

# 802.1x Kabelgebundene Authentifizierung auf einem Catalyst Switch der Serie 3550 und einem ACS Version 4.2 Konfigurationsbeispiel

## Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Beispielkonfiguration eines Switches](#)

[ACS-Konfiguration](#)

[Überprüfung](#)

[Fehlerbehebung](#)

## Einleitung

Dieses Dokument enthält ein einfaches IEEE 802.1x-Konfigurationsbeispiel mit Cisco Access Control Server (ACS) Version 4.2 und dem RADIUS-Protokoll (Remote Access Dial In User Service) für die kabelgebundene Authentifizierung.

## Voraussetzungen

### Anforderungen

Cisco empfiehlt Folgendes:

- Bestätigen Sie die IP-Verfügbarkeit zwischen ACS und dem Switch.
- Stellen Sie sicher, dass die UDP-Ports 1645 und 1646 zwischen ACS und dem Switch offen sind.

### Verwendete Komponenten

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

- Cisco Catalyst Switches der Serie 3550

- Cisco Secure ACS Version 4.2

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 Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

## Konfigurieren

### Beispielkonfiguration eines Switches

1. Geben Sie den folgenden Befehl ein, um den RADIUS-Server und den vorinstallierten Schlüssel zu definieren:

```
Switch(config)# radius-server host 192.168.1.3 key cisco123
```

2. Um die 802.1x-Funktionalität zu aktivieren, geben Sie den folgenden Befehl ein:

```
Switch(config)# dot1x system-auth-control
```

3. Geben Sie die folgenden Befehle ein, um AAA (Authentication, Authorization, and Accounting) und RADIUS-Authentifizierung und -Autorisierung global zu aktivieren:  
**Hinweis:** Dies ist erforderlich, wenn Attribute vom RADIUS-Server übergeben werden müssen. Andernfalls können Sie sie überspringen.

```
Switch(config)# aaa new-model
Switch(config)# aaa authentication dot1x default group radius
Switch(Config)# aaa authorization network default group radius
Switch(Config)# aaa accounting dot1x default start-stop group radius
```

```
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan
Switch(config-if)# authentication port-control auto (12.2.50 SE and later)
Switch(config-if)# dot1x port-control auto (12.2.50 SE and below)
Switch(config-if)# dot1x pae authenticator (version 12.2(25)SEE and below)
Switch(config-if)# dot1x timeout quiet-period
Switch(config-if)# dot1x timeout tx-period
```

### ACS-Konfiguration

1. Um den Switch als AAA-Client in ACS hinzuzufügen, navigieren Sie zu **Network Configuration > Add entry AAA client**, und geben Sie die folgenden Informationen ein:  
IP-Adresse: <IP>Gemeinsamer geheimer Schlüssel: <Schlüssel>Authentifizierung über Radius (Cisco IOS®/PIX 6.0)

**Network Configuration**

AAA Client Hostname: switch

AAA Client IP Address: 192.168.1.2

Shared Secret: cisco123

**RADIUS Key Wrap**

Key Encryption Key: [Empty]

Message Authenticator Code Key: [Empty]

Key Input Format:  ASCII  Hexadecimal

Authenticate Using: RADIUS (Cisco IOS/PIX 6.0)

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

Match Framed-IP-Address with user IP address for accounting packets from this AAA Client

You can use the wildcard asterisk (\*) for an octet in the IP address. For example, if you want every AAA client in your 192.168.13.1 Class C network to be represented by a single AAA client entry, enter 192.168.13.\* in the AAA Client IP Address box.

You can define ranges within an octet of an IP address. For example, if you want every AAA client with an IP address between 192.168.13.12 and 192.168.13.221 to be represented by a single AAA client entry, enter 192.168.13.12-221 in the AAA Client IP Address box.

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

**Shared Secret**

The Shared Secret is used to encrypt TACACS+ or the RADIUS AAA client and ACS. The shared secret must be configured in the AAA client and ACS identically, including case sensitivity.

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

**Network Device Group**

From the list, click the name of the Network Device Group (NDG) to which this AAA client belongs.

Note: To enable NDGs, click **Interface Configuration > Advanced Options > Network Device Groups**.

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

**RADIUS Key Wrap**

2. Um das Authentifizierungs-Setup zu konfigurieren, navigieren Sie zu **System Configuration > Global Authentication Setup**, und überprüfen Sie, ob das Kontrollkästchen **Allow MS-CHAP Version 2 Authentication (MS-CHAP-Authentifizierung Version 2 zulassen)** aktiviert ist:

**System Configuration**

EAP-TLS session timeout (minutes): 120

Select one of the following options for setting username during authentication:

Use Outer Identity

Use CN as Identity

Use SAN as Identity

**LEAP**

Allow LEAP (For Aironet only)

**EAP-MD5**

Allow EAP-MD5

AP EAP request timeout (seconds): 20

**MS-CHAP Configuration**

Allow MS-CHAP Version 1 Authentication

Allow MS-CHAP Version 2 Authentication

[Back to Help](#)

Use this page to specify settings for various authentication protocols.

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

**EAP Configuration**

EAP is a flexible request-response protocol for arbitrary authentication information (RFC 2284). EAP is layered on top of another protocol such as UDP, 802.1x or RADIUS and supports multiple "authentication" types.

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

**PEAP**

PEAP is the outer layer protocol for the secure tunnel.

Note: PEAP is a certificate-based authentication protocol. PEAP authentication can occur only after you have completed the required steps on the [ACS Certificate Setup page](#).

- **Allow EAP-MSCHAPv2** — Use to enable EAP-MSCHAPv2 within MS PEAP authentication. Enable this protocol for any repository that supports MS-CHAPv2, such as Microsoft AD, and the ACS Internal Database.
- **Allow EAP-GTC** — Use to enable EAP-GTC within Cisco PEAP authentication. Enable this protocol to support any database that supports PAP, including LDAP, OTP Servers, and the ACS Internal Database.
- **Allow Certificate Validation** — Use to enable the DPAD (PAP-TLV) control for certificate validation of

3. Um einen Benutzer zu konfigurieren, klicken Sie im Menü auf **User Setup** (Benutzereinrichtung), und führen Sie die folgenden Schritte aus:  
 Geben Sie die **Benutzerinformationen** ein: Network-Admin <Benutzername>. Klicken Sie auf **Hinzufügen/Bearbeiten**. Geben Sie den **richtigen Namen** ein: Network-Admin <beschreibender Name>. Fügen Sie eine **Beschreibung** hinzu: <Ihre Wahl>. Wählen Sie **Kennwortauthentifizierung**: Interne ACS-Datenbank. Geben Sie das **Kennwort** ein: ..... <Kennwort>. Bestätigen Sie das **Kennwort**: <Kennwort>. Klicken Sie auf **Senden**.

## Überprüfung

Das [Output Interpreter-Tool](#) ([nur](#) registrierte Kunden) unterstützt bestimmte **show**-Befehle. Verwenden Sie das Output Interpreter-Tool, um eine Analyse der **show**-Befehlsausgabe anzuzeigen.

Geben Sie die folgenden Befehle ein, um sicherzustellen, dass Ihre Konfiguration ordnungsgemäß funktioniert:

- Punkt 1x anzeigen
- dot1x-Zusammenfassung anzeigen
- show dot1x-Schnittstelle
- show authentication sessions interface <Schnittstelle>
- show authentication interface <Schnittstelle>

```
Switch(config)# show dot1x
```

```
Sysauthcontrol Enabled
Dot1x Protocol Version 3
```

```
Switch(config)# show dot1x summary
```

```
Interface PAE Client Status
```

```
Fa0/4 AUTH
```

```
Switch(config)# show dot1x interface fa0/4 detail
```

```
Dot1x Info for FastEthernet0/4
```

```
PAE = AUTHENTICATOR
PortControl = FORCE_AUTHORIZED
ControlDirection = Both
HostMode = SINGLE_HOST
QuietPeriod = 5
ServerTimeout = 0
SuppTimeout = 30
ReAuthMax = 2
MaxReq = 2
TxPeriod = 10
```

# Fehlerbehebung

In diesem Abschnitt finden Sie Debugbefehle, die Sie zur Fehlerbehebung bei Ihrer Konfiguration verwenden können.

**Hinweis:** Lesen Sie [Wichtige Informationen](#) zu [Debug-Befehlen](#), bevor Sie **Debug**-Befehle verwenden.

- `debug dot1x all`
- `debug authentication all`
- **Debug-Radius** (liefert die Informationen zum Radius auf Debugebene)
- `debug aaa authentication` (debug für Authentifizierung)
- `debug aaa Authorization` (debug for Authorization)

## 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.