# MODE D'EMPLOI

## I) EXIGENCES RELATIVES À LA SALLE DE CLASSE VIRTUELLE

+ **Aucune installation n'est requise**, tout fonctionne à partir du navigateur Internet.
+ Notre salle de classe virtuelle fonctionne avec la plupart des navigateurs Web, mais certains peuvent nécessiter l'installation d'un plug-in pour prendre en charge la technologie WebRTC. Nous vous recommandons donc d'utiliser le navigateur **Google Chrome**, qui ne nécessite pas de plugin.

  Vous pouvez le télécharger gratuitement ici : https://www.google.fr/chrome

  Si vous décidez d'utiliser un autre navigateur Internet, veuillez consulter la page d'assistance de votre navigateur pour installer le plug-in WebRTC.

Google Chrome

+ Nous vous recommandons de **désactiver les bloqueurs de fenêtres publicitaires** intempestives car ceux-ci peuvent, dans certains cas, empêcher le lancement de la salle de classe virtuelle.
+ Si vous avez besoin d'aide supplémentaire, veuillez vous référer à la **partie IV** de ce document.
+ Nous recommandons l'utilisation d'un casque, d'un microphone et d'une webcam.

  Pour une expérience optimale, nous vous recommandons de vous connecter à un réseau Ethernet à haut débit. Une connexion **WiFi à haut débit** devrait également assurer une expérience similaire.

+ **Avant le premier cours**, vérifiez votre connectivité et votre équipement à l'aide de ce test:

  https://visiagora.live-online-classes.com/fr-fr/troubleshooter/#/
+ Avant le premier cours, vous pouvez vous connecter à l'interface de démonstration pour tester les fonctionnalités de la salle de classe virtuelle :

  https://visiagora.live-online-classes.com/class_demo/
+ Si votre connexion Internet est trop lente, la vidéo sera automatiquement désactivée pour optimiser l'audio.

  Les salles de classe virtuelles détectent automatiquement la vitesse de la connexion Internet du professeur et de l'élève et optimisent la classe pour assurer la meilleure expérience. La vitesse de la connexion Internet est vérifiée à l'entrée dans la salle de classe virtuelle.

  La **qualité de la connexion Internet** est également indiquée sur la vidéo des participants dans le coin inférieur droit :

| CONNEXION BONNE/RAPIDE | CONNEXION MOYENNE/LENTE | CONNEXION TRÈS LENTE |
|---|---|---|
| avec une bonne connexion, les participants disposent d'une vidéo et d'un son d'excellente qualité. | avec une connexion lente, la qualité vidéo est réduite pour optimiser l'audio. | avec une connexion très lente, la vidéo est automatiquement désactivée pour optimiser l'audio. |

*Les enseignants et les élèves peuvent également désactiver manuellement la vidéo pour améliorer les performances en cliquant sur l'icône vidéo verte.*

## II) EXIGENCES DE SÉCURITÉ I PARE-FEU ET PORTS

**Un port de pare-feu fermé peut engendrer un problème de connectivité**, ce qui peut empêcher les connexions entrantes et sortantes. Pour pouvoir utiliser notre service, il y a 3 niveaux d'exigence concernant l'ouverture des ports de pare-feu, que vous trouverez ci-dessous:

**Exigence minimale :** le port TCP 443 doit être ouvert pour se connecter à notre salle de classe virtuelle. Certaines règles de pare-feu/proxy n'autorisent que le trafic SSL sur le port 443. Veillez à ce que le trafic non Web puisse également passer par ce port.

**Exigence recommandée :** en plus de l'exigence minimale, il est recommandé que le port UDP 3478 soit ouvert.

**Exigence optimale :** pour une expérience optimale, assurez-vous que les ports UDP 1025 - 65535 soient ouverts.

*Si vous rencontrez des problèmes concernant l'ouverture ou la fermeture des ports, veuillez vous référer à la Partie V de ce document (tutoriel pour ouvrir les ports requis).*

## III) SERVICE SUPPORT

Si vous continuez à rencontrer des problèmes de connexion, veuillez contacter l'équipe de soutien VISIAGORA en envoyant un courriel à **support@visiagora.com**.

Dans votre courriel, veuillez détailler la nature de votre problème et inclure des captures d'écran (Shift + Cmd + 4 sur Mac / Print Screen sur Windows) car cela nous permettra de vous aider le plus efficacement possible.

## IV) TUTORIEL DE DÉSACTIVATION DES BLOQUEURS DE FENÊTRES INTEMPESTIVES

**Sur Chrome :**

1. Sur votre ordinateur, ouvrez Chrome.
2. Dans le coin supérieur droit, cliquez sur ⋮ puis sur **Paramètres**.
3. En bas, cliquez sur **Paramètre avancés**.
4. Dans la section "Confidentialité et sécurité", cliquez sur **Paramètres de contenu**.
5. Cliquez sur **Fenêtres pop-up**.
6. En haut, réglez le paramètre sur **Autorisé**.

## V) TUTORIEL D'OUVERTURE DE PORTS D'UN PARE-FEU

**Méthode 1 : Ouvrir les ports du pare-feu WINDOWS**

1. Ouvrez le menu **Démarrer** ( ). Cliquez sur le logo Windows dans le coin inférieur gauche de l'écran.
2. Dans ce menu, tapez **Pare-feu Windows sécurité avancée**. Vous verrez alors apparaître le lien vers le programme de configuration du pare-feu.
   *Si vous y êtes invité, entrez le mot de passe administrateur. En effet, pour pouvoir ouvrir un port, vous devez avoir la permission car la sécurité de votre ordinateur est en jeu.*
3. Cliquez sur l'onglet **Action** en haut de l'écran, puis sur **Nouvelle règle**.
4. Cochez l'option **Port,** puis cliquez sur **Suivant**. Ici, vous pouvez taper les numéros des ports que vous voulez ouvrir.
5. Sélectionnez **TCP** ou **UDP**.
   *Pour plus de détails sur le choix du protocole, lisez la documentation de votre programme.*
6. Entrez une plage de ports. Cliquez sur le bouton **Ports locaux spécifiques** et, dans le champ à droite, entrez le port désiré. Si vous ouvrez plusieurs ports, séparez-les par des virgules. S'il s'agit d'une gamme complète de ports, tapez le numéro du premier port, un tiret, puis le numéro du dernier port.
   *Donc, pour ouvrir le port 8830, entrez 8830, pour ouvrir les ports 8830 et 8824, entrez 8830, 8824 et pour ouvrir tous les ports de 8830 à 8835, entrez 8830-8835.*
7. Cliquez sur **Suivant**.
8. Assurez-vous que le bouton **Autoriser la connexion** est activé. Dans le cas contraire, cliquez dessus pour l'activer, puis cliquez sur **Suivant**.
9. Vérifiez que les trois cases de la page **Profil** sont cochées. Ces trois cases sont appelées **Domaine**, **Privé** et **Public**.
10. Cliquez sur **Suivant**.
11. Donnez un nom à votre règle. Cliquez ensuite sur **Terminer**. Vos réglages seront sauvegardés.

### Méthode 2 : Désactiver le coupe-feu ou pare-feu sous Mac OS X

Le pare-feu ou coupe-feu d'un Mac est désactivé par défaut. Si vous n'avez pas activé votre pare-feu, vous n'avez rien de spécial à faire.

1. Si vous avez activé votre pare-feu ou coupe-feu, il est nécessaire de le désactiver pour utiliser nos services.
2. Cliquez sur le menu **Pomme** ( ). Il est dans la barre des menus dans le coin supérieur gauche.
3. Cliquez sur **Préférences Système**. C'est la deuxième option du menu déroulant.
4. Cliquez sur **Sécurité et confidentialité**. Cette icône en forme de maison est sur la première ligne.
5. Cliquez sur l'onglet **Coupe-feu** ou **Pare-feu** selon les modèles. Il est en troisième position sur la rangée des onglets.
6. **Débloquez l'accès au menu du pare-feu ou coupe-feu**. Cliquez sur le cadenas en bas et à gauche, entrez alors le mot de passe administrateur, puis cliquez sur **Déverrouiller**.
7. Cliquez sur **Désactiver le pare-feu ou coupe-feu**.
8. Quittez. Vos modifications ont été sauvegardées.

### Méthode 3 : Ouvrir les ports d'un pare-feu de routeur

1. **Trouvez l'adresse IP de votre routeur**. Elle est absolument nécessaire pour que vous puissiez accéder à la page de configuration du routeur.

   **WINDOWS** : ouvrez le menu **Démarrer** ( ), cliquez sur **Paramètres**, puis sur **Réseau** et **Internet**. Cliquez ensuite sur **Afficher vos propriétés réseau** et récupérez l'adresse inscrite à côté de **Passerelle par défaut**.

   **MAC** : ouvrez le menu **Pomme** ( ), cliquez sur **Préférences Système**, puis sur **Réseau**. Cliquez ensuite sur **Avancé**, puis sur **TCP/IP** et notez le numéro à droite de **Routeur**.
2. **Allez sur la page de configuration de votre routeur**. Ouvrez un navigateur Internet, puis tapez l'adresse IP de votre routeur dans la barre d'adresse.
3. **Entrez le nom d'utilisateur et le mot de passe**. Si votre routeur est déjà protégé, entrez le nom d'utilisateur et le mot de passe. Si ce n'est pas le cas, consultez le manuel d'utilisation (livret ou sur Internet) du routeur et trouvez le nom d'utilisateur et le mot de passe par défaut. Si vous avez perdu vos informations de connexion, réinitialisez votre routeur.
4. **Trouvez la rubrique Redirection de ports**. Chaque routeur a sa propre page de configuration, même si elles se ressemblent.

   Repérez les différentes rubriques aux noms variables :

   + redirection de ports;
   + applications;
   + jeux;
   + serveurs virtuels;
   + pare-feu;
   + protocole de protection;
   + si vous désirez voir plus de paramètres, allez voir dans la rubrique Paramètres avancés.
5. **Ouvrez le port choisi.** La procédure varie d'un routeur à l'autre, même si les informations demandées sont exactement les mêmes.
   + **Nom du service** ou **Description** : entrez le nom de l'application ou un nom descriptif.
   + **Type** ou **Protocole** : le choix s'opère entre TCP, UDP ou les deux. Si vous ne savez pas, cliquez sur **TCP/UDP**.
   + **Trafic entrant** ou **Port de début** : tapez le numéro du port à cet endroit-là. Pour une plage de ports, tapez le numéro du port le plus petit.
   + **Privé** ou **Port de fin** : tapez ici à nouveau le numéro du port. Pour une plage de ports, tapez le numéro du port le plus grand.
6. **Entrez l'adresse IP privée de votre ordinateur**. Tapez-la dans le champ intitulé **Adresse IP**. Pour trouver celle de votre ordinateur, lisez cet article si vous avez un PC ou celui-ci si vous avez un Mac.
7. **Enregistrez vos paramètres**. Cliquez sur **Enregistrer** ou **Appliquer**. Redémarrez le routeur afin que les changements soient pris en compte. Sur la ligne de la redirection de port, vous devrez, si ce n'est fait par défaut, cocher la case **Activé**.