GUIDE UTILISATEUR POSTES NON NORMALISÉS

CLIENT LÉGER

RPV CHECK POINT

Votre gouvernement

Québec

Table des matières

Introduction

Ce document présente la marche à suivre pour vous connecter au service d'extension VPN Check Point. Il y recense toutes les étapes : des préalables jusqu'à la déconnexion.

IMPORTANT : L'utilisateur est responsable d'utiliser uniquement son ordinateur professionnel pour accéder à ce réseau corporatif. Des actions légales pourraient être envisagées si des dommages étaient causés par votre appareil.

Préalables

Avant de commencer, assurez-vous d'avoir en votre possession les éléments suivants :

- Il est fortement recommandé d'utiliser un réseau filaire et non un réseau Wi-Fi pour assurer une stabilité de la connexion.
- Un ordinateur muni du système d'exploitation[1] **Windows 8**, **Windows 8.1, Windows 10 ou Windows 11** (pas supporté) ainsi que d'un jeton **physique ou virtuel activé**.
  1. Posséder des droits administrateurs de votre poste de travail.
  2. Un antivirus à jour et présent dans cette liste :
     - Apex One ;
     - Avast;
     - AVG;
     - Bit Defender;
     - CA Etrust;
     - CA Vet;
     - Cisco AMP
     - Forefront;
     - Forticlient ;
     - F-Secure;
     - McAfee;
     - Nod32 Eset;
     - Norton;
     - Panda;
     - Sophos;
     - Symantec;
     - Trend Micro;
     - Windows Defender;
     - Windows Live OneCare;
     - ZoneAlarm6 ou End point Security;
     - ZoneAlarm7 ou Integrity Antivirus;
- Un navigateur Web reconnu (Google Chrome, Mozilla Firefox ou Edge).

Note : seuls trois navigateurs sont pris en charge par la solution : Google Chrome, Mozilla Firefox et Edge. Assurez-vous d'avoir la plus récente version de l'un ou l'autre de ceux-ci. L'utilisation de **Google Chrome est recommandée** dans le présent cas.

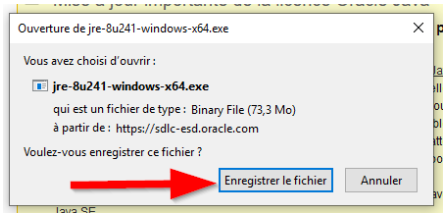
Si vous rencontrez des problèmes lors de l'authentification à la solution, veuillez communiquer avec le centre de service à la clientèle au 418 643-6758 ou au numéro sans frais 1 855 643-6758. Nous communiquerons avec vous dans les meilleurs délais. Toutefois, aucune assistance ne vous sera offerte pour l'installation des composantes sur votre poste de travail.

Télécharger la version 8 du java runtime environnement (JRE)

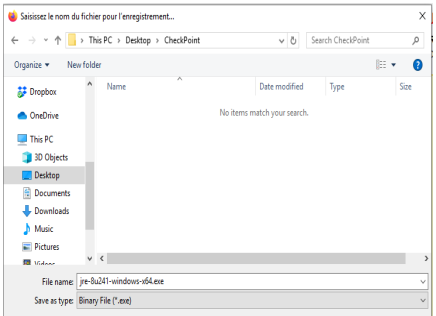
1. Cliquer sur l'hyperlien suivant ou copier le dans la barre d'adresse du navigateur, puis cliquez sur « ***Téléchargement gratuit de Java*** »;

2. Cliquer sur le bouton « ***Accepter et lancer le téléchargement gratuit*** »;

3. Dans la fenêtre qui apparaît, cliquer sur « ***Enregistrer le fichier*** »;



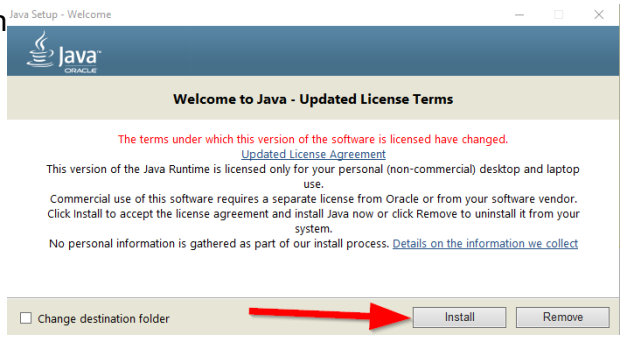
4. Sauvegarder le fichier dans un répertoire que vous aurez défini.



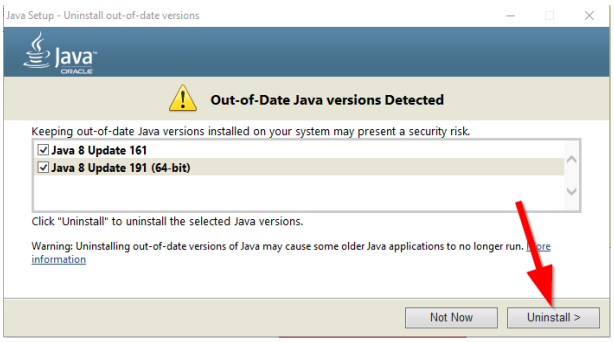
Installer la version 8 du JRE

1. Ouvrer le fichier une fois téléchargé, afin de lancer l'installation;

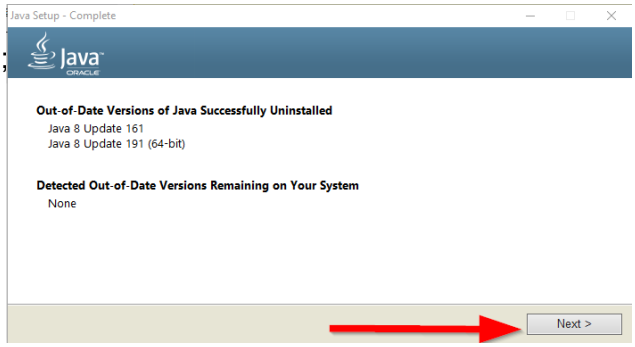
2. Dans la fenêtre qui apparaît, cliquez sur le bouton « ***Install*** »;



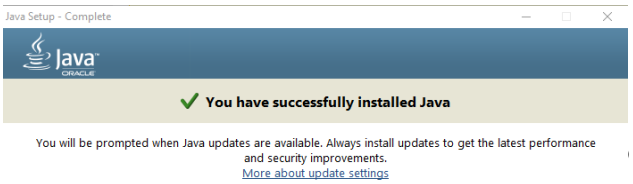
Note : Si des versions obsolètes du JRE sont trouvées pendant l'installation, il est possible de les supprimer en cliquant sur le bouton **Uninstall**.



3. Une fois la désinstallation des versions obsolètes terminée, cliquez sur « ***Next*** »;



4. Une fois l'installation du JRE terminée, cliquez sur le bouton « ***Close*** ».



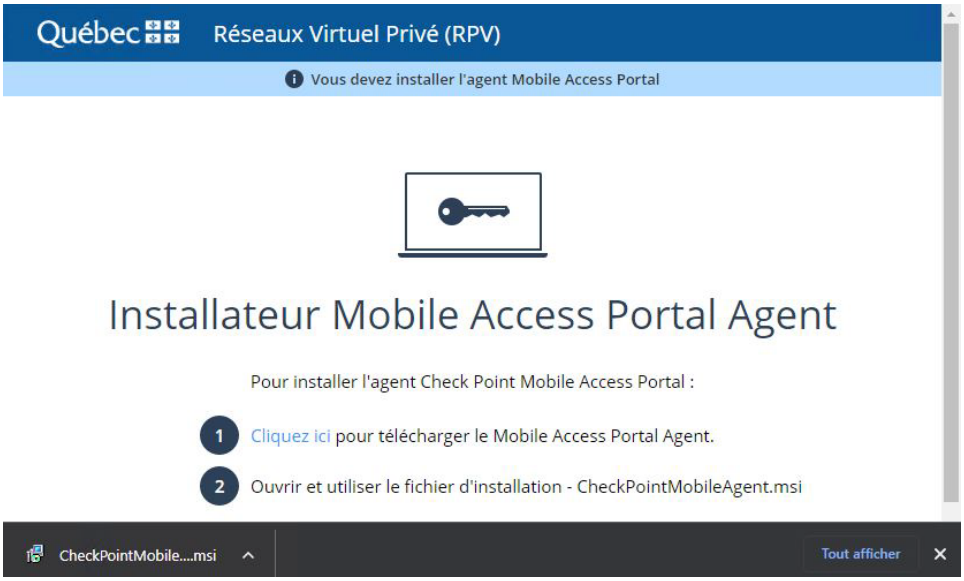
Accès au portail

1. Ouvrez votre navigateur et copiez l'adresse suivante dans la barre d'adresse : https://pnn.rpv.gouv.qc.ca/
2. Lorsque vous accédez au Portail, portez attention au présent message.

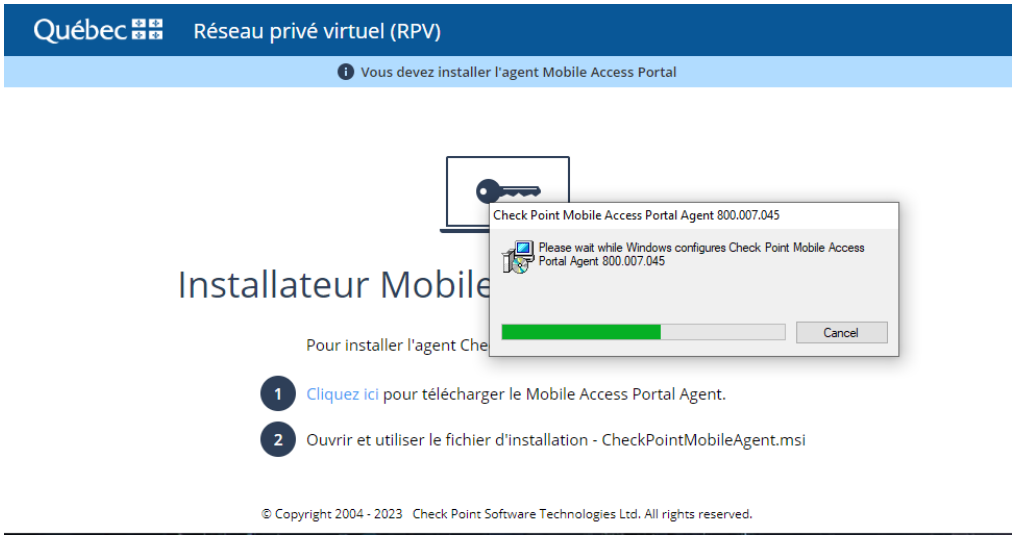
Installation du plugiciel Check Point

1. Quel que soit votre navigateur, lors du premier accès, l'installation du plugiciel est automatiquement proposée. Cliquez « ***Cliquez ici*** » pour le télécharger.

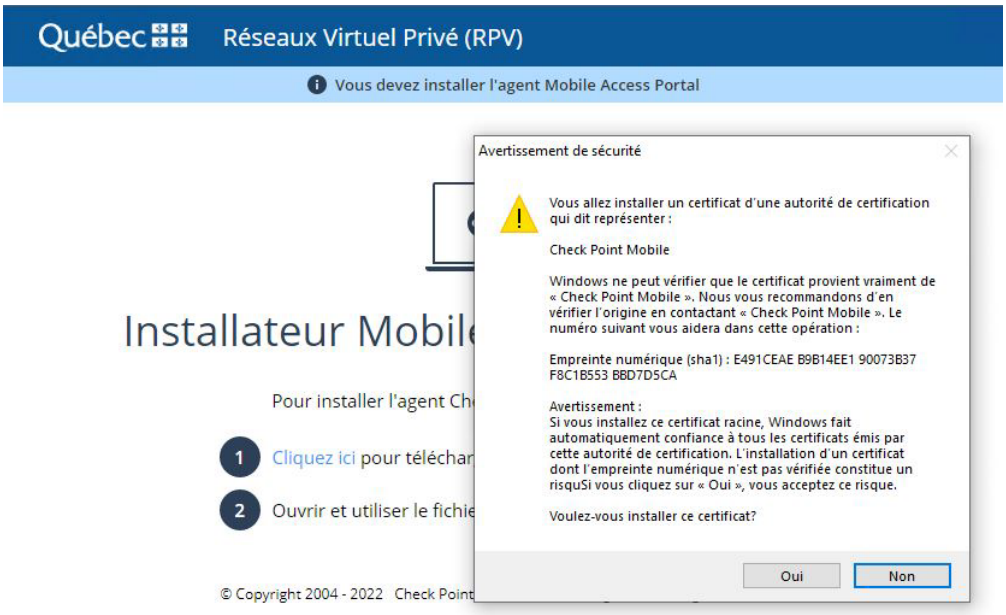
2. Un fois le téléchargement complété, double cliquer sur le fichier dans la barre au bas de la fenêtre;



3. Attendez la finalisation de l'installation de l'agent;



4. Autorisez l'installation du certificat sur la fenêtre d'avertissement de sécurité qui apparait en cliquant sur « ***Oui*** »;



5. Le plugiciel est maintenant installé. Reportez-vous maintenant à la section Vérification de la conformité du présent guide.

Vérification de la conformité

Cette étape valide plusieurs aspects du poste utilisé pour la connexion à distance. Il est requis de vérifier la conformité de celui-ci avant de passer à l'étape suivante.

La première étape est de passer l'étape de conformité. Celle-ci valide plusieurs aspects de la posture du poste utilisé pour la connexion. Il est fortement recommandé de réaliser cette étape avant de passer à la suivante.

Si le poste est conforme, il sera possible de passer à l'étape suivante, soit l'authentification. Voir la section **Authentification et connexion au réseau virtuel privé (VPN)**.

Dans le cas contraire, il faut remédier aux anomalies avant de pouvoir accéder au service. Voici les éléments de conformité requis :

- L'utilisation d'une version de Windows encore supportée par Microsoft.
- Les mises à jour Windows doivent être installées.
- Le mécanisme de contrôle du compte de l'utilisateur (UAC) doit être activé.
- Un antivirus reconnu doit être installé, actif et à jour.
- Si l'un de ces éléments n'est pas conforme, vous recevrez l'un ou l'autre des messages du tableau ci-dessous.

Messages d'erreur potentiels relatifs à la conformité

Nº de l'erreur	*Description*	*Résolution*
Erreur #RPV000000 ou #RPV000001	Le système d'exploitation utilisé n'est pas autorisé.	Utilisez un système d'exploitation autorisés : • Windows 8 • Windows 8.1 • Windows 10 • Windows 11 (Pas supporté) Installer les correctifs : Activer les mises à jour automatiques de Windows
Erreur #RPV000020	Le mécanisme de protection des données (UAC) n'est pas activé.	Activer UAC https://docs.microsoft.com/fr-fr/mem/intune/user-help/you-need-to-enable-uac-windows
Erreur #RPV000030	L'antivirus (AV) n'est pas reconnu.	Utiliser les antivirus suivants : • Apex One ; • Avast; • AVG; • Bit Defender; • CA Etrust; • CA Vet; • Cisco AMP • Forefront; • Forticlient ; • F-Secure; • McAfee; • Nod32 Eset; • Norton; • Panda; • Sophos; • Symantec; • Trend Micro; • Windows Defender; • Windows Live OneCare; • ZoneAlarm6 ou End point Security; • ZoneAlarm7 ou Integrity Antivirus;
Erreur #RPV000040	L'AV n'est pas actif ou le fichier de définition date de plus de deux semaines.	Activer l'AV Mettre à jour l'AV

Attention : Si votre ordinateur rencontre toutes les exigences et que vous avez tout de même une

erreur de conformité, veuillez essayer de supprimer vos fichiers temporaires à partir de votre navigateur. Sinon, essayez en navigation privée toujours à partir de votre fureteur. Ceci corrige souvent les erreurs de conformité.

Authentification et connexion au réseau virtuel privé (VPN)

Si les étapes d'installation et de conformité se sont déroulées correctement, la page d'authentification s'affichera.

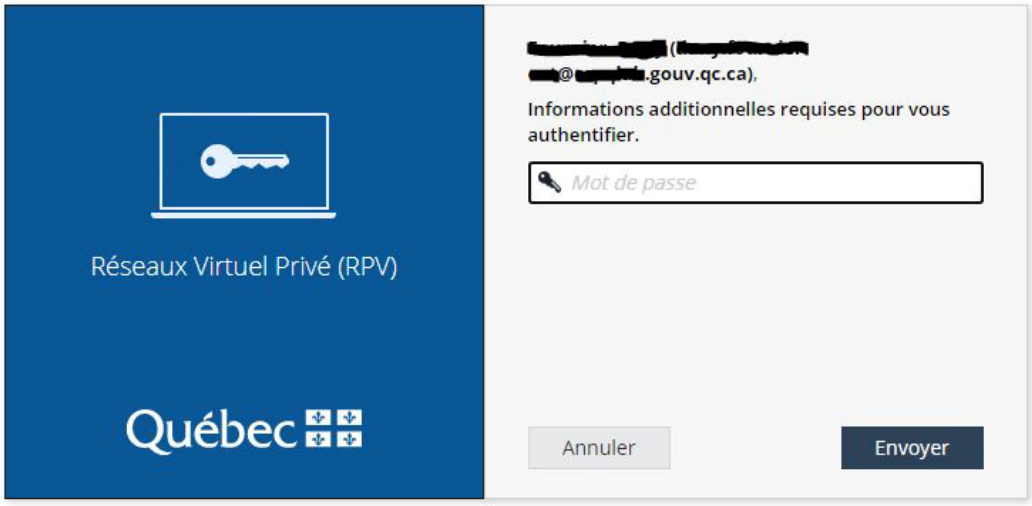
1. Dans un premier temps, choisir l'option de connexion appropriée;

NOTE:

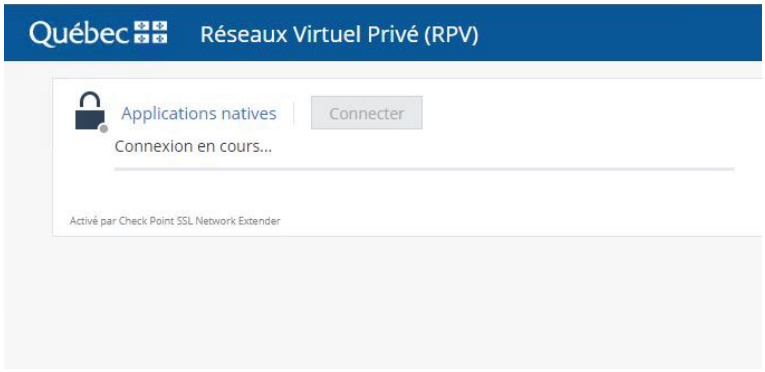
« ***Ancien Jeton*** » est NIP (4 chiffres) + Jeton (6 chiffres);

« ***Nouveau Jeton*** » est Jeton (6 chiffres).

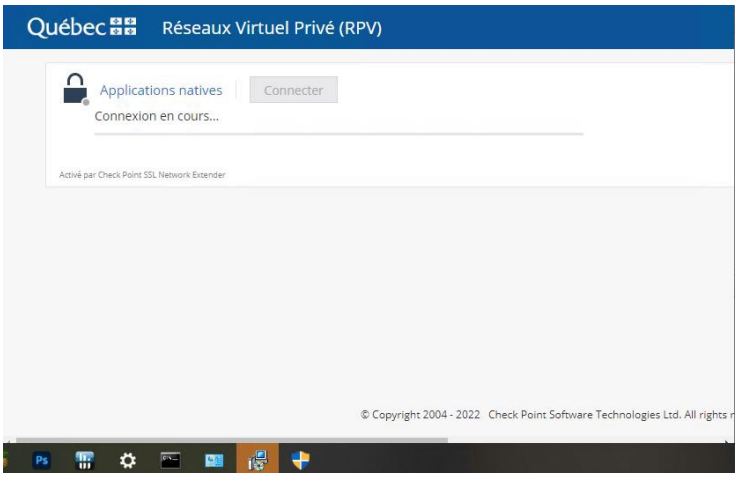
2. Saisissez votre adresse électronique comme utilisateur (ex : prénom.nom@mcn.gouv.qc.ca).
3. Saisir le code secret en fonction de l'option de connexion effectué précédemment;
4. Saisissez votre mot de passe utilisateur et cliquer sur envoyer pour finaliser la connexion;



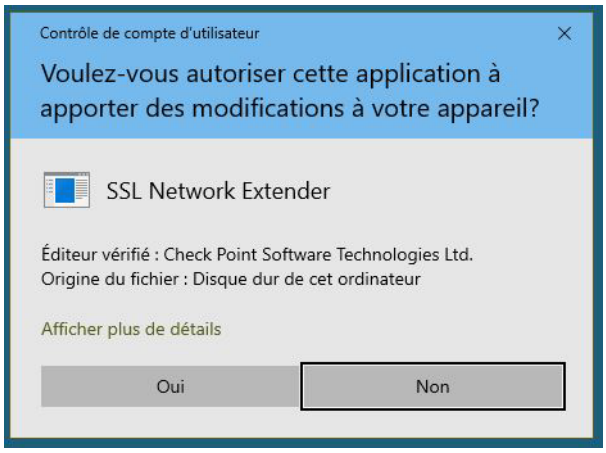
6. Cliquer sur « ***Connecter*** » pour effectuer la connexion RPV;



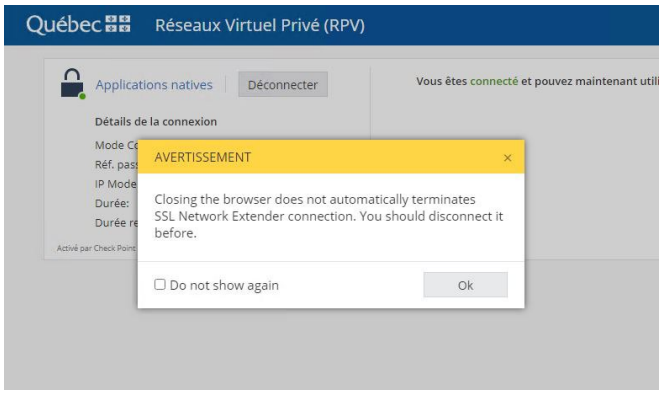
5. Si c'est le premier lancement, l'installation d'un second module est requise. Sélectionner le bouclier clignotant de la barre des tâches;



6. Dans la fenêtre suivante, cliquez sur le bouton « ***Oui*** »;



7. Prendre note du message d'avertissement;

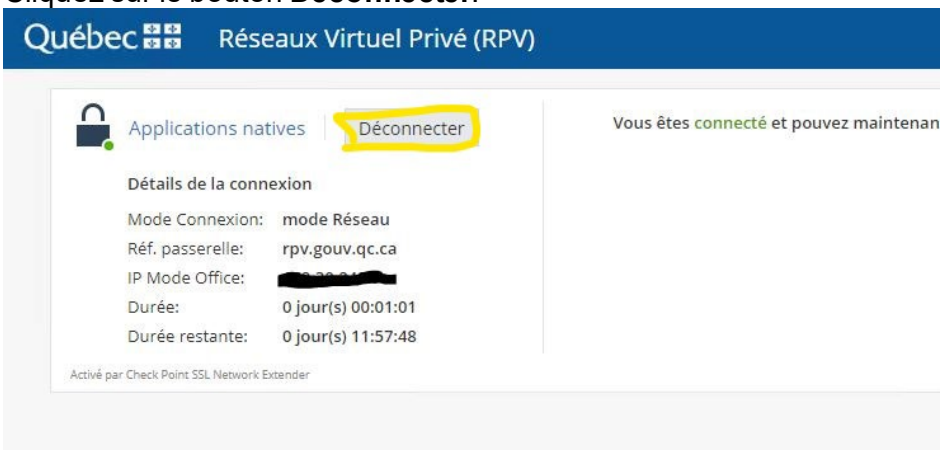


8. La connexion RPV est maintenant établie.

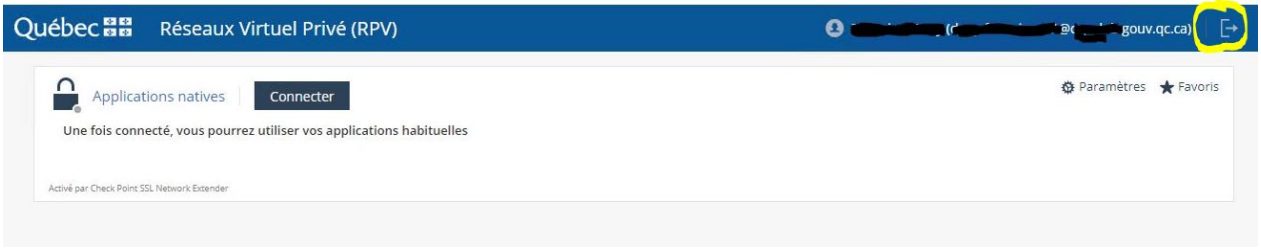
Déconnexion

Lorsque vous aurez terminé vos activités, vous devrez vous déconnecter. Cette étape très importante optimise l'utilisation de la solution par les autres utilisateurs.

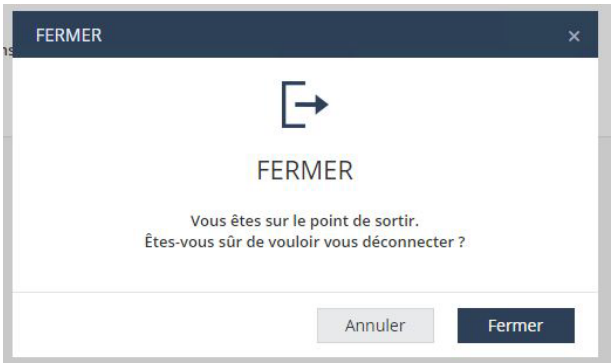
1. Cliquez sur le bouton **Déconnecter**.

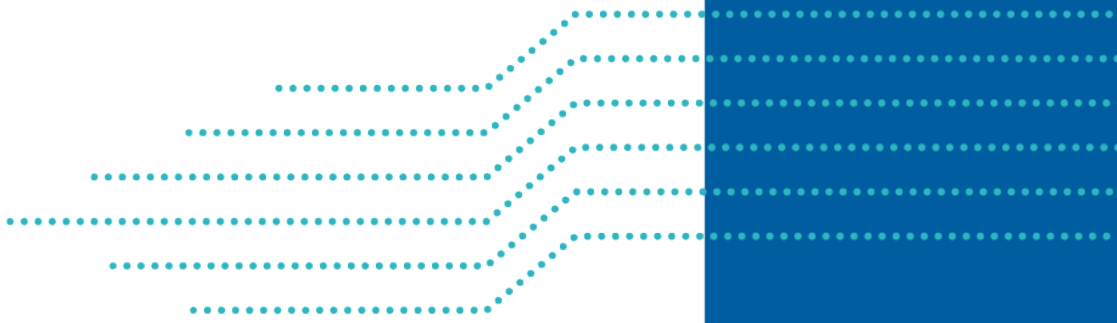


2. Cliquer sur l'icône de porte de sortie dans le coin supérieur droit;



3. Cliquez sur le bouton « ***Fermer*** ».





Québec