

Konfigurieren der 802.1X-Komponente für Access Points mit dem Controller 9800

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Hintergrundinformationen](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[Konfigurieren der LAP als 802.1x-Komponente](#)

[Wenn der Access Point bereits mit dem WLC verbunden ist:](#)

[Wenn der AP noch keinem WLC beigetreten ist:](#)

[Konfigurieren des Switches](#)

[Konfigurieren des ISE-Servers](#)

[Überprüfung](#)

[Authentifizierungstyp überprüfen](#)

[Überprüfen Sie 802.1x am Switch-Port.](#)

[Fehlerbehebung](#)

Einleitung

In diesem Dokument wird beschrieben, wie ein Cisco Access Point (AP) als 802.1x-Komponente konfiguriert wird, die auf einem Switch-Port gegenüber einem RADIUS-Server autorisiert werden kann.

Voraussetzungen

Anforderungen

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

- Wireless LAN Controller (WLC) und LAP (Lightweight Access Point)
- 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:

- WS-C3560CX, Cisco IOS® XE, 15.2(3r)E2
- C9800-CL-K9, Cisco IOS® XE, 17.6.1
- ISE 3.0
- LUFT-GAP3702
- AIR-AP 3802

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 verstehen.

Hintergrundinformationen

In dieser Konfiguration agiert der Access Point (AP) als 802.1x-Supplikant und wird vom Switch mithilfe der EAP-Methode EAP-FAST gegen die ISE authentifiziert.

Sobald der Port für die 802.1X-Authentifizierung konfiguriert ist, lässt der Switch keinen anderen Datenverkehr als 802.1X durch den Port, bis sich das mit dem Port verbundene Gerät erfolgreich authentifiziert hat.

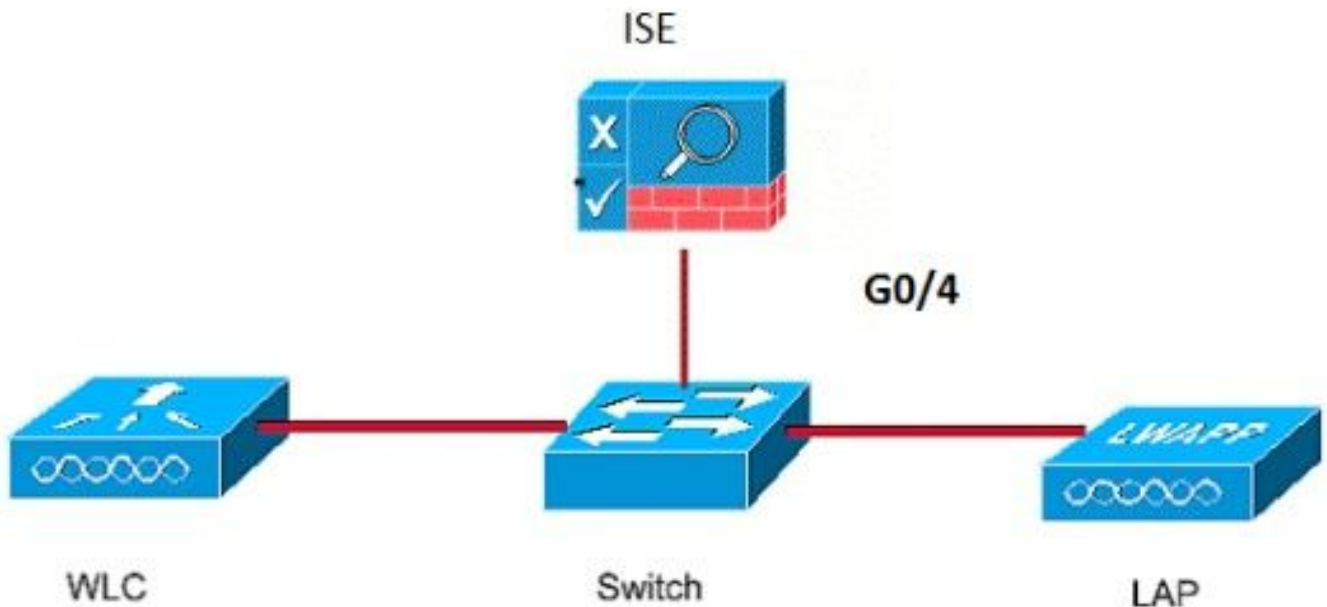
Ein AP kann authentifiziert werden, bevor er einem WLC beitrifft, oder nachdem er einem WLC beigetreten ist. In diesem Fall konfigurieren Sie 802.1X auf dem Switch, nachdem der LAP dem WLC beigetreten ist.

Konfigurieren

In diesem Abschnitt erfahren Sie, wie Sie die in diesem Dokument beschriebenen Funktionen konfigurieren können.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



Konfigurieren der LAP als 802.1x-Komponente

Wenn der Access Point bereits mit dem WLC verbunden ist:

Konfigurieren des 802.1x-Authentifizierungstyps und des LSC-AP-Authentifizierungstyps (Local Significant Certificate):

Schritt 1: Navigieren Sie zu Konfiguration > Tags & Profiles > AP Join > Klicken Sie auf der Seite AP Join Profile (AP-Join-Profil) auf Add (Hinzufügen), um ein neues Join-Profil hinzuzufügen, oder bearbeiten Sie ein AP-Join-Profil, wenn Sie auf dessen Namen klicken.

The screenshot shows the configuration page for AP Join Profiles on a Cisco Catalyst 9800-CL Wireless Controller. The page title is "Cisco Catalyst 9800-CL Wireless Controller 17.5.1". The navigation path is "Configuration > Tags & Profiles > AP Join". There are two buttons: "+ Add" and "X Delete". Below the buttons is a table with the following columns: "AP Join Profile Name" and "Description".

AP Join Profile Name	Description
<input type="checkbox"/> test	
<input type="checkbox"/> Dot1x	
<input type="checkbox"/> Split-Tunnel	
<input type="checkbox"/> default-ap-profile	default ap profile

At the bottom of the table, there is a pagination control showing "1" of 10 items per page.

Schritt 2: Navigieren Sie auf der Seite "AP Join Profile" (AP-Join-Profil) von AP > General (AP > Allgemein) zum Abschnitt "AP EAP Auth Configuration" (AP-EAP-Authentifizierungskonfiguration). Wählen Sie in der Dropdown-Liste EAP Type (EAP-Typ) den EAP-Typ EAP-FAST, EAP-TLS oder EAP-PEAP aus, um den dot1x-Authentifizierungstyp zu konfigurieren.

Edit AP Join Profile ✕

General Client CAPWAP **AP** Management Security ICap QoS

General Hyperlocation Packet Capture

Power Over Ethernet

Switch Flag

Power Injector State

Power Injector Type

Injector Switch MAC

Client Statistics Reporting Interval

5 GHz (sec)

2.4 GHz (sec)

AP EAP Auth Configuration

EAP Type

AP Authorization Type

Extended Module

Enable

Mesh

Profile Name [Clear](#)

Schritt 3: Wählen Sie in der Dropdown-Liste **AP Authorization Type (AP-Autorisierungstyp)** entweder CAPWAP DTLS + oder CAPWAP DTLS aus, und klicken Sie dann auf **Update & Apply to Device (Aktualisieren und auf Gerät anwenden)**.

Edit AP Join Profile ✕

General Client CAPWAP **AP** Management Security ICap QoS

General Hyperlocation Packet Capture

Power Over Ethernet

Switch Flag

Power Injector State

Power Injector Type

Injector Switch MAC

AP EAP Auth Configuration

EAP Type

AP Authorization Type

- CAPWAP DTLS
- CAPWAP DTLS +
- DOT1x port auth
- CAPWAP DTLS**
- Dot1x port auth

Client Statistics Reporting Interval

5 GHz (sec)

2.4 GHz (sec)

Extended Module

Enable

Mesh

Profile Name [Clear](#)

Konfigurieren Sie den 802.1x-Benutzernamen und das zugehörige Kennwort:

Schritt 1: Wählen Sie unter **Management > Credentials > Enter Dot1x username and password details** > Choose the appropriate 802.1x password type > Click **Update & Apply to Device** aus.

Edit AP Join Profile ✕

General Client CAPWAP AP **Management** Security ICap QoS

Device User **Credentials** CDP Interface

Dot1x Credentials

Dot1x Username	<input type="text" value="Dot1x"/>
Dot1x Password	<input type="password" value="••••••••"/>
Dot1x Password Type	<input type="text" value="clear"/>

Wenn der AP noch keinem WLC beigetreten ist:

Sie müssen in der LAP eine Konsole einrichten, um die Anmeldeinformationen festzulegen und die folgenden CLI-Befehle zu verwenden: (für Cheetah OS und Cisco IOS® APs)

CLI:

```
LAP# debug capwap console cli  
LAP# capwap ap dot1x username
```

So löschen Sie die dot1x-Anmeldedaten auf dem Access Point (falls erforderlich)

Bei Cisco IOS® APs muss der Access Point danach neu geladen werden:

CLI:

```
LAP# clear capwap ap dot1x
```

Bei Cisco COS APs muss der Access Point anschließend neu geladen werden:

CLI:

```
LAP# capwap ap dot1x disable
```

Konfigurieren des Switches

Aktivieren Sie dot1x auf dem Switch global, und fügen Sie den ISE-Server zum Switch hinzu.

CLI:

```
Enable
Configure terminal
aaa new-model
aaa authentication dot1x default group radius
aaa authorization network default group radius
dot1x system-auth-control
Radius-server host
```

Konfigurieren Sie den AP-Switchport.

CLI:

```
configure terminal
interface GigabitEthernet
switchport access vlan <>
switchport mode access
authentication order dot1x
authentication port-control auto
dot1x pae authenticator
spanning-tree portfast edge
end
```

Befindet sich der AP im **Flex Connect-Modus (lokales Switching)**, muss an der Switch-Schnittstelle eine zusätzliche Konfiguration vorgenommen werden, um mehrere MAC-Adressen am Port zuzulassen, da der Client-Datenverkehr auf AP-Ebene freigegeben wird:

```
authentication host-mode multi-host
```

Hinweis: Bedeutet, dass der Leser dies zur Kenntnis nehmen muss. Hinweise enthalten nützliche Vorschläge oder Verweise auf Material, das nicht in diesem Dokument behandelt wird.

Hinweis: Der Multi-Host-Modus authentifiziert die erste MAC-Adresse und lässt dann eine unbegrenzte Anzahl anderer MAC-Adressen zu. Aktivieren Sie den Host-Modus an den Switch-Ports, wenn der verbundene AP mit dem lokalen Switching-Modus konfiguriert wurde. Er lässt zu, dass der Datenverkehr des Clients den Switch-Port passiert. Wenn Sie einen sicheren Datenverkehrspfad benötigen, aktivieren Sie dot1x im WLAN, um die Client-Daten zu schützen.

Konfigurieren des ISE-Servers

Schritt 1: Fügen Sie den Switch als Netzwerkgerät zum ISE-Server hinzu. Navigieren Sie zu Administration > Network Resources > Network Devices > Klicken Sie auf Add > Geben Sie Geräte-Name und IP-Adresse ein, aktivieren Sie die RADIUS-Authentifizierungseinstellungen, geben Sie den gemeinsamen geheimen Wert an, oder belassen Sie den COA-Port (oder übernehmen Sie die Standardeinstellung) > Submit (Senden).

The screenshot shows the Cisco ISE Administration interface. The top navigation bar includes 'Administration - Network Resources'. The left sidebar has 'Network Devices' selected. The main content area is titled 'Network Devices' and shows a form for adding a new device. The form includes fields for Name (MySwitch), Description, IP Address (10.48.39.100 / 32), Device Profile (Cisco), Model Name, Software Version, Network Device Group, Location (All Locations), IPSEC (Is IPSEC Device), and Device Type (All Device Types). The 'RADIUS Authentication Settings' section is expanded and highlighted with a red box. It shows the following settings: Protocol (RADIUS), Shared Secret (masked), Use Second Shared Secret (unchecked), CoA Port (1700), RADIUS DTLS Settings (disabled), DTLS Required (unchecked), and Shared Secret (radius/dtls).

Schritt 2: Fügen Sie die AP-Anmeldeinformationen zur ISE hinzu. Navigieren Sie zu Administration > Identity Management > Identities > Users, und klicken Sie auf die Schaltfläche Add (Hinzufügen), um einen Benutzer hinzuzufügen. Sie müssen hier die Anmeldeinformationen eingeben, die Sie für Ihr AP-Join-Profil auf Ihrem WLC konfiguriert haben. Beachten Sie, dass der Benutzer hier in die Standardgruppe eingefügt wird. Dies kann jedoch an Ihre Anforderungen angepasst werden.

Schritt 3: Konfigurieren Sie auf der ISE die **Authentifizierungsrichtlinie** und die **Autorisierungsrichtlinie**. Gehen Sie zu **Policy > Policy Sets**, und wählen Sie den zu konfigurierenden Policy Set und den blauen Pfeil rechts aus. In diesem Fall wird der Standard-Richtliniensatz verwendet, der jedoch entsprechend der Anforderung angepasst werden kann.

Konfigurieren Sie dann die **Authentifizierungsrichtlinie** und die **Autorisierungsrichtlinie**. Die hier gezeigten Richtlinien sind die Standardrichtlinien, die auf dem ISE-Server erstellt wurden. Sie können jedoch an Ihre Anforderungen angepasst werden. In diesem Beispiel kann die Konfiguration folgendermaßen übersetzt werden: "Wenn kabelgebundenes 802.1X verwendet wird und der Benutzer auf dem ISE-Server bekannt ist, dann erlauben wir den Zugriff auf die Benutzer, für die die Authentifizierung erfolgreich war." Der WAP wird dann gegenüber dem ISE-Server autorisiert.

Authentication Policy (3)

Status	Rule Name	Conditions	Use	Hits	Actions
●	MAB	OR Wired_MAB Wireless_MAB	Internal Endpoints > Options	0	⚙️
●	Dot1X	OR Wired_802.1X Wireless_802.1X	All_User_ID_Stores > Options	6	⚙️
●	Default		All_User_ID_Stores > Options	0	⚙️

Authorization Policy (12)

Status	Rule Name	Conditions	Results	Profiles	Security Groups	Hits	Actions
●	Basic_Authenticated_Access	Network_Access_Authentication_Passed	PermitAccess x	Select from list	6	⚙️	
●	Default		DenyAccess x	Select from list	0	⚙️	

Schritt 4: Stellen Sie sicher, dass in den zulässigen Protokollen für den Standard-Netzwerkzugriff EAP-FAST zulässig ist. Navigieren Sie zu Policy > Policy Elements > Authentication > Results > Allowed Protocols > Default Network Access > Enable EAP-TLS > **Save** (Richtlinie > Richtlinienelemente > Authentifizierung > Ergebnisse > Zulässige Protokolle > Standard-Netzwerkzugriff > EAP-TLS zulassen > **Speichern**).

Cisco ISE Policy · Policy Elements

Results

Allowed Protocols Services List > Default Network Access

Allowed Protocols

Name: Default Network Access

Description: Default Allowed Protocol Service

Allowed Protocols

- Authentication Bypass
 - Process Host Lookup
- Authentication Protocols
 - Allow PAP/ASCII
 - Allow CHAP
 - Allow MS-CHAPv1
 - Allow MS-CHAPv2
 - Allow EAP-MD5
 - Allow EAP-TLS

Expand: Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy

Enable Stateless Session Resume

Session ticket time to live: 2 Hours

Proactive session ticket update will occur after: 90 % of Time To Live has expired

- Allow LEAP
- Allow PEAP
- Allow EAP-FAST
- Allow EAP-TTLS
- Allow TEAP

Überprüfung

Nutzen Sie diesen Abschnitt, um zu überprüfen, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Authentifizierungstyp überprüfen

Der Befehl show zeigt die Authentifizierungsinformationen eines AP-Profiles an:

CLI:

```
9800WLC#show ap profile name <profile-name> detailed
```

Beispiel:

```
9800WLC#show ap profile name default-ap-profile detailed
AP Profile Name      : Dot1x
...
Dot1x EAP Method     : [EAP-FAST/EAP-TLS/EAP-PEAP/Not-Configured]
LSC AP AUTH STATE   : [CAPWAP DTLS / DOT1x port auth / CAPWAP DTLS + DOT1x port auth]
```

Überprüfen Sie 802.1x am Switch-Port.

Der Befehl show zeigt den Authentifizierungsstatus von 802.1x auf dem Switch-Port an:

CLI:

```
Switch# show dot1x all
```

Ausgabebeispiel:

```
Sysauthcontrol      Enabled
Dot1x Protocol Version      3

Dot1x Info for GigabitEthernet0/8
-----
PAE                    = AUTHENTICATOR
QuietPeriod            = 60
ServerTimeout         = 0
SuppTimeout           = 30
ReAuthMax              = 2
MaxReq                 = 2
TxPeriod               = 30
```

Überprüfen Sie, ob der Port authentifiziert wurde.

CLI:

```
Switch#show dot1x interface <AP switch port number> details
```

Ausgabebeispiel:

```
Dot1x Info for GigabitEthernet0/8
-----
PAE                    = AUTHENTICATOR
QuietPeriod            = 60
ServerTimeout         = 0
```

```
SuppTimeout          = 30
ReAuthMax            = 2
MaxReq               = 2
TxPeriod             = 30
```

Dot1x Authenticator Client List

```
-----
EAP Method           = FAST
Supplicant           = f4db.e67e.dd16
Session ID           = 0A30279E00000BB7411A6BC4
  Auth SM State      = AUTHENTICATED
  Auth BEND SM State = IDLE
```

ED

Auth BEND SM State = IDLE

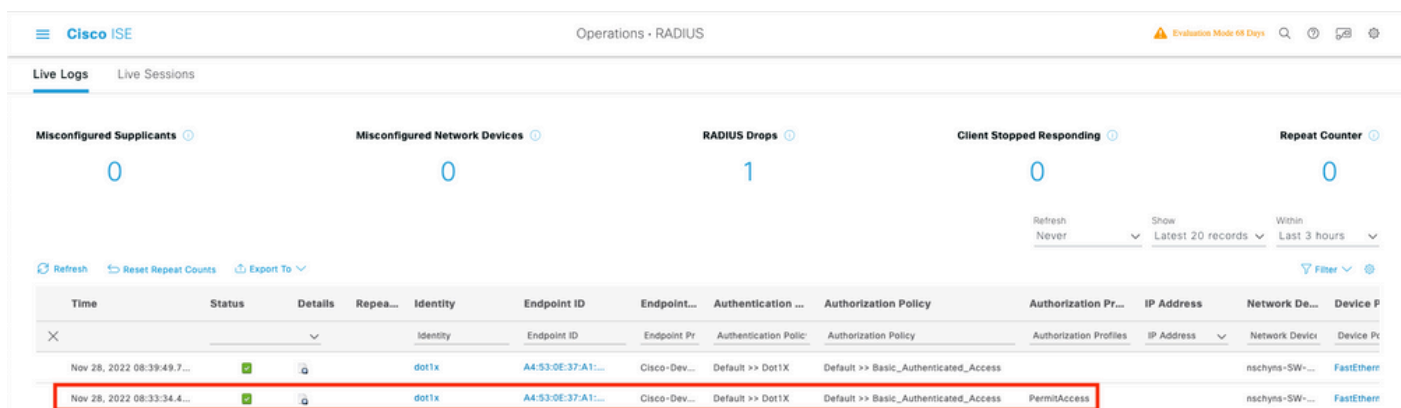
Aus CLI:

```
Switch#show authentication sessions
```

Ausgabebeispiel:

```
Interface  MAC Address  Method  Domain  Status  Fg  Session ID
Gi0/8     f4db.e67e.dd16  dot1x  DATA   Auth    0A30279E00000BB7411A6BC4
```

Wählen Sie in ISE Operations > Radius Livelogs (Operationen > Radius-Protokolle) aus, und bestätigen Sie, dass die Authentifizierung erfolgreich ist und das richtige Autorisierungsprofil per Push übermittelt wird.



The screenshot shows the Cisco ISE Operations - RADIUS interface. At the top, there are several summary cards: Misconfigured Supplicants (0), Misconfigured Network Devices (0), RADIUS Drops (1), Client Stopped Responding (0), and Repeat Counter (0). Below these cards is a table of live logs. The table has columns for Time, Status, Details, Repeats, Identity, Endpoint ID, Endpoint Name, Authentication Policy, Authorization Policy, Authorization Profiles, IP Address, Network Device, and Device Port. The second row of the table is highlighted with a red border, showing a successful authentication event on Nov 28, 2022 at 08:33:34.4. The 'Identity' column shows 'dot1x', 'Endpoint ID' shows 'A4-53-0E:37:A1...', 'Authentication Policy' shows 'Default >> Dot1X', 'Authorization Policy' shows 'Default >> Basic_Authenticated_Access', and 'Authorization Profiles' shows 'PermitAccess'.

Time	Status	Details	Repea...	Identity	Endpoint ID	Endpoint...	Authentication ...	Authorization Policy	Authorization Pr...	IP Address	Network De...	Device P
Nov 28, 2022 08:39:49.7...	✓	🔍		dot1x	A4-53-0E:37:A1...	Cisco-Dev...	Default >> Dot1X	Default >> Basic_Authenticated_Access			nschyns-SW...	FastEther
Nov 28, 2022 08:33:34.4...	✓	🔍		dot1x	A4-53-0E:37:A1...	Cisco-Dev...	Default >> Dot1X	Default >> Basic_Authenticated_Access	PermitAccess		nschyns-SW...	FastEther

Fehlerbehebung

Dieser Abschnitt enthält Informationen, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

1. Geben Sie den Befehl **ping** ein, um zu überprüfen, ob der ISE-Server vom Switch aus erreichbar ist.
2. Stellen Sie sicher, dass der Switch als AAA-Client auf dem ISE-Server konfiguriert ist.
3. Stellen Sie sicher, dass zwischen Switch und ISE-Server derselbe gemeinsame geheime Schlüssel verwendet wird.
4. Überprüfen Sie, ob EAP-FAST auf dem ISE-Server aktiviert ist.
5. Überprüfen Sie, ob die 802.1x-Anmeldeinformationen für die LAP konfiguriert sind und auf dem ISE-Server identisch sind.

Hinweis: Bei Benutzername und Passwort wird zwischen Groß- und Kleinschreibung unterschieden.

6. Wenn die Authentifizierung fehlschlägt, geben Sie die folgenden Befehle auf dem Switch ein:
debug dot1x und **debug authentication**.

Beachten Sie, dass Cisco IOS-basierte Access Points (802.11ac Wave 1) die TLS-Versionen 1.1 und 1.2 nicht unterstützen. Dies kann zu Problemen führen, wenn der ISE- oder RADIUS-Server so konfiguriert ist, dass nur TLS 1.2 in der 802.1X-Authentifizierung zugelassen wird.

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.