



# WebEx et la sécurité

**WebEx Communications France Sarl**

2 Rue de la Haye - BP 10901, 95731 ROISSY  
Charles de Gaulle Cedex, France

Tél. : 0800 945 177 ou 33 (0) 1 49 19 49 41, Fax : 33 (0) 1 49 19 49 42  
E-mail : france@webex.com

[www.webex.fr](http://www.webex.fr)

## Sommaire

Introduction	3
L'infrastructure sous-jacente	5
La sécurité des réunions WebEx	7
L'accréditation par des tiers	11
Conclusion	13



# Introduction

WebEx™ Communications, Inc. fournit des services de collaboration en temps réel à un nombre croissant d'entreprises dans le monde. Ces entreprises utilisent les applications WebEx pour de multiples activités telles que la vente, le marketing, la gestion de projet et le support client. WebEx compte des clients dans de nombreux secteurs d'activité, notamment dans la finance, l'industrie, le secteur high-tech et la santé. Dans la conception, le déploiement et la maintenance de son réseau, au sein de sa plate-forme et de ses applications, la sécurité des données est pour WebEx une priorité absolue. Ses offres répondent aux critères de sécurité des entreprises et des administrations les plus exigeantes, afin qu'elles puissent utiliser efficacement les services WebEx au quotidien en ayant l'assurance que leurs sessions de communication se déroulent en toute sécurité et en toute confidentialité.

L'objet de ce document est de fournir des informations sur les caractéristiques et les fonctionnalités de sécurité de données disponibles dans les différentes applications WebEx et inhérentes à l'infrastructure de communication MediaTone™ de WebEx.

Dans les pages qui suivent, nous examinerons :

- L'infrastructure MediaTone
- La sécurité des réunions WebEx
  - Configuration du site
  - Planifier une réunion
  - Lancer et rejoindre une réunion
  - Pendant la réunion
  - Sécurité au niveau de la couche de transport
  - Compatibilité avec les firewalls
  - Après la réunion
- L'accréditation par des tiers

Le lecteur de ce document est supposé être familiarisé avec les services et fonctionnalités de base de WebEx, notamment le réseau privé WebEx Mediatone Network. Les solutions de réunion en ligne et applications à valeur ajoutée de WebEx incluent :

- Meeting Center, pour la collaboration interactive des équipes ;
- Training Center, pour des formations efficaces via le Web ;
- Event Center, pour les séminaires à grande échelle sur le Web ;

*Dans la conception, le déploiement et la maintenance de son réseau, au sein de sa plate-forme et de ses applications, la sécurité des données est pour WebEx une priorité absolue. Ses offres répondent aux critères de sécurité des entreprises et des administrations les plus exigeantes.*



- Support Center, pour les sessions de support à distance ;
- Sales Center, pour les réunions commerciales en ligne ;
- SMARTtech, pour créer et administrer un réseau d'ordinateurs accessibles à distance ;
- GlobalWatch, pour le contrôle de performance des réunions.

WebEx offre également des services intégrés de conférence audio et VoIP, et de vidéoconférence mono- et multi-points.

Le lecteur doit se familiariser avec les principaux rôles existants dans les différentes applications WebEx : Hôte, Présentateur et Participants.

#### **Hôte**

L'hôte est la personne qui programme et lance la session WebEx. Il contrôle le déroulement de la réunion et, en tant que présentateur initial, peut accorder aux participants des privilèges de présentateur. L'hôte peut aussi lancer une conférence audio durant la réunion, verrouiller la salle et exclure des participants.

#### **Présentateur**

Le présentateur partage des présentations, des applications spécifiques ou la totalité de son poste de travail. Il contrôle les outils d'annotation et peut accorder et révoquer le droit des participants à contrôler à distance les applications et le poste de travail partagés.

#### **Participant**

Le participant a des responsabilités minimales et son rôle se limite généralement à la visualisation du contenu de la session.

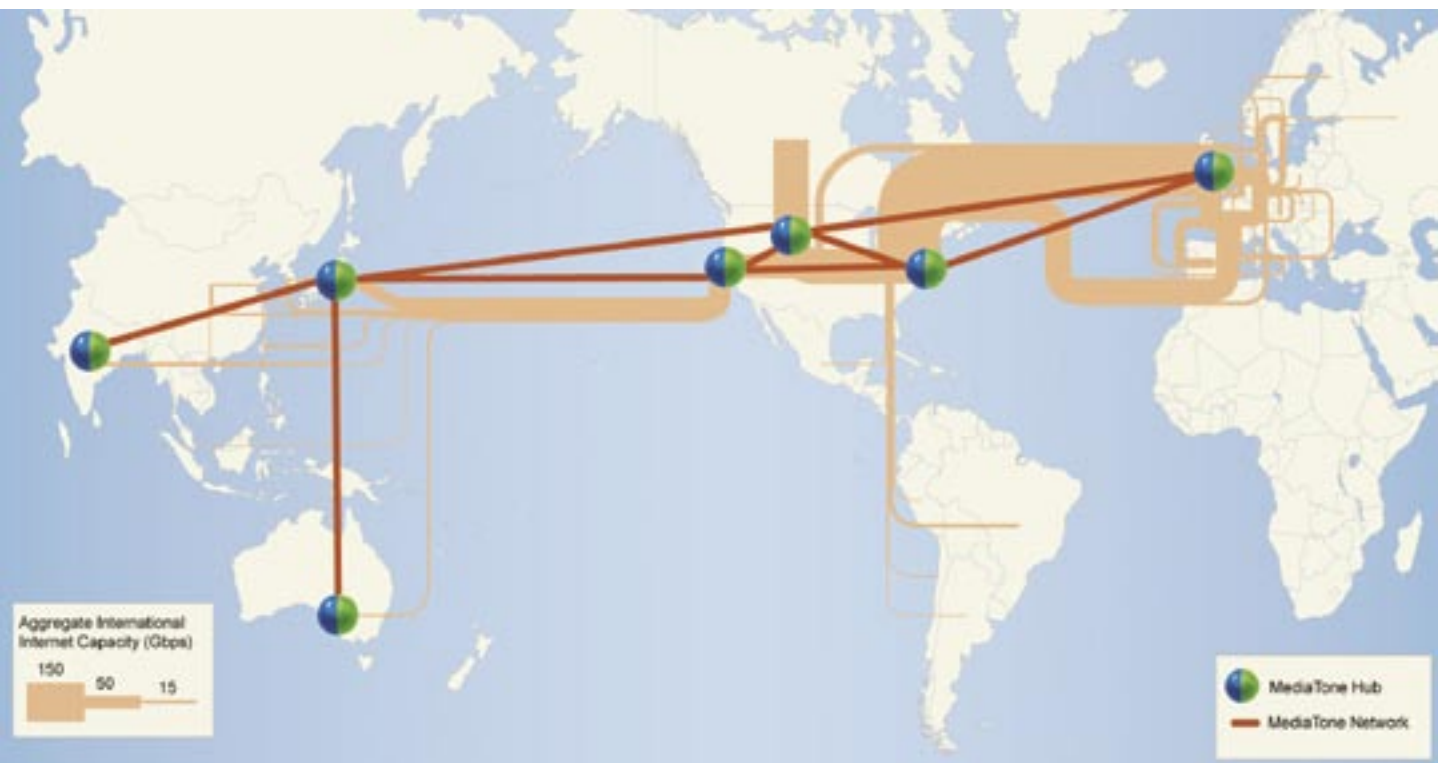
Sauf mention contraire, les caractéristiques décrites dans ce document s'appliquent à tous les services et applications WebEx.



# L'infrastructure sous-jacente

## Le réseau WebEx MediaTone Network

Le WebEx MediaTone Network est une infrastructure de réseau spécialement conçue et construite pour les communications Web en temps réel. Le réseau se compose d'une série de centres de données répartis dans le monde entier et stratégiquement localisés près des principaux points d'accès Internet. Entre les centres de données WebEx, le trafic est acheminé sur un réseau dédié haut débit.



## Une architecture commutée

WebEx est le seul fournisseur à avoir déployé un réseau distribué mondial de commutateurs MediaTone (MediaTone Switch). Grâce à cette architecture exclusive, les données d'une session issues de la machine du présentateur et arrivant sur celles des participants sont transportées et aiguillées – mais jamais stockées de manière permanente – sur WebEx MediaTone Network. Cette organisation diffère de celle des autres solutions de réunion en ligne qui utilisent un modèle à base de serveurs où les contenus sensibles peuvent être stockés durablement sur les serveurs du fournisseur. Contrairement à ce modèle, les sessions WebEx sont totalement éphémères et fonctionnent de la même manière qu'une communication vocale sur une ligne téléphonique standard. Outre une sécurité inégalée, cette architecture offre une infrastructure hautement disponible et extrêmement évolutive qui échappe aux limitations physiques imposées par les solutions à base de serveurs locaux.



*Spécialisé et certifié, le personnel de sécurité de WebEx est également régulièrement formé par les fournisseurs et les experts du secteur pour rester à la pointe des problématiques et des méthodes de sécurité.*

## **Les centres de données**

Le contenu des sessions WebEx est distribué grâce aux équipements installés dans les centres de données créés et exploités par WebEx. Ces centres sont situés à Mountain View, Californie ; Denver, Colorado ; Reston, Virginie ; Londres, Royaume-Uni ; et Tokyo, Japon. Chacun de ces centres fonctionne 24h/24 – 7j/7. WebEx a aussi des nœuds de communication à Melbourne (Australie) et Bangalore (Inde).

L'accès à ces installations est strictement réservé aux personnes figurant sur la liste d'approbation d'accès gérée par l'équipe de sécurité de WebEx décrite ci-après. Des systèmes de sécurité biométriques complètent le dispositif de contrôle d'accès.

## **L'équipe de sécurité**

WebEx a un département dédié à la sécurité qui est placé sous l'autorité directe du CIO de la société. Cette équipe comprend un analyste légiste certifié GIAC (Global Information Assurance Certification), deux spécialistes de la sécurité des systèmes d'information (CISSP), un analyste d'intrusions certifié GIAC et un spécialiste de la gestion des systèmes de sécurité (ISSMP). Spécialisé et certifié, le personnel de sécurité de WebEx est également régulièrement formé par les fournisseurs et les experts du secteur pour rester à la pointe des problématiques et des méthodes de sécurité.

La séparation des responsabilités qui existe entre le personnel de sécurité et les autres équipes de WebEx est un facteur important qui a notamment permis à la société d'obtenir les certifications WebTrust et SAS-70 de Type II (présentées plus loin dans ce document).



### Les hôtes ont accès aux fonctionnalités suivantes :

- Lancer/planifier une réunion WebEx ;
- Attribuer/révoquer des privilèges « Présentateur » ;
- Attribuer/révoquer des privilèges « Hôte » ;
- Mettre fin à une session de partage d'application pour tous les participants ;
- Limiter l'accès à une réunion commencée ;
- Exclure des participants ;
- Mettre fin à la réunion ;
- Activer/désactiver les fonctionnalités intégrées de téléconférence pour chaque participant ;
- Prendre des notes à l'aide des fonctionnalités intégrées de prise de notes, accorder ce privilège à un participant et envoyer ces notes à chaque participant avant de clore la réunion.

### Les présentateurs ont accès aux fonctionnalités suivantes :

- Voir la liste des participants à la session ;
- Permettre/interdire aux participants de sauvegarder ou d'imprimer les présentations ou les documents partagés pendant la session ;
- Permettre/interdire aux participants de changer de page dans une présentation ou un document partagé ;
- Permettre/interdire aux participants d'envoyer des messages texte aux autres participants, au présentateur ou aux deux ;
- Permettre/interdire aux participants d'enregistrer la session ;
- Céder temporairement à un participant le contrôle d'une application partagée.
- Suspendre temporairement le partage d'application ou d'ordinateur pour que les participants ne puissent pas voir ce que fait le présentateur, par exemple quand il veut accéder en toute sécurité à des parties sensibles de l'application ;
- Fonctionnalités garantissant la confidentialité des échanges (Chat privé, annotations prise de notes etc) entre les participants en cours de brevetage.

## La sécurité des réunions WebEx

### Configuration du site de réunions WebEx

Le module WebEx Site Administration permet aux clients d'appliquer leurs règles de sécurité à l'ensemble de leur site WebEx. Par exemple, la fonctionnalité permettant au présentateur de partager son poste de travail peut être désactivée de manière permanente. Les autorisations accordées à ce niveau s'appliquent à toutes les sessions créées sur le site. Les autres fonctions de sécurité au niveau de la configuration du site par l'administrateur couvrent :

- L'interdiction de lister les réunions ;
- La saisie obligatoire de l'adresse e-mail des participants ;
- La saisie obligatoire de mot de passe ;
- La définition des critères de mot de passe ;
- Les restrictions d'accès au site – L'administrateur peut décider que l'authentification est obligatoire pour tous les utilisateurs – hôtes et participants. Il peut ainsi s'assurer que toute personne accédant au site, que ce soit pour consulter des informations (par exemple la liste des réunions) ou accéder à une réunion, a préalablement été authentifiée ;
- L'approbation préalable des demandes de « Mot de passe oublié » ;
- L'obligation d'attribuer un mot de passe à chaque réunion.

### Planifier une réunion

En plus des paramètres de sécurité définis au niveau du site, un hôte peut paramétrer les contrôles d'accès suivants :

*(NB : les hôtes ne peuvent pas annuler les paramètres définis au niveau du site)*

#### • Réunion listée ou non-listée

— Cette option permet aux hôtes de faire figurer ou non leurs réunions sur le calendrier. Elles ne sont en outre accessibles que par un lien envoyé via le processus d'invitation par mail ou, à partir de la page d'accueil de la réunion, et ce par les participants en possession du numéro de cette réunion. Dans ce cas, l'hôte doit explicitement avoir informé les participants de l'existence de la réunion.

#### • Réunion ouverte ou protégée par un mot de passe

— L'hôte peut demander aux participants de saisir un mot de passe avant de rejoindre la réunion et peut également exclure le mot de passe de la réunion des mails d'invitation.

*Pour mieux comprendre le format UCF, on peut le comparer au format PDF. Un PDF est une représentation chiffrée et allégée de l'objet original. Le contenu encodé ne contient aucun élément original mais seulement une représentation de ces éléments qui est interprétée par le viewer Adobe Acrobat. WebEx Meeting Service Manager fonctionne de la même manière. Sur la machine du présentateur, il crée une représentation codée de l'objet original et envoie cette représentation aux participants. Les contenus encodés ne contiennent aucun élément de la présentation source et ne peuvent être lus que par le WebEx Meeting Service Manager. Cette approche présente deux avantages majeurs : une moindre consommation de bande passante, les éléments encodés étant de deux à trois fois plus légers que la source, et une plus grande sécurité dans la mesure où aucun texte en clair ni contenu original ne sort de la machine du présentateur.*

*Une fois que le WebEx Meeting Service Manager a encodé le contenu de la présentation sur la machine du présentateur, il attribue au contenu un identifiant (session ID) connu uniquement de lui et du Meeting Service Manager de chaque participant. WebEx utilise cette technique pour empêcher d'éventuels hackers de reconstituer le contenu des sessions.*

- **Participation sur invitation**

— Pour mieux contrôler les accès, l'hôte peut utiliser une « liste de contrôle d'accès » par le biais des fonctions d'invitation et spécifier que seuls les utilisateurs invités à la réunion peuvent y participer, à condition d'avoir répondu à l'invitation et d'avoir été explicitement acceptés par l'hôte.

Si cette mesure n'est pas déjà activée au niveau du site, l'hôte peut choisir de ne pas envoyer d'e-mail d'invitation, ce qui lui permet de garder le contrôle sur la diffusion des informations d'accès à la réunion.

Les clients peuvent utiliser et combiner à leur guise les fonctionnalités précédemment décrites pour créer un environnement WebEx conforme à leurs propres règles de sécurité.

## **Lancer et rejoindre une réunion**

Les réunions WebEx doivent être lancées par un hôte. Celui-ci doit s'identifier en saisissant son identifiant et son mot de passe pour accéder au site WebEx. Une fois authentifié, il peut lancer une réunion. L'hôte est celui qui a le premier niveau de contrôle de la réunion et en est le présentateur initial. A ce titre, il peut à tout moment accorder à tout participant des droits d'hôte ou de présentateur et les révoquer. Il peut aussi à tout moment mettre fin à la session pour tous les participants ou exclure ceux de son choix.

Le site WebEx peut être configuré pour permettre aux participants d'entrer en réunion avant l'hôte. Avant l'arrivée de l'hôte, les participants ne peuvent pas partager de présentations ni utiliser les autres fonctionnalités du service de réunion, à l'exception du chat.

## **La sécurité pendant la réunion**

Pendant la réunion, la sécurité est d'abord assurée par le WebEx Meeting Service Manager (gestionnaire de services de réunion). Cet outil est conçu pour délivrer en temps réel et de manière sécurisée des contenus multimédias à chaque participant d'une session WebEx. Les contenus qu'un présentateur partage avec les participants ne sont que des représentations des données originales. Ces contenus sont encodés au format WebEx UCF (Universal Communications Format), une technologie propriétaire optimisée pour le partage de contenus.

### **WebEx Meeting Service Manager :**

- Ne peut être appelé qu'à partir d'un navigateur Web et ne peut pas être lancé de manière indépendante ;
- Est numériquement signé par Verisign ;
- Est le seul moyen possible de participer à une session WebEx ;
- Est entièrement dépendant des connexions établies pour chaque session sur le réseau WebEx MediaTone ;



*Les paramètres de chaque session WebEx sont uniques et sont générés par le switch MediaTone. Pour pouvoir entrer dans une réunion, chaque participant authentifié doit, en plus du cookie de session, avoir accès à ces paramètres de session.*

- Prend en charge le processus d'encodage qui chiffre toutes les données partagées ;
- Chiffre tout le contenu des présentations partagées en utilisant la norme de chiffrement AES ;
- Crypte la connexion au réseau MediaTone en utilisant la norme de chiffrement SSL 128 bits ;
- Fournit une identification de chaque participant à la réunion.

Il est impossible de participer à une session WebEx sans l'étroite coordination entre le Meeting Service Manager et les switches du réseau MediaTone. Les données d'une session WebEx étant partagées via le Meeting Service Manager et celui-ci devant établir une connexion avec un switch MediaTone, ces paramètres de sécurité s'appliquent pendant toute la durée de la session. En résumé, chaque session est dynamique et implique une « poignée de main » entre le Meeting Service Manager et le switch MediaTone.

Pour rejoindre une réunion, chaque connexion WebEx Meeting Service Manager doit être authentifiée avant d'établir une connexion avec le switch MediaTone. Le processus d'authentification utilise un cookie unique par client et par session pour confirmer l'identité de chaque participant essayant d'entrer dans la session WebEx. Les paramètres de chaque session WebEx sont uniques et sont générés par le switch MediaTone. Pour pouvoir entrer dans une réunion, chaque participant authentifié doit, en plus du cookie de session, avoir accès à ces paramètres de session.

### **Sécurité au niveau de la couche de transport**

En plus de toutes les protections évoquées au niveau de la couche applicative, pour une sécurité extrême, WebEx chiffre par défaut tous les contenus de présentation en utilisant l'algorithme AES (Advanced Encryption Standard) et donne la possibilité de sécuriser totalement les contenus en cryptant le canal de communication entre le WebEx Meeting Service Manager et le switch MediaTone en créant un tunnel SSL (Secure Sockets Layer) 128 bits.

Au lieu d'utiliser le port 80 du firewall (trafic Internet HTTP standard) pour passer à travers le firewall, SSL utilise le port 443 (trafic HTTPS). Ceci permet aux clients de restreindre l'accès au port 80 sans affecter le trafic WebEx.

Enfin, les participants à une réunion WebEx se connectent au réseau WebEx MediaTone via une connexion logique ; il n'y a pas de connexion de poste à poste entre les machines locales. La connexion logique est contrôlée par le WebEx Meeting Service Manager et est exclusivement dédiée aux communications de la



*Les seules informations relatives à une session que WebEx conserve sont les EDR (Event Detail Records). WebEx les utilise à des fins de reporting ou de facturation.*

session WebEx. Il est par conséquent impossible d'utiliser cette connexion pour toute autre tâche que celles autorisées par le WebEx Meeting Service Manager.

### **Comptabilité avec les firewalls**

Le WebEx Meeting Service Manager se met en communication avec le switch WebEx pour établir une connexion fiable et sûre. Au moment de l'instanciation, c'est le WebEx Meeting Service Manager qui détermine la meilleure méthode de communication. Dans le processus d'établissement de cette connexion, le WebEx Meeting Service Manager essaie de se connecter en TCP (port 1270) ou en HTTP/HTTPS (ports 80/443). Très souvent le port 1270 est bloqué par un firewall. Dans ce cas, le WebEx Meeting Service Manager fait passer toutes les communications WebEx par un tunnel HTTP/HTTPS. Si le site WebEx incorpore une connexion SSL, tout le trafic est transporté en HTTPS (port 443). Quelle que soit la connexion établie au moment de l'instanciation, grâce à cette communication entre le Meeting Service Manager et le switch WebEx, aucune configuration spécifique des firewalls n'est nécessaire pour autoriser le passage des sessions WebEx.

### **Après la réunion**

Une fois la réunion terminée, aucune information de la session n'est conservée sur les switches Media ni sur les PC des participants. Si un hôte a choisi d'enregistrer cette session, l'enregistrement sera placé soit sur une machine cliente soit dans la zone sécurisée MyRecordings, séparée de l'environnement de communication partagé WebEx. Ce procédé est comparable à celui des messageries vocales et du téléphone. Les messages vocaux sont stockés à l'écart du réseau de communication, bien que celui puisse accéder aux messages. Le réseau lui-même ne conserve aucun contenu, qui se trouve dans les messages.

Les seules informations relatives à une session que WebEx conserve sont les EDR (Event Detail Records). WebEx les utilise à des fins de reporting ou de facturation. Les EDR sont stockés dans la base de données opérationnelle de WebEx et sont accessibles aux clients depuis leur site WebEx dès lors qu'ils se sont connectés en utilisant leur identifiant d'hôte. Ils peuvent aussi être téléchargés depuis le site WebEx ou via des API WebEx.



*Contrairement à tout autre label prétendant protéger les données privées du consommateur ou de l'entreprise, WebTrust est le seul certificat délivré par un tiers indépendant du demandeur. Pour conserver le sceau WebTrust, WebEx est soumis chaque année à un processus de re-certification.*

*Pour plus d'informations sur WebTrust, consulter le site :*

<http://www.webtrust.net/>



*SAS-70 est le cadre de référence qui permet à WebEx de divulguer ses activités et son processus de contrôle dans un format de reporting unifié.*

*Pour plus d'informations sur SAS 70, consulter le site :*

<http://www.sas70.com/>



## L'accréditation par des tiers

### WebTrust

WebEx a obtenu le sceau WebTrust par Ernst & Young LLP. WebTrust est un label de confiance décerné aux entreprises qui respectent en permanence les normes établies par l'American Institute of Chartered Public Accountants (AICPA) et le Canadian Institute of Chartered Accountants (CICA) reconnus dans le monde entier.

Le principe de sécurité WebTrust définit un cadre global pour la sécurité des données transmises sur Internet et stockées sur les systèmes de commerce électronique. Au cours d'un audit WebTrust, l'auditeur évalue l'adéquation du site aux critères WebTrust. Adossé à l'AICPA et au CICA, WebTrust est le seul sceau donnant aux clients l'assurance qu'ils peuvent faire confiance à l'entreprise certifiée et lui confier ce qu'ils ont de plus précieux : leurs informations privées.

La vérification indépendante est la clé de voûte de WebTrust. Contrairement à tout autre label prétendant protéger les données privées du consommateur ou de l'entreprise, WebTrust est le seul sceau délivré par un tiers indépendant du demandeur. Pour conserver le sceau WebTrust, WebEx est soumis chaque année à un processus de re-certification.

### SAS-70 de Type II

Ernst & Young LLP réalise également chaque année un audit SAS 70 de Type II de WebEx et fournit à la société le rapport correspondant. Développé par l'American Institute of Certified Public Accountants (AICPA), SAS 70 est une norme internationalement reconnue pour l'audit des organisations de services. L'audit SAS-70 de Type II est largement reconnu et signifie que les activités de contrôle de WebEx ont été soumises à des vérifications approfondies. Le rapport qui en résulte permet à WebEx de démontrer que la société a mis en place les contrôles et garanties appropriés pour traiter et manipuler les données appartenant à ses clients.

SAS-70 est le cadre de référence qui permet à WebEx de publier ses activités et son processus de contrôle dans un format de reporting unifié. L'audit SAS-70 de Type II et le rapport correspondant certifient qu'un auditeur indépendant (Ernst & Young) examine de manière continue les contrôles et garanties mis en place par WebEx pour assurer la confidentialité et la sécurité des données de ses clients. Le rapport d'audit SAS-70 de WebEx peut être communiqué aux équipes d'audit et de sécurité des entreprises clientes dans le cadre d'un accord de confidentialité.



### **L'engagement de WebEx**

WebEx considère que la confidentialité et la sécurité sont de la plus haute importance pour ses clients et ses partenaires. C'est pourquoi WebEx s'engage à :

- Faire appel à des auditeurs formés et certifiés WebTrust et SAS-70 pour contrôler ses procédures et ses règles de sécurité ;
- Appliquer les normes les plus élevées en vigueur sur Internet ;
- Auditer régulièrement son environnement de production pour maintenir sa sécurité au plus haut niveau.

### **Remarques sur la conformité HIPAA**

WebEx n'est pas une entreprise liée au secteur de la santé et n'a aucun contrôle sur le choix des contenus partagés par les utilisateurs pendant les sessions WebEx. Cependant, le réseau privé WebEx MediaTone Network est conçu de telle manière qu'aucune information partagée au cours d'une réunion WebEx n'est stockée ou conservée sur les switches WebEx. Cette architecture, associée aux dispositions de sécurité décrites dans ce document, permet aux entités concernées par l'HIPAA de se conformer aux directives de la loi se rapportant à l'utilisation, à la divulgation et au stockage des informations médicales.



## Conclusion

Partout dans le monde, des entreprises et des administrations utilisent au quotidien les applications et services de WebEx. Cela n'aurait jamais été possible si WebEx n'avait pas de tout temps veillé à intégrer des normes et des principes de sécurité rigoureux dans le développement et l'exploitation de son infrastructure et de ses services. La sécurité des données reste la plus haute priorité de WebEx. Cela permet à la société d'atteindre son principal objectif : fournir à ses clients les services de communication en temps réel les plus efficaces et les plus sûrs du marché.

©2005 WebEx Communications Inc. WebEx, WebEx MediaTone et le logo WebEx sont des marques déposées de WebEx Communications Inc. Tous droits réservés. Les autres marques citées sont la propriété de leurs détenteurs respectifs.

### Implantations commerciales :

Amériques & Canada

Tel. : +1.877.509.3239

[AmericasInfo@webex.com](mailto:AmericasInfo@webex.com)

China (Hong-Kong)

Tel. : + 852.8201.0228

[AsiaPacInfo@webex.com](mailto:AsiaPacInfo@webex.com)

France

Tel. : 0800.945.177

[france@webex.com](mailto:france@webex.com)

Inde

Tel. : 080.2228.6377/17030 9330

[sales@cyberbazaarindia.com](mailto:sales@cyberbazaarindia.com)

Royaume-Uni

Tel. : 0800.389.9772

[europe@webex.com](mailto:europe@webex.com)

Japon

Tel. : + 81 3 5501 3272

[JapanInfo@webex.com](mailto:JapanInfo@webex.com)

Australie & Nouvelle Zélande

Tel. : + 61 (0)3.9653.9581

[AsiaPacInfo@webex.com](mailto:AsiaPacInfo@webex.com)

Corée

Tel. : +82.2.2108.5900

[webex@okmodern.com](mailto:webex@okmodern.com)

