

Configuration et dépannage d'un ATA 186 avec contrôleurs d'accès Cisco IOS

Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Components Used](#)

[Conventions](#)

[Diagramme du réseau](#)

[Enregistrement de l'ATA 186 avec le contrôleur d'accès](#)

[Ajout de sécurité](#)

[Authentifier le point de terminaison au niveau du contrôleur d'accès avec un ID H.323](#)

[Authentifier le point de terminaison au niveau du contrôleur d'accès avec une adresse E.164](#)

[Authentifier le point de terminaison au niveau du contrôleur d'accès avec un ID H.323 et un mot de passe](#)

[Authentifier le point de terminaison au niveau du contrôleur d'accès avec une adresse et un mot de passe E.164](#)

[Authentifier le point de terminaison au niveau du contrôleur d'accès avec un ID H.323 et un mot de passe à l'aide du séparateur](#)

[Vérification](#)

[Dépannage](#)

[Dépannage du contrôleur d'accès](#)

[Dépannage de l'ATA 186](#)

[Exemples de débogages pour les appels effectués à partir de l'ATA 186](#)

[Informations connexes](#)

[Introduction](#)

L'adaptateur de téléphone analogique Cisco (ATA) 186 est un adaptateur combiné-Ethernet faisant interface entre des téléphones analogiques traditionnels et des réseaux téléphoniques basés sur IP. L'ATA 186 dispose de deux ports vocaux qui ne peuvent prendre en charge que les téléphones à tonalité analogique traditionnels. Contrairement aux ports FXS (Foreign Exchange Station) classiques, ceux-ci ne peuvent pas être interfacés avec un autocommutateur privé (PBX), car l'ATA 186 ne peut pas envoyer de chiffres sur ces ports. Avec cette configuration, vous pouvez utiliser les deux ports vocaux avec des adresses E.164 différentes sur chacun.

[Conditions préalables](#)

[Conditions requises](#)

Ce document suppose que le lecteur connaît le contenu du document [Configuration de base de Cisco ATA 186](#).

Cette configuration nécessite que ATA 186 soit à la version 2.0 ou ultérieure, à l'aide du jeu de fonctions H.323.

Assurez-vous qu'il existe une connectivité IP entre les périphériques ATA 186, de passerelle et de gardien d'accès. Vérifiez également que l'ATA 186 est accessible via la méthode de serveur Web pour une configuration ultérieure.

[Components Used](#)

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- ATA 186 avec version 2.12
- Cisco 3640 avec le logiciel Cisco IOS® Version 12.1 comme passerelle
- Cisco 2600 avec la version 12.2 du logiciel Cisco IOS comme contrôleur d'accès

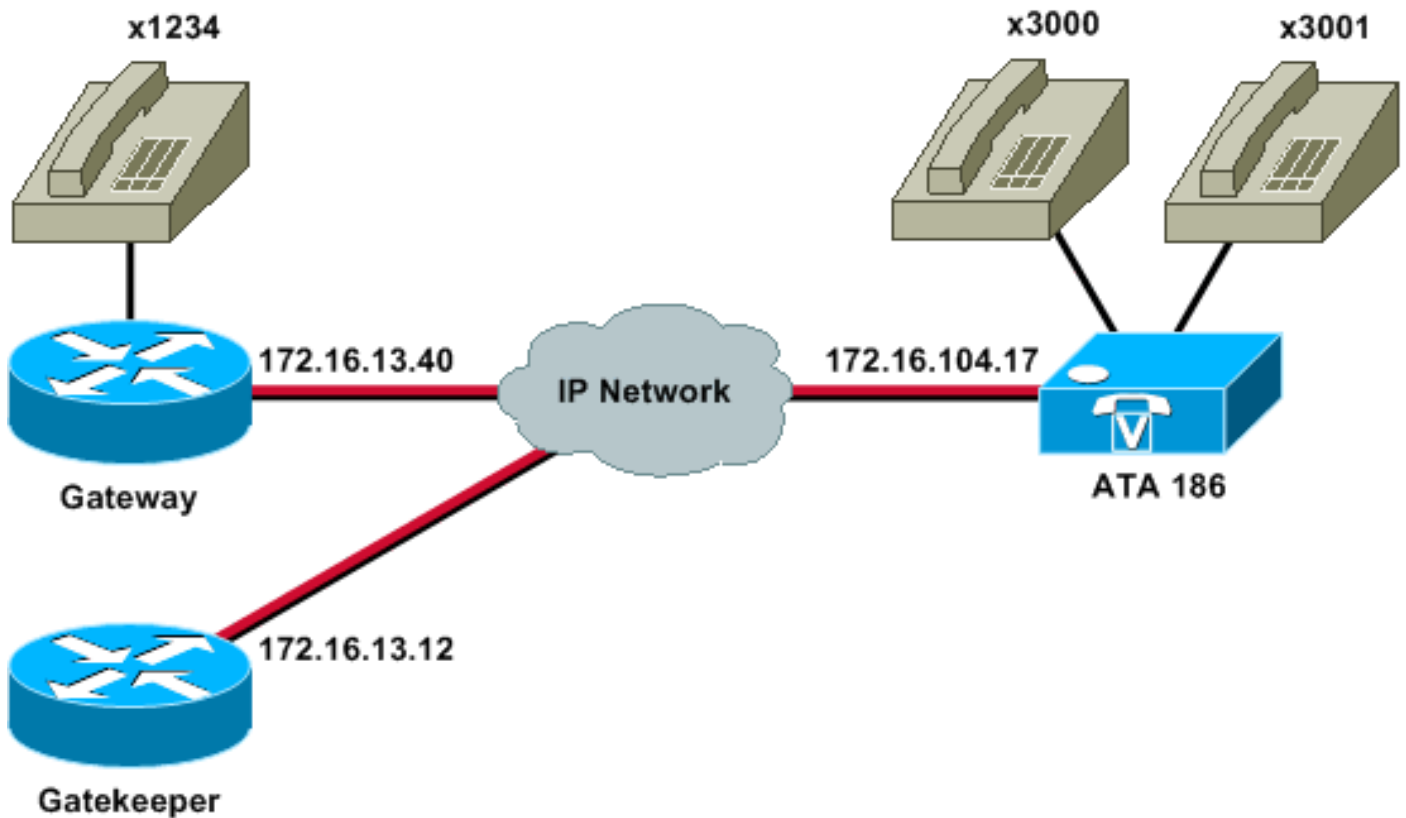
Les informations présentées dans ce document ont été créées à partir de périphériques dans un environnement de laboratoire spécifique. All of the devices used in this document started with a cleared (default) configuration. Si vous travaillez dans un réseau opérationnel, assurez-vous de bien comprendre l'impact potentiel de toute commande avant de l'utiliser.

[Conventions](#)

For more information on document conventions, refer to the [Cisco Technical Tips Conventions](#).

[Diagramme du réseau](#)

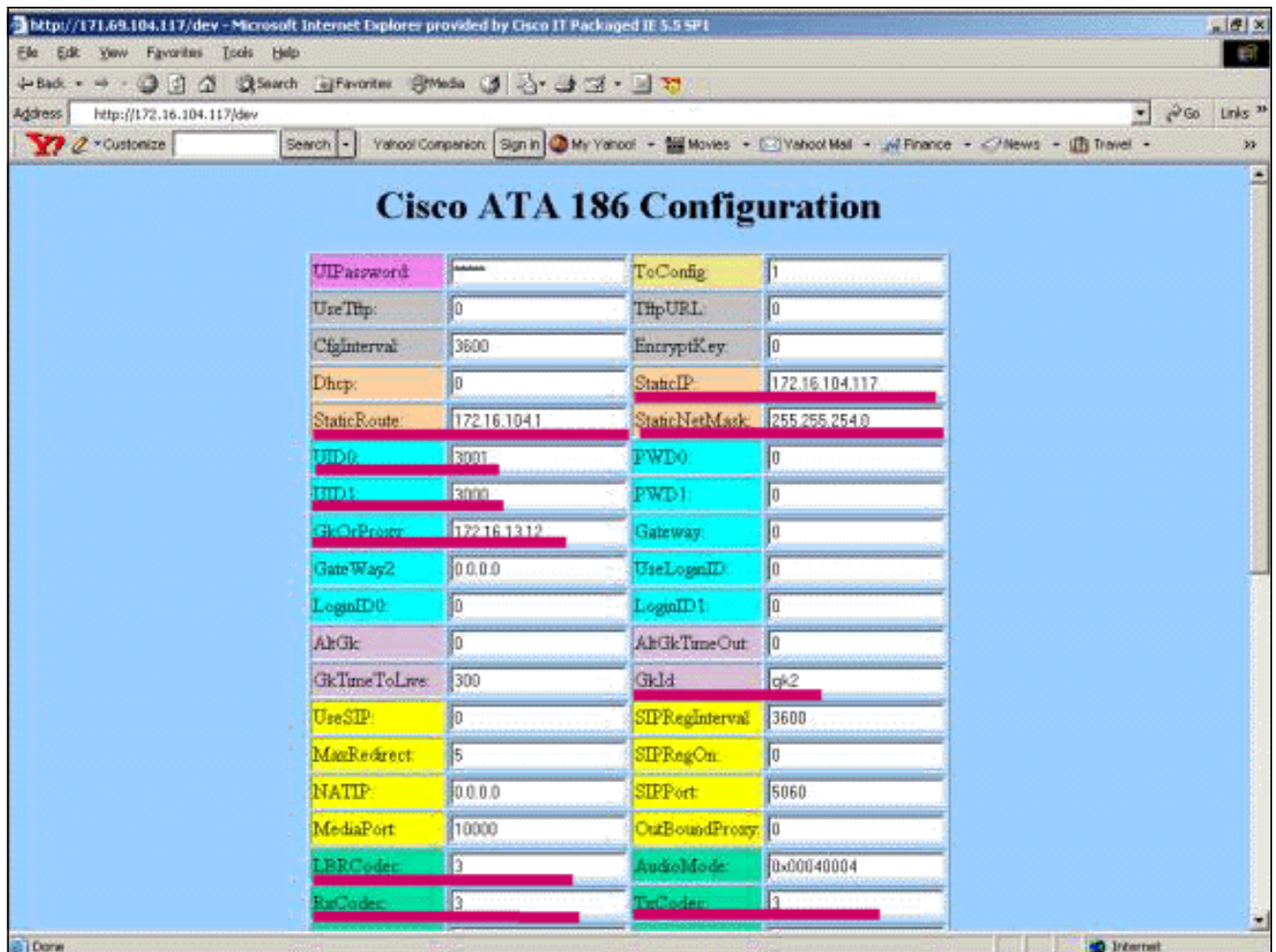
Ce document utilise la configuration réseau suivante :



Enregistrement de l'ATA 186 avec le contrôleur d'accès

Suivez ces instructions pour enregistrer l'ATA 186 avec le contrôleur d'accès.

1. Dans un champ Adresse ou Emplacement du navigateur Web, tapez l'URL **http://*ip_address_of_ata*/dev** pour accéder à l'écran de configuration ATA 186, où *ip_address_of_ata* est l'adresse IP de l'ATA 186 que vous enregistrez. Dans cet exemple, l'URL est **http://172.16.104.117/dev**. La fenêtre Cisco ATA 186 Configuration s'affiche. **Remarque** : les champs soulignés sont les paramètres configurés appropriés pour ce scénario.



L'adressage IP peut être effectué de manière statique ou dynamique, comme expliqué dans le document [Configuration de base de Cisco ATA 186](#). Dans l'écran précédent, l'adresse IP statique est utilisée.

2. Dans la fenêtre Cisco ATA 186 Configuration, configurez les champs suivants :UID0 et UID1 : configurez les adresses E.164 des ports vocaux 0 et 1.Les deux ports vocaux ne peuvent pas avoir la même adresse E.164, car l'ATA 186 ne peut pas rechercher si l'un des ports est occupé. Si les deux ports vocaux reçoivent la même adresse E.164, l'appel est toujours envoyé au premier port vocal. Si ce port est occupé, le signal occupé est envoyé à l'appelant.RxCodec et TxCodec : configurez l'ID du codec.G.723.1 : ID de codec 0.G.711a : ID de codec 1.G.711u : ID de codec 2.G.729a : ID de codec 3.Dans la configuration ci-dessous, le codec G.729r8 est utilisé sur l'ATA 186 et sur la passerelle.LBRCodec : configurez comme 0 ou 3, en fonction du codec choisi.LBRC est 0 : le codec G.723.1 est disponible à tout moment sur les deux ports FXS. Chaque ligne peut gérer deux appels G.723.1 dans un état non conférence. Par conséquent, jusqu'à quatre appels G.723.1 peuvent être maintenus dans le Cisco ATA 186. Un exemple est l'appel en attente.LBRC est 3—G.729a est disponible sur l'un des deux ports FXS sur la base du premier arrivé premier servi. Si la passerelle Cisco IOS est configurée avec le codec G.729 par défaut, un seul port ATA 186 peut être utilisé. Pour empêcher l'échec du deuxième appel, configurez une classe de codec voix sur la passerelle pour négocier le deuxième appel à l'aide d'un codec G.711. Pour plus d'informations, reportez-vous à la section [Négociation du codec de Compréhension des codecs : Complexité, support matériel, MOS et document de négociation](#).GKOrProxy : configurez l'adresse IP du contrôleur d'accès.Une fois cette opération effectuée, tout ce qui est composé à partir des ports vocaux ATA 186 est envoyé au contrôleur d'accès.

3. Cliquez sur le bouton **Appliquer**, puis rechargez la page. L'ATA 186 prend 10 secondes pour se reconfigurer.

Ces exemples sont des configurations pertinentes pour le contrôleur d'accès et la passerelle Cisco IOS :

Contrôleur d'accès 2610

```
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
 !
```

Passerelle 3640

```
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. !
```

Ajout de sécurité

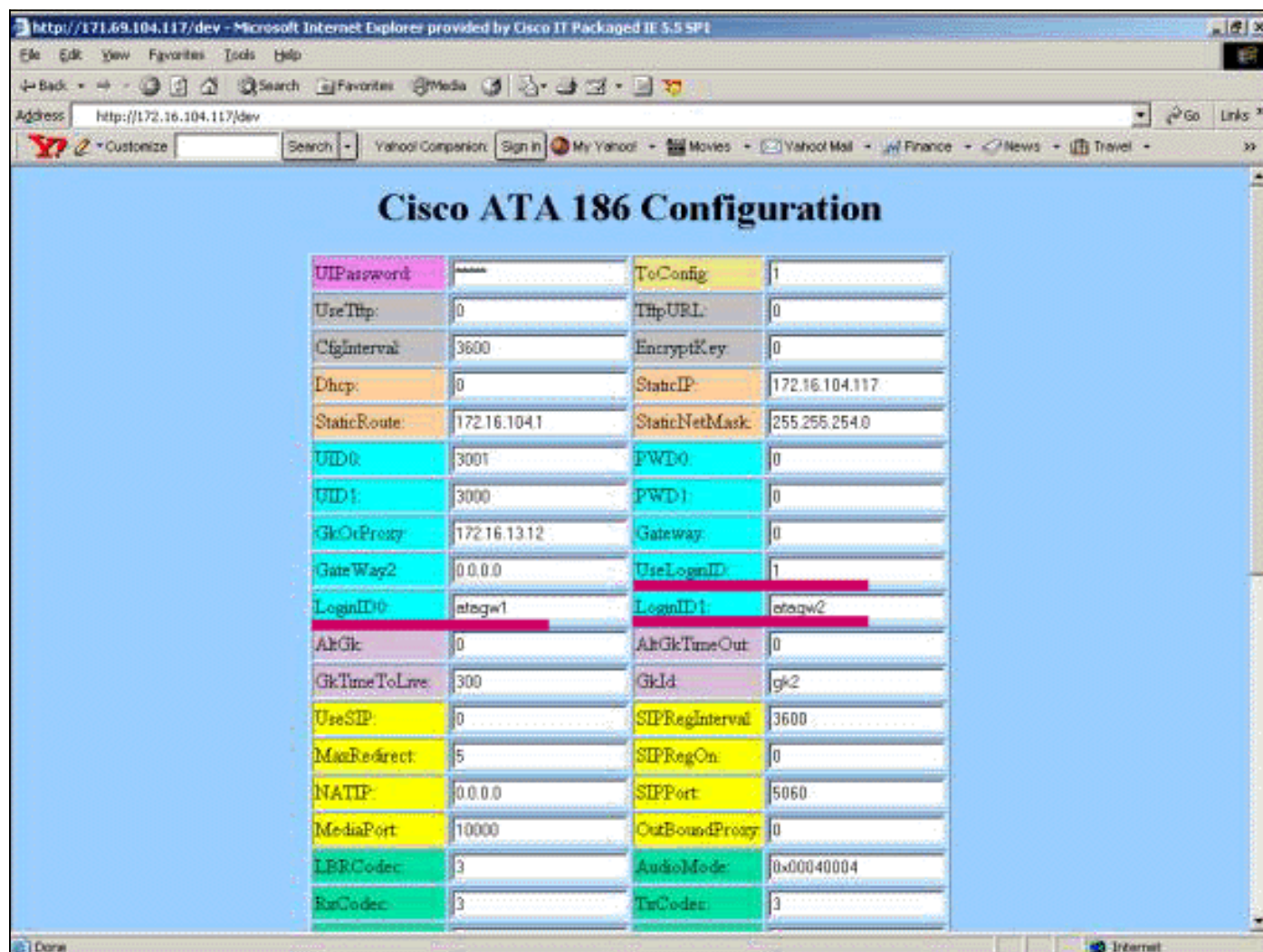
Depuis la version 2.12 du logiciel ATA, les options de cette section sont disponibles pour ajouter la sécurité.

Authentifier le point de terminaison au niveau du contrôleur d'accès avec un ID H.323

Procédez comme suit pour configurer l'ATA 186 afin de l'enregistrer avec l'ID H.323 :

1. Définissez le champ AutMethod sur 0 (la valeur par défaut est 1). La valeur hexadécimale à configurer pour ce champ est 0x0.
2. Définissez le champ UseLoginID sur 1.
3. Configurez LoginID0 et LoginID1 avec les ID H.323 pour l'ATA 186. L'ATA 186 s'enregistre comme deux terminaux H.323 différents, un pour chaque port.

Voici un exemple de configuration de travail pour le contrôleur d'accès lors de l'utilisation d'ATA avec la méthode d'authentification H.323 ID :



Parameter	Value	Parameter	Value
UIPassword	*****	ToConfig	1
UseHttp	0	HttpURL	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	172.16.13.12	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
LCRCCodec	3	AudioMode	0x00040004
ExCodec	3	TxCodec	3

Contrôleur d'accès 2610

```
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 !

```

[Authentifier le point de terminaison au niveau du contrôleur d'accès avec une adresse E.164](#)

Procédez comme suit pour configurer l'ATA 186 afin de l'enregistrer avec l'adresse E.164 :

1. Définissez le champ AutMethod sur **0** (la valeur par défaut est 1). La valeur hexadécimale à configurer pour ce champ est 0x0.
2. Définissez le champ UseLoginID sur **0**. L'ATA utilise les champs UID0 et UID1 pour être authentifié par le contrôleur d'accès.

Voici un exemple de configuration de travail pour le contrôleur d'accès et la passerelle lors de l'utilisation d'ATA avec la méthode d'authentification E.164 ID :

Contrôleur d'accès 2610

```

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 !

```

[Authentifier le point de terminaison au niveau du contrôleur d'accès avec un ID H.323 et un mot de passe](#)

Procédez comme suit pour configurer l'ATA 186 pour l'enregistrement avec l'ID et le mot de passe H.323 :

1. Définissez le champ AutMethod sur **1** (la valeur par défaut est 1). La valeur hexadécimale à configurer pour ce champ est 0x1. Ce champ est défini pour indiquer que l'ATA recherche maintenant le mot de passe.
2. Définissez le champ UseLoginID sur **1**.
3. Configurez LoginID0 et LoginID1 avec les ID H.323 pour l'ATA 186. L'ATA 186 s'enregistre comme deux terminaux H.323 différents, un pour chaque port.
4. Configurez PWD0 et PWD1 avec le mot de passe de chaque port. **Remarque** : l'ATA utilise le mot de passe pour générer le jeton. Ce jeton est envoyé au contrôleur d'accès pour

authentification.

5. Configurez NTP avec l'adresse IP du serveur NTP (Network Time Protocol). Le contrôleur d'accès et l'ATA doivent avoir des horloges synchronisées avec le même serveur NTP.

Remarque : l'horodatage est utilisé pour la génération de jetons. Pour plus d'informations, reportez-vous au [Guide de dépannage de la sécurité de Gateway to Gatekeeper \(H.235\) et Gatekeeper to Gatekeeper \(IZCT\)](#).

Voici un exemple de configuration de travail pour le contrôleur d'accès et la passerelle lors de l'utilisation d'ATA avec la méthode d'authentification H.323 ID et mot de passe :

```
Contrôleur d'accès 2610

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 !
```

Remarque : Pour plus d'informations sur la sécurité du contrôleur d'accès, reportez-vous au [Guide de dépannage de sécurité de Gateway to Gatekeeper \(H.235\) et de Gatekeeper to Gatekeeper \(IZCT\)](#).

[Authentifier le point de terminaison au niveau du contrôleur d'accès avec une adresse et un mot de passe E.164](#)

Procédez comme suit pour configurer l'ATA 186 pour l'enregistrement avec l'ID et le mot de passe E.164 :

1. Définissez le champ AutMethod sur 1 (la valeur par défaut est 1). La valeur hexadécimale à configurer pour ce champ est 0x0. Ce champ est défini pour indiquer que l'ATA recherche maintenant le mot de passe.
2. Définissez le champ UseLoginID sur 0.
3. Configurez UID0 et UID1 avec les ID E.164 pour l'ATA 186. L'ATA 186 s'enregistre comme deux terminaux H.323 différents, un pour chaque port.
4. Configurez PWD0 et PWD1 avec le mot de passe de chaque port. **Remarque :** l'ATA utilise le mot de passe pour générer le jeton. Ce jeton est envoyé au contrôleur d'accès pour authentification.
5. Configurez NTP avec l'adresse IP du serveur NTP. Le contrôleur d'accès et l'ATA doivent avoir des horloges synchronisées avec le même serveur NTP.

Remarque : l'horodatage est utilisé pour la génération de jetons. Pour plus d'informations, reportez-vous au [Guide de dépannage de la sécurité de Gateway to Gatekeeper \(H.235\) et Gatekeeper to Gatekeeper \(IZCT\)](#).

Voici un exemple de configuration de travail pour le contrôleur d'accès et la passerelle lors de l'utilisation d'ATA avec l'ID E.164 et la méthode d'authentification par mot de passe :

```
Contrôleur d'accès 2610

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 !
```

Remarque : Pour plus d'informations sur la sécurité du contrôleur d'accès, reportez-vous au [Guide de dépannage de sécurité de Gateway to Gatekeeper \(H.235\) et de Gatekeeper to Gatekeeper \(IZCT\)](#).

[Authentifier le point de terminaison au niveau du contrôleur d'accès avec un ID H.323 et un mot de passe à l'aide du séparateur](#)

Procédez comme suit pour configurer l'ATA 186 pour l'enregistrement avec l'ID et le mot de passe H.323 :

1. Définissez le champ AutMethod sur **1** (la valeur par défaut est 1). La valeur hexadécimale configurée pour ce champ est 0x1. Ce champ est défini pour indiquer que l'ATA recherche maintenant le mot de passe.
2. Définissez le champ UseLoginID sur **1**.
3. Configurez LoginID0 et LoginID1 avec les ID H.323, suivis du séparateur et du mot de passe de l'ATA 186. Par exemple, LoginID0 est **atagw1=cisco**. L'ATA 186 s'enregistre comme deux terminaux H.323 différents, un pour chaque port. **Remarque :** l'ATA utilise le mot de passe pour générer le jeton. Ce jeton est envoyé au contrôleur d'accès pour authentification.
4. Configurez NTP avec l'adresse IP du serveur NTP. Le contrôleur d'accès et l'ATA doivent avoir des horloges synchronisées avec le même serveur NTP.

Remarque : l'horodatage est utilisé pour la génération de jetons. Pour plus d'informations, reportez-vous au [Guide de dépannage de la sécurité de Gateway to Gatekeeper \(H.235\) et Gatekeeper to Gatekeeper \(IZCT\)](#).

Voici un exemple de configuration de travail pour le contrôleur d'accès et la passerelle lorsque vous utilisez ATA avec la méthode d'authentification H.323 ID et mot de passe à l'aide d'un séparateur :

```
Contrôleur d'accès 2610

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 !

```

Remarque : Pour plus d'informations sur la sécurité du contrôleur d'accès, reportez-vous au [Guide de dépannage de sécurité de Gateway to Gatekeeper \(H.235\) et de Gatekeeper to Gatekeeper \(IZCT\)](#).

Vérification

L'exemple de cette section montre l'enregistrement du point de terminaison du contrôleur d'accès.

Pour vérifier la configuration, exécutez la commande **show gatekeeper endpoint**.

```

                                     GATEKEEPER ENDPOINT
REGISTRATION

CallSignalAddr  Port  RASignalAddr  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

```

Remarque : l'ATA 186 s'enregistre en tant que terminal H.323 (**TERM**) et non en tant que passerelle H.323. Ceci est fait délibérément pour que seuls les appels destinés à l'ATA 186 lui soient envoyés.

Remarque : Vous ne pouvez pas avoir d'adresse dans le champ de passerelle ATA. Vous ne pouvez pas configurer l'ATA 186 pour qu'il fonctionne avec le contrôleur d'accès et la passerelle.

Dépannage

Cette section fournit des informations pour dépanner votre configuration.

L'adaptateur ATA 186 ne fournit pas de tonalité s'il n'est pas enregistré avec le contrôleur d'accès. Si l'ATA 186 ne s'enregistre pas auprès du contrôleur d'accès, vérifiez les éléments suivants :

- Il existe une connectivité IP entre l'ATA 186 et le contrôleur d'accès.
- Les champs UID0 et UID1 ATA 186 sont configurés correctement. Si les champs UID sont définis sur 0, l'ATA 186 ne tente pas de s'enregistrer auprès du contrôleur d'accès. Au moins, le champ UID0 doit être une valeur différente de zéro, pour que l'ATA 186 démarre le processus d'enregistrement. Si les deux ports ATA 186 (UID0 et UID1) ont des adresses

E.164 non nulles, l'ATA 186 tente de s'enregistrer avec les deux ports. L'ATA 186 ne fournit pas de tonalité, même si l'un des ports ne peut pas s'enregistrer.

- Le contrôleur d'accès est configuré correctement. Si le contrôleur d'accès est configuré avec un préfixe de zone locale, l'adresse E.164 de l'ATA 186 doit être incluse. Si la sécurité est configurée sur le contrôleur d'accès, l'ATA 186 doit être configuré en conséquence.

En outre, vérifiez que le champ UseSIP est défini sur 0. Ceci est nécessaire pour configurer l'ATA 186 en mode H.323. Si le champ UseSIP est défini sur 1, l'ATA 186 n'envoie pas la demande d'enregistrement au contrôleur d'accès.

Dépannage du contrôleur d'accès

Lorsque la sécurité est configurée, émettez la commande [debug aaa authentication](#).

Si aucune sécurité n'est configurée, émettez la commande [debug ras](#).

Remarque : l'ATA 186 s'enregistre séparément pour les deux ports vocaux. L'ATA 186, par conséquent, est authentifié deux fois plus de terminaux H.323 différents, comme indiqué dans ce débogage :

```
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'
```

Pour plus d'exemples de dépannage, référez-vous à [Dépannage des problèmes d'enregistrement du contrôleur d'accès](#).

Dépannage de l'ATA 186

Lorsque vous travaillez avec des contrôleurs d'accès et des passerelles tiers, l'outil de dépannage de l'ATA 186 est très utile. Pour activer l'outil de dépannage ATA 186, procédez comme suit :

1. Dans le champ ATA Nprintf, configurez l'adresse IP du PC qui se trouve sur le même sous-réseau que l'ATA 186.
2. Le port spécifié après l'adresse doit être **9001**.
3. À l'invite DOS sur le PC, lancez le programme **conservateur.exe**.

Vous pouvez télécharger le programme conservateur.exe à partir du [Cisco Software Center](#) (clients [enregistrés](#) uniquement).

Le programme conservateur.exe est inclus dans le dernier fichier ZIP de version du logiciel ATA 186.

[Exemples de débogages pour les appels effectués à partir de l'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:MsAck

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
```

Exemple de débogage ATA de tonalité nulle

Les deux ports vocaux ont besoin d'une adresse E.164 unique, sinon l'ATA reçoit un Rejeter du contrôleur d'accès. Pendant ce temps, l'ATA 186 sera enregistré avec un port vocal en tant que terminal H.323, mais il n'y aura pas de tonalité.

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

Informations connexes

- [Configuration de base Cisco ATA 186](#)
- [Configuration et dépannage d'un ATA 186 avec une passerelle Cisco IOS](#)
- [Contrôleur d'accès hautes performances Cisco : configuration du contrôleur d'accès](#)
- [Configuration de la voix sur IP](#)
- [Assistance technique concernant la technologie vocale](#)
- [Assistance concernant les produits vocaux et de communications unifiées](#)
- [Dépannage des problèmes de téléphonie IP Cisco](#)
- [Support et documentation techniques - Cisco Systems](#)