ISE（インラインタギング）を使用したTrustSec(SGT)の設定

内容

はじめに

前提条件

- 要件
- 使用するコンポーネント

設定

- ネットワーク図
- 目標
- コンフィギュレーション
  - ISEでのTrustSecの設定
  - TrustSec AAAサーバとしてのCisco ISEの設定
  - スイッチがCisco ISEのRADIUSデバイスとして追加されるように設定および確認する
  - Cisco ISEでTrustSecデバイスとして追加されるWLCの設定と確認
  - TrustSecのデフォルト設定が許容可能であることを確認する（オプション）
  - ワイヤレスユーザ用のセキュリティグループタグの作成
  - 制限付きWebサーバのスタティックIP-to-SGTマッピングの作成
  - 証明書認証プロファイルの作成
  - 以前の証明書認証プロファイルを使用したIDソースシーケンスの作成
  - ワイヤレスユーザ（従業員およびコンサルタント）に適切なSGTを割り当てる
  - 実際のデバイス（スイッチおよびWLC）へのSGTの割り当て
  - 出力ポリシーを指定するSGACLの定義
  - Cisco ISEのTrustSecポリシーマトリックスでのACLの適用
- CatalystスイッチでのTrustSecの設定
  - CatalystスイッチでAAAにCisco TrustSecを使用するためのスイッチの設定
  - Cisco ISEに対してスイッチを認証するためのRADIUSサーバでのPACキーの設定
  - スイッチをCisco ISEに認証するためのCTSクレデンシャルの設定
  - CatalystスイッチでのCTSのグローバルな有効化
  - 制限付きWebサーバのスタティックIP-to-SGTマッピングの作成（オプション）
  - CatalystスイッチでのTrustSecの確認
- WLCでのTrustSecの設定
  - Cisco ISEでRADIUSデバイスとして追加されるWLCの設定と確認
  - Cisco ISEでTrustSecデバイスとして追加されるWLCの設定と確認
  - WLCのPACプロビジョニングの有効化
  - WLCでのTrustSecの有効化
  - PACがWLCでプロビジョニングされていることの確認
  - Cisco ISEからWLCへのCTS環境データのダウンロード
  - トラフィックに対するSGACLのダウンロードと適用の有効化
  - WLCとアクセスポイントに2のSGTを割り当てる(TrustSec_Devices)
  - WLCでのインラインタギングの有効化
  - Catalystスイッチでのインラインタギングの有効化

確認

はじめに

このドキュメントでは、Identity Services Engine(ISE)を使用して、Catalystスイッチおよびワイヤレス LANコントローラ(WLC)上でTrustSecを設定および確認する方法について説明します。

前提条件

次の項目に関する知識があることが推奨されます。

- Cisco TrustSec(CTS)コンポーネントの基礎知識
- Catalyst スイッチの CLI 設定に関する基本的な知識
- CiscoワイヤレスLANコントローラ(WLC)のGUI設定に関する基本的な知識
- Identity Services Engine（ISE）設定の経験

要件

Cisco ISEをネットワークに導入し、エンドユーザがワイヤレスまたは有線に接続する際は、802.1x（またはその他の方法）でCisco ISEに認証する必要があります。Cisco ISEは、ワイヤレスネットワークへの認証後に、トラフィックにセキュリティグループタグ(SGT)を割り当てます。

この例では、エンドユーザはCisco ISEの個人所有デバイスの持ち込み(BYOD)ポータルにリダイレクトされ、証明書がプロビジョニングされます。これにより、エンドユーザはBYODポータルの手順を完了した後、Extensible Authentication Protocol-Transport Layer Security(EAP-TLS)を使用してワイヤレスネットワークに安全にアクセスできます。

使用するコンポーネント

このドキュメントの情報は、次のハードウェアとソフトウェアのバージョンに基づいています。

- Cisco Identity Services Engineバージョン2.4
- Cisco Catalyst 3850スイッチバージョン3.7.5E
- Cisco WLCバージョン8.5.120.0
- ローカルモードのCisco Aironetワイヤレスアクセスポイント

Cisco TrustSecを導入する前に、ご使用のCisco CatalystスイッチまたはCisco WLC+APモデル+ソフトウェアバージョンで次の機能がサポートされていることを確認します。

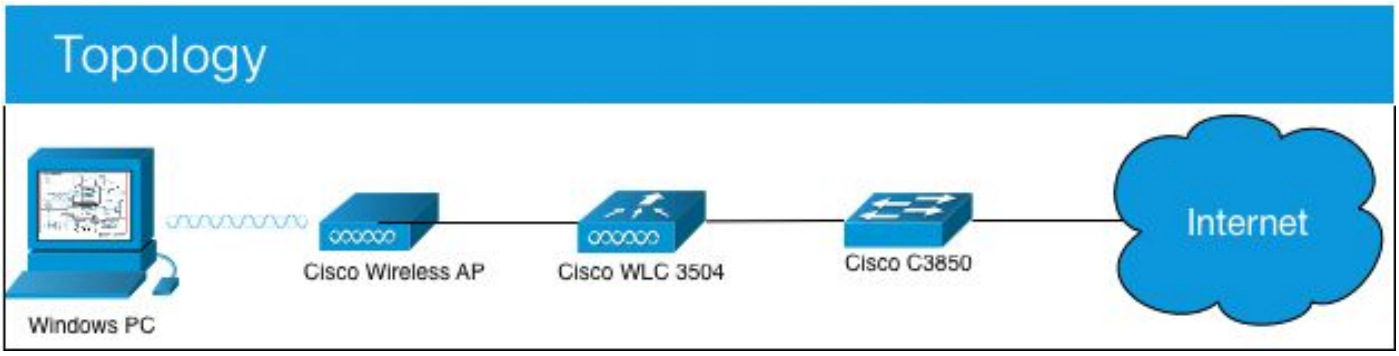
- TrustSec/セキュリティグループタグ
- インラインタギング（使用しない場合は、インラインタギングの代わりにSXPを使用できます）
- IPからSGTへの静的マッピング（必要に応じて）
- サブネットからSGTへのスタティックマッピング（必要な場合）
- VLANからSGTへのスタティックマッピング（必要な場合）

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始していま

す。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

設定

ネットワーク図



この例では、WLCは、コンサルタントからの場合はSGT 15、従業員からの場合は+ SGT 7としてパケットをタグ付けします。

これらのパケットがSGT 15からSGT 8の場合、スイッチはこれらのパケットを拒否します（コンサルタントはSGT 8としてタグ付けされたサーバにアクセスできません）。

スイッチは、SGT 7からSGT 8のパケットを許可します（従業員はSGT 8としてタグ付けされたサーバにアクセスできます）。

目標

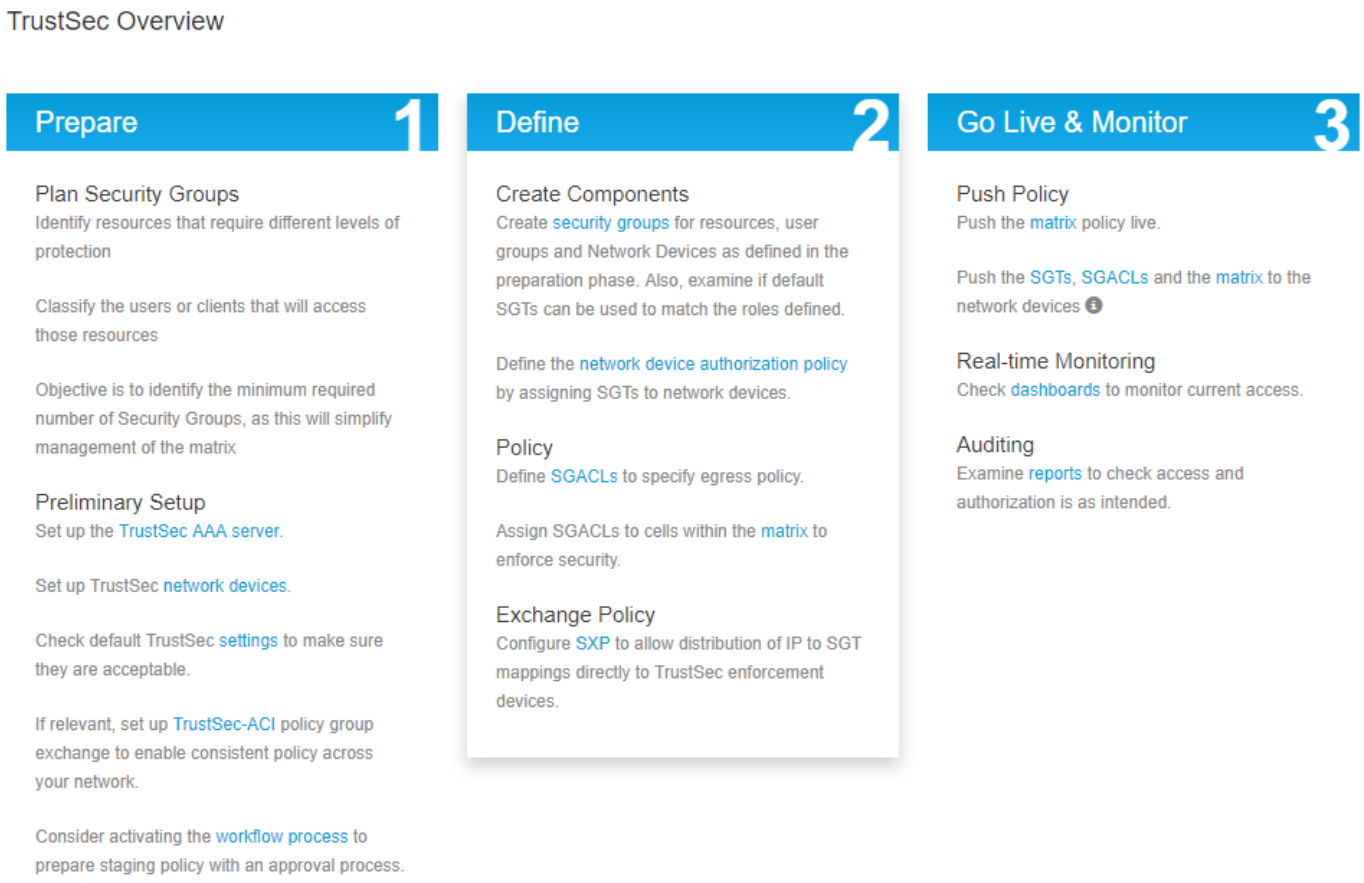
誰でもGuestSSIDにアクセスできる。
コンサルタントはEmployeeSSIDにアクセスできるが、アクセスは制限される
従業員はフルアクセスでEmployeeSSIDにアクセスできます。

デバイス	IP アドレス	VLAN
ISE	10.201.214.230	463
Catalyst スイッチ	10.201.235.102	1115
WLC	10.201.214.229	463
アクセス ポイント	10.201.214.138	455

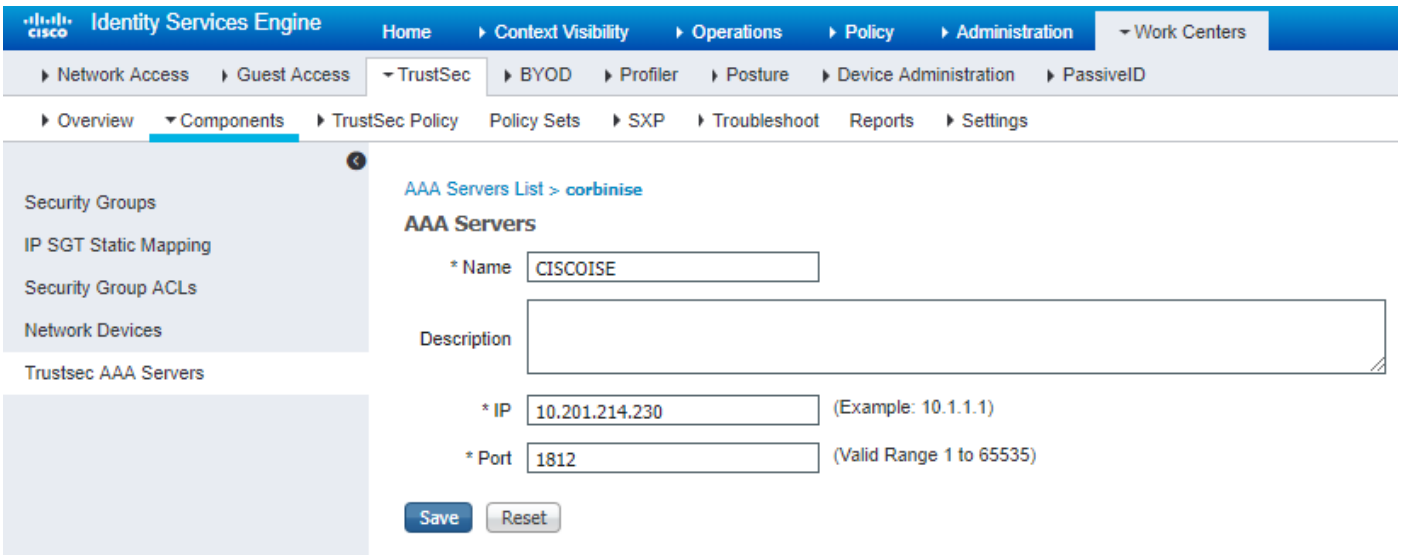
[名前(Name)]	ユーザ名	ADグループ	SG	SGT
ジェイソン・スミス	ジャスミス	コンサルタント	BYODコンサルタント	15
サリー・スミス	スミス	従業員	BYOD従業員	7
該当なし	該当なし	該当なし	TrustSec_Devices	2

コンフィギュレーション

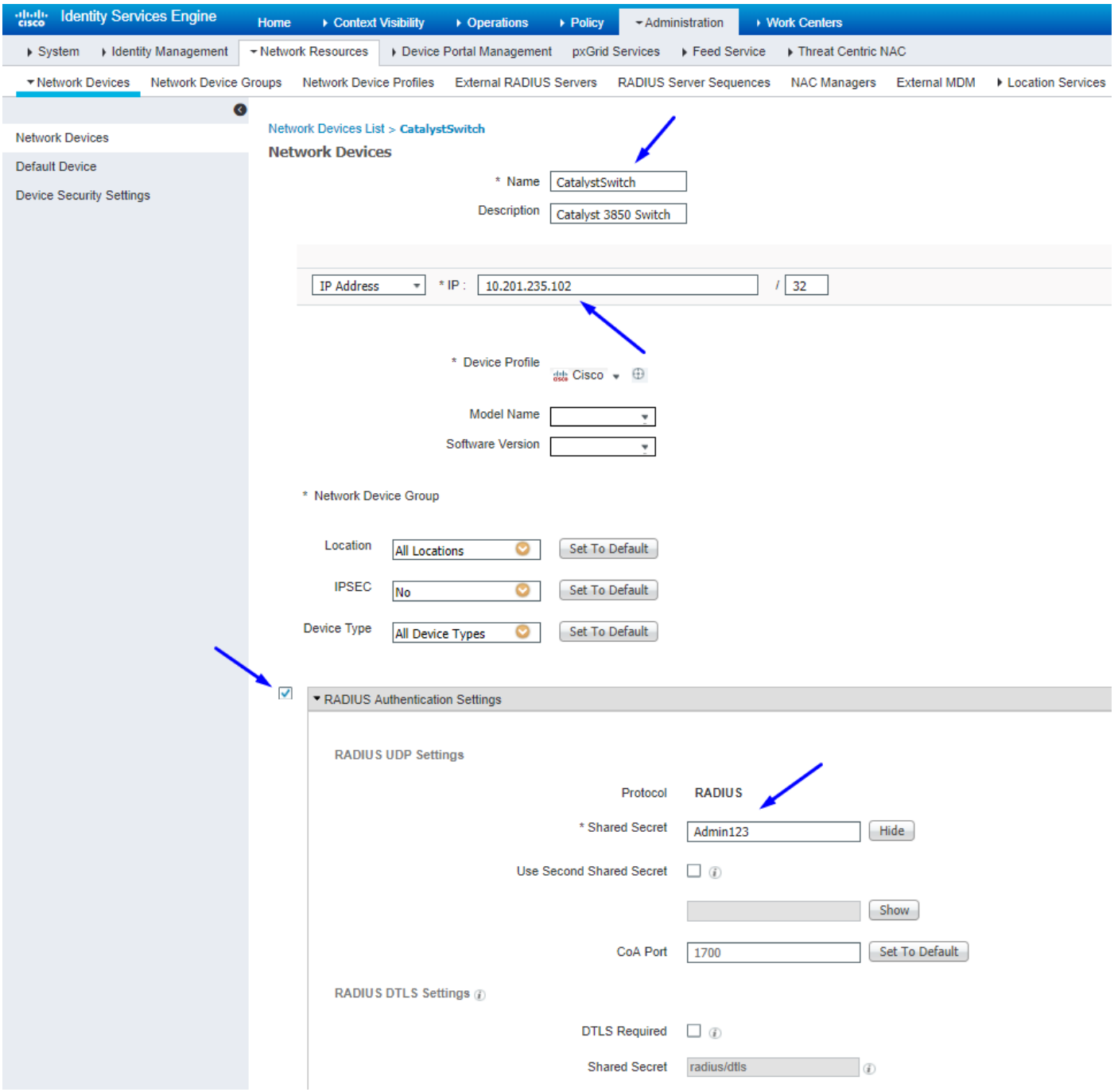
ISEでのTrustSecの設定



TrustSec AAAサーバとしてのCisco ISEの設定

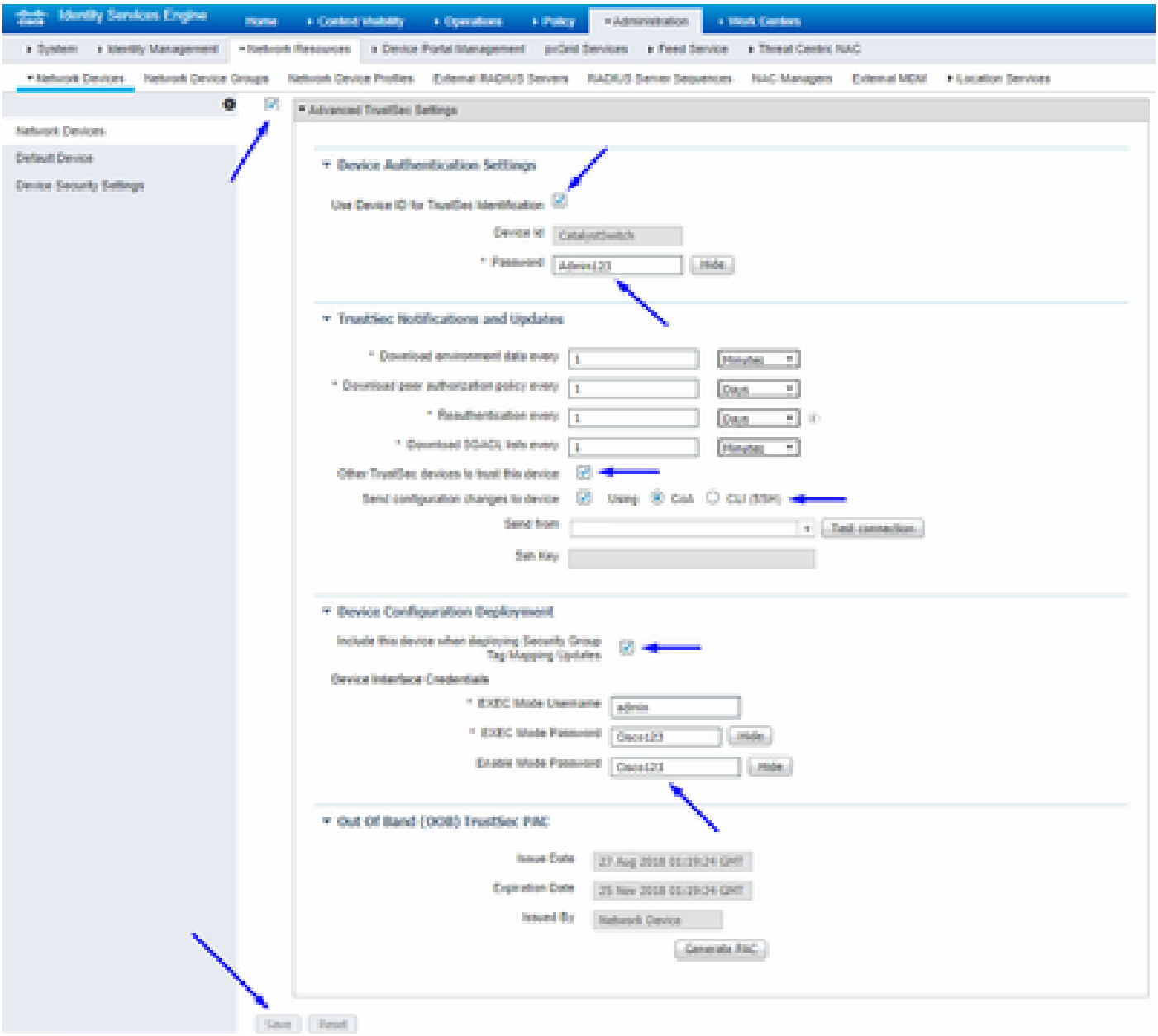


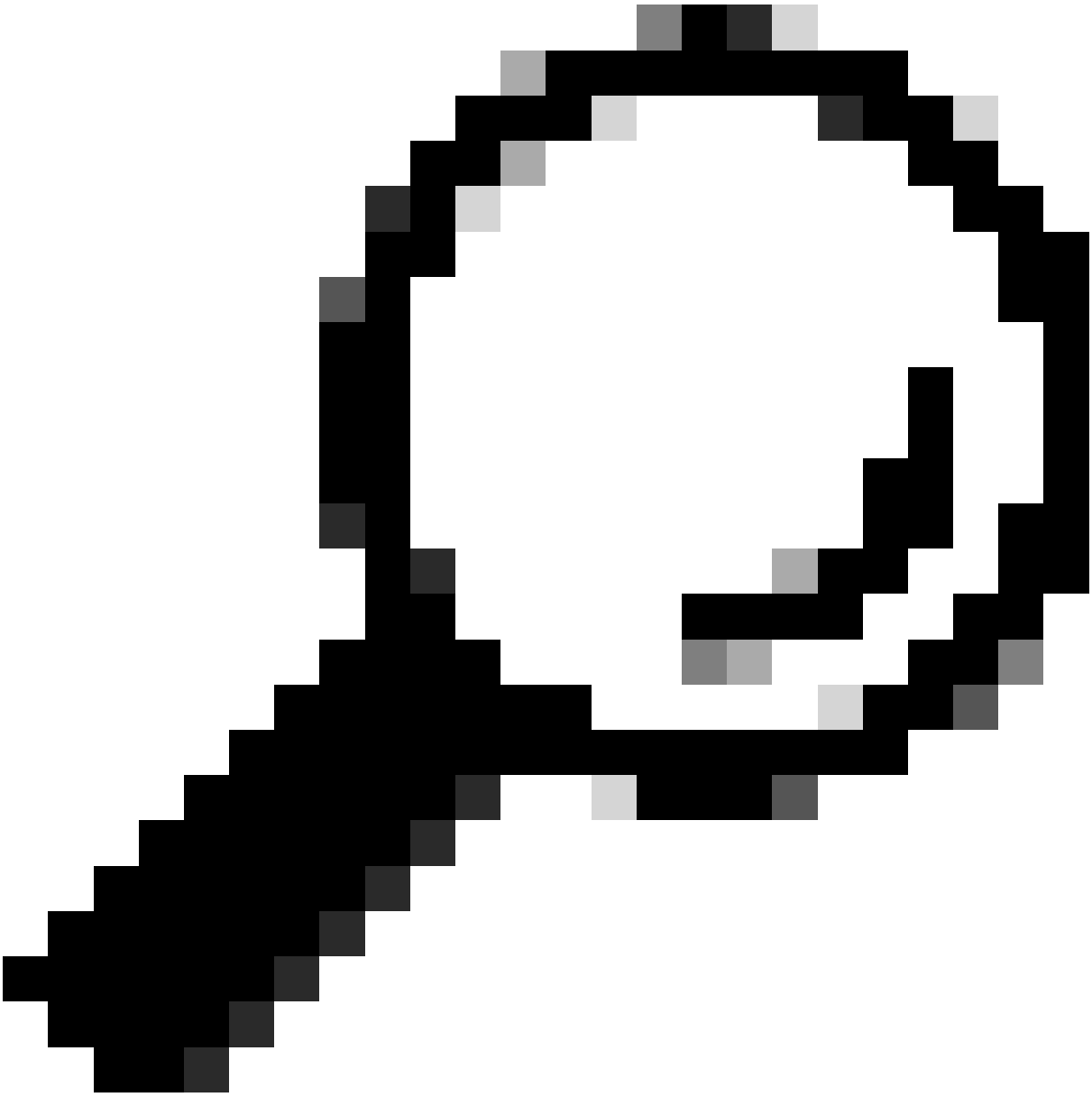
スイッチがCisco ISEのRADIUSデバイスとして追加されるように設定および確認する



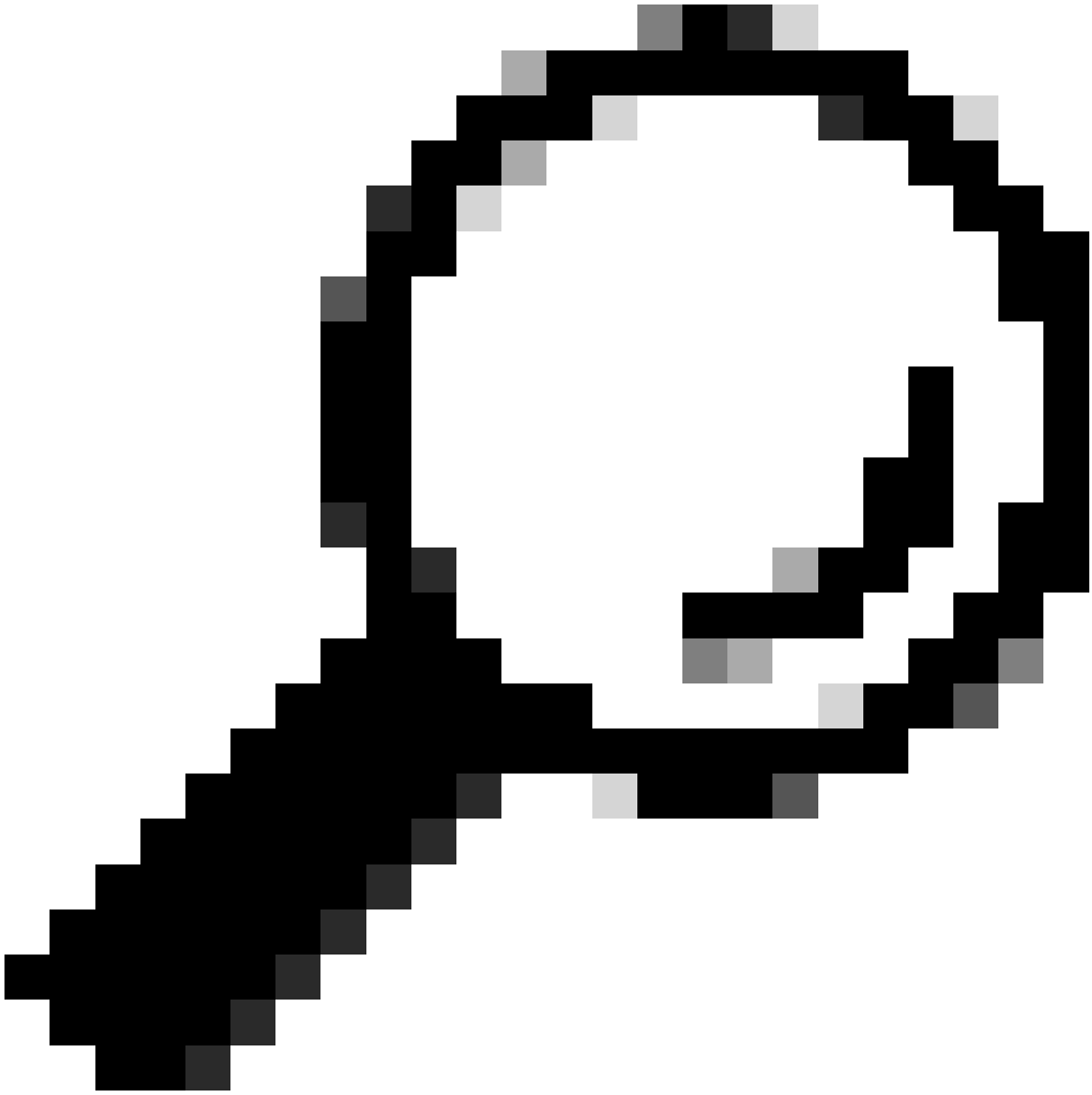
Cisco ISEでTrustSecデバイスとして追加されるWLCの設定と確認

SSHのログインクレデンシャルを入力します。これにより、Cisco ISEはスタティックIP-to-SGTマッピングをスイッチに導入できます。
これらはCisco ISE Web GUIのWork Centers > TrustSec > Components > IP SGT Static Mappingsで次のように作成します。


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

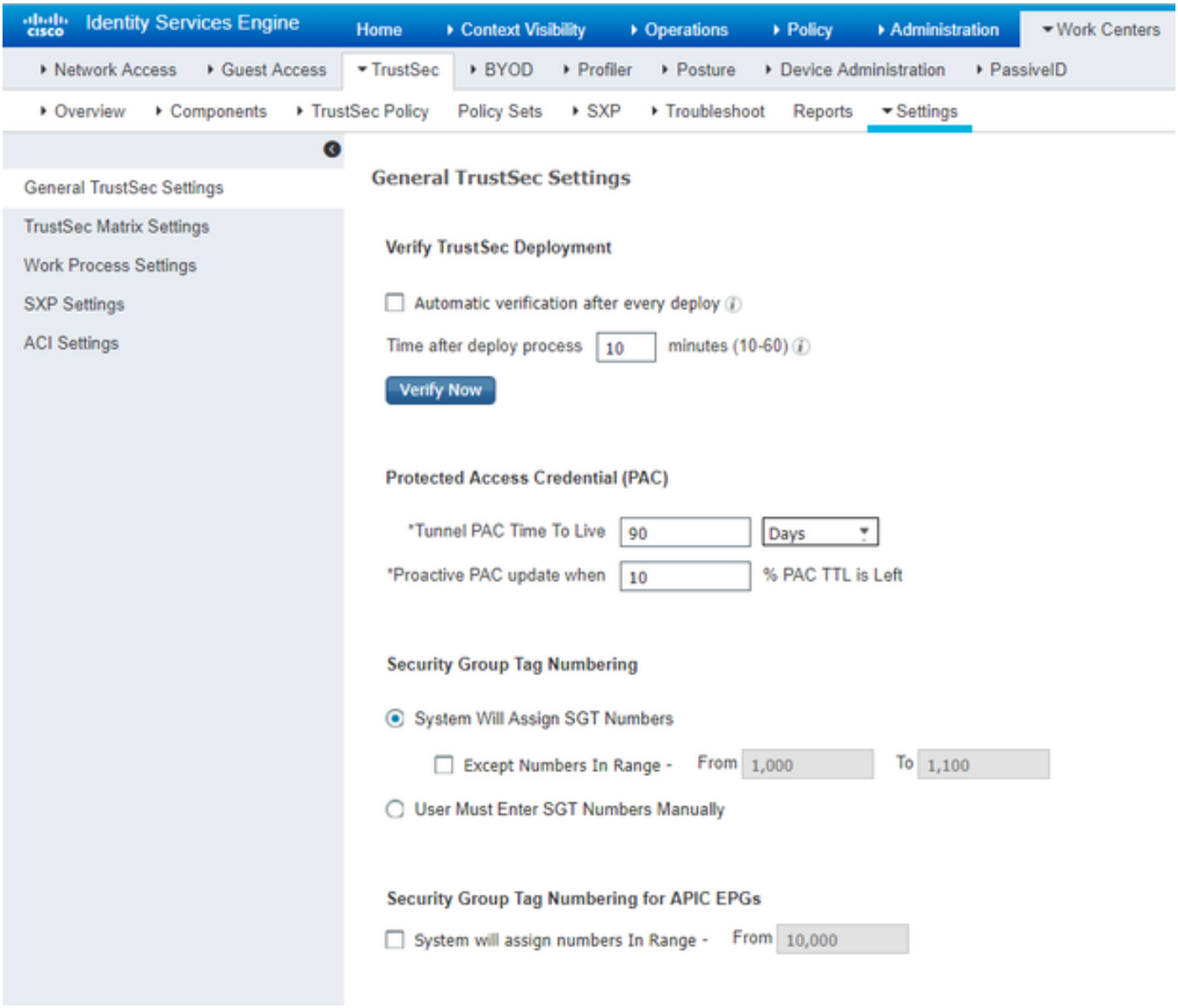


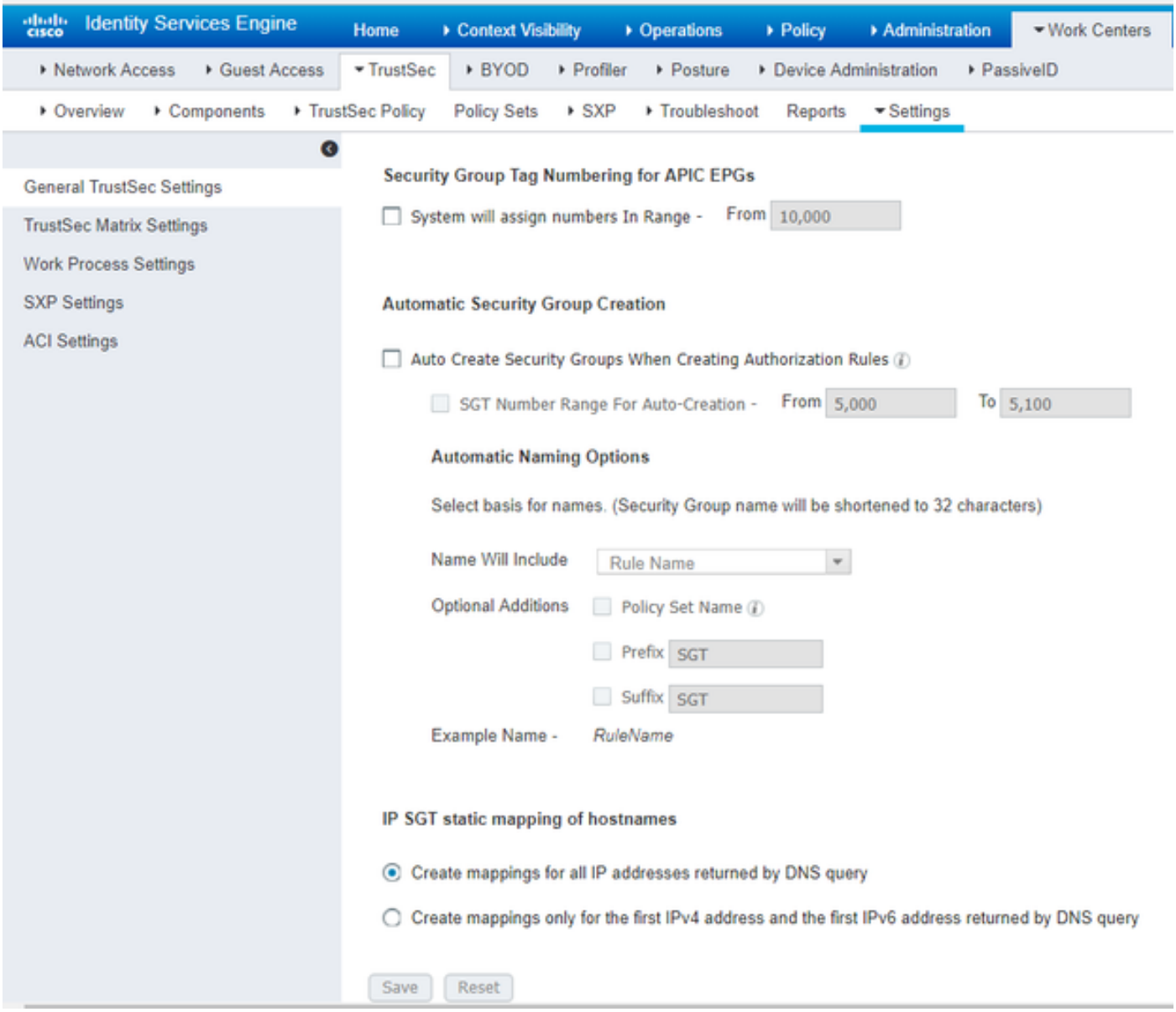
ヒント：まだCatalystスイッチでSSHを設定していない場合は、このガイド「Catalystスイッチでのセキュアシェル(SSH)の設定方法」を使用できます。



ヒント:Cisco ISEがSSH経由でCatalystスイッチにアクセスできるようにしたくない場合は、代わりにCLIを使用して、Catalystスイッチ上でIPとSGTの静的マッピングを作成できます（このステップを参照）。

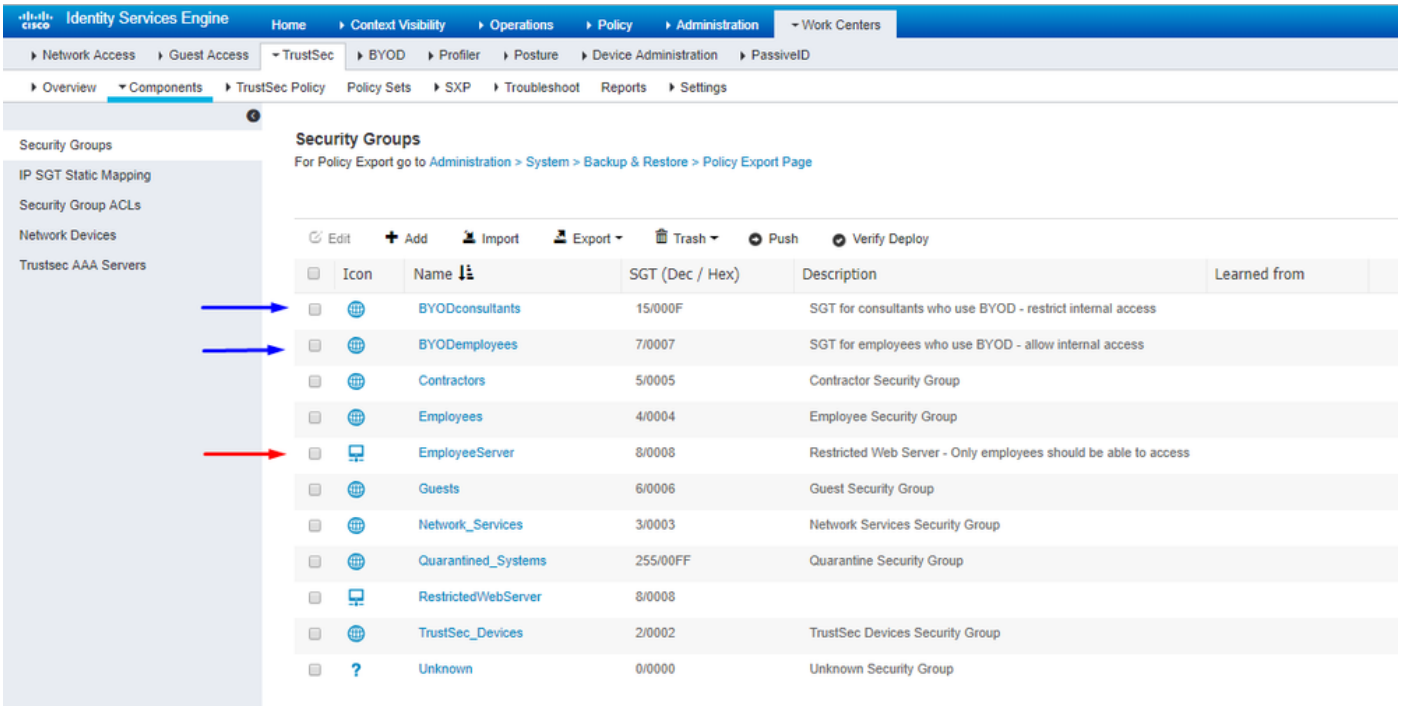
TrustSecのデフォルト設定が許容可能であることを確認する（オプション）


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



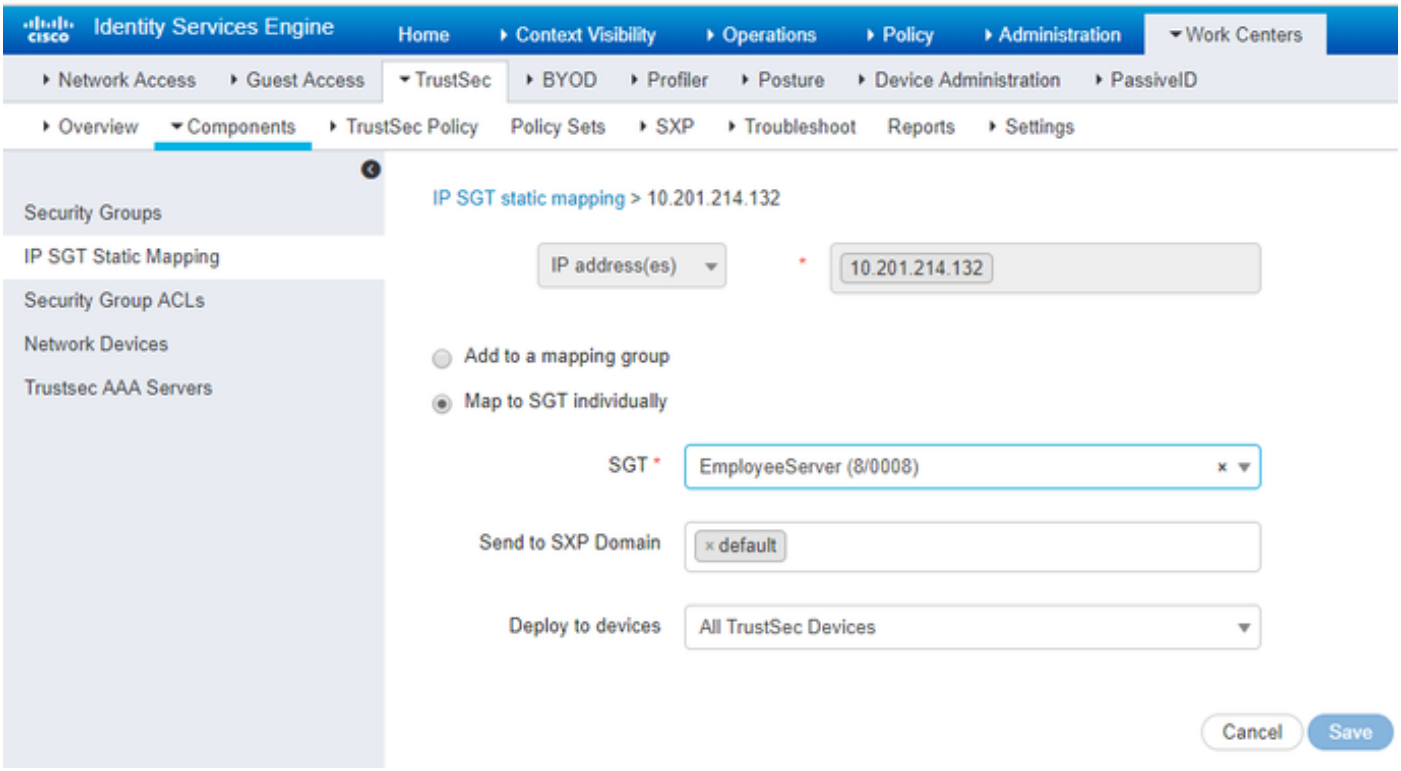
ワイヤレスユーザ用のセキュリティグループタグの作成

BYODコンサルタント用セキュリティグループの作成 – SGT 15
BYOD従業員用セキュリティグループの作成 – SGT 7

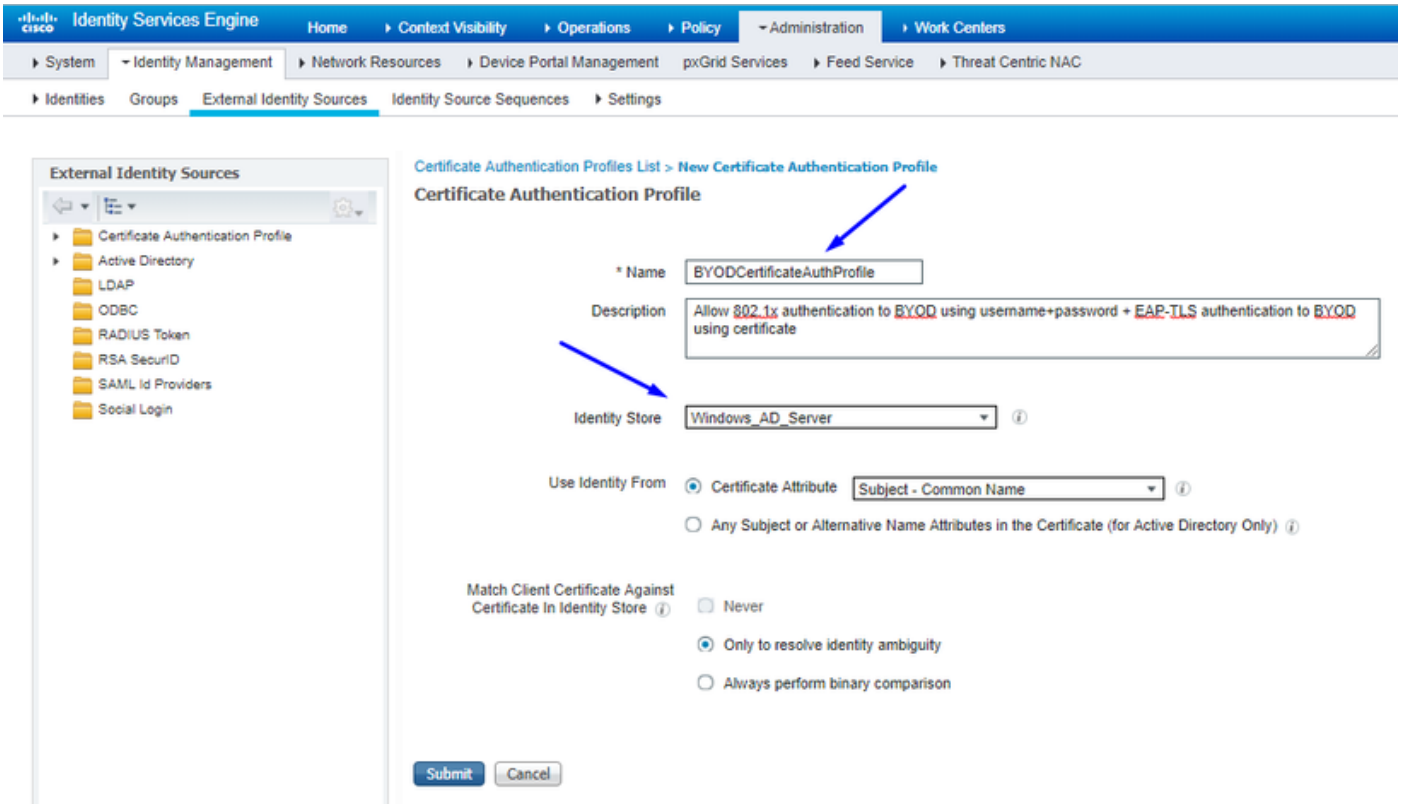


制限付きWebサーバのスタティックIP-to-SGTマッピングの作成

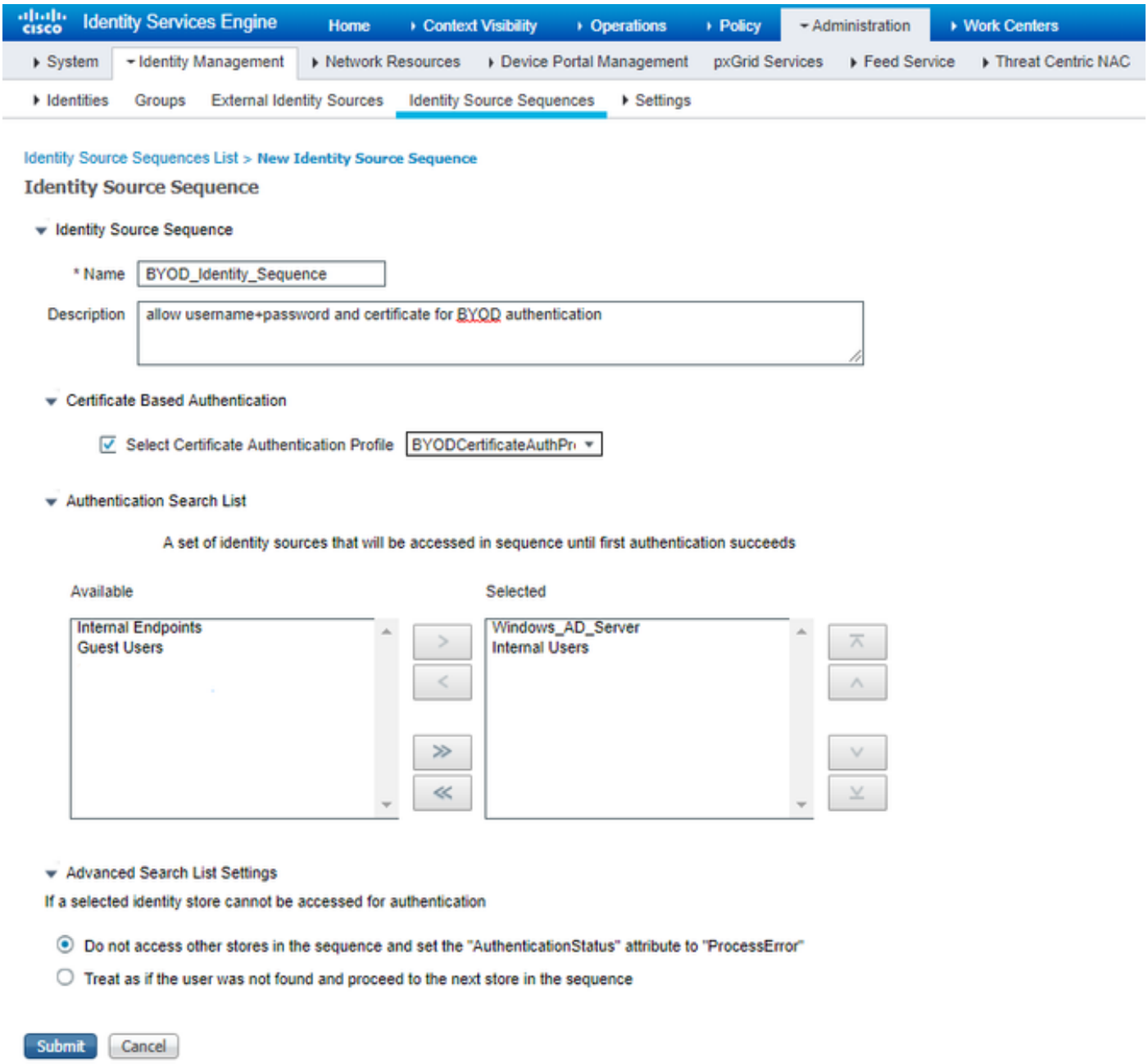
MAC認証バイパス(MAB)、802.1x、プロファイルなどでCisco ISEに対して認証されないネットワーク内の他のIPアドレスまたはサブネットに対して、これを実行します。



証明書認証プロファイルの作成

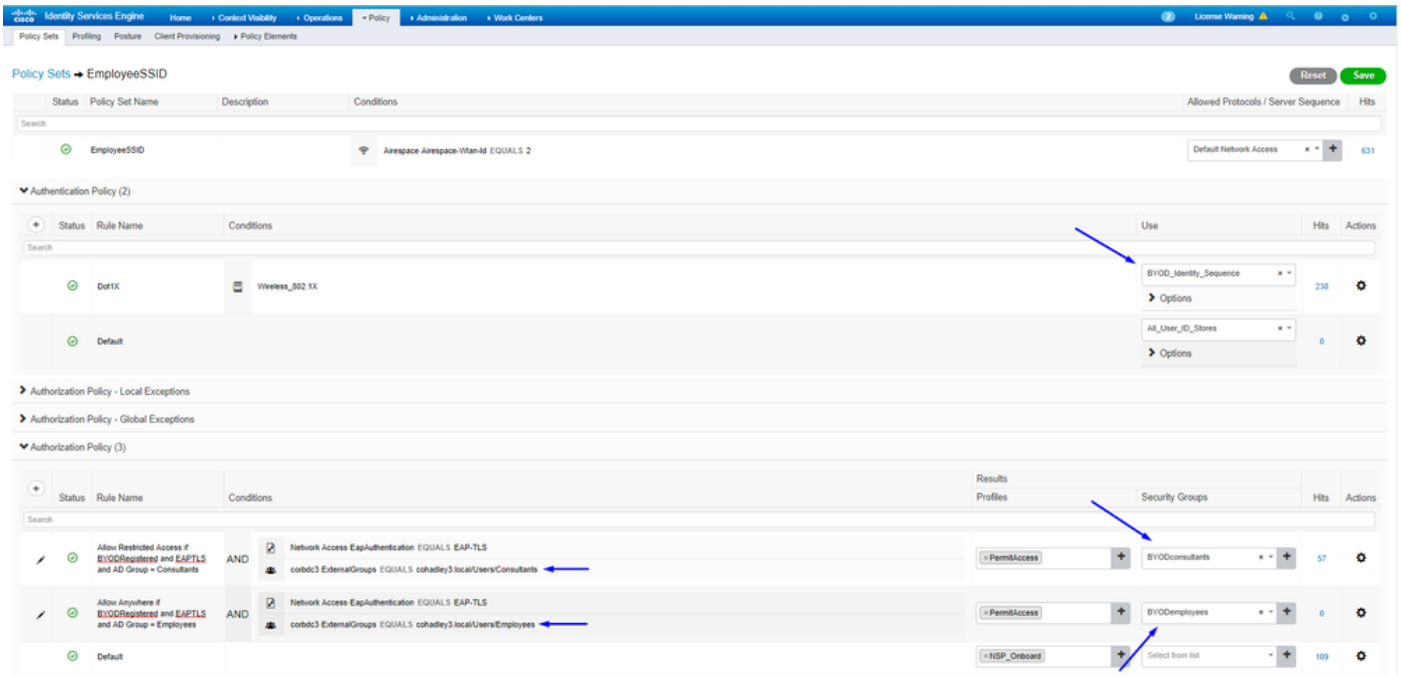


以前の証明書認証プロファイルを使用したIDソースシーケンスの作成

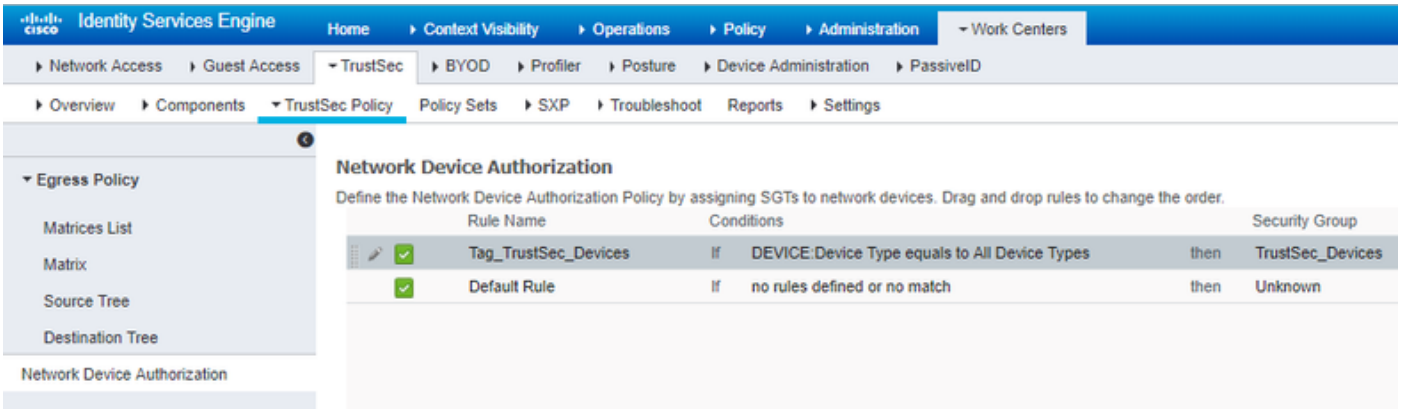


ワイヤレスユーザ（従業員およびコンサルタント）に適切なSGTを割り当てる

[名前(Name)]	ユーザ名	ADグループ	SG	SGT
ジェイソン・スミス	ジャスミス	コンサルタント	BYODコンサルタント	15
サリー・スミス	スミス	従業員	BYOD従業員	7
該当なし	該当なし	該当なし	TrustSec_Devices	2

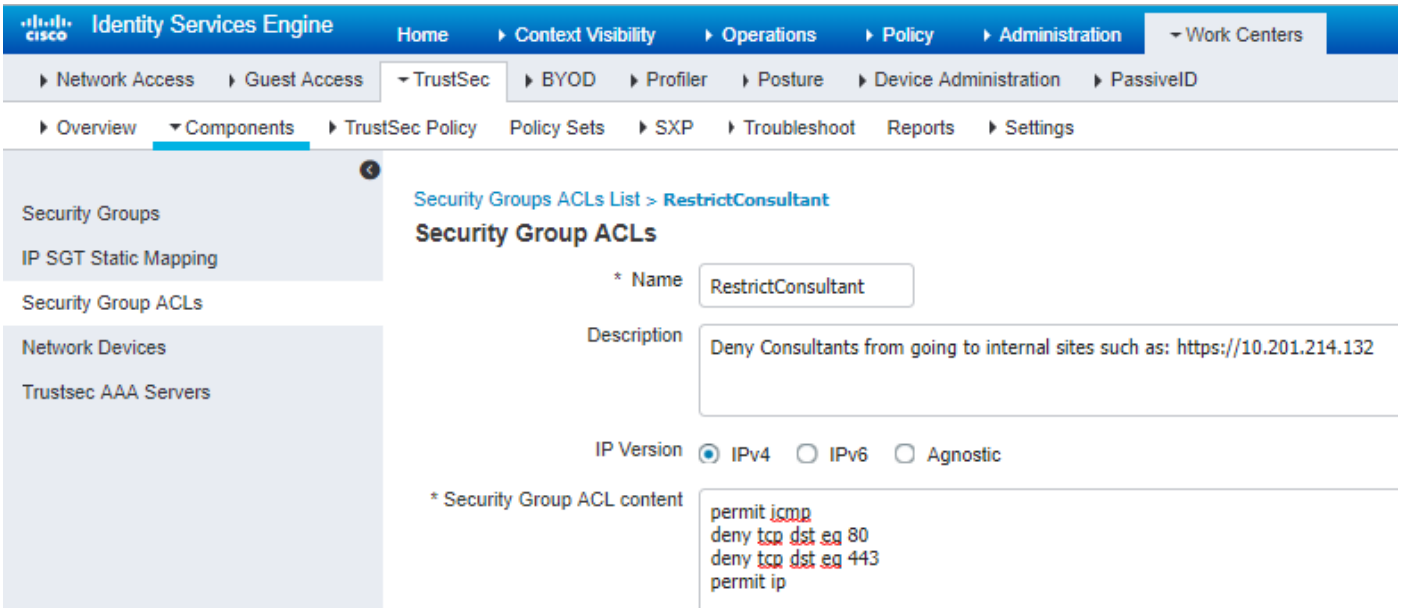


実際のデバイス（スイッチおよびWLC）へのSGTの割り当て

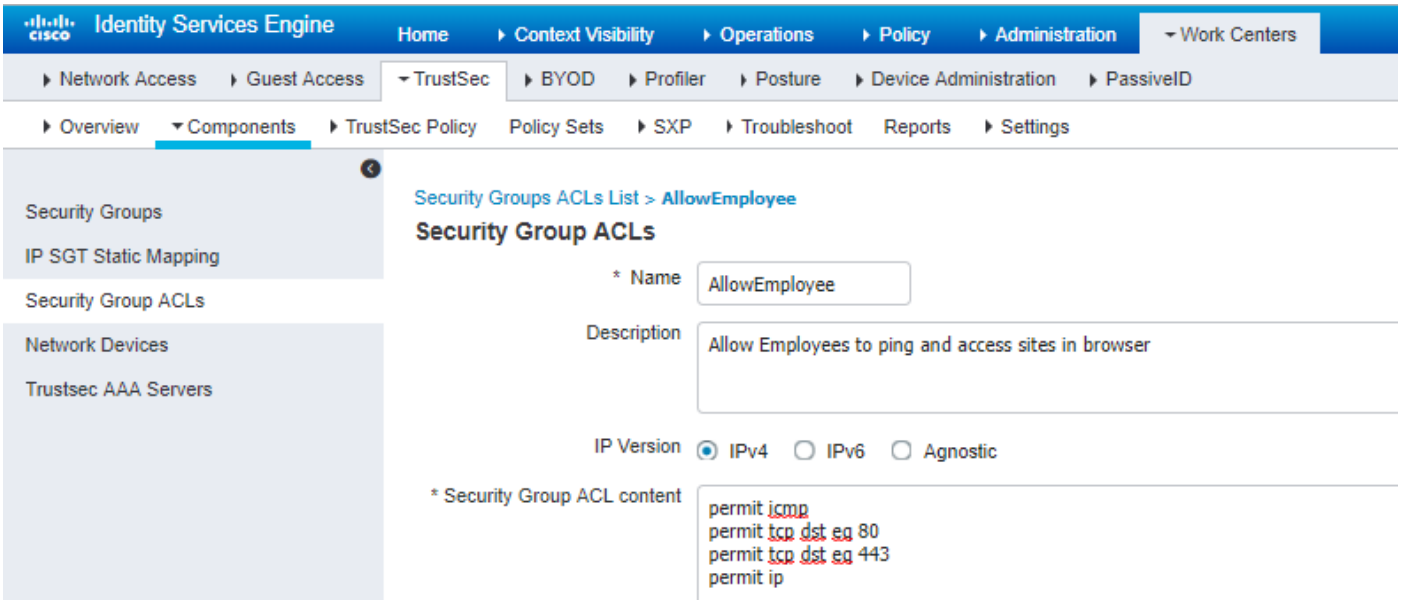


出力ポリシーを指定するSGACLの定義

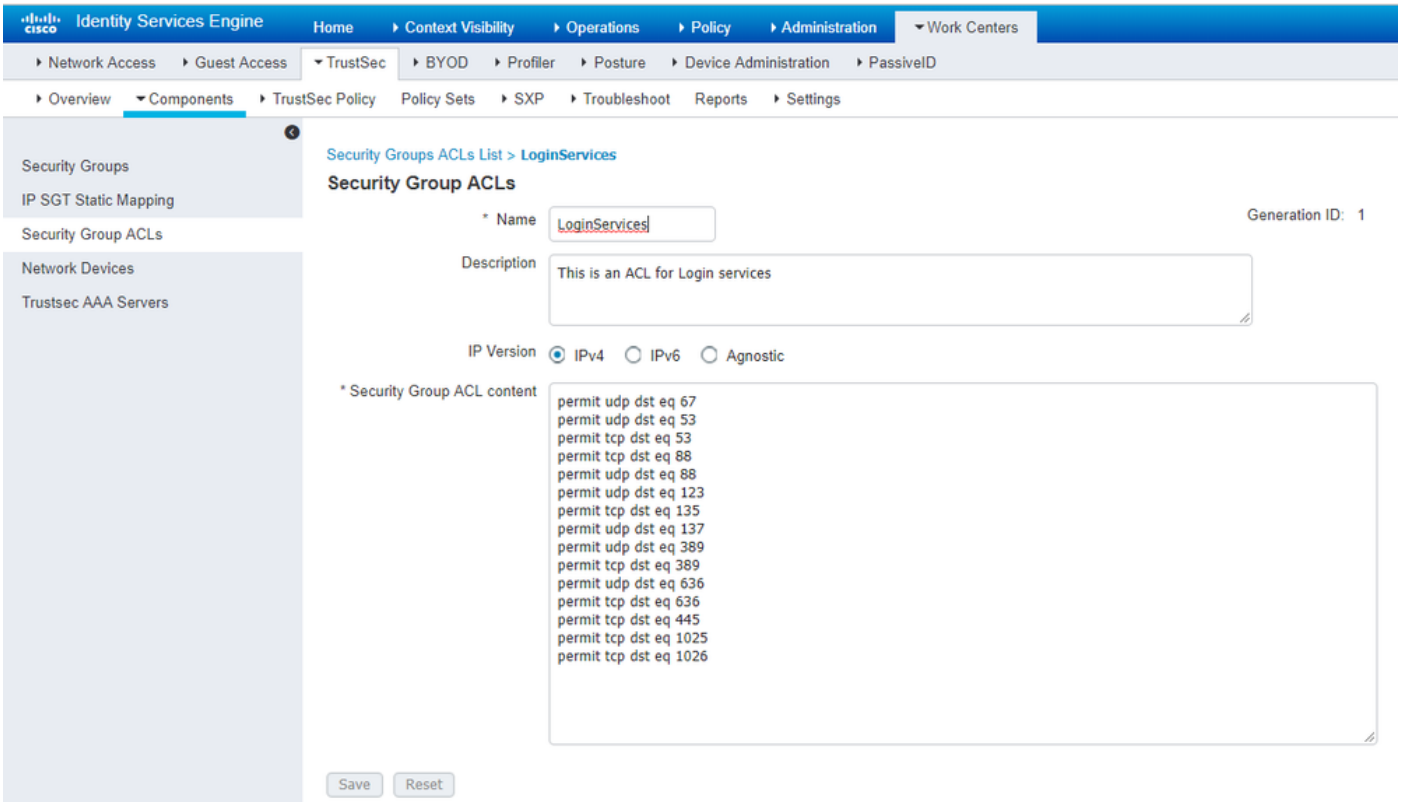
コンサルタントは外部の任意の場所からアクセスできるが、内部のアクセスは制限：



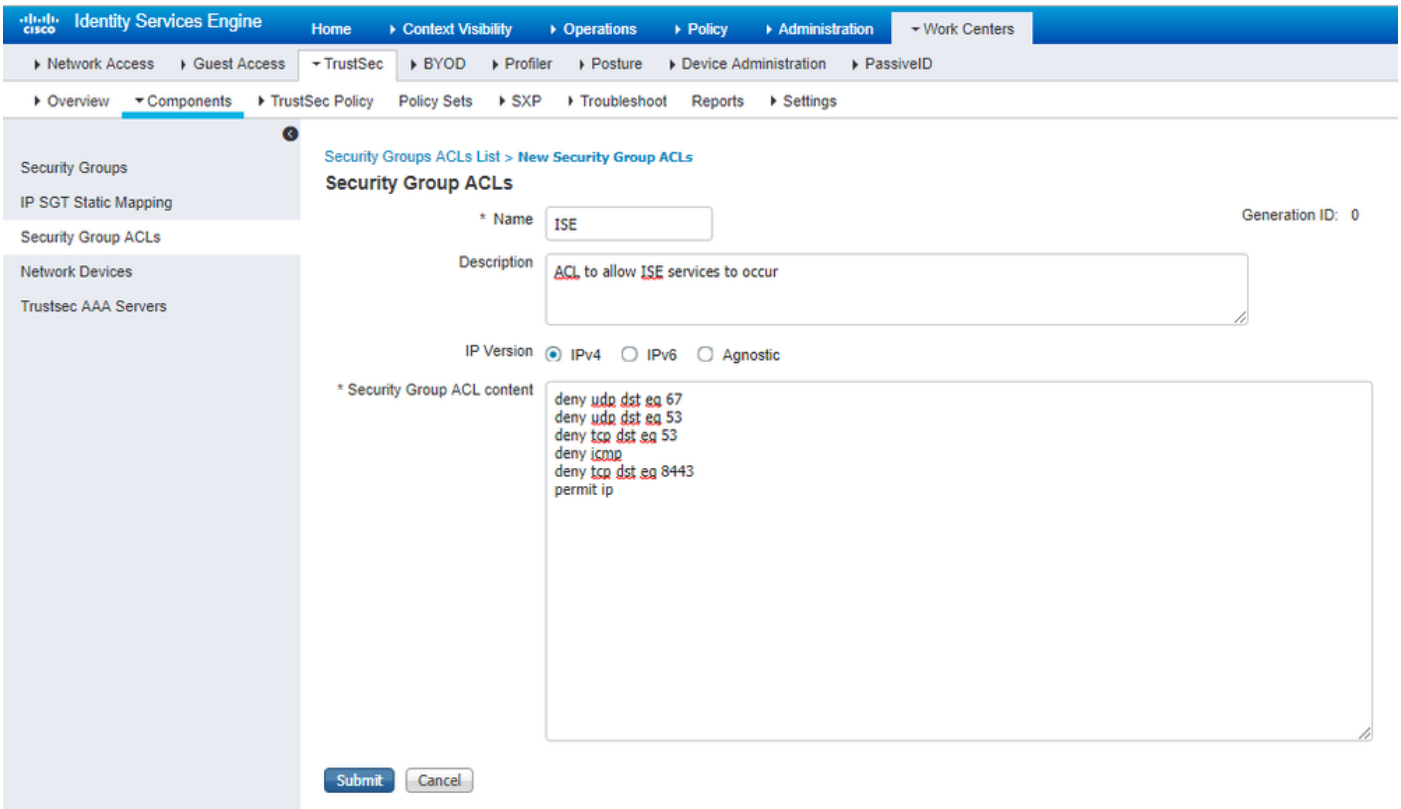
従業員が外部および内部の任意の場所からアクセスできるようにする：



他のデバイスから基本サービスへのアクセスを許可する（オプション）：



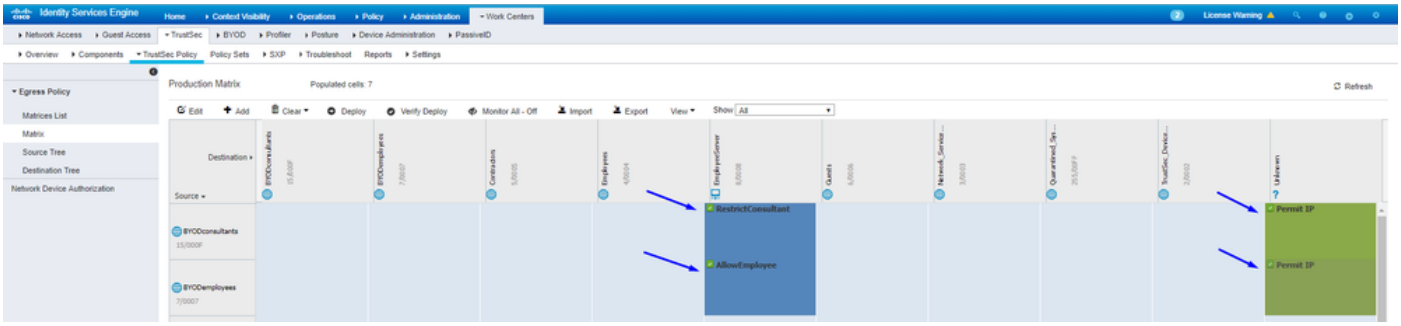
すべてのエンドユーザをCisco ISEにリダイレクトします（BYODポータルリダイレクション用）。DNS、DHCP、ping、またはWebAuthトラフィックはCisco ISEに送信できないため、これらを含めないでください。



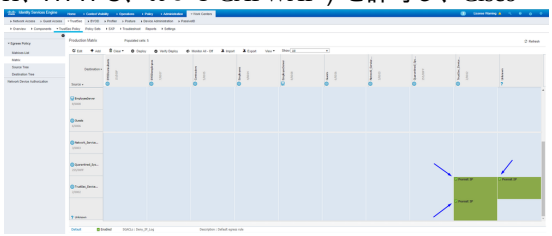
Cisco ISEのTrustSecポリシーマトリックスでのACLの適用

コンサルタントは外部のあらゆる場所からアクセスできるが、https://10.201.214.132などの内部Webサーバは制限される

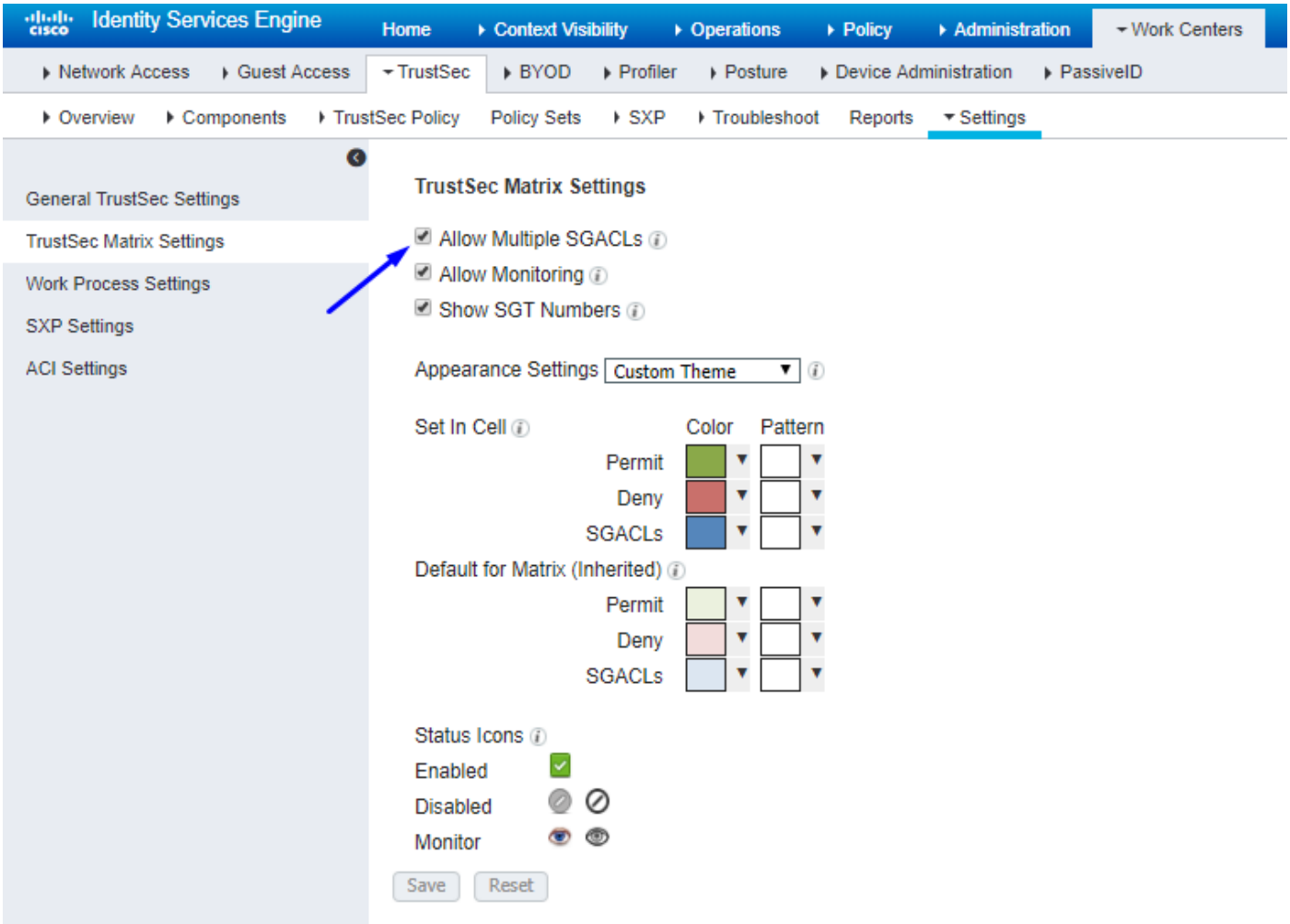
従業員が外部の任意の場所にアクセスできるようにし、内部Webサーバを許可する：



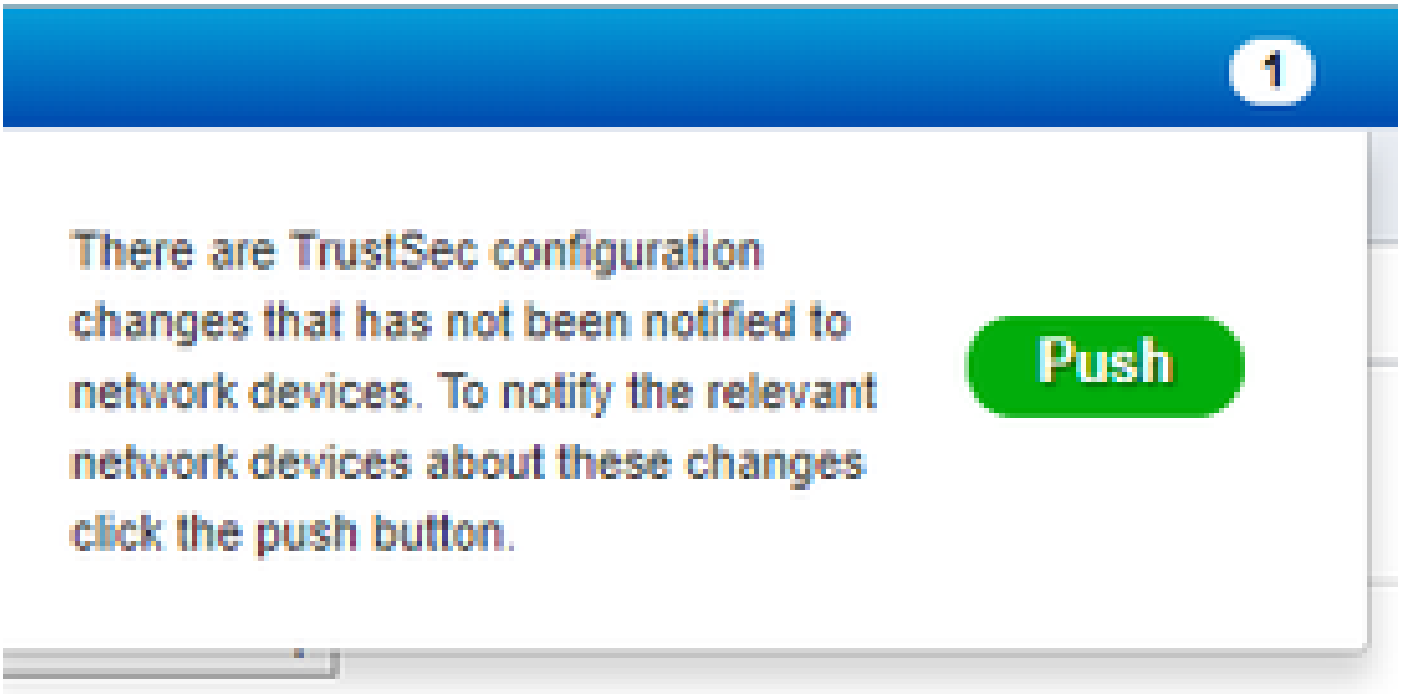
ネットワーク上のデバイス（スイッチとWLC）との間の管理トラフィック（SSH、HTTPS、およびCAPWAP）を許可し、Cisco TrustSecを導入した後にSSHまたはHTTPSアクセスが失われないようにします。



Cisco ISEで Allow Multiple SGACLsを有効にします。

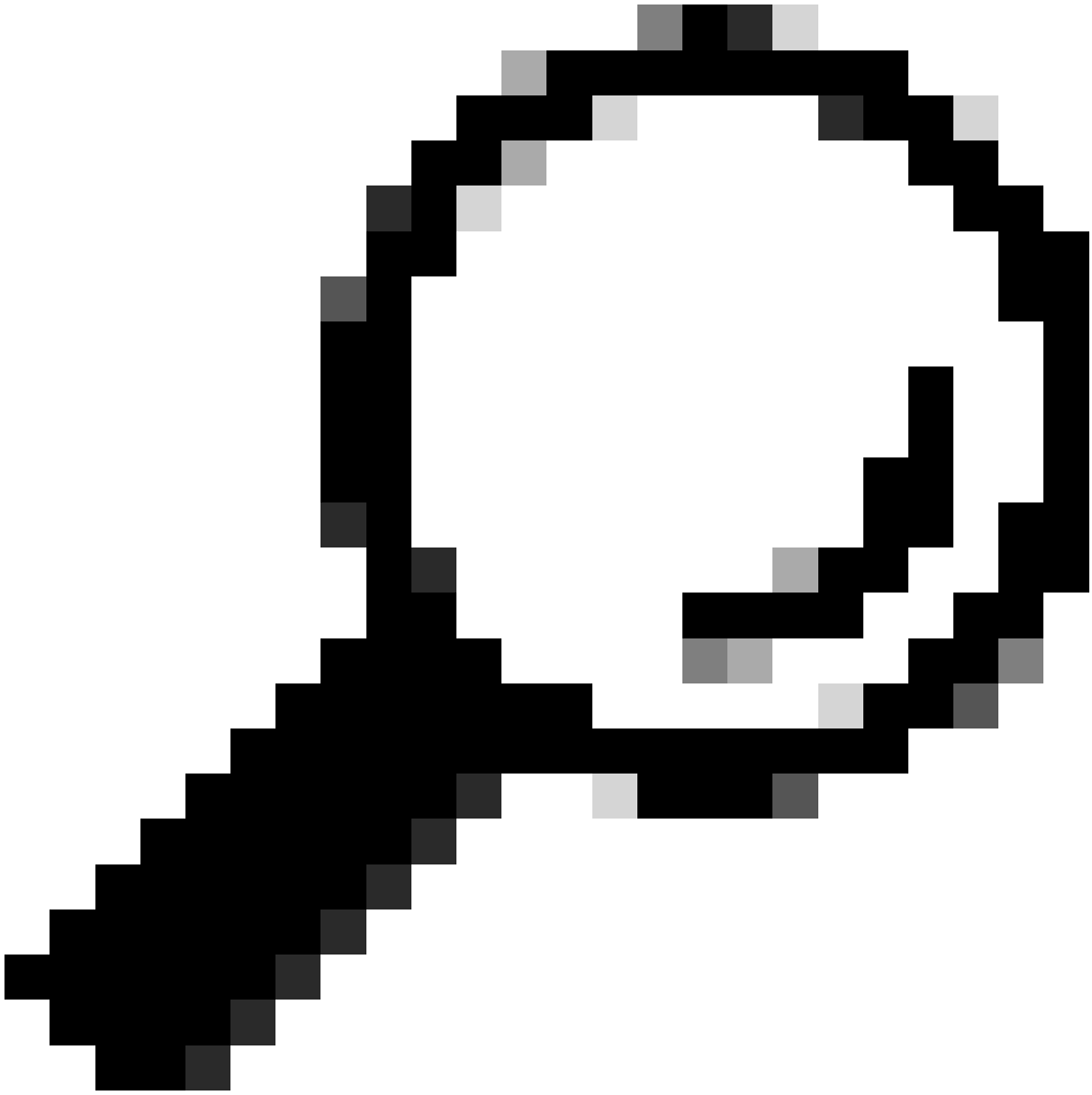


Cisco ISEの右上隅にあるPushをクリックして、設定をデバイスに適用します。この作業は後で行う必要があります。



CatalystスイッチでのTrustSecの設定

CatalystスイッチでAAAにCisco TrustSecを使用するためのスイッチの設定



ヒント：このドキュメントでは、ワイヤレスユーザがCisco ISEによるBYODをすでに完了していることを前提としています。

太字で示されているコマンドは、BYODワイヤレスがISEと連動するようにこの前にすでに設定されています。

<#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

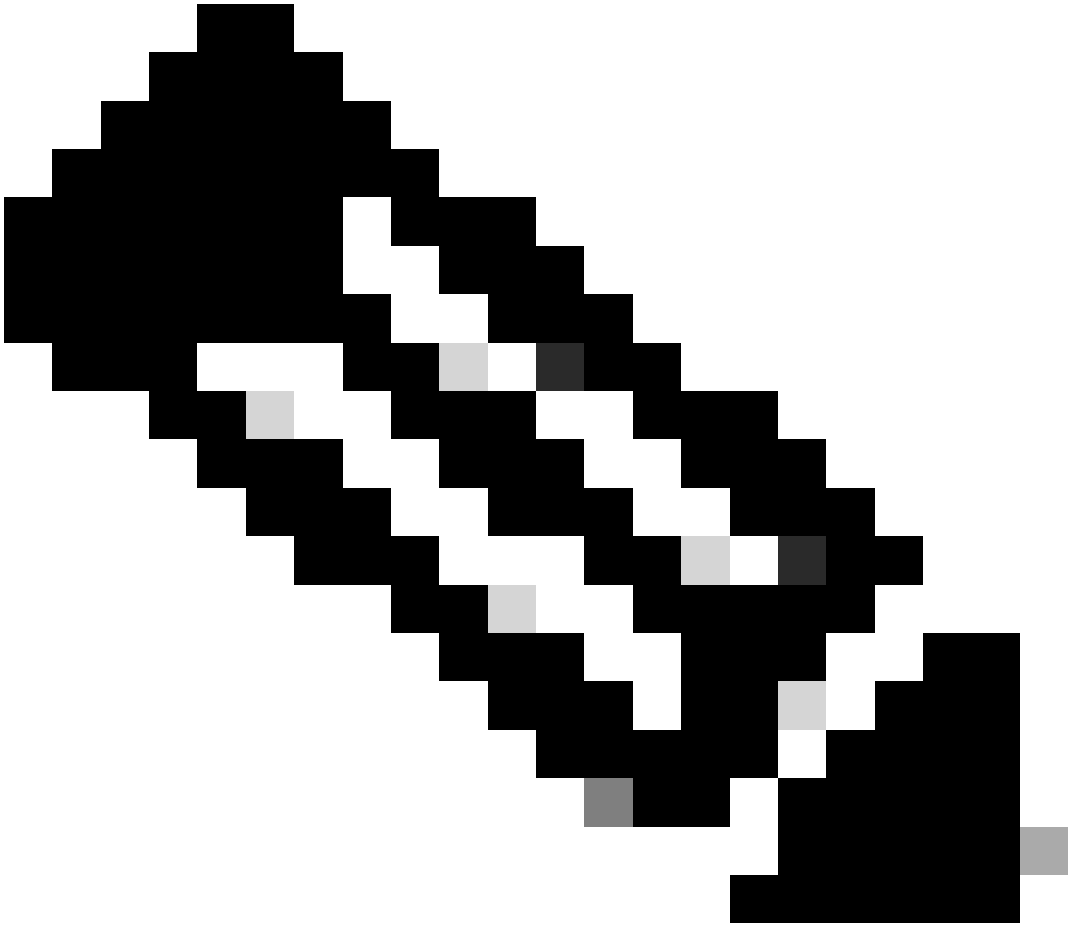
CatalystSwitch(config)#aaa authorization network default group AAASERVER

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



注:PACキーは、 **Administration > Network Devices > Add Device > RADIUS Authentication Settings** セクションで指定したRADIUS共有秘密と同じである必要があります。

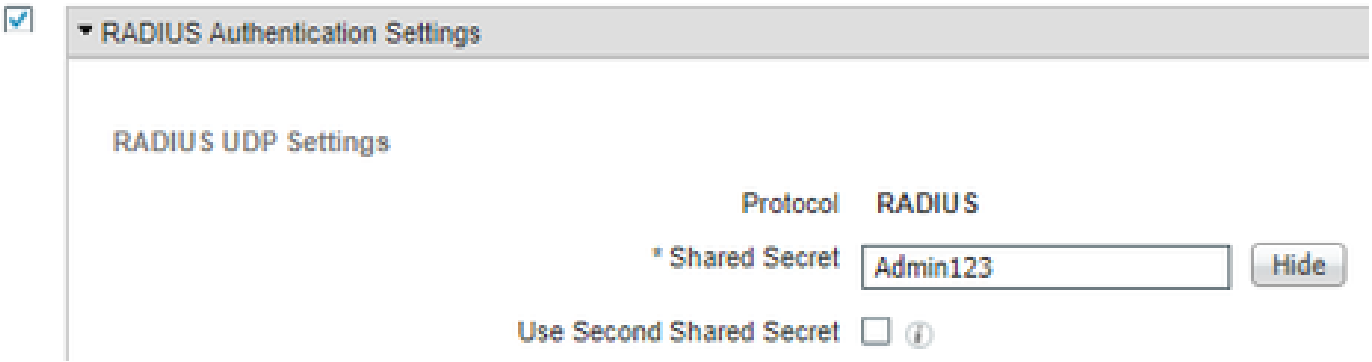
<#root>

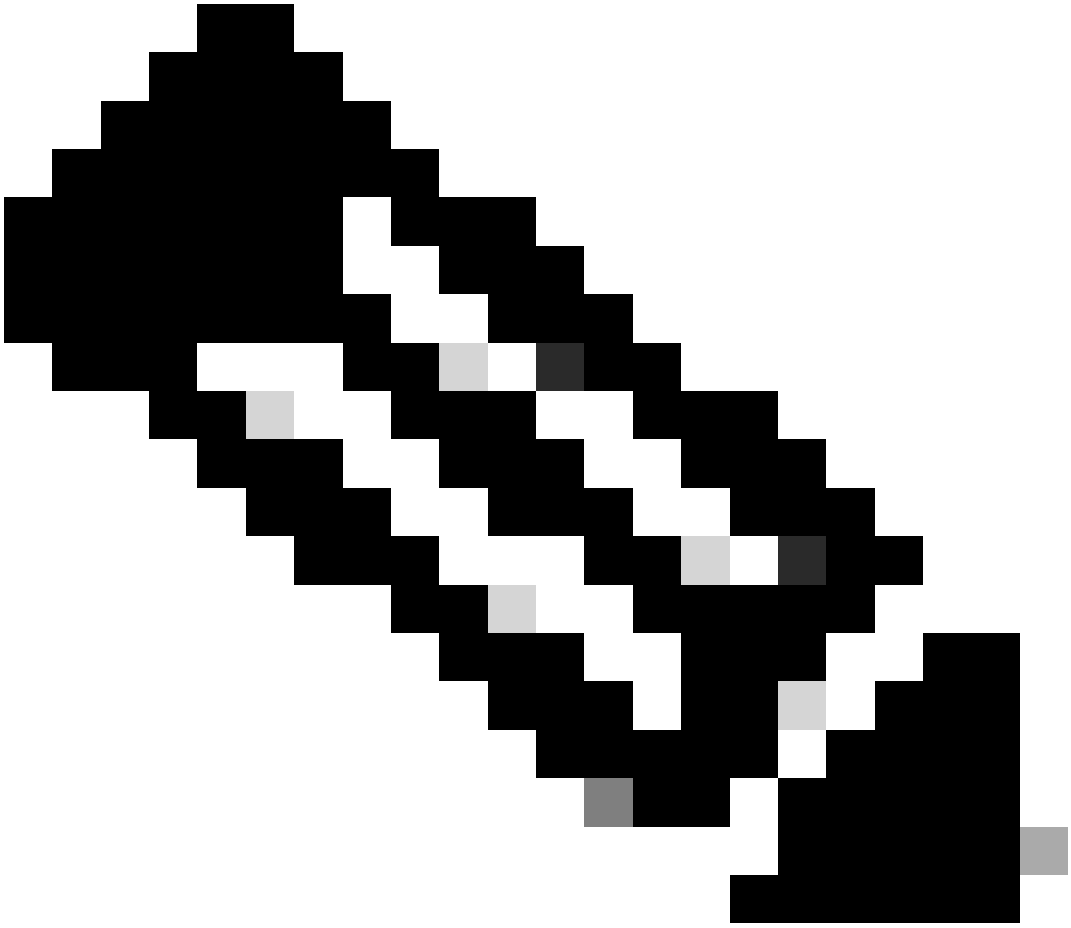
```
CatalystSwitch(config)#radius-server attribute 6 on-for-login-auth

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
```

Cisco ISEに対してスイッチを認証するためのRADIUSサーバでのPACキーの設定

```
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
```

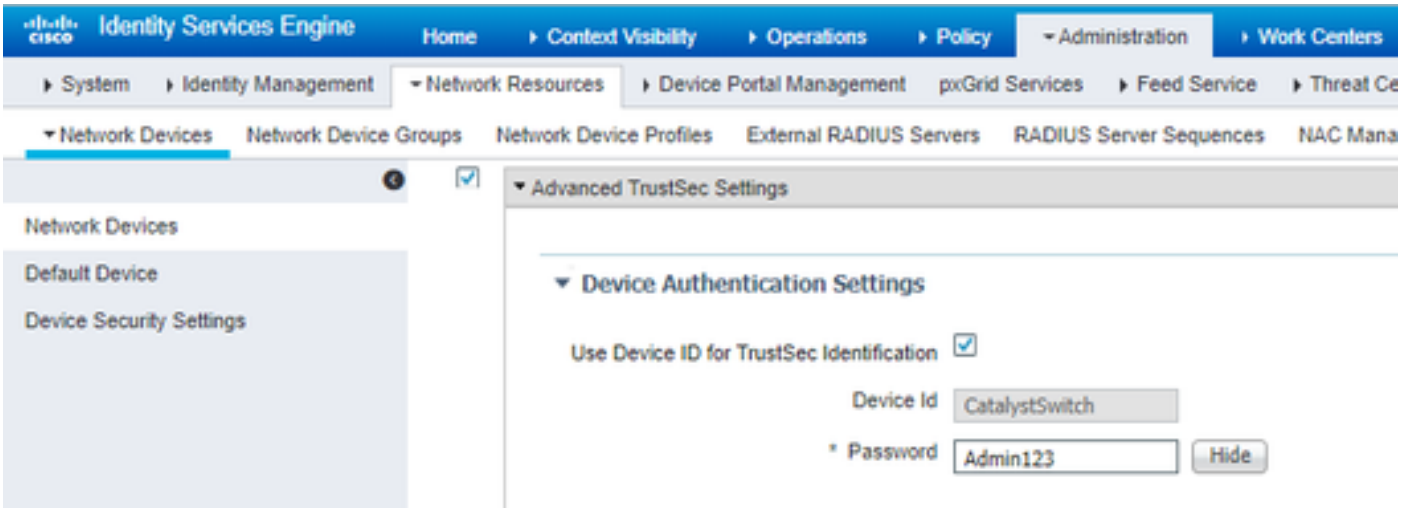


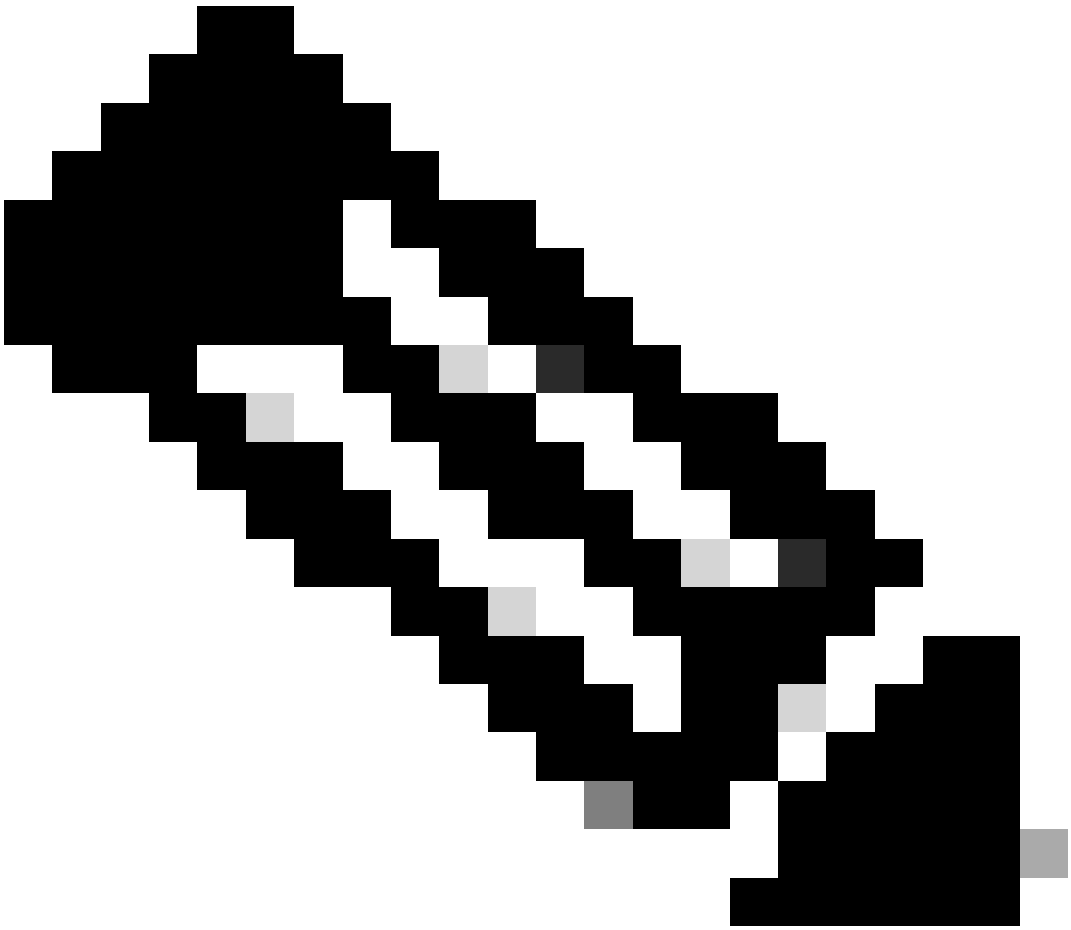


注:PACキーは、Cisco ISEの **Administration > Network Devices > Add Device > RADIUS Authentication Settings** セクションで指定したRADIUS共有秘密と同じである必要があります（画面キャプチャを参照）。

スイッチをCisco ISEに認証するためのCTSクレデンシャルの設定

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





注：CTSクレデンシャルは、デバイスID +パスワードと同じでなければなりません。CTSクレデンシャルは、Cisco ISEのAdministration > Network Devices > Add Device > Advanced TrustSec Settingsセクションで指定したデバイスID +パス

ワードと同じである必要があります（画面キャプチャを参照）。

次に、PACを更新してCisco ISEに再びアクセスできるようにします。

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

Catalystスイッチでの CTSのグローバルな有効化

```
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)
```

制限付きWebサーバのスタティックIP-to-SGTマッピングの作成（オプション）

この制限付きWebサーバは、これまで認証のためにISEを経由することはないため、スイッチCLIまたはISE Web GUIを使用して手動でタグ付けする必要があります。これは、シスコに数多く存在するWebサーバの1つです。

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

Catalystスイッチでの TrustSecの確認

```
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: 000200B800030001000400010EF2E1222E67EB4630A8B22D1FF0216C10006009C0003010025D40D409A0DDAF352A3F1A9884AC3F6
 Refresh timer is set for 12w5d
```

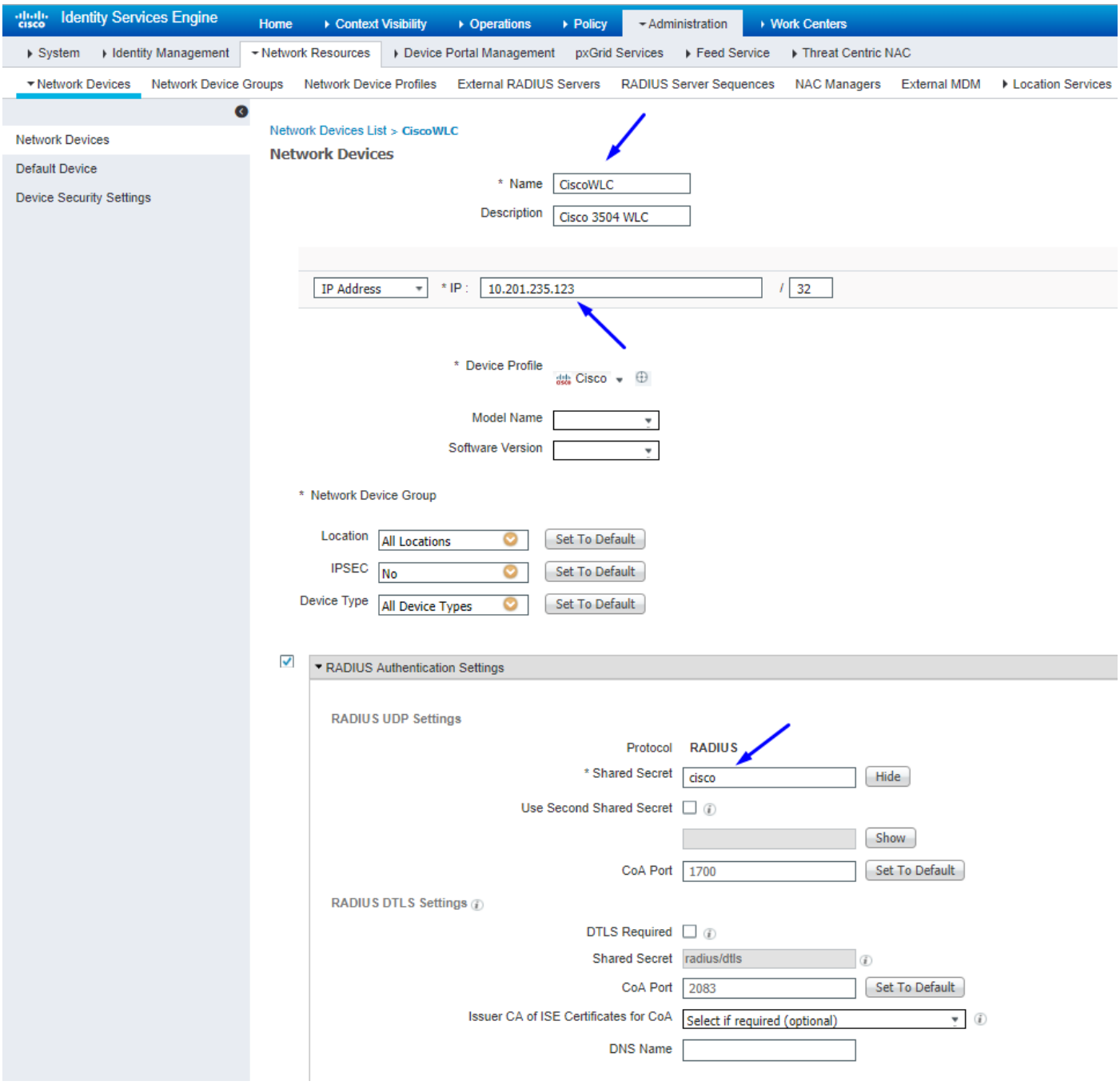
```
CatalystSwitch#cts refresh environment-data
Environment data download in progress
```

```
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
```

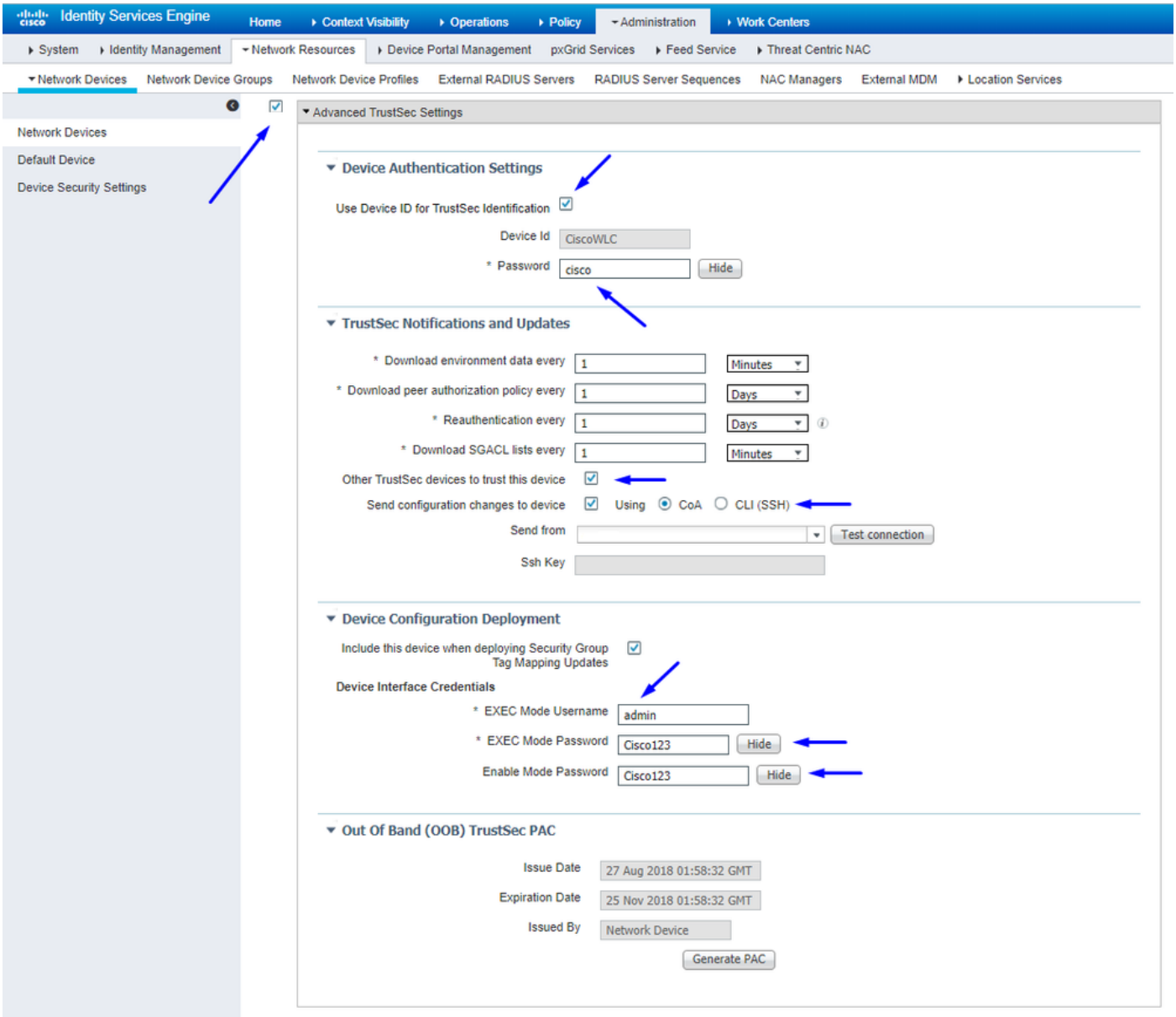
WLCでのTrustSecの設定

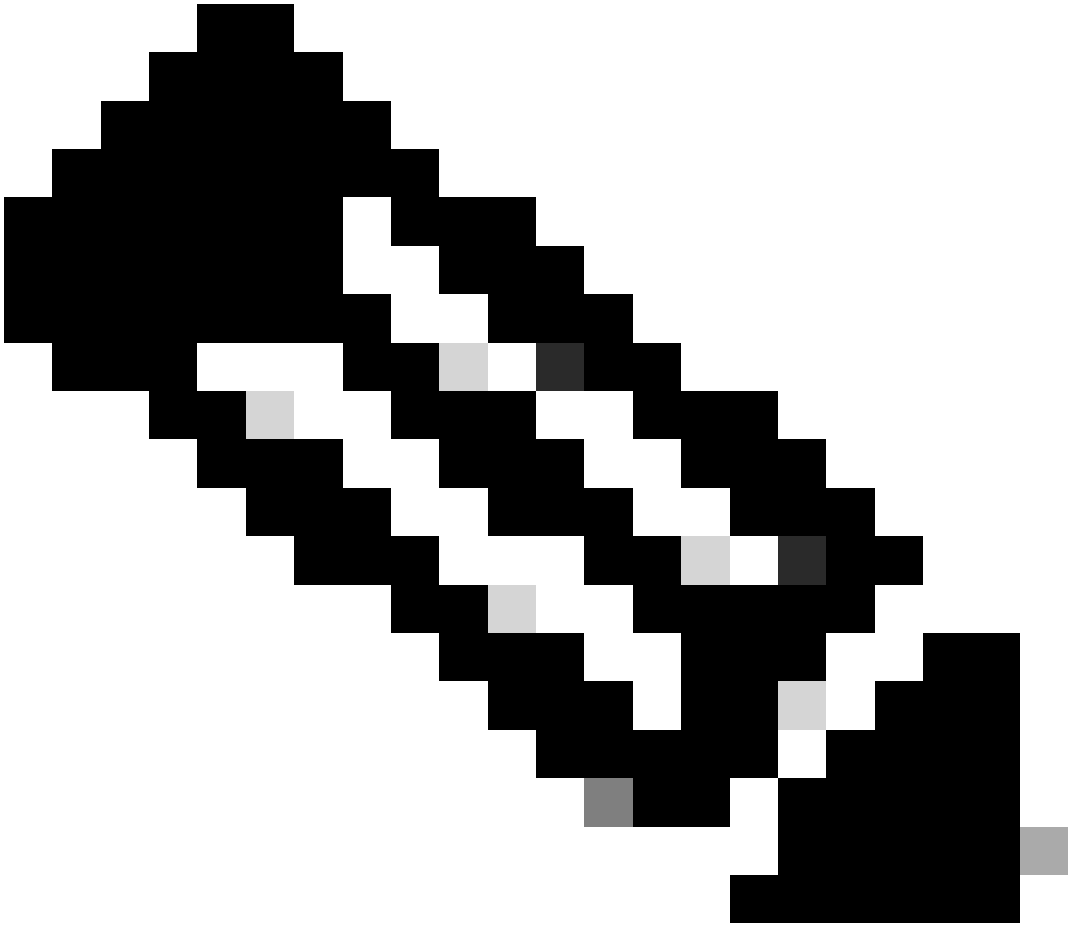
Cisco ISEでRADIUSデバイスとして追加されるWLCの設定と確認



Cisco ISEでTrustSecデバイスとして追加されるWLCの設定と確認

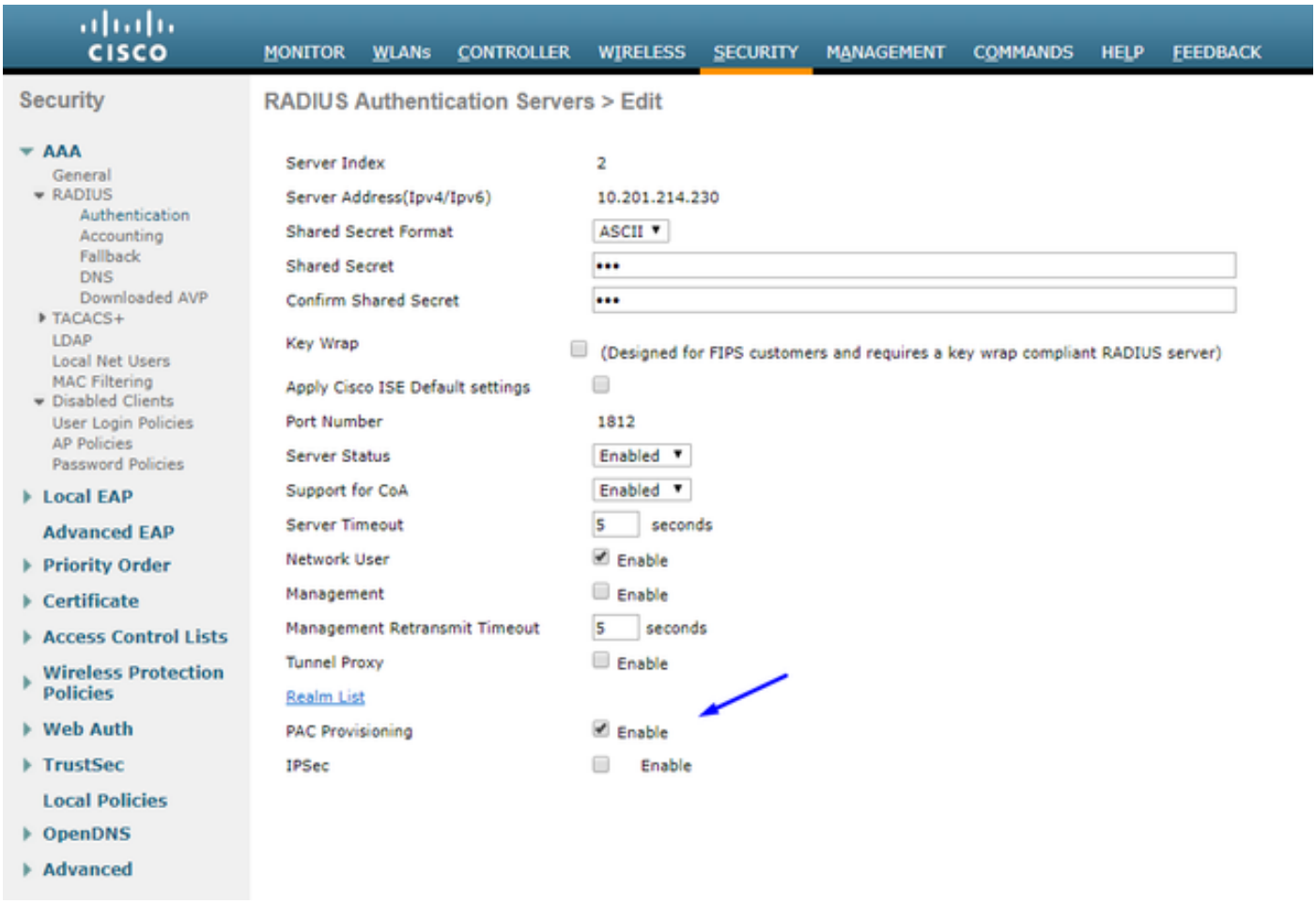
このステップにより、Cisco ISEはIPからSGTへのスタティックなマッピングをWLCに導入できます。これらのマッピングは、前の手順でCisco ISE Web GUIの**Work Centers** > **TrustSec** > **Components** > **IP SGT Static Mappings**で作成しました。


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

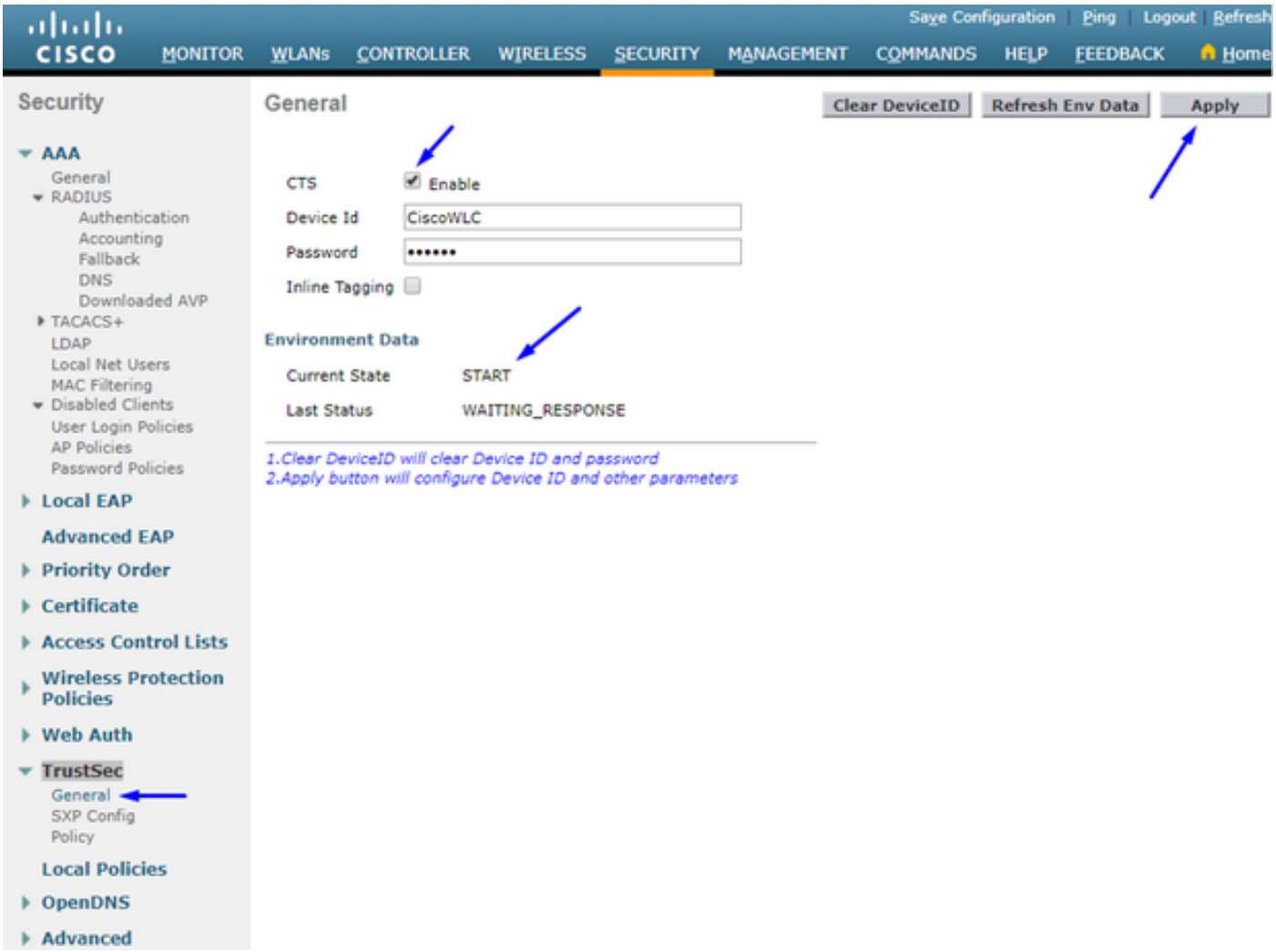


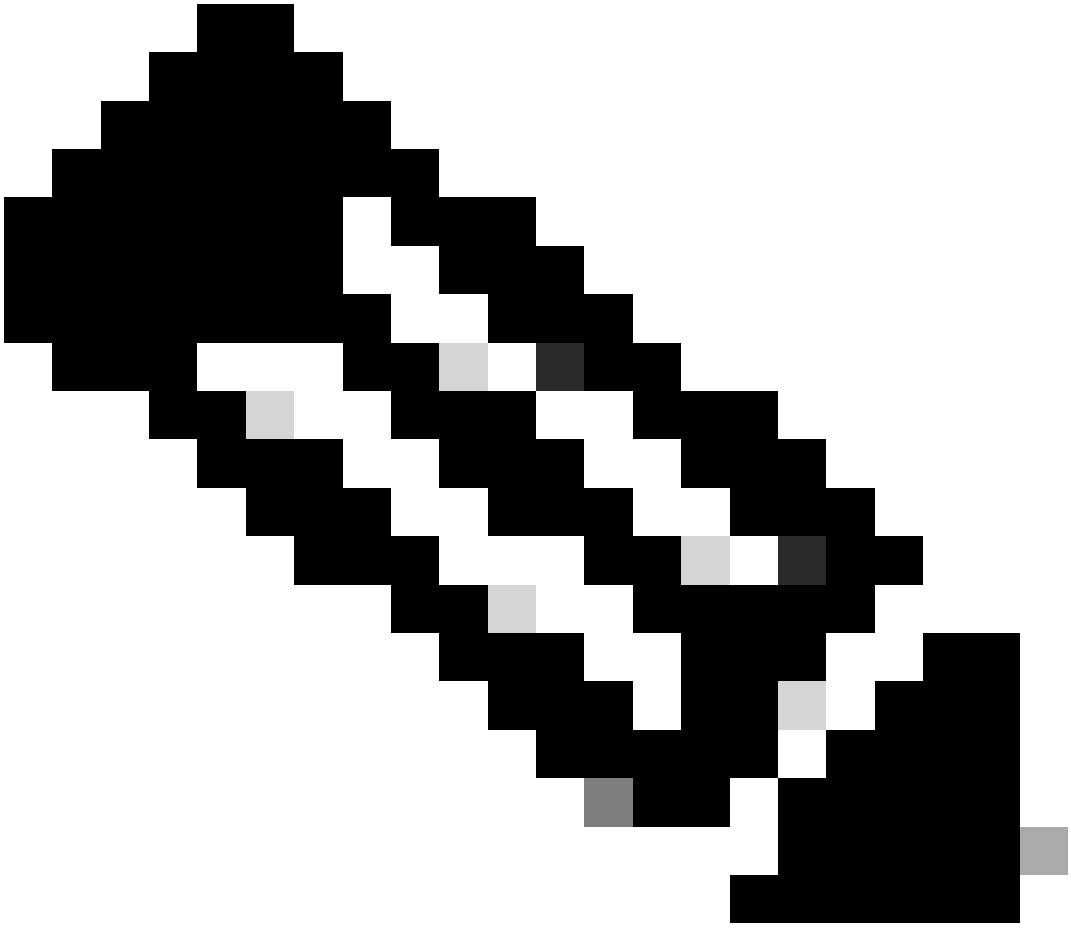
注：この Device Id と Password は後の手順でWLC Web UIのSecurity > TrustSec > Generalで使用します。

WLCのPACプロビジョニングの有効化



WLCでのTrustSecの有効化

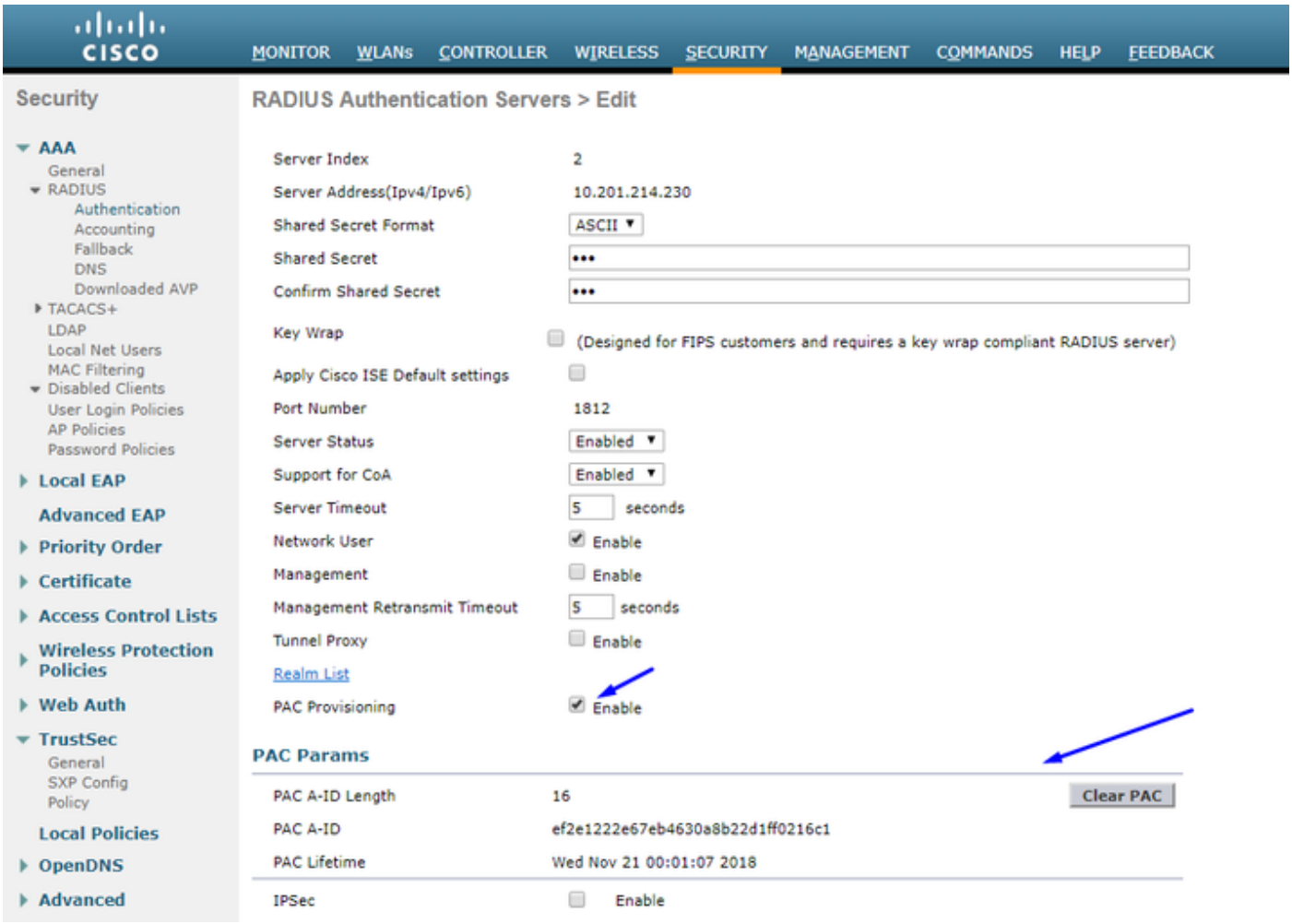

Save Configuration | Ping | Logout | Refresh
CISCO
MONITOR WLANs CONTROLLER WIRELESS SECURITY MANAGEMENT COMMANDS HELP FEEDBACK Home
Security
AAA
General
RADIUS
Authentication
Accounting
Fallback
DNS
Downloaded AVP
TACACS+
LDAP
Local Net Users
MAC Filtering
Disabled Clients
User Login Policies
AP Policies
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



注:CTSおよ Device Id び Password は、Cisco ISEのAdministration > Network Devices > Add Device > Advanced TrustSec Settingsセクションで指定した Device Id および Password と同じにする必要があります。

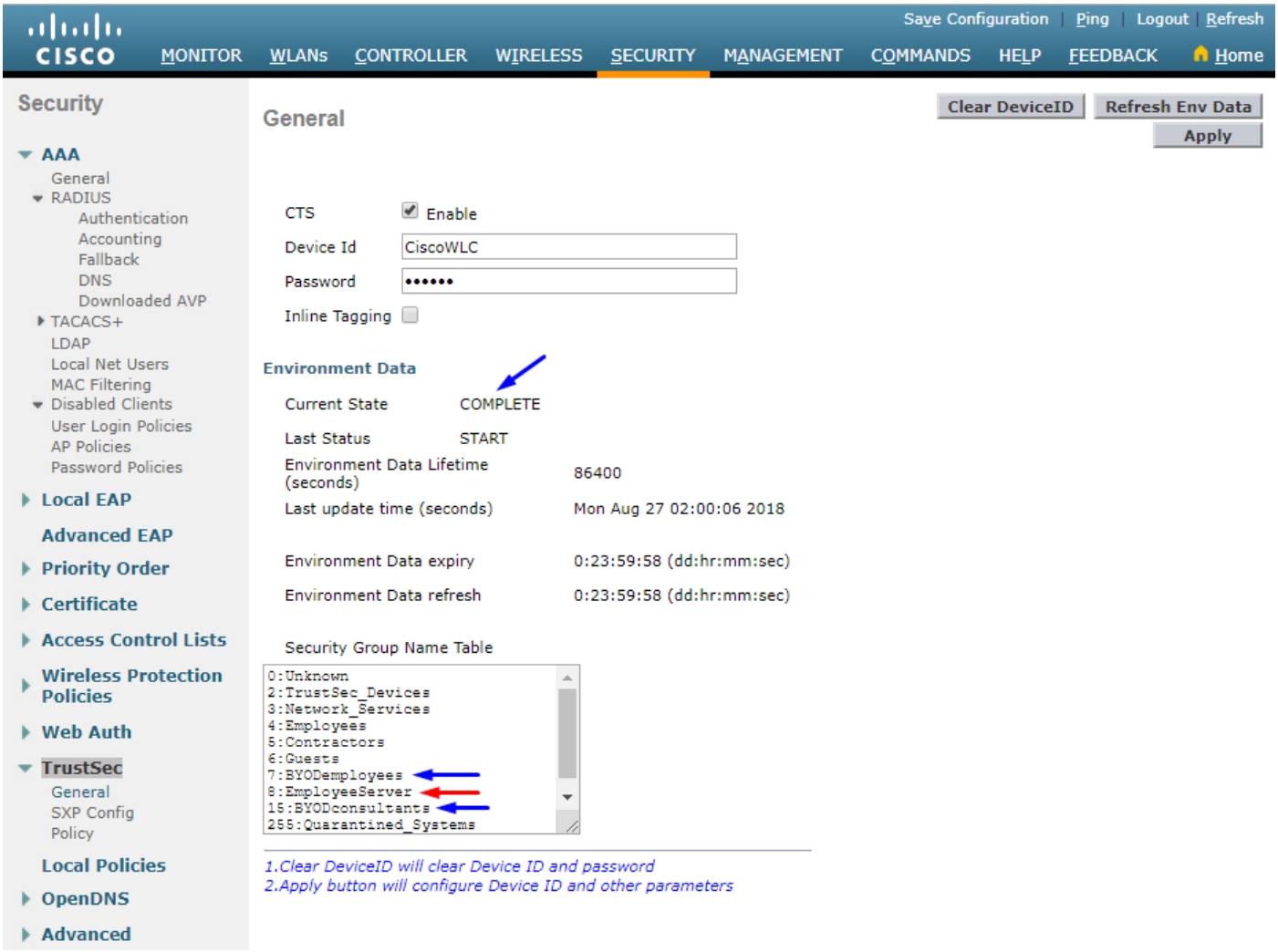
PACがWLCでプロビジョニングされていることの確認

Refresh Env Dataをクリックすると、WLCにPACが正常にプロビジョニングされたことが表示されます（このステップで実行します）。



Cisco ISEからWLCへのCTS環境データのダウンロード

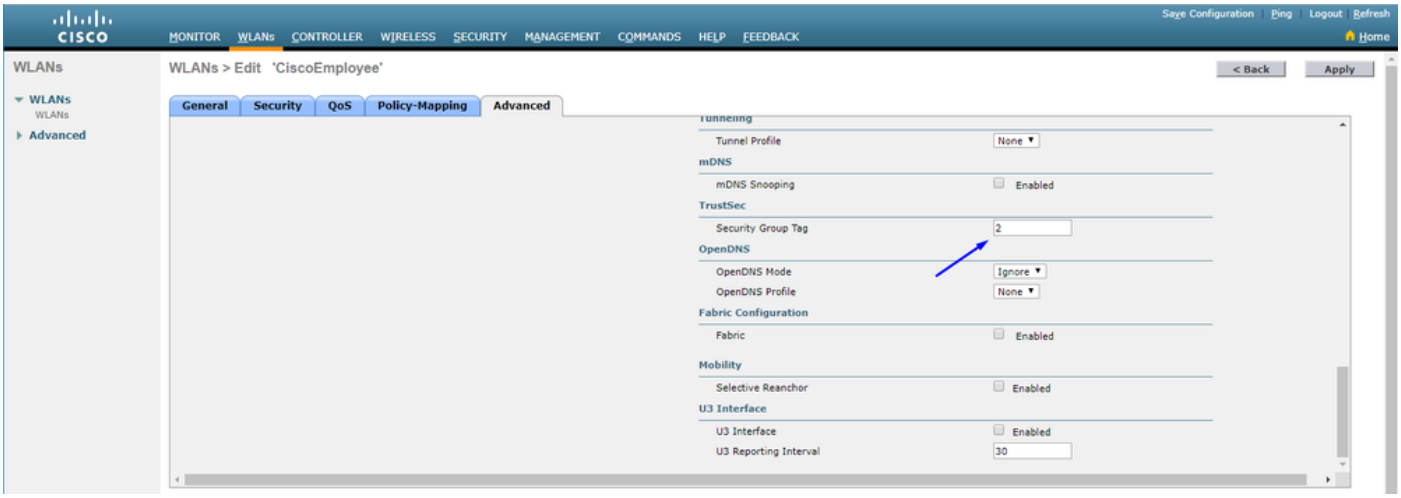
Refresh Env Dataをクリックすると、WLCがSGTをダウンロードします。



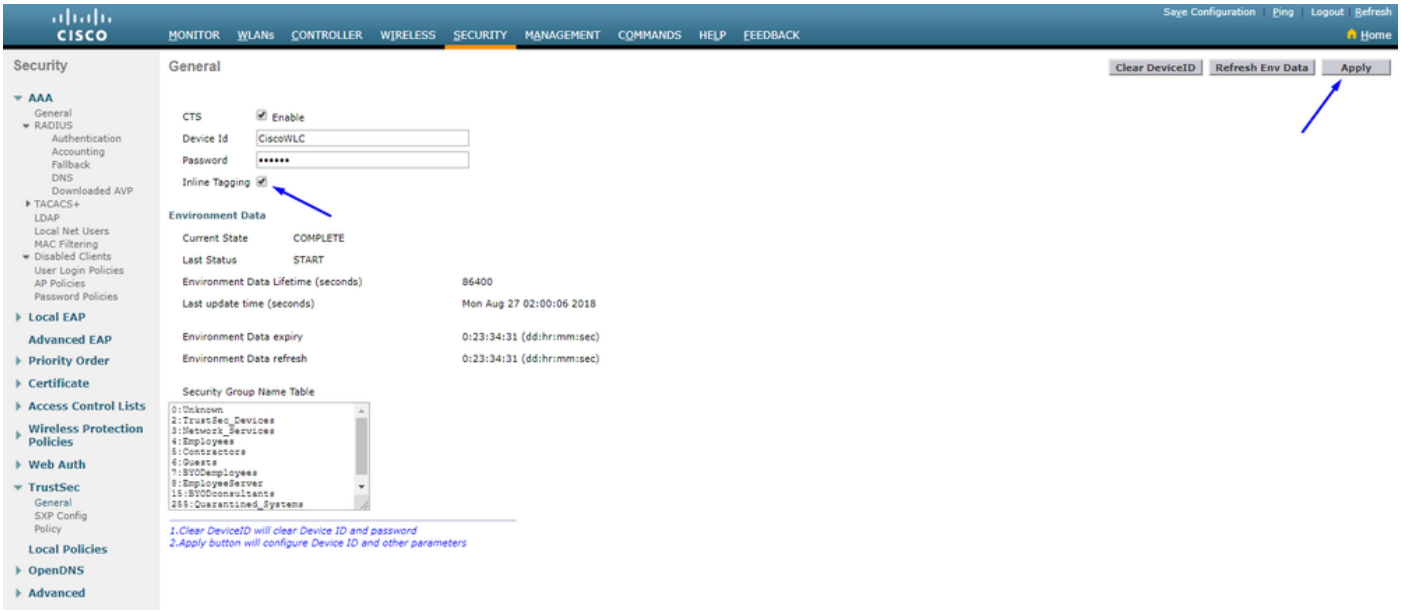
トラフィックに対するSGACLのダウンロードと適用の有効化

WLCとアクセスポイントに2のSGTを割り当てる(TrustSec_Devices)

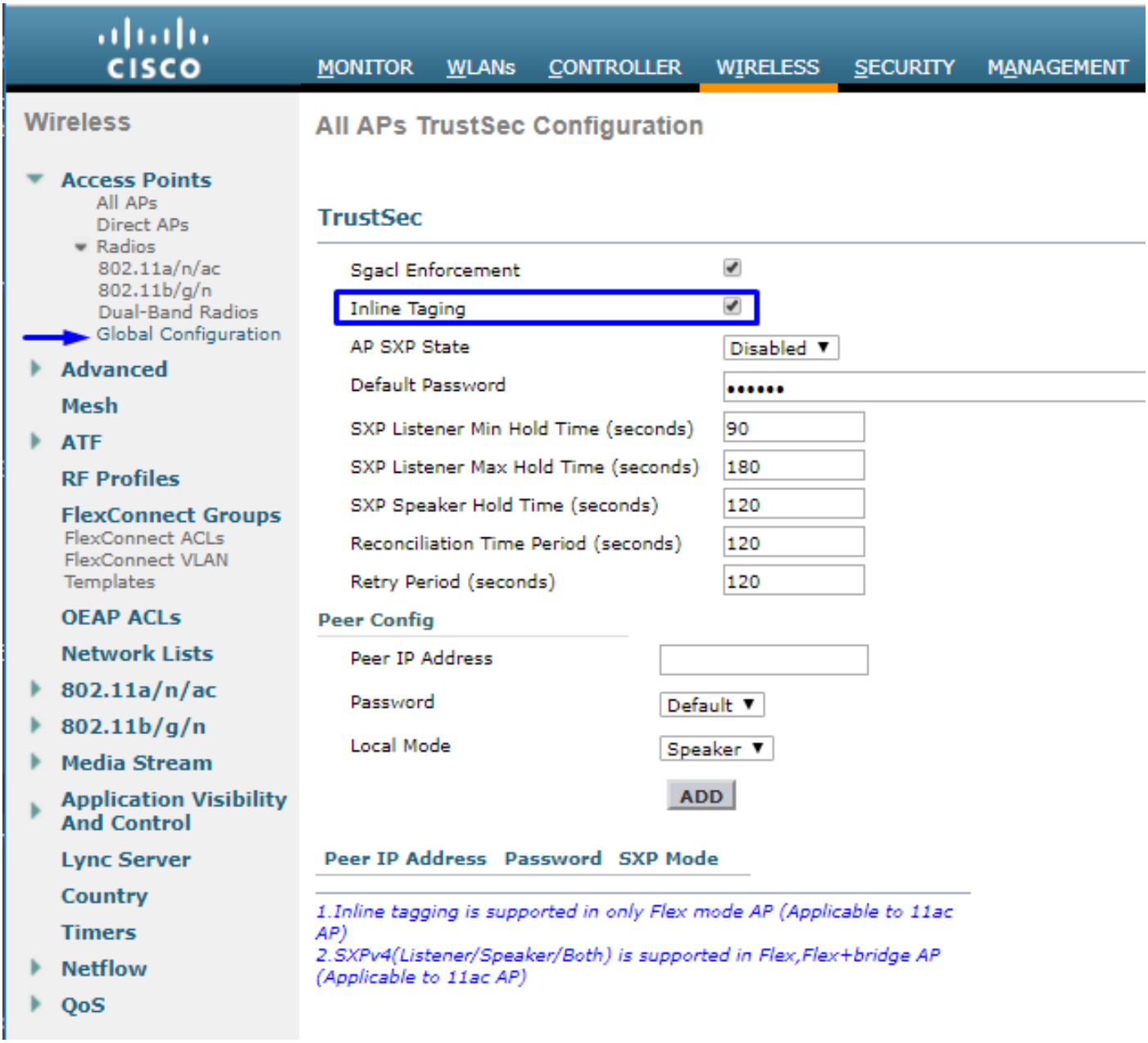
WLC+WLANに2(TrustSec_Devices)のSGTを割り当て、スイッチを介したWLC+APとの間のトラフィック（SSH、HTTPS、およびCAPWAP）を許可します。



WLCでのインラインタギングの有効化



下にスク **Wireless** > **Access Points** > **Global Configuration** ロールダウンして、 **TrustSec Config**を選択します。



Catalystスイッチでのインラインタギングの有効化

<#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
```

確認

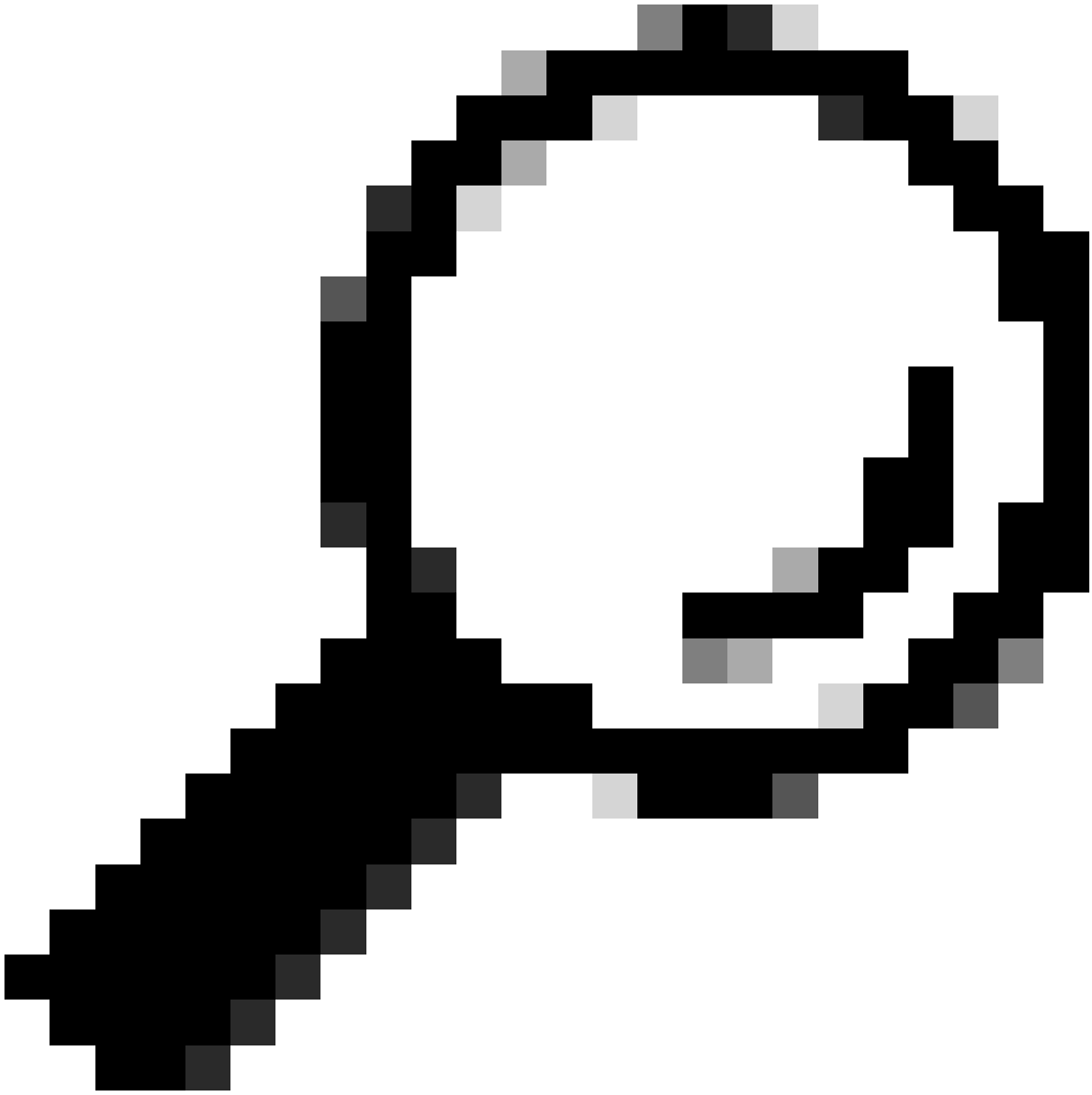
CatalystSwitch#show platform acl counters hardware | SGACLを含む

出力IPv4 SGACLドロップ(454):10フレーム

出力IPv6 SGACLドロップ(455):0フレーム

出力IPv4 SGACLセルドロップ(456):0フレーム

出力IPv6 SGACLセルドロップ(457):0フレーム



ヒント：代わりにCisco ASR、Nexus、またはCisco ASAを使用する場合は、次に示すドキュメントが、SGTタグが適用されていることを確認するのに役立ちます：『TrustSec Troubleshooting Guide』。

ユーザ名jsmith、パスワードAdmin123を使用して無線に対して認証を行うと、スイッチでdeny ACLが検出されます。

This site can't be reached

10.201.214.132 took too long to respond.

Try:

Checking the connection

ERR_CONNECTION_TIMED_OUT

RELOAD

翻訳について
シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。