IBNS 2.0およびインターフェイステンプレートを使用した有線802.1X AP認証の標準化

内容

はじめに

このドキュメントでは、IBNS 2.0インターフェイステンプレートを使用した802.1X設定について説明します。

問題の説明

ポートセキュリティにIEEE 802.1Xを使用することは、一般的なベストプラクティスです。ネットワークセキュリティの向上に加え、ネットワーク全体でアクセスポートの設定を標準化できるため、スイッチの導入も簡素化されます。

このガイドでは、単一の標準化されたスイッチポート設定をエンドデバイスとシスコアクセスポイント(AP)の両方に使用する方法について説明します。 すべてのスイッチポートが最初は標準アクセスポートとして動作し、IEEE 802.1X認証を実行する一方で、認証されたAPには、その展開シナリオに応じて異なる動作モードが必要な場合があります。

複数のSSIDからのクライアントトラフィックはローカルでブリッジされるため、特に、FlexConnectローカルスイッチングモードで動作するAPは、トランクポートで動作する必要があります。その結果、認証が成功した後、スイッチインターフェイスはアクセスポートからトランクポートに動的に移行する必要があります。

単純なエンドデバイスではなく、インフラストラクチャデバイスを接続するアクセスポートでは、デフォルトのアクセスポートの動作とは異なるインターフェイス設定が必要になることがよくあります。

そのため、認証プロセス中にスイッチインターフェイスの設定を動的に変更する必要があります。長年にわたり、Auto SmartPortsやEmbedded Event Manager(EEM)アプレットなど、この動作を実現するためにいくつかのアプローチが使用されてきました。現在、推奨されるソリューションはIBNS 2.0 [1]とインターフェイステンプレートの組み合わせです。これにより、認証が成功した後にインターフェイス設定を動的に変更するためのスケーラブルで一貫性のある方法が提供されます。

アプローチ

正常に機能するセットアップには、次に示すさまざまなコンポーネントが適切に設定されている必要があります

- Radiusサーバ(Identity Service Engine)
- 最大 300 のアクセス ポイント グループ
- アクセスポイント/ワイヤレスLANコントローラ

既存のドキュメント（最後の「参考資料」を参照）が存在するため、このドキュメントでは特定のシナリオに焦点を当て、既存のドキュメントを参考資料として参照します。

要件

次の項目に関する知識があることが推奨されます。

- ワイヤレスLANコントローラ(WLC)とLightweight AP(LAP)

- CiscoスイッチおよびISEでの802.1x
- Extensible Authentication Protocol（EAP）
- Remote Authentication Dial-In User Service（RADIUS）

使用するコンポーネント

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

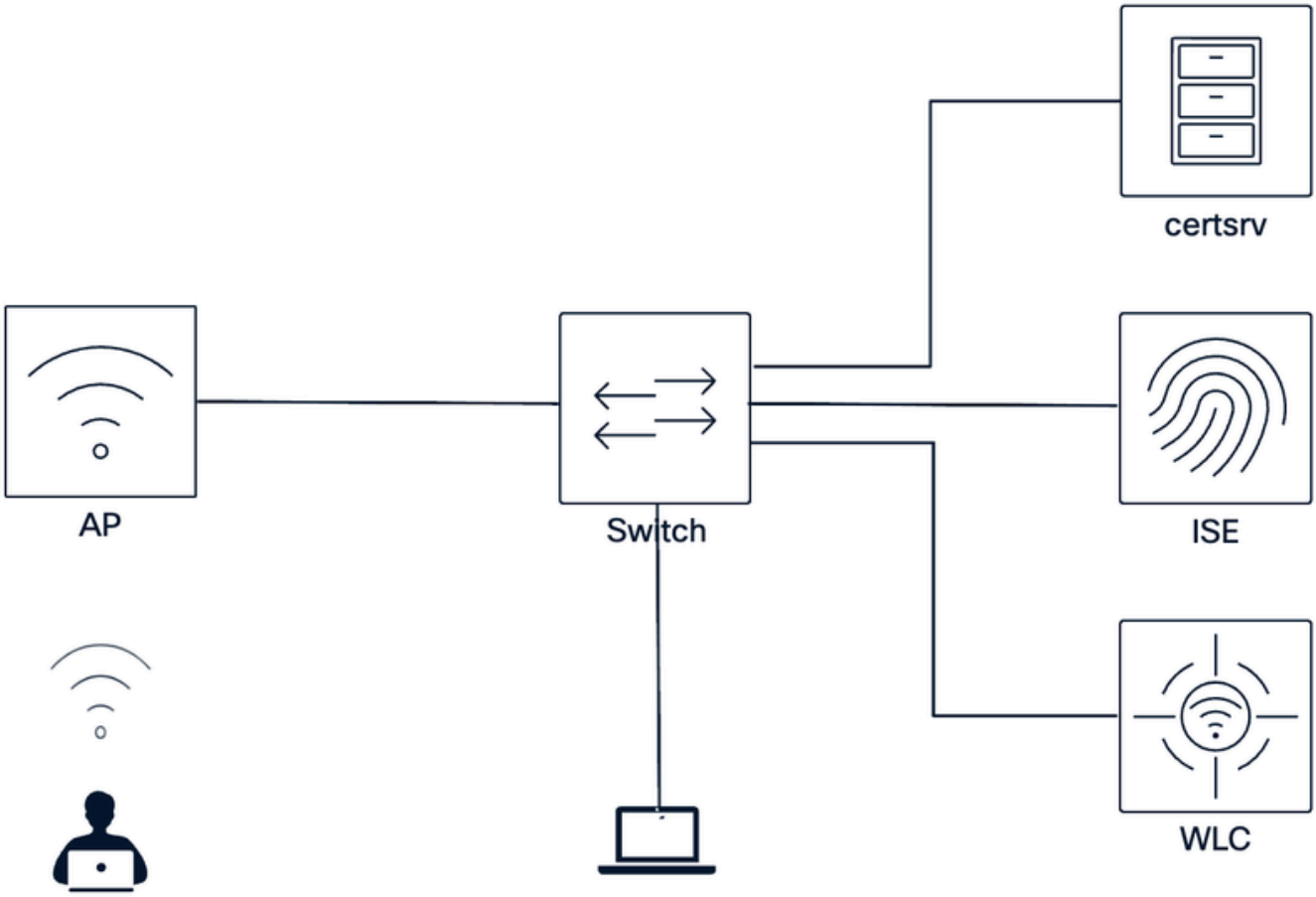
- Cisco C9350 - IOS XE 26.1.1a
- Cisco C9800-40 WLC:IOS XE 26.1.1
- ISEバージョン3.5パッチ1
- AP CW917x、CW916x

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たものです。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。

設定はnetascode.cisco.comのデータモデルにも記載されており、設定を簡単に複製できるように、スイッチングとISEを対象としています。

コンフィギュレーション

ネットワーク図



セットアップ例

この目的のために、単一のシナリオに焦点を当て、設定の抜粋と手順ごとのガイダンスを提供します。その方法にはさまざまなバリエーションがあるため、それらを指摘し、この目的のために既存のドキュメントを参照します。

このガイドで説明するシナリオ：

- EAP-FAST認証を使用したAP有線Dot1X
- C9800 WLCを使用してプロビジョニングされたDot1Xクレデンシャル
- Flex Connectローカルスイッチングモードの AP

この設計では、スイッチポートは最初に、MABフォールバックを使用する一般的なクローズドモードの802.1X設定を使用します。最初のオンボーディング時に、APにはまだ802.1Xクレデンシャルがない可能性があるため、ISEはWLCまたはCatalyst Centerに到達するのに十分な制限付きアクセス権を持つMABを介してAPを認可できます。クレデンシャルまたは証明書がプロビジョニングされた後、APは有線802.1X認証を実行します。ISEは、AP_FLEX_TRUNKインターフェイス

テンプレートに適用される許可結果を返し、ポートを必要なFlexConnectトランク設定に変換します。

Variations				
Auth Types	MAB	EAP-FAST	EAP-PEAP	EAP-TLS
Provisioning of AP Dot1x supplicant	Wireless LAN Controller	Catalyst Center		
Certificate Rollout method	SCEP	EST		

表1：その他のバリエーションとオプションの概要

AP の設定

有線Dot1x認証をAPと組み合わせて使用するには、選択した認証方式に応じたクレデンシャルまたは証明書を、最初にAPに展開する必要があります。

Cisco Catalyst AP Dot1xサプリカントは通常、EAP-FAST、EAP-PEAP、またはEAP-TLSのいずれかをサポートします。また、MABもオプションの1つです。特に、APがEAPタイプの認証を実行できるようにするために、最初にクレデンシャルまたは証明書を収集する必要がある場合に有効です。

- MAB:
  - AP側の設定は不要
  - ハードウェアMACアドレスの管理にはツールが必要
  - 簡単にスプーフィングできる
  - 共通のポート設定が可能

- EAP-FAST：
  - ユーザ名/パスワードベース
  - 展開が容易
  - ISEで有効にされた匿名インバンドPACプロビジョニングが必要

- EAP-PEAP:

    - ユーザ名/パスワードベース
    - サーバー検証に証明書が必要です
    - 証明書の更新を適宜計画する必要があります

- EAP-TLS:
    - Certificate Based
    - 証明書の更新を適宜計画する必要があります

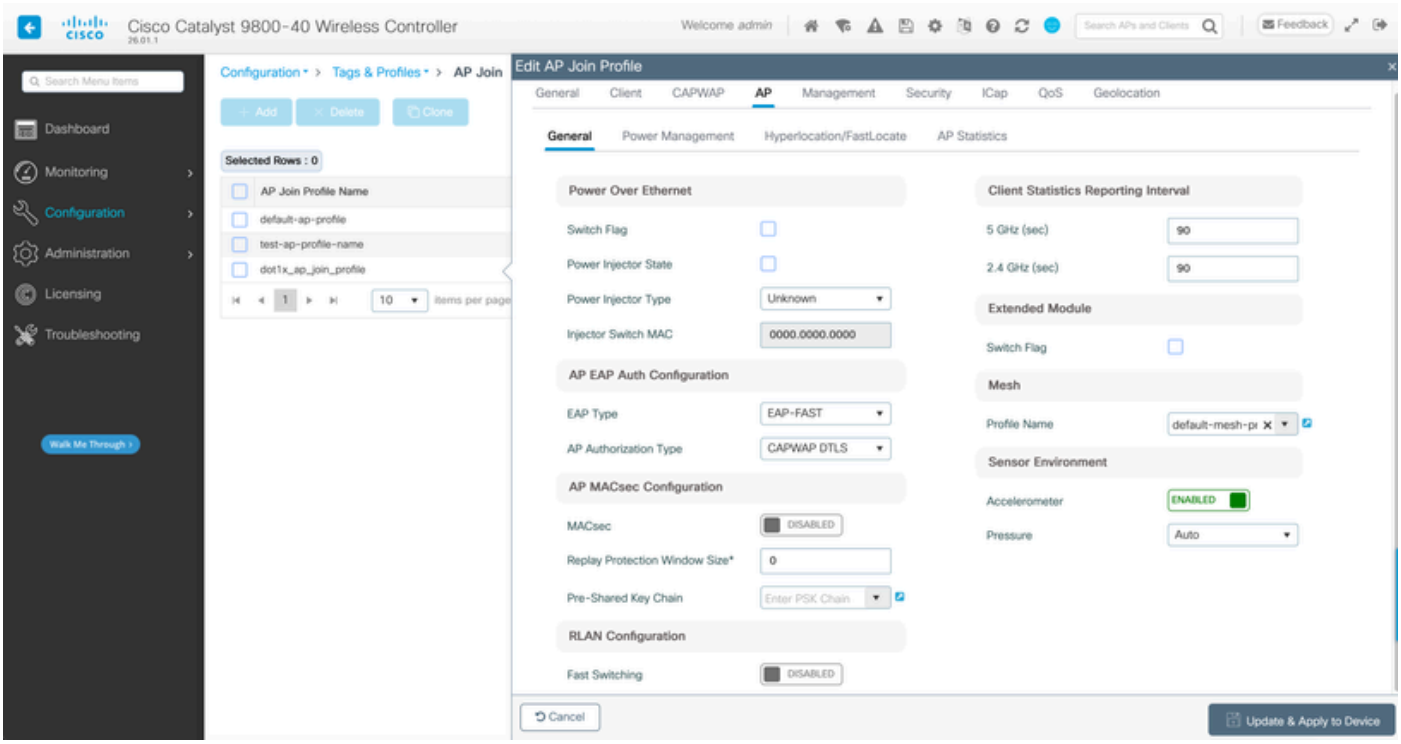
AP有線Dot1Xサプリカントを設定するには、ワイヤレスLANコントローラ(WLC)を使用する方法と、ここで説明するCatalyst Centerを使用する方法の2通りがあります。これらの詳細に入る前に、使用する認証のタイプを事前に選択しておく必要があります。

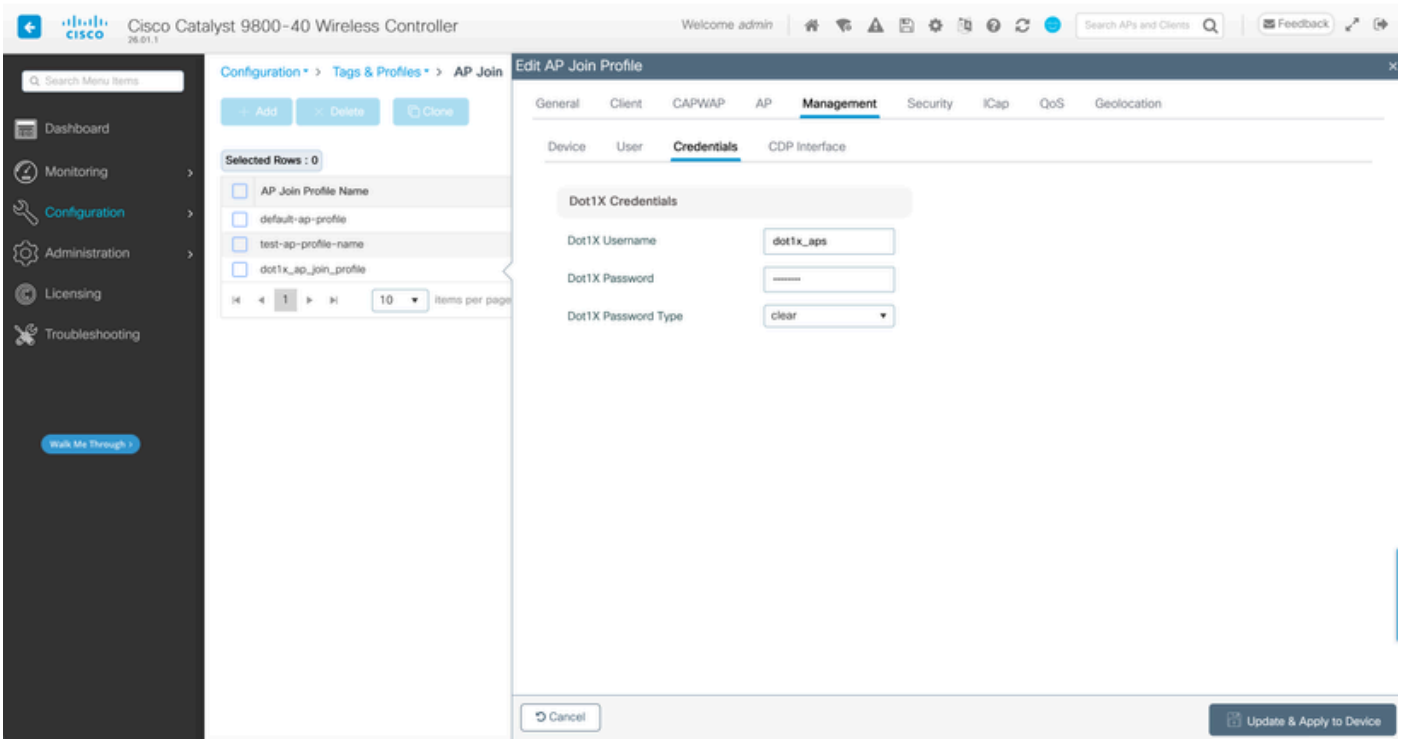
Cisco 9800ワイヤレスLANコントローラ経由の有線Dot1Xのセットアップ

証明書ベースの認証（EAP-PEAPまたはEAP-TLS [1]）を選択した場合は、次の手順として、SCEP [2]またはEST [3]を介してローカルで有効なAP証明書(LSC)を発行する方法を決定する必要があります。

このシナリオのようにEAP-FASTを使用する場合、AP加入プロファイルを生成すれば十分です。AP加入プロファイルでは、Dot1Xのユーザとパスワードを入力し、その加入プロファイルをサイトタグにバインドしてAPに割り当てます。

GUI での設定





CLI での設定

```
ap profile dot1x_ap_join_profile
 country DE
description dot1x_ap_join_profile
 dot1x eap-type eap-fast
 dot1x username <DOT1X_USER> password 0 <DOT1X_PASSWORD>
```

Catalyst Centerプラグアンドプレイによる有線Dot1Xのセットアップ

PnP [4]を機能させるには、Catalyst CenterをISEと統合する必要があります。これは、ISEによるEAP認証のためにAP側からサーバ検証を実行できる必要がある証明書のために必要です。デバイス側の証明書の場合、APはCatalyst Center CAによって発行された証明書を取得します。この証明書は、デフォルトで独自に組み込まれているか、各CAのSubCA/SCEPによって設定されている場合に取得されます。

PnPによるセットアッププロセスでは、デバイスがWLCに参加する前に証明書やクレデンシャルをプロビジョニングできます。

スイッチの設定

認証はセキュリティメカニズムであるだけでなく、スイッチポート設定を標準化する方法でもあります。したがって、これらの部分では、これを実現するために必要な要素について説明します。これは設定例であり、確認して設定に適応させる必要があります。一般に、この設定では、停止したRadiusシナリオや再認証などを適切に処理するDot1xおよびフォールバックMABが許可されます。

グローバルRADIUS属性：

```
!
radius-server attribute 6 on-for-login-auth
radius-server attribute 6 support-multiple
radius-server attribute 8 include-in-access-req
radius-server attribute 25 access-request include
radius-server attribute 31 mac format ietf upper-case
radius-server attribute 31 send nas-port-detail mac-only
radius-server dead-criteria time 5 tries 3
radius-server deadtime 3
!
ip radius source-interface <RADIUS-SOURCE-INTERFACE>
!
```

Radiusサーバグループ：

```
!
radius server client-radius-server01
 address ipv4 <ISE01-PSN-IP> auth-port 1812 acct-port 1813
 timeout 10
 retransmit 1
 automate-tester username dummy ignore-acct-port probe-on key 6 <RADIUS-SECRET>
!
!
```

```
aaa group server radius client-radius-group
 server name client-radius-server01
 ip radius source-interface <RADIUS-SOURCE-INTERFACE>
!
```

AAA設定：

```
!
aaa new-model
aaa session-id common
!
aaa authentication dot1x default group client-radius-group
aaa authorization network default group client-radius-group
aaa accounting Identity default start-stop group client-radius-group
aaa accounting update newinfo periodic 2880
!
aaa server radius dynamic-author
 client <ISE01-PSN-IP> server-key 6 <RADIUS-SECRET>
!
```

IBNS2.0クラスマップおよびサービステンプレート：

```
!
service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
 voice vlan
service-template DEFAULT_CRITICAL_DATA_TEMPLATE
service-template CRITICAL_AUTH_VLAN
 vlan <CRITICAL-AUTH-VLAN>
!
class-map type control subscriber match-all AAA_SVR_DOWN_AUTHD_HOST
 match authorization-status authorized
 match result-type aaa-timeout
!
class-map type control subscriber match-all AAA_SVR_DOWN_UNAUTHD_HOST
 match authorization-status unauthorized
 match result-type aaa-timeout
!
class-map type control subscriber match-all DOT1X
 match method dot1x
!
class-map type control subscriber match-all DOT1X_FAILED
 match method dot1x
 match result-type method dot1x authoritative
!
class-map type control subscriber match-all DOT1X_MEDIUM_PRIO
 match authorizing-method-priority gt 20
!
class-map type control subscriber match-all DOT1X_NO_RESP
 match method dot1x
 match result-type method dot1x agent-not-found
!
class-map type control subscriber match-all DOT1X_TIMEOUT
 match method dot1x
```

```
 match result-type method dot1x method-timeout
!
class-map type control subscriber match-any IN_CRITICAL_AUTH
 match activated-service-template CRITICAL_AUTH_VLAN
 match activated-service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
!
class-map type control subscriber match-all MAB
 match method mab
!
class-map type control subscriber match-all MAB_FAILED
 match method mab
 match result-type method mab authoritative
!
class-map type control subscriber match-none NOT_IN_CRITICAL_AUTH
 match activated-service-template CRITICAL_AUTH_VLAN
 match activated-service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
!
```

IBNS 2.0サービスポリシー：

```
!
policy-map type control subscriber WiredDot1xClosedAuth_1X_MAB
 event inactivity-timeout match-all
  10 class always do-until-failure
   10 clear-session
 event session-started match-all
  10 class always do-until-failure
   10 authenticate using dot1x retries 2 retry-time 0 priority 10
 event agent-found match-all
  10 class always do-until-failure
   10 terminate mab
   20 authenticate using dot1x priority 20
 event aaa-available match-all
  10 class IN_CRITICAL_AUTH do-until-failure
   10 clear-session
  20 class NOT_IN_CRITICAL_AUTH do-until-failure
   10 resume reauthentication
 event authentication-failure match-first
  10 class DOT1X_FAILED do-until-failure
   10 terminate dot1x
   20 authenticate using mab priority 20
  20 class AAA_SVR_DOWN_UNAUTHD_HOST do-until-failure
   10 activate service-template CRITICAL_AUTH_VLAN
   20 activate service-template DEFAULT_CRITICAL_VOICE_TEMPLATE
   30 authorize
   40 pause reauthentication
  30 class AAA_SVR_DOWN_AUTHD_HOST do-until-failure
   10 pause reauthentication
   20 authorize
  40 class DOT1X_NO_RESP do-until-failure
  10 terminate dot1x
  20 authenticate using mab priority 20
 50 class MAB_FAILED do-until-failure
  10 terminate mab
  20 authentication-restart 60
 60 class DOT1X_TIMEOUT do-until-failure
  10 authenticate using mab priority 20
 70 class always do-until-failure
```

```
  10 terminate dot1x
  20 terminate mab
  30 authentication-restart 60
!
```

インターフェイステンプレート：

```
!
template AP_FLEX_TRUNK
 dot1x pae authenticator
 dot1x timeout supp-timeout 7
 dot1x max-req 3
 switchport trunk native vlan <TRUNK-NATIVE-VLAN>
 switchport trunk allowed vlan <TRUNK-ALLOWED-VLANS>
 switchport mode trunk
 mab
 access-session host-mode multi-host peer
 access-session closed
 access-session port-control auto
 authentication periodic
 authentication timer reauthenticate server
 service-policy type control subscriber WiredDot1xClosedAuth_1X_MAB
!
template DEFAULT-ACCESS-PORT
 dot1x pae authenticator
 dot1x timeout supp-timeout 7
 dot1x max-req 3
 switchport mode access
 mab
 access-session host-mode multi-domain
 access-session closed
 access-session port-control auto
 authentication periodic
 authentication timer reauthenticate server
 service-policy type control subscriber WiredDot1xClosedAuth_1X_MAB
!
```

インターフェイス設定：

```
!
interface TenGigabitEthernet1/0/1
 switchport access vlan <DEFAULT-ACCESS-VLAN>
 switchport mode access
 dot1x timeout tx-period 7
 dot1x max-reauth-req 3
 source template DEFAULT-ACCESS-PORT
 spanning-tree portfast
 spanning-tree bpduguard enable
!
```

グローバル必須：

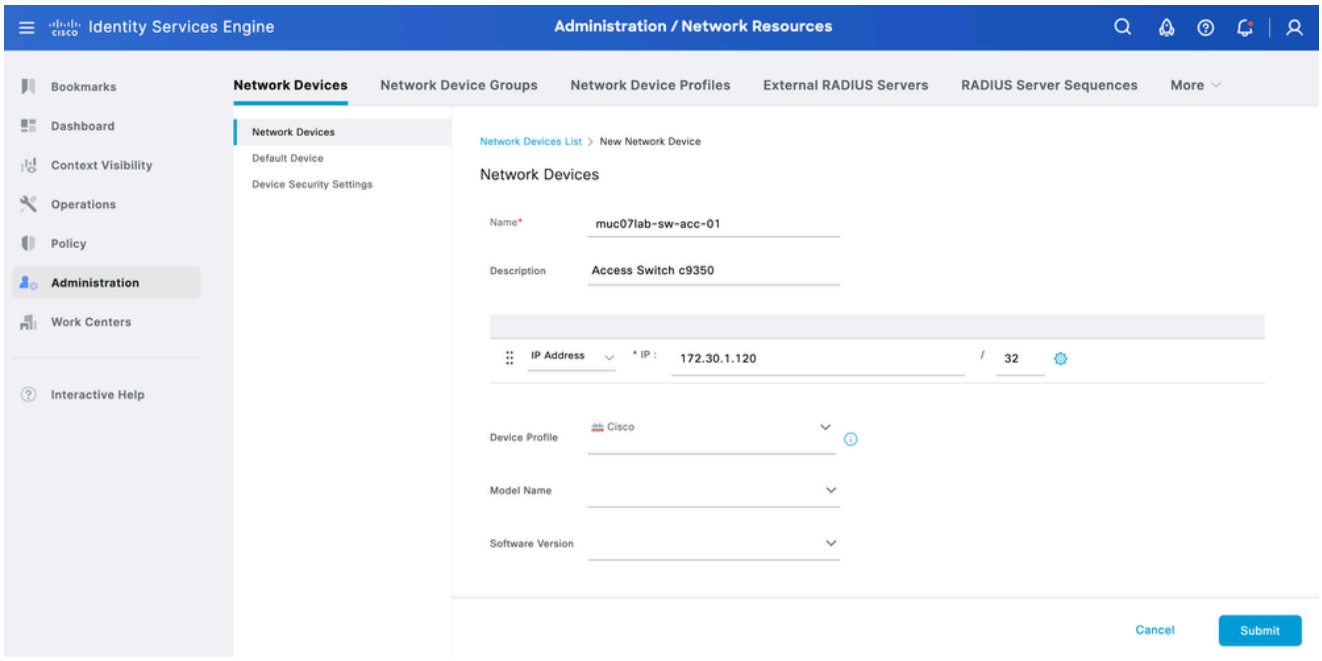
```
!
dot1x system-auth-control
!
access-session interface-template sticky timer 60
!
```

注:CW9178を使用する場合、認証中にAPは2つのMACアドレスを提示します。スイッチポートがerr-disabled状態にならないようにするため、最初にポートをhost-mode multi-authに設定する必要があります。802.1X認証に成功した後、ポート設定を動的にホストモードマルチホストに変更することをお勧めします。

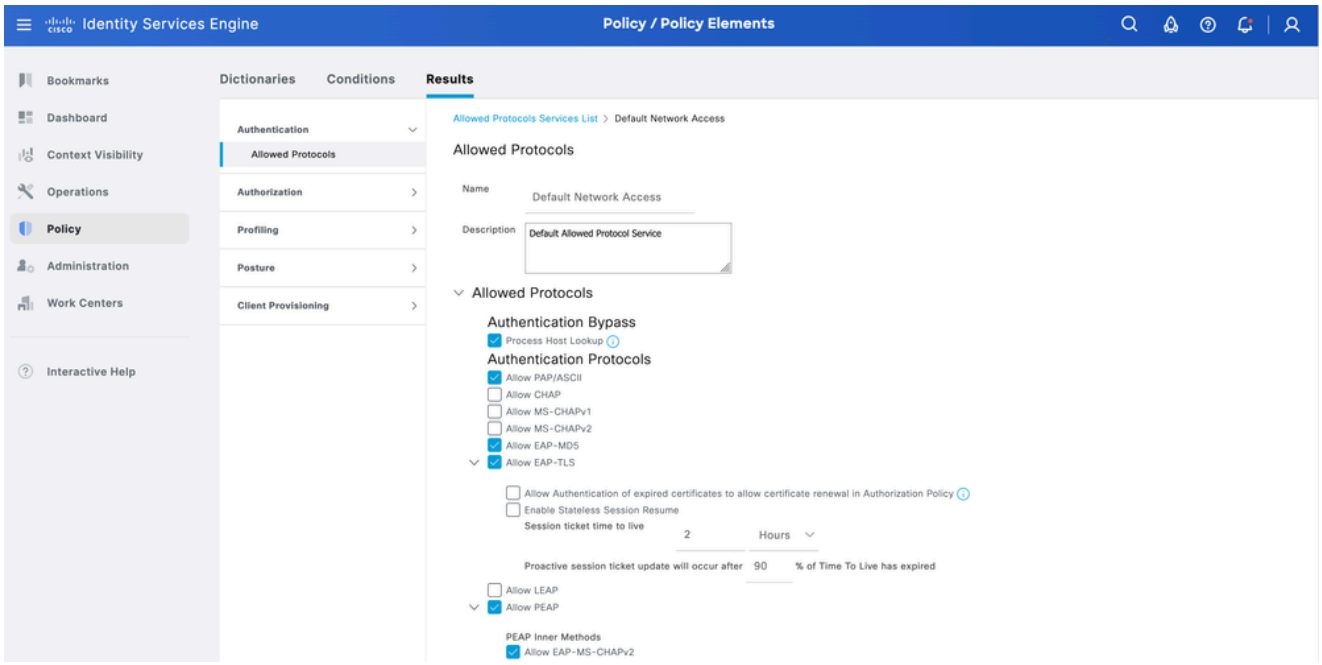
Identity Services Engineの設定

最後に、認証を許可するようにRADIUSサーバを設定する必要もあります。有線Dot1xについては、広範なガイド[5]があるため、この場合は関連する部分だけに焦点を当てます。

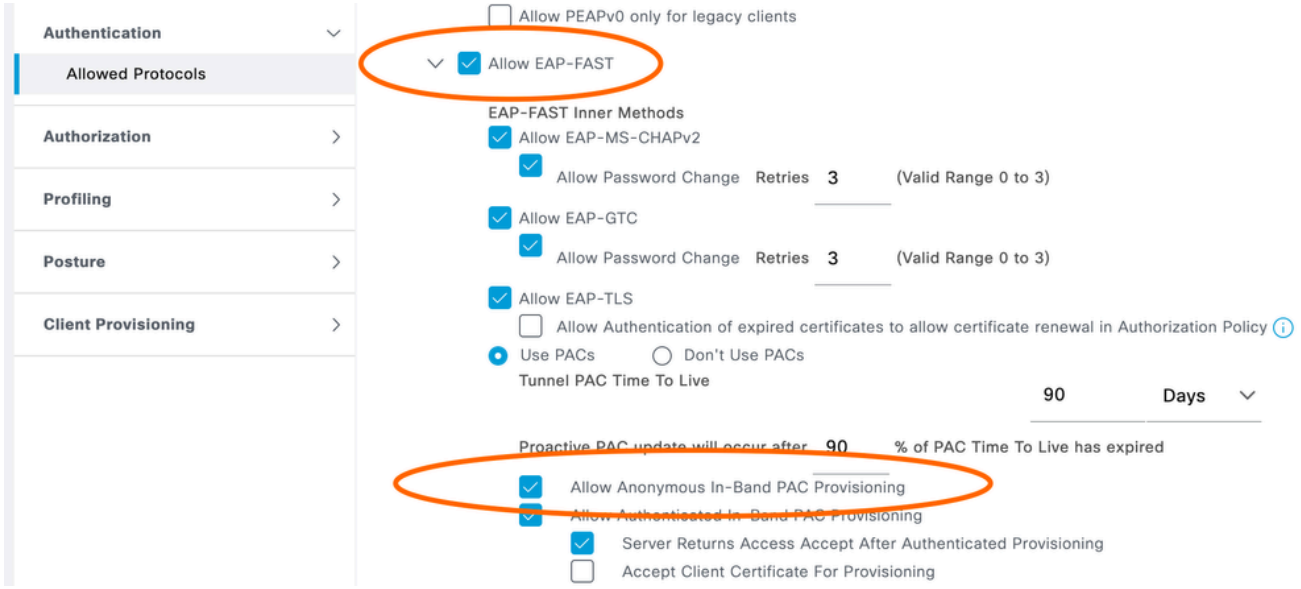
1. スイッチをネットワークアクセスデバイスとして追加します。
   > Administration > Network Resources > Network Devices > Add



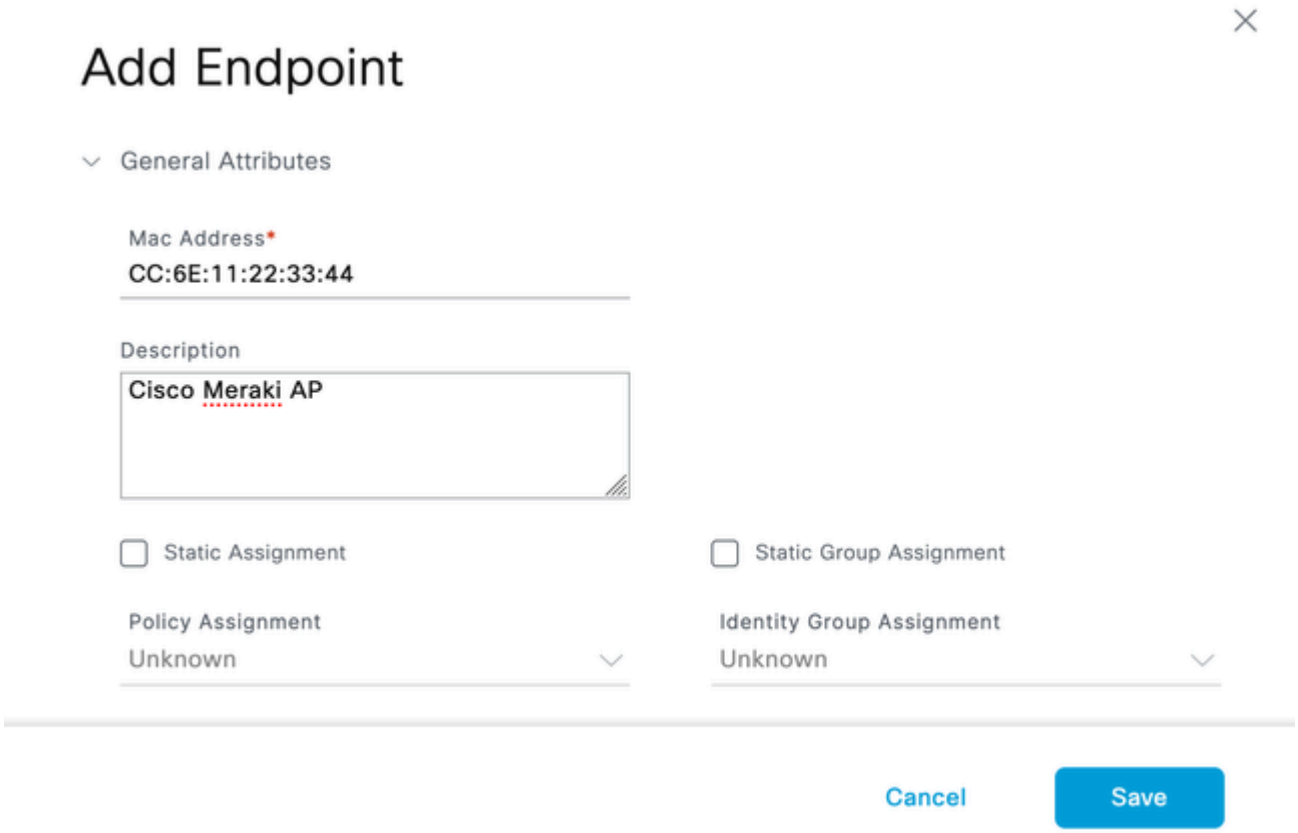
2. 使用しているEAPプロトコルをイネーブルにします。
   > Policy > Policy Elements > Results > Authentication > Allowed Protocols



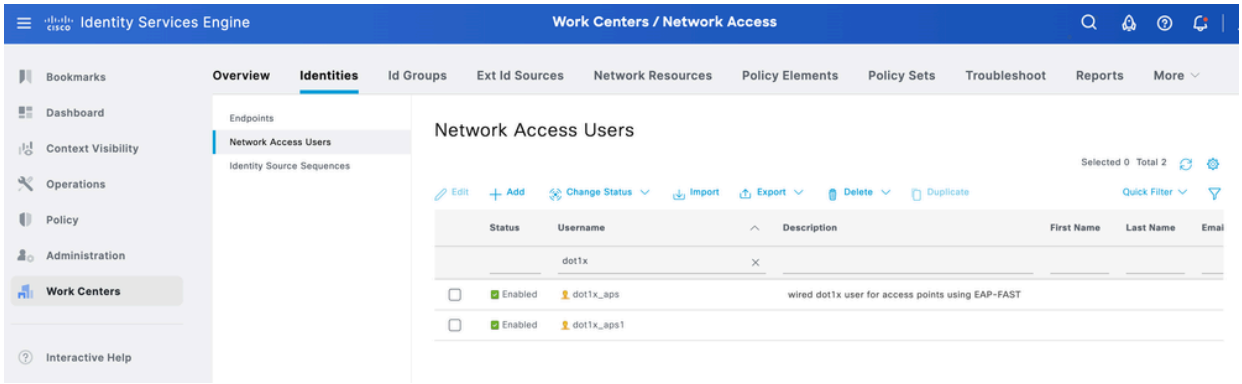
3. このシナリオでは、EAP-FASTを使用しているため、「匿名インバンドPACプロビジョニング」を有効にする必要があることに注意してください。



4. IDの追加
   > [ワークセンター] > [ネットワークアクセス] > [アイデンティティ]
   a. 正常に動作させるには、通常、このプロセスは2つのステップで構成されます。最初は、APにクレデンシャルがないため、EAP認証に応答できません。その結果、スイッチポートは最初にMABを使用してAPを認証する必要があります。これは、一般的な認可ポリシー、ロケーションベースのポリシー、またはデバイスプロファイリングに基づくことができます。使用されるポリシーに関係なく、APがCAPWAP経由でWLCから、またはプラグアンドプレイ(PnP)経由でCisco Catalyst Center(CAC)からクレデンシャルを取得できるようにするには、初期MAB認証が成功する必要があります。

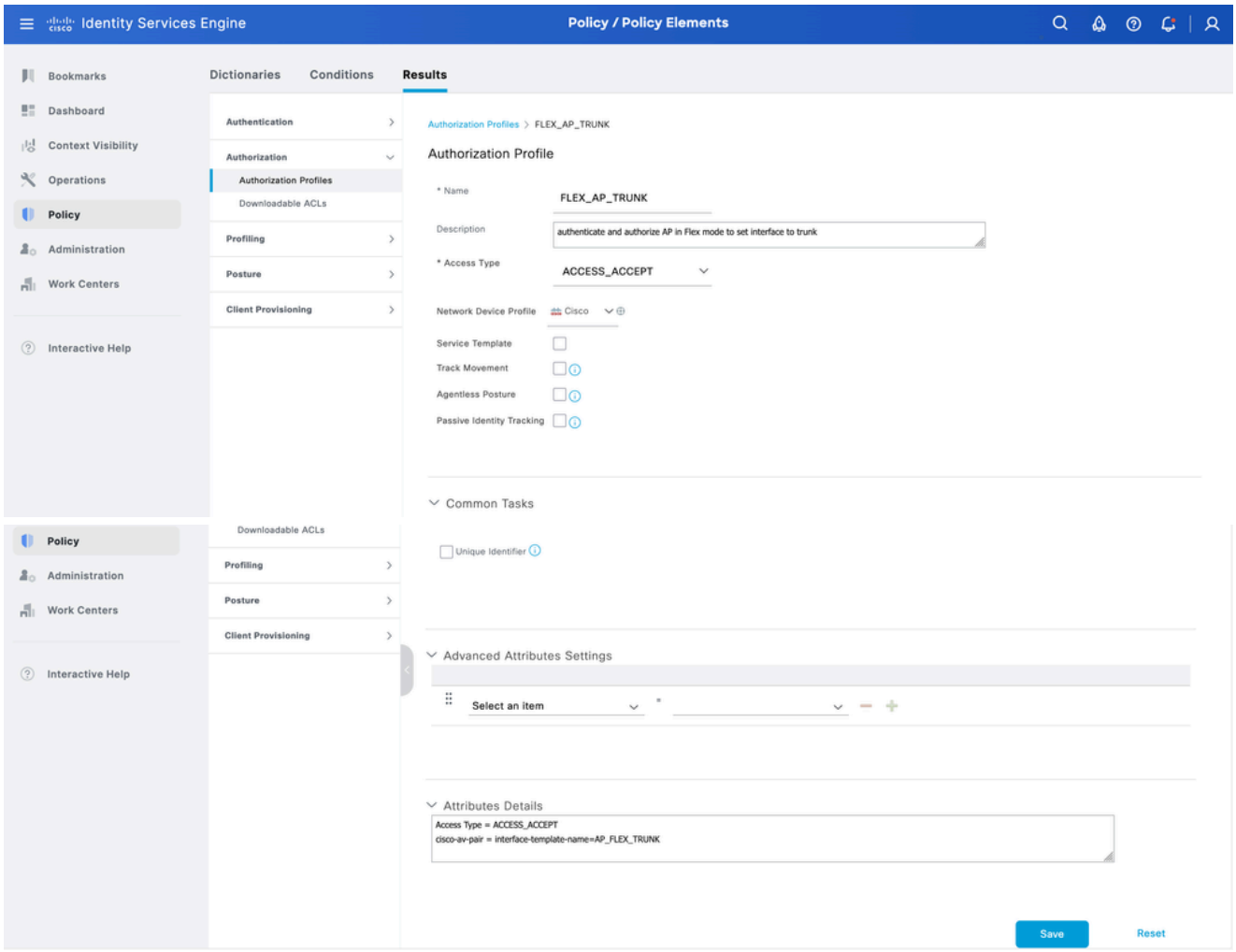


b. APがクレデンシャル/証明書を収集すると、AP有線Dot1XサプリカントはEAPoLに応答し、Dot1XはAPのフルアクセスを可能にする後続の認証方式です。
このシナリオでは、ユーザ名/パスワードを追加する必要があります。

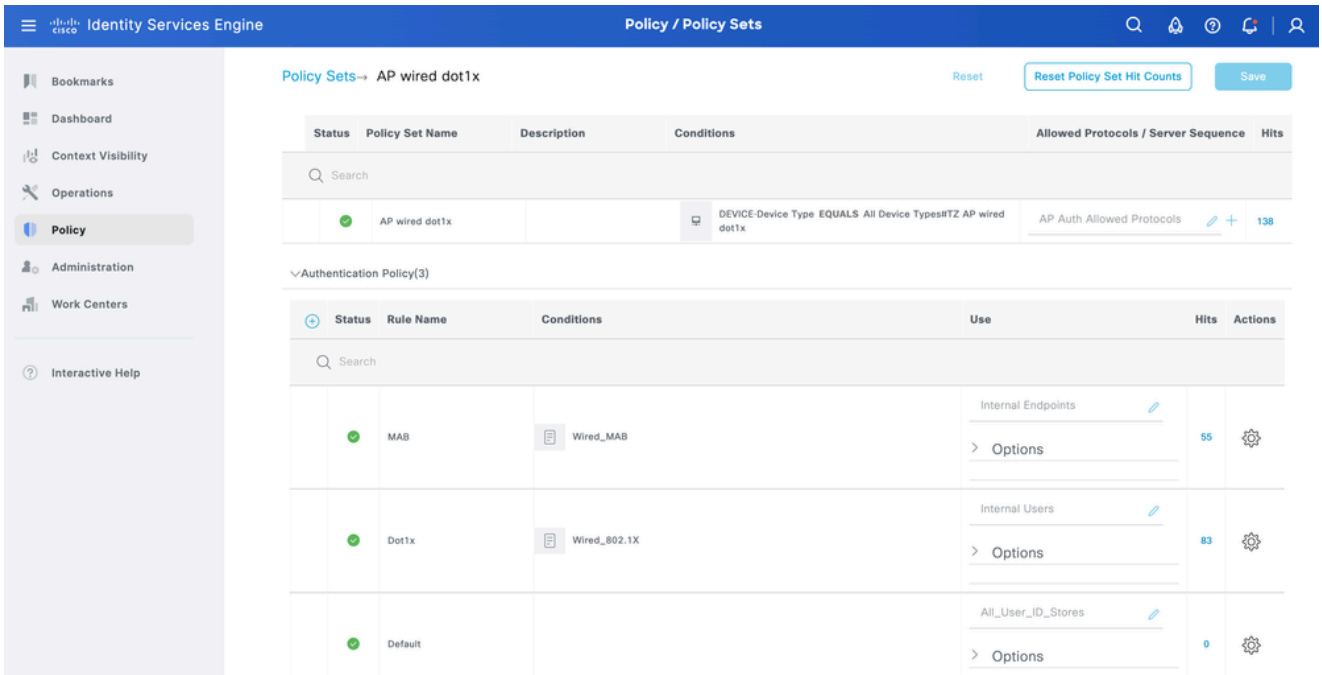


5. 認証プロファイルの作成
許可プロファイルは、必要なAVペアで応答します。この例では、スイッチポートを動的に変更するため、インターフェイステンプレートを設定する必要があります。
> Policy > Policy Elements > Results > Authorization > Authorization Profiles

名前：FLEX_AP_TRUNK
アクセスタイプ： ACCESS_ACCEPT
インターフェイステンプレート：AP_FLEX_TRUNK

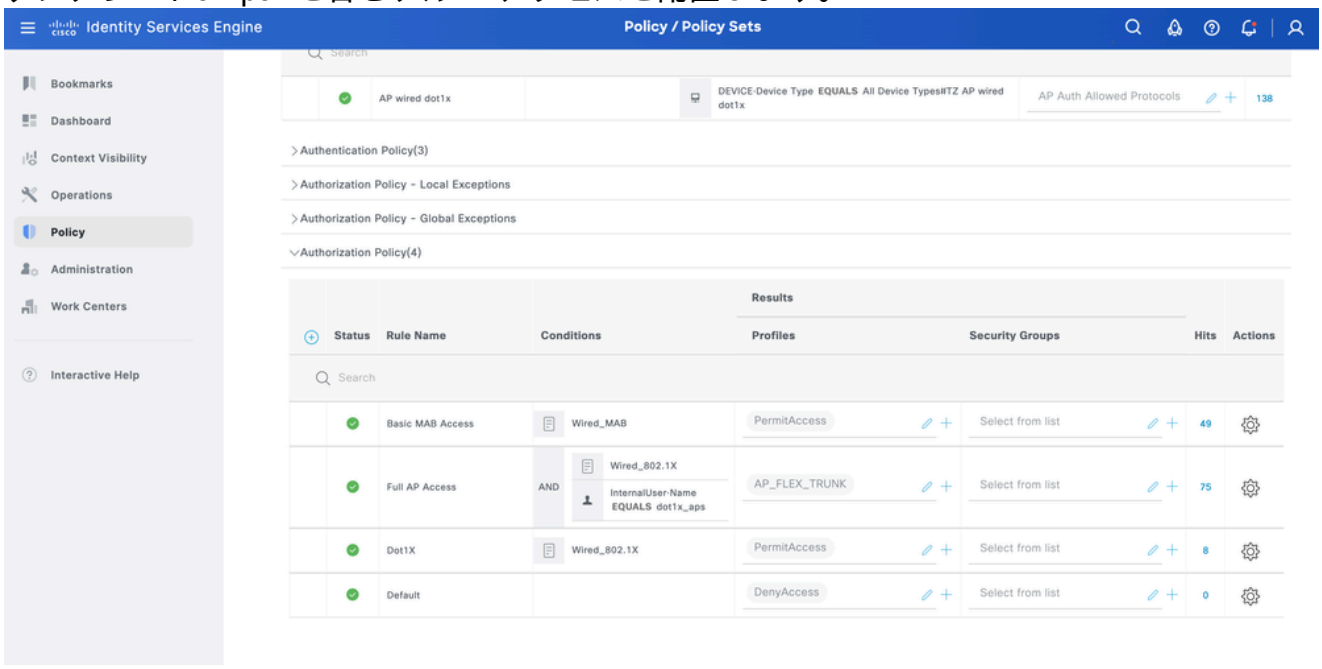


6. 認証ポリシーの作成
   MABおよび有線Dot1Xを許可し、適切なIDストアでエンドポイント/ユーザを検索する認証ポリシーを作成します。



MABのニーズに応じて限定的なアクセス許可結果と、Dot1xの参照されたインターフェイス

テンプレートav-pairを含むフルAPアクセスを配置します。



確認

この設定を行ったら、APをスイッチに接続します。前提条件として、デフォルトのネットワーク設定、この場合はオプション43がWLCを指すアクセスVLANのDHCPプール、およびAPからWLCへのCAPWAP通信が可能であることが想定されています。

AP コマンド

```
show ap authentication status
show crypto
show crypto pki trustpool
```

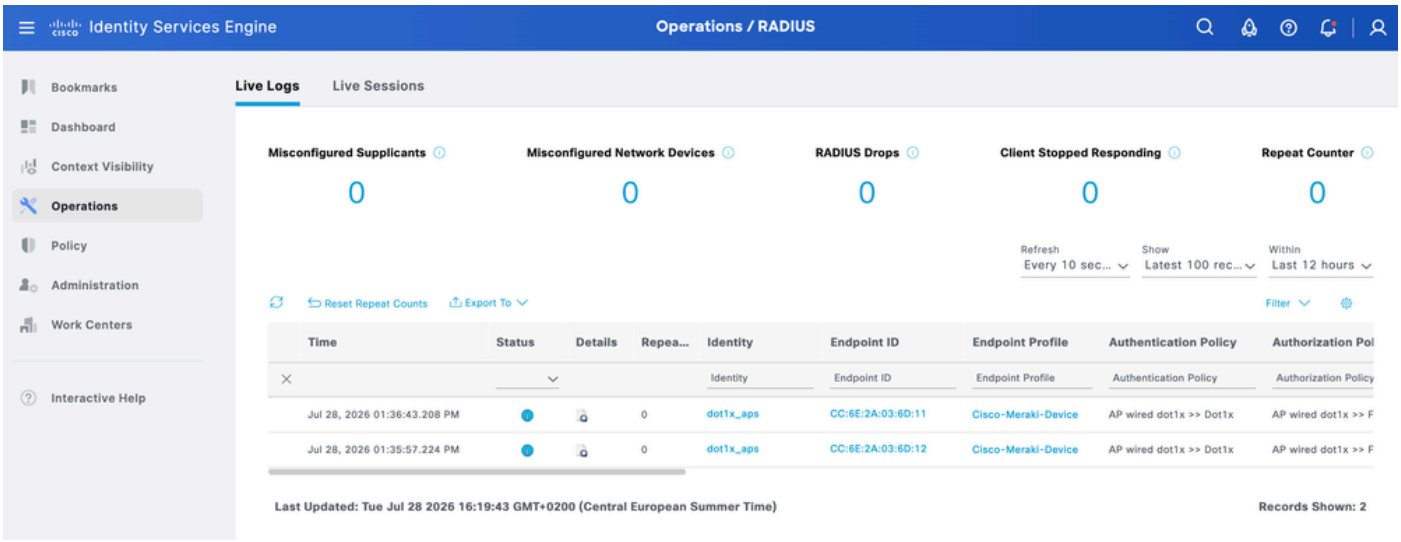
スイッチ コマンド

```
show access-session
show aaa servers
show access-session interface <INTERFACE> details
show template interface binding target <INTERFACE>
show derived-config interface <INTERFACE>

Sample output:
!
C9350-02-R11#show access-session interface te1/0/1
Interface MAC Address Method Domain Status Fg Session ID
-----------------------------------------------------------------------------------------
```

```
Te1/0/1 6cef.1122.3344 dot1x DATA Auth 09FE1FAC000000948FF60A2F
```

ISE



略語一覧

略語	拡張
[AAA]	認証、認可、アカウンティング
AP	アクセス ポイント
認証	CA1 を関連付けます
認証Z	許可
CA	認証局（CA）
シスコ	クライアント情報シグナリングプロトコル
Dot1x	IEEE 802.1X
EAP	Extensible Authentication Protocol（拡張認証プロトコル）
EST	セキュアな転送を介した登録
FAST	セキュアトンネリングを介した柔軟な認証
IBNS（イブン）	Identity Based Networkingサービス
ISE	Identity Services Engine
MAB	MAC認証バイパス
ナド	ネットワークアクセスデバイス

PEAP	Protected Extensible Authentication Protocol(PEAP)
SCEP	簡易証明書登録プロトコル(SCEP)
[TLS]	Transport Layer Security
WLC	ワイヤレス LAN コントローラ

参考資料

[1] LSCを使用したPEAPまたはEAP-TLS用のAPでの802.1Xの設定

[2] 9800 WLC上でローカルで有効な証明書プロビジョニングを行うためのSCEPの設定

[3] Cisco Wireless ESTオンプレミス導入ガイド

[4] Secure AP onboarding- Enhanced Network Securityの概要

[5] ISEセキュア有線アクセス規範的導入ガイド

[6] LSCの設定ガイドのセクション

[7] 9800コントローラを使用したアクセスポイントの802.1Xサプリカントの設定

[8] Dot1xを使用したFlexconnect APスイッチポートの保護

[9] Cisco Catalyst 9800シリーズワイヤレスコントローラソフトウェアコンフィギュレーションガイド、Cisco IOS XE 17.18.x - 802.1x

[11] Cisco Catalyst Centerユーザガイド、リリース3.2.x:Cisco IOS XEデバイスのAPプロファイルの管理設定の設定

[12] IBNS 2.0およびインターフェイステンプレートを使用したデフォルトのスイッチポート設定

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。