

اياتاذ لجسمل ا فيضلا لخدم نيوكت لاثم ISE نم 1.3 رادصلل

المحتويات

- [المقدمة](#)
- [المتطلبات الأساسية](#)
- [المتطلبات](#)
- [المكونات المستخدمة](#)
- [الطوبولوجيا والتدفق](#)
- [التكوين](#)
- [WLC](#)
- [محرك خدمات كشف الهوية \(ISE\)](#)
- [التحقق من الصحة](#)
- [استكشاف الأخطاء وإصلاحها](#)
- [التهيئة الاختيارية](#)
- [إعدادات التسجيل الذاتي](#)
- [إعدادات ضيف تسجيل الدخول](#)
- [إعدادات تسجيل الجهاز](#)
- [إعدادات توافق جهاز الضيف](#)
- [إعدادات BYOD](#)
- [الحسابات المعتمدة من الكفيل](#)
- [تقديم بيانات الاعتماد عبر خدمة SMS](#)
- [تسجيل الأجهزة](#)
- [وضعية](#)
- [بيود](#)
- [تغيير شبكة VLAN](#)
- [معلومات ذات صلة](#)

المقدمة

يحتوي الإصدار 1.3 من ISE (Cisco Identity Services Engine) على نوع جديد من Guest Portal يسمى Self Registered Guest Portal، والذي يسمح للمستخدمين الضيوف بالتسجيل الذاتي عند حصولهم على حق الوصول إلى موارد الشبكة. تسمح لك هذه البوابة بتكوين ميزات متعددة وتخصيصها. يوضح هذا المستند كيفية تكوين هذه الوظيفة واستكشاف أخطائها وإصلاحها.

المتطلبات الأساسية

المتطلبات

Cisco يوصي أن يتلقى أنت خبرة مع ISE تشكيل ومعرفة الأساسية من هذا موضوع:

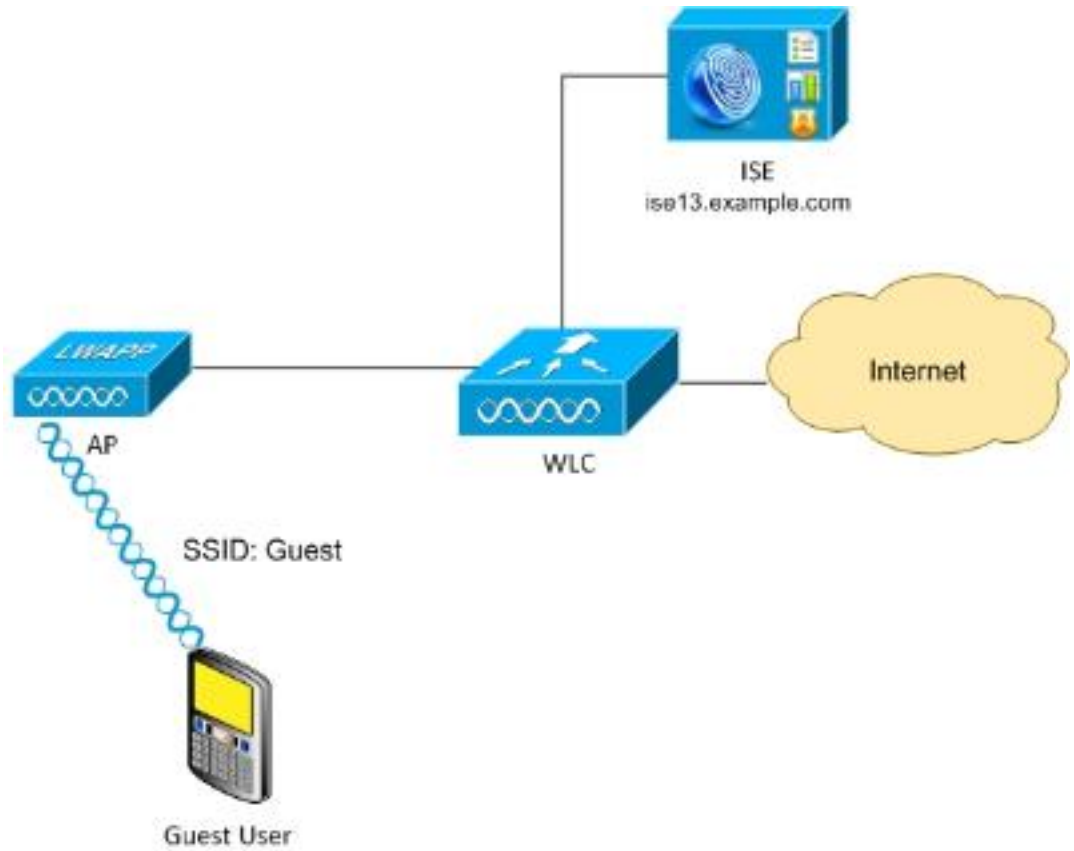
- عمليات نشر ISE وتدفق الضيوف
- تكوين وحدات التحكم في الشبكة المحلية (LAN) اللاسلكية (WLC)

المكونات المستخدمة

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

- نظام التشغيل Microsoft Windows 7
- Cisco WLC، الإصدار 7.6 والإصدارات الأحدث
- برنامج ISE، الإصدار 3.1 والإصدارات الأحدث

الطوبولوجيا والتدفق



يقدم هذا السيناريو خيارات متعددة متاحة للمستخدمين الضيوف عند إجراء التسجيل الذاتي.

فيما يلي التدفق العام:

الخطوة 1. إرتباطات المستخدم الضيف لمعرفة مجموعة الخدمة (SSID): الضيف. هذه شبكة مفتوحة مع تصفية MAC باستخدام ISE للمصادقة. تطابق هذه المصادقة قاعدة التحويل الثانية في ISE ويتم إعادة توجيه ملف تعريف التحويل إلى المدخل المسجل ذاتيا للضيف. ترجع ISE قبول وصول RADIUS باستخدام أزواج Cisco-AV:

- قائمة التحكم في الوصول إلى url-redirect-acl (حركة المرور التي يجب إعادة توجيهها، واسم قائمة التحكم في الوصول (ACL) المحدد محليا على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC))
- إعادة توجيه URL (حيث يتم إعادة توجيه حركة المرور هذه إلى ISE)

الخطوة 2. تتم إعادة توجيه المستخدم الضيف إلى ISE. بدلا من توفير بيانات الاعتماد لتسجيل الدخول، يقوم المستخدم بالنقر فوق "ليس لديك حساب". تتم إعادة توجيه المستخدم إلى صفحة يمكن إنشاء هذا الحساب فيها. قد

يتم تمكين رمز تسجيل سري إختياري من أجل تقييد امتياز التسجيل الذاتي للأشخاص الذين يعرفون هذه القيمة السرية. بعد إنشاء الحساب، يتم توفير بيانات اعتماد المستخدم (اسم المستخدم وكلمة المرور) وتسجيل الدخول باستخدام بيانات الاعتماد هذه.

الخطوة 3. ISE يرسل تغيير RADIUS للتحويل (reauthentication) CoA إلى ال WLC. يقوم WLC بإعادة مصادقة المستخدم عندما يرسل RADIUS Access-Request بسمة التحويل فقط. تستجيب ISE باستخدام قائمة التحكم في الوصول (ACL) الخاصة ب Airespace والمحددة محليا على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)، والتي توفر الوصول إلى الإنترنت فقط (يعتمد الوصول النهائي للمستخدم الضيف على سياسة التحويل).

لاحظ أنه بالنسبة لجلسات عمل بروتوكول المصادقة المتوسع (EAP)، يجب على ISE إرسال إنهاء خدمة CoA من أجل تشغيل إعادة المصادقة لأن جلسة EAP تكون بين المقدم و ISE. ولكن بالنسبة ل MAB (تصفية MAC)، تكون إعادة مصادقة CoA كافية، ولا حاجة إلى إلغاء الاقتران/إلغاء مصادقة العميل اللاسلكي.

الخطوة 4. لدى المستخدم الضيف حق الوصول المرغوب إلى الشبكة.

يمكن تمكين العديد من الميزات الإضافية مثل الوضع وجلب الجهاز الخاص بك (BYOD) (ستتم مناقشته لاحقا).

التكوين

WLC

1. إضافة خادم RADIUS الجديد للمصادقة والمحاسبة. انتقل إلى الأمان < RADIUS > AAA < المصادقة لتمكين RADIUS CoA (RFC 3576).

The screenshot shows the Cisco WLC configuration interface for RADIUS Authentication Servers. The top navigation bar includes 'MONITOR', 'WLANs', 'CONTROLLER', 'WIRELESS', and 'SECURITY'. The left sidebar shows the 'Security' menu with 'AAA' expanded to 'RADIUS'. The main content area is titled 'RADIUS Authentication Servers > Edit' and displays the following configuration details:

Server Index	2
Server Address	10.62.97.21
Shared Secret Format	ASCII
Shared Secret	...
Confirm Shared Secret	...
Key Wrap	<input type="checkbox"/> (Designed for FIPS custome
Port Number	1812
Server Status	Enabled
Support for RFC 3576	Enabled
Server Timeout	5 seconds
Network User	<input checked="" type="checkbox"/> Enable
Management	<input checked="" type="checkbox"/> Enable
IPSec	<input type="checkbox"/> Enable

هناك تكوين مشابه للمحاسبة. ينصح أيضا بتكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) لإرسال SSID في سمة معرف المحطة المتصل، والتي تسمح ل ISE بتكوين القواعد المرنة استنادا إلى SSID:

Security

RADIUS Authentication Servers

Acct Call Station ID Type [1](#) IP Address

Auth Call Station ID Type AP MAC Address:SSID

2. تحت علامة التبويب شبكات WLAN، قم بإنشاء ضيف شبكة LAN اللاسلكية (WLAN) وتكوين الواجهة الصحيحة. ضبط تأمين الطبقة 2 إلى لا شيء باستخدام تصفية MAC. في خوادم الأمان/المصادقة والتفويض والمحاسبة (AAA)، حدد عنوان IP ISE لكل من المصادقة والمحاسبة. على علامة التبويب خيارات متقدمة، قم بتعيين تجاوز AAA وتعيين حالة التحكم في الدخول إلى الشبكة (NAC) على RADIUS NAC (دعم CoA).

3. انتقل إلى الأمان < قوائم التحكم في الوصول < قوائم التحكم في الوصول وقم بإنشاء قائمتي وصول:

GuestRedirect، الذي يسمح بحركة المرور التي لا ينبغي إعادة توجيهها ويعيد توجيه جميع حركة المرور الأخرى للإنترنت، الذي يتم رفضه لشبكات الشركات وبسمح به لجميع الشبكات الأخرى

هنا مثال لقائمة التحكم بالوصول (ACL) الخاصة ب GuestRedirect (يلزم إستثناء حركة المرور من/إلى ISE من إعادة التوجيه):

Security

Access Control Lists > Edit

General

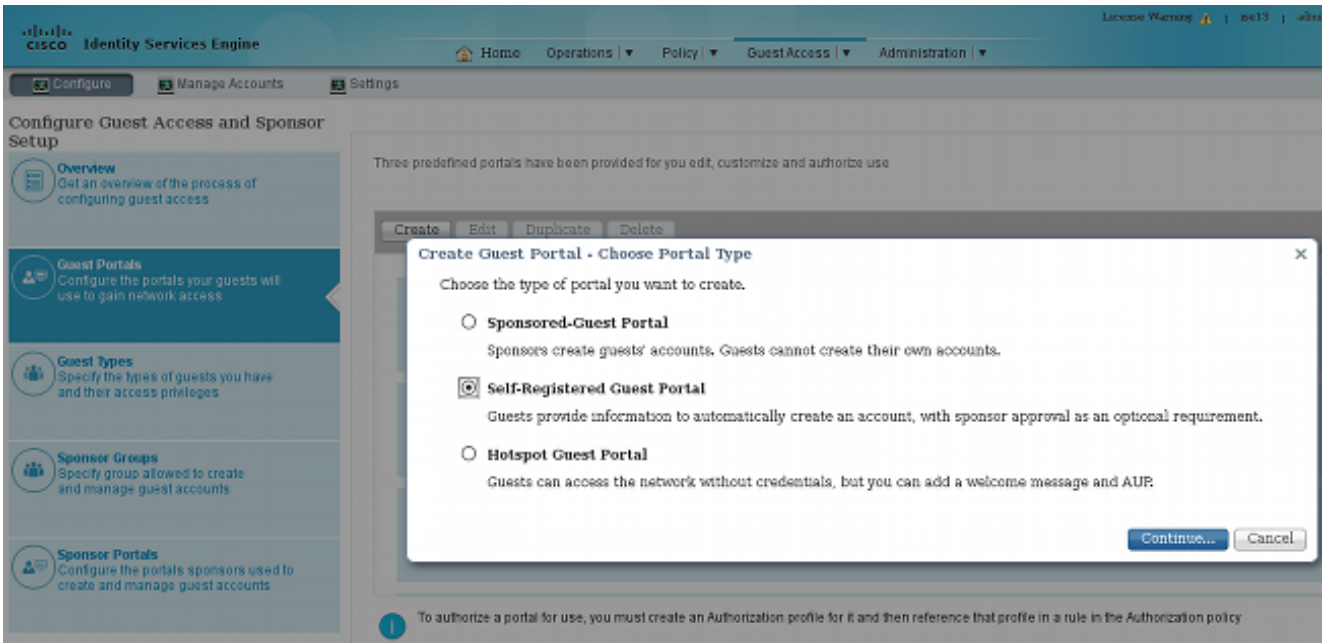
Access List Name GuestRedirect

Deny Counters 0

Seq	Action	Source IP/Mask	Destination IP/Mask	Protocol	Source Port	Dest Port	DSCP	Direction
1	Permit	10.62.97.21 /	0.0.0.0 /	Any	Any	Any	Any	Any
2	Permit	255.255.255.255 /	0.0.0.0 /	Any	Any	Any	Any	Any
		0.0.0.0 /	10.62.97.21 /	Any	Any	Any	Any	Any
		0.0.0.0 /	255.255.255.255 /	Any	Any	Any	Any	Any

محرك خدمات كشف الهوية (ISE)

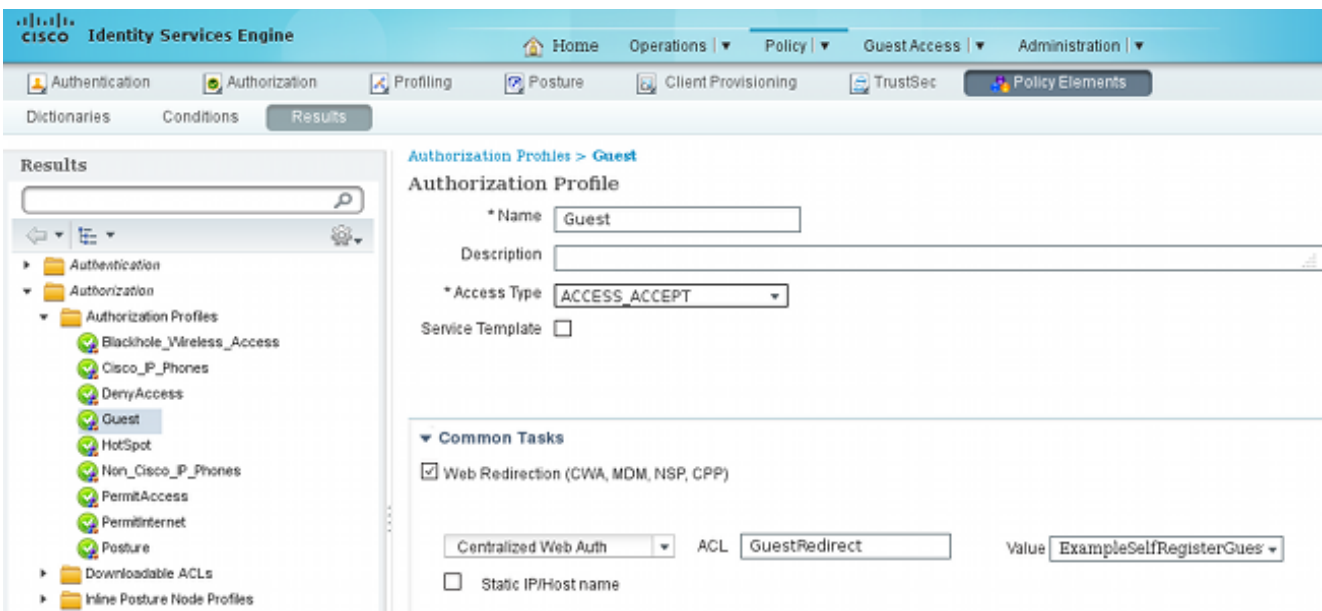
انتقل إلى Guest Access (وصول الضيف) < Configure (تكوين) < Guest Portal (بوابات الضيف)، ثم قم بإنشاء نوع مدخل جديد، مدخل الضيف المسجل ذاتيا:



أختر اسم المدخل الذي ستم الإشارة إليه في ملف تعريف التحويل. اضبط كل الإعدادات الأخرى على القيمة الافتراضية. تحت "تخصيص صفحة المدخل"، يمكن تخصيص كافة الصفحات المعروضة.

تكوين ملفات تعريف التحويل:

Guest (مع إعادة التوجيه إلى اسم مدخل Guest و ACL GuestRedirect)



PermitInternet (مع Airespace ACL Equal Internet)

The screenshot shows the Cisco Identity Services Engine (ISE) interface. The top navigation bar includes 'Home', 'Operations', and 'Policy'. Below the navigation bar, there are tabs for 'Authentication', 'Authorization', 'Profiling', 'Posture', and 'Client Provisioning'. The 'Results' tab is active, showing a search bar and a tree view of the configuration hierarchy. The 'Authorization Profiles' section is expanded, and the 'PermitInternet' profile is selected. The profile configuration shows the name 'PermitInternet', a description field, and the access type set to 'ACCESS_ACCEPT'. Under 'Common Tasks', the 'Airespace ACL Name' is checked and set to 'Internet'.

4. للتحقق من قواعد التحويل، انتقل إلى نهج < تحويل. في ISE صيغة 1.3 افتراضيا ل failed ماك صحة هوية 4. مجرى جانبي (MAB) صحة هوية (لم يتم العثور على عنوان MAC) تستمر صحة المصادقة (غير مرفوضة). وهذا مفيد جدا لبوابات الضيوف لأنه لا توجد حاجة لتغيير أي شيء في قواعد المصادقة الافتراضية.

The screenshot shows the Cisco Identity Services Engine (ISE) interface for configuring an Authorization Policy. The top navigation bar includes 'Home', 'Operations', 'Policy', 'Guest Access', and 'Administration'. Below the navigation bar, there are tabs for 'Authentication', 'Authorization', 'Profiling', 'Posture', 'Client Provisioning', 'TrustSec', and 'Policy Elements'. The 'Authorization Policy' section is active, showing a dropdown menu for 'First Matched Rule Applies' set to 'First Matched Rule Applies'. Below this, there is a section for 'Exceptions (0)' and a 'Standard' section. The 'Standard' section contains a table with the following data:

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Guest	if GuestEndpoints AND Radius:Called-Station-ID CONTAINS Guest	then PermitInternet
✓	Guest_Authenticate	if Radius:Called-Station-ID CONTAINS Guest	then Guest

لا ينتمي المستخدمون الجدد الذين يقترنون ب SSID للضيف إلى أي مجموعة هوية. ولهذا السبب تتطابق مع القاعدة الثانية، التي تستخدم ملف تعريف تحويل Guest لإعادة توجيهها إلى "مدخل الضيف" الصحيح.

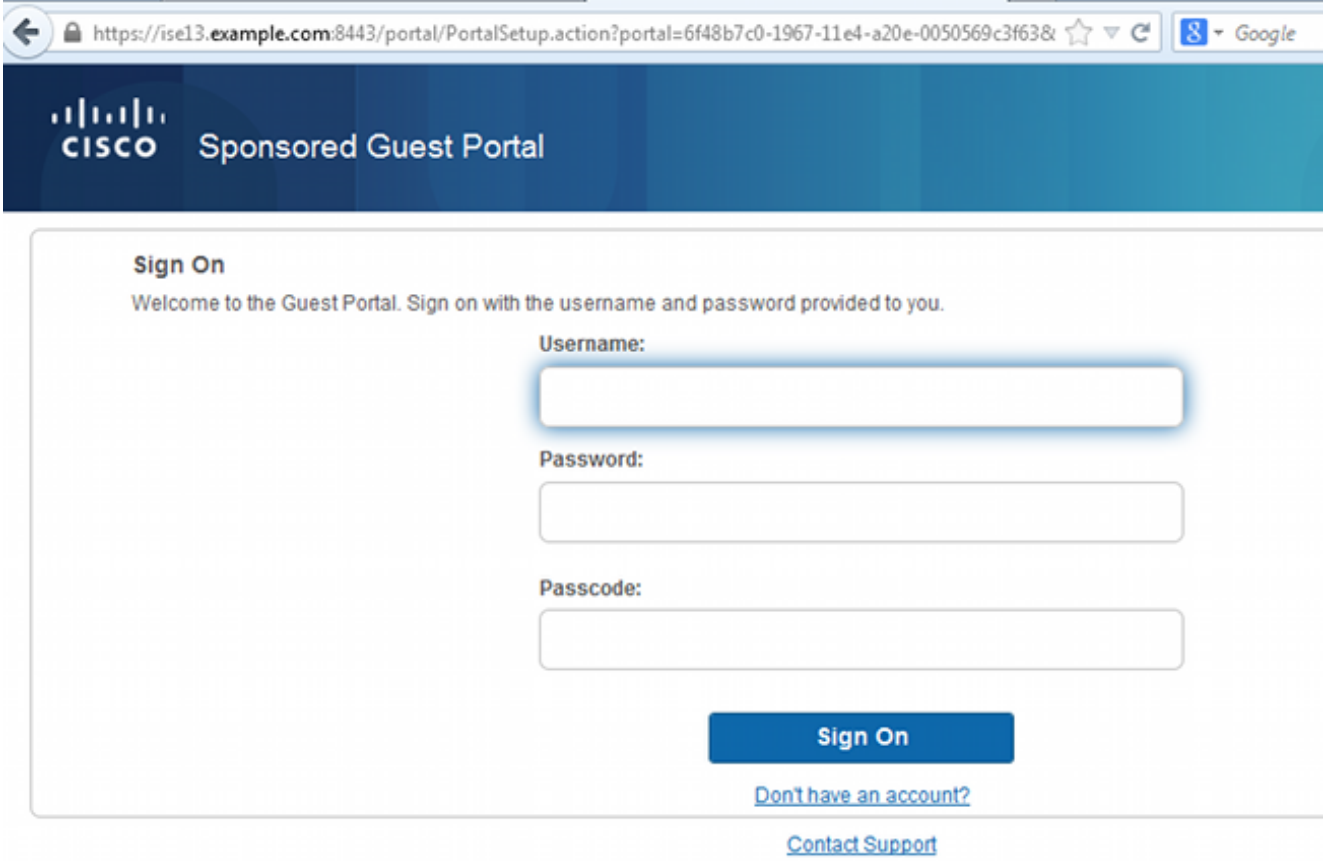
بعد أن يقوم المستخدم بإنشاء حساب وتسجيل الدخول بنجاح، يرسل ISE RADIUS CoA ويقوم عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) بإعادة المصادقة. في هذه المرة، تتم مطابقة القاعدة الأولى مع ملف تعريف التحويل PermitInternet وإرجاع اسم قائمة التحكم في الوصول (ACL) الذي يتم تطبيقه على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC).

5. إضافة عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) كجهاز وصول إلى الشبكة من الإدارة < موارد

التحقق من الصحة

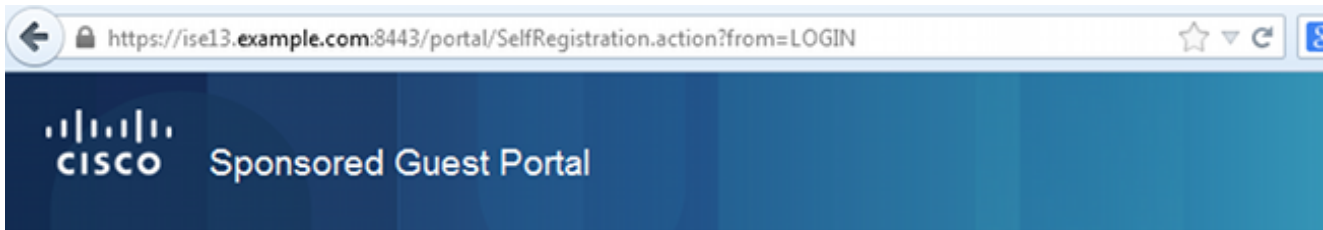
استخدم هذا القسم لتأكيد عمل التكوين بشكل صحيح.

1. بعد إقرانك بـ SSID الضيف واكتب URL، تتم إعادة توجيهك إلى صفحة تسجيل الدخول:



The screenshot shows a web browser window with the URL: <https://ise13.example.com:8443/portal/PortalSetup.action?portal=6f48b7c0-1967-11e4-a20e-0050569c3f63&>. The page header features the Cisco logo and the text "Sponsored Guest Portal". The main content area is titled "Sign On" and includes the following text: "Welcome to the Guest Portal. Sign on with the username and password provided to you." Below this text are three input fields: "Username:", "Password:", and "Passcode:". A blue "Sign On" button is positioned below the input fields. At the bottom of the form, there are two links: "Don't have an account?" and "Contact Support".

2. بما أنه لا توجد لديك أية بيانات اعتماد بعد، فيجب عليك إختيار خيار **عدم وجود حساب؟**. صفحة جديدة تسمح بعرض إنشاء الحساب. إذا تم تمكين خيار "رمز التسجيل" ضمن تكوين "مدخل الضيف"، تكون هذه القيمة السرية مطلوبة (وهذا يضمن أنه يسمح فقط للأشخاص الذين لديهم أذونات صحيحة بالتسجيل الذاتي).



Create Account

Please provide us with some information so we can create an account for you.

Registration Code*

Username

First name

Last name

Email address

Phone number

إذا كانت هناك أي مشاكل مع كلمة المرور أو سياسة المستخدم، انتقل إلى **Guest Access** < إعدادات > نهج 3. كلمة مرور الضيف أو وصول الضيف < إعدادات > نهج اسم مستخدم الضيف in order to غيرت الإعدادات. فيما يلي مثال:

▶ Guest Email Settings

Identify the SMTP server and specify

▶ Guest Locations and SSIDs

Specify the locations where you want

▶ Guest Password Policy

Specify the policy settings that will

▼ Guest Username Policy

Specify the policy settings that will

Configure username requirements that will be enforced for guest usernames. Usernames

Username Length

 Minimum username length: (1-64 characters)

Username Criteria for Known Guests

If data is available, base username on:

- First name and last name
- Email address

Characters Allowed in Randomly-Generated Usernames

Alphabetic:	<input type="text" value="All(a-z)"/>
Minimum alphabetic:	<input type="text" value="8"/> (0-64)
Numeric:	<input type="text" value="All(0-9)"/>
Minimum numeric:	<input type="text" value="0"/> (0-64)
Special:	<input type="text" value="All supported"/>
Minimum special:	<input type="text" value="0"/> (0-64)

4. بعد إنشاء الحساب بنجاح، تقدم لك بيانات الاعتماد (كلمة المرور التي تم إنشاؤها وفقا لنهج كلمة المرور للضيف):

The screenshot shows the 'Account Created' page of the Cisco Sponsored Guest Portal. The browser address bar displays the URL: https://ise13.example.com:8443/portal/CreateAccount.action?from=SELF_REGISTRATION. The page header features the Cisco logo and the text 'Sponsored Guest Portal'. The main content area has a title 'Account Created' and a sub-header 'Use the following information to sign on to the network.' Below this, the following user details are listed: Username: guest1, Password: =_yU, First name: michal, Last name: garcarz, Email: mgarcarz@cisco.com, and Phone number: 666666666. A blue 'Sign On' button is positioned at the bottom right of the main content area. A link for 'Contact Support' is located at the bottom center of the page.

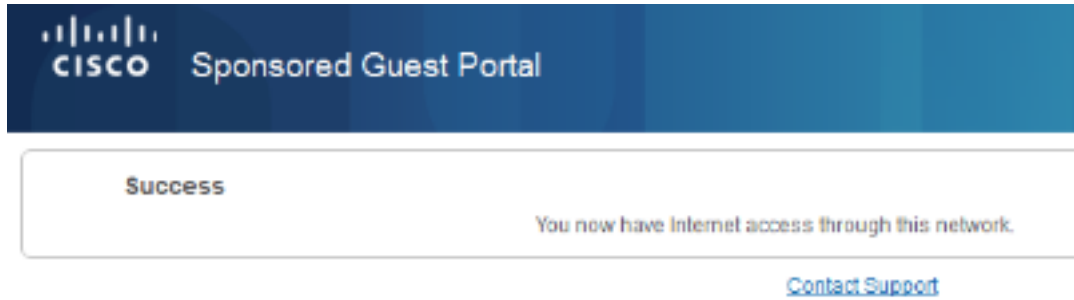
انقر فوق تسجيل الدخول وقم بتوفير بيانات الاعتماد (قد يكون رمز مرور الوصول الإضافي مطلوباً إذا تم تكويته، تحت مدخل Guest، وهذه آلية أمان أخرى تسمح فقط لأولئك الذين يعرفون كلمة المرور بتسجيل الدخول).

The screenshot shows the 'Sign On' page of the Cisco Sponsored Guest Portal. The page header features the Cisco logo and the text 'Sponsored Guest Portal'. The main content area has a title 'Sign On' and a sub-header 'Welcome to the Guest Portal. Sign on with the username and password provided to you.' Below this, there are three input fields: 'Username:' with the value 'guest1', 'Password:' with masked characters '***', and 'Passcode:' with the value 'cisco'. A blue 'Sign On' button is positioned at the bottom right of the main content area.

6. عند نجاح هذا الإجراء، يمكن تقديم سياسة إستخدام مقبولة إختيارية (AUP) (في حالة تكوينها أسفل مدخل Guest). قد يتم عرض صفحة Post Access (القابلة للتكوين أيضاً ضمن Guest Portal).

The screenshot shows the 'Post Access' page of the Cisco Sponsored Guest Portal. The page header features the Cisco logo and the text 'Sponsored Guest Portal'. The main content area has a title 'Post Access' and a sub-header 'Click Continue to connect to the network. You're very close to gaining network access.' A blue 'Continue' button is positioned at the bottom right of the main content area. A link for 'Contact Support' is located at the bottom center of the page.

تؤكد الصفحة الأخيرة أنه قد تم منح حق الوصول:



استكشاف الأخطاء وإصلاحها

يوفر هذا القسم معلومات يمكنك استخدامها لاستكشاف أخطاء التكوين وإصلاحها.

وفي هذه المرحلة، يقدم ISE السجلات التالية:

The screenshot shows the Cisco Identity Services Engine (ISE) dashboard. At the top, there are navigation tabs for Home, Operations, Policy, Guest Access, and Administration. Below these are several status indicators: Misconfigured Supplicants (0), Misconfigured Network Devices (0), RADIUS Drops (82), and Client Stopped Responding (0). The main section displays a table of live sessions with columns for Time, Status, Det..., Repeat Count, Identity, Authentication Policy, Authorization Policy, Authorization Profiles, Identity Group, and Event. The table shows several successful authentication events for the 'quest1' user.

Time	Status	Det...	Repeat Count	Identity	Authentication Policy	Authorization Policy	Authorization Profiles	Identity Group	Event
2014-08-01 13:19:52...	🔴		0	quest1					Session State is Started
2014-08-01 13:19:52...	🟢			quest1	Default >> MAB	Default >> Guest	PermitInternet	User Identity Gro...	Authorize-Only succeeded
2014-08-01 13:19:52...	🟢			quest1				GuestType_DAILY	Dynamic Authorization succeeded
2014-08-01 13:18:29...	🟢			quest1					Guest Authentication Passed
2014-08-01 13:16:31...	🟢			64:66:B3:08:23	Default >> MAB >> ..	Default >> Guest...	Guest		Authentication succeeded

هنا هو التدفق:

- يواجه المستخدم الضيف قاعدة التحويل الثانية (Guest_Authenticate) وبعاد توجيهه إلى Guest ("نجاح المصادقة").

- يتم إعادة توجيه الضيف للتسجيل الذاتي. بعد تسجيل الدخول بنجاح (باستخدام الحساب الذي تم إنشاؤه حديثاً)، يرسل ISE إعادة مصادقة CoA، وهو ما تم تأكيده بواسطة عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) ("نجاح التفويض الديناميكي").

- تقوم عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) بإجراء إعادة المصادقة باستخدام السمة Authorize-Only ويتم إرجاع اسم قائمة التحكم في الوصول ("Authorize-Only"). يتم تزويد الضيف بوصول الشبكة الصحيح.

التقارير (العمليات < التقارير < تقارير ISE < تقارير وصول الضيوف < تقرير الضيف الرئيسي) تؤكد أيضاً أن:

The screenshot shows the Master Guest Report table. It has columns for Logged At, Guest User Name, MAC Address, IP Address, Operation, User Name, Message, and AUP Acceptance. The table shows two rows of data for the user 'quest1'.

Logged At	Guest User Name	MAC Address	IP Address	Operation	User Name	Message	AUP Acceptance
2014-08-01 13:18:49.9	quest1	64-66-B3-08-23-A3	10.221.0.218				Guest user has accepted the use policy
2014-08-01 13:18:08.7	quest1	64-66-B3-08-23-A3	10.221.0.218	Add	SelfRegistration		

يمكن للمستخدم الكفيل (بامتيازات صحيحة) التحقق من الحالة الحالية لمستخدم ضيف.

يؤكد هذا المثال إنشاء الحساب، ولكن لم يتم المستخدم بتسجيل الدخول أبدا ("انتظار تسجيل الدخول الأولي"):

The screenshot shows the Cisco Sponsor Portal interface. At the top, there is a navigation bar with the Cisco logo and 'Sponsor Portal' text. A dropdown menu shows 'Welcome sponsor'. Below the navigation bar, there are several buttons: 'Create Accounts', 'Manage Accounts (1)', 'Pending Accounts (0)', and 'Notices (0)'. A table of actions is displayed, including 'Resend', 'Extend', 'Edit', 'Suspend', 'Reinstate', 'Delete', 'Reset Password', and 'Print'. The main content area displays user details for 'michal garcarz' with the following information:

First name:	michal
Last name:	garcarz
Username:	guest1
Password:	=_yU
Email address:	mgarcarz@cisco.com
Company:	
Phone number:	666666666
Person being visited(email):	
Reason for visit:	
Guest type:	DAILY
SMS provider:	
State:	Awaiting Initial Login
From date:	08/01/2014 12:58
To date:	08/02/2014 12:58
Location:	
SSID:	
Language:	English
Group tag:	
Time left:	0,23,47

التهيئة الاختيارية

لكل مرحلة من هذا التدفق، يمكن تكوين خيارات مختلفة. يتم تكوين كل هذا لكل مدخل ضيف في **Guest Access** < تكوين < بوابات الضيف < PortalName < تحرير < سلوك المدخل وإعدادات التدفق. تتضمن الإعدادات الأكثر أهمية:

إعدادات التسجيل الذاتي

- نوع الضيف - يصف المدة التي يكون فيها الحساب نشطا وخيارات انتهاء صلاحية كلمة المرور وساعات تسجيل الدخول والخيارات (وهذا هو مزيج من ملف تعريف الوقت ودور الضيف من الإصدار 1.2 من ISE)
- رمز التسجيل - في حالة التمكين، يسمح فقط للمستخدمين الذين يعرفون الرمز السري بالتسجيل الذاتي (يجب توفير كلمة المرور عند إنشاء الحساب)
- AUP - قبول سياسة الاستخدام أثناء التسجيل الذاتي
- متطلب موافقة الكفيل على حساب الضيف أو تنشيطه

إعدادات ضيف تسجيل الدخول

- رمز الوصول - في حالة التمكين، يسمح فقط للمستخدمين الضيوف الذين يعرفون الرمز السري بتسجيل الدخول
- AUP - قبول سياسة الاستخدام أثناء التسجيل الذاتي
- خيار تغيير كلمة المرور

إعدادات تسجيل الجهاز

- بشكل افتراضي، يتم تسجيل الجهاز تلقائياً

إعدادات توافق جهاز الضيف

- يسمح بوضع داخل التدفق

إعدادات BYOD

- السماح لمستخدمي الشركات الذين يستخدمون البوابة كضيوف بتسجيل أجهزتهم الشخصية

الحسابات المعتمدة من الكفيل

إذا تم تحديد خيار **مطالبة الضيوف المسجلين ذاتياً** بالمصادقة، فيجب اعتماد الحساب الذي تم إنشاؤه بواسطة الضيف من قبل كفيل. قد تستخدم هذه الميزة البريد الإلكتروني لتسليم إعلام إلى الكفيل (للموافقة على حساب الضيف):

إذا لم يتم تكوين خادم بروتوكول نقل البريد البسيط (SMTP) أو الافتراضي من الإعلام من البريد الإلكتروني، فلن يتم إنشاء الحساب:

Account Created

Use the following information to sign on to the network.

Email send failure

First name:michal
Last name:garcarz
Email:mgarcarz@cisco.com

[Sign On](#)

يؤكد السجل من guest.log أن عنوان "عمومي من" المستخدم للإعلام مفقود:

```
.ERROR [http-bio-10.62.97.21-8443-exec-9][ ] guestaccess 22:35:24,271 2014-08-01
-::flowmanager.step.guest.SelfRegStepExecutor -:7AAF75982E0FCD594FE97DE2970D472F
Catch GuestAccessSystemException on sending email for approval: sendApproval
Notification: From address is null. A global default From address can be
.configured in global settings for SMTP server
عندما يكون لديك تكوين البريد الإلكتروني المناسب، يتم إنشاء الحساب:
```



▶ Guest Account Purge Policy

Specify when to delete expired guest accounts :

▶ Custom Fields

Add custom fields that can be used for creating

▼ Guest Email Settings

Identify the SMTP server and specify the email

SMTP server: outbound.cisco.com

Configure SMTP server at:

[Administration](#) > [System](#) > [Settings](#) > [SMTP](#)

Enable email notifications to guests

Use default email address

Default email address:

Use email address from sponsor

Account Created

Use the following information to sign on to the network.

First name:michal

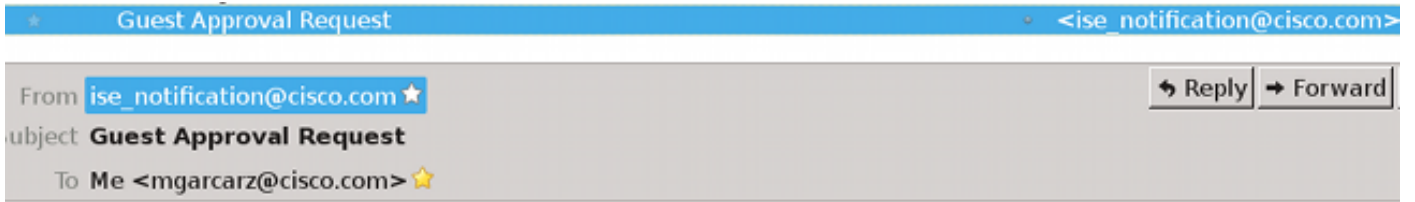
Last name:garcarz

Email:mgarcarz@cisco.com

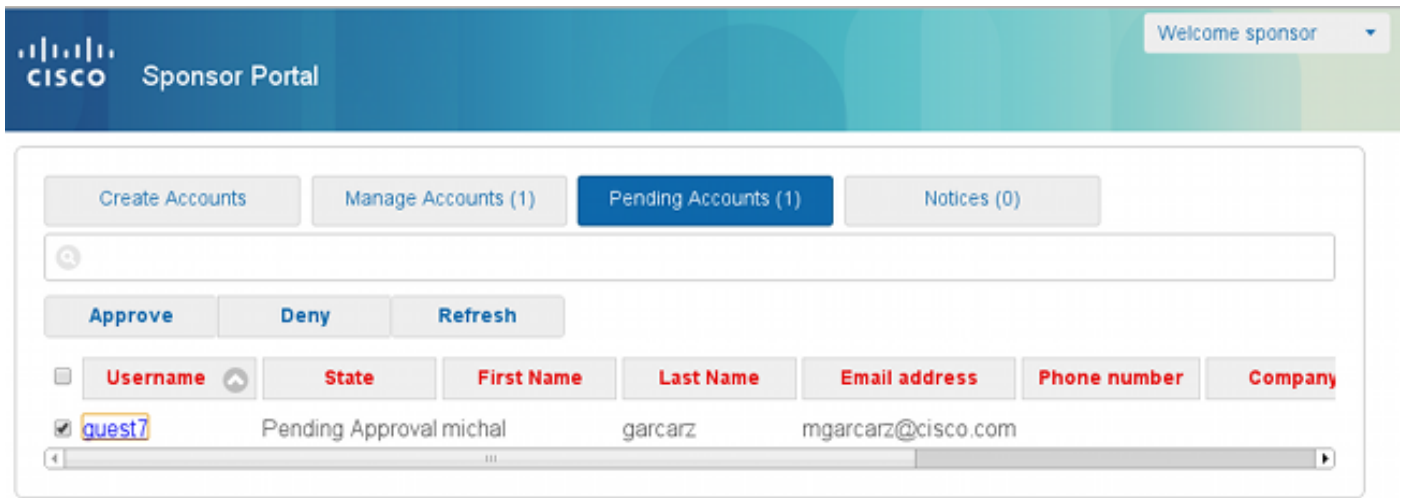
[Sign On](#)

بعد أن تقوم بتمكين خيار مطالبة الضيوف المسجلين ذاتيا بأن يكونوا معتمدين ، يتم إزالة حقل اسم المستخدم وكلمة المرور تلقائيا من قسم تضمين هذه المعلومات في صفحة نجاح التسجيل الذاتي. ولهذا السبب، عندما يكون هناك حاجة إلى موافقة الكفيل، لا يتم عرض بيانات اعتماد المستخدمين الضيوف بشكل افتراضي على صفحة الويب التي تقدم معلومات لإظهار أن الحساب قد تم إنشاؤه. وبدلا من ذلك، يجب تسليمها بواسطة خدمات الرسائل القصيرة (SMS) أو البريد الإلكتروني. يجب تمكين هذا الخيار في إعلام إرسال بيانات الاعتماد عند الموافقة باستخدام قسم (وضع علامة بريد إلكتروني/SMS).

يتم تسليم بريد إلكتروني للإخطار إلى الكفيل:



يقوم الكفيل بتسجيل الدخول إلى بوابة الكفيل ويوافق على الحساب:



من هذه النقطة، يتم السماح للمستخدم الضيف بتسجيل الدخول (باستخدام بيانات الاعتماد التي تم تلقيها عبر البريد الإلكتروني أو الرسائل النصية القصيرة).

في الخلاصة، هناك ثلاثة عناوين بريد إلكتروني مستخدمة في هذا التدفق:

- إعلام عنوان "من". ويتم تحديد هذا بشكل ثابت أو يؤخذ من حساب الكفيل ويستخدم كعنوان من بالنسبة لكل من: الإخطار إلى الكفيل (للموافقة) وتفاصيل بيانات الاعتماد إلى الضيف. ويتم تكوين هذا تحت **Guest Access** (وصول الضيف) < **Configure** (تكوين) < إعدادات < إعدادات البريد الإلكتروني للضيف.
- إعلام عنوان "إلى". ويتم استخدام هذا الأمر لإبلاغ الكفيل باستلامه حساباً للموافقة عليه. ويتم تكوين هذا في مدخل **Guest Portal** ضمن **Guest Portal Portal Name > Configure > Guest Portal Portal Name > Require Self-Registered Guest Portal Name > Require to Approved** (طلب الموافقة على البريد الإلكتروني إلى).

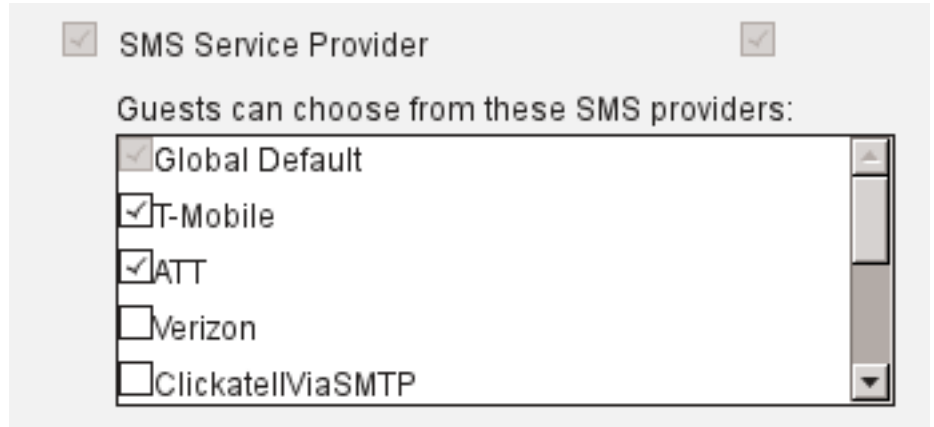
• عنوان "إلى" للضيف. وهذا ما يقدمه المستخدم الضيف أثناء التسجيل. في حالة تحديد إرسال إعلام بيانات الاعتماد عند الموافقة باستخدام البريد الإلكتروني، يتم تسليم البريد الإلكتروني الذي يحتوي على تفاصيل بيانات الاعتماد (اسم المستخدم وكلمة المرور) إلى الضيف.

تقديم بيانات الاعتماد عبر خدمة SMS

يمكن أيضا تسليم بيانات اعتماد الضيوف بواسطة SMS. يجب تكوين هذه الخيارات:

.1

أختر موفر خدمة SMS:

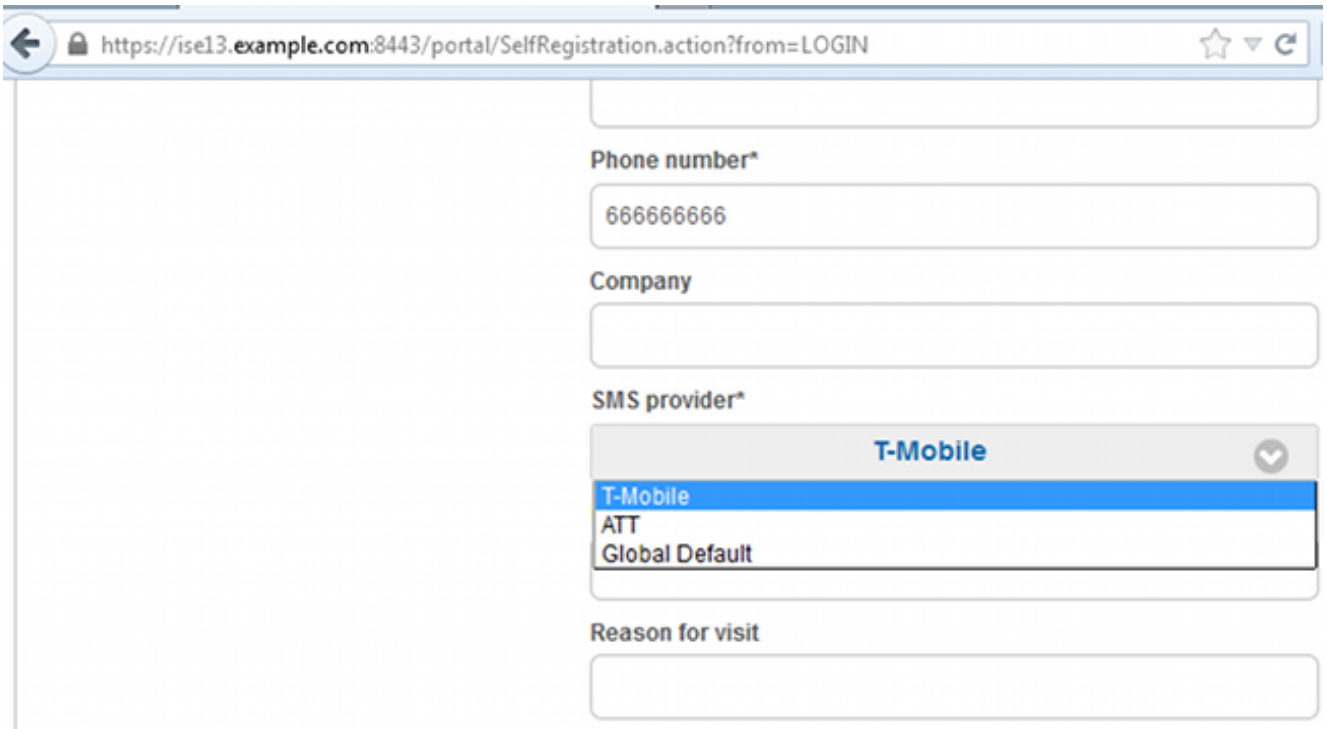


.2

حدد خانة الاختيار إرسال إعلام بيانات الاعتماد عند الموافقة باستخدام SMS.

.3

ثم يطلب من المستخدم الضيف إختيار الموفر المتوفر عند إنشاء حساب:



.4

يتم تسليم رسالة SMS باستخدام الموفر المختار ورقم الهاتف:

Account Created

Use the following information to sign on to the network.

First name:michal
Last name:garcarz
Email:mgarcarz@cisco.com
Phone number:6666666666
SMS Provider:Global Default

Sign On

5. يمكنك تكوين موفري خدمة SMS ضمن الإدارة < النظام < الإعدادات < بوابة SMS.

تسجيل الأجهزة

إذا تم تحديد الخيار السماح للضيوف بتسجيل الأجهزة بعد أن يقوم أحد المستخدمين الضيوف بتسجيل الدخول وقبول بروتوكول المصادقة والتفويض والمحاسبة (AUP)، فيمكنك تسجيل الأجهزة:

CISCO Sponsored Guest Portal

Device Registration

You can add a maximum of \$guest.device_limit\$ devices. Enter a device ID and device description. The device ID is the MAC address or Wi-Fi address of the device. It is an alphanumeric ID in this format: A1:B3:E5:19:6F:BB

Device ID

Device Description

Manage Devices (1)

64:66:B3:08:23:A3	<input type="button" value="Delete"/>
-------------------	---------------------------------------

لاحظ أنه قد تمت إضافة الجهاز تلقائياً بالفعل (وهو في قائمة إدارة الأجهزة). وذلك لأنه تم تحديد تسجيل أجهزة الضيوف تلقائياً.

وضعية

إذا تم تحديد خيار طلب توافق الجهاز الضيف، فسيتم تزويد المستخدمين الضيوف بوكيل يقوم بتنفيذ الوضعية (NAC/Web Agent) بعد تسجيل الدخول وقبول بروتوكول AUP (وإجراء تسجيل الجهاز اختياريًا). يقوم ISE بمعالجة قواعد إمداد العميل لتحديد الوكيل الذي يجب توفيره. ثم يقوم الوكيل الذي يتم تشغيله على المحطة بتنفيذ الوضع (وفقاً لقواعد الوضع) وإرسال النتائج إلى ISE، الذي يرسل إعادة مصادقة CoA لتغيير حالة التحويل إذا لزم الأمر.

قد تبدو قواعد التحويل المحتملة مشابهة لما يلي:

► Exceptions (0)

Standard

Status	Rule Name	Conditions (identity groups and other conditions)	Permissions
✓	Guest_Compliant	if GuestEndpoints AND (Radius:Called-Station-ID CONTAINS Guest AND Session:PostureStatus EQUALS Compliant)	then PermitInternet
✓	Guest	if GuestEndpoints AND Radius:Called-Station-ID CONTAINS Guest	then LimitedAccess
✓	Guest_Authenticate	if Radius:Called-Station-ID CONTAINS Guest	then Guest

أول المستخدمين الجدد الذين يواجهون قاعدة Guest_Authenticate أعيد توجيههم إلى مدخل Self Register بعد أن يقوم المستخدم بالتسجيل الذاتي وتسجيل الدخول، يقوم CoA بتغيير حالة التحويل ويتم تزويد المستخدم بإمكانية وصول محدودة لتنفيذ الوضع والمعالجة. لا تقوم CoA بتغيير حالة التفويض مرة أخرى إلا بعد توفير وكيل NAC وتوافق المحطة على توفير الوصول إلى الإنترنت.

تتضمن المشاكل النموذجية في الوضع عدم وجود قواعد تزويد العميل الصحيحة:



Sponsored Guest Portal

Device Security Check



ISE is not able to apply an access policy to your log-in session at this time. Please close this browser, wait approximately one minute, and try to connect again. If you are still not able to log-in, please contact your network administrator.

[Contact Support](#)

كما يمكن تأكيد ذلك إذا قمت بفحص ملف guest.log (جديد في الإصدار 1.3 من ISE):

```
.ERROR [http-bio-10.62.97.21-8443-exec-9][ ] guestaccess 21:35:08,435 2014-08-01  
-::flowmanager.step.guest.ClientProvStepExecutor -:7AAF75982E0FCD594FE97DE2970D472F  
CP Response is not successful, status=NO_POLICY
```

بيود

إذا تم تحديد خيار السماح للموظفين باستخدام أجهزة شخصية على الشبكة، فيمكن حينئذ لمستخدمي الشركة الذين يستخدمون هذه البوابة المرور عبر تدفق BYOD وتسجيل الأجهزة الشخصية. بالنسبة للمستخدمين الضيوف، لا يغير هذا الإعداد أي شيء.

ماذا يعني "الموظفون الذين يستخدمون البوابة كضيوف"؟

بشكل افتراضي، يتم تكوين بوابات الضيوف باستخدام مخزن الهوية **Guest_Portal_Sequence**:

Portal Settings

HTTPS port: * (8000 - 8999)

Allowed interfaces: * Gigabit Ethernet 0
 Gigabit Ethernet 1
 Gigabit Ethernet 2
 Gigabit Ethernet 3

Certificate Group Tag: *

Configure certificates at:
[Administration > System > Certificates > System Certificates](#)

Identity source sequence: *

Configure identity source sequence at:
[Administration > Identity Management > Identity Source Sequences](#)

هذا هو تسلسل المتجر الداخلي الذي يحاول المستخدمين الداخليين أولاً (قبل المستخدمين الضيوف):

Identity Services Engine Home Operations Policy

System Identity Management Network Resources Device Portal Management

Identities Groups External Identity Sources Identity Source Sequences Settings

[Identity Source Sequences List > Guest_Portal_Sequence](#)

Identity Source Sequence

Identity Source Sequence

* Name

Description

Certificate Based Authentication

Select Certificate Authentication Profile

Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available	Selected
Internal Endpoints	Internal Users
AD1	Guest Users
	All_AD_Instances

في هذه المرحلة على مدخل الضيف، يقدم المستخدم بيانات اعتماد معرفة في مخزن المستخدمين الداخليين وتحديث إعادة توجيه BYOD:

1

2

3

4

BYOD Welcome

Welcome to the BYOD portal.

Access to this network requires your device to be configured for enhanced security. Click Start to provide device information before components are installed on your device.

Start

I want guest access only

بهذه الطريقة يمكن لمستخدمي الشركة تنفيذ BYOD للأجهزة الشخصية.

عندما يتم توفير بيانات اعتماد Guest Users بدلا من بيانات اعتماد Internal Users، يستمر التدفق العادي (بدون BYOD).

تغيير شبكة VLAN

هذا خيار مماثل لتغيير شبكة VLAN الذي تم تكوينه ل Guest Portal في الإصدار 1.2 من ISE. وهو يسمح لك بتشغيل ActiveX أو تطبيق جافا، والذي يشغل DHCP لإطلاق وتجديد. يلزم هذا عندما تقوم CoA بتشغيل تغيير شبكة VLAN لنقطة النهاية. عند استخدام MAB، لا تدرك نقطة النهاية أي تغيير في شبكة VLAN. حل ممكن هو تغيير شبكة VLAN (إصدار/تجديد DHCP) باستخدام وكيل NAC. خيار آخر هو طلب عنوان IP جديد عبر التطبيق الصغير الذي تم إرجاعه على صفحة الويب. يمكن تكوين تأخير بين الإصدار/التجديد. هذا الخيار غير مدعوم للأجهزة المحمولة.

معلومات ذات صلة

- [Cisco ISE Configuration Guide على Posture Services](#)
- [BYOD اللاسلكي مع محرك خدمات الهوية](#)
- [دعم ISE SCEP لمثال تكوين BYOD](#)
- [دليل مسؤولي Cisco ISE 1.3](#)
- [مثال على تكوين مصادقة الويب المركزية على شبكة LAN اللاسلكية \(WLC\) ومحرك خدمات كشف الهوية \(ISE\)](#)
- [المصادقة المركزية للويب مع نقاط الوصول FlexConnect APs على عنصر التحكم في الشبكة المحلية](#)
- [اللاسلكية \(WLC\) مع مثال تكوين ISE](#)
- [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 ةيرشبلاو
امك ةقيد نوك تنل ةللأل ةمچرت لصف أن ةظحال مچرئ. ةصاغل مهتغب
Cisco يلخت. فرتحم مچرت مامدقي يتل ةيفارتحال ةمچرتل عم لالحل وه
ىل إامئاد ةوچرلاب يصوت و تامچرتل هذه ةقد نع اهتيلوئسم Cisco
Systems (رفوتم طبارلا) يلصلأل يزيلچنل دن تسمل