچنل دن تسمل