

# EAP-Authentifizierung mit RADIUS-Server

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Konfigurieren](#)

[Netzwerk-EAP oder offene Authentifizierung mit EAP](#)

[Authentifizierungsserver definieren](#)

[Definieren von Client-Authentifizierungsmethoden](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Fehlerbehebungsverfahren](#)

[Fehlerbehebung bei Befehlen](#)

[Zugehörige Informationen](#)

## Einführung

Dieses Dokument enthält eine Beispielkonfiguration eines Cisco IOS®-basierten Access Points für die EAP-Authentifizierung (Extensible Authentication Protocol) von Wireless-Benutzern für eine Datenbank, auf die von einem RADIUS-Server zugegriffen wird.

Aufgrund der passiven Rolle, die der Access Point im EAP übernimmt (überbrückt Wireless-Pakete vom Client in kabelgebundene Pakete, die für den Authentifizierungsserver bestimmt sind, und umgekehrt), wird diese Konfiguration mit praktisch allen EAP-Methoden verwendet. Zu diesen Methoden gehören (aber nicht beschränkt auf) LEAP, Protected EAP (PEAP)-MS-Challenge Handshake Authentication Protocol (CHAP) Version 2, PEAP-Generic Token Card (GTC), EAP-Flexible Authentication via Secure Tunneling (FAST), EAP-Transport Layer Security (TLS) und EAP-Tunneled TLS (TTLS). Sie müssen den Authentifizierungsserver für jede dieser EAP-Methoden entsprechend konfigurieren.

In diesem Dokument wird erläutert, wie der Access Point (AP) und der RADIUS-Server (Cisco Secure ACS) im Konfigurationsbeispiel dieses Dokuments konfiguriert werden.

## Voraussetzungen

### Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

- Sie kennen die Cisco IOS-GUI oder -CLI.
- Sie kennen die Konzepte der EAP-Authentifizierung.

## Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Cisco Aironet AP-Produkte, die Cisco IOS ausführen.
- Es wird angenommen, dass im Netzwerk nur ein virtuelles LAN (VLAN) vorhanden ist.
- Ein RADIUS-Authentifizierungsserver-Produkt, das erfolgreich in eine Benutzerdatenbank integriert werden kann. Dies sind die unterstützten Authentifizierungsserver für Cisco LEAP und EAP-FAST: Cisco Secure Access Control Server (ACS) Cisco Access Registrar (CAR) Funk Steel Beled RADIUS Link-Merge Dies sind die unterstützten Authentifizierungsserver für Microsoft PEAP-MS-CHAP Version 2 und PEAP-GTC: Microsoft Internet Authentication Service (IAS) Cisco Secure ACS Funk Steel Beled RADIUS Link-Merge Jeder zusätzliche Authentifizierungsserver, den Microsoft autorisieren kann. **Hinweis:** GTC- oder Einmalkennwörter erfordern zusätzliche Dienste, die zusätzliche Software auf Client- und Serverseite sowie Hardware- oder Software-Token-Generatoren erfordern. Weitere Informationen darüber, welche Authentifizierungsserver mit ihren Produkten für EAP-TLS, EAP-TTLS und andere EAP-Methoden unterstützt werden, erhalten Sie vom Hersteller des Client-Suppliants.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

## Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den [Cisco Technical Tips Conventions](#) (Technische Tipps zu Konventionen von Cisco).

## Konfigurieren

Diese Konfiguration beschreibt, wie die EAP-Authentifizierung auf einem IOS-basierten Access Point konfiguriert wird. Im Beispiel in diesem Dokument wird LEAP als Methode der EAP-Authentifizierung mit RADIUS-Server verwendet.

**Hinweis:** Verwenden Sie das [Command Lookup Tool](#) (nur [registrierte](#) Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Wie bei den meisten kennwortbasierten Authentifizierungsalgorithmen ist Cisco LEAP anfällig für Wörterbuchangriffe. Dies ist kein neuer Angriff oder keine neue Schwachstelle von Cisco LEAP. Die Erstellung einer strikten Kennwortrichtlinie ist die effektivste Methode, um Wörterbuchangriffe zu verhindern. Dies umfasst die Verwendung sicherer Passwörter und den regelmäßigen Ablauf von Passwörtern. Unter [Dictionary Attack auf Cisco LEAP](#) finden Sie weitere Informationen zu Wörterbuchangriffen und deren Verhinderung.

In diesem Dokument wird diese Konfiguration sowohl für die GUI als auch für die CLI verwendet:

- Die IP-Adresse des Access Points lautet 10.0.0.106.
- Die IP-Adresse des RADIUS-Servers (ACS) lautet 10.0.0.3.

## Netzwerk-EAP oder offene Authentifizierung mit EAP

Bei jeder EAP/802.1x-basierten Authentifizierungsmethode können Sie die Unterschiede zwischen Netzwerk-EAP und offener Authentifizierung mit EAP infrage stellen. Diese Elemente beziehen sich auf die Werte im Feld Authentifizierungsalgorithmus in den Headern der Management- und Zuordnungspakete. Die meisten Hersteller von Wireless-Clients setzen dieses Feld auf den Wert 0 (Open Authentication) und signalisieren dann den Wunsch, die EAP-Authentifizierung später im Zuordnungsprozess durchzuführen. Cisco legt den Wert anders fest, als bei Beginn der Verknüpfung mit dem Netzwerk-EAP-Flag.

Wenn Ihr Netzwerk über Clients verfügt, die:

- Cisco Clients - Verwenden Sie Network-EAP.
- Drittanbieter-Clients (einschließlich CCX-kompatibler Produkte) - Verwenden Sie Open mit EAP.
- Kombination von Cisco und Drittanbieter-Clients - Wählen Sie Network-EAP und Open mit EAP.

## Authentifizierungsserver definieren

Der erste Schritt in der EAP-Konfiguration besteht darin, den Authentifizierungsserver zu definieren und eine Beziehung mit ihm herzustellen.

1. Gehen Sie auf der Registerkarte "Access Point Server Manager" (unter der Menüoption **Security > Server Manager**) wie folgt vor: Geben Sie die IP-Adresse des Authentifizierungsservers im Feld Server ein. Geben Sie den Shared Secret und die Ports an. Klicken Sie auf **Apply**, um die Definition zu erstellen und die Dropdown-Listen zu füllen. Legen Sie unter "Default Server Priorities" (Standardserverprioritäten) das Feld "EAP Authentication Type Priority 1" (EAP-Authentifizierungstyp Priorität 1) auf die Server-IP-Adresse fest. Klicken Sie auf **Übernehmen**.

The screenshot shows the Cisco 1200 Access Point configuration interface. The top header displays 'Cisco 1200 Access Point' and 'SERVER MANAGER' tabs. The main content area is divided into several sections:

- Backup RADIUS Server:** Contains fields for 'Backup RADIUS Server' (Hostname or IP Address) and 'Shared Secret'. Buttons for 'Apply', 'Delete', and 'Cancel' are present.
- Corporate Servers:** Includes a 'Current Server List' with a dropdown menu set to 'RADIUS'. A list shows '< NEW >' and '10.0.0.3'. A 'Delete' button is below the list. To the right, fields for 'Server' (10.0.0.3), 'Shared Secret', 'Authentication Port (optional): 1645', and 'Accounting Port (optional): 1646' are visible. Buttons for 'Apply' and 'Cancel' are at the bottom right.
- Default Server Priorities:** Contains six sections for setting priorities:
  - EAP Authentication:** Priority 1 is set to 10.0.0.3.
  - MAC Authentication:** All priorities are set to < NONE >.
  - Accounting:** All priorities are set to < NONE >.
  - Admin Authentication (RADIUS):** All priorities are set to < NONE >.
  - Admin Authentication (TACACS+):** Priority 1 is set to 10.0.0.3.
  - Proxy Mobile IP Authentication:** All priorities are set to < NONE >.

Red circles highlight the IP address '10.0.0.3', the authentication port '1645', and the accounting port '1646'.

Close Window Copyright (c) 1992-2004 by Cisco Systems, Inc.

Sie können diese Befehle auch über die CLI ausführen:

```
AP#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
AP(config)#aaa group server radius rad_eap
```

```
AP(config-sg-radius)#server 10.0.0.3 auth-port 1645 acct-port 1646
```

```

AP(config-sg-radius)#exit

AP(config)#aaa new-model

AP(config)#aaa authentication login eap_methods group rad_eap

AP(config)#radius-server host 10.0.0.3 auth-port 1645
acct-port 1646 key labap1200ip102

AP(config)#end

AP#write memory

```

2. Der Access Point muss im Authentifizierungsserver als AAA-Client konfiguriert werden. In Cisco Secure ACS erfolgt dies beispielsweise auf der Seite [Network Configuration \(Netzwerkkonfiguration\)](#), auf der der Name des Access Points, die IP-Adresse, der gemeinsam genutzte geheime Schlüssel und die Authentifizierungsmethode (RADIUS Cisco Aironet oder RADIUS Cisco IOS/PIX) definiert sind. Informationen zu anderen Nicht-ACS-Authentifizierungsservern finden Sie in der Dokumentation des Herstellers.

**Network Configuration**

AAA Client Hostname: AP

AAA Client IP Address: 10.0.0.106

Key: sharedsecret

Authenticate Using: RADIUS (Cisco IOS/PIX)

Single Connect TACACS+ AAA Client (Record stop in accounting on failure).

Log Update/Watchdog Packets from this AAA Client

Log RADIUS Tunneling Packets from this AAA Client

Replace RADIUS Port info with Username from this AAA Client

Buttons: Submit, Submit + Restart, Cancel

**Help**

- [AAA Client Hostname](#)
- [AAA Client IP Address](#)
- [Key](#)
- [Network Device Group](#)
- [Authenticate Using](#)
- [Single Connect TACACS+ AAA Client](#)
- [Log Update/Watchdog Packets from this AAA Client](#)
- [Log RADIUS Tunneling Packets from this AAA Client](#)
- [Replace RADIUS Port info with Username from this AAA Client](#)

**AAA Client Hostname**

The AAA Client Hostname is the name assigned to the AAA client.

[\[Back to Top\]](#)

Stellen Sie sicher, dass der Authentifizierungsserver so konfiguriert ist, dass er die gewünschte EAP-Authentifizierungsmethode ausführt. Bei einem Cisco Secure ACS, der LEAP ausführt, konfigurieren Sie beispielsweise die LEAP-Authentifizierung auf der Seite [System Configuration - Global Authentication Setup \(Systemkonfiguration - Globale Authentifizierung\)](#). Klicken Sie auf **Systemkonfiguration** und anschließend auf **Globales Authentifizierungs-Setup**. Weitere Nicht-ACS-Authentifizierungsserver oder andere EAP-Methoden finden Sie in der Dokumentation des Herstellers.

**CISCO SYSTEMS** **System Configuration**

Select	Help
<ul style="list-style-type: none"> <li> User Setup</li> <li> Group Setup</li> <li> Shared Profile Components</li> <li> Network Configuration</li> <li> System Configuration</li> <li> Interface Configuration</li> <li> Administration Control</li> <li> External User Databases</li> <li> Reports and Activity</li> <li> Online Documentation</li> </ul>	<ul style="list-style-type: none"> <li> <a href="#">Service Control</a></li> <li> <a href="#">Logging</a></li> <li> <a href="#">Date Format Control</a></li> <li> <a href="#">Local Password Management</a></li> <li> <a href="#">CiscoSecure Database Replication</a></li> <li> <a href="#">ACS Backup</a></li> <li> <a href="#">ACS Restore</a></li> <li> <a href="#">ACS Service Management</a></li> <li> <a href="#">IP Pools Server</a></li> <li> <a href="#">IP Pools Address Recovery</a></li> <li> <a href="#">ACS Certificate Setup</a></li> <li> <a href="#">Global Authentication Setup</a></li> </ul> <p style="text-align: center;"> Back to Help</p>
	<ul style="list-style-type: none"> <li>• <a href="#">Service Control</a></li> <li>• <a href="#">Logging</a></li> <li>• <a href="#">Date Format Control</a></li> <li>• <a href="#">Local Password Management</a></li> <li>• <a href="#">CiscoSecure Database Replication</a></li> <li>• <a href="#">RDBMS Synchronization</a></li> <li>• <a href="#">ACS Backup</a></li> <li>• <a href="#">ACS Restore</a></li> <li>• <a href="#">ACS Service Management</a></li> <li>• <a href="#">IP Pools Address Recovery</a></li> <li>• <a href="#">IP Pools Server</a></li> <li>• <a href="#">VoIP Accounting Configuration</a></li> <li>• <a href="#">ACS Certificate Setup</a></li> <li>• <a href="#">Global Authentication Configuration</a></li> </ul> <hr/> <p><b>Service Control</b></p> <p>Select to open the page from which you can stop or restart Cisco Secure ACS services.</p> <p><a href="#">[Back to Top]</a></p>

Dieses Bild zeigt Cisco Secure ACS, konfiguriert für PEAP, EAP-FAST, EAP-TLS, LEAP und EAP-MD5.

**CISCO SYSTEMS** **System Configuration**

**Edit** **Help**

**Global Authentication Setup**

**EAP Configuration** ?

**PEAP**

Allow EAP-MSCHAPv2

Allow EAP-GTC

Cisco client initial message:

PEAP session timeout (minutes):

Enable Fast Reconnect:

---

**EAP-FAST**

Allow EAP-FAST

Active master key TTL:

Retired master key TTL:

PAC TTL:

Client initial message:

Authority ID Info:

Allow automatic PAC provisioning:

EAP-FAST master server:

Actual EAP-FAST server status: **Master**

---

**EAP-TLS**

Allow EAP-TLS

Select one or more of the following options:

Certificate SAN comparison

Certificate CN comparison

Certificate Binary comparison

EAP-TLS session timeout (minutes):

---

**LEAP**

Allow LEAP (For Aironet only)

---

**EAP-MD5**

Allow EAP-MD5

AP EAP request timeout (seconds):

---

**MS-CHAP Configuration** ?

Allow MS-CHAP Version 1 Authentication

Allow MS-CHAP Version 2 Authentication

[? Back to Help](#)

**Help**

- [PEAP](#)
- [EAP-FAST](#)
- [EAP-TLS](#)
- [LEAP](#)
- [EAP-MD5](#)
- [AP EAP request timeout](#)
- [MS-CHAP Configuration](#)

This page specifies settings for various authentication protocols.

[\[Back to Top\]](#)

**PEAP**

*Note: PEAP is a certificate-based authentication protocol. PEAP authentication can occur only after you have*

## [Definieren von Client-Authentifizierungsmethoden](#)

Sobald der Access Point weiß, wohin er Client-Authentifizierungsanforderungen senden soll, konfigurieren Sie ihn so, dass er diese Methoden akzeptiert.

**Hinweis:** Diese Anweisungen gelten für eine WEP-basierte Installation. Informationen zu WPA (das statt WEP Chiffren verwendet) finden Sie unter [Übersicht über die WPA-Konfiguration](#).

1. Gehen Sie auf der Registerkarte "Access Point Encryption Manager" (**Sicherheit > Verschlüsselungs-Manager**) wie folgt vor: Geben Sie an, dass Sie die **WEP-Verschlüsselung** verwenden möchten. Angeben, dass WEP **obligatorisch** ist. Stellen Sie sicher, dass die Schlüssellänge auf **128 Bit** eingestellt ist. Klicken Sie auf **Übernehmen**.

The screenshot shows the configuration interface for a Cisco 1200 Access Point. The main title is "Cisco 1200 Access Point". The interface is divided into several sections:

- Navigation Menu:** Includes HOME, EXPRESS SET-UP, EXPRESS SECURITY, NETWORK MAP, ASSOCIATION, NETWORK INTERFACES, SECURITY (with sub-items like Admin Access, Encryption Manager, SSID Manager, Server Manager, Local RADIUS Server, Advanced Security), SERVICES, WIRELESS SERVICES, SYSTEM SOFTWARE, and EVENT LOG.
- Radio Selection:** RADIO0-802.11B and RADIO1-802.11A tabs are visible.
- Security: Encryption Manager - Radio0-802.11B:**
  - Encryption Modes:** "None" is unselected. "WEP Encryption" is selected and circled in red, with a dropdown menu set to "Mandatory". "Cipher" is unselected.
  - Cisco Compliant TKIP Features:** "Enable MIC" and "Enable Per Packet Keying" are unchecked.
  - Key Size:** A dropdown menu is set to "WEP 128 bit".
- Encryption Keys:** A table with four rows for Encryption Key 1 through 4. Each row has a radio button (Key 2 is selected), a text input field for the key, and a dropdown menu for the key size (all set to "128 bit").
- Global Properties:**
  - Broadcast Key Rotation Interval:** "Disable Rotation" is selected. "Enable Rotation with Interval" is unselected, with a text input field containing "DISABLED" and "(10-10000000 sec)".
  - WPA Group Key Update:** "Enable Group Key Update On Membership Termination" and "Enable Group Key Update On Member's Capability Change" are both unchecked.
- Buttons:** "Apply-Radio0", "Apply-All", and "Cancel" are located at the bottom right.

Close Window Copyright (c) 1992-2004 by Cisco Systems, Inc.

Sie können diese Befehle auch über die CLI ausführen:

```
AP#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
AP(config)#interface dot11radio 0
```

```
AP(config-if)#encryption mode wep mandatory
```

```
AP(config-if)#end
```

```
AP#write memory
```

2. Führen Sie die folgenden Schritte auf der Registerkarte "SSID Manager" des Access Points aus (unter dem Menüelement **Security > SSID Manager**): Wählen Sie die gewünschte SSID aus. Aktivieren Sie unter "Authentifizierungsmethoden akzeptiert" das Kontrollkästchen **Öffnen**, und wählen Sie in der Dropdown-Liste **With EAP aus**. Aktivieren Sie das Kontrollkästchen **Network-EAP**, wenn Sie über Cisco Client-Karten verfügen. Siehe Diskussion im Abschnitt [Network EAP oder Open Authentication with EAP](#). Klicken Sie auf **Übernehmen**.

RADIO0-802.11B

RADIO1-802.11A

Hostname AP

12:47:46 Mon Sep 20 2004

- HOME
- EXPRESS SET-UP
- EXPRESS SECURITY
- NETWORK MAP +
- ASSOCIATION +
- NETWORK INTERFACES +
- SECURITY**
- Admin Access
- Encryption Manager
- SSID Manager**
- Server Manager
- Local RADIUS Server
- Advanced Security
- SERVICES +
- WIRELESS SERVICES +
- SYSTEM SOFTWARE +
- EVENT LOG +

## Security: SSID Manager - Radio0-802.11B

### SSID Properties

#### Current SSID List

< NEW >
labap1200

**SSID:**

**VLAN:**  [Define VLANs](#)

**Network ID:**  (0-4096)

Delete-Radio0

Delete-All

### Authentication Settings

#### Methods Accepted:

Open Authentication:

Shared Authentication:

Network EAP:

#### Server Priorities:

##### EAP Authentication Servers

Use Defaults [Define Defaults](#)

Customize

Priority 1:

Priority 2:

Priority 3:

##### MAC Authentication Servers

Use Defaults [Define Defaults](#)

Customize

Priority 1:

Priority 2:

Priority 3:

Portions of this image not relevant to the discussion have been edited for clarity

### Global Radio0-802.11B SSID Properties

**Set Guest Mode SSID:**

**Set Infrastructure SSID:**   Force Infrastructure Devices to associate only to this SSID

Apply

Cancel

Sie können diese Befehle auch über die CLI ausführen:

```
AP#configure terminal
```

Enter configuration commands, one per line. End with CNTL/Z.

```
AP(config)#interface dot11radio 0
```

```
AP(config-if)#ssid labap1200
```

```
AP(config-if-ssid)#authentication open eap eap_methods
```

```
AP(config-if-ssid)#authentication network-eap eap_methods
```

```
AP(config-if-ssid)#end
```

```
AP#write memory
```

Wenn Sie die grundlegende Funktionalität mit einer grundlegenden EAP-Konfiguration bestätigen, können Sie zu einem späteren Zeitpunkt zusätzliche Funktionen und eine Schlüsselverwaltung hinzufügen. Vereinfachen Sie die Fehlerbehebung durch komplexere Funktionen auf funktionalen Fundamenten.

## Überprüfen

Dieser Abschnitt enthält Informationen zur Bestätigung, dass Ihre Konfiguration ordnungsgemäß funktioniert.

Bestimmte **show**-Befehle werden vom [Output Interpreter Tool](#) unterstützt (nur [registrierte](#) Kunden), mit dem Sie eine Analyse der **show**-Befehlsausgabe anzeigen können.

- **show radius server-group all**: Zeigt eine Liste aller konfigurierten RADIUS-Servergruppen im Access Point an.

## Fehlerbehebung

### Fehlerbehebungsverfahren

Führen Sie diese Schritte aus, um eine Fehlerbehebung für Ihre Konfiguration durchzuführen.

1. Erstellen Sie im clientseitigen Dienstprogramm oder in der clientseitigen Software ein neues Profil oder eine neue Verbindung mit denselben oder ähnlichen Parametern, um sicherzustellen, dass die Konfiguration des Clients nicht beschädigt wird.
2. Um Funkprobleme zu vermeiden, die eine erfolgreiche Authentifizierung verhindern, deaktivieren Sie vorübergehend die Authentifizierung, wie in den folgenden Schritten gezeigt: Verwenden Sie in der CLI die Befehle **no authentication open eap\_methods**, **no authentication network-eap eap\_methods** und **authentication open**. Deaktivieren Sie in der GUI auf der Seite SSID Manager die Option **Network-EAP**, aktivieren Sie **Open (Öffnen)**, und setzen Sie die Dropdown-Liste auf **No Addition (Kein Hinzufügen)** zurück. Wenn der Client erfolgreich eine Zuordnung vornimmt, trägt RF nicht zum Zuordnungsproblem bei.
3. Überprüfen Sie, ob die gemeinsamen geheimen Kennwörter zwischen dem Access Point und dem Authentifizierungsserver synchronisiert werden. Andernfalls können Sie die folgende

## Fehlermeldung erhalten:

Invalid message authenticator in EAP request

Aktivieren Sie in der CLI den RADIUS-Server-Host x.x.x auth-port x acct-port x-key

<shared\_secret>. Geben Sie auf der Seite "Server Manager" in der GUI erneut den freigegebenen geheimen Schlüssel für den entsprechenden Server in das Feld "Shared Secret" (Gemeinsam genutzter geheimer Schlüssel) ein. Der gemeinsame geheime Eintrag für den Access Point auf dem RADIUS-Server muss das gleiche geheime Kennwort enthalten wie zuvor.

4. Entfernen Sie alle Benutzergruppen aus dem RADIUS-Server. Manchmal können Konflikte zwischen vom RADIUS-Server definierten Benutzergruppen und Benutzergruppen in der zugrunde liegenden Domäne auftreten. Überprüfen Sie die Protokolle des RADIUS-Servers auf fehlgeschlagene Versuche, und geben Sie an, warum diese Versuche fehlgeschlagen sind.

## Fehlerbehebung bei Befehlen

Bestimmte **show**-Befehle werden vom [Output Interpreter Tool](#) unterstützt (nur [registrierte](#) Kunden), mit dem Sie eine Analyse der **show**-Befehlsausgabe anzeigen können.

[Debuggen-Authentifizierungen](#) bieten eine Menge Details zum Erfassen und Interpretieren der Ausgabe von Debuggen in Bezug auf EAP.

**Hinweis:** Bevor Sie **Debugbefehle** ausgeben, lesen Sie die Informationen [Wichtige Informationen über Debug-Befehle](#).

- **debug dot11 aaa authentifizierer state-machine:** Zeigt wichtige Abteilungen (oder Zustände) der Verhandlung zwischen dem Client und dem Authentifizierungsserver an. Im Folgenden finden Sie eine Ausgabe einer **erfolgreichen** Authentifizierung:

```
*Mar 1 02:37:46.846: dot11_auth_dot1x_send_id_req_to_client: Sending
identity request to 0040.96ac.dd05
*Mar 1 02:37:46.846: dot11_auth_dot1x_send_id_req_to_client:
0040.96ac.dd05 timer started for 30 seconds
*Mar 1 02:37:46.930: dot11_auth_dot1x_run_rfsm: Executing
Action(CLIENT_WAIT,EAP_START) for 0040.96ac.dd05
*Mar 1 02:37:46.931: dot11_auth_dot1x_send_id_req_to_client:
Sending identity request to 0040.96ac.dd05 (client)
*Mar 1 02:37:46.931: dot11_auth_dot1x_send_id_req_to_client: Client
0040.96ac.dd05 timer started for 30 seconds
*Mar 1 02:37:46.938: dot11_auth_dot1x_run_rfsm: Executing
Action(CLIENT_WAIT,CLIENT_REPLY) for 0040.96ac.dd05
*Mar 1 02:37:46.938: dot11_auth_dot1x_send_response_to_server:
Sending client 0040.96ac.dd05 data (User Name) to server
*Mar 1 02:37:46.938: dot11_auth_dot1x_send_response_to_server:
Started timer server_timeout 60 seconds
*Mar 1 02:37:47.017: dot11_auth_dot1x_run_rfsm: Executing
Action(SERVER_WAIT,SERVER_REPLY) for 0040.96ac.dd05
*Mar 1 02:37:47.017: dot11_auth_dot1x_send_response_to_client:
Forwarding server message(Challenge) to client 0040.96ac.dd05
*Mar 1 02:37:47.018: dot11_auth_dot1x_send_response_to_client:
Started timer client_timeout 20 seconds
*Mar 1 02:37:47.025: dot11_auth_dot1x_run_rfsm: Executing
Action(CLIENT_WAIT,CLIENT_REPLY) for 0040.96ac.dd05
*Mar 1 02:37:47.025: dot11_auth_dot1x_send_response_to_server:
Sending client 0040.96ac.dd05 data(User Credentials) to server
-----Lines Omitted for simplicity-----
*Mar 1 02:37:47.030: dot11_auth_dot1x_send_response_to_client:
```

```

Started timer client_timeout 20 seconds
*Mar 1 02:37:47.041: dot11_auth_dot1x_run_rfsm: Executing Action
(SERVER_WAIT,SE RVER_PASS) for 0040.96ac.dd05
*Mar 1 02:37:47.041: dot11_auth_dot1x_send_response_to_client:
Forwarding server message(Pass Message) to client
0040.96ac.dd05
*Mar 1 02:37:47.042: dot11_auth_dot1x_send_response_to_client:
Started timer client_timeout 30 seconds
*Mar 1 02:37:47.043: %DOT11-6-ASSOC: Interface Dot11Radio0,
Station TACWEB 0040 .96ac.dd05 Associated KEY_MGMT[NONE] (Client stays
associated to the access point)

```

**Hinweis:** In Cisco IOS Software-Versionen, die älter als 12.2(15)JA sind, lautet die Syntax dieses Debug-Befehls **debug dot1a dot1x state-machine**.

- **debug dot11 aaa authentifizierer process:** Zeigt die einzelnen Dialogeinträge der Verhandlung zwischen dem Client und dem Authentifizierungsserver an.**Hinweis:** In Cisco IOS Software-Versionen, die älter als 12.2(15)JA sind, lautet die Syntax dieses Befehls **debug dot11 aaa dot1x process**.
- **debug radius authentication:** Zeigt die RADIUS-Verhandlungen zwischen Server und Client an, die beide vom Access Point überbrückt werden. Dies ist eine Ausgabe für **fehlgeschlagene Authentifizierung:**

```

*Mar 1 02:34:55.086: RADIUS/ENCODE(00000031):Orig. component type = DOT11
*Mar 1 02:34:55.086: RADIUS: AAA Unsupported Attr: ssid [264] 5
*Mar 1 02:34:55.086: RADIUS: 73 73 69 [ssi]
*Mar 1 02:34:55.086: RADIUS: AAA Unsupported Attr: interface [157] 3
*Mar 1 02:34:55.087: RADIUS: 32 [2]
*Mar 1 02:34:55.087: RADIUS(00000031): Config NAS IP: 10.0.0.106
*Mar 1 02:34:55.087: RADIUS/ENCODE(00000031): acct_session_id: 47
*Mar 1 02:34:55.087: RADIUS(00000031): Config NAS IP: 10.0.0.106
*Mar 1 02:34:55.087: RADIUS(00000031): sending
*Mar 1 02:34:55.087: RADIUS(00000031): Send Access-Request
to 10.0.0.3 :164 5 id 1645/61, len 130
*Mar 1 02:34:55.088: RADIUS: authenticator 0F 6D B9 57 4B A3 F2 0E -
56 77 A4 7E D3 C2 26 EB
*Mar 1 02:34:55.088: RADIUS: User-Name [1] 8 "wirels"
*Mar 1 02:34:55.088: RADIUS: Framed-MTU [12] 6 1400
*Mar 1 02:34:55.088: RADIUS: Called-Station-Id [30] 16 "0019.a956.55c0"
*Mar 1 02:34:55.088: RADIUS: Calling-Station-Id [31] 16 "0040.96ac.dd05"
*Mar 1 02:34:55.088: RADIUS: Service-Type [6] 6 Login [1]
*Mar 1 02:34:55.088: RADIUS: Message-Authenticato[80] 18
*Mar 1 02:34:55.089: RADIUS: 73 8C 59 C4 98 51 53 9F 58 4D 1D EB A5
4A AB 88 [s?Y??QS?XM???J??]
*Mar 1 02:34:55.089: RADIUS: EAP-Message [79] 13
*Mar 1 02:34:55.089: RADIUS: NAS-Port-Id [87] 5 "299"
*Mar 1 02:34:55.090: RADIUS: NAS-IP-Address [4] 6 10.0.0.106
*Mar 1 02:34:55.090: RADIUS: Nas-Identifier [32] 4 "ap"
*Mar 1 02:34:55.093: RADIUS: Received from id 1645/61
10.0.0.3 :1645, Access-Challenge, len 79
*Mar 1 02:34:55.093: RADIUS: authenticator 72 FD C6 9F A1 53 8F D2 -
84 87 49 9B B4 77 B8 973
-----Lines Omitted-----
*Mar 1 02:34:55.117: RADIUS(00000031): Config NAS IP: 10.0.0.106
*Mar 1 02:34:55.118: RADIUS/ENCODE(00000031): acct_session_id: 47
*Mar 1 02:34:55.118: RADIUS(00000031): Config NAS IP: 10.0.0.106
*Mar 1 02:34:55.118: RADIUS(00000031): sending
*Mar 1 02:34:55.118: RADIUS(00000031): Send Access-Request to
10.0.0.3 :164 5 id 1645/62, len 168
*Mar 1 02:34:55.118: RADIUS: authenticator 49 AE 42 83 C0 E9 9A A7 -
07 0F 4E 7C F4 C7 1F 24
*Mar 1 02:34:55.118: RADIUS: User-Name [1] 8 "wirels"

```

```

*Mar 1 02:34:55.119: RADIUS: Framed-MTU [12] 6 1400
-----Lines Omitted-----
*Mar 1 02:34:55.124: RADIUS: Received from id 1645/62
10.0.0.3 :1645, Access-Reject, len 56
*Mar 1 02:34:55.124: RADIUS: authenticator A6 13 99 32 2A 9D A6 25 -
AD 01 26 11 9A F6 01 37
*Mar 1 02:34:55.125: RADIUS: EAP-Message [79] 6
*Mar 1 02:34:55.125: RADIUS: 04 15 00 04 [????]
*Mar 1 02:34:55.125: RADIUS: Reply-Message [18] 12
*Mar 1 02:34:55.125: RADIUS: 52 65 6A 65 63 74 65 64 0A 0D
[Rejected??]
*Mar 1 02:34:55.125: RADIUS: Message-Authenticato[80] 18
*Mar 1 02:34:55.126: RADIUS(00000031): Received from id 1645/62
*Mar 1 02:34:55.126: RADIUS/DECODE: EAP-Message fragments, 4, total 4 bytes
*Mar 1 02:34:55.126: RADIUS/DECODE: Reply-Message fragments, 10, total 10 bytes
*Mar 1 02:34:55.127: %DOT11-7-AUTH_FAILED: Station
0040.96ac.dd05 Authentication failed

```

- **debug aaa authentication:** Zeigt die AAA-Verhandlungen für die Authentifizierung zwischen dem Clientgerät und dem Authentifizierungsserver an.

## Zugehörige Informationen

- [Debugauthentifizierungen](#)
- [Konfigurieren von Authentifizierungstypen](#)
- [LEAP-Authentifizierung auf einem lokalen RADIUS-Server](#)
- [Konfigurieren von RADIUS- und TACACS+-Servern](#)
- [Konfigurieren von Cisco Secure ACS für Windows 3.2 mit PEAP-MS-CHAPv2-Computerauthentifizierung](#)
- [Cisco Secure ACS für Windows 3.2 mit EAP-TLS-Computerauthentifizierung](#)
- [Konfigurieren von PEAP/EAP auf Microsoft IAS](#)
- [Fehlerbehebung bei Microsoft IAS als RADIUS-Server](#)
- [Microsoft 802.1X-Authentifizierungs-Client](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)