Standardisierung der kabelgebundenen 802.1X-AP-Authentifizierung mit IBNS 2.0 und Schnittstellenvorlagen

Inhalt

Einleitung

In diesem Dokument wird die 802.1X-Konfiguration unter Verwendung von IBNS 2.0-Schnittstellenvorlagen beschrieben.

Problemaussage

Die Verwendung von IEEE 802.1X für die Port-Sicherheit ist eine gängige Best Practice. Neben der Verbesserung der Netzwerksicherheit wird auch die Switch-Bereitstellung durch eine

standardisierte Access-Port-Konfiguration im gesamten Netzwerk vereinfacht.

In diesem Leitfaden wird beschrieben, wie eine einzelne, standardisierte Switch-Port-Konfiguration sowohl für Endgeräte als auch für Cisco Access Points (APs) verwendet werden kann. Während anfänglich jeder Switch-Port als Standard-Access-Port fungiert und eine IEEE 802.1X-Authentifizierung durchführt, kann ein authentifizierter AP je nach Bereitstellungsszenario einen anderen Betriebsmodus erfordern.

Insbesondere APs im FlexConnect Local Switching-Modus müssen auf einem Trunk-Port betrieben werden, da der Client-Datenverkehr von mehreren SSIDs lokal überbrückt wird. Daher muss die Switch-Schnittstelle nach erfolgreicher Authentifizierung dynamisch von einem Zugriffsport zu einem Trunk-Port übergehen.

Access-Ports, die Infrastrukturgeräte anstelle einfacher Endgeräte verbinden, erfordern häufig Schnittstellenkonfigurationen, die sich vom Standardverhalten der Access-Ports unterscheiden.

Daher muss die Switch-Schnittstellenkonfiguration während des Authentifizierungsprozesses dynamisch geändert werden. Im Laufe der Jahre wurden hierzu verschiedene Ansätze verwendet, darunter Auto SmartPorts und Embedded Event Manager (EEM)-Applets. Heute wird die IBNS 2.0 []-Lösung in Kombination Schnittstellenvorlagen empfohlen, die eine skalierbare und konsistente Methode für die dynamische Änderung der Schnittstellenkonfiguration nach erfolgreicher Authentifizierung bietet.

Ansatz

Für eine funktionierende Einrichtung müssen verschiedene Komponenten richtig konfiguriert sein:

- Radius-Server (Identity Service Engine)
- Switch
- Access Point/Wireless LAN-Controller

Da es bereits Dokumentationen gibt (siehe Referenzen am Ende), konzentrieren wir uns auf ein bestimmtes Szenario in diesem Dokument und verweisen auf vorhandene Dokumentationen als unterstützendes Material.

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Wireless LAN Controller (WLC) und Lightweight APs (LAP)
- 802.1x auf Cisco Switches und der ISE
- Extensible Authentication Protocol (EAP)
- RADIUS (Remote Authentication Dial-In User Service)

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

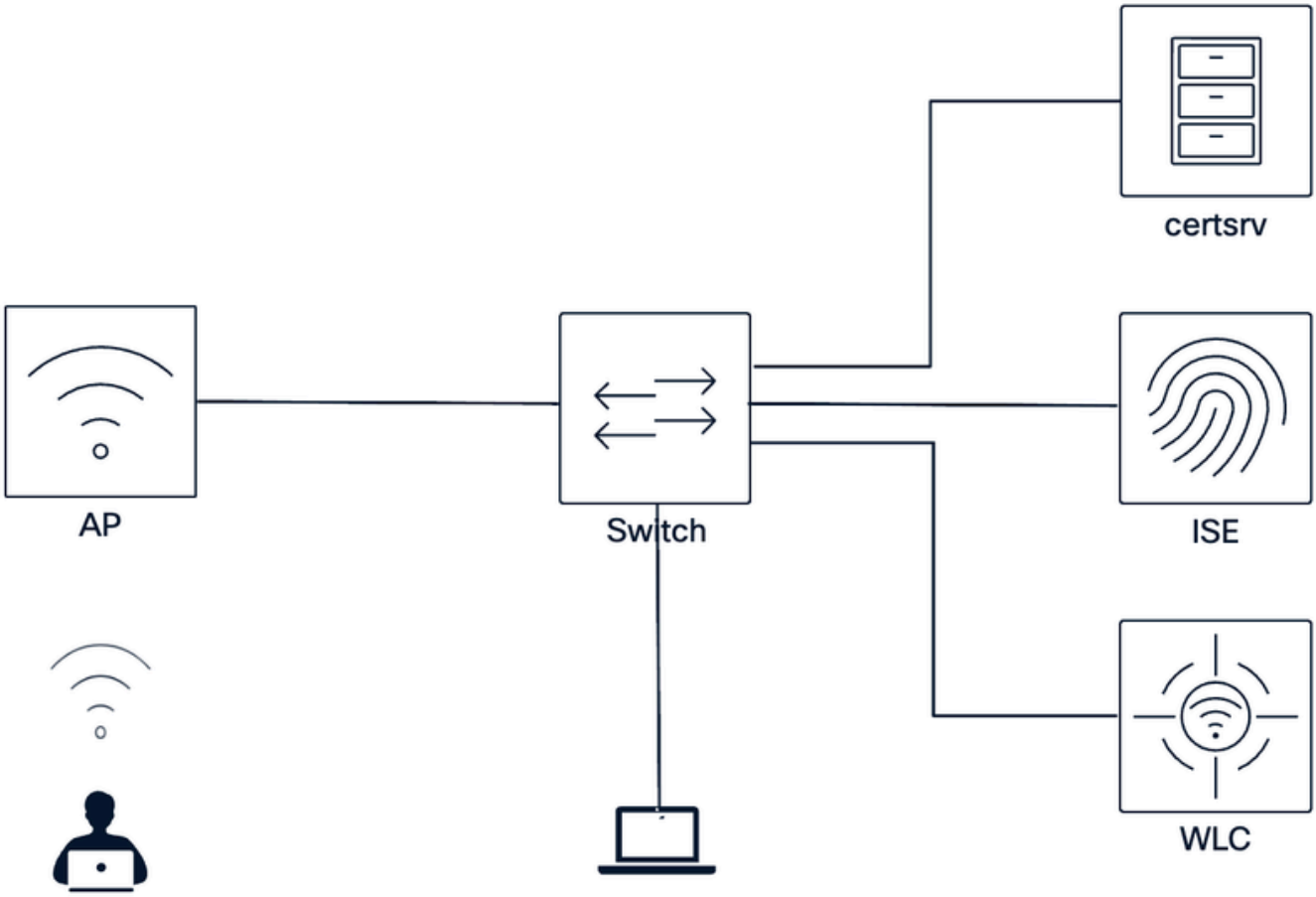
- Cisco C9350 - IOS XE 26.1.1a
- Cisco C980-40 WLC - IOS XE 26.1.1
- ISE Version 3.5 Patch 1
- AP CW917x, CW916x

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Die Konfiguration ist auch in netascode.cisco.com für Switching und ISE dokumentiert, um die Konfiguration einfach zu replizieren.

Konfiguration

Netzwerkdiagramm



Beispieleinrichtung

Zu diesem Zweck konzentrieren wir uns auf ein einzelnes Szenario und stellen Konfigurationsabschnitte sowie schrittweise Anleitungen zur Verfügung. Da es im Laufe der Zeit verschiedene Varianten gibt, weisen wir darauf hin und verweisen zu diesem Zweck auf bestehende Dokumentationen.

In diesem Leitfaden behandeltes Szenario:

- Verdrahteter AP Dot1X mit EAP-FAST-Authentifizierung
- Bereitstellung von Dot1X-Anmeldedaten über C9800 WLC
- AP im Flex Connect Local Switching-Modus

Bei diesem Design verwendet der Switch-Port zunächst eine gemeinsame 802.1X-Konfiguration im geschlossenen Modus mit MAB-Fallback. Beim ersten Onboarding verfügt der Access Point möglicherweise noch nicht über 802.1X-Anmeldedaten, sodass die ISE den Access Point über MAB autorisieren kann, wobei der eingeschränkte Zugriff ausreicht, um den WLC oder das

Catalyst Center zu erreichen. Nachdem die Anmeldeinformationen oder Zertifikate bereitgestellt wurden, führt der WAP eine kabelgebundene 802.1X-Authentifizierung durch. ISE gibt dann ein Autorisierungsergebnis zurück, das für die Schnittstellenvorlage AP_FLEX_TRUNK gilt, und konvertiert den Port in die erforderliche FlexConnect-Trunk-Konfiguration.

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		

Tabelle 1: Weitere Varianten und Optionen im Überblick

AP-Konfiguration

Um die kabelgebundene Dot1x-Authentifizierung in Kombination mit Ihrem Access Point zu verwenden, müssen Sie den Access Points je nach ausgewählter Authentifizierungsmethode zuerst Anmeldeinformationen und/oder Zertifikate bereitstellen.

Die Cisco Catalyst AP Dot1x-Komponente unterstützt im Allgemeinen entweder EAP-FAST, EAP-PEAP oder EAP-TLS. Darüber hinaus kann MAB auch eine Option sein, zumal die APs an erster Stelle die Anmeldeinformationen oder Zertifikate erfassen müssen, um eine EAP-Typauthentifizierung ausführen zu können.

- MAB:
  - Keine Konfiguration auf der AP-Seite erforderlich
  - Das Management von Hardware-MAC-Adressen erfordert Tools
  - Kann leicht getrübt werden
  - Ermöglicht gemeinsame Port-Konfiguration

- EAP-FAST:
  - Benutzername/Kennwort-basiert
  - Einfache Bereitstellung

    - Anonyme In-Band-PAC-Bereitstellung auf ISE erforderlich

- EAP-PEAP:
    - Benutzername/Kennwort-basiert
    - Erfordert Zertifikate für Servervalidierung
    - Die Zertifikaterneuerung muss entsprechend geplant werden.

- EAP-TLS:
    - Zertifikatbasiert
    - Die Zertifikaterneuerung muss entsprechend geplant werden.

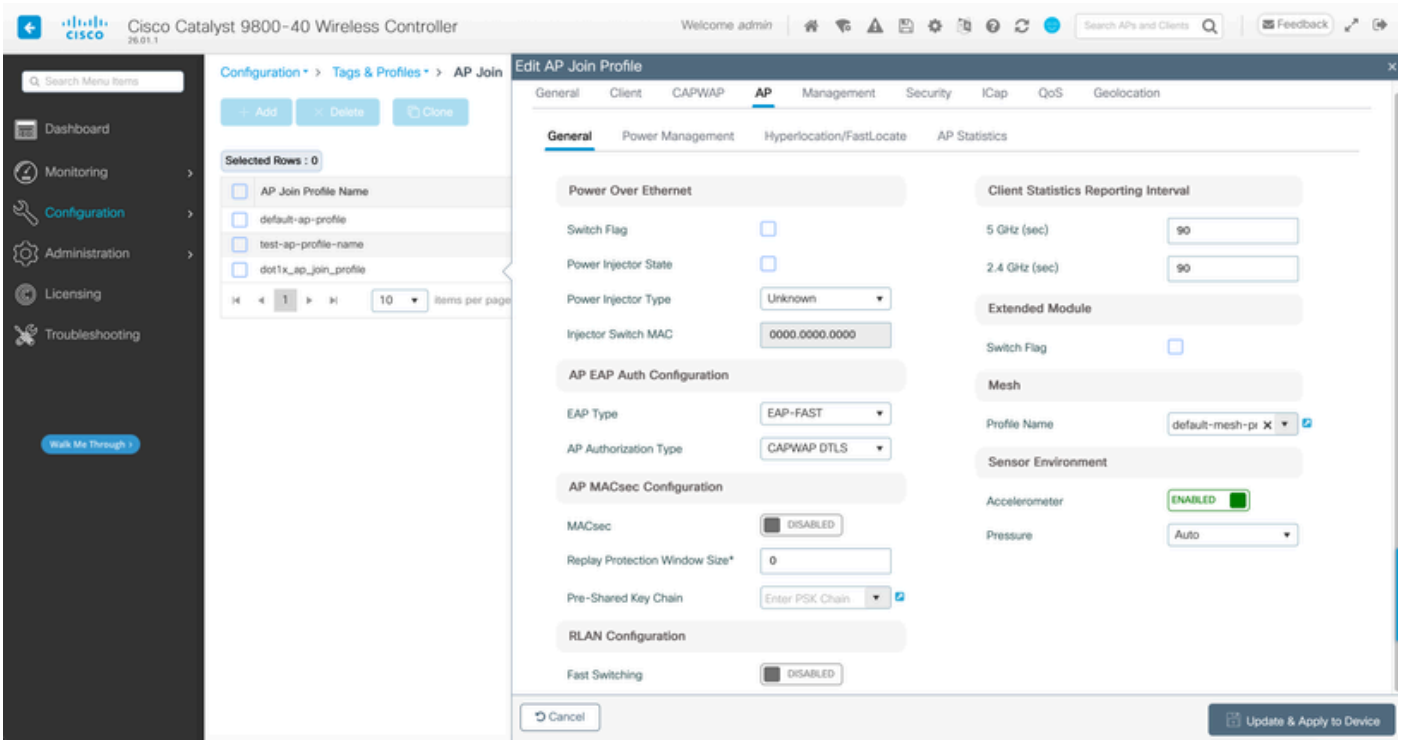
Für die Konfiguration der kabelgebundenen Dot1X-Komponente des Access Points gibt es zwei Ansätze, entweder über den Wireless LAN Controller oder über das Catalyst Center, die hier beschrieben werden. Bevor Sie auf diese Details eingehen, muss der Authentifizierungstyp zuvor ausgewählt werden.

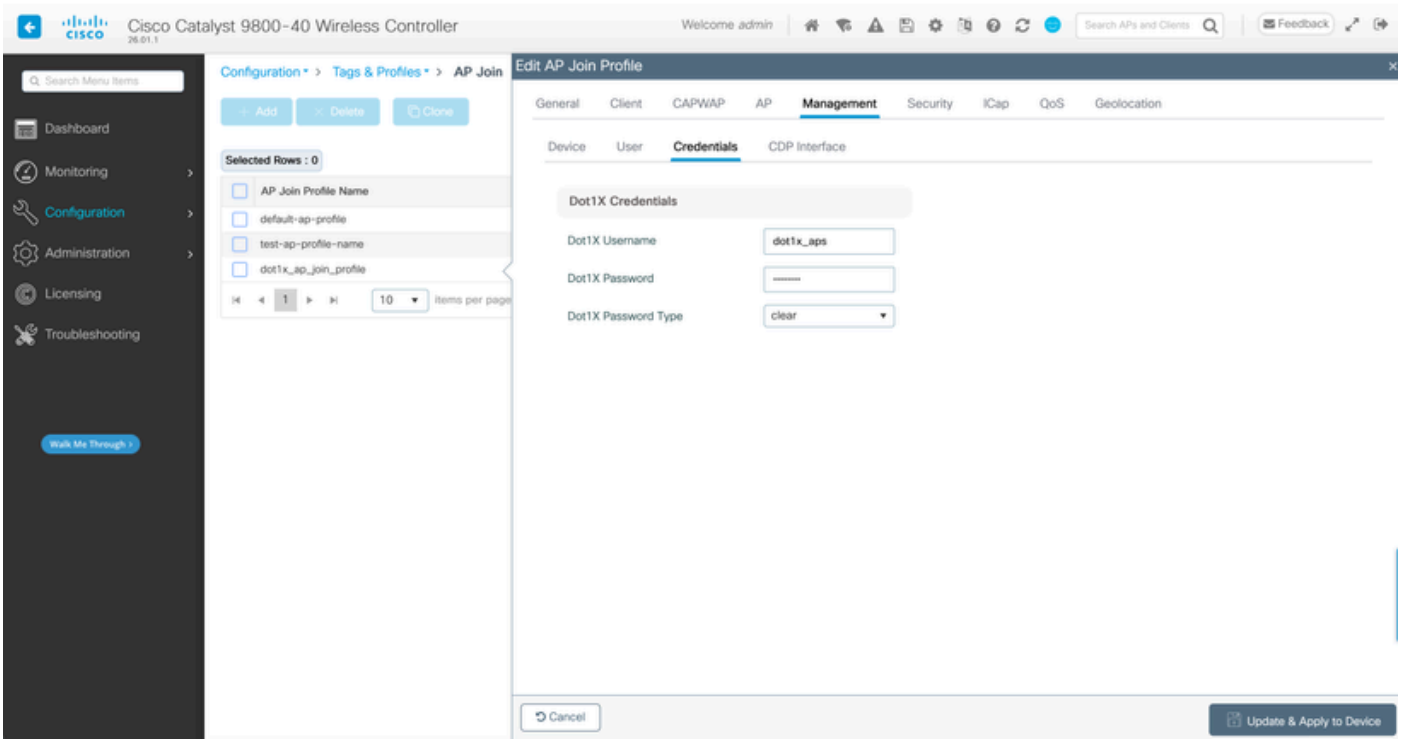
Einrichten des kabelgebundenen Dot1X über Cisco 9800 Wireless LAN-Controller

Wenn Sie sich für eine zertifikatbasierte Authentifizierung (EAP-PEAP oder EAP-TLS [1]) entschieden haben, müssen Sie als nächsten Schritt entscheiden, wie Sie entweder über SCEP [2] oder EST [3] lokal signifikante AP-Zertifikate (LSCs ausstellen

Wenn Sie EAP-FAST wie in unserem Szenario verwenden, ist es ausreichend, ein AP-Join-Profil zu generieren, in dem Sie den Dot1X-Benutzer und das Kennwort eingeben, dieses Join-Profil an ein Site-Tag binden und es den APs zuweisen.

GUI-Konfiguration





CLI-Konfiguration

```
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>
```

Einrichten von kabelgebundenen Dot1X über Catalyst Center Plug and Play

Damit PnP [4] funktioniert, muss Catalyst Center in die ISE integriert werden. Dies ist teilweise aufgrund der Zertifikate erforderlich, die erforderlich sind, um die Servervalidierung von der AP-Seite aus für die EAP-Authentifizierung mit der ISE durchführen zu können. Für das geräteseitige Zertifikat erhalten APs ein von der Catalyst Center CA ausgestelltes Zertifikat, das entweder standardmäßig integriert ist oder von einer SubCA/SCEP der jeweiligen CA konfiguriert wurde.

Der Einrichtungsprozess über PnP ermöglicht die Bereitstellung von Zertifikaten und/oder Anmeldedaten, bevor das Gerät den WLCs beitritt.

Switch-Konfiguration

Neben der Authentifizierung als Sicherheitsmechanismus dient sie auch zur Standardisierung von Switch-Port-Konfigurationen. Diese Teile beschreiben daher die hierfür erforderlichen Elemente. Dies ist eine Beispielkonfiguration, die überprüft und an Ihre Konfiguration angepasst werden muss. Im Allgemeinen ermöglicht diese Konfiguration Dot1x und Fallback-MAB mit ordnungsgemäßer Behandlung von Dead Radius-Szenarien, Neuauthentifizierung usw.

Globale Radius-Attribute:

```
!
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-Servergruppe:

```
!
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-Konfiguration:

```
!
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 Class-Map und Service-Template:

```
!
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-Servicerichtlinie:

```
!
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
!
```

Schnittstellenvorlagen:

```
!
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
!
```

Schnittstellenkonfiguration:

```
!
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
!
```

Global verpflichtend:

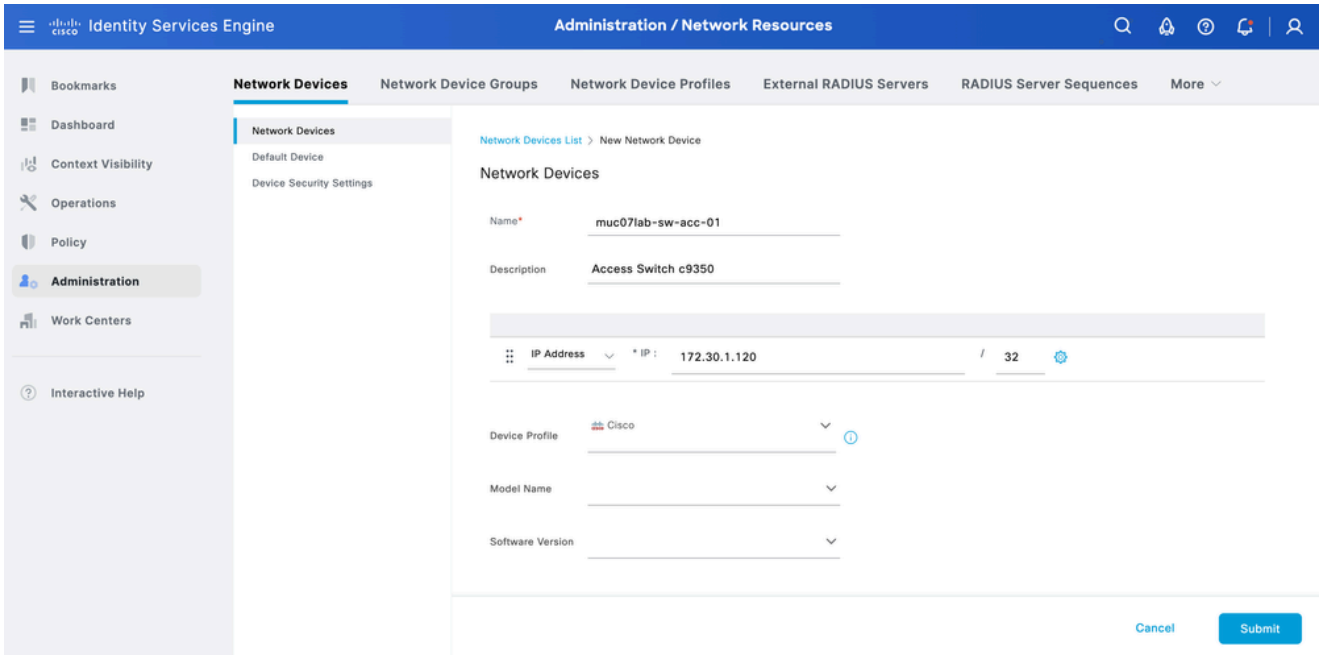
```
!
dot1x system-auth-control
!
access-session interface-template sticky timer 60
!
```

Anmerkung: Bei Verwendung eines CW9178 stellt der AP während der Authentifizierung zwei MAC-Adressen dar. Um zu verhindern, dass der Switch-Port in den Status "err-disabled" wechselt, muss dieser Port zunächst für Multi-Auth im Host-Modus konfiguriert werden. Nach erfolgreicher 802.1X-Authentifizierung wird empfohlen, die Port-Konfiguration dynamisch in Host-Modus Multi-Host zu ändern.

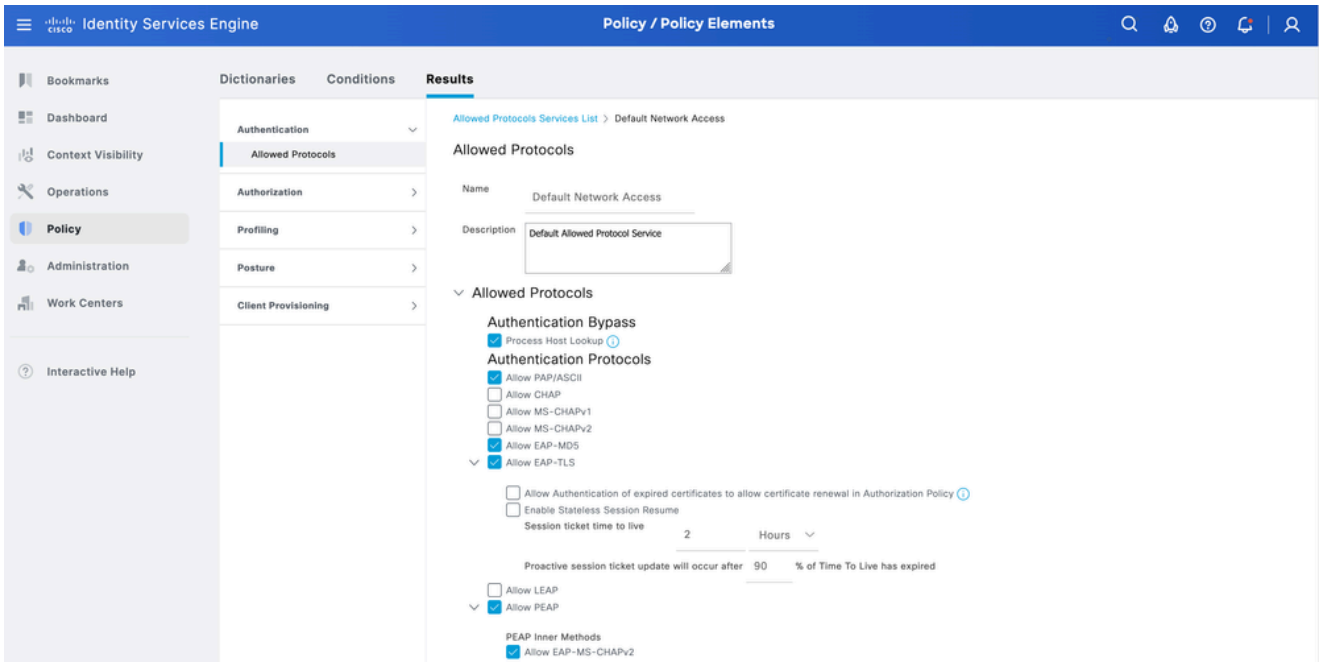
Identity Services Engine-Konfiguration

Schließlich muss auch der RADIUS-Server konfiguriert werden, um die Authentifizierung zu ermöglichen. Für kabelgebundenen Dot1x gibt es einen ausführlichen Leitfaden [5] sodass wir uns in diesem Fall nur auf die relevanten Teile konzentrieren.

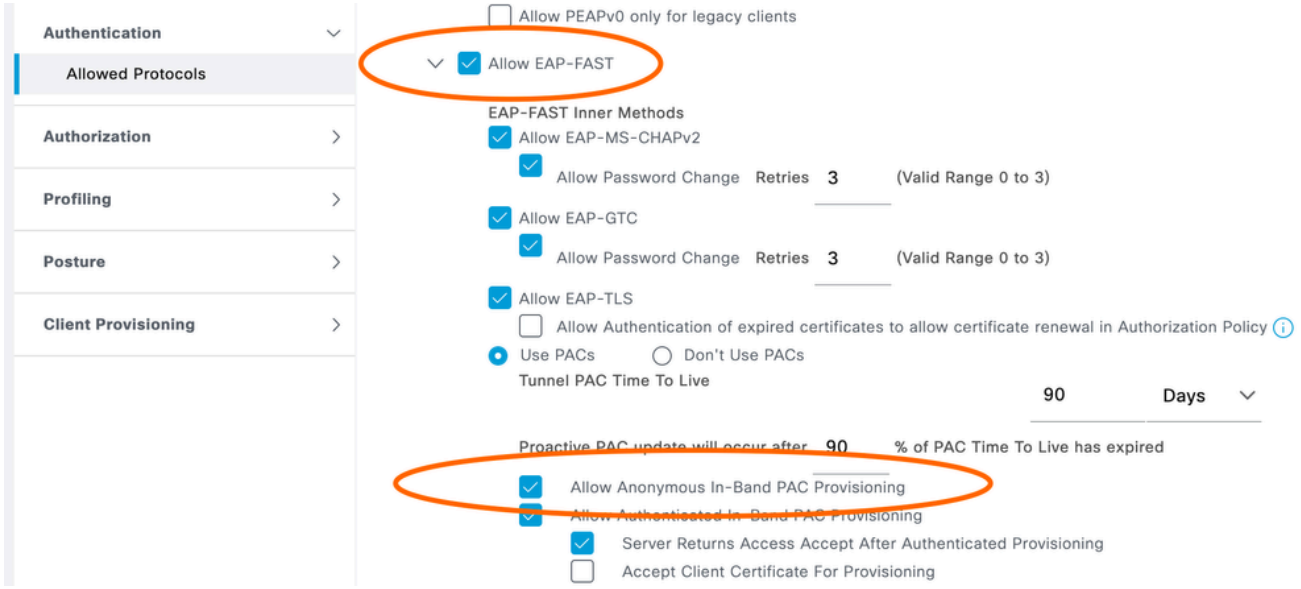
1. Fügen Sie den Switch als Netzwerkzugriffsgerät hinzu:
   > Administration > Network Ressources > Network Devices > Add



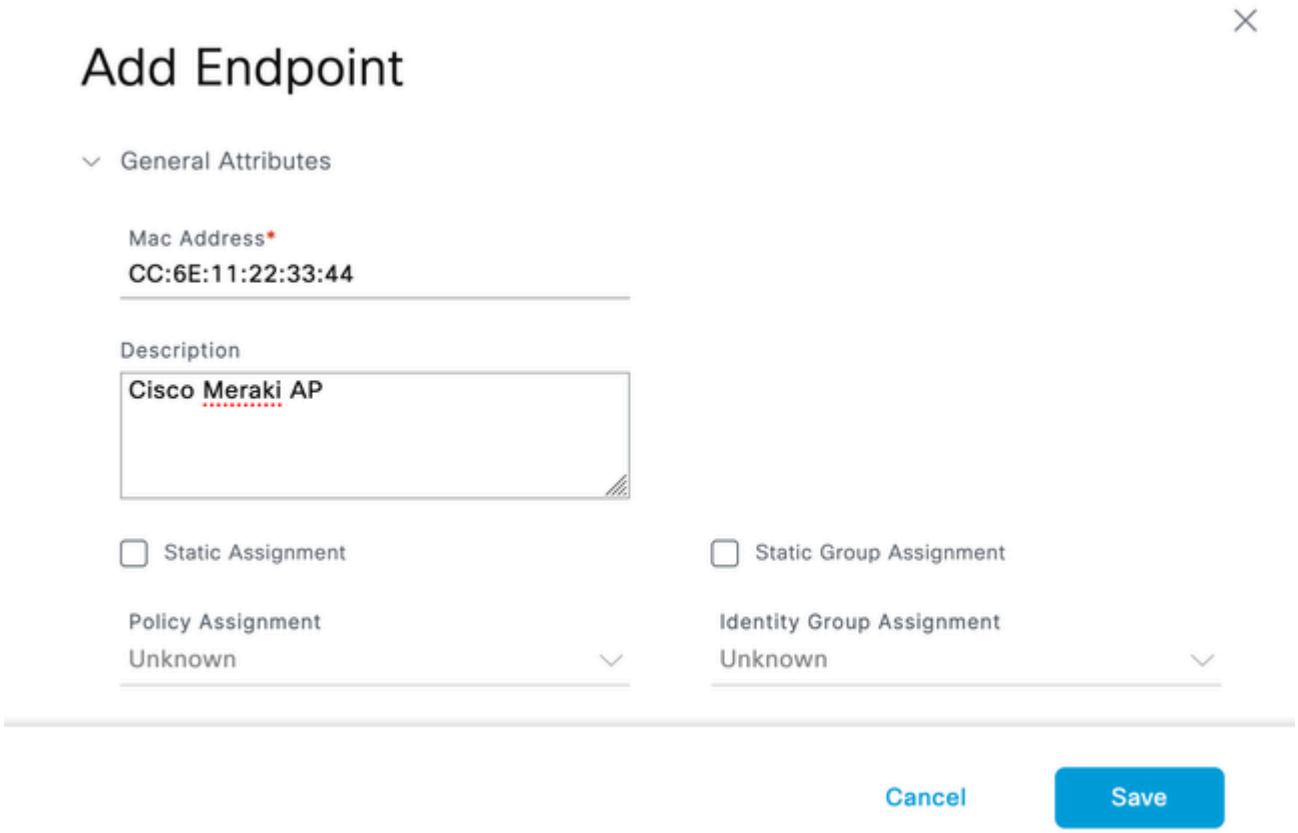
2. Aktivieren Sie das verwendete EAP-Protokoll:
   > Richtlinie > Richtlinienelemente > Ergebnisse > Authentifizierung > Zulässige Protokolle



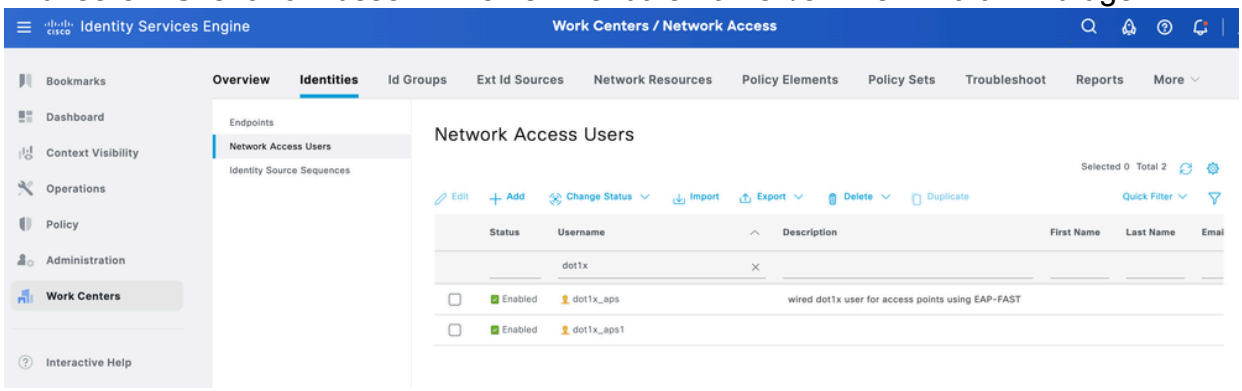
3. Beachten Sie bei unserem Szenario, bei dem wir EAP-FAST verwenden, dass die "Anonyme In-Band-PAC-Bereitstellung" aktiviert sein muss:



4. Identitäten hinzufügen
   > Work Centers > Network Access > Identities
   a. Für einen erfolgreichen Betrieb besteht der Prozess in der Regel aus zwei Schritten. Der WAP verfügt anfänglich über keine Anmeldeinformationen und kann daher nicht auf die EAP-Authentifizierung reagieren. Daher muss der Switch-Port den AP zuerst mithilfe von MAB authentifizieren. Dies kann auf einer generischen Autorisierungsrichtlinie, einer standortbasierten Richtlinie oder einer Geräteprofilerstellung basieren. Unabhängig von der verwendeten Richtlinie muss die ursprüngliche MAB-Authentifizierung erfolgreich sein, damit der AP seine Anmeldeinformationen vom WLC über CAPWAP oder vom Cisco Catalyst Center über Plug and Play (PnP) abrufen kann.

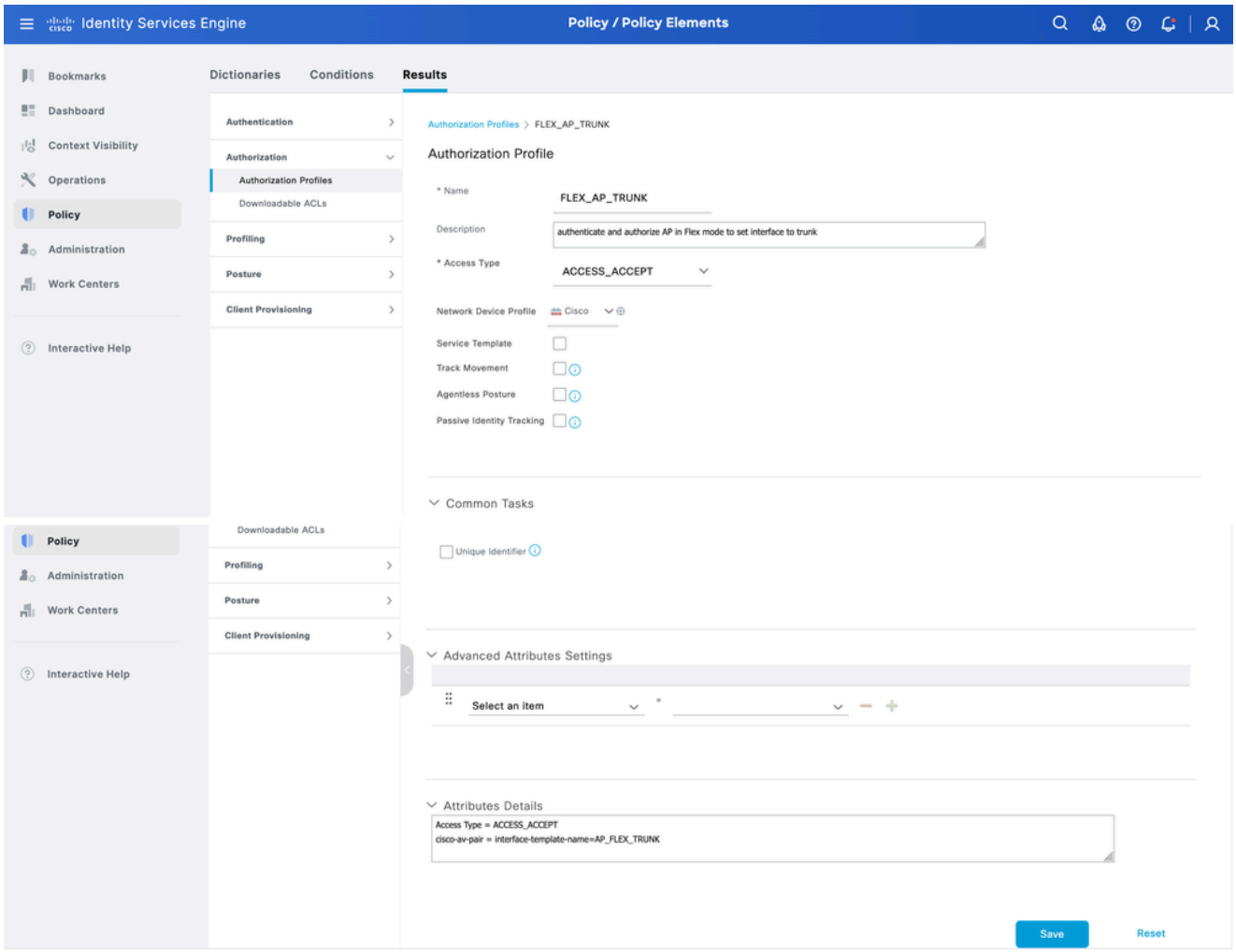


b. Nachdem der WAP die Anmeldeinformationen/das Zertifikat erfasst hat, antwortet die mit dem WAP verdrahtete Dot1X-Komponente auf EAPoL, und Dot1X ist die nachfolgende Authentifizierungsmethode, die den WAP für den vollständigen Zugriff aktiviert.
In unserem Szenario müssen wir einen Benutzernamen/ein Kennwort hinzufügen:

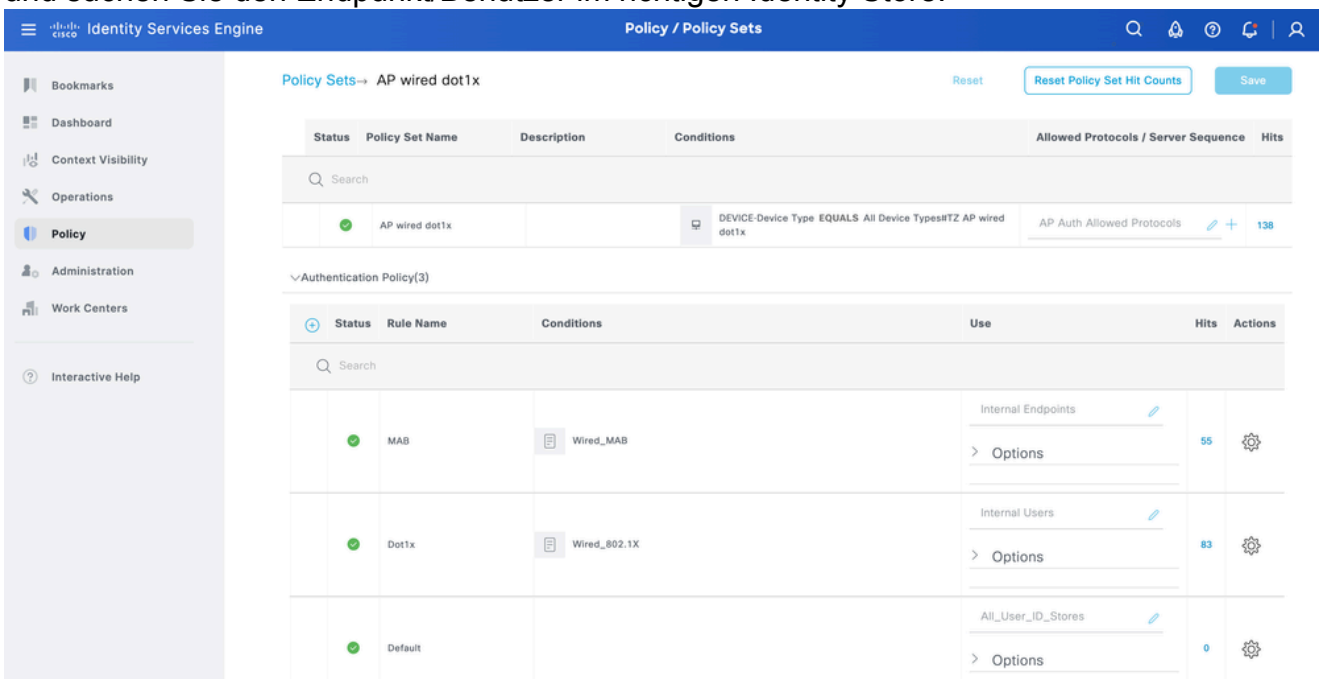


5. Erstellen des Autorisierungsprofils
Das Autorisierungsprofil antwortet mit dem erforderlichen AV-Paar. In unserem Fall muss die Schnittstellenvorlage konfiguriert werden, da der Switch-Port dynamisch geändert wird:
> Richtlinie > Richtlinienelemente > Ergebnisse > Autorisierung > Autorisierungsprofile

Name: FLEX_AP_TRUNK
Zugriffstyp: ACCESS_ACCEPT
Schnittstellenvorlage: AP_FLEX_TRUNK

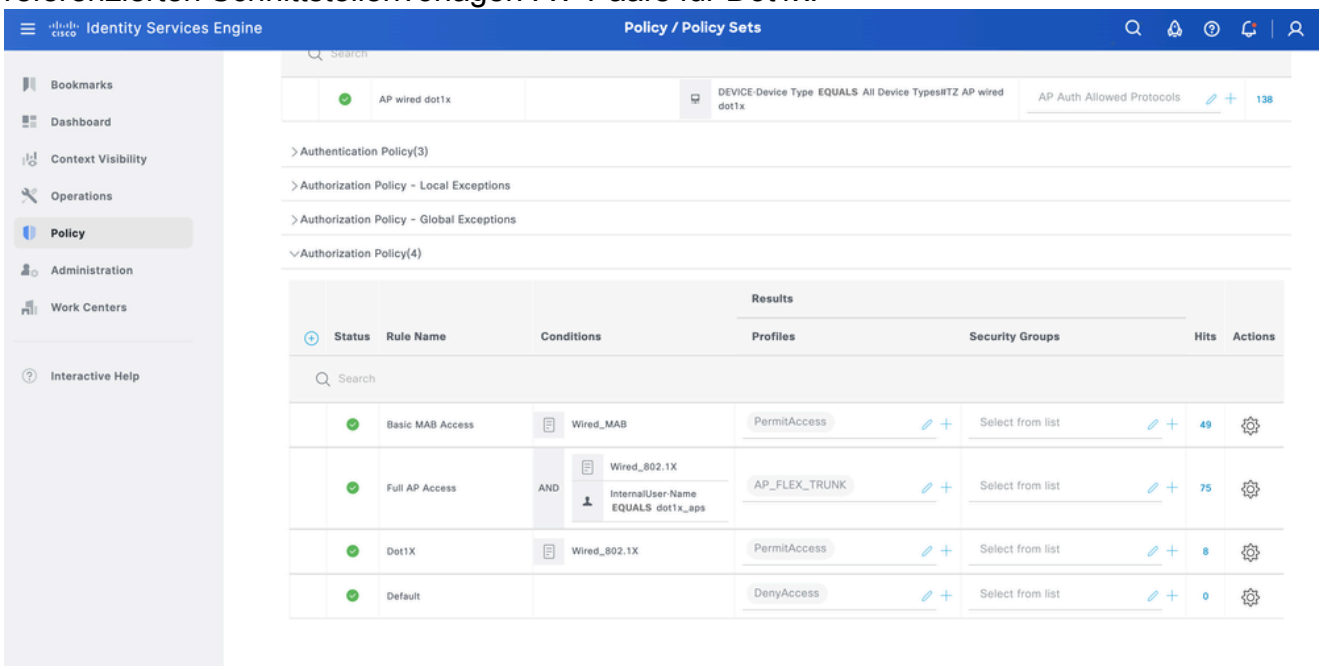


6. Autorisierungsrichtlinie erstellen
   Erstellen Sie eine Authentifizierungsrichtlinie, die MAB und kabelgebundenen Dot1X zulässt, und suchen Sie den Endpunkt/Benutzer im richtigen Identity Store.



Stellen Sie ein eingeschränktes Ergebnis für die Zugriffsautorisierung bereit, je nach Ihren

Anforderungen für MAB, und einen vollständigen AP-Zugriff, einschließlich des referenzierten Schnittstellenvorlagen-AV-Paars für Dot1x:



Überprüfung

Schließen Sie den Access Point nach der Konfiguration an den Switch an. Als Voraussetzung ist zu erwarten, dass die Standard-Netzwerkeinstellungen, in unserem Fall ein DHCP-Pool im Access VLAN mit Option 43 auf den WLC und CAPWAP-Kommunikation für den AP auf den WLC möglich ist.

AP-Befehle

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

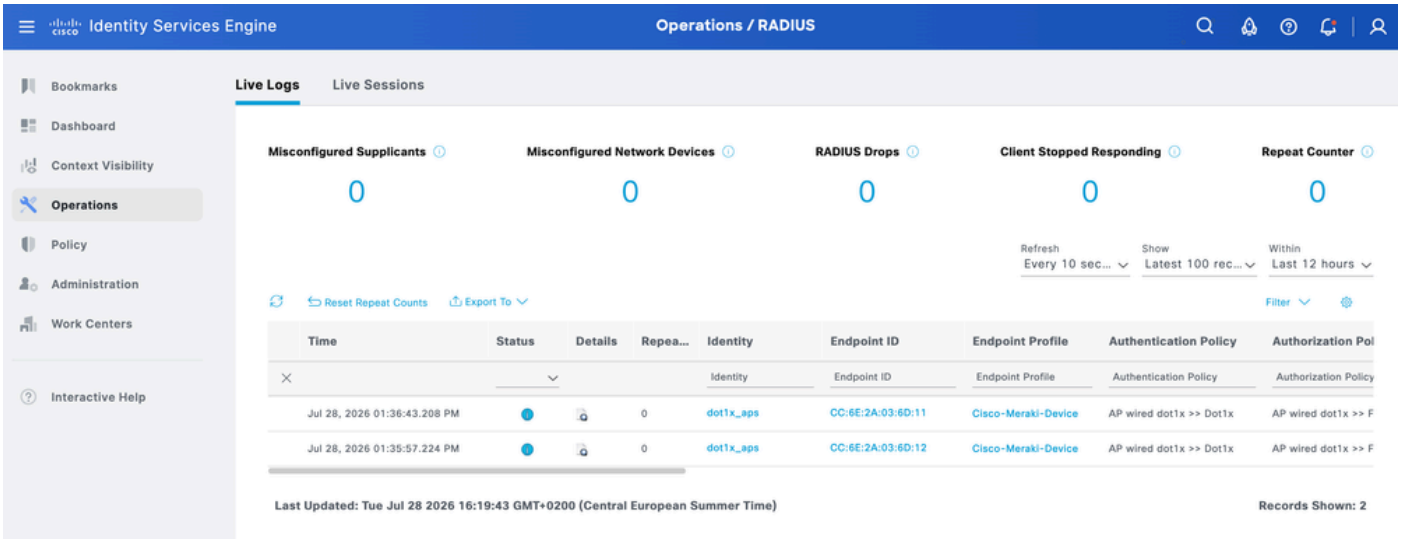
Switch-Befehle

```
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



Liste der Abkürzungen

Abkürzung	Erweiterung
AAA	authentisierung, ermächtigung und buchhaltung
AP	access point
AuthC	authentifizierung
AuthZ	Autorisierung
CA	Zertifizierungsstelle
CISP	Client Information Signaling Protocol
Punkt 1x	IEEE 802.1X
EAP	Erweiterbares Authentifizierungsprotokoll
EST	Registrierung über sichere Übertragung
SCHNELL	Flexible Authentifizierung durch sicheres Tunneling
IBNS	Identitätsbasierte Netzwerkservices
ISE	Identity Services Engine
MAB	MAC-Authentifizierungs-Umgehung

NAD	Netzwerkzugriffsgerät
PEAP	Protected Extensible Authentication Protocol
SCEP	Einfaches Zertifikatregistrierungsprotokoll
TLS	Transport Layer Security
WLC	Wireless LAN-Controller

Referenzen

[1] Konfigurieren von 802.1X auf APs für PEAP oder EAP-TLS mit LSC

[2] Konfigurieren von SCEP für die Bereitstellung von Zertifikaten mit lokaler Bedeutung auf dem 9800 WLC

[3] Cisco Wireless EST - Bereitstellungsleitfaden vor Ort

[4] Sicheres AP-Onboarding - Eine Einführung in die verbesserte Netzwerksicherheit

[5] ISE-Leitfaden zur Bereitstellung von sicherem kabelgebundenen Zugriff

[6] Konfigurationsanleitung für LSC

[7] 802.1X-Komponente für Access Points mit Controller 9800 konfigurieren

[8] Sicherung eines Flexconnect AP-Switch-Ports mit Dot1x

[9] Software-Konfigurationsleitfaden für Cisco Catalyst Wireless-Controller der Serie 9800, Cisco IOS XE 17.18.x - 802.1x

[11] Cisco Catalyst Center User Guide, Release 3.2.x - Configure management settings for an AP profile for Cisco IOS XE devices

[12] Verwendung von IBNS 2.0 und Schnittstellenvorlagen für eine Standard-Switch-Port-Konfiguration

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.