

# Konfigurieren der 802.1X-Authentifizierung auf Catalyst Wireless Controllern der Serie 9800

## Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konfigurieren](#)

[Netzwerkdiagramm](#)

[WLC-Konfiguration](#)

[AAA-Konfiguration auf 9800 WLCs](#)

[WLAN-Profilkonfiguration](#)

[Richtlinienprofilkonfiguration](#)

[Richtlinien-Tag-Konfiguration](#)

[Richtlinien-Tag-Zuweisung](#)

[ISE-Konfiguration](#)

[WLC auf der ISE angeben](#)

[Neuen Benutzer auf ISE erstellen](#)

[Erstellen des Autorisierungsprofils](#)

[Erstellen eines Policy Sets](#)

[Authentifizierungsrichtlinie erstellen](#)

[Autorisierungsrichtlinie erstellen](#)

[Überprüfung](#)

[Fehlerbehebung](#)

[Fehlerbehebung am WLC](#)

[Fehlerbehebung auf der ISE](#)

## Einleitung

In diesem Dokument wird die Einrichtung eines WLAN mit 802.1X-Sicherheit auf einem Cisco Catalyst Wireless Controller der Serie 9800 beschrieben.

## Voraussetzungen

### Anforderungen

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

- 802.1x

### Verwendete Komponenten

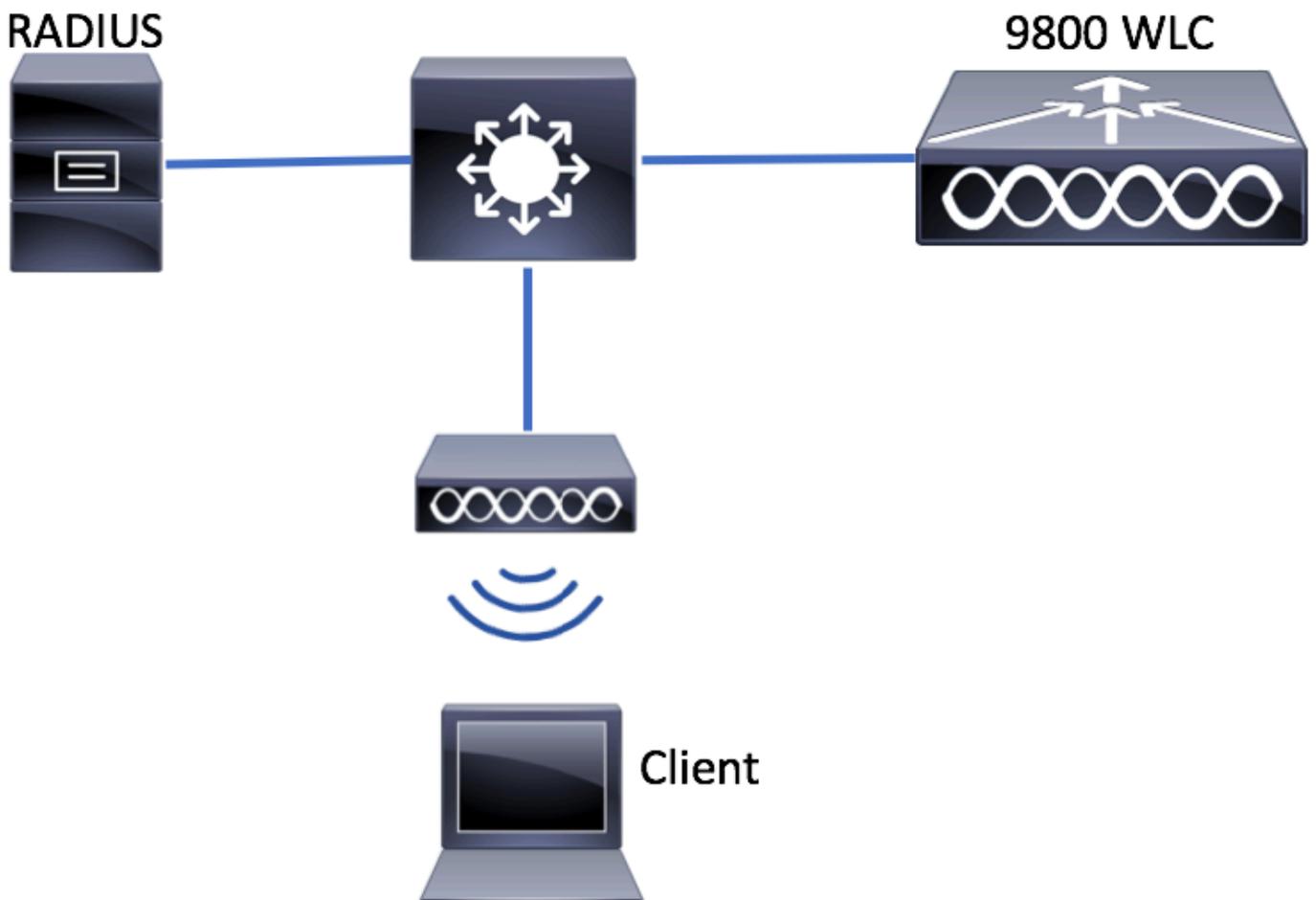
Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- Catalyst Wireless Controller der Serie 9800 (Catalyst 9800-CL)
- Cisco IOS® XE Gibraltar 17.3.x
- Cisco ISE 3.0

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.

## Konfigurieren

### Netzwerkdiagramm



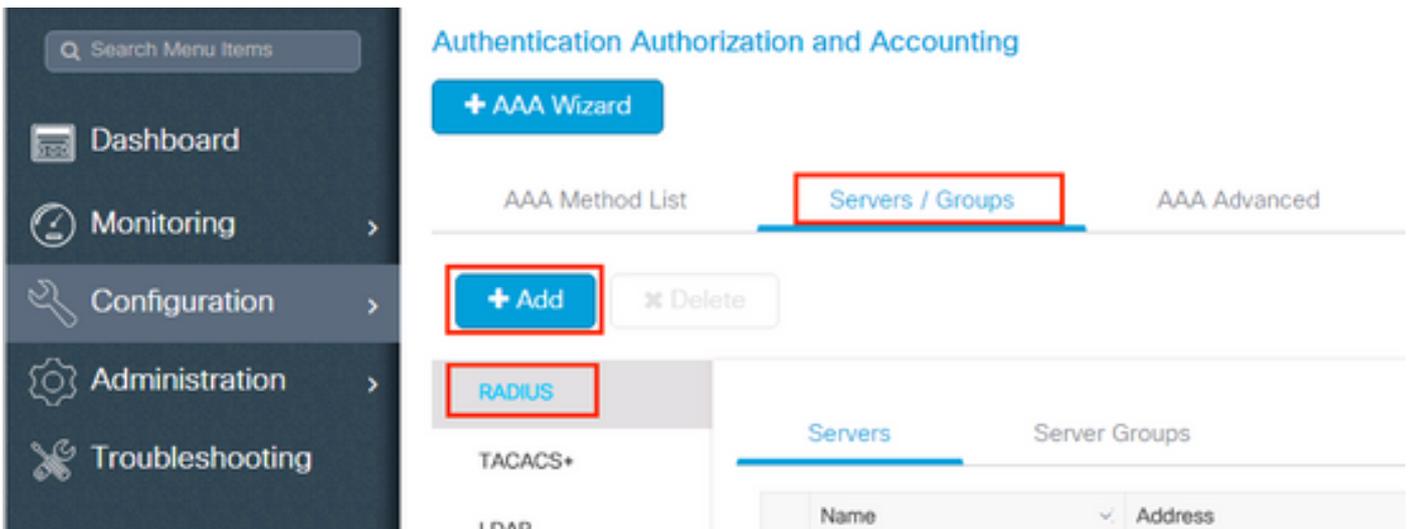
### WLC-Konfiguration

#### AAA-Konfiguration auf 9800 WLCs

#### GUI:

Schritt 1: Deklarieren des RADIUS-Servers Navigieren Sie zu **Configuration > Security > AAA > Servers /**

Groups > RADIUS > Servers > + Add und geben Sie die RADIUS-Serverinformationen ein.



Stellen Sie sicher, dass **Support für CoA** aktiviert ist, wenn Sie beabsichtigen, Central Web Authentication (oder andere Sicherheitsfunktionen, die eine Autorisierungsänderung erfordern) in Zukunft zu verwenden.

Create AAA Radius Server

Name*	ISE-kcg	Clear PAC Key	<input type="checkbox"/>
IPv4/IPv6 Server Address*	172.16.0.11	Set New PAC Key	<input type="checkbox"/>
Shared Secret*	.....		
Confirm Shared Secret*	.....		
Auth Port	1812		
Acct Port	1813		
Server Timeout (seconds)	1-1000		
Retry Count	0-100		
Support for CoA	ENABLED <input checked="" type="checkbox"/>		

Schritt 2: Hinzufügen des RADIUS-Servers zu einer RADIUS-Gruppe Navigieren Sie zu **Configuration > Security > AAA > Servers / Groups > RADIUS > Server Groups > + Add**. Geben Sie Ihrer Gruppe einen Namen, und verschieben Sie den Server, den Sie zuvor in der Liste **Assigned Servers**.

Create AAA Radius Server Group ✕

Name\*

Group Type

MAC-Delimiter

MAC-Filtering

Dead-Time (mins)

Available Servers

Assigned Servers

Schritt 3: Erstellen einer Liste von Authentifizierungsmethoden Navigieren Sie zu **Configuration > Security > AAA > AAA Method List > Authentication > + Add**.

Q Search Menu Items

Dashboard

Monitoring >

**Configuration** >

Administration >

## Authentication Authorization and Accounting

Servers / Groups

---

General

Authorization

Name	
	<input type="button" value="x Del"/>

Geben Sie die Informationen ein:

Quick Setup: AAA Authentication

Method List Name\* list-name

Type\* dot1x

Group Type group

Fallback to local

Available Server Groups

- radius
- ldap
- tacacs+
- ISE-kcg-grp

Assigned Server Groups

- ISE-grp-name

Cancel Save & Apply to Device

## CLI:

```
# config t
# aaa new-model

# radius server <radius-server-name>
# address ipv4 <radius-server-ip> auth-port 1812 acct-port 1813
# timeout 300
# retransmit 3
# key <shared-key>
# exit

# aaa group server radius <radius-grp-name>
# server name <radius-server-name>
# exit

# aaa server radius dynamic-author
# client <radius-server-ip> server-key <shared-key>
# aaa authentication dot1x <dot1x-list-name> group <radius-grp-name>
```

## Hinweis zur AAA Dead-Server-Erkennung

Nachdem Sie den RADIUS-Server konfiguriert haben, können Sie überprüfen, ob er als "ALIVE" gilt:

```
#show aaa servers | s WNCDC Platform State from WNCDC (1) : current UP Platform State from WNCDC (2) : current UP Platform State from WNCDC (3) : current UP Platform State from WNCDC (4) : current UP ...
```

Sie können die **dead criteria**, sowie die **deadtime** auf Ihrem WLC, insbesondere wenn Sie mehrere RADIUS-Server verwenden.

```
#radius-server dead-criteria time 5 tries 3 #radius-server deadtime 5
```

**Hinweis:** **dead criteria** ist das Kriterium, anhand dessen ein RADIUS-Server als ausgefallen markiert wird. Die Kommission wird um die Beantwortung folgender Fragen ersucht: 1. Ein

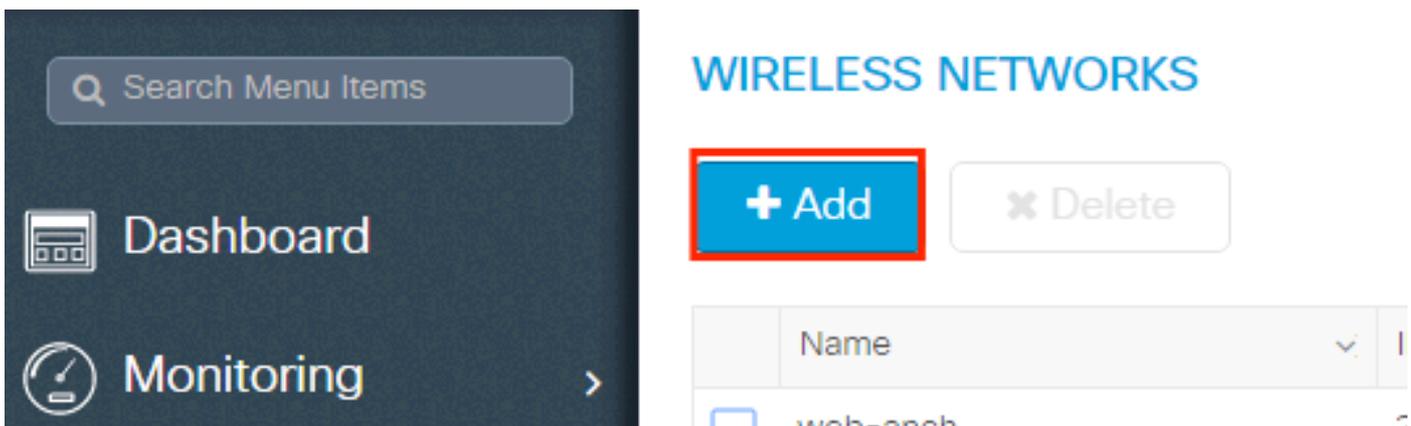
Timeout (in Sekunden), das die Zeitspanne von dem Zeitpunkt, zu dem der Controller das letzte Mal ein gültiges Paket vom RADIUS-Server empfangen hat, bis zu dem Zeitpunkt, zu dem der Server als ausgefallen markiert ist, angibt. 2. Ein Zähler, der die Anzahl aufeinander folgender Zeitüberschreitungen angibt, die auf dem Controller auftreten müssen, bevor der RADIUS-Server als ausgefallen markiert wird.

**Hinweis:** `deadtime` gibt die Zeitdauer (in Minuten) an, die der Server in den "Dead"-Status versetzt wird, nachdem "Dead Criteria" ihn als "Dead" markiert hat. Nach Ablauf der Deadtime markiert der Controller den Server als UP (ALIVE) und benachrichtigt die registrierten Clients über die Statusänderung. Ist der Server nach dem Status als UP noch nicht erreichbar und ist das Dead-Kriterium erfüllt, so wird der Server für das Deadtime-Intervall erneut als Dead markiert.

## WLAN-Profilkonfiguration

### GUI:

Schritt 1: WLAN erstellen. Navigieren Sie zu **Configuration > Wireless > WLANs > + Add**, und konfigurieren Sie das Netzwerk nach Bedarf.



Schritt 2: Geben Sie die WLAN-Informationen ein

### Add WLAN

General Security Advanced

Profile Name*	<input type="text" value="prof-name"/>	Radio Policy	<input type="text" value="All"/>
SSID	<input type="text" value="ssid-name"/>	Broadcast SSID	<input checked="" type="checkbox"/> ENABLED
WLAN ID*	<input type="text" value="1"/>		
Status	<input checked="" type="checkbox"/> ENABLED		

Schritt 3: Navigieren Sie zum und wählen Sie die erforderliche Sicherheitsmethode aus. In diesem Fall **WPA2 + 802.1x**.

### Add WLAN

General Security Advanced

Layer2 Layer3 AAA

Layer 2 Security Mode	<input type="text" value="WPA + WPA2"/>	Fast Transition	<input type="text" value="Adaptive Enab..."/>
MAC Filtering	<input type="checkbox"/>	Over the DS	<input checked="" type="checkbox"/>
Protected Management Frame		Reassociation Timeout	<input type="text" value="20"/>
PMF	<input type="text" value="Disabled"/>		
WPA Parameters			
WPA Policy	<input type="checkbox"/>		

**Add WLAN**

PMF Disabled

**WPA Parameters**

WPA Policy

WPA2 Policy

WPA2 Encryption

- AES(CCMP128)
- CCMP256
- GCMP128
- GCMP256

Auth Key Mgmt 802.1x

Cancel Save & Apply to Device

Schritt 4: Über die **security > AAA** die unter Schritt 3 erstellte Authentifizierungsmethode im Abschnitt AAA Configuration on 9800 WLC auswählen.

**Add WLAN**

General **Security** Advanced

Layer2 Layer3 **AAA**

Authentication List list-name

Local EAP Authentication

Cancel Save & Apply to Device

**CLI:**

```
# config t
# wlan <profile-name> <wlan-id> <ssid-name>
# security dot1x authentication-list <dot1x-list-name>
# no shutdown
```

## Richtlinienprofilkonfiguration

In einem Richtlinienprofil können Sie neben anderen Einstellungen (wie Zugriffskontrolllisten [ACLs], Quality of Service [QoS], Mobility Anchor, Timer usw.) festlegen, welchem VLAN die Clients zugewiesen werden sollen.

Sie können entweder Ihr Standardrichtlinienprofil verwenden oder ein neues Profil erstellen.

### GUI:

Navigieren Sie zu **Configuration > Tags & Profiles > Policy Profile**, und konfigurieren Sie entweder Ihr **Standard-Richtlinienprofil** oder erstellen Sie ein neues.

Policy Profile

+ Add

Policy Profile Name	Description
<input type="checkbox"/> voice	
<input type="checkbox"/> default-policy-profile	default policy profile

Navigation: 1 items per page, 10 items per page

Stellen Sie sicher, dass das Profil aktiviert ist.

Wenn sich Ihr Access Point (AP) im lokalen Modus befindet, stellen Sie außerdem sicher, dass im Richtlinienprofil **Central Switching** und **Central Authentication** aktiviert sind.

## Edit Policy Profile

General | Access Policies | QOS and AVC | Mobility | Advanced

⚠ Configuring in enabled state will result in loss of connectivity for clients associated with this profile.

Name\*

Description

Status **ENABLED**

Passive Client  DISABLED

Encrypted Traffic Analytics  DISABLED

### CTS Policy

Inline Tagging

SGACL Enforcement

Default SGT

### WLAN Switching Policy

Central Switching

Central Authentication

Central DHCP

Central Association Enable

Flex NAT/PAT

Wählen Sie auf der Registerkarte "Access Policies" (Zugriffsrichtlinien) das VLAN aus, dem die Clients zugewiesen werden müssen.

## Edit Policy Profile

General | **Access Policies** | QOS and AVC | Mobility | Advanced

### WLAN Local Profiling

HTTP TLV Caching

RADIUS Profiling

DHCP TLV Caching

Local Subscriber Policy Name

### VLAN

VLAN/VLAN Group

Multicast VLAN

### WLAN ACL

IPv4 ACL

IPv6 ACL

### URL Filters

Pre Auth

Post Auth

Wenn im Feld "Access-Accept" ISE-Rückgabeattribute (z. B. "VLAN Assignment") vorhanden sein sollen, aktivieren Sie AAA override im Advanced Registerkarte:

Edit Policy Profile ✕

---

General
Access Policies
QOS and AVC
Mobility
Advanced

**WLAN Timeout**

Session Timeout (sec)

Idle Timeout (sec)

Idle Threshold (bytes)

Client Exclusion Timeout (sec)

**Fabric Profile**

**Umbrella Parameter Map**

**mDNS Service Policy**

[Clear](#)

**DHCP**

IPv4 DHCP Required

DHCP Server IP Address

[Show more >>>](#)

**WLAN Flex Policy**

VLAN Central Switching

Split MAC ACL

**Air Time Fairness Policies**

2.4 GHz Policy

5 GHz Policy

**AAA Policy**

Allow AAA Override

NAC State

Policy Name  ✕

↶ Cancel

📄
Update & Apply to Device

**CLI:**

```
# config
# wireless profile policy <policy-profile-name>
# aaa-override # central switching # description "<description>" # vlan <vlanID-or-VLAN_name> #
no shutdown
```

**Richtlinien-Tag-Konfiguration**

Das Policy Tag (Richtlinien-Tag) dient zum Verknüpfen der SSID mit dem Richtlinienprofil. Sie können entweder ein neues Richtlinien-Tag erstellen oder das Standard-Richtlinien-Tag verwenden.

**Hinweis:** Das default-policy-Tag ordnet dem default-policy-Profil automatisch alle SSIDs mit einer WLAN-ID zwischen 1 und 16 zu. Sie kann weder geändert noch gelöscht werden. Wenn Sie über ein WLAN mit der ID 17 oder höher verfügen, kann das default-policy-tag nicht verwendet werden.

**GUI:**

Navigieren Sie zu **Configuation > Tags & Profiles > Tags > Policy** und fügen Sie ggf. ein neues hinzu.

Search Menu Items

Dashboard

Monitoring >

Configuration >

Administration >

Troubleshooting

### Manage Tags

Policy Site RF AP

+ Add x Delete

Policy Tag Name	Description
<input type="checkbox"/> central-anchor	
<input type="checkbox"/> default-policy-tag	default policy-tag

1 10 items per page

Verknüpfen Sie Ihr WLAN-Profil mit dem gewünschten Richtlinienprofil.

### Add Policy Tag

Name\* PolicyTagName

Description Enter Description

+ Add x Delete

WLAN Profile Policy Profile

0 10 items per page No items to display

Cancel Save & Apply to Device

**Add Policy Tag** ✕

Name\*

Description

+ Add ✕ Delete

WLAN Profile	Policy Profile
◀ ◁ 0 ▷ ▶	10 items per page
No items to display	

Map WLAN and Policy

WLAN Profile\*  Policy Profile\*

✕ ✓

↶ Cancel Save & Apply to Device

**Add Policy Tag** ✕

Name\*

Description

+ Add ✕ Delete

WLAN Profile	Policy Profile
<input type="checkbox"/> prof-name	default-policy-profile
◀ ◁ 1 ▷ ▶	10 items per page
1 - 1 of 1 items	

↶ Cancel Save & Apply to Device

**CLI:**

```
# config t
# wireless tag policy <policy-tag-name>
# wlan <profile-name> policy <policy-profile-name>
```

**Richtlinien-Tag-Zuweisung**

Weisen Sie den erforderlichen APs das Richtlinien-Tag zu.

**GUI:**

Um das Tag einem AP zuzuweisen, navigieren Sie zu **Configuration > Wireless > Access Points > AP Name > General Tags**, die entsprechende Policy-Tag-Nummer zuzuweisen, und klicken Sie dann auf **Update & Apply to Device**.

The screenshot shows the 'Edit AP' configuration page with the following details:

- General Tab:** AP Name\* (AP3802-02-WS), Location\* (default location), Base Radio MAC (00:42:68:c6:41:20), Ethernet MAC (00:42:68:a0:d0:22), Admin Status (Enabled), AP Mode (Local), Operation Status (Registered), Fabric Status (Disabled).
- Tags Section:** Policy (default-policy-tag), Site (default-site-tag), RF (default-rf-tag).
- Version Section:** Primary Software Version (10.0.200.50), Predownloaded Status (N/A), Predownloaded Version (N/A), Next Retry Time (N/A), Boot Version (1.0.0), IOS Version (10.0.200.02), Mini IOS Version (0.0.0.0).
- IP Config Section:** IP Address (172.16.0.207), Static IP (unchecked).
- Time Statistics Section:** Up Time (9 days 1 hrs 17 mins 24 secs), Controller Associated Time (0 days 3 hrs 26 mins 41 secs), Controller Association Latency (8 days 21 hrs 50 mins 33 secs).

Buttons: Cancel (left), Update & Apply to Device (right, highlighted).

**Hinweis:** Beachten Sie, dass bei einer Änderung des Richtlinien-Tags an einem Access Point dessen Verknüpfung mit dem 9800 WLC gelöscht wird und dieser dann einige Augenblicke später wieder hinzugefügt wird.

Um dieselbe Policy Tag mehreren APs zuzuweisen, navigieren Sie zu **Configuration > Wireless Setup > Advanced > Start Now > Apply**.



## 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.