

# Konfigurieren und Beheben von Fehlern bei einem ATA 186 mit Cisco IOS Gatekeepers

## Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Netzwerkdiagramm](#)

[Registrieren des ATA 186 beim Gatekeeper](#)

[Hinzufügen von Sicherheit](#)

[Authentifizierung des Endpunkts am Gatekeeper mit einer H.323-ID](#)

[Authentifizierung des Endpunkts am Gatekeeper mit einer E.164-Adresse](#)

[Authentifizierung des Endgeräts am Gatekeeper mit einer H.323-ID und einem Kennwort](#)

[Authentifizierung des Endpunkts am Gatekeeper über eine E.164-Adresse und ein E.164-Kennwort](#)

[Authentifizierung des Endpunkts am Gatekeeper mit einer H.323-ID und einem Kennwort mithilfe der Trennlinie](#)

[Überprüfen](#)

[Fehlerbehebung](#)

[Fehlerbehebung beim "Vorzimmerlöwen"](#)

[Fehlerbehebung beim ATA 186](#)

[Beispieldebuggen für Anrufe aus dem ATA 186](#)

[Zugehörige Informationen](#)

## [Einführung](#)

Der Cisco Analog Telephone Adaptor (ATA) 186 ist ein Adapter, der den Anschluss von Hörer an Ethernet übernimmt und normale analoge Telefone mit IP-basierten Telefonienetzen verbindet. Der ATA 186 verfügt über zwei Sprachports, die nur ältere analoge Tonwahltelefone unterstützen. Anders als die Ports der regulären Foreign Exchange Station (FXS) können diese nicht mit einer privaten Zweigstelle (PBX) verbunden werden, da der ATA 186 an diesen Ports keine Nummern senden kann. Mit dieser Konfiguration können Sie beide Sprach-Ports mit jeweils unterschiedlichen E.164-Adressen verwenden.

## [Voraussetzungen](#)

## [Anforderungen](#)

In diesem Dokument wird davon ausgegangen, dass der Leser mit dem Inhalt des Dokuments [Cisco ATA 186 Basic Configuration](#) vertraut ist.

Für diese Konfiguration muss der ATA 186 mit dem H.323-Feature-Set mit Version 2.0 oder höher ausgestattet sein.

Stellen Sie sicher, dass zwischen den ATA 186-, Gateway- und Gatekeeper-Geräten eine IP-Verbindung besteht. Stellen Sie außerdem sicher, dass der Zugriff auf den ATA 186 über die Webservermethode für weitere Konfigurationen möglich ist.

## Verwendete Komponenten

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

- ATA 186 mit Version 2.12
- Cisco 3640 mit Cisco IOS<sup>®</sup> Softwareversion 12.1 als Gateway
- Cisco 2600 mit Cisco IOS Software, Version 12.2 als Gatekeeper

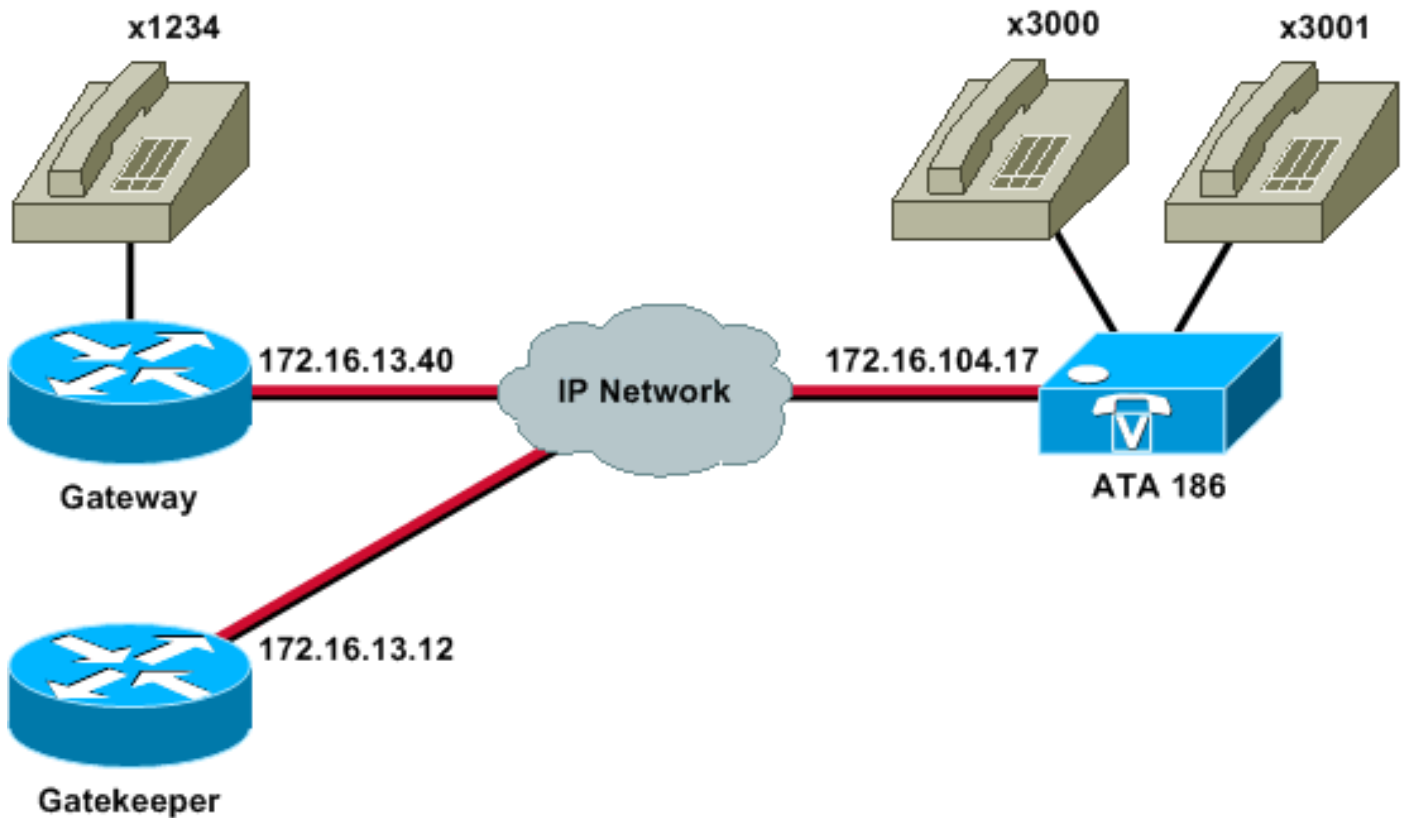
Die in diesem Dokument enthaltenen Informationen wurden aus Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Sie in einem Live-Netzwerk arbeiten, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen, bevor Sie es verwenden.

## Konventionen

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

## Netzwerkdiagramm

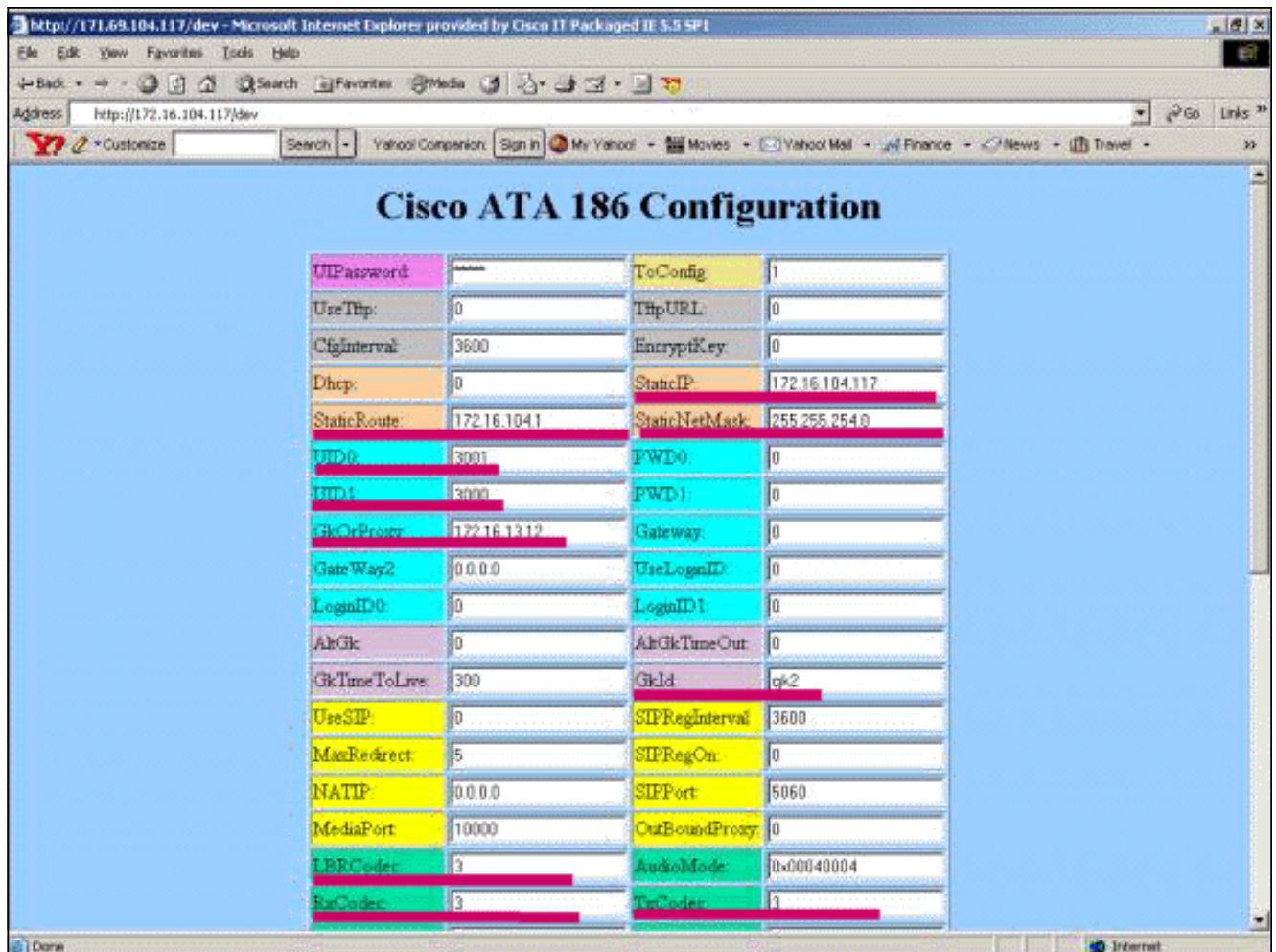
In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:



## Registrieren des ATA 186 beim Gatekeeper

Befolgen Sie diese Anweisungen, um den ATA 186 beim Gatekeeper zu registrieren.

1. Geben Sie in das Adressfeld des Webbrowsers den URL **http://ip\_address\_of\_ata/dev** ein, **um** auf den Konfigurationsbildschirm ATA 186 zuzugreifen, wobei *ip\_address\_of\_ata* die IP-Adresse des ATA 186 ist, den Sie registrieren. In diesem Beispiel lautet die URL **http://172.16.104.117/dev**. Das Konfigurationsfenster für den Cisco ATA 186 wird angezeigt. **Hinweis:** Die unterstrichenen Felder sind die relevanten konfigurierten Parameter für dieses Szenario.



Die IP-Adressierung kann statisch oder dynamisch erfolgen, wie im Dokument [Cisco ATA 186 Basic Configuration](#) erläutert. Im vorherigen Bildschirm wird die statische IP-Adresse verwendet.

2. Konfigurieren Sie im Konfigurationsfenster des Cisco ATA 186 die folgenden Felder: UID0 und UID1: Konfigurieren der E.164-Adressen der Sprach-Ports 0 und 1. Beide Sprach-Ports können nicht dieselbe E.164-Adresse haben, da der ATA 186 nicht jagen kann, wenn einer der Ports belegt ist. Wenn beiden Sprach-Ports dieselbe E.164-Adresse zugewiesen ist, wird der Anruf immer an den ersten Sprach-Port gesendet. Wenn dieser Port belegt ist, wird das Besetztzeichen an den Anrufer gesendet. RxCodec und TxCodec: Konfigurieren Sie die Codec-ID. G.723.1 - Codec-ID 0. G.711a - Codec-ID 1. G.711u - Codec-ID 2. G.729a: Codec-ID 3. In der unten gezeigten Konfiguration wird der G.729a-Codec auf dem ATA 186 und auf dem Gateway verwendet. LBRCodec (LBRCodec): Konfigurieren Sie als 0 oder 3, basierend auf dem ausgewählten Codec. LBR ist 0 - Der G.723.1-Codec ist für beide FXS-Ports jederzeit verfügbar. Jede Leitung kann zwei G.723.1-Anrufe ohne Konferenzfunktion aufrechterhalten. Aus diesem Grund können im Cisco ATA 186 bis zu vier G.723.1-Anrufe aufrechterhalten werden. Ein Beispiel ist die Anklopfen-Funktion. LBR ist 3 - G.729a ist für einen der beiden FXS-Ports auf Basis des "first-come-first-service" verfügbar. Wenn das Cisco IOS-Gateway mit dem Standard-G.729-Codec konfiguriert ist, kann nur ein ATA 186-Port verwendet werden. Um zu verhindern, dass der zweite Anruf fehlschlägt, konfigurieren Sie eine Sprach-Codec-Klasse auf dem Gateway, um den zweiten Anruf mit einem G.711-Codec auszuhandeln. Ausführliche Informationen finden Sie im Abschnitt [Codec-Aushandlung](#) im [Abschnitt Codecs](#): Dokument [zu Komplexität, Hardware-Support, MOS und Verhandlung](#). GkOrProxy: Konfigurieren Sie die IP-Adresse des Gatekeeper. Anschließend wird alles, was von den ATA 186-Sprach-Ports gewählt wird, an den Gatekeeper gesendet.

3. Klicken Sie auf die Schaltfläche **Übernehmen** und laden Sie die Seite dann neu. Die Neukonfiguration des ATA 186 dauert 10 Sekunden.

Diese Beispiele sind relevante Konfigurationen für Cisco IOS Gatekeeper und Gateway:

### 2610-Gatekeeper

```
interface Ethernet0/0
 ip address 172.16.13.12 255.255.255.224
 half-duplex
 h323 interface
 h323 h323-id pro
 h323 gatekeeper ipaddr 172.16.13.12
 h323 t120 bypass
 !
dial-peer cor custom
 !
 !
 !
gatekeeper
 zone local gk2 cisco.com 172.16.13.12
no shutdown
 !
```

### 3640-Gateway

```
interface Ethernet0/0
 ip address 172.16.13.40 255.255.255.224
 half-duplex
 !
ip classless
ip route 0.0.0.0 0.0.0.0 172.16.13.33
ip http server
 !
 !
 !
voice-port 3/0/0
 !
voice-port 3/0/1
 !
dial-peer cor custom
 !
 !
 !
dial-peer voice 1 pots
 destination-pattern 34
 port 3/0/0
 !
dial-peer voice 2 pots
 destination-pattern 45
 port 3/0/1
 !
dial-peer voice 100 pots
 destination-pattern 1234
 port 3/0/0
 !
dial-peer voice 3000 voip
 destination-pattern 300.
 session target ras
!--- Dial-peer to send the calls to ATA. !
```



## Hinzufügen von Sicherheit

Ab Version 2.12 der ATA-Software stehen die in diesem Abschnitt beschriebenen Optionen zum Hinzufügen von Sicherheit zur Verfügung.

### Authentifizierung des Endpunkts am Gatekeeper mit einer H.323-ID

Führen Sie die folgenden Schritte aus, um den ATA 186 so zu konfigurieren, dass er sich mit der H.323-ID registriert:

1. Legen Sie im Feld AutoMethod den Wert **0 fest** (der Standardwert ist 1). Der Hexadezimalwert, der für dieses Feld konfiguriert werden soll, ist 0x0.
2. Legen Sie im Feld UseLoginID (Anmelde-ID verwenden) **1 fest**.
3. Konfigurieren Sie LoginID0 und LoginID1 mit den H.323-IDs für den ATA 186. Der ATA 186 zeichnet sich durch zwei verschiedene H.323-Terminals aus, von denen einer für jeden Port.

Dies ist eine Beispiel-Arbeitskonfiguration für den Gatekeeper, wenn ATA mit der H.323-ID-Authentifizierungsmethode verwendet wird:

Parameter	Value	Parameter	Value
UIPassword	-----	ToConfig	1
UseTtp	0	TtpURL	0
CfgInterval	3600	EncryptKey	0
Dhcp	0	StaticIP	172.16.104.117
StaticRoute	172.16.104.1	StaticNetMask	255.255.254.0
UID0	3001	PWD0	0
UID1	3000	PWD1	0
GkOrProxy	172.16.131.2	Gateway	0
GateWay2	0.0.0.0	UseLoginID	1
LoginID0	atagw1	LoginID1	atagw2
AltGk	0	AltGkTimeOut	0
GkTimeToLive	300	GkId	gk2
UseSIP	0	SIPRegInterval	3600
MaxRedirect	5	SIPRegOn	0
NATIP	0.0.0.0	SIPPort	5060
MediaPort	10000	OutBoundProxy	0
LBRCodec	3	AudioMode	0x00040004
RxCCodec	3	TrCodec	3

#### 2610-Gatekeeper

```
aaa authentication login default local
aaa authentication login cisco none
aaa authentication login h323 local
```

```

aaa session-id common
enable password ww
!
username atagw1
!--- Same as the LoginID0 and LoginID1 fields. username
atagw2 username 3640
!--- Same as the H.323 ID configured on the gateway. !
gatekeeper zone local gk2 cisco.com 172.16.13.12
security any
!--- Register after the H.323 ID or E.164 address is
authenticated. no shutdown !

```

## Authentifizierung des Endpunkts am Gatekeeper mit einer E.164-Adresse

Führen Sie die folgenden Schritte aus, um den ATA 186 so zu konfigurieren, dass er sich bei der E.164-Adresse registriert:

1. Legen Sie im Feld AutoMethod den Wert **0 fest** (der Standardwert ist 1). Der Hexadezimalwert, der für dieses Feld konfiguriert werden soll, ist 0x0.
2. Legen Sie im Feld UseLoginID (Anmelde-ID verwenden) **0 fest**. Der ATA verwendet die Felder UID0 und UID1, um vom Gatekeeper authentifiziert zu werden.

Dies ist eine Beispiel-Arbeitskonfiguration für den Gatekeeper und das Gateway bei Verwendung von ATA mit der E.164-ID-Authentifizierungsmethode:

### **2610-Gatekeeper**

```

aaa authentication login default local
aaa authentication login cisco none
aaa authentication login h323 local
aaa session-id common
enable password ww
!
username 3001
!--- Same as the UID0. username 3000
!--- Same as the UID1. ! gatekeeper zone local gk2
cisco.com 172.16.13.12 security any
!--- Register after the H.323 ID or E.164 address is
authenticated. no shutdown !

```

## Authentifizierung des Endgeräts am Gatekeeper mit einer H.323-ID und einem Kennwort

Führen Sie die folgenden Schritte aus, um den ATA 186 so zu konfigurieren, dass er sich mit der H.323-ID und dem Kennwort anmeldet:

1. Legen Sie im Feld AutMethod den Wert **1 fest** (der Standardwert ist 1). Der Hexadezimalwert, der für dieses Feld konfiguriert werden soll, ist 0x1. Dieses Feld gibt an, dass der ATA jetzt nach dem Kennwort sucht.
2. Legen Sie im Feld UseLoginID (Anmelde-ID verwenden) **1 fest**.
3. Konfigurieren Sie LoginID0 und LoginID1 mit den H.323-IDs für den ATA 186. Der ATA 186 zeichnet sich durch zwei verschiedene H.323-Terminals aus, von denen einer für jeden Port.
4. Konfigurieren Sie PWD0 und PWD1 mit dem Kennwort für jeden Port. **Hinweis:** Der ATA verwendet das Kennwort, um das Token zu generieren. Dieses Token wird zur

Authentifizierung an den Gatekeeper gesendet.

5. Konfigurieren Sie NTP mit der IP-Adresse des NTP-Servers (Network Time Protocol). Der Gatekeeper und der ATA müssen Uhren mit demselben NTP-Server synchronisiert haben.

**Hinweis:** Der Zeitstempel wird für die Tokenerstellung verwendet. Weitere Informationen finden Sie im [Leitfaden Gateway zu Gatekeeper \(H.235\) und Gatekeeper \(IZCT\) zur Fehlerbehebung bei Sicherheitsrisiken](#).

Dies ist eine Beispiel-Arbeitskonfiguration für den Gatekeeper und das Gateway, wenn ATA mit der Authentifizierungsverfahren für H.323-ID und -Kennwort verwendet wird:

```
2610-Gatekeeper

aaa authentication login default local
aaa authentication login cisco none
aaa authentication login h323 local
aaa session-id common
enable password ww
!
username atagw1 password cisco
!--- Same as the LoginID0 and PWD0 fields. username
atagw2 password cisco
!--- Same as the LoginID1 and PWD1 fields. ! gatekeeper
zone local gk2 cisco.com 172.16.13.12 security token
required-for registration
!--- Register after the H.323 ID or E.164 address and
token is authenticated. no shutdown !
```

**Hinweis:** Weitere Informationen zur Gatekeeper-Sicherheit finden Sie im [Leitfaden zur Fehlerbehebung für Gateway zu Gatekeeper \(H.235\) und Gatekeeper zu Gatekeeper \(IZCT\)](#).

## [Authentifizierung des Endpunkts am Gatekeeper über eine E.164-Adresse und ein E.164-Kennwort](#)

Führen Sie die folgenden Schritte aus, um den ATA 186 so zu konfigurieren, dass er sich mit der E.164-ID und dem zugehörigen Kennwort anmeldet:

1. Legen Sie im Feld AuthMethod den Wert **1 fest** (der Standardwert ist 1). Der Hexadezimalwert, der für dieses Feld konfiguriert werden soll, ist 0x0. Dieses Feld gibt an, dass der ATA jetzt nach dem Kennwort sucht.
2. Legen Sie im Feld UseLoginID (Anmelde-ID verwenden) **0 fest**.
3. Konfigurieren Sie UID0 und UID1 mit den E.164-IDs für den ATA 186. Der ATA 186 zeichnet sich durch zwei verschiedene H.323-Terminals aus, von denen einer für jeden Port.
4. Konfigurieren Sie PWD0 und PWD1 mit dem Kennwort für jeden Port. **Hinweis:** Der ATA verwendet das Kennwort, um das Token zu generieren. Dieses Token wird zur Authentifizierung an den Gatekeeper gesendet.
5. Konfigurieren Sie NTP mit der IP-Adresse des NTP-Servers. Der Gatekeeper und der ATA müssen Uhren mit demselben NTP-Server synchronisiert haben.

**Hinweis:** Der Zeitstempel wird für die Tokenerstellung verwendet. Weitere Informationen finden Sie im [Leitfaden Gateway zu Gatekeeper \(H.235\) und Gatekeeper \(IZCT\) zur Fehlerbehebung bei Sicherheitsrisiken](#).

Dies ist eine Beispiel-Arbeitskonfiguration für den Gatekeeper und das Gateway, wenn ATA mit



der E.164-ID- und Kennwortauthentifizierungsmethode verwendet wird:

### 2610-Gatekeeper

```
aaa authentication login default local
aaa authentication login cisco none
aaa authentication login h323 local
aaa session-id common
enable password ww
!
username 3001 password cisco
!--- Same as the UID0 and PWD0 fields. username 3000
password cisco

!--- Same as the UID1 and PWD1 fields. ! gatekeeper zone
local gk2 cisco.com 172.16.13.12 security token
required-for registration
!--- Register after the H.323 ID or E.164 address and
token is authenticated. no shutdown !
```

**Hinweis:** Weitere Informationen zur Gatekeeper-Sicherheit finden Sie im [Leitfaden zur Fehlerbehebung für Gateway zu Gatekeeper \(H.235\)](#) und [Gatekeeper zu Gatekeeper \(IZCT\)](#).

### Authentifizierung des Endpunkts am Gatekeeper mit einer H.323-ID und einem Kennwort mithilfe der Trennlinie

Führen Sie die folgenden Schritte aus, um den ATA 186 so zu konfigurieren, dass er sich mit der H.323-ID und dem Kennwort anmeldet:

1. Legen Sie im Feld AutMethod den Wert **1 fest** (der Standardwert ist 1). Der für dieses Feld konfigurierte Hexadezimalwert ist 0x1. Dieses Feld gibt an, dass der ATA jetzt nach dem Kennwort sucht.
2. Legen Sie im Feld UseLoginID (Anmelde-ID verwenden) **1 fest**.
3. Konfigurieren Sie LoginID0 und LoginID1 mit den H.323-IDs, gefolgt von der Trennlinie und dem Kennwort für den ATA 186. Beispiel: LoginID0 ist **atagw1=cisco**. Der ATA 186 zeichnet sich durch zwei verschiedene H.323-Terminals aus, von denen einer für jeden Port. **Hinweis:** Der ATA verwendet das Kennwort, um das Token zu generieren. Dieses Token wird zur Authentifizierung an den Gatekeeper gesendet.
4. Konfigurieren Sie NTP mit der IP-Adresse des NTP-Servers. Der Gatekeeper und der ATA müssen Uhren mit demselben NTP-Server synchronisiert haben.

**Hinweis:** Der Zeitstempel wird für die Tokenerstellung verwendet. Weitere Informationen finden Sie im [Leitfaden Gateway zu Gatekeeper \(H.235\)](#) und [Gatekeeper \(IZCT\) zur Fehlerbehebung bei Sicherheitsrisiken](#).

Dies ist eine Beispiel-Arbeitskonfiguration für den Gatekeeper und das Gateway bei Verwendung von ATA mit der H.323-ID- und Kennwortauthentifizierungsmethode mithilfe einer Trennlinie:

### 2610-Gatekeeper

```
aaa authentication login default local
aaa authentication login cisco none
aaa authentication login h323 local
aaa session-id common
```

```

enable password ww
!
username atagw1 password cisco
!--- Same as the LoginID0 and PWD0 fields. username
atagw2 password cisco
!--- Same as the LoginID1 and PWD1 fields. ! gatekeeper
zone local gk2 cisco.com 172.16.13.12 security h323-id
security password separator =
!--- Register after the H.323 ID or E.164 address and
token is authenticated. no shutdown !

```

**Hinweis:** Weitere Informationen zur Gatekeeper-Sicherheit finden Sie im [Leitfaden zur Fehlerbehebung für Gateway zu Gatekeeper \(H.235\) und Gatekeeper zu Gatekeeper \(IZCT\)](#).

## Überprüfen

Das Beispiel in diesem Abschnitt zeigt die Registrierung von Gatekeeper-Endpunkten.

Führen Sie zum Überprüfen der Konfiguration den Befehl **show gatekeeper endpoint aus**.

```

                                GATEKEEPER ENDPOINT
REGISTRATION

CallSignalAddr  Port  RASSignalAddr  Port  Zone Name  Type      Flags
-----
172.16.13.40    1720  172.16.13.40   50923  gk2        VOIP-GW   E164-ID: 1234
                                           H323-ID: 3640
172.16.13.43    1720  172.16.13.43   58400  gk2        VOIP-GW   H323-ID: 3660-2
172.16.104.117  1720  172.69.85.90   1719   gk2        TERM      E164-ID: 3000
172.16.104.117  1721  172.69.85.90   1739   gk2        TERM      E164-ID: 3001
Total number of active registrations=3

```

**Hinweis:** Der ATA 186 wird als H.323-Terminal (**TERM**) und nicht als H.323-Gateway registriert. Dies geschieht bewusst, sodass nur die Anrufe, die für den ATA 186 vorgesehen sind, an den ATA gesendet werden.

**Hinweis:** Im Feld für das ATA-Gateway können Sie keine Adresse angeben. Sie können den ATA 186 nicht für die Arbeit mit dem Gatekeeper und dem Gateway konfigurieren.

## Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Der ATA 186 gibt keinen Wählton aus, wenn er nicht erfolgreich beim Gatekeeper registriert wurde. Wenn der ATA 186 nicht beim Gatekeeper registriert ist, überprüfen Sie die folgenden Punkte:

- Zwischen dem ATA 186 und dem Gatekeeper bestehen IP-Verbindungen.
- Die Felder ATA 186 UID0 und UID1 sind korrekt konfiguriert. Wenn die UID-Felder auf 0 gesetzt sind, versucht der ATA 186 nicht, sich beim Gatekeeper anzumelden. Das Feld UID0 muss mindestens einen Wert von 0 (null) aufweisen, damit der ATA 186 den Registrierungsprozess startet. Wenn beide ATA 186-Ports (UID0 und UID1) E.164-Adressen mit einer E.164-Adresse von nicht null haben, versucht der ATA 186, sich bei beiden Ports zu

registrieren. Der ATA 186 bietet keinen Wählton, selbst wenn einer der Ports nicht registriert werden kann.

- Der Gatekeeper ist korrekt konfiguriert. Wenn der Gatekeeper mit einem Präfix für die lokale Zone konfiguriert ist, muss die E.164-Adresse des ATA 186 enthalten sein. Wenn die Sicherheit auf dem Gatekeeper konfiguriert ist, muss der ATA 186 entsprechend konfiguriert werden.

Überprüfen Sie außerdem, ob das UseSIP-Feld auf 0 gesetzt ist. Dies ist erforderlich, um den ATA 186 im H.323-Modus zu konfigurieren. Wenn das UseSIP-Feld auf 1 festgelegt ist, sendet der ATA 186 die Registrierungsanfrage nicht an den Gatekeeper.

## Fehlerbehebung beim "Vorzimmerlöwen"

Wenn die Sicherheit konfiguriert ist, geben Sie den [Befehl debug aaa authentication aus](#).

Wenn keine Sicherheit konfiguriert ist, führen Sie den [Befehl debug ras aus](#).

**Hinweis:** Der ATA 186 wird für die beiden Sprachports separat registriert. Daher wird der ATA 186 doppelt so unterschiedliche H.323-Terminals authentifiziert, wie in diesem Debugging gezeigt:

```
4w4d: AAA/AUTHEN/CONT (3800768902): continue_login (user='atagw1')
4w4d: AAA/AUTHEN (3800768902): status = GETPASS
4w4d: AAA/AUTHEN/CONT (3800768902): Method=LOCAL
4w4d: AAA/AUTHEN (3800768902): status = PASS
4w4d: AAA: parse name=<no string> idb type=-1 tty=-1
4w4d: AAA/MEMORY: create_user (0x83149EFC) user='atagw2'ruser='NULL' port='NULL'
rem_addr='NULL' authen_type=ASCII service=LOGIN priv=0 initial_task_id='0'
4w4d: AAA/AUTHEN/START (294225678): port='' list='h323' action=LOGIN service=LOGIN
4w4d: AAA/AUTHEN/START (294225678): found list h323
4w4d: AAA/AUTHEN/START (294225678): Method=LOCAL
4w4d: AAA/AUTHEN (294225678): status = GETPASS
4w4d: AAA/H323: Password:
4w4d: AAA/AUTHEN/CONT (294225678): continue_login (user='atagw2')
4w4d: AAA/AUTHEN (294225678): status = GETPASS
4w4d: AAA/AUTHEN/CONT (294225678): Method=LOCAL
4w4d: AAA/AUTHEN (294225678): status = PASS
4w4d: AAA: parse name=<no string> idb type=-1 tty=-1
4w4d: AAA/MEMORY: create_user (0x831910C0) user='3660' ruser='NULL' port='NULL'
rem_addr='NULL' authen_type=ASCII service=LOGIN priv=0 initial_task_id='0'
```

Weitere Beispiele zur Fehlerbehebung finden Sie unter [Fehlerbehebung bei Gatekeeper-Registrierungsproblemen](#).

## Fehlerbehebung beim ATA 186

Wenn Sie mit Gateways und Gateways von Drittanbietern arbeiten, ist das Tool zur Fehlerbehebung am ATA 186 sehr hilfreich. Um das Fehlerbehebungstool ATA 186 zu aktivieren, gehen Sie wie folgt vor:

1. Konfigurieren Sie im Feld ATA Nprintf die IP-Adresse des PCs, der sich im gleichen Subnetz wie der ATA 186 befindet.
2. Der nach der Adresse angegebene Port muss **9001** sein.
3. Führen Sie an der DOS-Eingabeaufforderung des PCs das Programm **continental.exe** aus.

Sie können das Programm continv.exe vom [Cisco Software Center](#) herunterladen (nur [registrierte Kunden](#)).

Das Programm persistent v.exe ist in der neuesten ATA 186-Softwareversion ZIP-Datei enthalten.

## Beispieldebuggen für Anrufe aus dem ATA 186

D:\Documents and Settings\sshafiqu\My Documents\voice\ata>prserv.exe

GK<-1: KPA-RRQ:300 sec

GK->1: RCF:TTL 300

```
!--- ATA was reset after the gatekeeper configuration was added. WStop:0 Wed Feb 06 19:06:54
2002 Hello from 171.69.85.90(0) Build 1109a: v2.12 ata186 Successfully Registered with the
Gatekeeper GK zone<gk2>172.16.13.12: 3000 GK zone:gk2 0x13e138 delayed RRQ: 48 ticks: 300 GK
zone<gk2>172.16.13.12: 3001 GK zone:gk2 0x141e58 delayed RRQ: 56 ticks: 300 BMK : gk2 GK<-1:
KPA-RRQ:300 sec BMK : gk2 GK<-0: KPA-RRQ:300 sec GK->1: RCF:TTL 300 GK->0: RCF:TTL 300 SCC->(0
0) <cmd 0> 3000 active @0xab45555a (GK @0xac100d0c) !--- Call made from voice port 0. [0]DTMF 1
[0]DTMF 2 [0]DTMF 3 [0]DTMF 4 [0]DTMF # Calling 1234 SCC->(0 0) <cmd 16> CLIP\ \SCC->(0 0) <cmd
2> \<0 0> dial<1234> GK<-0: ARQ: 0
GK->0: ACF:0:direct call
IRR in 240 sec
CallRasCallBack: 1 33e15eb 33e206b 33e39b0
Connect to <0xac100d28 1720>>..
>>>>>>> TX CALLER ID : 0x1          0x80 6
Q931<-0:Setup:CRV 25006
Q931->0:Proceeding
Connect H245...
H245 TCP conn ac100d28 11006
CESE/MSDSE start:<0 0 0 0>
capSize = 3
H245->0:Cese
RemoteInputCap <15 5>
RemoteInputCap <15 4>
RemoteInputCap <15 1>
RemoteInputCap <4 11>
MODE FRAME : 11 2
RemoteAudioCap <4 10>
Capability set accepted
H245->0:MSD: <rn tt> = <0x269c 60>
H245->0:CeseAck
H245->0:MsdAck
h323.c 1837: cstate : 3
->H245<0> OLC
H245<-0:LcseOpen
set TX audio to G729/G729A 2 fpp
SetG723Mode: 2 0
H245->0:LcseOpen
H245->0:OLC mode 10
remote OpenLogicalReq G711/G729(10) : 2 fpp
OpenRtpRxPort(0,0x0,4000):14
RTP Rx Init: 0, 0
RTP->0:<0xab45555a 4000>
H245->0:LcseOpenAck
RTP<-0:<0xac100d28 17304>
[0]Enable encoder 18
RTP TX[0]:SSRC_ID = 4af964c0
RTP Tx Init: 0, 0
[0]DPKT 1st: 861812319 861812079, pt 18
Enable LEC adapt [0]=1
H323Dispatcher : 3 3
[0]Received pi=8 in q931
Q931->0:Progress
Q931->0:Connect
SCC:ev=12[0:0] 3 0
```

```
Q931->0:ReleaseComplete: reason 16, tone = 13
H245<-0:EndSessionCmd 1
0: Close RTPRX
write TCP err : 13 -33
[0:0]Rel LBRC Res
Q931<-*:ReleaseComplete
!--- ATA side hangs up the call. write TCP err : 12 -33 GK<-0: DRQ:0
!--- Disconnect request sent by ATA. SCC:ev=13[0:0] 4 0 [0:0]SCC: Disconnected GK->0: DCF
!--- Disconnect confirm received. SCC->(0 0) <cmd 1> [0]MPT mode 0
```

## Beispiel für Debug ohne Wählen-ATA

Beide Sprach-Ports benötigen eine eindeutige E.164-Adresse. Andernfalls erhält der ATA eine Ablehnung vom Gatekeeper. Während dieser Zeit wird der ATA 186 mit einem Sprachport als H.323-Terminal registriert, es gibt jedoch keinen Wählen-ATA.

```
K<-0: GRQ
BMK : gk2
GK->0: GCF:GK@0xac100d0c-1719
BMK : gk2
Secured RRQ
GK<-0: RRQ
GK->0:RRJ: reason 4
```

## Zugehörige Informationen

- [Cisco ATA 186 - Grundkonfiguration](#)
- [Konfigurieren und Beheben von Fehlern bei einem ATA 186 mit einem Cisco IOS Gateway](#)
- [Cisco High Performance Gatekeeper - Konfigurieren des Gatekeeper](#)
- [Konfigurieren von Voice over IP](#)
- [Unterstützung von Sprachtechnologie](#)
- [Produkt-Support für Sprach- und Unified Communications](#)
- [Fehlerbehebung bei Cisco IP-Telefonie](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)