

# Configuration du contrôleur d'accès Cisco CallManager 3.3

## Contenu

[Introduction](#)

[Conditions préalables](#)

[Conditions requises](#)

[Composants utilisés](#)

[Conventions](#)

[Configurez le garde-porte et le joncteur réseau dans le Cisco CallManager](#)

[Ajoutez un garde-porte](#)

[Ajoutez un joncteur réseau H.225 contrôlé par garde-porte](#)

[Configurez le garde-porte sur le routeur](#)

[Configuration du contrôleur d'accès d'échantillon](#)

[Debugs](#)

[Suivi de Cisco CallManager](#)

[Vérifiez](#)

[Dépannez](#)

[Informations connexes](#)

## [Introduction](#)

Un périphérique de garde-porte, également connu sous le nom de Fonction Cisco Multimedia Conference Manager (MCM), prend en charge l'enregistrement H.225, l'admission, et le message de Protocol d'état (RAS) réglé qui est en service pour le contrôle d'admission d'appel, l'allocation de bande passante, et la résolution de modèle de cadran (routage d'appels). Le garde-porte peut fournir ces services pour des transmissions entre les batteries de Cisco CallManager et H.323 les réseaux. Vous pouvez configurer de plusieurs périphériques de garde-porte pour chaque batterie de Cisco CallManager aussi bien que configurer les garde-portes alternatifs pour la Redondance. Pour les détails alternatifs de configuration du contrôleur d'accès, référez-vous à la [documentation MCM](#).

La configuration du contrôleur d'accès avec le Cisco CallManager comporte de ces deux étapes :

1. [Configurez le garde-porte et le joncteur réseau dans le Cisco CallManager.](#)
2. [Configurez le garde-porte sur le routeur.](#)

## [Conditions préalables](#)

### [Conditions requises](#)

Ce document est destiné pour le personnel de réseau qui déploient les réseaux de Téléphonie sur IP. Les lecteurs de ce document devraient avoir connaissance des sujets suivants :

1. Configuration de voix sur ip
2. Concepts de Téléphonie sur IP

## Composants utilisés

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

- SpB de version 3.3(2) de Cisco CallManager - 171.69.85.171
- Version c3640-ix-mz.122-15.T2 du garde-porte IOS® - 172.16.13.7

Les informations contenues dans ce document ont été créées à partir des périphériques d'un environnement de laboratoire spécifique. Tous les périphériques utilisés dans ce document ont démarré avec une configuration effacée (par défaut). Si votre réseau est opérationnel, assurez-vous que vous comprenez l'effet potentiel de toute commande.

## Conventions

Pour plus d'informations sur les conventions utilisées dans ce document, reportez-vous aux [Conventions relatives aux conseils techniques Cisco](#).

## Configurez le garde-porte et le joncteur réseau dans le Cisco CallManager

Chaque batterie de Cisco CallManager peut s'inscrire à un ou plusieurs garde-portes. Cette section décrit comment configurer le garde-porte dans le Cisco CallManager. Vous devez également configurer des périphériques de joncteur réseau à la page de configuration de joncteur réseau. Voyez la section de [configuration de joncteur réseau](#) pour des détails.

## Ajoutez un garde-porte

Employez cette procédure afin d'ajouter un périphérique de garde-porte.

1. Sélectionnez le **périphérique** > le **garde-porte** afin d'afficher la page de configuration du contrôleur d'accès.
2. Écrivez les paramètres appropriés. Voir le [tableau 1](#) pour des informations sur différentes options. Les valeurs par défaut sont utilisées pour cette installation.
3. **Insertion de clic** afin d'ajouter le nouveau garde-porte. La liste de The Gatekeepers affiche les mises à jour de page, et le nom du nouveau garde-porte.

## Options de configuration du contrôleur d'accès

Le tableau 1 décrit les configurations de configuration du contrôleur d'accès.

Tableau 1 :

Champ	Description
Nom d'hôte/adresse IP	Écrivez le nom d'adresse IP ou de Système de noms de domaine (DNS) du garde-porte dans le champ approprié. Vous pouvez enregistrer de plusieurs garde-portes pour chaque batterie de Cisco CallManager.
Description	Écrivez un nom descriptif pour le garde-porte.
Time to Live de demande d'enregistrement	Ne changez pas cette valeur à moins que vous ayez une instruction de faire ainsi par un ingénieur de support technique de Cisco. Écrivez le temps en quelques secondes. La valeur par défaut spécifie 60 secondes. Le champ de Time to Live de demande d'enregistrement indique la durée que le garde-porte considère une demande d'enregistrement (RRQ) valide. Le système doit envoyer une keepalive RRQ au garde-porte avant le Time to Live RRQ expire. Le Cisco CallManager envoie un RRQ au garde-porte afin d'enregistrer et mettre à jour ultérieurement une connexion avec le garde-porte. Le garde-porte peut confirmer (RCF) ou refuser (RRJ) la demande.
Délai d'attente de relance d'enregistrement	Ne changez pas cette valeur à moins que vous ayez une instruction de faire ainsi par un ingénieur de support technique de Cisco. Écrivez le temps en quelques secondes. La valeur par défaut spécifie 300 secondes. Le champ de délai d'attente de relance d'enregistrement indique la durée que le Cisco CallManager attend avant qu'il relance l'enregistrement de garde-porte après qu'une tentative défectueuse d'enregistrement.
Périphérique d'enable	Cette case te permet pour enregistrer ce garde-porte avec le Cisco CallManager. Par défaut, cette case reste cochée. L'unregister le garde-porte du Cisco CallManager, décochent cette case. Les unregisters de garde-porte dans approximativement une minute après que vous mettez à jour ce champ.

Vous pouvez configurer des joncteurs réseau dans la gestion de Cisco CallManager afin de fonctionner dans l'un ou l'autre de ces manières :

- Joncteurs réseau contrôlés par Non garde-porte
- [Joncteurs réseau garde-porte Garde-porte](#)

**Note:** Ce document se concentre *seulement* sur la façon configurer les joncteurs réseau H.225 garde-porte Garde-porte.

[Joncteur réseau garde-porte Garde-porte](#)

Dans ce cas, il est suffisant communiquer un joncteur réseau simple d'intercluster avec toutes les batteries distantes. De même, un joncteur réseau H.225 simple est nécessaire pour communiquer avec tous les points finaux H.323 garde-porte garde-porte. Vous devez également configurer des modèles d'artère ou conduire des groupes afin de conduire les appels à et du garde-porte. Dans cette configuration, le garde-porte détermine dynamiquement l'adresse IP appropriée pour la destination de chaque appel à un périphérique distant, et les utilisations locales de Cisco CallManager cette adresse IP afin de se terminer l'appel.

Cette configuration fonctionne bien dans de grands aussi bien que plus réduits systèmes. Pour de grands systèmes où beaucoup de batteries existent, aides de cette configuration afin d'éviter la configuration de différents joncteurs réseau d'intercluster entre chaque batterie.

Si vous configurez les joncteurs réseau garde-porte garde-porte, le Cisco CallManager crée automatiquement un périphérique de jonction virtuelle. L'adresse IP de ce périphérique change dynamiquement afin de refléter l'adresse IP du périphérique distant que le garde-porte détermine. Utilisez les joncteurs réseau quand vous configurez les modèles d'artère ou conduisez les groupes qui conduisent des appels à et d'un garde-porte.

### [Ajoutez un joncteur réseau H.225 contrôlé par garde-porte](#)

Employez cette procédure afin d'ajouter un joncteur réseau H.225 contrôlé par garde-porte.

1. Dans le **périphérique** > le **joncteur réseau** choisis de Cisco CallManager Administration, choisis **ajoutez un nouveau joncteur réseau**. Vous voyez alors une autre page.
2. Le **joncteur réseau H.225** choisi (garde-porte contrôlé) et sélectionnent alors **ensuite**. Vous voyez alors une autre page.
3. Spécifiez le nom du périphérique et les informations de Pool d'appareils. Dans cette configuration toutes autres valeurs sont laissées en tant que par défaut.
4. À la même page spécifiez l'adresse IP et le terminal type de garde-porte. Dans la section de préfixe de technologie spécifiez la technologie appropriée (par exemple le préfixe 1#\*) et dans la case de zone sélectionnez la zone appropriée (par exemple SJGK1).
5. Sélectionnez l'**insertion** et la sélectionnez **CORRECT** au message qui indique pour remettre à l'état initial le joncteur réseau.
6. La page régénère. Le **joncteur réseau** choisi de **remise** et choisissent la **reprise** ou la **remise** convenablement.

### [Configuration d'un schéma d'acheminement](#)

Configurez un modèle d'artère afin de conduire des appels à chaque joncteur réseau garde-porte garde-porte.

Référez-vous à la [configuration de modèle d'artère](#) pour de plus amples informations.

Dans la configuration de modèle d'artère, spécifiez le modèle pour conduire l'appel vers le périphérique de joncteur réseau.

Ce graphique représente un exemple de la façon configurer un modèle d'artère dans le Cisco CallManager. Utilisez le modèle approprié d'artère selon votre plan de routage.

### [Configurez le garde-porte sur le routeur](#)

Le Cisco CallManager s'inscrit à un garde-porte avec l'utilisation de son adresse IP et H.323 de l'ID. Vous pouvez spécifier l'adresse IP de CallManager dans une de ces manières :

- En configuration statique, employez la commande de **<address> d'ipaddr gw de <prefix> de [gw-type-prefix](#)** sur le garde-porte afin de spécifier chaque adresse IP de Cisco CallManager explicitement.
- En configuration dynamique, quand un Cisco CallManager s'inscrit au garde-porte, il envoie son adresse IP et le préfixe spécifié de technologie au garde-porte. Le garde-porte enregistre alors ce Cisco CallManager comme appareil voip garde-porte valide.

Afin de spécifier la plage numérique de répertoire pour un Cisco CallManager particulier, utilisez la commande de [zone prefix](#) de configurer la plage sur le garde-porte. Par exemple, cette commande spécifie le DN pour la zone SJGK1 qui commence à partir de 408-527.

```
zone prefix SJGK1 408527*
```

Le nombre maximal d'appels actifs qui sont permis pour chaque zone dépend des codecs en service pour chaque appel et la bande passante qui est allouée pour la zone. Le Cisco CallManager demande des bandes passantes différentes pour différents codecs :

Codecs	Bande passante demandée de CallManager
G.711	128 kpbs
G.729	16 Kbit/s
G.723	14 Kbps

Les régions d'utilisation dans le Cisco CallManager afin de spécifier les codecs tapent. Employez la [commande bandwidth](#) sur le garde-porte afin de spécifier la bande passante disponible. Par exemple, cette commande alloue 512 Kbps à la zone SJGK1.

```
bandwidth total zone SJGK1 512
```

Avec une allocation de 512 Kbps, la zone SJGK1 dans cet exemple peut la prendre en charge jusqu'à :

- 4 G.711 appels ou
- 32 G.729 appels ou
- 36 G.723 appels en même temps

**Note:** Dans un scénario où le garde-porte contrôle plusieurs zones, Cisco vous recommande se servent de la commande d'**interzone de bande passante**. La commande de **total de bande passante** peut entraîner des questions dans quelques configurations. Pour plus d'informations sur des considérations de garde-porte, référez-vous à la section de *configuration du contrôleur d'accès centralisée de [conception de réseaux de référence de solution Cisco de téléphonie IP](#)*.

## [Configuration du contrôleur d'accès d'échantillon](#)

```
interface FastEthernet0/0  
ip address 172.16.13.7 255.255.255.224
```

```
duplex auto
speed auto
```

```
gatekeeper
zone local SJGK1 cisco.com
zone prefix SJGK1 408*
gw-type-prefix 1#* default-technology
no shutdown
```

*!--- The Cisco CallManager trunks register and appear as VoIP-GW. 3640-1#show gatekeeper endpoints*

```
                GATEKEEPER ENDPOINT REGISTRATION
                =====
CallSignalAddr  Port  RASSignalAddr  Port  Zone Name      Type      Flags
-----
171.69.85.31    1720  171.69.85.31   4724   SJGK1          TERM
    E164-ID: 3166188111
171.69.85.171  4613  171.69.85.171  1160   SJGK1          VOIP-GW
    H323-ID: TrunkDevice1GK_1
Total number of active registrations = 2
```

Pour plus d'informations sur la façon configurer le garde-porte, référez-vous au [VoIP avec le garde-porte](#).

## Debugs

Dans cet exemple de scénario, le téléphone IP fait un appel pour H.323 le client de NetMeeting (NetMeeting est directement inscrit au garde-porte). Le Cisco CallManager envoie alors l'appel au garde-porte par le joncteur réseau de garde-porte. C'est la sortie pour le [debug ras](#) commandent sur le garde-porte.

```
Oct 15 06:06:22.595: RAS INCOMING PDU ::=

value RasMessage ::= admissionRequest :
{
  requestSeqNum 4343
  callType pointToPoint : NULL
  endpointIdentifier {"61C97A1000000001"}
  destinationInfo
  {
    dialedDigits : "3166188111"
  }
  srcInfo
  {
    dialedDigits : "4085273175"
  }
  srcCallSignalAddress ipAddress :
  {
    ip 'AB4555AB'H
    port 1720
  }
  bandwidth 1280
  callReferenceValue 8
  conferenceID '80480FB2D81C911D08000000AC10F07F'H
  activeMC FALSE
  answerCall FALSE
  canMapAlias TRUE
  callIdentifier
  {
    guid '80480FB2D81C911D08000000AC10F07F'H
```

```
    }
    gatekeeperIdentifier {"SJGK1"}
}
```

```
Oct 15 06:06:22.599: ARQ (seq# 4343) rcvd
Oct 15 06:06:22.603: H225 NONSTD OUTGOING PDU ::=
```

```
value ACFnonStandardInfo ::=
{
  srcTerminalAlias
  {
    e164 : "4085273175"
  }
  dstTerminalAlias
  {
    e164 : "3166188111"
  }
}
```

```
Oct 15 06:06:22.603: H225 NONSTD OUTGOING ENCODE BUFFER::= 00 01048073
B85A64A8 01048064 994BB444
Oct 15 06:06:22.603:
Oct 15 06:06:22.603: RAS OUTGOING PDU ::=
```

```
value RasMessage ::= admissionConfirm :
{
  requestSeqNum 4343
  bandwidth 1280
  callModel direct : NULL
  destCallSignalAddress ipAddress :
  {
    ip 'AB45551F'H
    port 1720
  }
  irrFrequency 240
  nonStandardData
  {
    nonStandardIdentifier h221NonStandard :
    {
      t35CountryCode 181
      t35Extension 0
      manufacturerCode 18
    }
    data '0001048073B85A64A801048064994BB444'H
  }
  willRespondToIRR FALSE
  uuiesRequested
  {
    setup FALSE
    callProceeding FALSE
    connect FALSE
    alerting FALSE
    information FALSE
    releaseComplete FALSE
    facility FALSE
    progress FALSE
    empty FALSE
  }
}
```

```
Oct 15 06:06:22.611: RAS OUTGOING ENCODE BUFFER::= 2B 8010F640 050000AB
45551F06 B800EF40 B5000012 11000104 8073B85A 64A
80104 8064994B B4442800 C0000100 020000
Oct 15 06:06:22.615:
```

```
Oct 15 06:06:22.615: IPSOCK_RAS_sendto: msg length 48 from 172.16.13.7:1719
to 171.69.85.171: 1160
Oct 15 06:06:22.615: RASLib::RASSendACF: ACF (seq# 4343) sent to 171.69.85.171
Oct 15 06:06:25.439: RecvUDP_IPSockData successfully rcvd message of
length 113 from 171.69.85.31:4724
Oct 15 06:06:25.439: RAS INCOMING ENCODE BUFFER::= 26 D0000B03 C0003600
31004200 38004600 41004500 38003000 30003000 300
03000 30003000 32020480 64994BB4 44048064 994BB444 00AB4555 1F06B800
00AB4555 AB06B800 013ED080 480FB2D8 1C911D08 000000
AC 10F07F44 E0200100 11008048 0FB2D81C 911D0800 0000AC10 F07F0100
Oct 15 06:06:25.443:
```

## Suivi de Cisco CallManager

```
!--- Cisco CallManager sends the RRQ to the gatekeeper. 10/14/2003 23:26:40.082 CCM|value
V2Message ::= registrationRequest : { requestSeqNum 4372, protocolIdentifier { 0 0 8 2250 0 2 },
discoveryComplete FALSE, callSignalAddress { ipAddress : { ip 'AB4555AB'H,
    !--- 171.69.85.171 is the IP address of the Cisco CallManager. port 4613 } },
rasAddress { ipAddress : { ip 'AB4555AB'H, port 1160 } }, terminalType { gateway { protocol {
h323 : { }, voice : { supportedPrefixes { { prefix e164 : "1#*"
    }
    }
    }
    }
    },
    },
    mc FALSE,
    undefinedNode FALSE
  },
  gatekeeperIdentifier "SJGK1",
  endpointVendor
  {
    vendor
    {
      t35CountryCode 181,
      t35Extension 0,
      manufacturerCode 18
    }
  },
  timeToLive 60,
  keepAlive TRUE,
  endpointIdentifier "61C97A1000000001"
}
```

```
!--- Registration is confirmed at this point (there is omission of some output). 10/14/2003
23:26:40.142 CCM|value V2Message ::= registrationConfirm : { requestSeqNum 4372,
protocolIdentifier { 0 0 8 2250 0 4 }, callSignalAddress { }, gatekeeperIdentifier "SJGK1",
  endpointIdentifier "61C97A1000000001",
  timeToLive 60,
  willRespondToIRR FALSE
}
```

```
!--- Cisco CallManager sends Admission Request (ARQ) to !--- the gatekeeper in order to place
the call. 10/14/2003 23:27:26.063 CCM|value V2Message ::= admissionRequest :
{
  requestSeqNum 4376,
  callType pointToPoint : NULL,
  endpointIdentifier "61C97A1000000001",
  destinationInfo
  {
    e164 : "3166188111"
```



```
!--- This is the phone number of the called !--- party that is the NetMeeting client. },
srcInfo { e164 : "4085273175"
!--- This is the phone number of the calling party !--- that is the IP phone. },
srcCallSignalAddress ipAddress : { ip 'AB4555AB'H, port 1720 }, bandwidth 1280,
callReferenceValue 13, conferenceID '806076A3DB1C911D0D000000AC10F07F'H, activeMC FALSE,
answerCall FALSE, canMapAlias TRUE, callIdentifier { guid '806076A3DB1C911D0D000000AC10F07F'H },
gatekeeperIdentifier "SJGK1"
}
```

```
!--- This line indicates the client that sends this request.
<NID::171.69.85.171><CT::1,100,90,1.1098993><IP::172.16.240.127>
```

```
!--- Here is the Advanced Communications Function (ACF) !--- message from the gatekeeper.
10/14/2003 23:27:26.093 CCM|value V2Message ::= admissionConfirm : { requestSeqNum 4376,
bandwidth 1280,
```

```
!--- For a G.711 call, the bandwidth confirmed is 128 kbps. callModel direct : NULL,
destCallSignalAddress ipAddress : { ip 'AB4555AB'H, port 4613 }, irrFrequency 240,
nonStandardData { nonStandardIdentifier h221NonStandard : { t35CountryCode 181, t35Extension 0,
manufacturerCode 18 }, data '0001048073B85A64A801048064994BB444'H }, willRespondToIRR FALSE,
uuiesRequested { setup FALSE, callProceeding FALSE, connect FALSE, alerting FALSE, information
FALSE, releaseComplete FALSE, facility FALSE, progress FALSE, empty FALSE } } !--- Cisco
CallManager displays the RAS information. 10/14/2003 23:27:26.143 CCM|SPROCRas - {
h323-uu-pdu
```

```
{
h323-message-body setup :
{
protocolIdentifier { 0 0 8 2250 0 2 },
sourceAddress
{
e164 : "4085273175",
h323-ID : "4085273175"
},
sourceInfo
{
terminal
{
},
mc FALSE,
undefinedNode FALSE
},
destinationAddress
{
e164 : "3166188111"
},
activeMC FALSE,
conferenceID '806076A3DB1C911D0D000000AC10F07F'H,
conferenceGoal create : NULL,
callType pointToPoint : NULL,
sourceCallSignalAddress ipAddress :
{
ip 'AB4555AB'H,
port 1720
},
callIdentifier
{
guid '806076A3DB1C911D0D000000AC10F07F'H
},
mediaWaitForConnect FALSE,
canOverlapSend FALSE
},
h245Tunneling FALSE,
nonStandardControl
{
{
```

```
nonStandardIdentifier h221NonStandard :
{
  |<CLID::ADESALU-SUNPC-Cluster><NID::171.69.85.171>
10/14/2003 23:27:26.143 CCM|t35CountryCode 181,
  t35Extension 0,
  manufacturerCode 18
},
data '80440400010100'H
}
}
```

## Vérifiez

Aucune procédure de vérification n'est disponible pour cette configuration.

## Dépannez

Il n'existe actuellement aucune information de dépannage spécifique pour cette configuration.

## Informations connexes

- [VoIP avec contrôleur d'accès](#)
- [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](#)