تكوين TrustSec (SGTs) باستخدام ISE (وضع علامات داخل السطر)

المحتويات

المقدمة

يوضح هذه المستند كيفية تكوين TrustSec والتحقق من صحته على محول Catalyst ووحدة تحكم الشبكة المحلية اللاسلكية باستخدام محرك خدمات الهوية.

المتطلبات الأساسية

توصي Cisco بأن تكون لديك معرفة بالمواضيع التالية:

- معرفة أساسية بمكونات Cisco TrustSec (CTS)
- معرفة الأساسية ال CLI تشكيل من مادة حفازة مفتاح
- معرفة أساسية بتكوين واجهة المستخدم الرسومية (GUI) لوحدات التحكم في شبكة LAN اللاسلكية من Cisco (WLC)
- تجربة تكوين محرك خدمات الهوية (ISE)

المتطلبات

يجب نشر Cisco ISE في شبكتك، كما يجب على المستخدمين النهائيين المصادقة على Cisco ISE باستخدام 802.1x (أو طريقة أخرى) عند توصيلهم بشبكة السلكية أو سلكية. يعين Cisco ISE حركة المرور الخاصة بهم رقم مجموعة الأمان (SGT) بمجرد أن يقوموا بالمصادقة على الشبكة اللاسلكية الخاصة بك.

في مثالنا، تتم إعادة توجيه المستخدمين النهائيين إلى ISE إحضار بوابة الجهاز الخاص بك (BYOD) ويتم تزويدهم بشهادة تتيح لهم الوصول بأمان إلى الشبكة اللاسلكية بمجرد إكمال خطوات باستخدام بروتوكول المصادقة المتوسع - أمان طبقة النقل (EAP-TLS) مدخل BYOD.

المكونات المستخدمة

تستند المعلومات الواردة في هذا المستند إلى إصدارات المكونات المادية والبرامج التالية:

- Cisco Identity Services Engine، الإصدار 2.4
- المحول Cisco Catalyst 3850 Switch، الإصدار 3.7.5E
- Cisco WLC، الإصدار 8.5.120.0
- نقطة الوصول اللاسلكية Cisco Aironet في الوضع المحلي

قبل نشر Cisco TrustSec، تحقق من أن محول Cisco Catalyst Switch و/أو Cisco WLC+AP Modules + إصدار البرنامج لديه دعم ل:

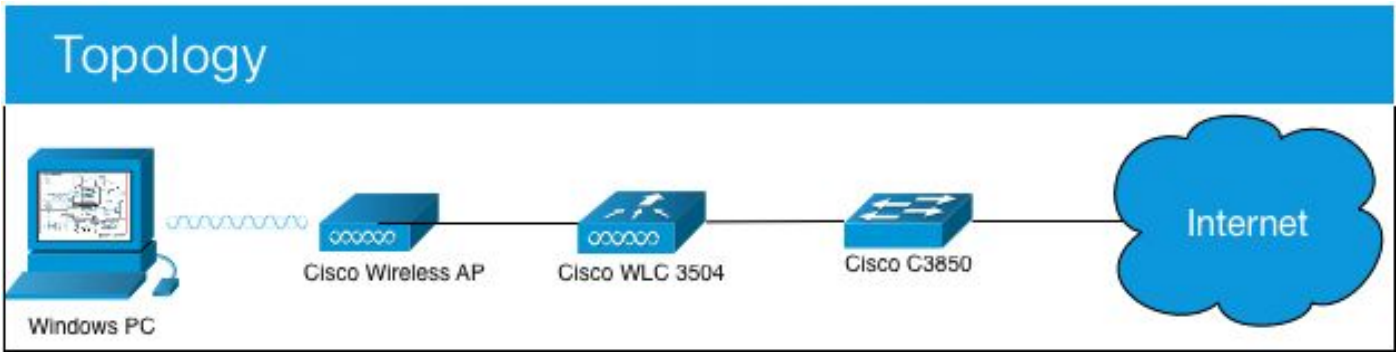
- علامات مجموعة الأمان/TrustSec
- وضع علامات في السطر (إذا لم يكن، يمكنك إستخدام SXP بدلا من وضع علامات في السطر)
- تعيينات ثابتة من بروتوكول الإنترنت (IP) إلى الرقيب (عند الحاجة)

- تعييناتالشبكاتالفرعيةالثابتةللرقيب (إذا لزم الأمر)
- تعييناتالشبكةالمحليةالظاهريةVLAN) (الثابتةإلىالرقيب (إذا لزم الأمر)

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

التكوين

الرسم التخطيطي للشبكة



في هذا المثال، تقوم عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) بتمييز الحزم على أنها الرقيب 15 إذا كان من مستشار، + الرقيب 7 إذا كان من موظف.

ويرفض المفتاح هذه الحزم إذا كانت من الرقيب 15 إلى الرقيب 8 (لا يمكن للمستشاري الوصول إلى الخوادم التي تم وضع علامة عليها كالرقيب 8).

يسمح المحول لتلك الحزم إذا كانت من الرقيب 7 إلى الرقيب 8 (يمكن للموظفين الوصول إلى الخوادم التي تم وضع علامة عليها كالرقيب 8).

هدف

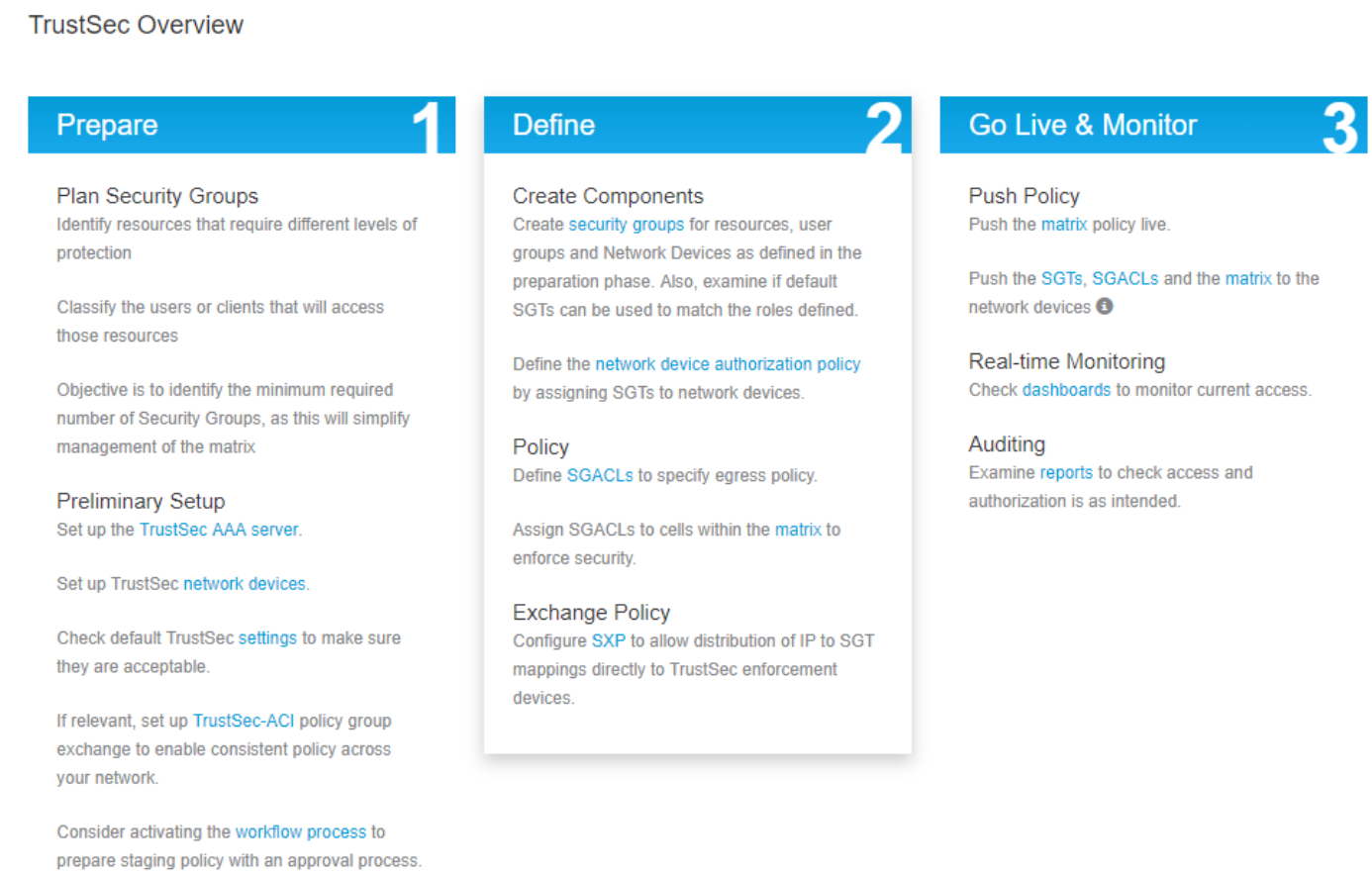
السماح لأي شخص بالوصول إلى GuestSSID.
السماح للمستشاري بالوصول إلى EmployeeSSID، ولكن مع تقييد الوصول.
السماح للموظفين بالوصول إلى EmployeeSSID مع الوصول الكامل.

في المثال التالي	عنوان IP	VLAN
محرك خدمات كشف الهوية (ISE)	10.201.214.230	463
المحول Catalyst Switch	10.201.235.102	1115
WLC	10.201.214.229	463
نقطة الوصول	10.201.214.138	455

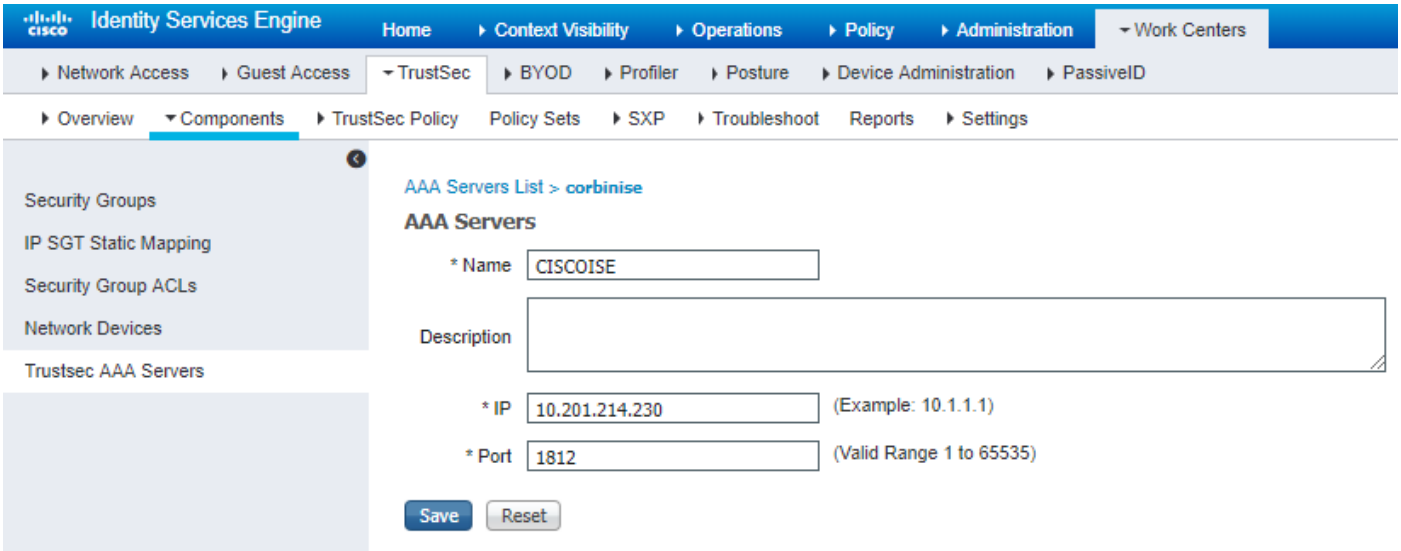
الاسم	Username	المجموعة الإعلانية	س.ج	رقيب
جايسون سميث	جيسميث	الاستشاريون	استشاريون	15
ساليسميث	سميث	الموظفون	موظفو بايود	7
غير متوفر	غير متوفر	غير متوفر	TrustSec_Devices	2

التكوينات

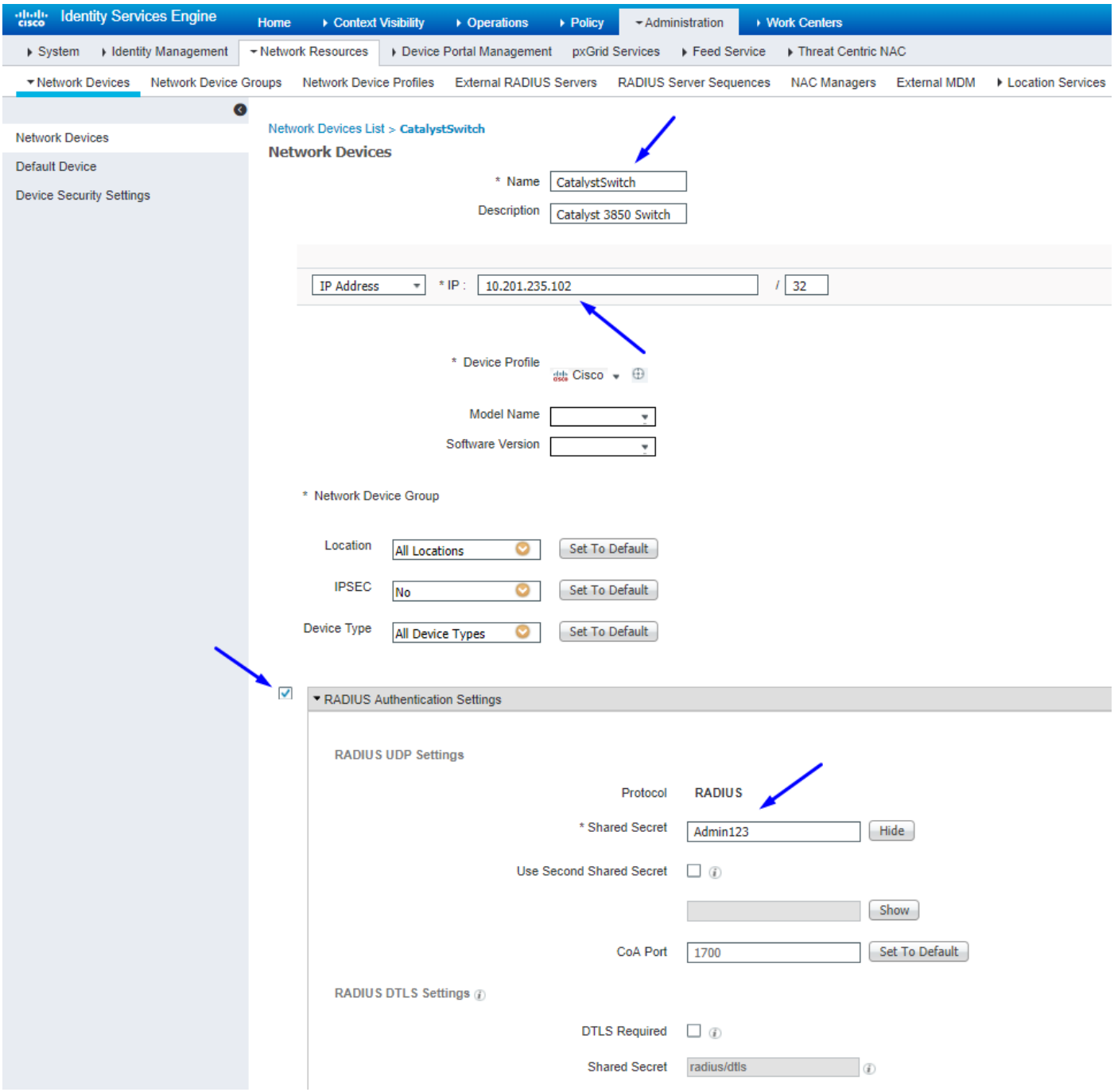
تكوين TrustSec على ISE



تكوين Cisco ISE كخادم TrustSec AAA

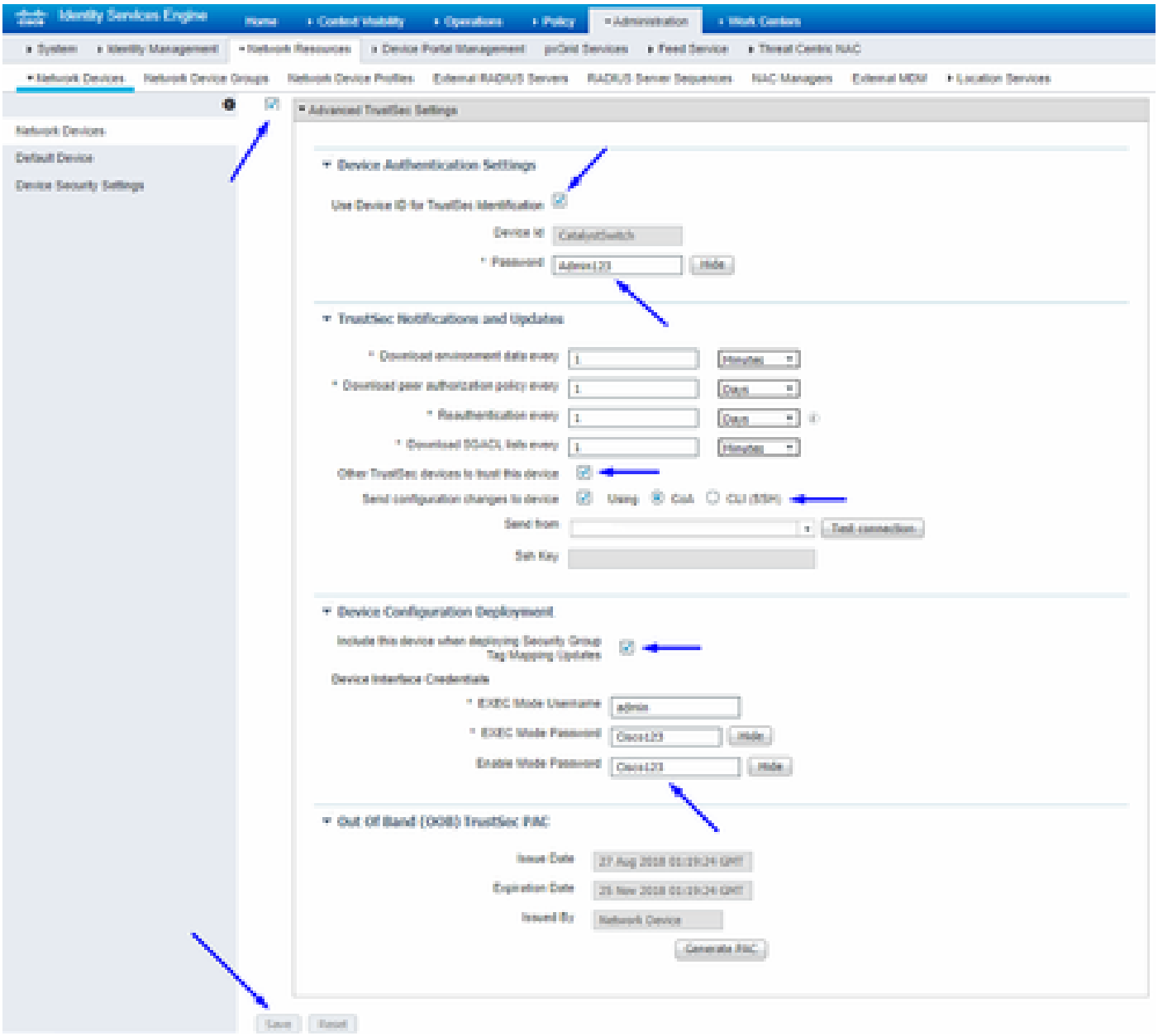


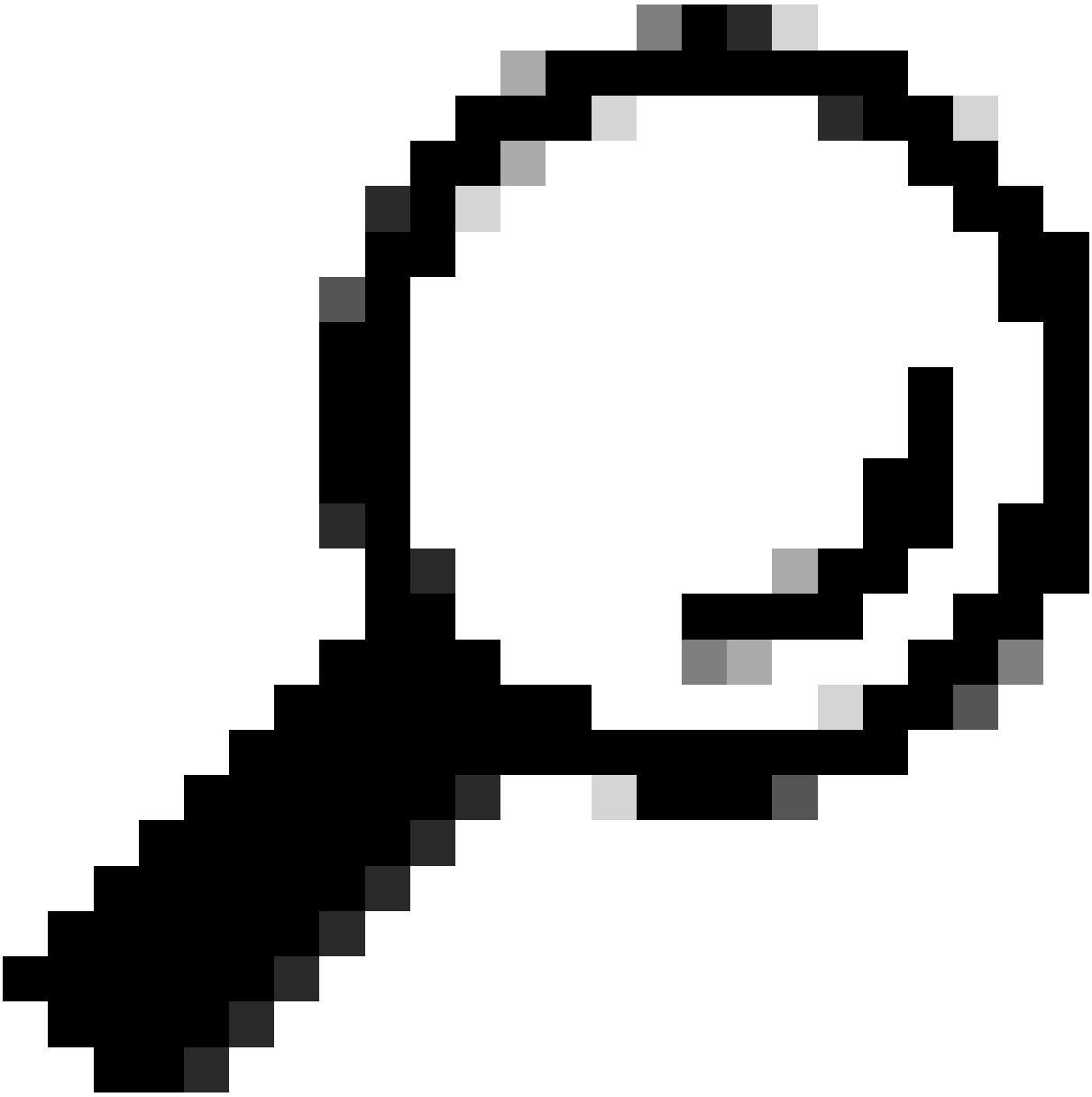
التكوين والتحقق من إضافة المحول كجهاز RADIUS في Cisco ISE



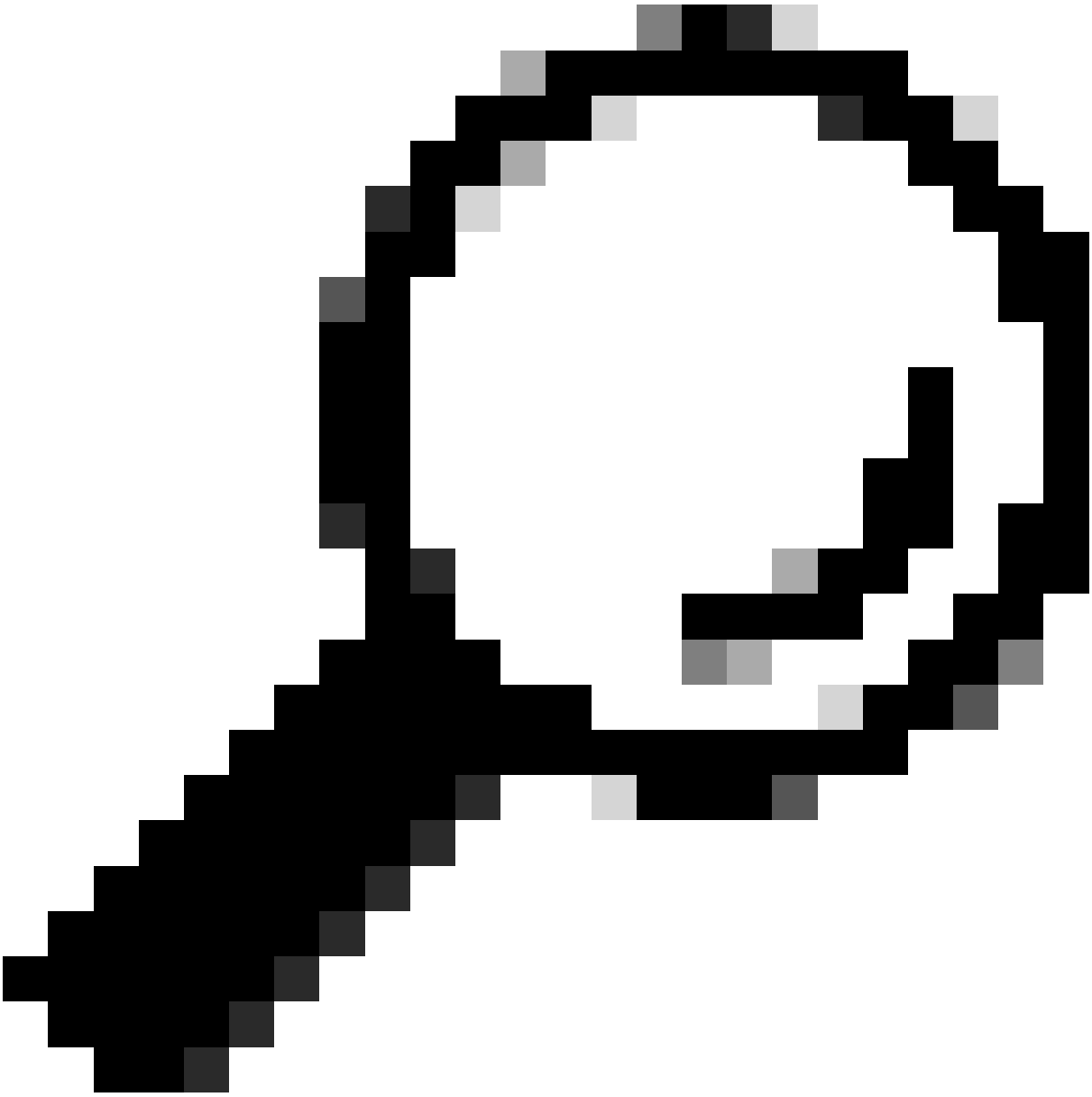
تتم إضافة تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) والتحقق منه كجهاز TrustSec في Cisco ISE

أدخل بيانات اعتماد تسجيل الدخول لـ SSH. وهذا يمكن Cisco ISE من نشر تعيينات IP إلى الرقيب الثابتة إلى المحول.
يمكنك إنشاء هذه العناصر في واجهة المستخدم الرسومية (GUI) عبر الويب من Cisco ISE تحت Work Centers > TrustSec > Components > IP SGT Static Mappings كما هو موضح هنا:


Identity Services Engine
Home
Context Visibility
Operations
Policy
Administration
Work Centers
System
Identity Management
Network Resources
Device Portal Management
pxGrid Services
Feed Service
Threat Centric NAC
Network Devices
Network Device Groups
Network Device Profiles
External RADIUS Servers
RADIUS Server Sequences
NAC Managers
External MDM
Location Services
Network Devices
Default Device
Device Security Settings
Advanced TrustSec Settings
Device Authentication Settings
Use Device ID for TrustSec Identification
Device Id
CatalystSwitch
* Password
Admin123
Hide
TrustSec Notifications and Updates
* Download environment data every
1
Minutes
* Download peer authorization policy every
1
Days
* Reauthentication every
1
Days
* Download SGACL lists every
1
Minutes
Other TrustSec devices to trust this device
Send configuration changes to device
Using
CoA
CLI (SSH)
Send from
Test Connection
Ssh Key
Device Configuration Deployment
Include this device when deploying Security Group Tag Mapping Updates
Device Interface Credentials
* EXEC Mode Username
admin
* EXEC Mode Password
Cisco123
Hide
Enable Mode Password
Cisco123
Hide
Out Of Band (OOB) TrustSec PAC
Issue Date
27 Aug 2018 01:19:24 GMT
Expiration Date
25 Nov 2018 01:19:24 GMT
Issued By
Network Device
Generate PAC
Save
Reset

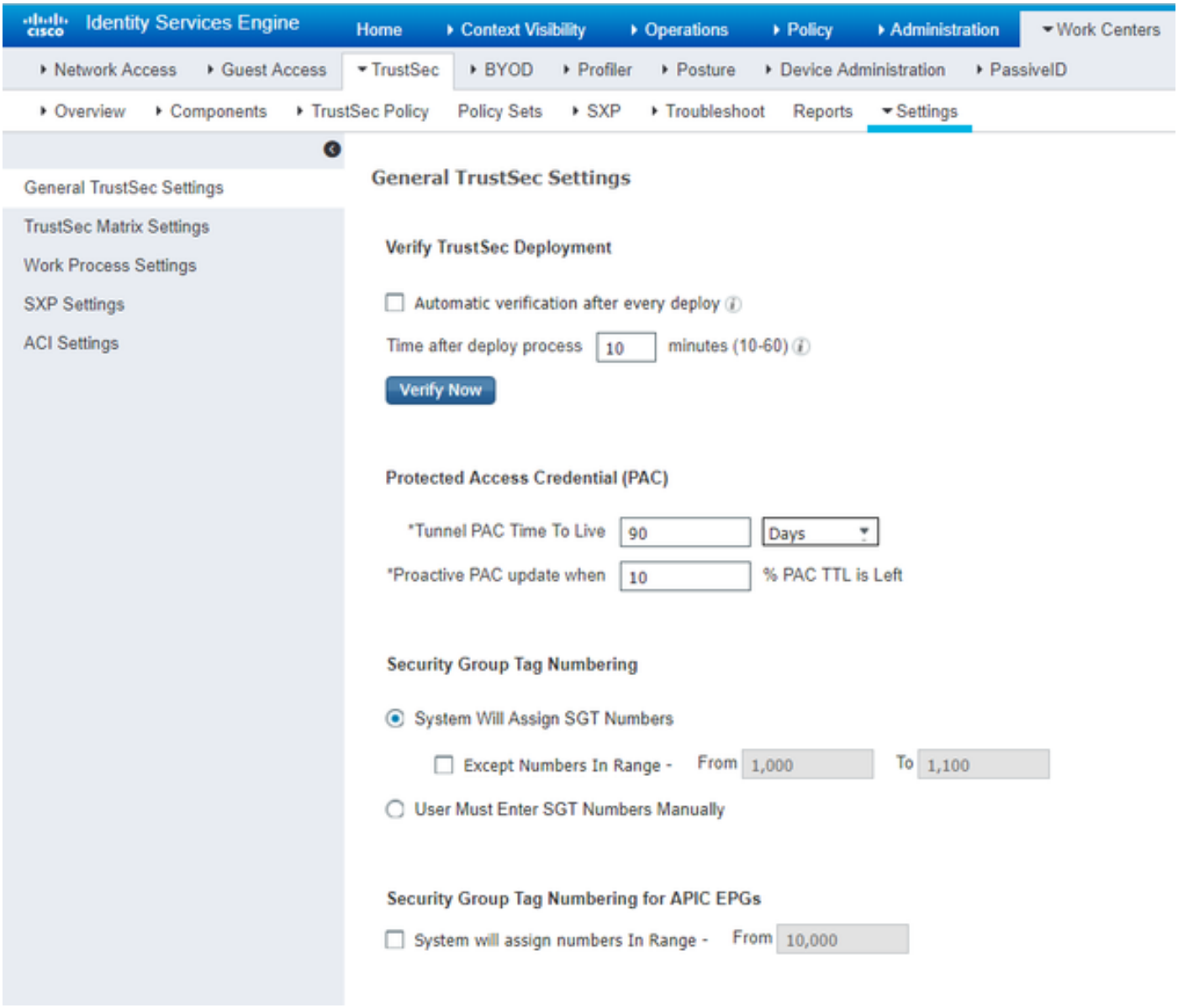


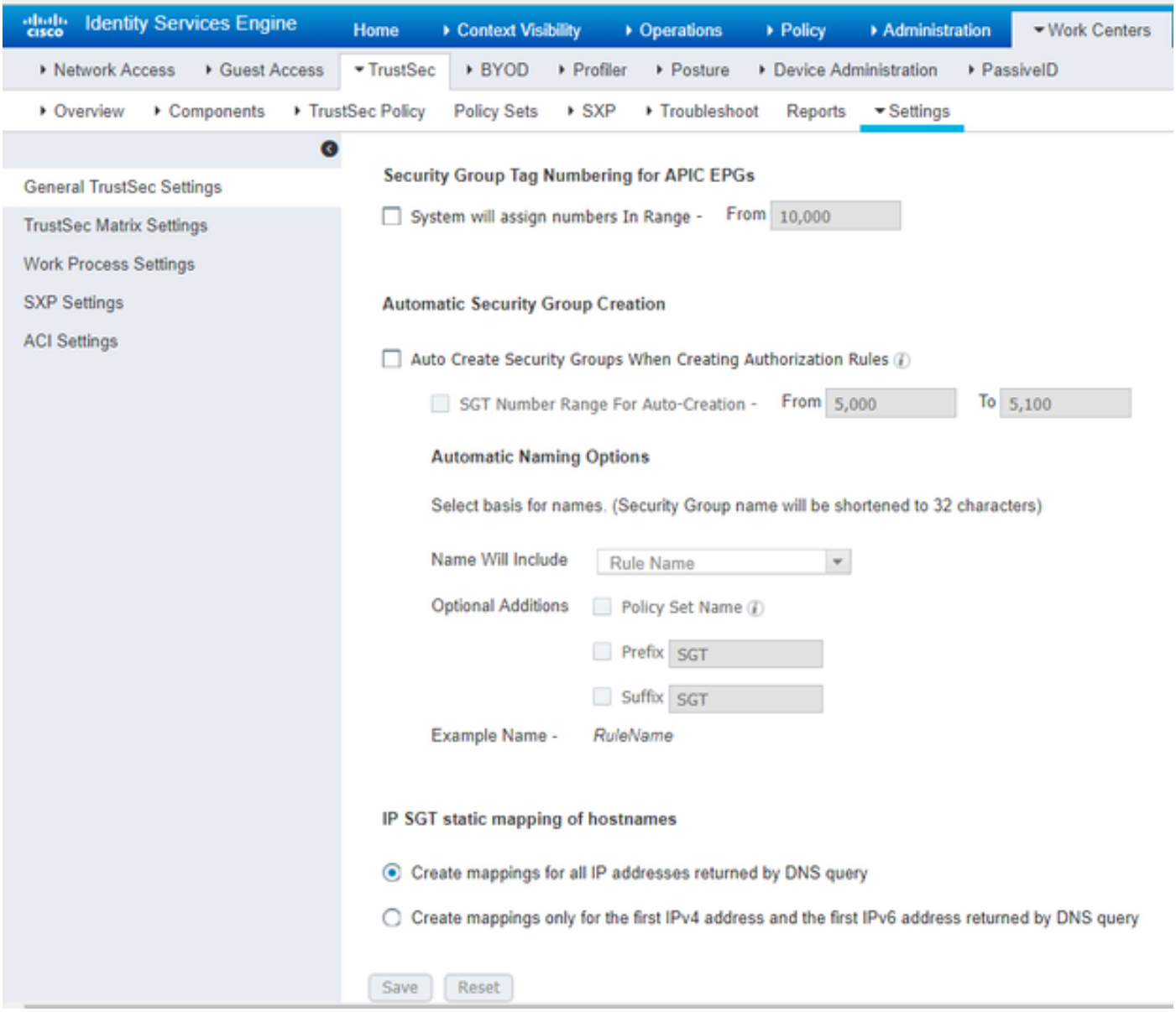
تلميح: إذا لم تقم بتكوين SSH على محول Catalyst لديك، فيمكنك إستخدام هذا الدليل: كيفية تكوين طبقة الأمان (SSH) على محول Catalyst.



تلميح: إذا لم تكن ترغب في تمكين Cisco ISE للوصول إلى محول Catalyst عبر SSH، فيمكنك إنشاء تعيينات ثابتة لبروتوكول IP إلى SGT على محول Catalyst باستخدام واجهة سطر الأوامر (CLI) بدلاً من ذلك (موضح في خطوة هنا).

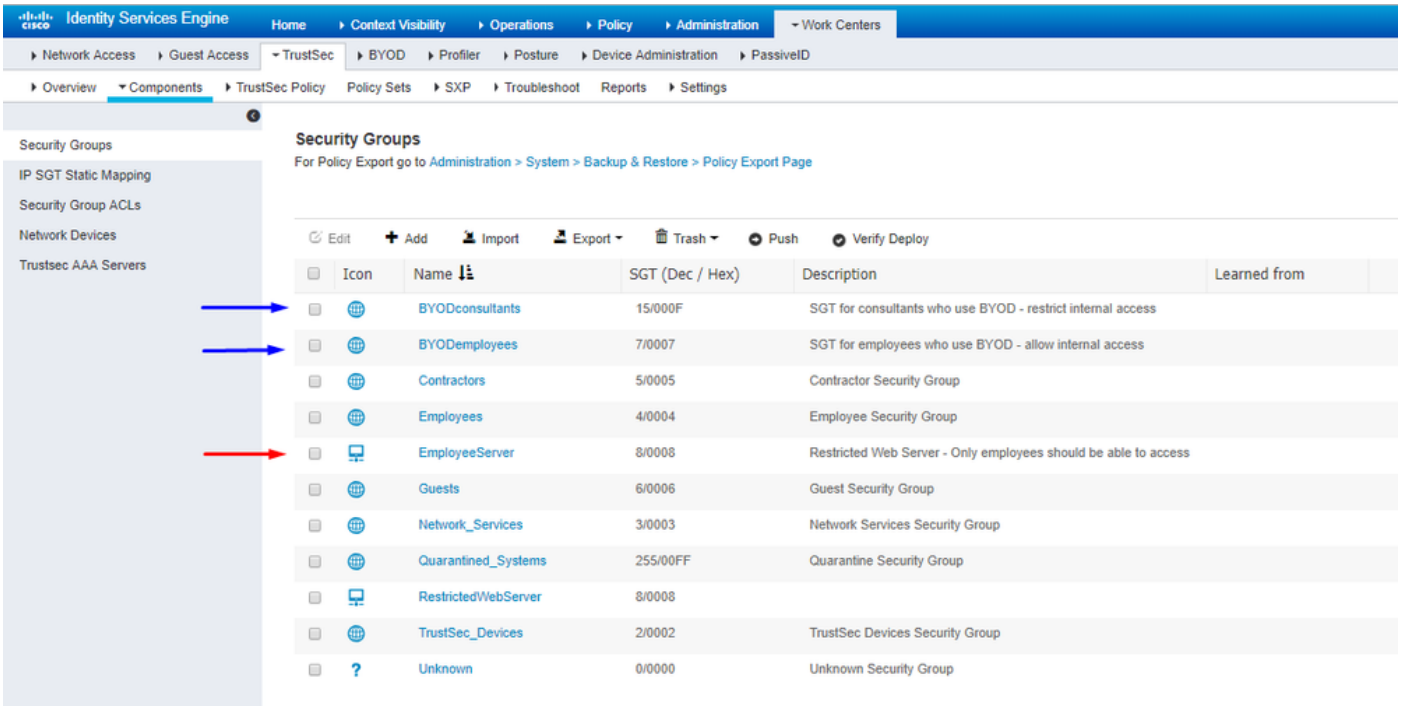
تحقق من إعدادات TrustSec الافتراضية للتأكد من أنها مقبولة (اختيارية)


Identity Services Engine
Home
Context Visibility
Operations
Policy
Administration
Work Centers
Network Access
Guest Access
TrustSec
BYOD
Profiler
Posture
Device Administration
PassiveID
Overview
Components
TrustSec Policy
Policy Sets
SXP
Troubleshoot
Reports
Settings
General TrustSec Settings
TrustSec Matrix Settings
Work Process Settings
SXP Settings
ACI Settings
General TrustSec Settings
Verify TrustSec Deployment
Automatic verification after every deploy
Time after deploy process 10 minutes (10-60)
Verify Now
Protected Access Credential (PAC)
*Tunnel PAC Time To Live 90 Days
*Proactive PAC update when 10 % PAC TTL is Left
Security Group Tag Numbering
System Will Assign SGT Numbers
Except Numbers In Range - From 1,000 To 1,100
User Must Enter SGT Numbers Manually
Security Group Tag Numbering for APIC EPGs
System will assign numbers In Range - From 10,000



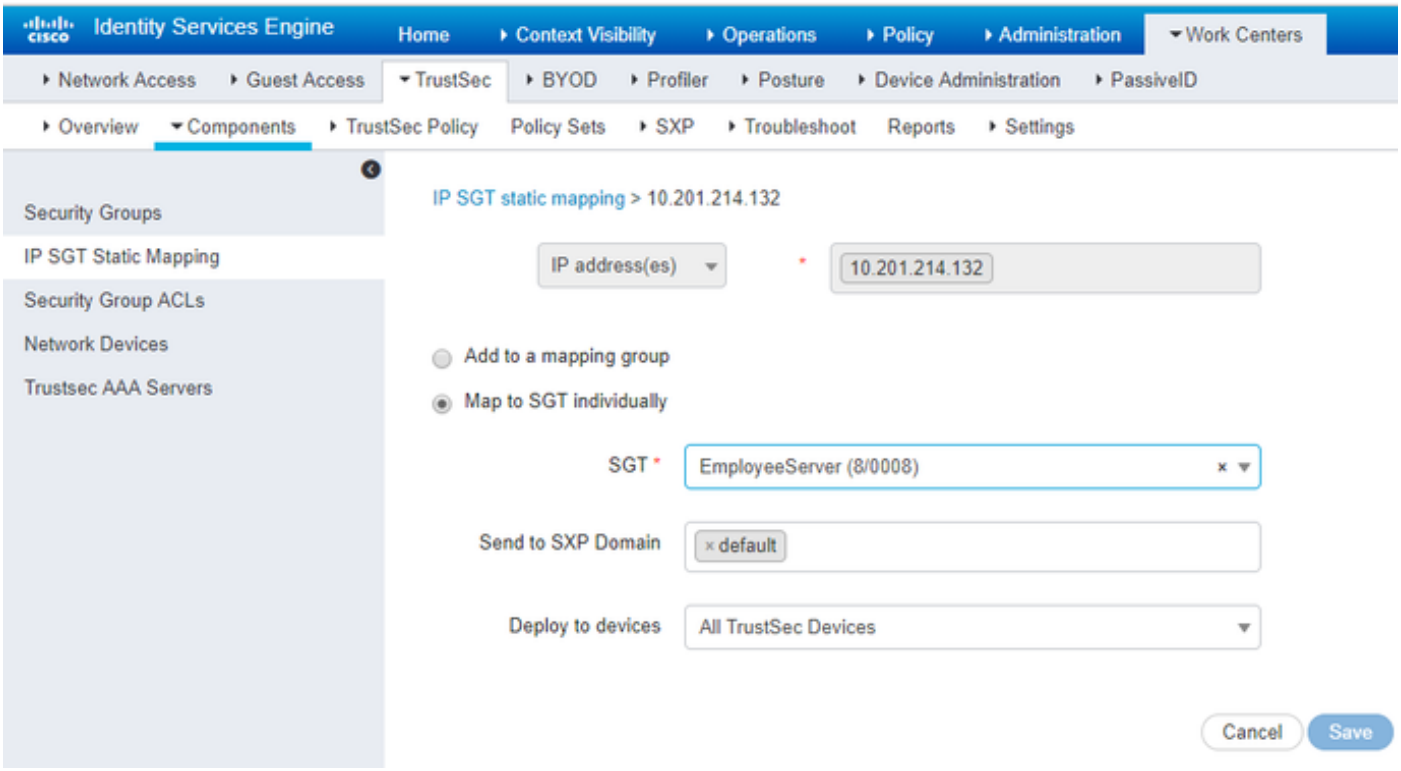
إنشاء علامات مجموعة تأمين للمستخدمين اللاسلكيين

إنشاء مجموعة أمان لمستشاري BYOD - الرقيب 15
قم بإنشاء مجموعة أمنية للموظفين في الفريق أول - الرقيب 7

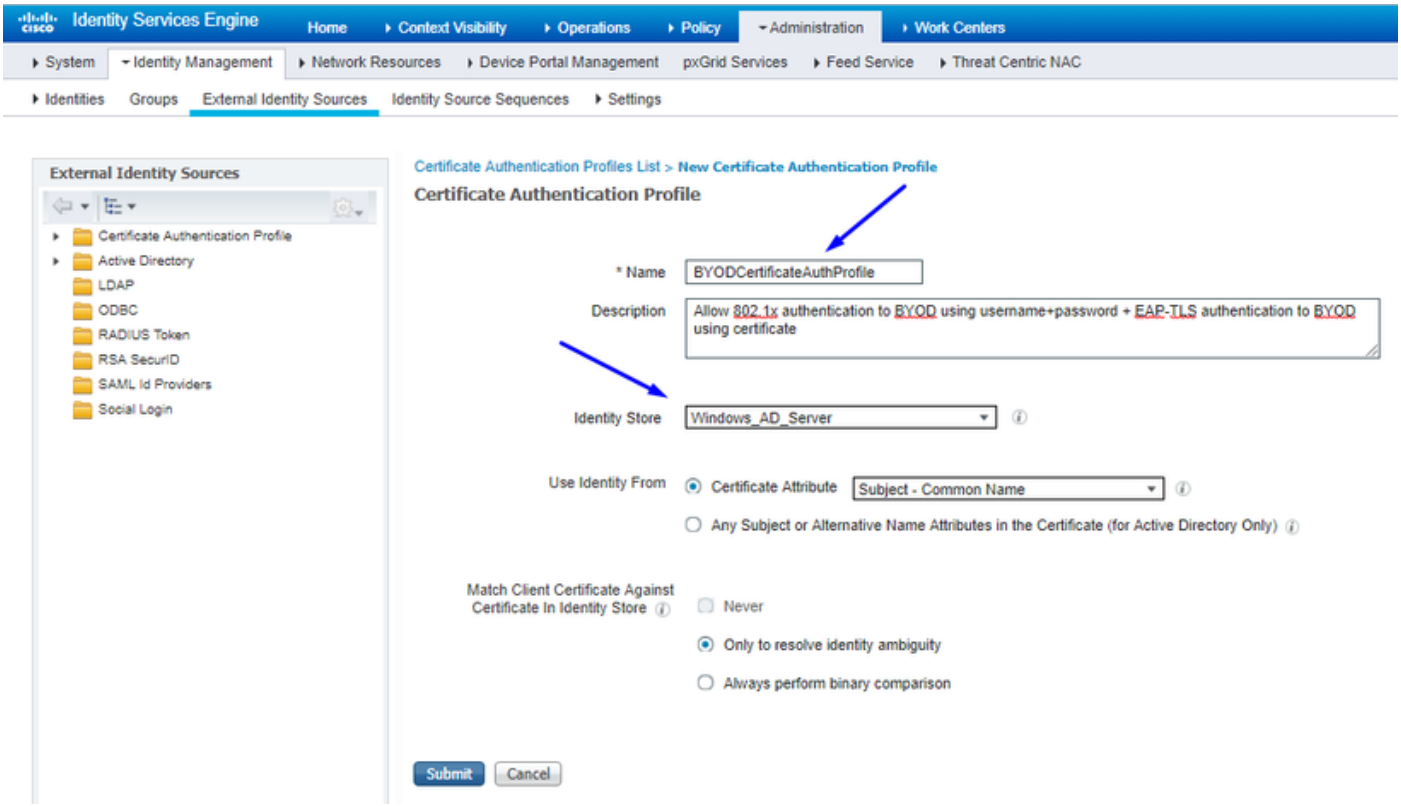


إنشاء تخطيط ساكن إستاتيكي من IP إلى SGT لخادم الويب المقيد

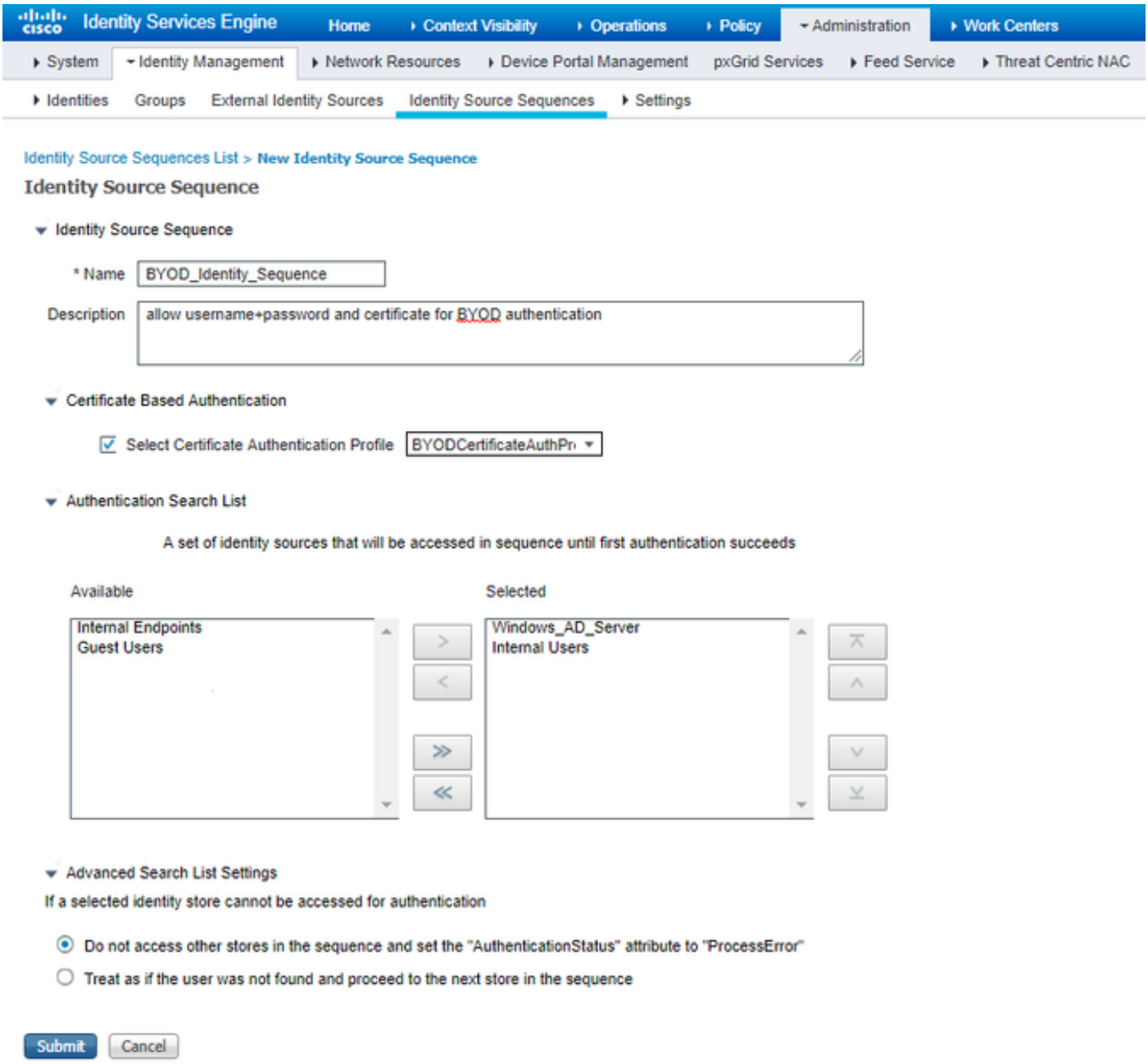
قم بذلك لأي عناوين IP أخرى أو شبكات فرعية في شبكتك ال تصادق إلى Cisco ISE مع تجاوز مصادقة MAC (MAB)، 802.1x، توصيفات، وهكذا.



إنشاء ملف تعريف مصادقة الشهادة

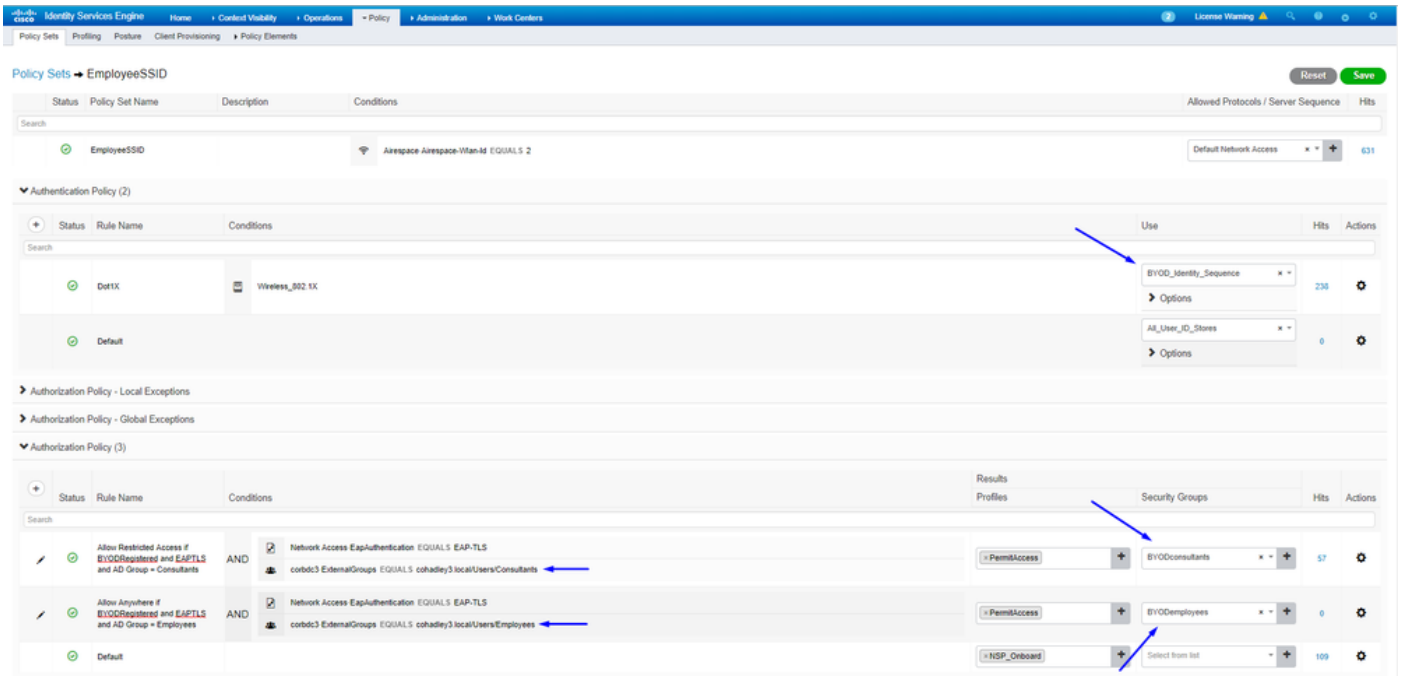


إنشاء تسلسل مصدر هوية بملف تعريف مصادقة الشهادة من قبل

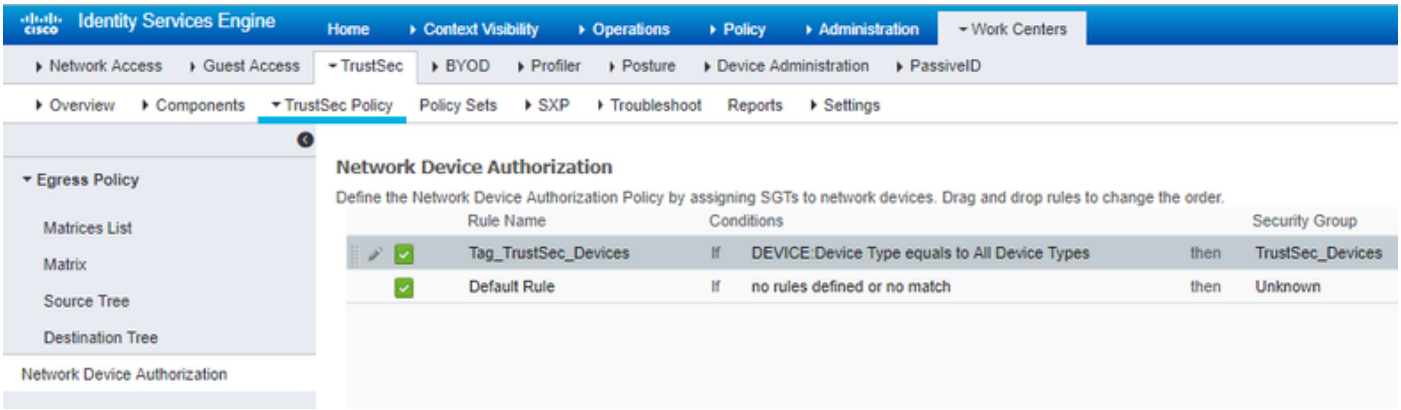


قم بتعيين المستخدمين اللاسلكيين (الموظفين والمستشارين) ورقيب مناسب

الاسم	Username	المجموعة الإعلانية	س.ج	رقيب
جايسون سميث	جيسميث	الاستشاريون	استشاريون	15
ساليي سميث	سميث	الموظفون	موظفو بايود	7
غير متوفر	غير متوفر	غير متوفر	TrustSec_Devices	2

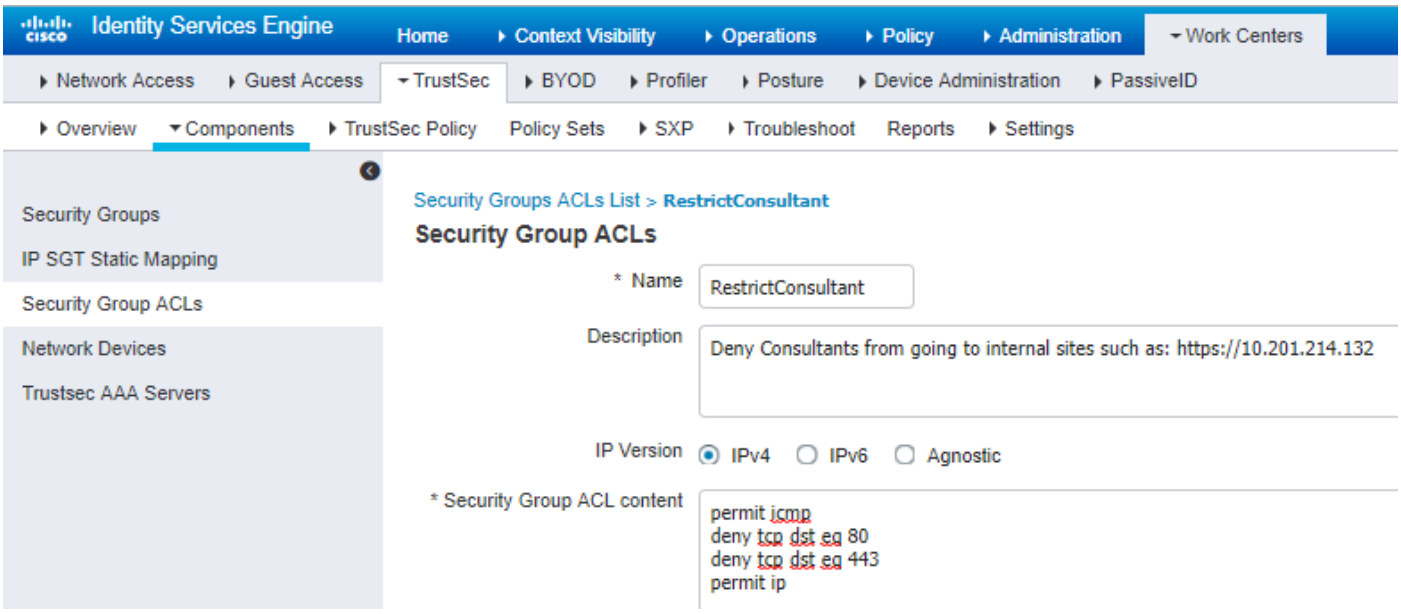


قم بتعيين الرقيب على الأجهزة الفعلية (المحول وعنصر التحكم في الشبكة المحلية اللاسلكية (WLC))

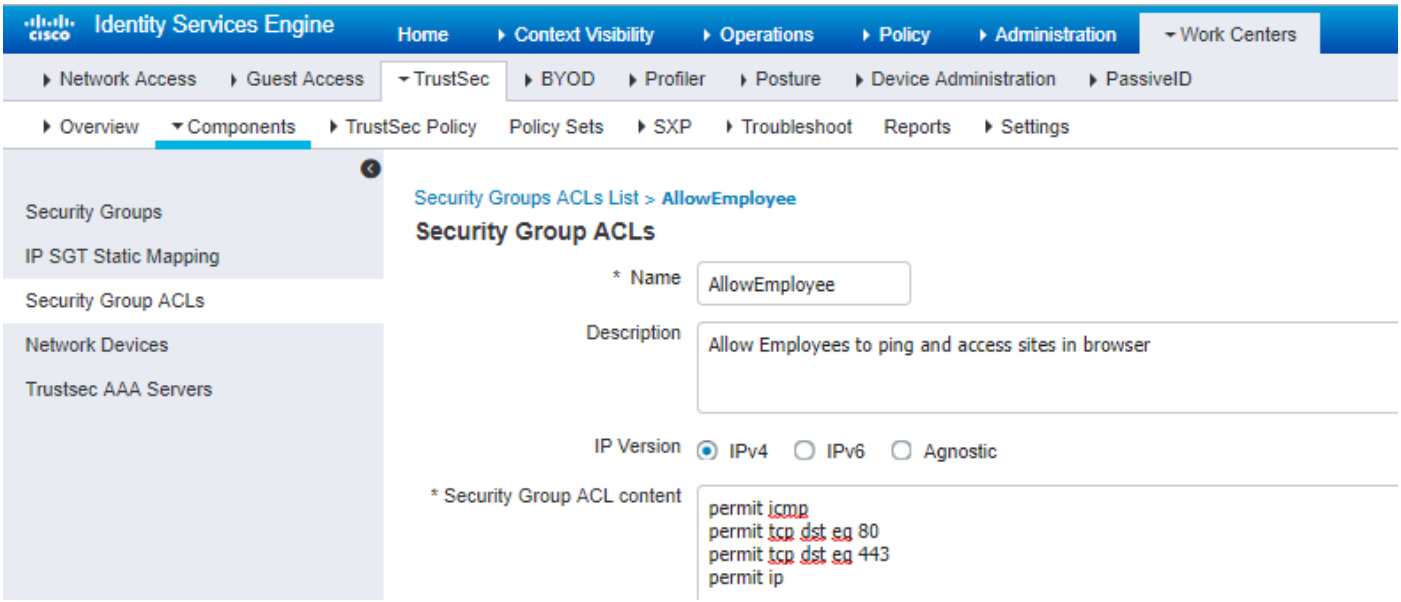


قم بتحديد SGACLs لتحديد سياسة الخروج

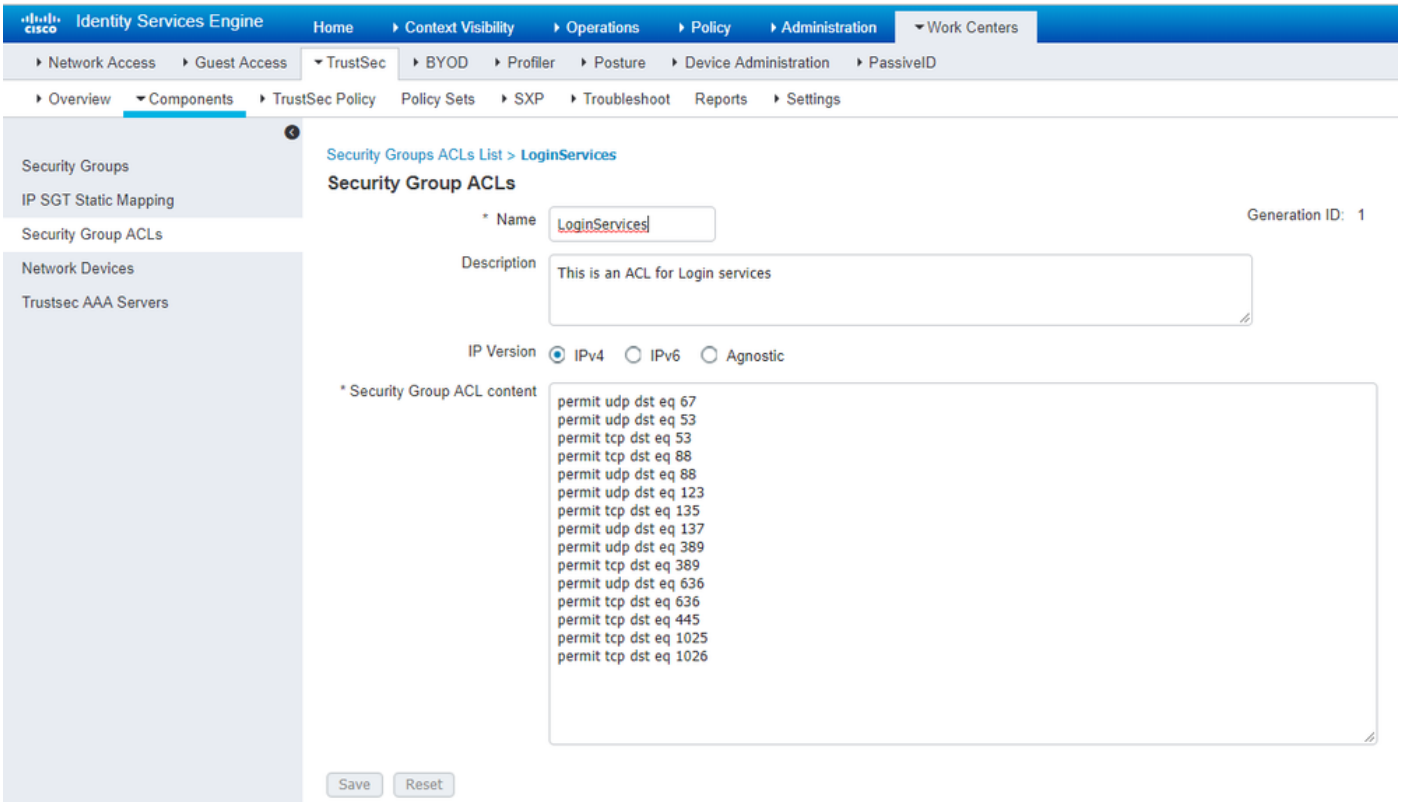
السماح للمستشاريين بالوصول إلى أي مكان خارجي، ولكن مع تقييد ما هو داخلي:



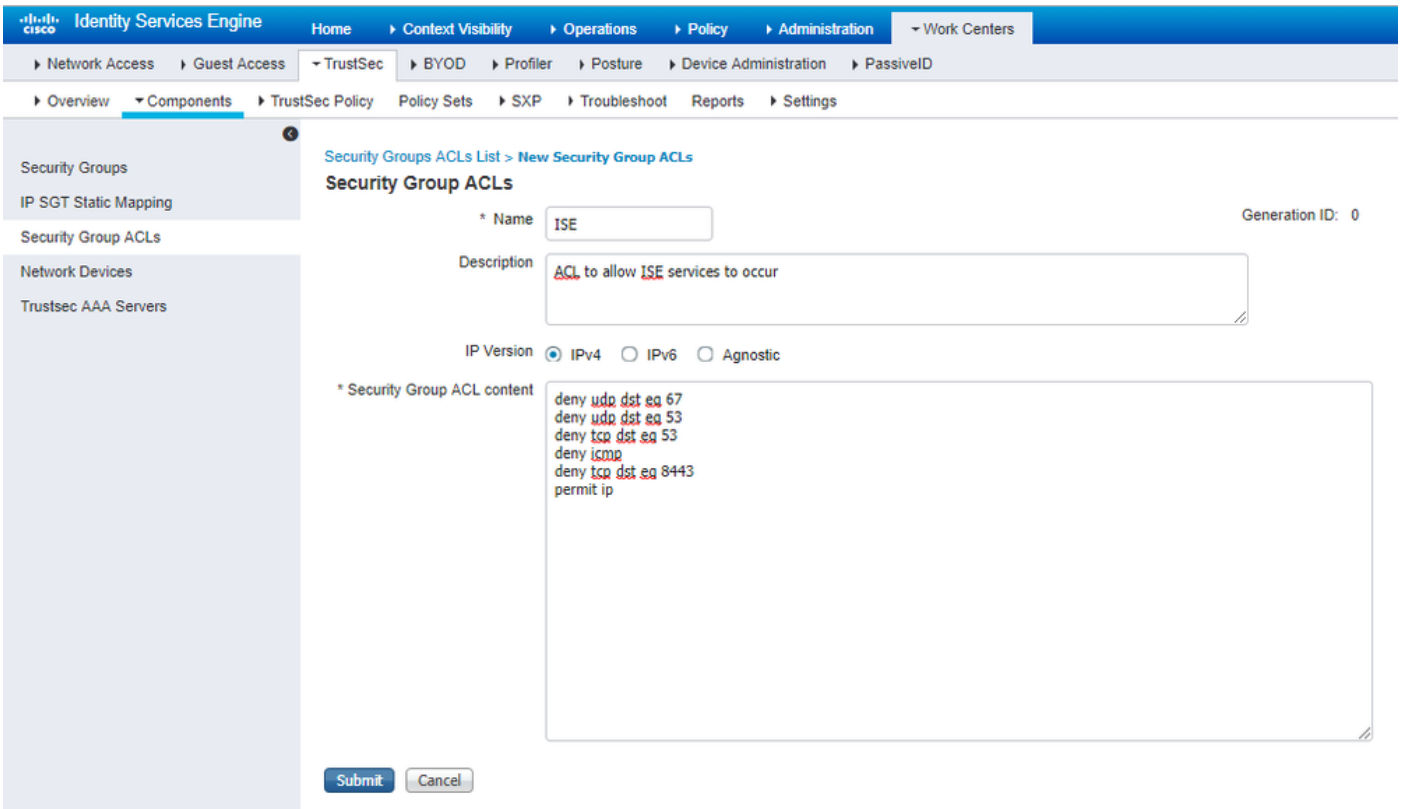
السماح للموظفين بالوصول إلى أي مكان خارجي وأي مكان داخلي:



السماح للأجهزة الأخرى بالوصول إلى الخدمات الأساسية (إختياري):



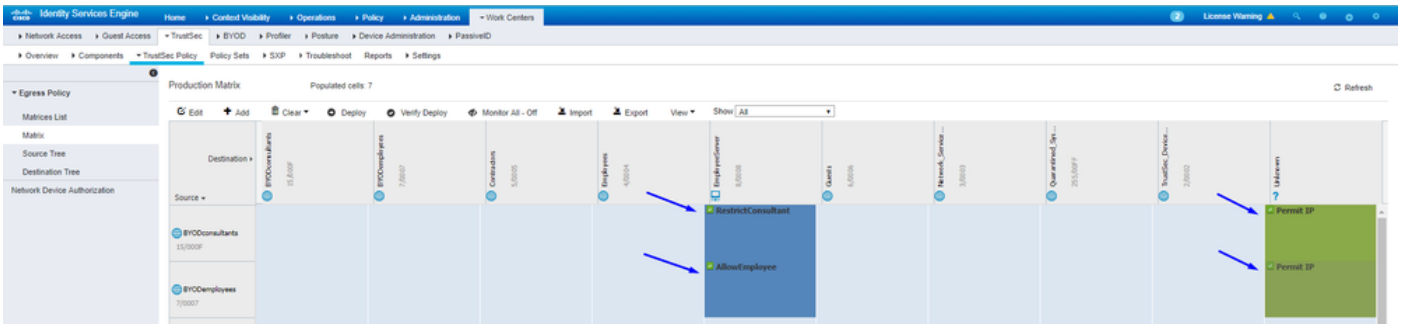
إعادة توجيه جميع المستخدمين النهائيين إلى Cisco ISE (إعادة توجيه مدخل BYOD). ال تقم بتضمين حركة مرور DNS أو DHCP أو ping أو WebAuth ألنها ال يمكن أن تنتقل إلى Cisco ISE:



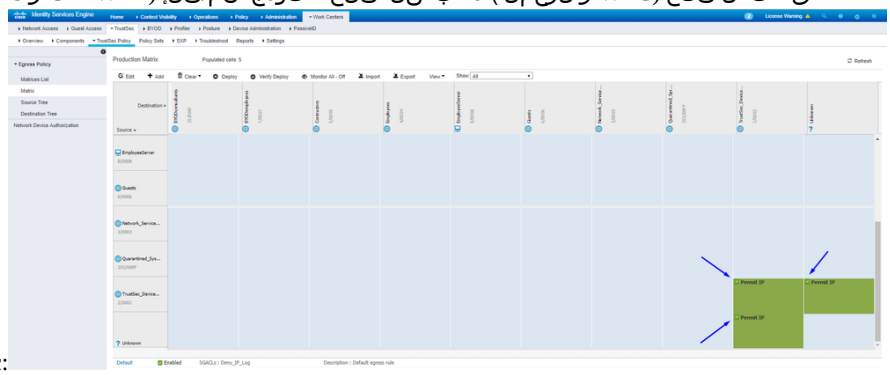
فرض قوائم التحكم في الوصول (ACL) الخاصة بك على مصفوفة سياسة TrustSec في Cisco ISE

السماح للمستشاريين بالوصول إلى أي مكان خارجي، ولكن تقييد خوادم الويب الداخلية، مثل https://10.201.214.132

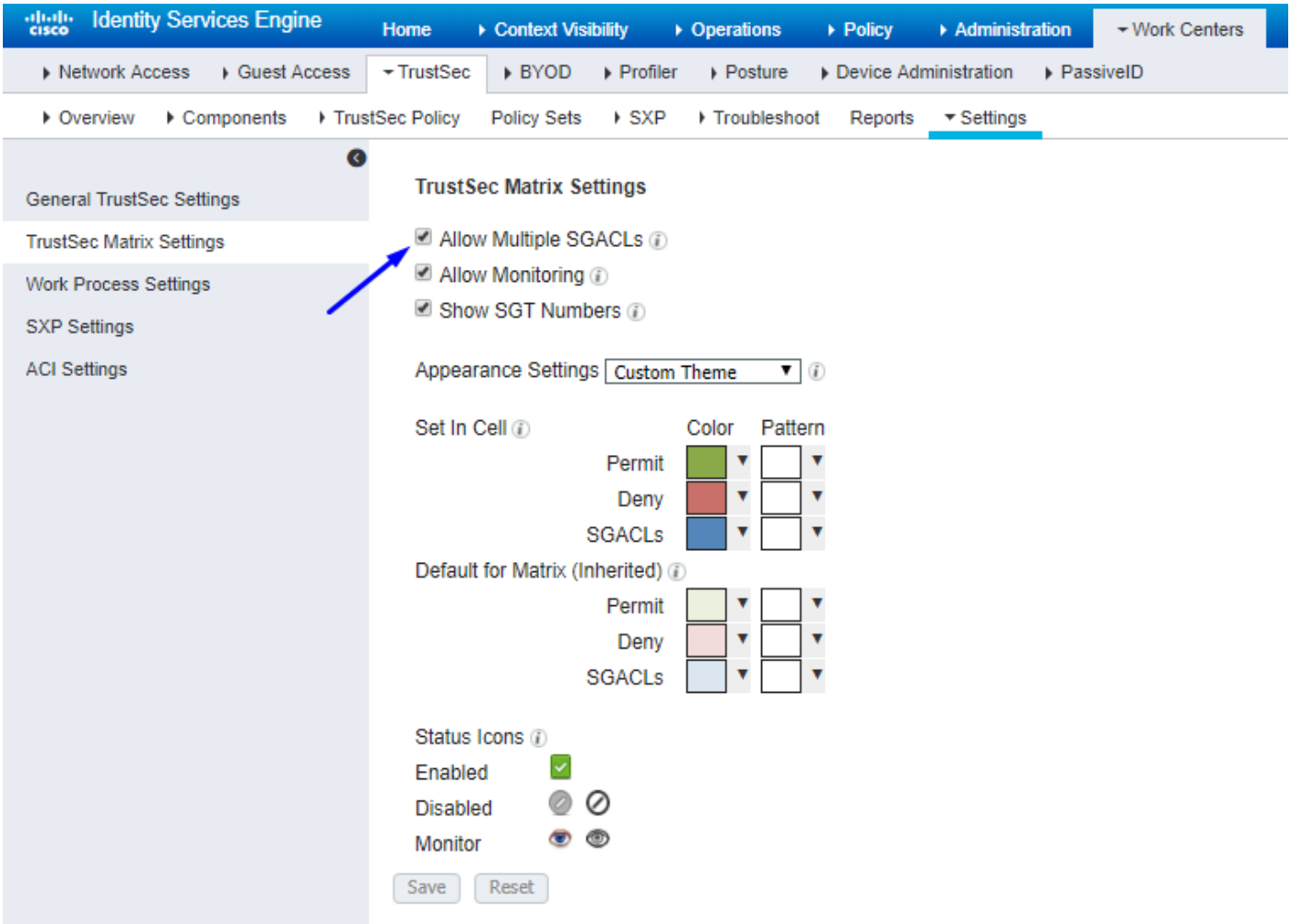
السماح للموظفين بالوصول إلى أي مكان خارجي والسماح بخوادم ويب الداخلية:



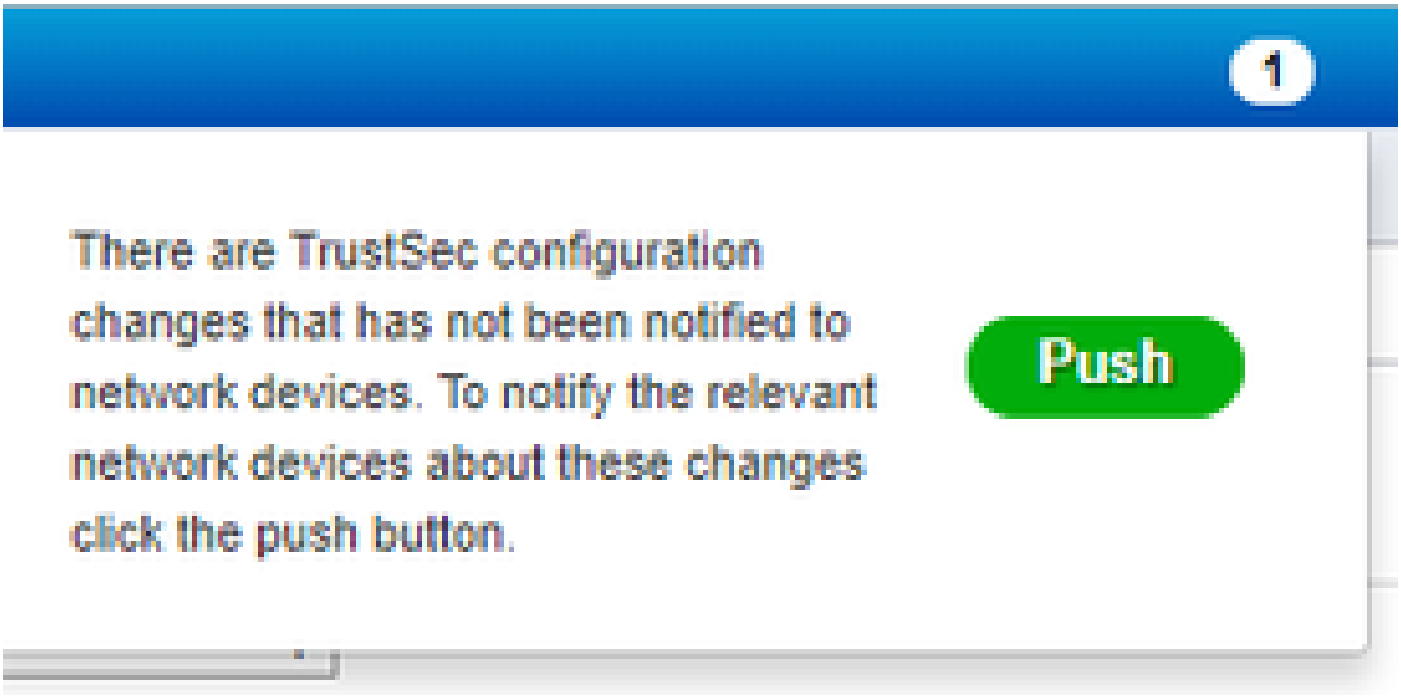
السماح بحركة مرور بيانات الإدارة (SSH و HTTPS و CAPWAP) إلى/من أجهزتك على الشبكة (المحول و WLC) حتى لا تفقد وصول SSH أو HTTPS بمجرد نشر Cisco TrustSec:



تمكين Cisco ISE من Allow Multiple SGACLs:

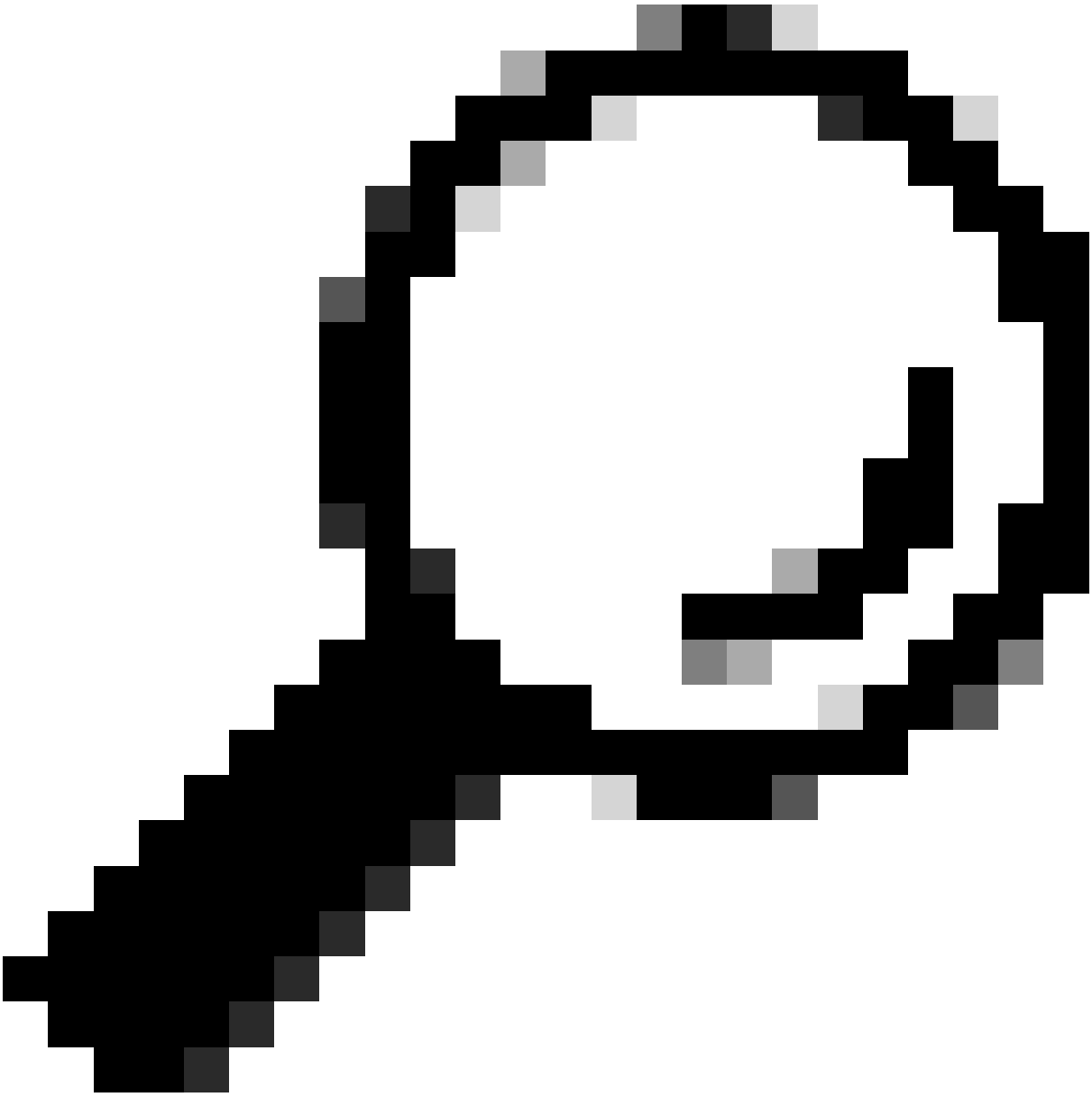


انقر Push في الزاوية العليا اليمنى من Cisco ISE، لدفع التكوين الخاص بك لأسفل إلى أجهزتك. يجب عليك القيام بذلك مرة أخرى لاحقا أيضا:



تكوين TrustSec على محول Catalyst

تكوين المحول لاستخدام Cisco TrustSec ل AAA على محول Catalyst



تلميح: يفترض هذا المستند أن المستخدمين اللاسلكيين لديك انجحوا بالفعل في BYOD بواسطة Cisco ISE قبل التكوين الظاهر هنا.

تم تكوين الأوامر الموضحة بالأسود مسبقا قبل هذا (لكي تعمل وحدة BYOD Wireless مع ISE).

<#root>

CatalystSwitch(config)#aaa new-model

CatalystSwitch(config)#aaa server radius policy-device

CatalystSwitch(config)#ip device tracking

CatalystSwitch(config)#radius server CISCOISE

CatalystSwitch(config-radius-server)#address ipv4 10.201.214.230 auth-port 1812 acct-port 1813

CatalystSwitch(config)#aaa group server radius AAASERVER
CatalystSwitch(config-sg-radius)#server name CISCOISE

CatalystSwitch(config)#aaa authentication dot1x default group radius
CatalystSwitch(config)#cts authorization list SGLIST
CatalystSwitch(config)#aaa authorization network SGLIST group radius

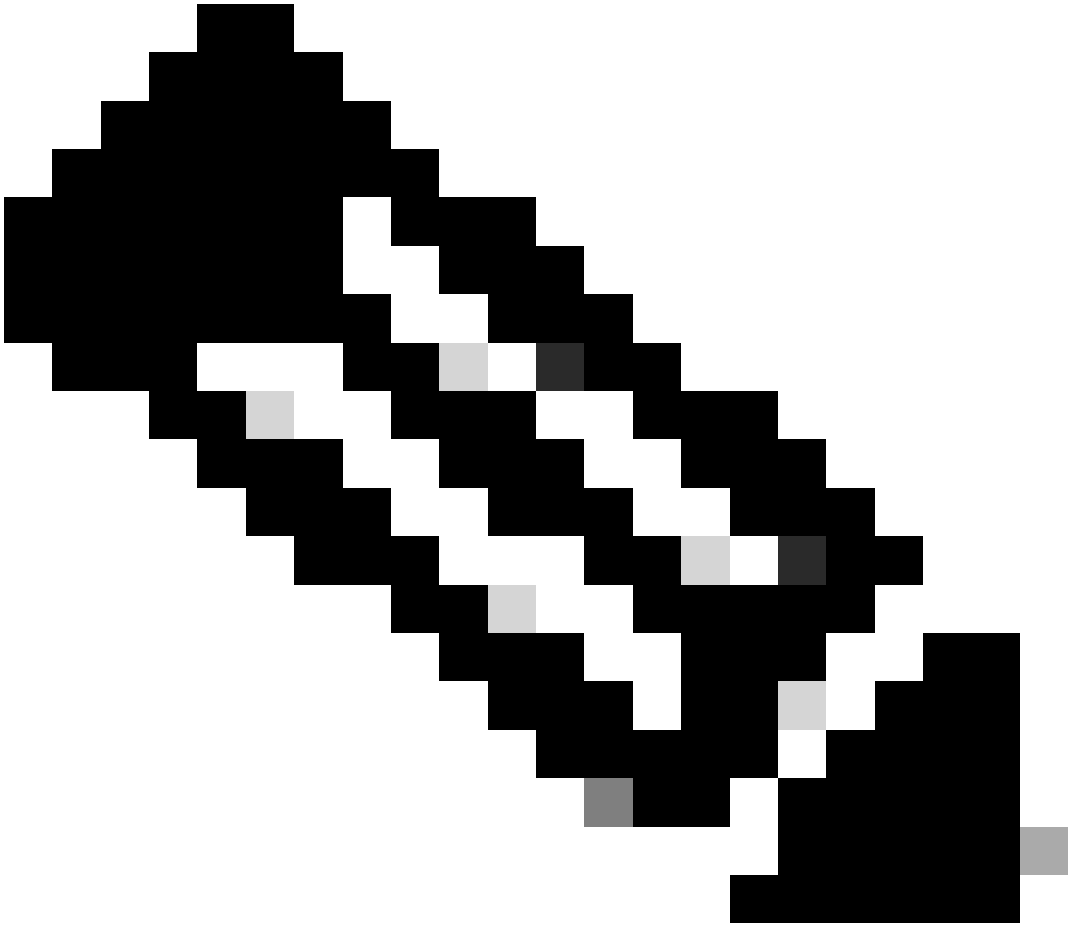
CatalystSwitch(config)#aaa authorization network default group AAASERVER

CatalystSwitch(config)#aaa authorization auth-proxy default group AAASERVER

CatalystSwitch(config)#aaa accounting dot1x default start-stop group AAASERVER

CatalystSwitch(config)#aaa server radius policy-device

CatalystSwitch(config)#aaa server radius dynamic-author
CatalystSwitch(config-locsvr-da-radius)#client 10.201.214.230 server-key Admin123



ملاحظة: يجب أن يكون مفتاح مسوغات الوصول المحمي هو نفسه سر RADIUS المشترك الذي حددته في **Administration** > **Network Devices** > **Add Device** > **RADIUS Authentication Settings** القسم.

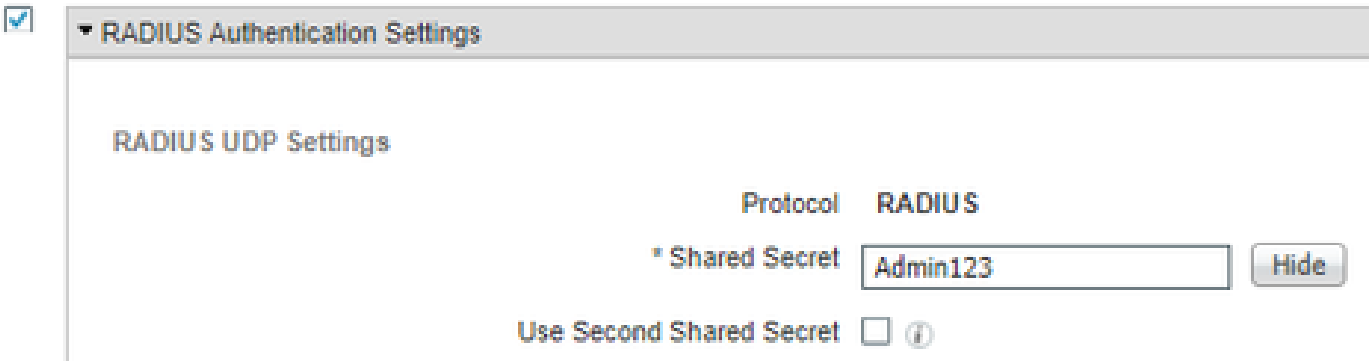
<#root>

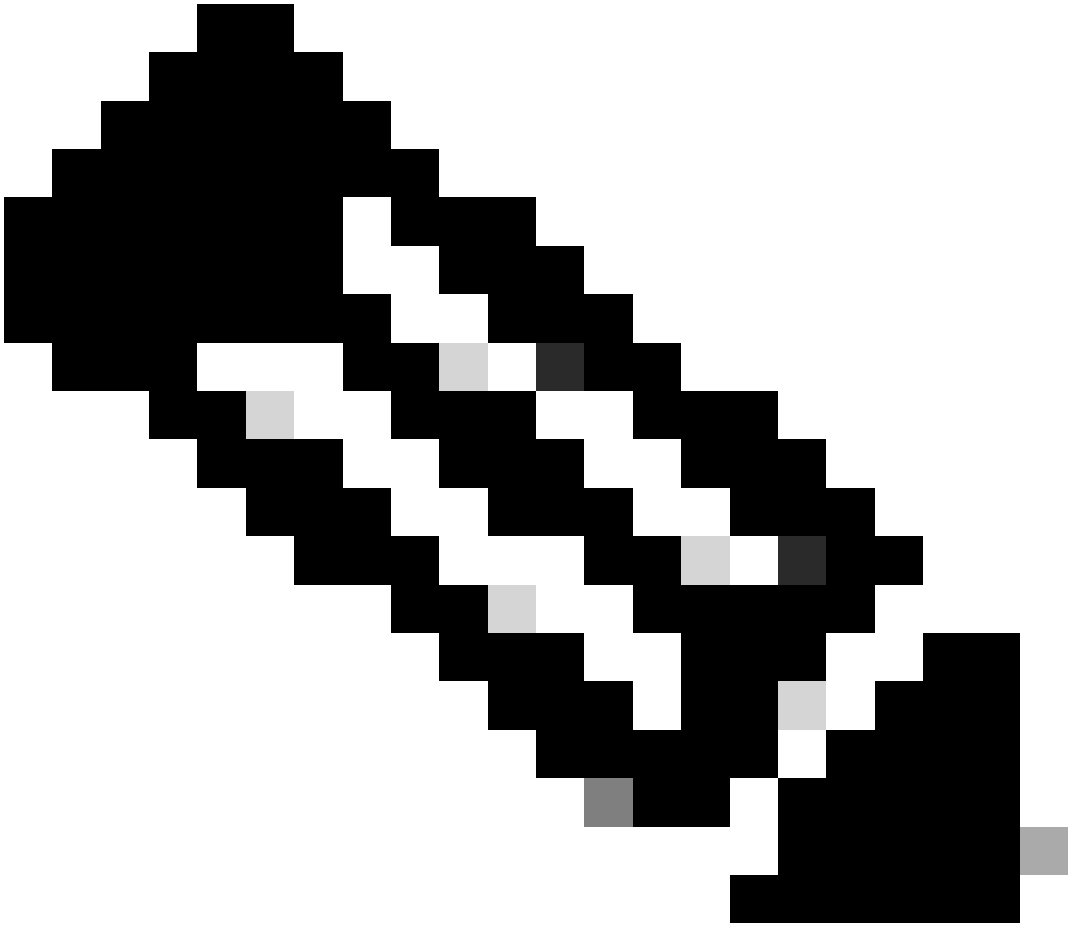
```
CatalystSwitch(config)#radius-server attribute 6 on-for-login-auth

CatalystSwitch(config)#radius-server attribute 6 support-multiple
```

```
CatalystSwitch(config)#radius-server attribute 8 include-in-access-req


CatalystSwitch(config)#radius-server attribute 25 access-request include


CatalystSwitch(config)#radius-server vsa send authentication
CatalystSwitch(config)#radius-server vsa send accounting

CatalystSwitch(config)#dot1x system-auth-control
```

تكوين مفتاح PAC ضمن خادم RADIUS لمصادقة المحول على Cisco ISE

```
CatalystSwitch(config)#radius server CISCOISE
CatalystSwitch(config-radius-server)#address ipv4 10.201.214.230 auth-port 1812 acct-port 1813
CatalystSwitch(config-radius-server)#pac key Admin123
```

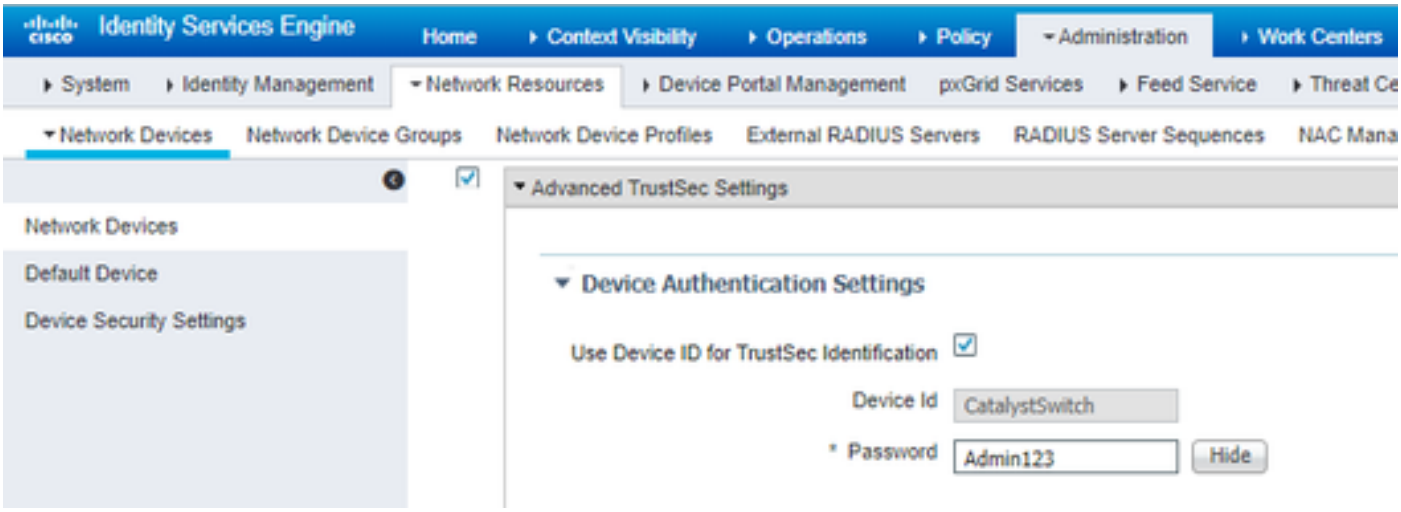


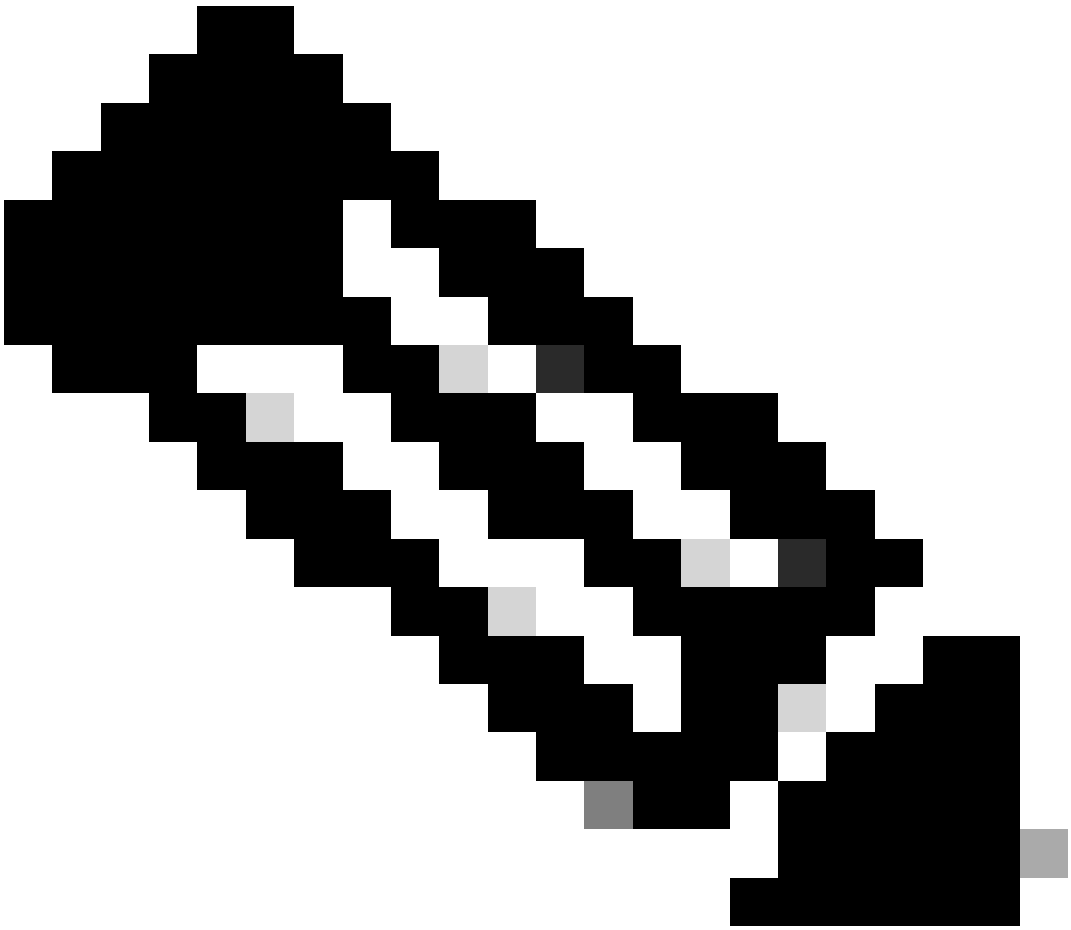


ملاحظة: يجب أن يكون مفتاح مسوغات الوصول المحمي وه نفسه سر RADIUS المشترك الذي حددته تحت **Administration** > **Network Devices** > **Add Device** > **RADIUS Authentication Settings** القسم في Cisco ISE (كما هو موضح في التقاط الشاشة).

تكوين بيانات اعتماد CTS لمصادقة المحول على Cisco ISE

```
CatalystSwitch#cts credentials id CatalystSwitch password Admin123
```





ملاحظة: يجب أن تكون بيانات اعتماد CTS هي نفسها معرف الجهاز + كلمة المرور التي حددتها في بيانات اعتماد CTS يجب أن تكون نفسها معرف الجهاز + كلمة المرور التي حددتها في Administration > Network Devices > Add Device >

Advanced TrustSec Settings القسم في Cisco ISE (يظهر في التقاط الشاشة).

بعد ذلك، قم بتحديث ثيسوم غوسم الوصول المحمي الخاص بك حتى يصل إلى Cisco ISE مرة أخرى:

```
CatalystSwitch(config)#radius server CISCOISE
CatalystSwitch(config-radius-server)#exit
 Request successfully sent to PAC Provisioning driver.
```

تمكين CTS بشكل عام على محول Catalyst

```
CatalystSwitch(config)#cts role-based enforcement
CatalystSwitch(config)#cts role-based enforcement vlan-list 1115 (choose the vlan that your end user devices are on only)
```

تعيين ثابت من IP إلى SGT لخوادم الويب المحظورة (إختياري)

الا يأتي خادم الويب المقيد من الخلال ISE للمصادقة أبدا، لذلك يجب عليك تمييزه يدويا باستخدام Switch CLI أو ISE Web GUI، والذي يعد واحد من العديد من خوادم الويب في Cisco.

```
CatalystSwitch(config)#cts role-based sgt-map 10.201.214.132 sgt 8
```

التحقق من TrustSec على محول Catalyst

```
CatalystSwitch#show cts pac
 AID: EF2E1222E67EB4630A8B22D1FF0216C1
 PAC-Info:
 PAC-type = Cisco Trustsec
 AID: EF2E1222E67EB4630A8B22D1FF0216C1
 I-ID: CatalystSwitch
 A-ID-Info: Identity Services Engine
 Credential Lifetime: 23:43:14 UTC Nov 24 2018
 PAC-Opaque: 000200B80003000100040010EF2E1222E67EB4630A8B22D1FF0216C10006009C0003010025D40D409A0DDAF352A3F1A9884AC3F6
 Refresh timer is set for 12w5d
```

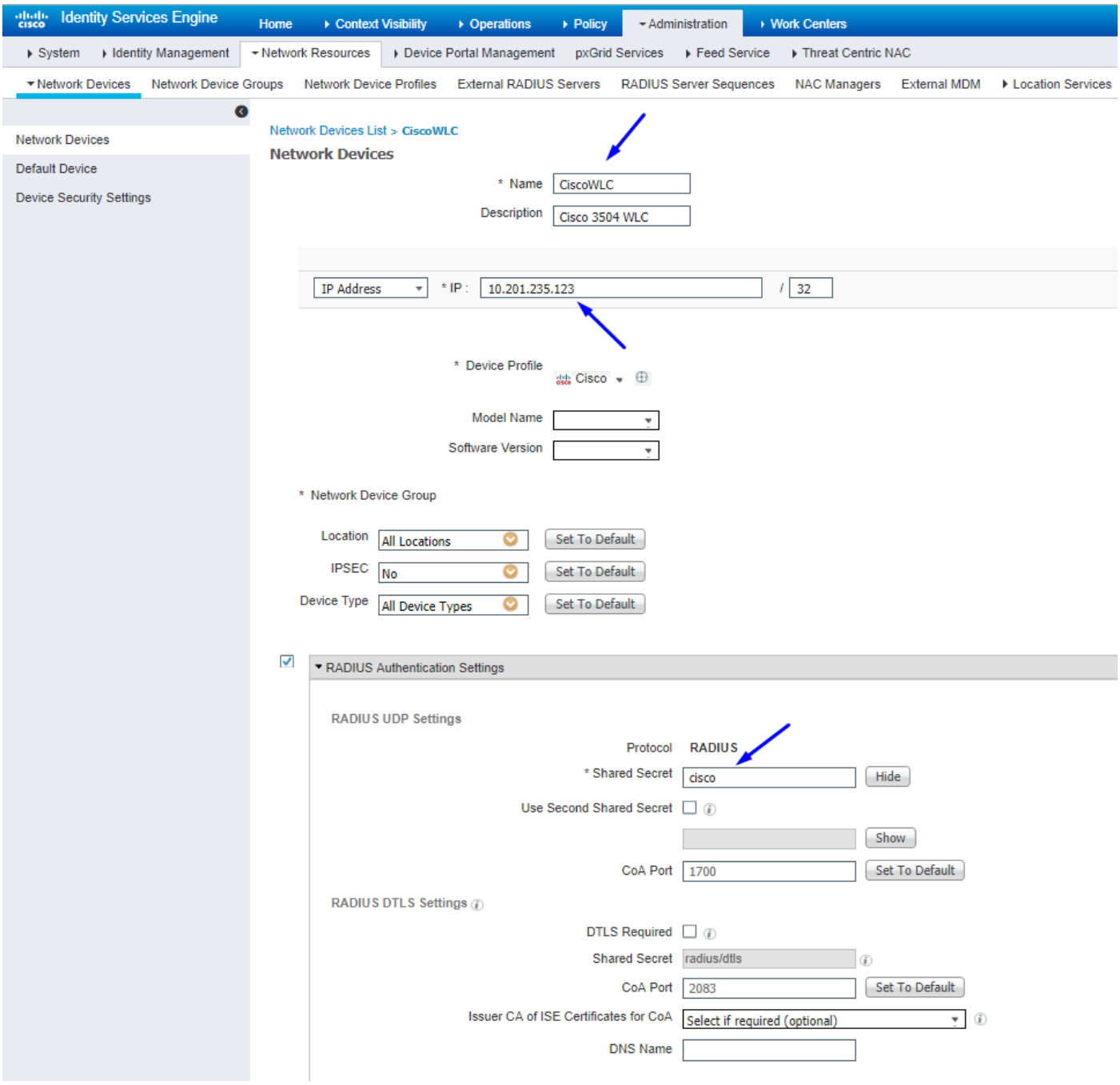
```
CatalystSwitch#cts refresh environment-data
Environment data download in progress
```

```
CatalystSwitch#show cts environment-data
CTS Environment Data
====================
Current state = COMPLETE
Last status = Successful
Local Device SGT:
 SGT tag = 2-02:TrustSec_Devices
Server List Info:
Installed list: CTSServerList1-0001, 1 server(s):
 *Server: 10.201.214.230, port 1812, A-ID EF2E1222E67EB4630A8B22D1FF0216C1
 Status = ALIVE flag(0x11)
 auto-test = TRUE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime = 20 secs
Multicast Group SGT Table:
Security Group Name Table:
 0001-31 :
 0-00:Unknown
 2-00:TrustSec_Devices
 3-00:Network_Services
 4-00:Employees
 5-00:Contractors
 6-00:Guests
 7-00:BYODemployees
 8-00:EmployeeServer
 15-00:BYODconsultants
 255-00:Quarantined_Systems
Transport type = CTS_TRANSPORT_IP_UDP
Environment Data Lifetime = 86400 secs
Last update time = 16:04:29 UTC Sat Aug 25 2018
Env-data expires in 0:23:57:01 (dd:hr:mm:sec)
Env-data refreshes in 0:23:57:01 (dd:hr:mm:sec)
Cache data applied = NONE
State Machine is running
```

```
CatalystSwitch#show cts role-based sgt-map all
Active IPv4-SGT Bindings Information

IP Address SGT Source
============================================
10.201.214.132 8 CLI
10.201.235.102 2 INTERNAL

IP-SGT Active Bindings Summary
============================================
Total number of CLI bindings = 1
Total number of INTERNAL bindings = 1
Total number of active bindings = 2
```

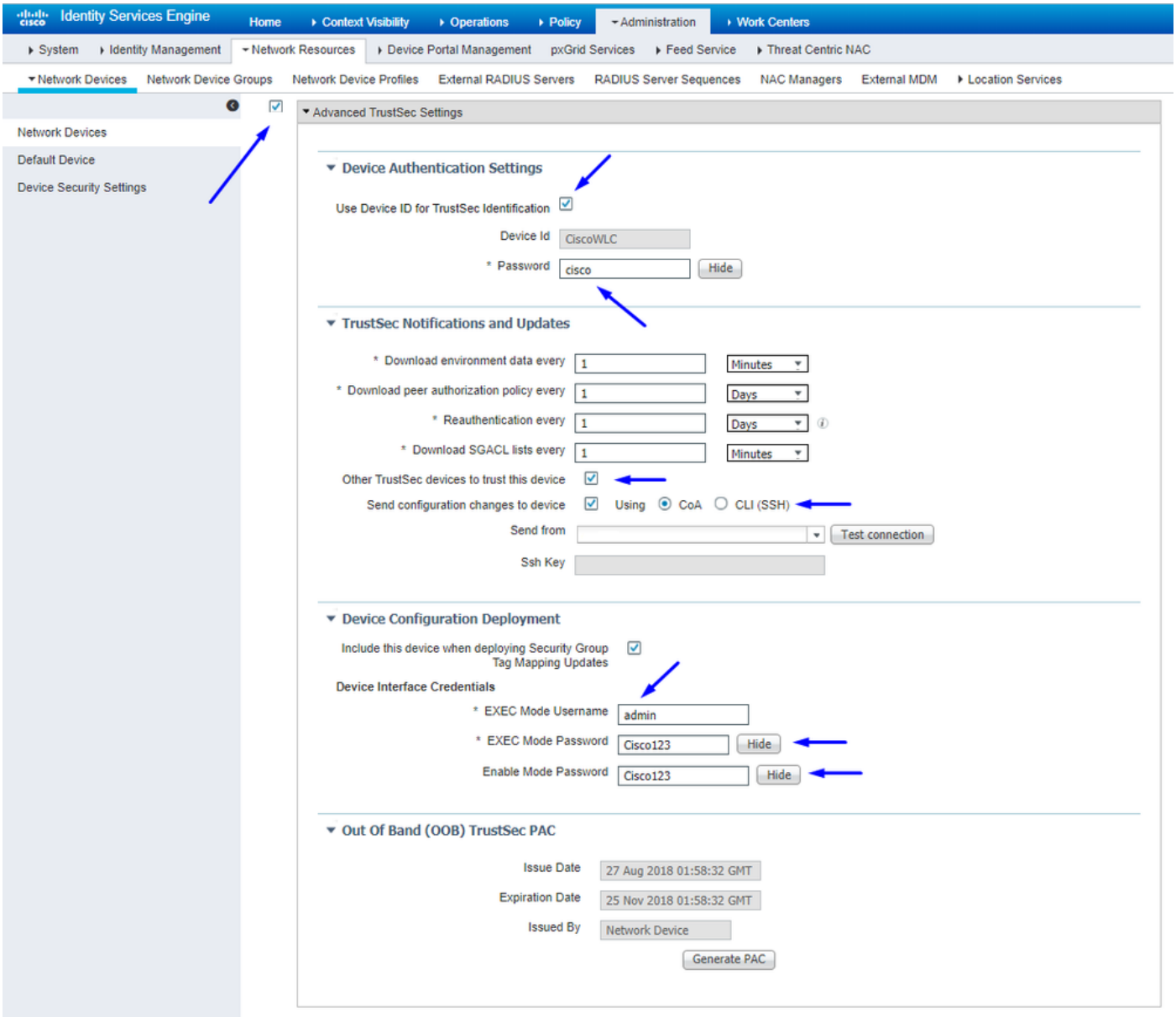
تكوين TrustSec على WLC

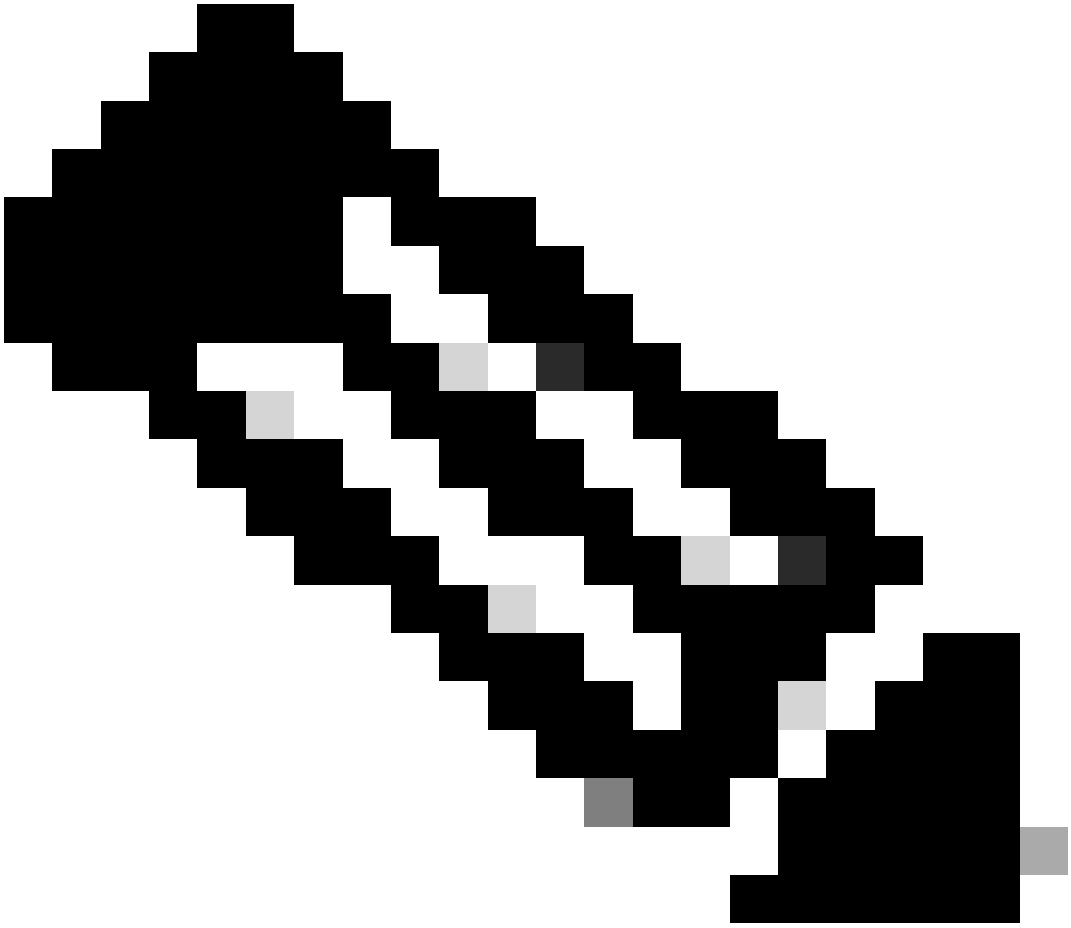
التكوين والتحقق من إضافة عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) كجهاز RADIUS في Cisco ISE



تتم إضافة تكوين عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) والتحقق منه كجهاز TrustSec في Cisco ISE

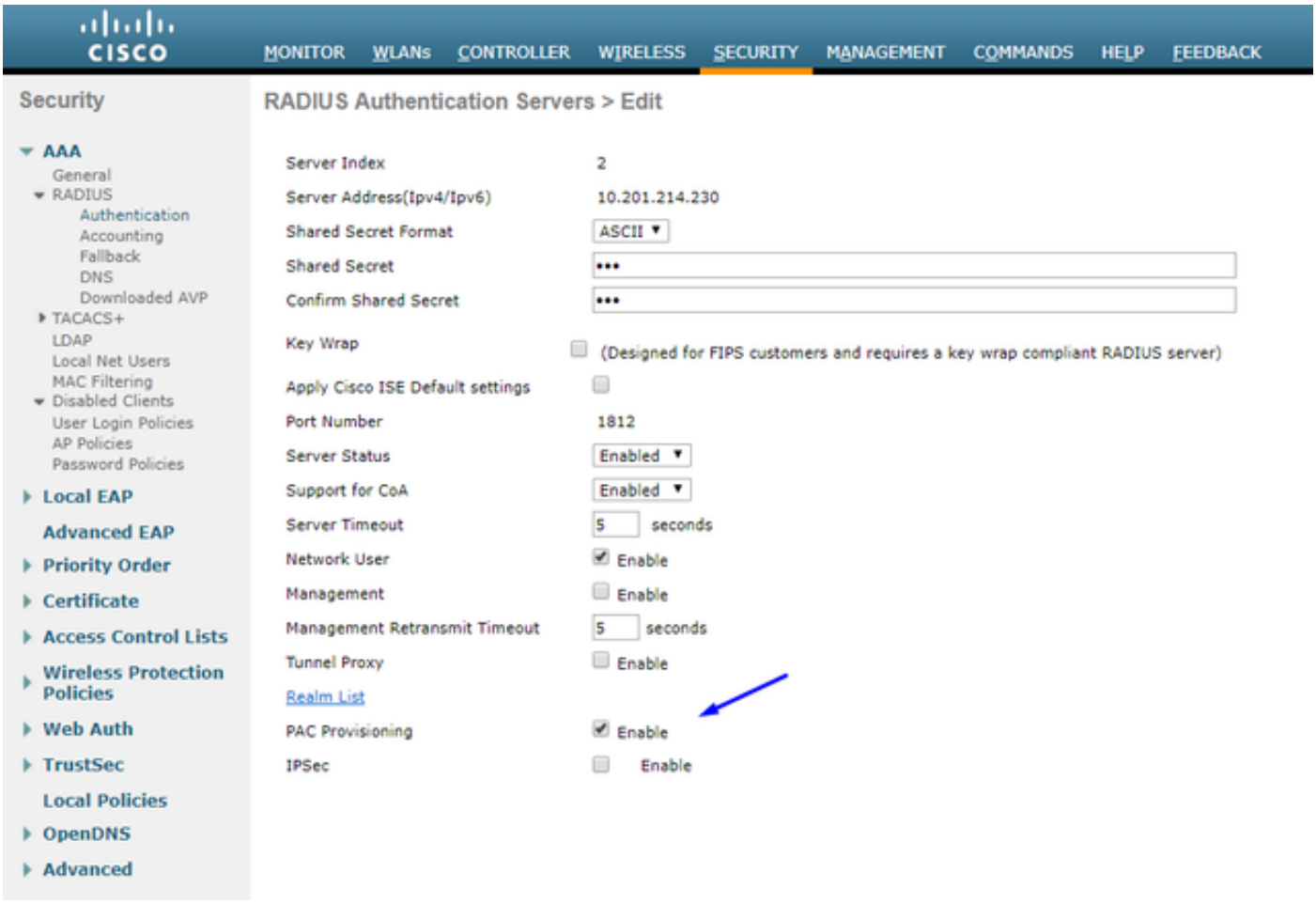
تمكن هذه الخطوة Cisco ISE من نشر تعيينات IP إلى الرقيب الثابتة إلى عنصر التحكم في الشبكة المحلية اللاسلكية (WLC). لقد قمت بإنشاء هذه التعيينات في واجهة المستخدم الرسومية (GUI) الخاصة ب Cisco ISE Web **GUI** في **مراكز العمل > TrustSec > المكونات > تعيينات IP الثابتة** لرقيب IP في خطوة سابقة.


Identity Services Engine
Home
Context Visibility
Operations
Policy
Administration
Work Centers
System
Identity Management
Network Resources
Device Portal Management
pxGrid Services
Feed Service
Threat Centric NAC
Network Devices
Network Device Groups
Network Device Profiles
External RADIUS Servers
RADIUS Server Sequences
NAC Managers
External MDM
Location Services
Network Devices
Default Device
Device Security Settings
Advanced TrustSec Settings
Device Authentication Settings
Use Device ID for TrustSec Identification
Device Id
CiscoWLC
* Password
cisco
Hide
TrustSec Notifications and Updates
* Download environment data every
1
Minutes
* Download peer authorization policy every
1
Days
* Reauthentication every
1
Days
* Download SGACL lists every
1
Minutes
Other TrustSec devices to trust this device
Send configuration changes to device
Using
CoA
CLI (SSH)
Send from
Test connection
Ssh Key
Device Configuration Deployment
Include this device when deploying Security Group Tag Mapping Updates
Device Interface Credentials
* EXEC Mode Username
admin
* EXEC Mode Password
Cisco123
Hide
Enable Mode Password
Cisco123
Hide
Out Of Band (OOB) TrustSec PAC
Issue Date
27 Aug 2018 01:58:32 GMT
Expiration Date
25 Nov 2018 01:58:32 GMT
Issued By
Network Device
Generate PAC

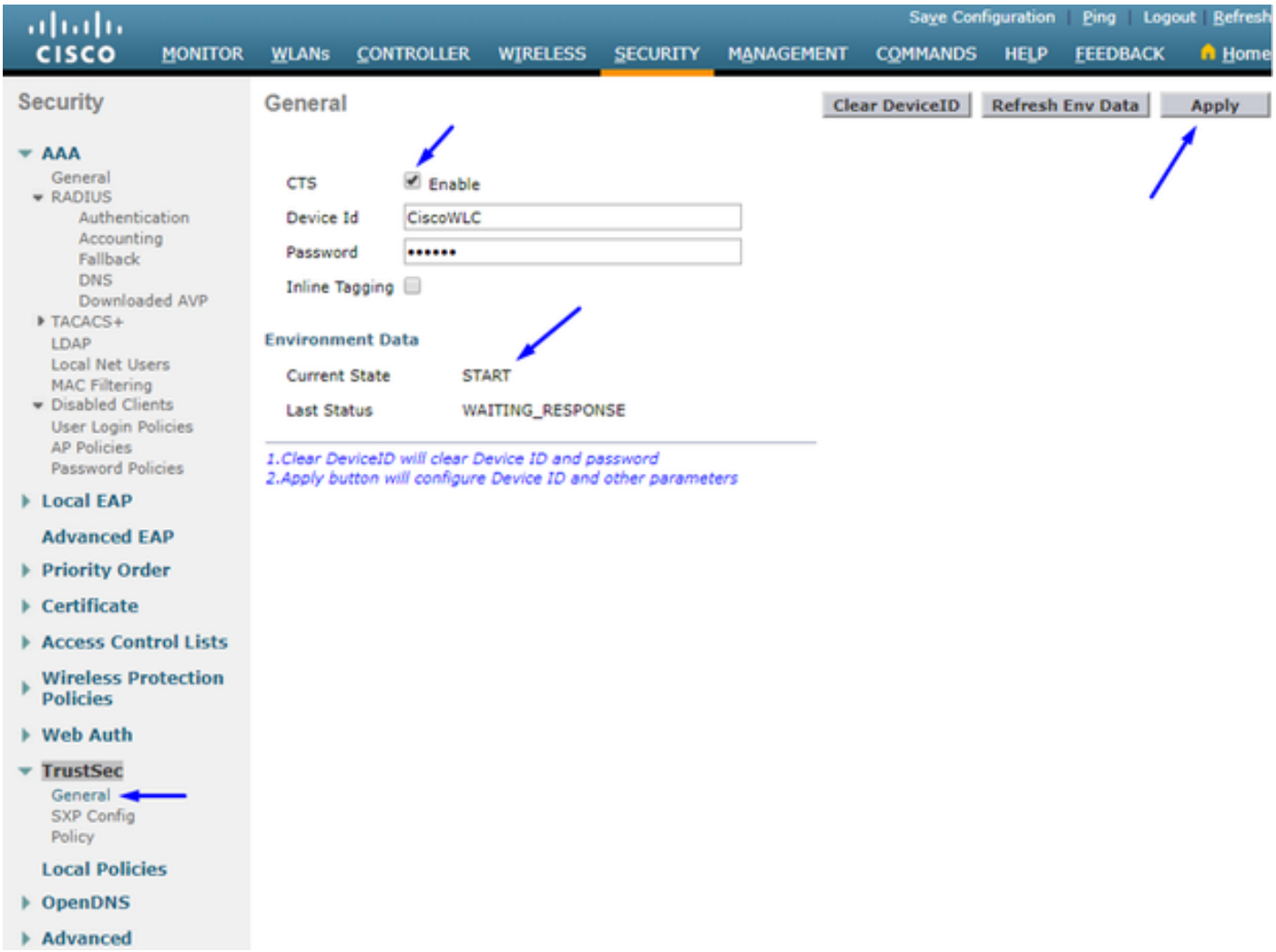


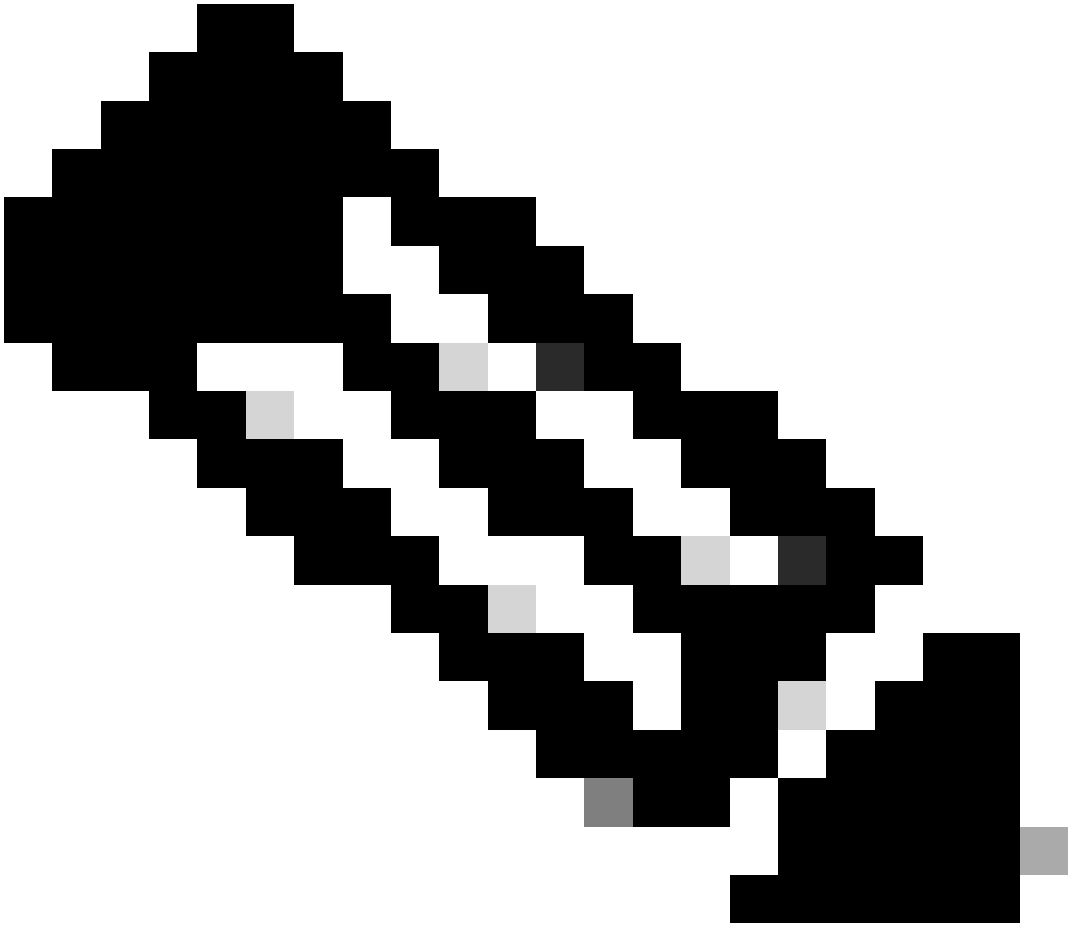
ملاحظة: نحن نستخدم هذه Device Id وفي خطوة Password الحالية، في Security > TrustSec > General واجهة مستخدم ويب WLC.

تمكين توفير مسوغات الوصول المحمي (PAC) من WLC



تمكين TrustSec على WLC

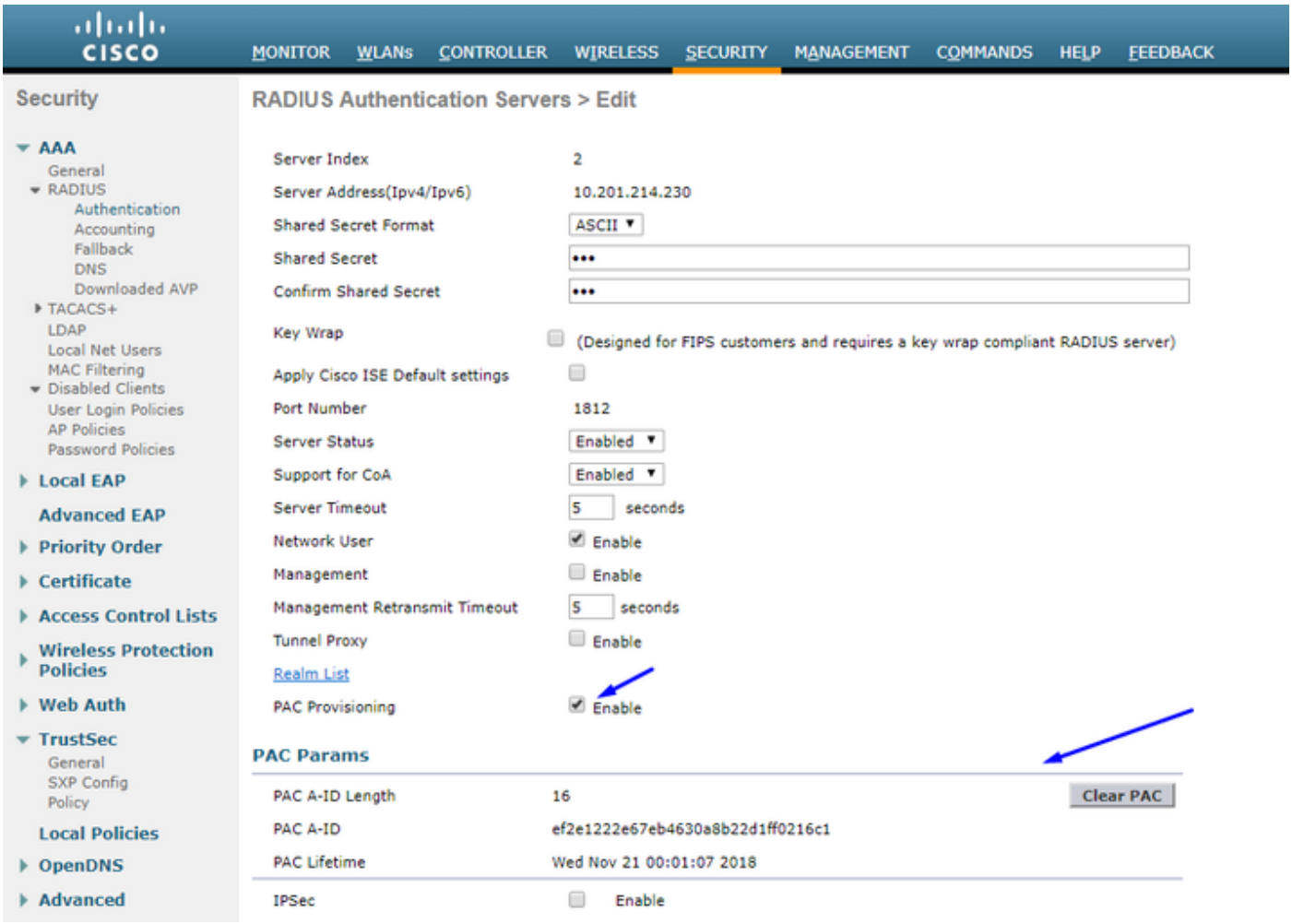

Save Configuration | Ping | Logout | Refresh
CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK Home
Security
AAA
General
RADIUS
Authentication
Accounting
Fallback
DNS
Downloaded AVP
TACACS+
LDAP
Local Net Users
MAC Filtering
Disabled Clients
User Login Policies
AP Policies
Password Policies
Local EAP
Advanced EAP
Priority Order
Certificate
Access Control Lists
Wireless Protection Policies
Web Auth
TrustSec
General
SXP Config
Policy
Local Policies
OpenDNS
Advanced
General
Clear DeviceID
Refresh Env Data
Apply
CTS
Enable
Device Id
CiscoWLC
Password
Inline Tagging
Environment Data
Current State
START
Last Status
WAITING_RESPONSE
1.Clear DeviceID will clear Device ID and password
2.Apply button will configure Device ID and other parameters



ةظحالم: CTS Device Id وهيجب Password أن تكون هي نفسها Device Id وتلك Password التي حددتها في Administration > Network Devices > Add Device > Advanced TrustSec Settings القسم في Cisco ISE.

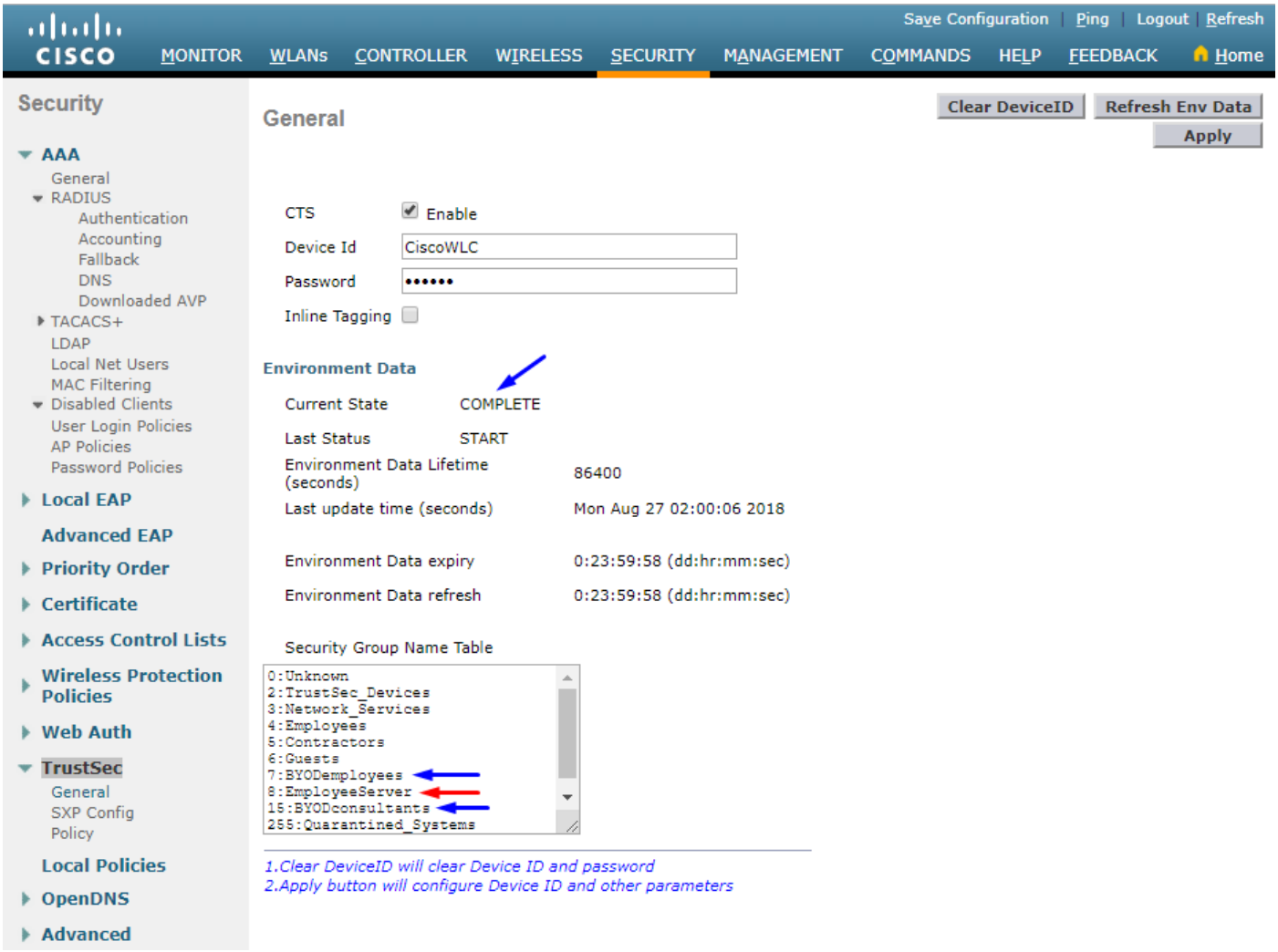
التحقق من توفير مسوغات الوصول المحمي (PAC) على عنصر التحكم في الشبكة المحلية اللاسلكية (WLC)

ترى أن عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) تم توفير مسوغ الوصول المحمي (PAC) بنجاح بعد النقرRefresh Env Data (توقوم بهذا في هذه الخطوة):



تنزيل بيانات بيئة CTS من Cisco ISE إلى WLC

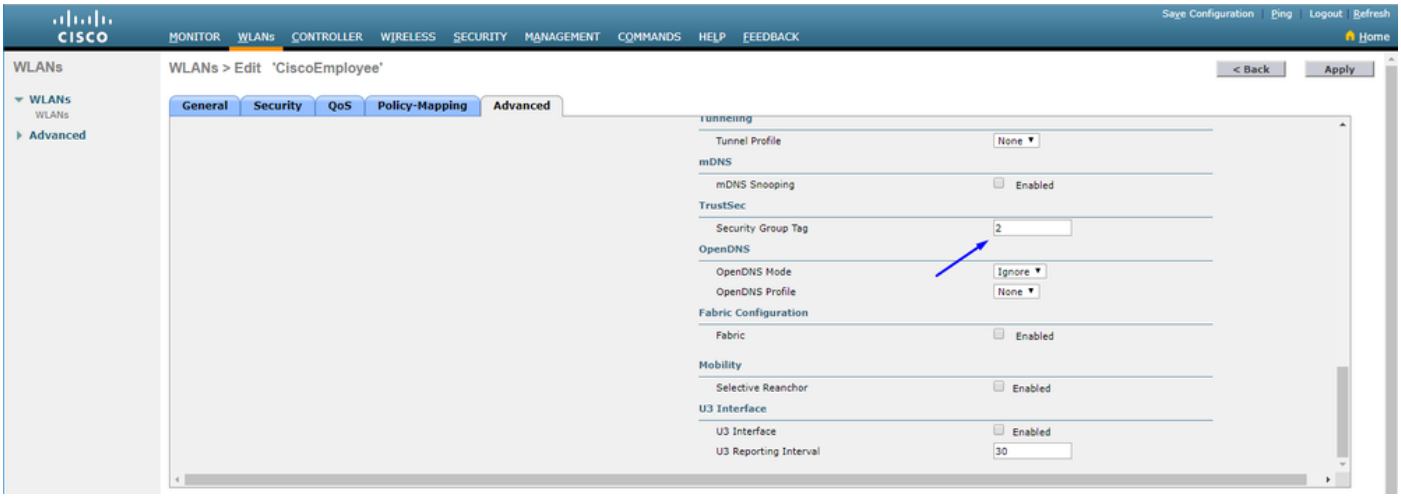
بعد النقرRefresh Env Data، تقوم وحدة التحكم في الشبكة المحلية اللاسلكية (WLC) بتنزيل الرقاع.



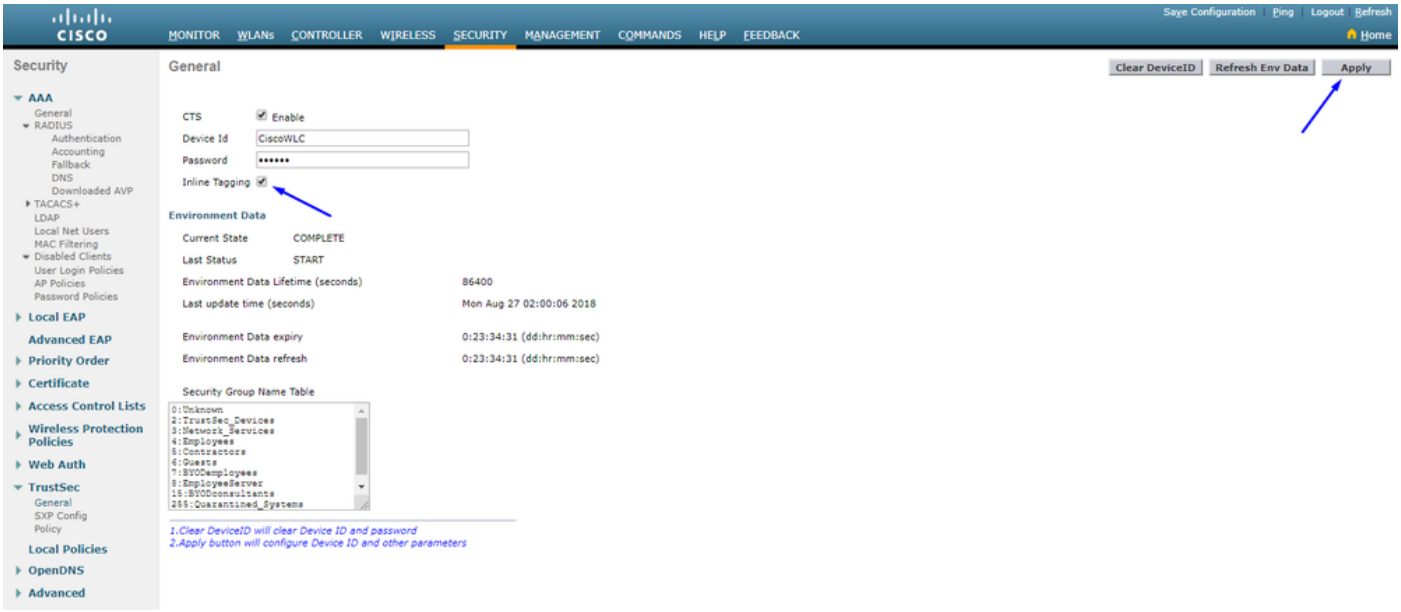
تمكين تنزيلات SGACL وتنفيذها على حركة المرور

قم بتخصيص عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) ونقطة الوصول مع الرقيب 2 (TrustSec_Devices)

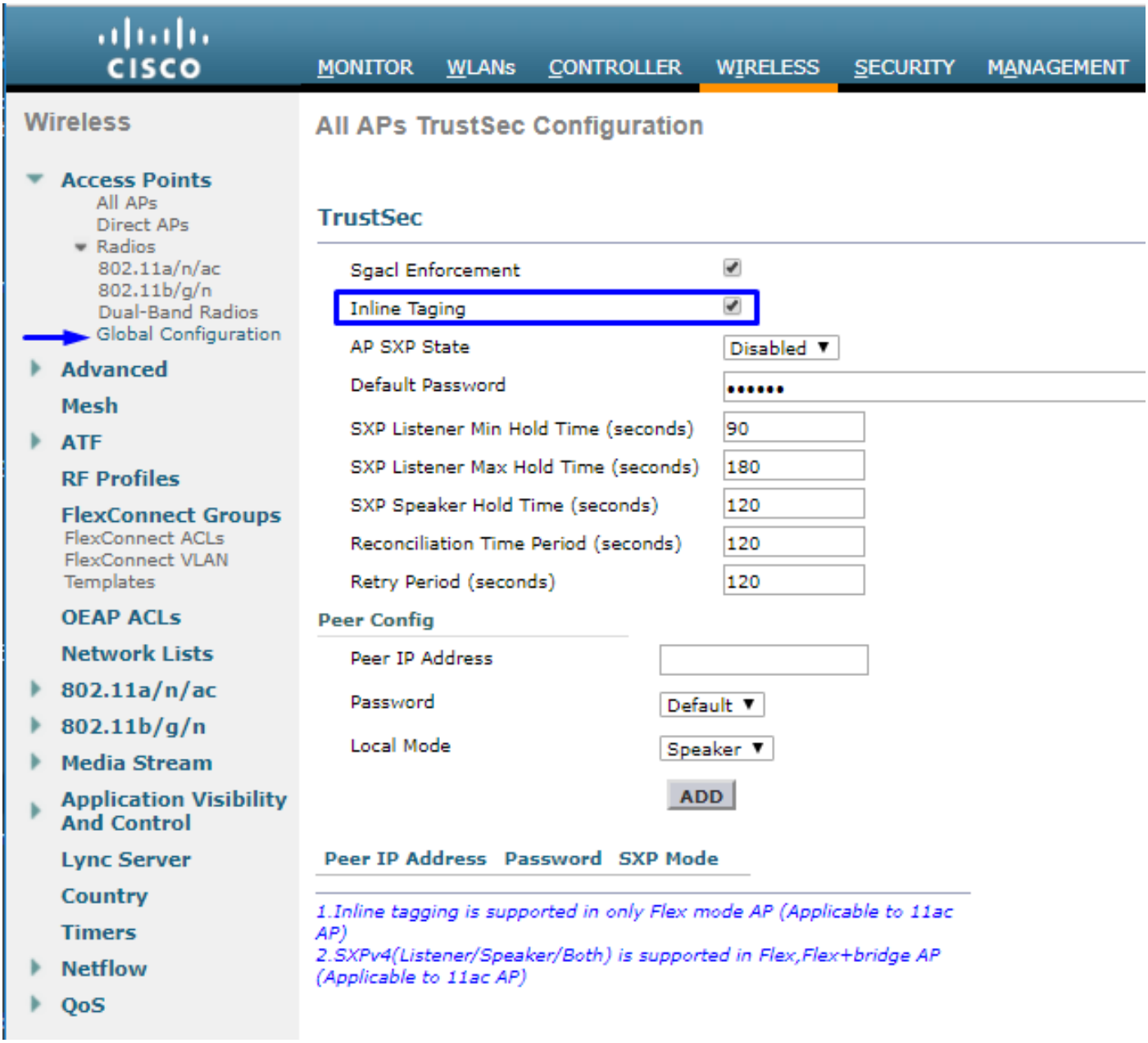
امنح عنصر التحكم في الشبكة المحلية اللاسلكية (WLC+WLAN) رقيبا من 2 (TrustSec_Devices) للسماح بحركة المرور إلى/من عنصر التحكم في الشبكة المحلية اللاسلكية (WLC) + نقطة الوصول من خلال المحول. (CAPWAP و HTTPS و SSH)



تمكين وضع العلامات داخل السطر على WLC



تحت **Wireless** > **Access Points** > **Global Configuration** انزلق لأسفل وحدد **TrustSec Config**.



تمكين وضع العلامات داخل السطر على محول Catalyst

<#root>

CatalystSwitch(config)#interface TenGigabitEthernet1/0/48

CatalystSwitch(config-if)#description goestoWLC

CatalystSwitch(config-if)#switchport trunk native vlan 15

CatalystSwitch(config-if)#switchport trunk allowed vlan 15,455,463,1115

CatalystSwitch(config-if)#switchport mode trunk

```
CatalystSwitch(config-if)#cts role-based enforcement
CatalystSwitch(config-if)#cts manual
CatalystSwitch(config-if-cts-manual)#policy static sgt 2 trusted
```

التحقق من الصحة

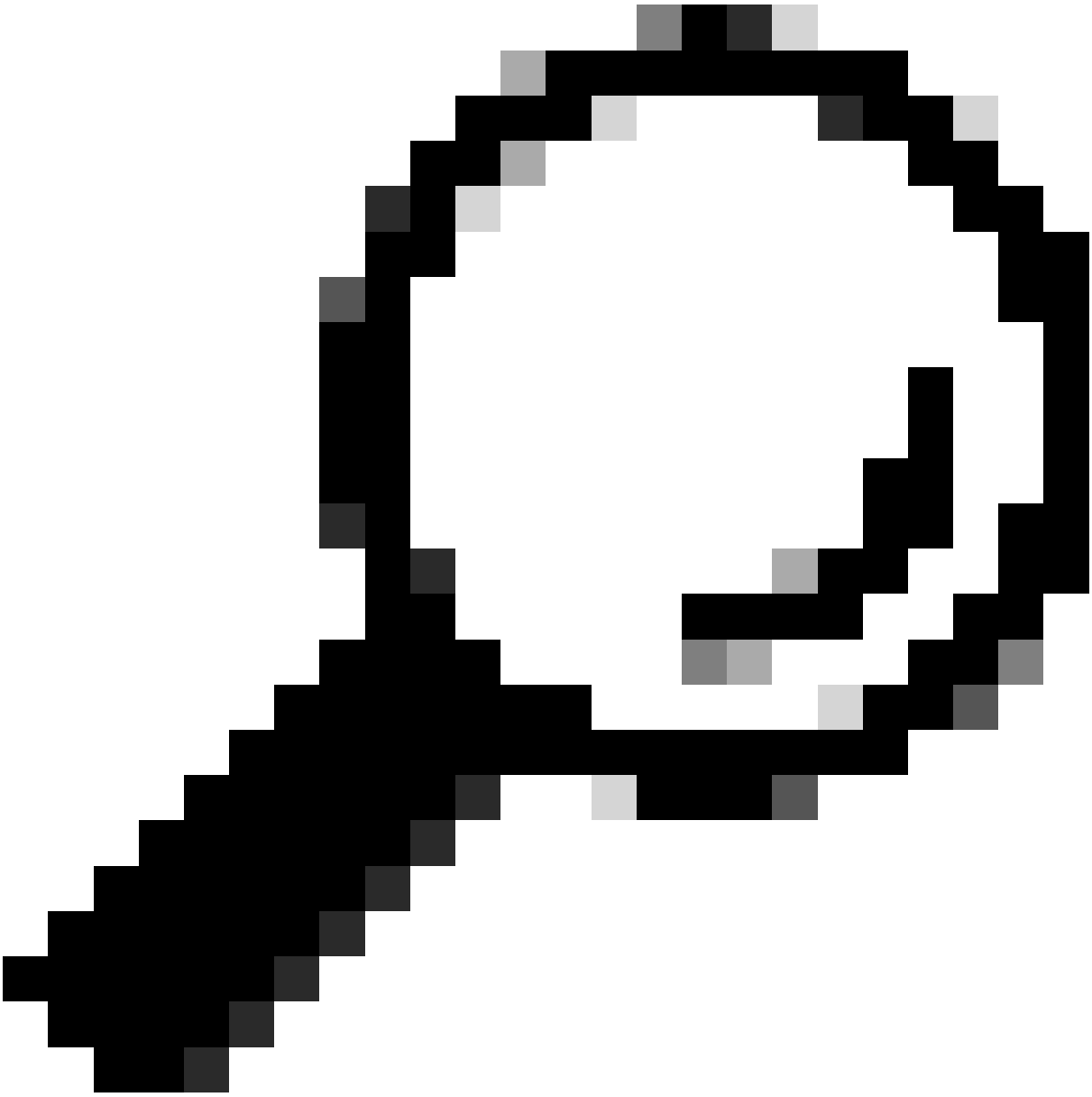
أجهزة عدادات قائمة التحكم في الوصول للنظام الأساسي Catalyst Switch#show | inc sgacl

إسقاط قائمة التحكم في الوصول الخاصة بالإصدار الرابع من بروتوكول الإنترنت (SGACL) عند الخروج (454): 10 إطارات

إسقاط قائمة التحكم في الوصول ل IPv6 (455) مخرج: 0 إطارات

إسقاط خلية IPv4 SGACL (456) من المخرج: 0 إطارات

إسقاط خلية IPv6 sgacl (457) مخرج: 0 إطارات



تلميح: إذا كنت تستخدم Cisco ASR أو Nexus أو Cisco ASA بدلا من ذلك، فيمكن للمستند المدرج هنا أن يساعد في التحقق من فرض عمليات الرقيب الخاص بك: دليل أستكشاف الأخطاء وإصلاحها TrustSec.

قم بالمصادقة على الشبكة اللاسلكية باستخدام اسم المستخدم jsmith password admin123 - تواجه قائمة التحكم في الوصول (ACL) للرفض في المجول:

This site can't be reached

10.201.214.132 took too long to respond.

Try:

Checking the connection

ERR_CONNECTION_TIMED_OUT

RELOAD

حول هذه الترجمة
ترجمت Cisco هذا المستند باستخدام مجموعة من التقنيات الآلية والبشرية لتقديم محتوى دعم للمستخدمين في جميع أنحاء العالم بلغتهم الخاصة. يُرجى ملاحظة أن أفضل ترجمة آلية لن تكون دقيقة كما هو الحال مع الترجمة الاحترافية التي يقدمها مترجم محترف. تخلي Cisco Systems مسئوليتها عن دقة هذه الترجمات وتُوصي بالرجوع دائمًا إلى المستند الإنجليزي الأصلي (الرابط متوفر).