



National Défense
Defence nationale

Sous-ministre adjoint (Gestion de l'information)



Console d'administrateur de la gestion des appareils mobiles d'entreprise (GAME)

Version : 2.1
Date : 14 février, 2019
Produit par : DDCGI

Historique du document

Date	Version	Description de la modification	Auteur
14 Février 2019	2.1	Version francophone finale	Andrew Mayotte

Table des matières

1. Introduction.....	4
2. Conditions préalables pour accéder la console d'administrateur de la GAME	4
2.1 Compte d'administrateur	4
2.2 Jeton de sécurité Entrust IdentityGuard	4
2.3 Installation du logiciel Citrix.....	5
3. Accéder la console d'administrateur de la GAME	7
3.1 Se connecter au portail de SPC	7
3.2 Se connecter à la console d'administrateur de la GAME.....	8
4. Gestion des appareils mobiles	15
4.1 Recherche rapide d'utilisateur (Android et iOS).....	15
4.2 Réinitialiser le mot de passe de déverrouillage de l'appareil (Android et iOS) .	17
4.3 Réinitialiser le mot de passe de l'espace de travail Knox (Android seulement)	21
4.4 Supprimer les données de l'appareil à distance (Android et iOS)	23
4.5 Désactiver/Réactiver l'espace de travail Knox (Android seulement)	27
4.6 Définir le mot de passe d'activation (Android et iOS).....	30
4.7 Redémarrer l'appareil à distance (iOS seulement).....	33
4.8 Afficher le rapport de l'appareil (Android et iOS).....	36
4.9 Afficher les actions de l'appareil (Android et iOS)	38
4.10 Mettre à jour les informations de l'appareil (Android et iOS).....	41
4.11 Supprimer uniquement les données professionnelles (Android et iOS)	43
5. Administration générale.....	44
5.1 Exporter la liste des utilisateurs et appareils	44
5.2 Modifier les informations du compte d'un utilisateur.....	50

1. Introduction

Public cible

Le présent document s'adresse particulièrement au personnel ci-dessous :

- Centres de gestion de services (CGS)
- Centre des opérations des services de la Défense (COSDEF)
- Administrateurs de la GAME des partenaires

Description du service de la GAME

Le service de la GAME de Services Partagés Canada (SPC) offre la gestion contrôlée et sécurisée des appareils mobiles Android et iOS pour le Gouvernement du Canada.

De plus, les appareils Android sont enregistrés avec « Knox Mobile Enrollment » et les appareils iOS sont enregistrés avec « Apple Device Enrollment Program » permettant d'activer plus facilement les appareils et assurer que les appareils ne peuvent être utilisés en dehors du service de la GAME.

Le service de la GAME utilise la version 12.9 de la plateforme « BlackBerry Unified Endpoint Management (UEM) ».

2. Conditions préalables pour accéder la console d'administrateur de la GAME

2.1 Compte d'administrateur

Les administrateurs de la GAME recevront de SPC les informations ci-dessous :

- Nom d'utilisateur et mot de passe
- Mot de passe à usage unique (OTP) Entrust pour configurer le jeton de sécurité (voir section 2.2 ci-dessous)

2.2 Jeton de sécurité Entrust IdentityGuard

Un jeton de sécurité, également appelé «jeton matériel» ou «jeton logiciel», est requis pour accéder à la console d'administrateur de la GAME. Le jeton est obtenu soit à l'aide de l'application Entrust IdentityGuard installée sur un appareil Android ou iOS, soit à l'aide d'un jeton matériel Entrust. Suivez les étapes décrites dans l'un des documents ci-dessous pour compléter cette étape :

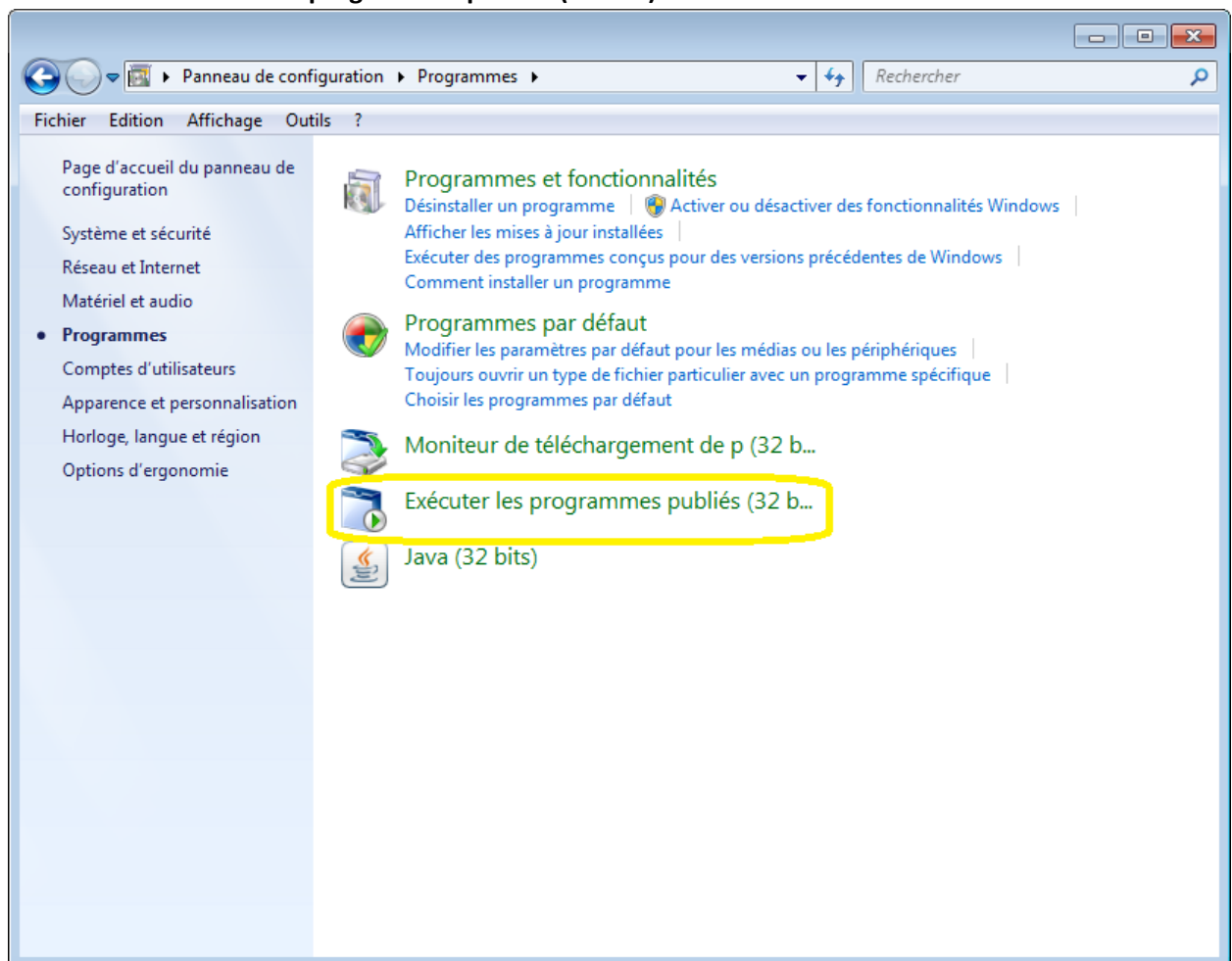
- [Guide de l'utilisateur de SPC pour le jeton logiciel Android Entrust IdentityGuard](#)
- [Guide de l'utilisateur de SPC pour le jeton logiciel iOS Entrust IdentityGuard](#)
- [Guide de l'utilisateur de SPC pour le jeton matériel Entrust IdentityGuard](#)

Remarque : Ces documents de Services Partagés Canada (SPC) sont hébergés sur le site GCpédia de SPC. Afin d'ouvrir ces documents, vous devez être sur le réseau du RED (DWAN). De plus, il se peut que vous devez copier-coller le lien dans votre navigateur web afin d'y accéder.

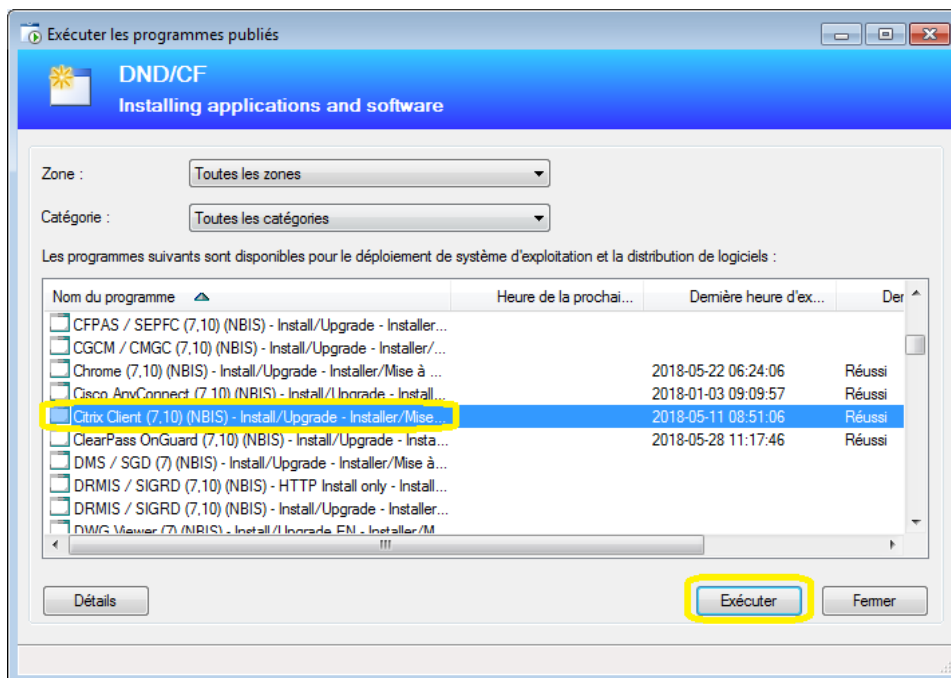
2.3 Installation du logiciel Citrix

La console d'administrateur de la GAME est une application web qui s'exécute dans un environnement Citrix hébergé sur un serveur de SPC. Le logiciel Citrix doit être installé avant d'accéder à la console d'administrateur de la GAME. Suivez les étapes ci-dessous pour installer le logiciel Citrix sur un ordinateur du RED (DWAN) :

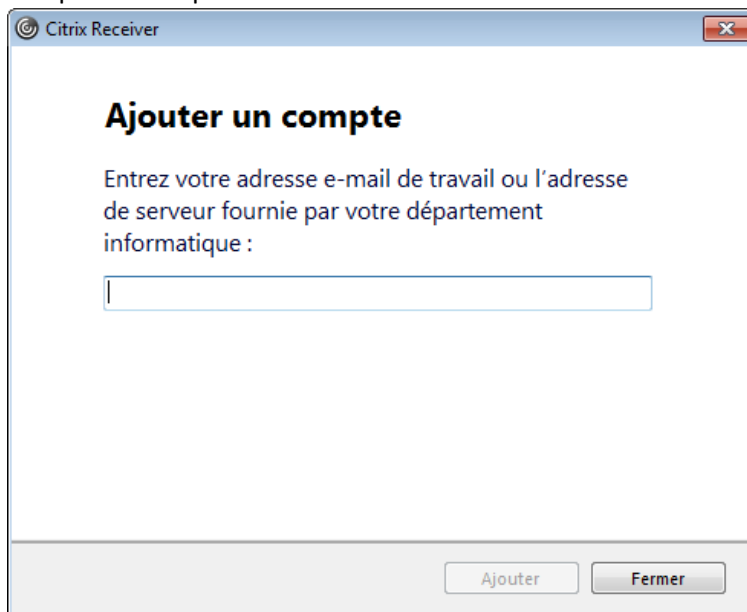
1. Accédez le **panneau de configuration** (menu Démarrer -> Panneau de configuration) et sélectionnez **Programmes**
2. Sélectionnez **Exécuter les programmes publiés (32 bits)**



3. Sélectionnez **Citrix Client (7, 10) (NBIS) – Installer/Mise à jour** et sélectionnez **Exécuter**



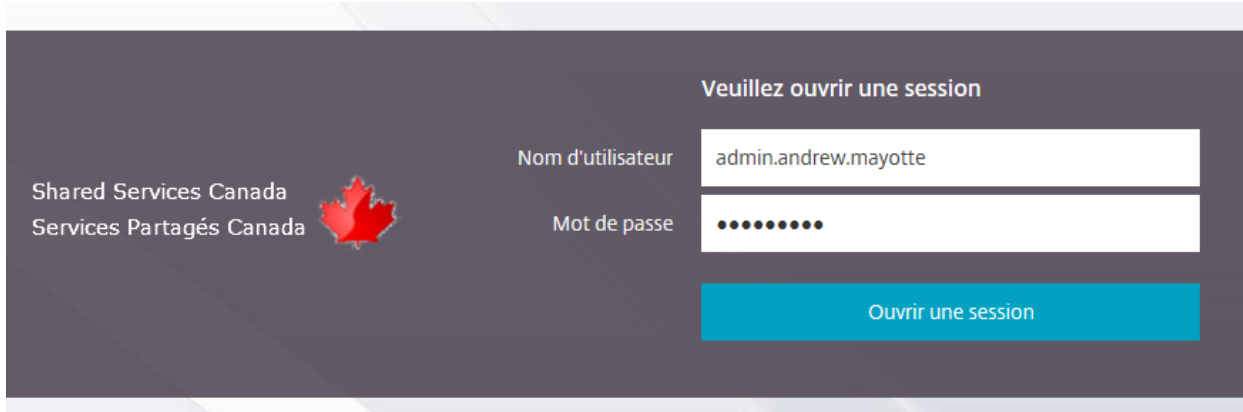
- 4. Une fenêtre « Ajouter un compte » apparaît lorsque l'installation du logiciel Citrix est complétée. Simplement **Fermer** cette fenêtre.



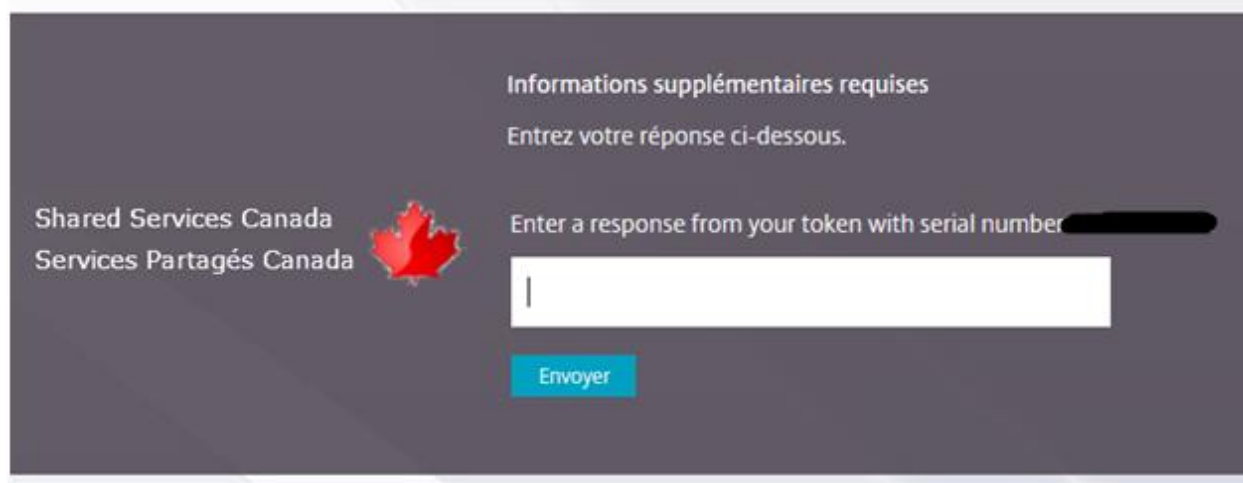
3. Accéder la console d'administrateur de la GAME

3.1 Se connecter au portail de SPC

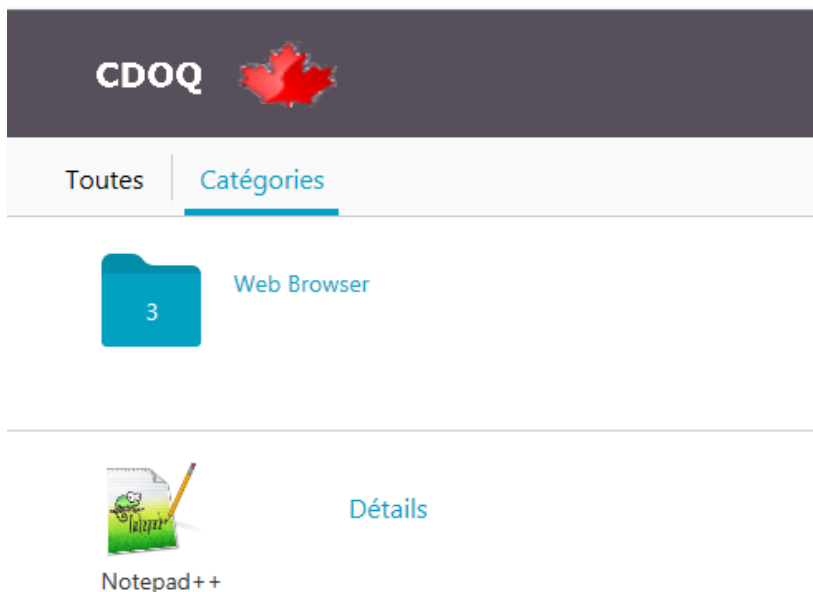
1. Avec un navigateur web, entrez <https://appadmin-dev1.ssc-spc.gc.ca/vpn/index.html> dans la barre d'adresse afin d'accéder au portail de SPC. Ensuite, tapez votre nom d'utilisateur (admin.prénom.nomdefamille) et mot de passe et sélectionnez Ouvrir une session.



2. À la page suivante, entrez le code de sécurité de votre jeton logiciel ou matériel Entrust IdentityGuard et sélectionnez Envoyer.

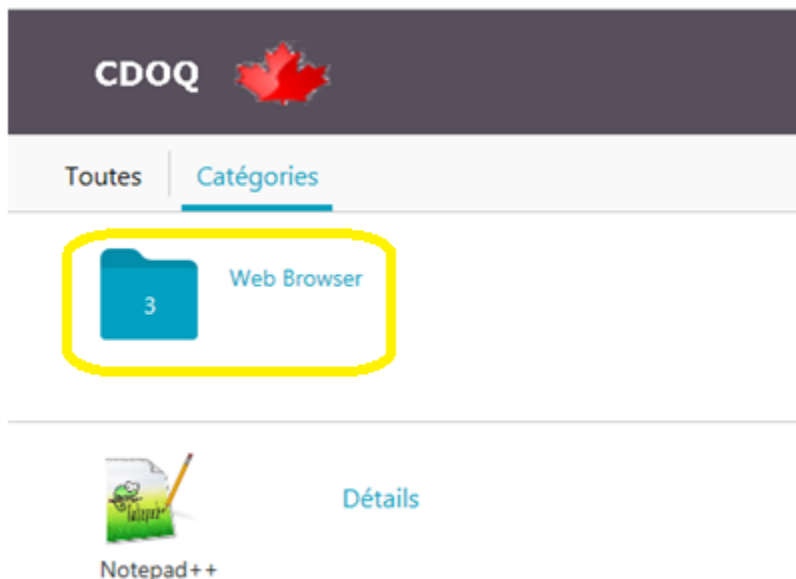


3. La page ci-dessous s'affiche

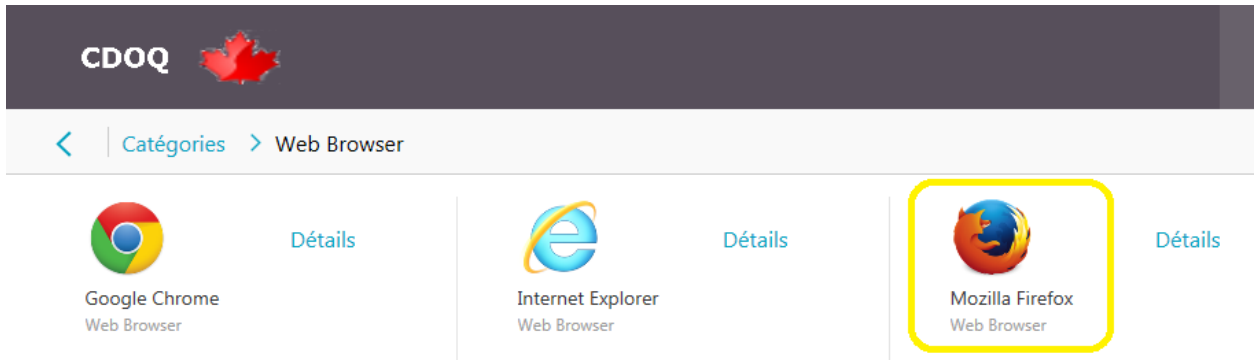


3.2 Se connecter à la console d'administrateur de la GAME

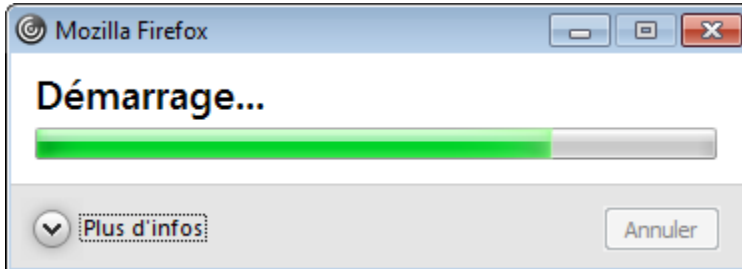
- 1) Sélectionnez « Web Browser »



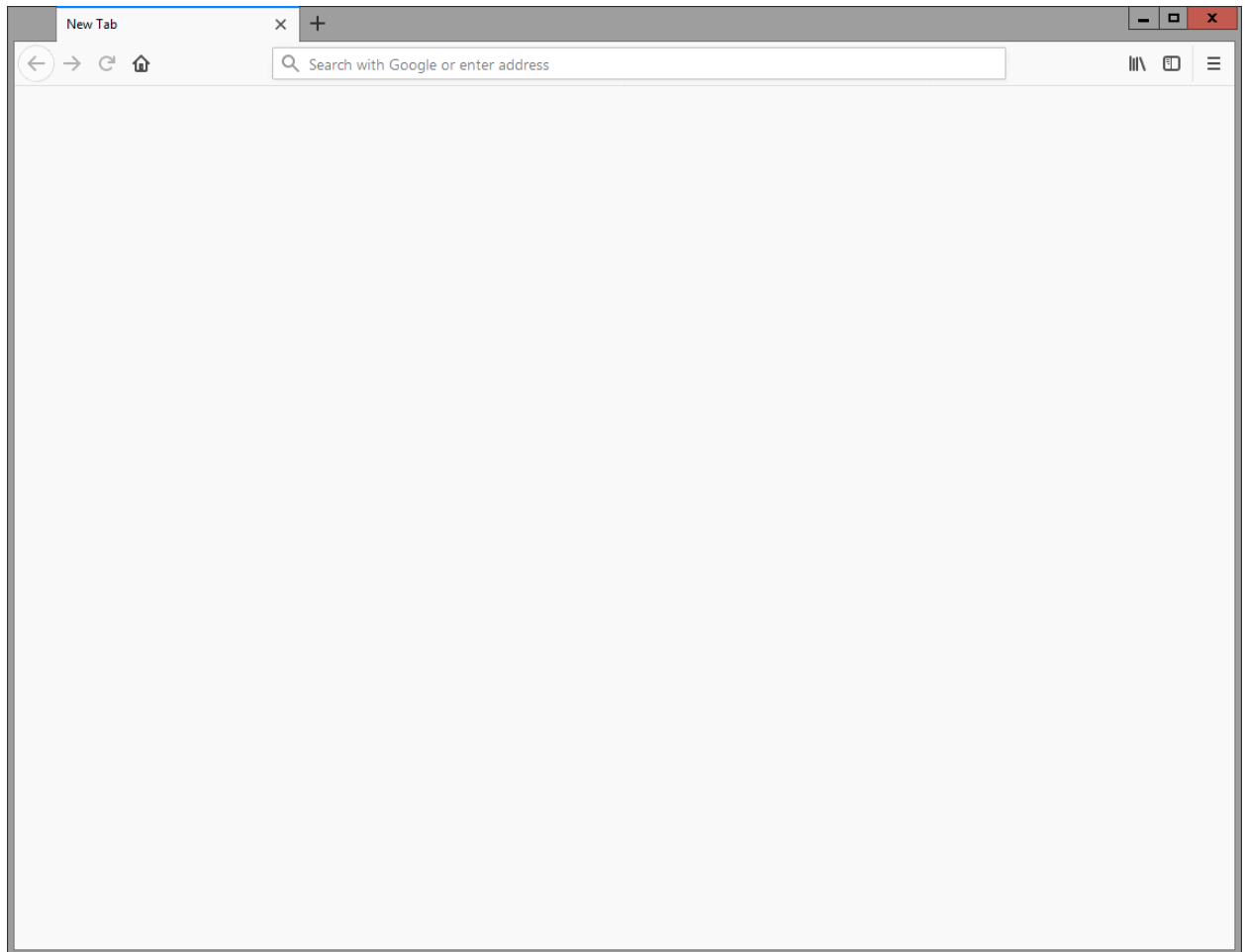
- 2) Sélectionnez le navigateur web Firefox. *Remarque : Ne pas sélectionner Internet Explorer ou Google Chrome. Ces deux navigateurs web éprouvent des problèmes techniques avec la console d'administrateur de la GAME.*



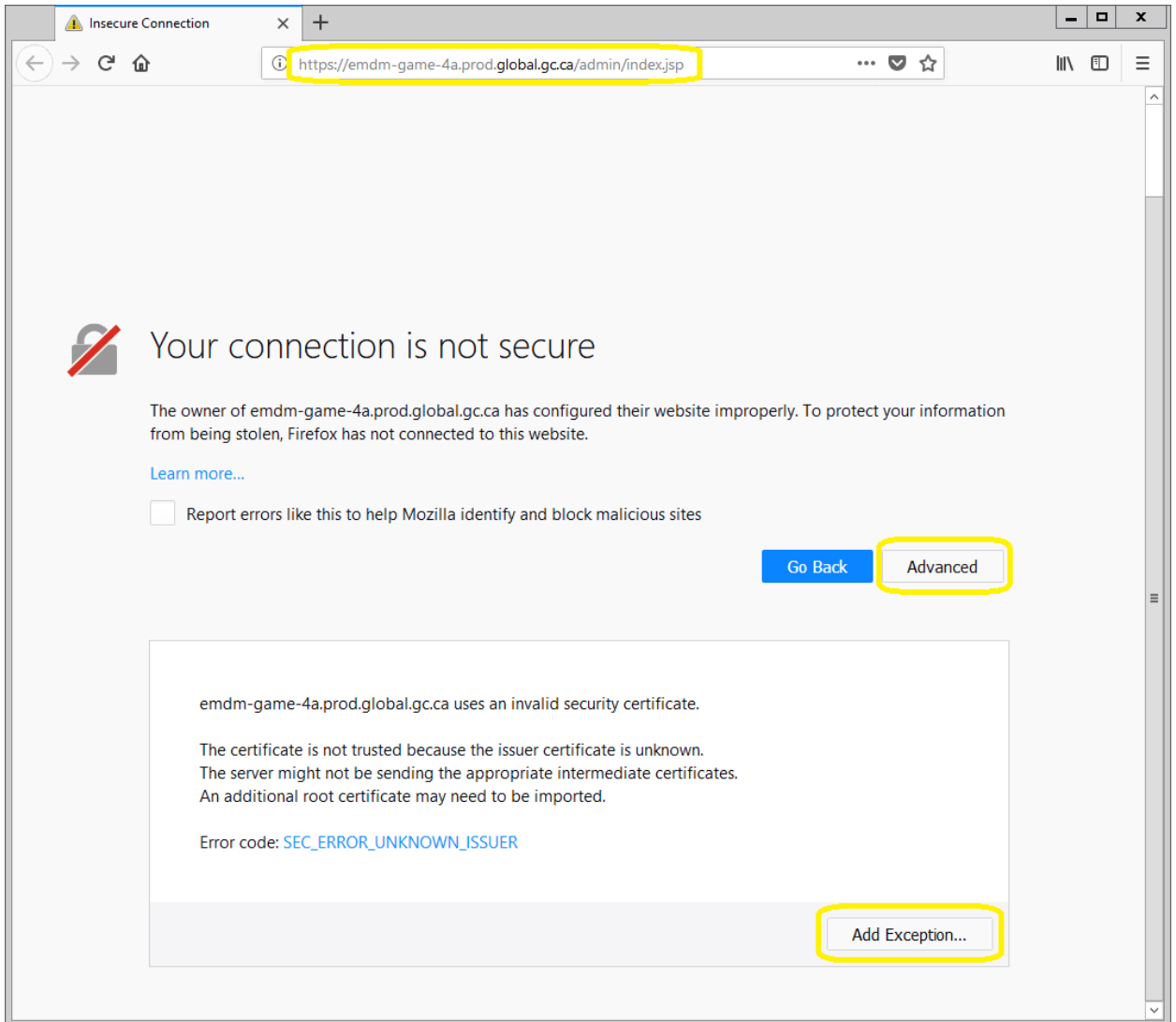
- 3) Firefox démarre dans l'environnement Citrix. Firefox sera en Anglais.



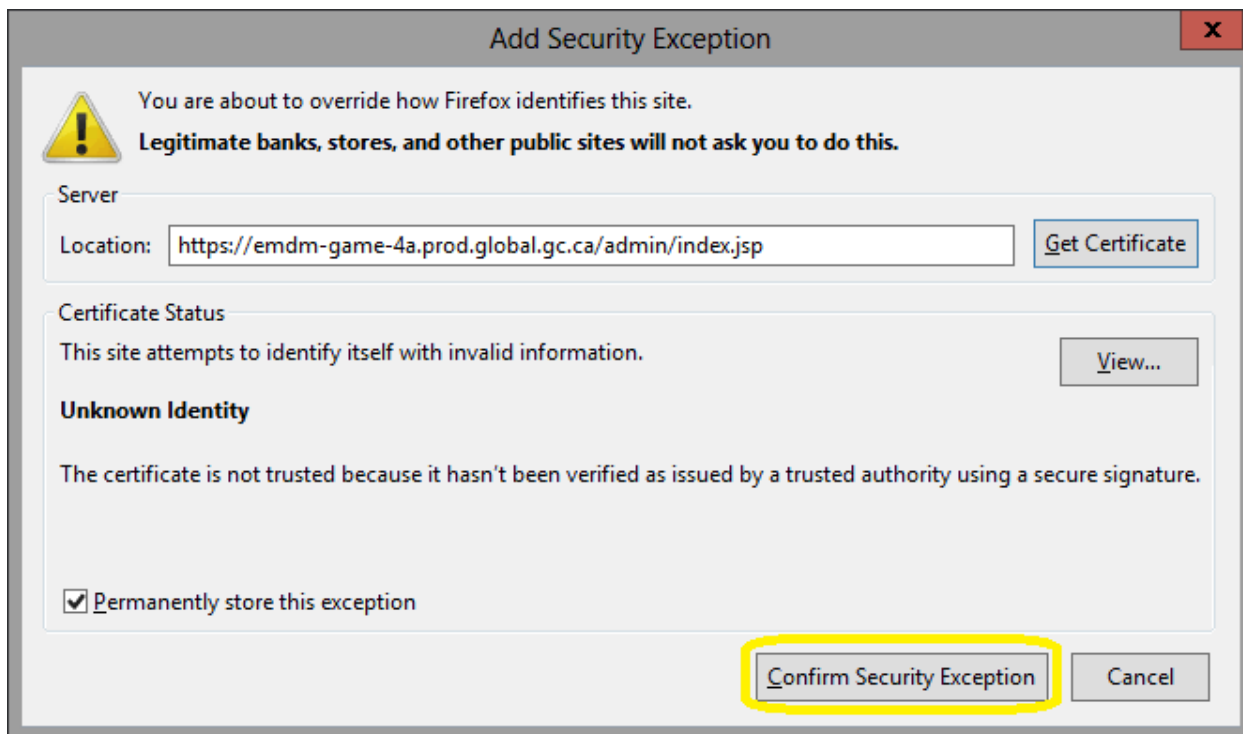
- 4) Si vous êtes demandé comment ouvrir une adresse HTTP, sélectionnez Firefox.
5) Vous devez maintenant voir le navigateur Firefox avec une page blanche/grise.



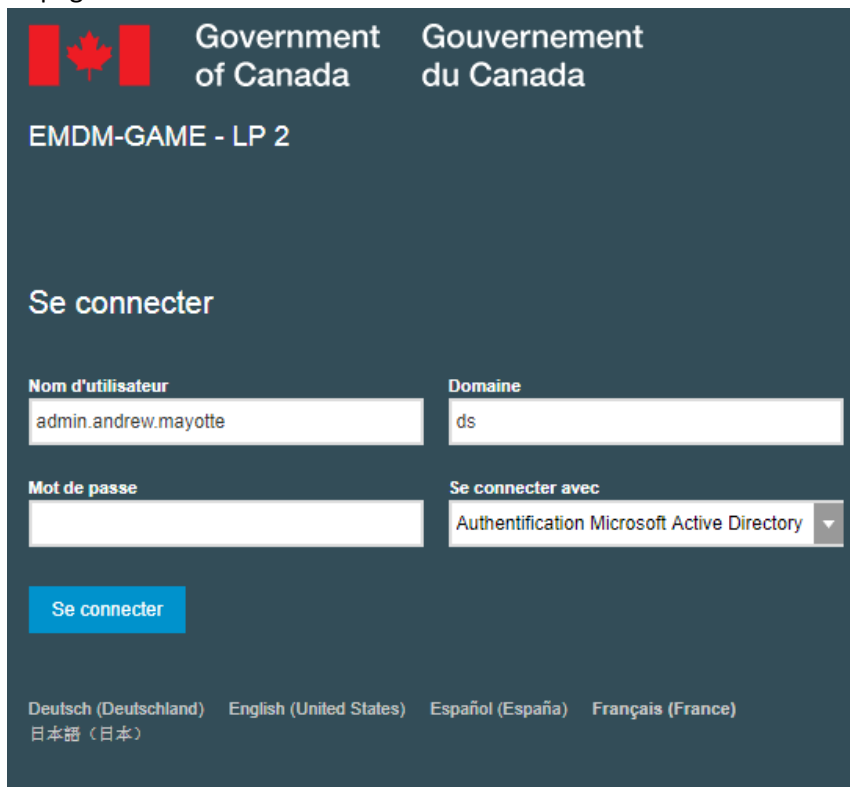
- 6) Dans la barre d'adresse du navigateur Firefox, entrez <https://emdm-game-4a.prod.global.gc.ca/admin/index.jsp?locale=fr> afin d'accéder à la console d'administrateur de la GAME en français
- 7) Il est possible que la première fois vous accéder à la console que Firefox indique une erreur de connexion. Si oui, sélectionnez « Advanced » et ensuite sélectionnez « Add Exception »



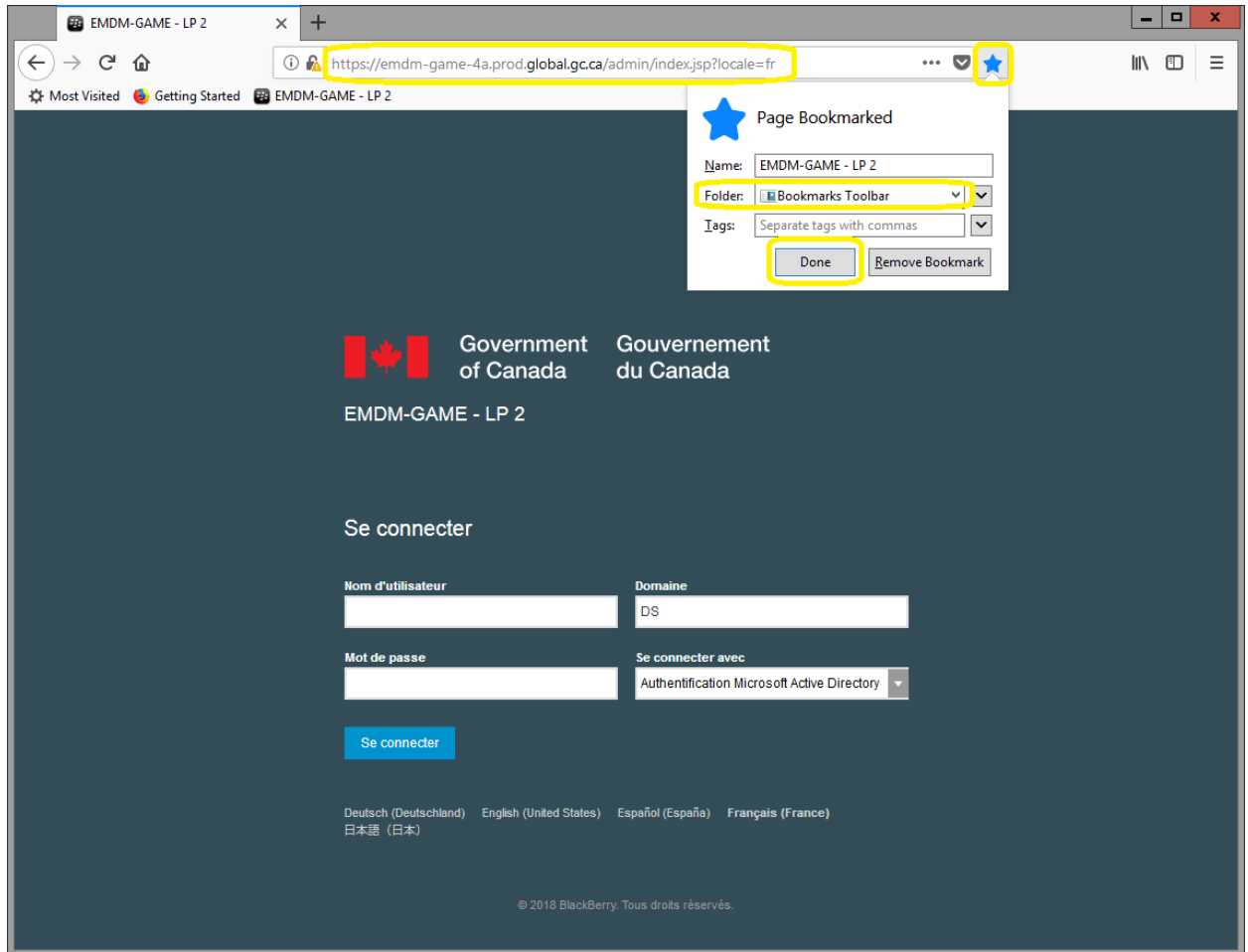
8) Sélectionnez « Confirm Security Exception »



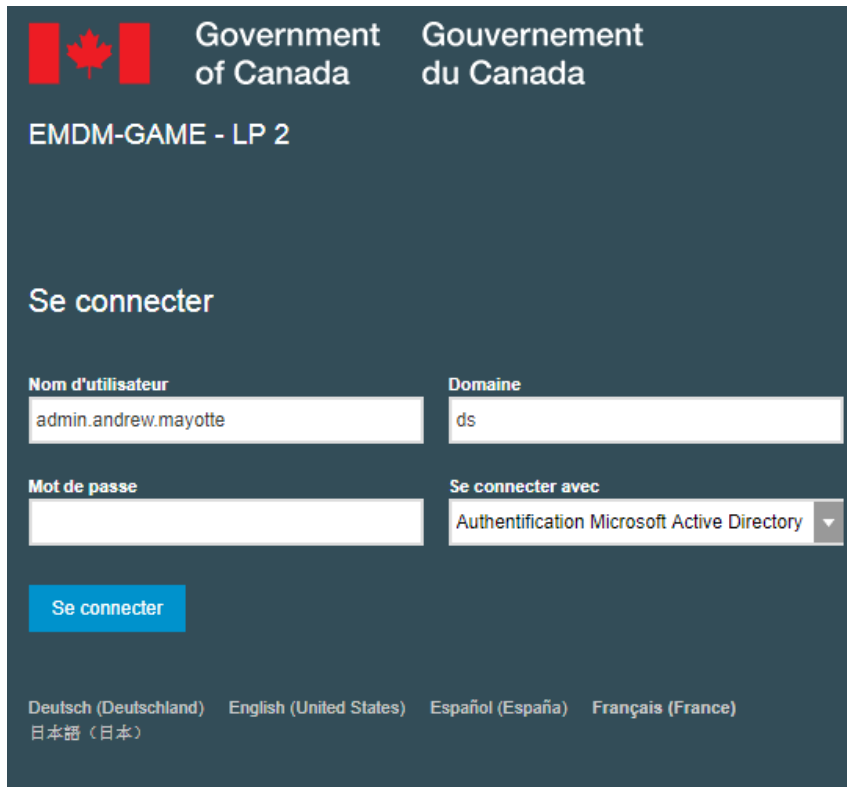
9) La page d'authentification de la console d'administrateur de la GAME s'affiche



10) Ajoutez la console d'administrateur de la GAME à la barre des favoris de Firefox pour y accéder plus rapidement dans le futur.

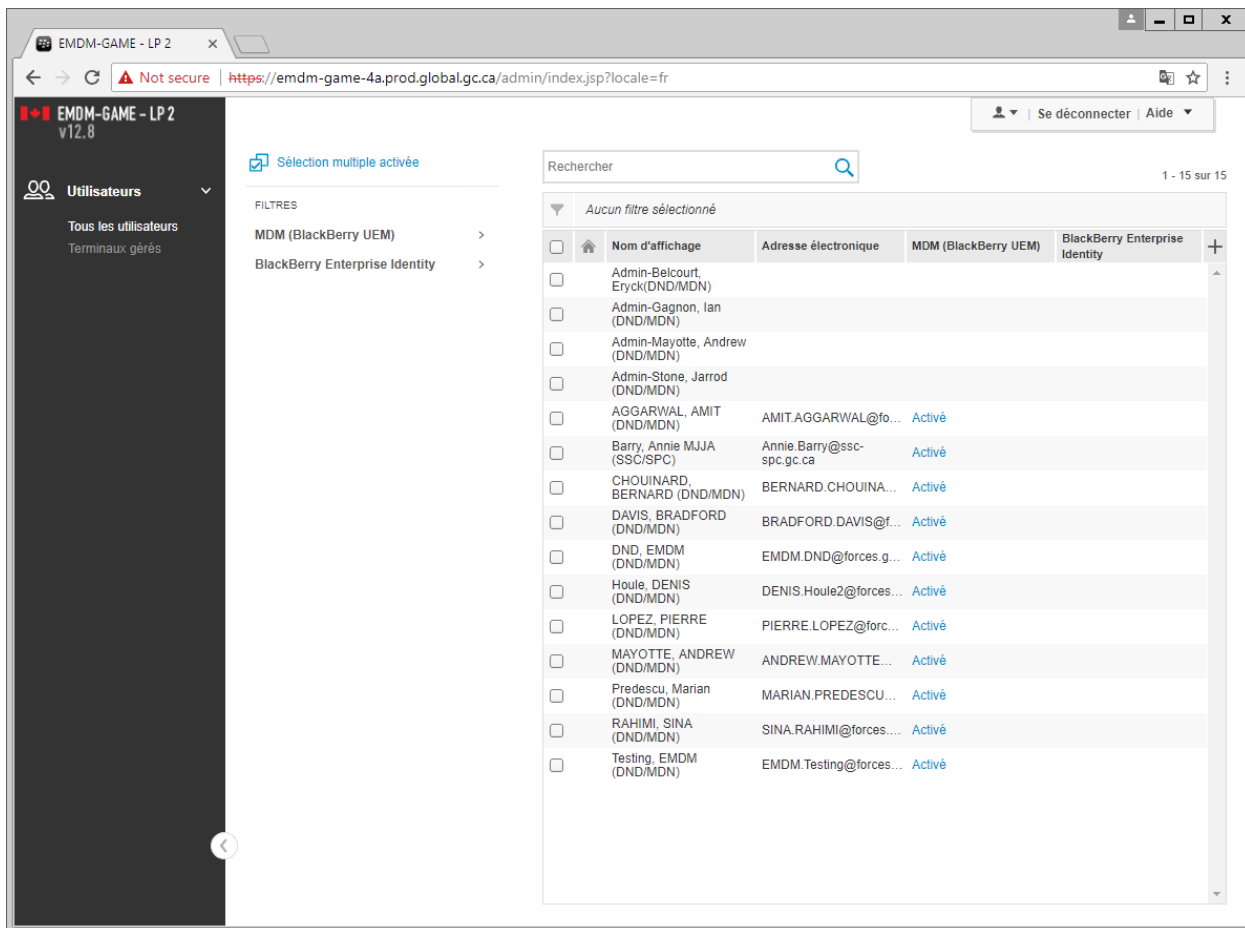


- 11) Entrez votre nom d'utilisateur (admin.prénom.nomdefamille) et mot de passe. Ensuite, sélectionnez Se connecter. *Remarque : Ne touchez pas aux champs Domaine et Se connecter avec.*



The screenshot shows a login page for the Government of Canada. At the top, there is a logo with the Canadian flag and the text "Government of Canada" and "Gouvernement du Canada". Below this, the page title "EMDM-GAME - LP 2" is displayed. The main heading is "Se connecter". There are four input fields: "Nom d'utilisateur" (username) containing "admin.andrew.mayotte", "Domaine" (domain) containing "ds", "Mot de passe" (password), and "Se connecter avec" (login method) set to "Authentification Microsoft Active Directory". A blue "Se connecter" button is located below the password field. At the bottom, there are language options: "Deutsch (Deutschland)", "English (United States)", "Español (España)", "Français (France)", and "日本語 (日本)".

12) Une fois connectée à la console, vous percevrez la page ci-dessous :

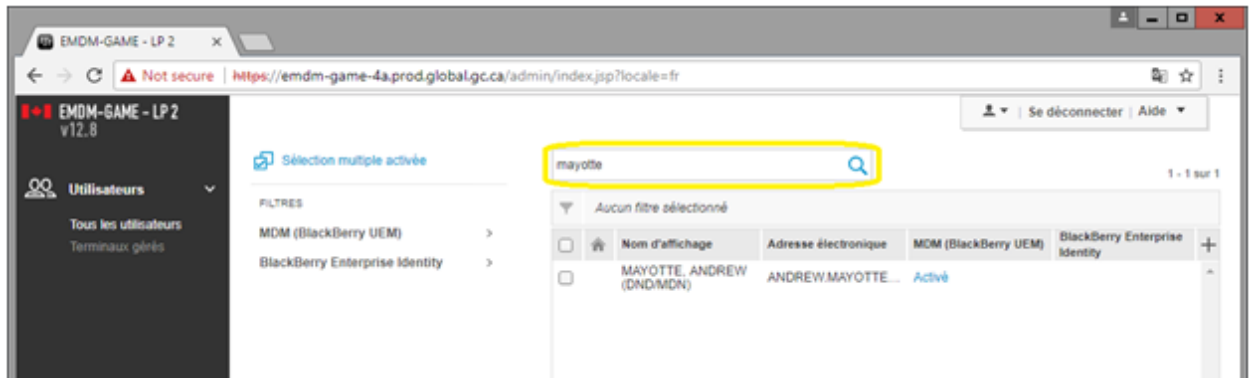


4. Gestion des appareils mobiles

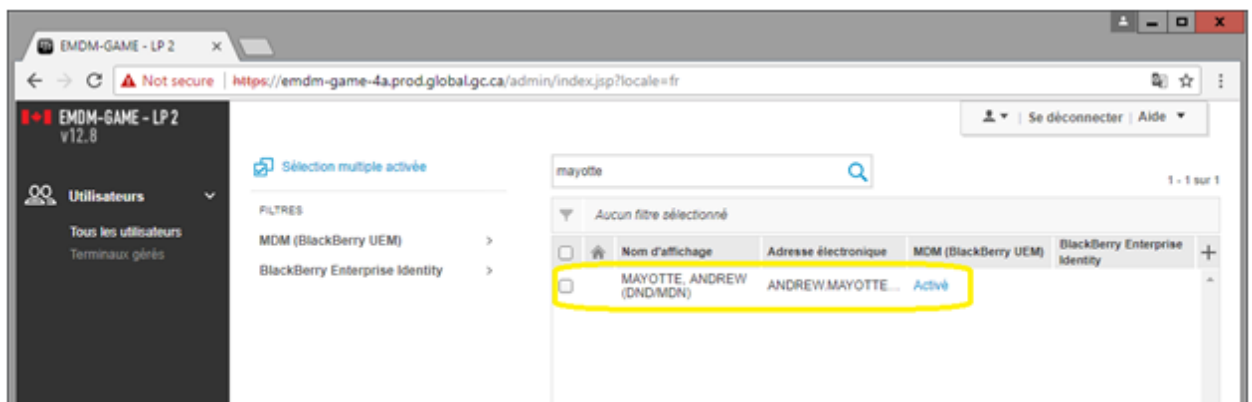
4.1 Recherche rapide d'utilisateur (Android et iOS)

Cette fonction permet à l'administrateur de la GAME de trouver rapidement un utilisateur afin de gérer leur appareil mobile.

1. Recherchez l'utilisateur à l'aide de la fonction de recherche rapide d'utilisateur. Tapez le nom complet de l'utilisateur pour préciser la recherche.



2. Cliquez sur l'utilisateur afin d'afficher leur compte de la GAME



3. Le compte de la GAME de l'utilisateur s'affiche vous permettant de gérer leur appareil mobile

The screenshot shows the EMDM-GAME administrator console. The main content area displays user management for 'MAYOTTE, ANDREW (DND/MDN)'. There are filters for 'All users', 'Dept - DND-MDM', 'Global - Certificates (Indirect)', and 'Global - Distribution (Indirect)'. Below the filters, there are two circular icons: 'TERMINAUX GÉRÉS' (with a '1' notification) and 'ENTERPRISE IDENTITY'. A 'Synthèse des données utilisateur' section shows 'Samsung Galaxy S7' with '1 sur 10 terminaux activés'. A 'Mot de passe d'activation du terminal' section indicates it expired on '31 mai 2018 13:37 (-04:00)' and includes a 'Définir le mot de passe d'activation' button. A 'BlackBerry 2FA' section provides instructions for activation. On the right, a 'Stratégie informatique et profils' table lists assigned profiles.

Profil attribué	Attribution	État
WP-04 Stratégie informatique	Groupe	
DND E-mail	Groupe	
Work and Personal Activation	Groupe	
MDM Connectivity Connectivité d'entreprise	Groupe	
Default Conformité	Par défaut	
Default BlackBerry Dynamics	Par défaut	
Default Connectivité BlackBerry Dynamics	Par défaut	
Default Enterprise Management Agent	Par défaut	

4.2 Réinitialiser le mot de passe de déverrouillage de l'appareil (Android et iOS)

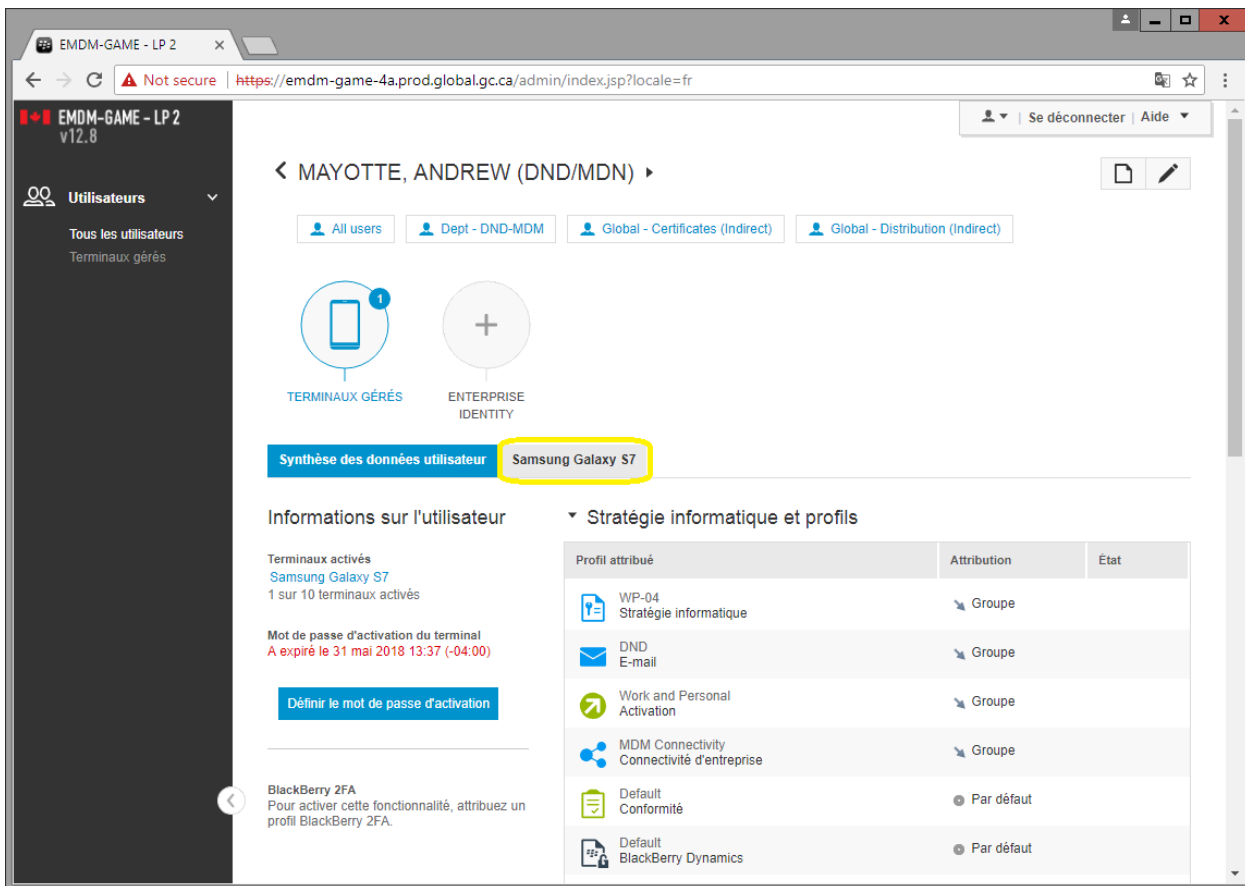
L'appareil doit être connecté à un réseau cellulaire ou Wifi afin de réinitialiser le mot de passe de déverrouillage de l'appareil.

Remarque pour les appareils Android : Les appareils Android ont 2 mots de passe différents, un pour déverrouiller l'appareil et un pour accéder à l'espace de travail Knox. L'utilisateur peut choisir d'utiliser le même mot de passe pour les deux. S'il le fait, il aura probablement besoin d'une [réinitialisation du mot de passe de l'espace de travail Knox](#) en plus d'une réinitialisation du mot de passe de déverrouillage de l'appareil.

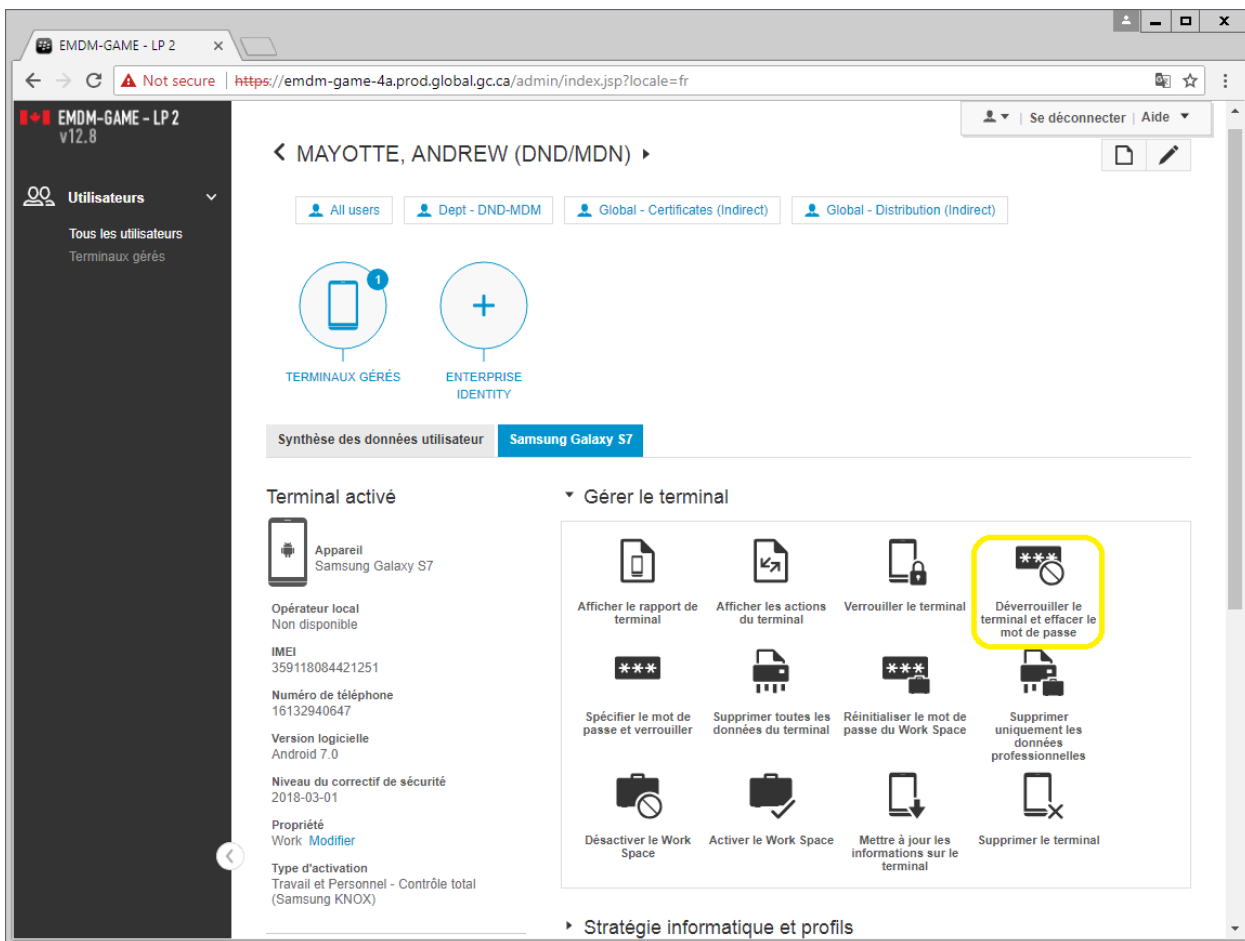
Remarque pour les appareils iOS : Les appareils iOS utilisent un seul mot de passe pour déverrouiller l'appareil et accéder aux applications professionnelles.

- 1) Recherchez l'utilisateur et ouvrez leur compte de la GAME

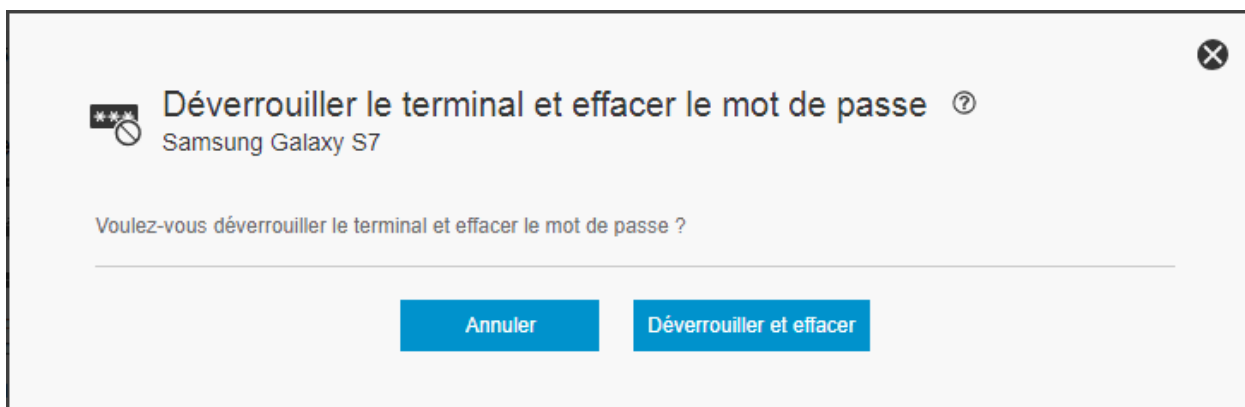
- 2) Sous le compte de l'utilisateur, sélectionnez l'appareil mobile de l'utilisateur (par exemple, Samsung Galaxy S7 ou Apple iPhone 8).



- 3) Sous Gérer le terminal, sélectionnez **Déverrouillez le terminal et effacer le mot de passe**

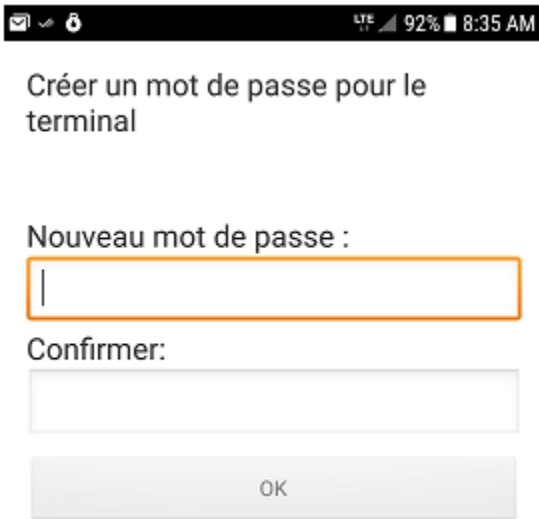


- 4) Dans la fenêtre Déverrouillez le terminal et effacer le mot de passe, sélectionnez **Déverrouillez et effacer**

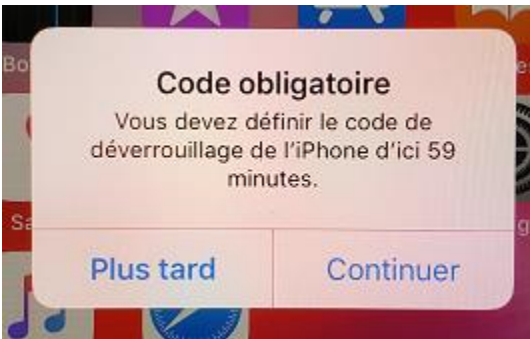


- 5) En l'espace d'une minute ou deux, l'appareil de l'utilisateur sera déverrouillé et il sera invité à créer un nouveau mot de passe de déverrouillage.

Appareil Android :



Appareil iOS :

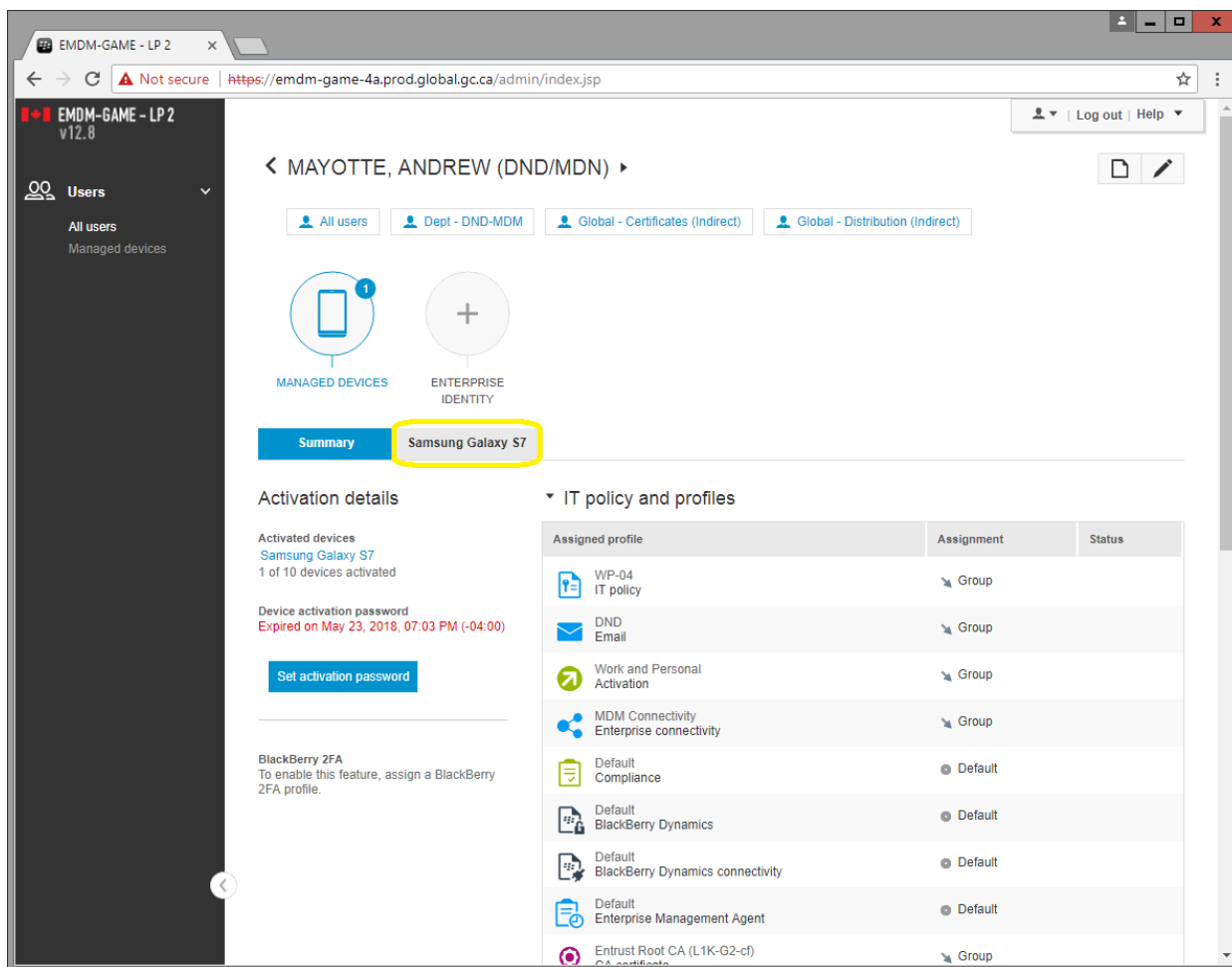


4.3 Réinitialiser le mot de passe de l'espace de travail Knox (Android seulement)

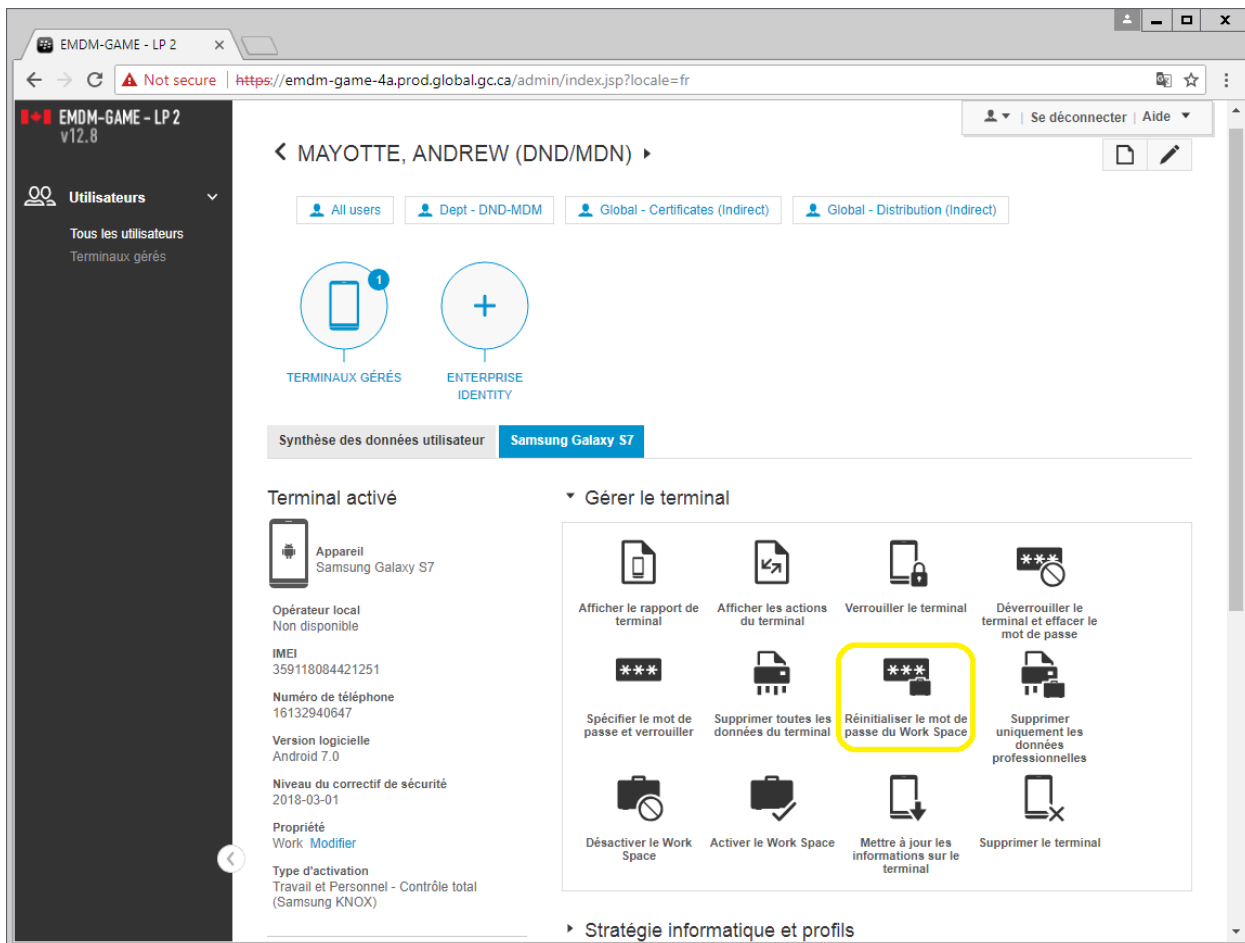
L'appareil doit être connecté à un réseau cellulaire ou Wifi afin de réinitialiser le mot de passe de l'espace de travail Knox

Cette fonction réinitialise le mot de passe de l'espace de travail Knox et invite l'utilisateur à créer un nouveau mot de passe.

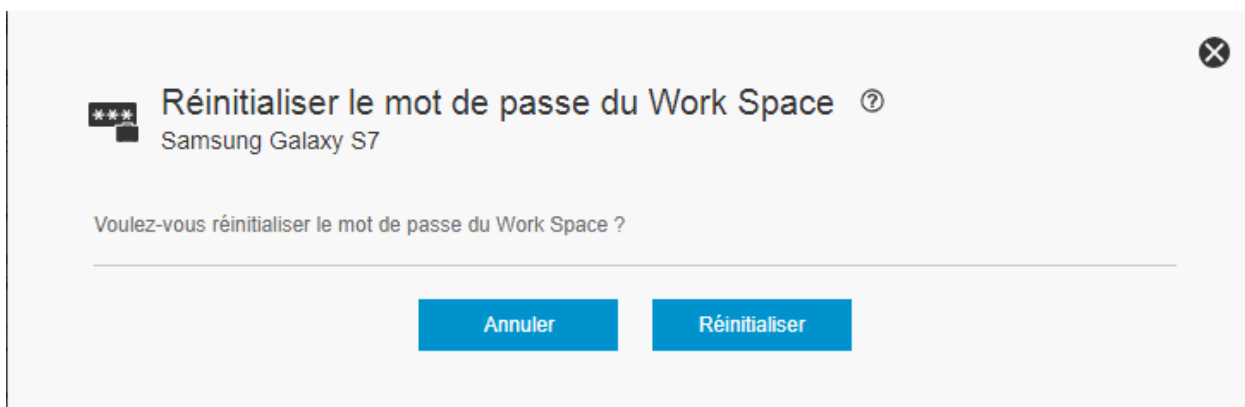
- 1) Recherchez l'utilisateur et ouvrez leur compte de la GAME
- 2) Sous le compte de l'utilisateur, sélectionnez l'appareil mobile Android de l'utilisateur (par exemple, Samsung Galaxy S7).



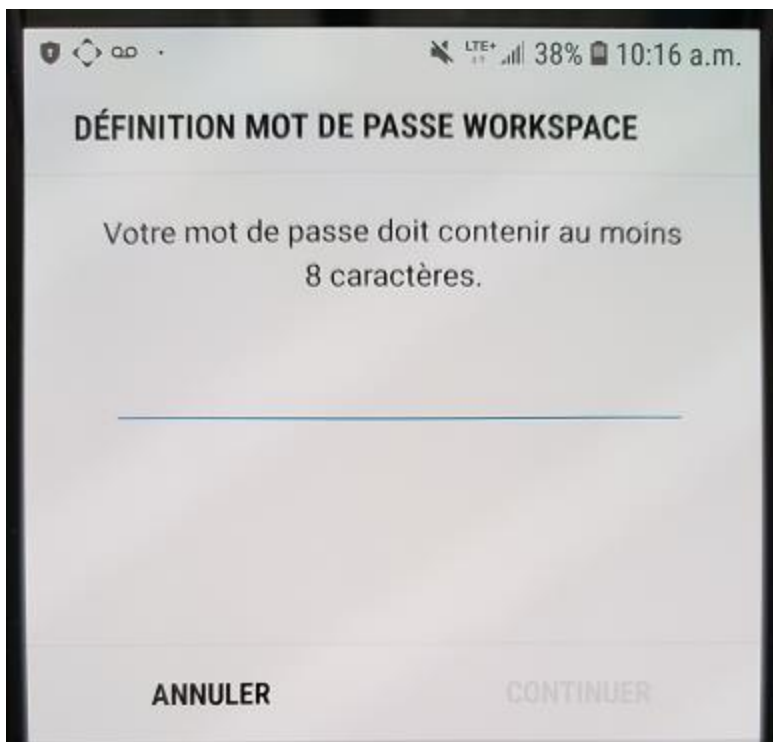
- 3) Sous Gérer le terminal, sélectionnez **Réinitialiser le mot de passe du Work Space**



4) Dans la fenêtre Réinitialiser le mot de passe du Work Space, sélectionnez **Réinitialiser**



5) En l'espace d'une minute ou deux, l'utilisateur sera invité à créer un nouveau mot de passe de l'espace de travail Knox



4.4 Supprimer les données de l'appareil à distance (Android et iOS)

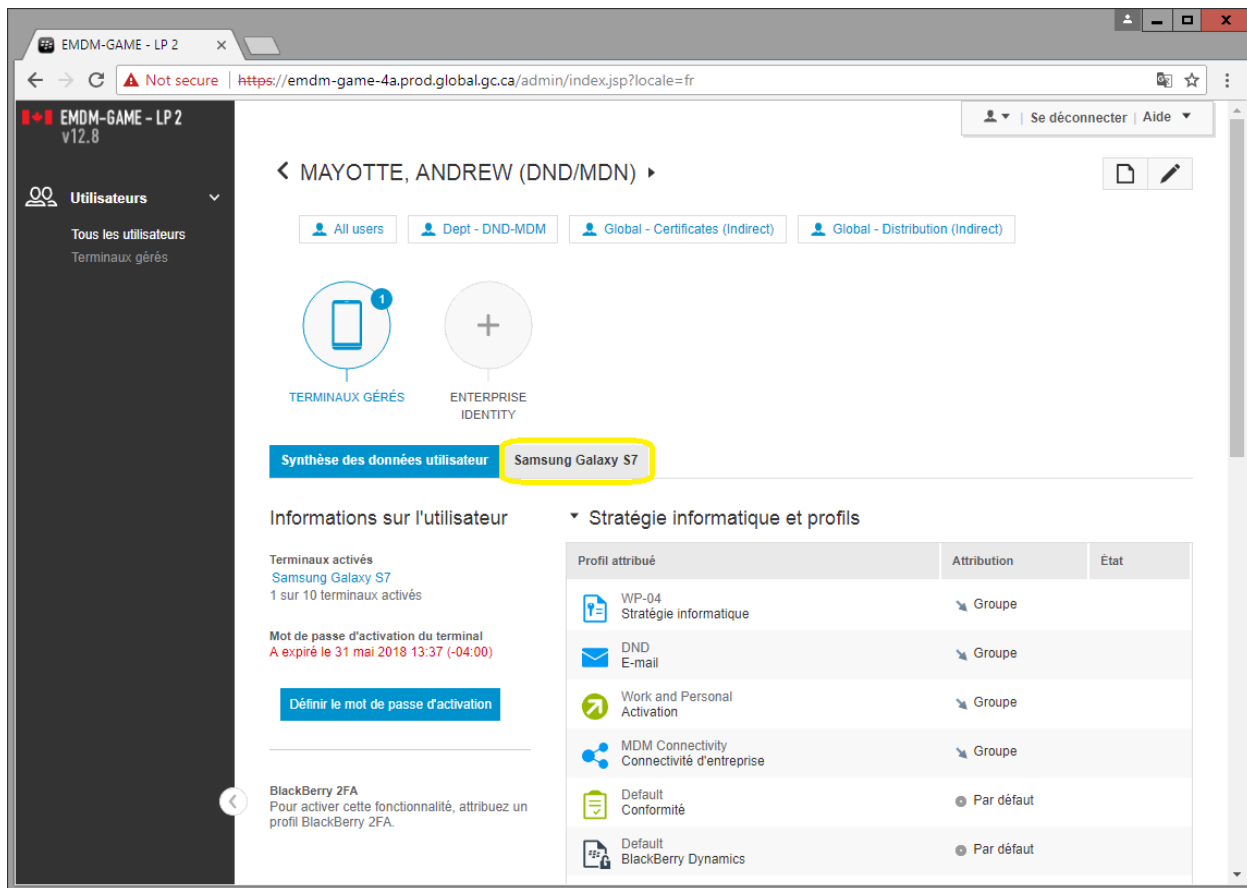
L'appareil doit être connecté à un réseau cellulaire ou Wifi afin de supprimer les données de l'appareil à distance.

Cette fonction supprime toutes les données de l'appareil et effectue une réinitialisation des paramètres par défaut.

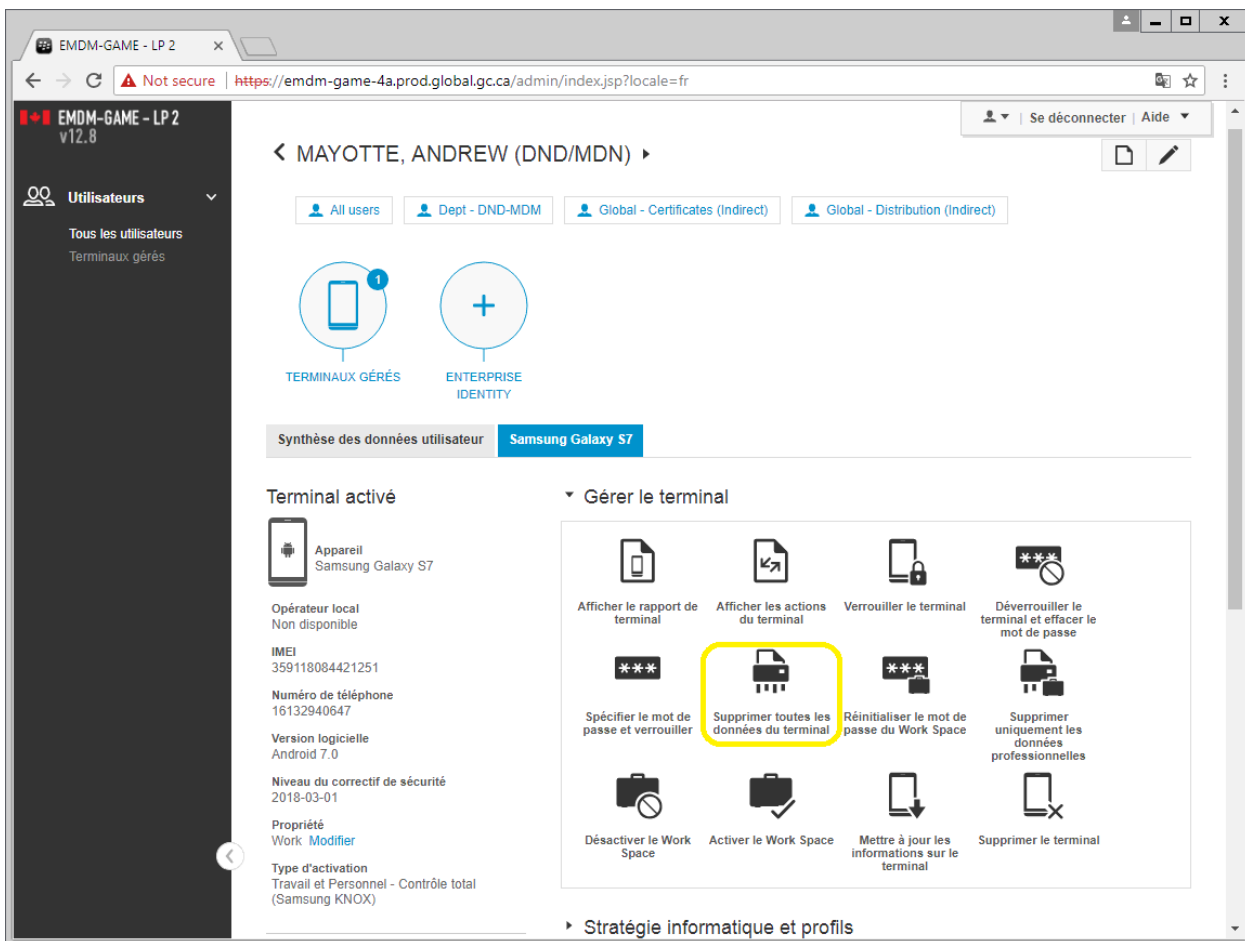
Remarque pour les appareils Android : Cette fonction désactive également la protection de l'appareil Google.

Remarque pour les appareils iOS : Cette fonction ne désactive PAS le verrouillage d'activation d'Apple. Si un utilisateur était connecté à l'appareil avec un compte iCloud / Apple, l'appareil exigera ce compte après l'effacement.

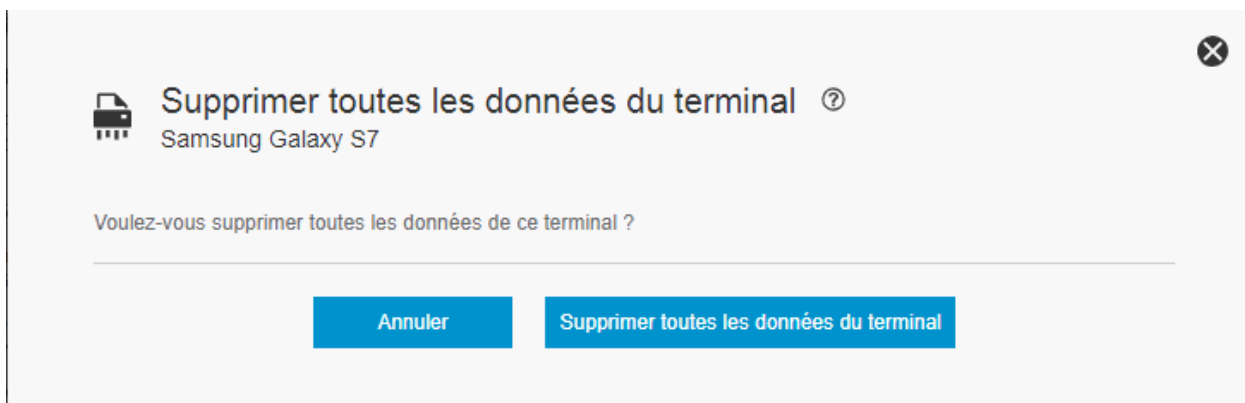
- 1) Recherchez l'utilisateur et ouvrez leur compte de la GAME
- 2) Sous le compte de l'utilisateur, sélectionnez l'appareil mobile de l'utilisateur (par exemple, Samsung Galaxy S7 ou Apple iPhone 8).



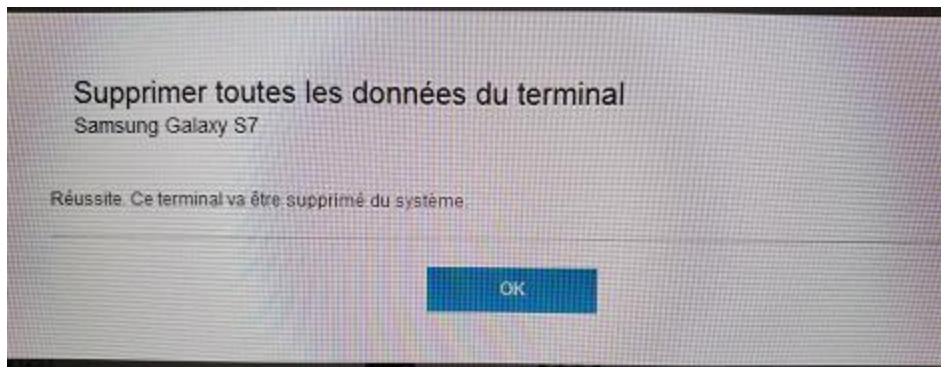
- 3) **Important:** Si l'appareil a été perdu ou volé, notez toutes les informations pertinentes de l'appareil (marque, modèle, numéro IMEI, numéro de téléphone, opérateur, etc.), car ces informations seront nécessaires pour l'enquête de la police militaire et pour demander un appareil de remplacement.
- 4) Sous Gérer le terminal, sélectionnez **Supprimer toutes les informations du terminal**



- 5) Dans la fenêtre Supprimer toutes les données du terminal, sélectionnez **Supprimer toutes les données du terminal**



- 6) En l'espace d'une minute ou deux, l'appareil effacera toutes les données et effectuera une réinitialisation des paramètres par défaut. La console d'administrateur de la GAME affiche une confirmation lorsque l'effacement à distance est réussi.



Appareil Android :



Appareil iOS :

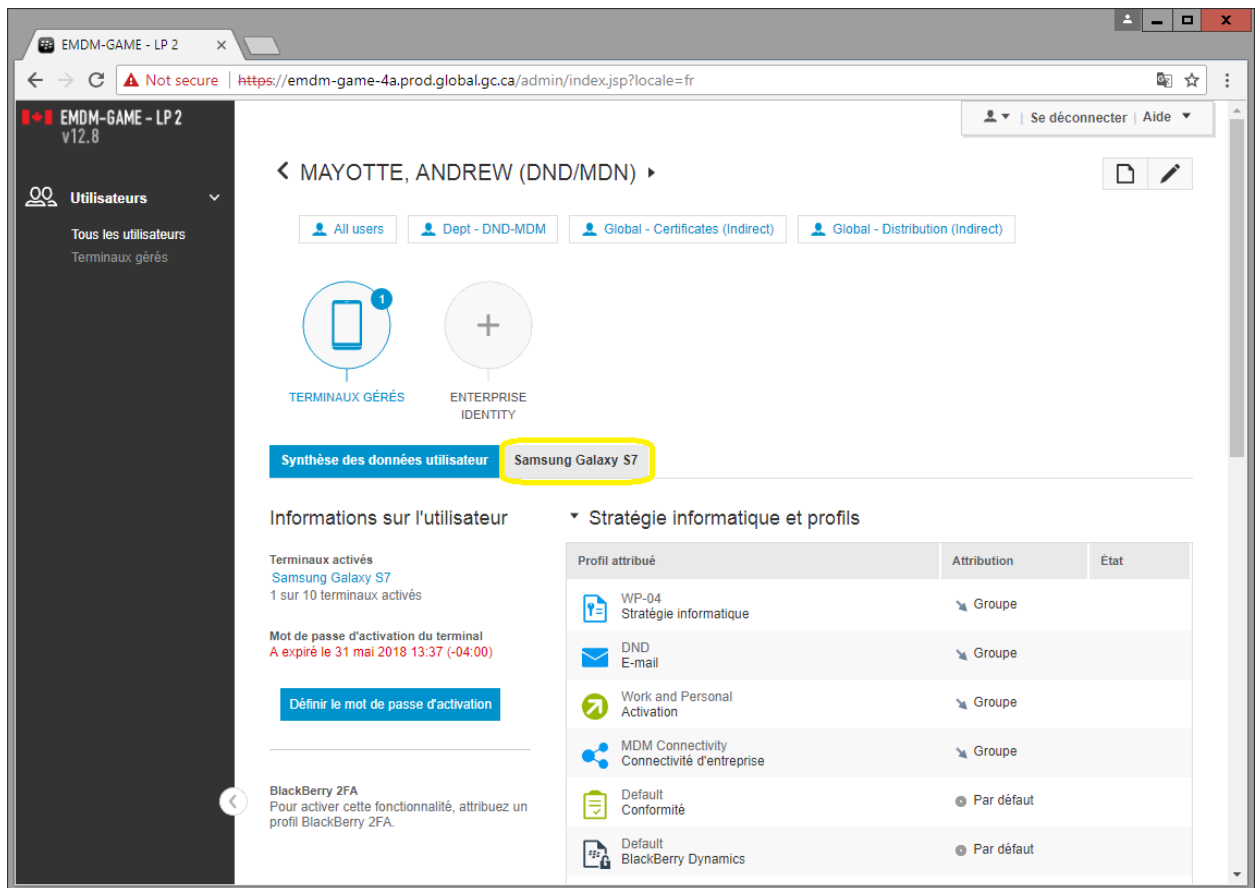


4.5 Désactiver/Réactiver l'espace de travail Knox (Android seulement)

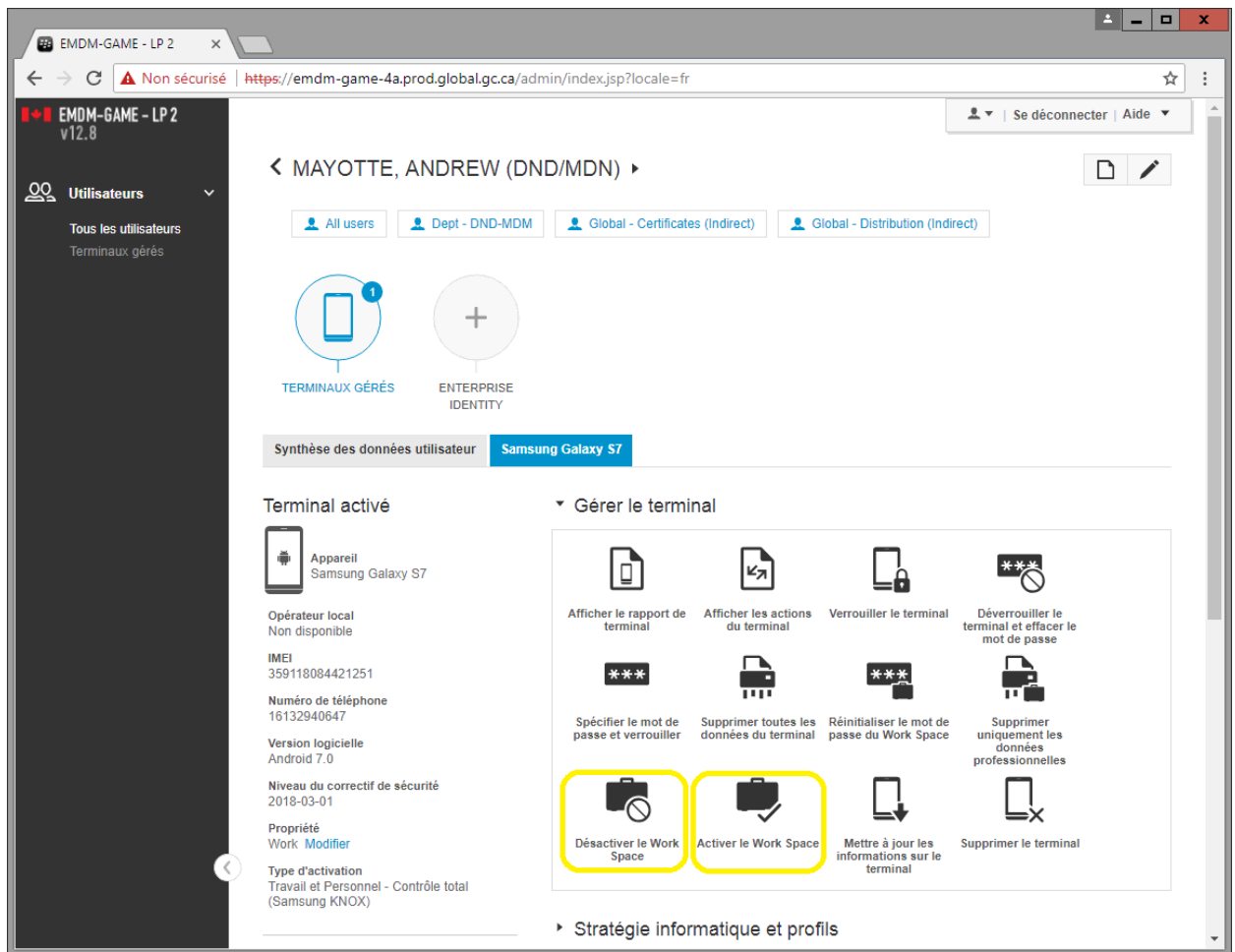
L'appareil doit être connecté à un réseau cellulaire ou Wifi afin de désactiver/réactiver l'espace de travail Knox.

Cette fonction désactive ou réactive l'accès à l'espace de travail Knox d'un appareil Android. La fonction ne supprime pas l'espace de travail.

- 1) Recherchez l'utilisateur et ouvrez leur compte de la GAME
- 2) Sous le compte de l'utilisateur, sélectionnez l'appareil Android de l'utilisateur (par exemple, Samsung Galaxy S7).

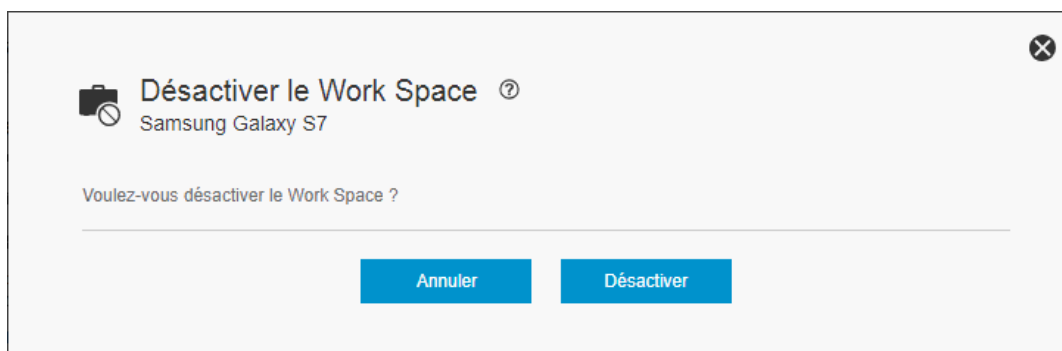


- 3) Sous Gérer le terminal, sélectionnez soit **Déactiver le Work Space** ou **Activer le Work Space** selon les circonstances

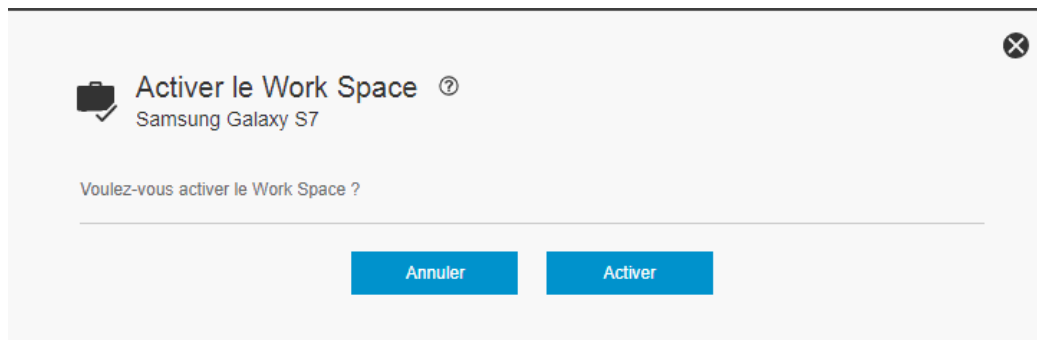


4) Confirmez votre choix

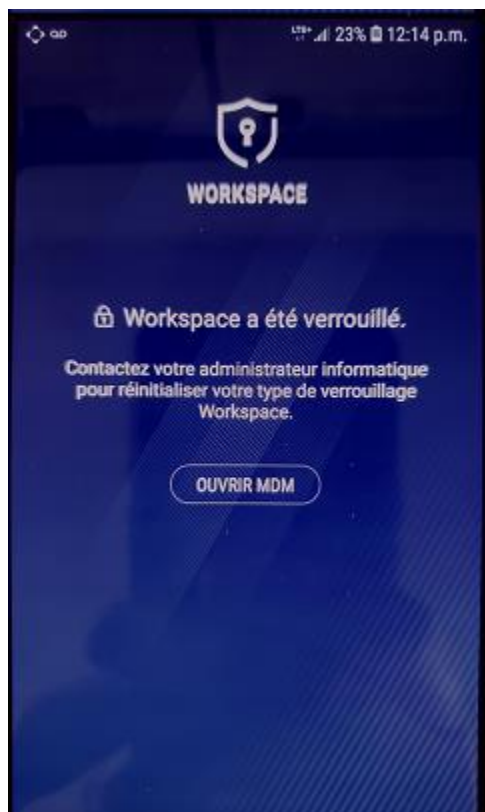
Désactiver :



Activer :



Remarque : Lorsque l'espace de travail est désactivé, le message ci-dessous apparaît sur l'appareil lorsque l'utilisateur tente d'accéder à l'espace de travail Knox:



4.6 Définir le mot de passe d'activation (Android et iOS)

Cette fonction définit un mot de passe d'activation afin d'activer un nouvel appareil ou réactiver un appareil existant.

Remarque : les instructions pour activer un appareil mobile sont disponibles séparément de ce document.

- 1) Recherchez l'utilisateur et ouvrez leur compte de la GAME
- 2) Sous Informations sur l'utilisateur, sélectionnez **Définir le mot de passe d'activation**

- 3) Dans la fenêtre Définir le mot de passé d'activation du terminal :
- a. **Option d'activation** : *Activation du terminal par défaut*
 - b. **Mot de passe d'activation** : *Définir le mot de passe d'activation du terminal*
 - c. **Mot de passe d'activation du terminal** : *Définis un mot de passe de votre choix (par exemple, Canada150)*
 - d. **Expiration de la période d'activation du terminal** : *Définis une période de votre choix (par exemple, 2 jours)*
 - e. **La période d'activation expire à l'issue de l'activation du premier terminal** : *Facultative*
 - f. **Modèle d'email d'activation** :
 - i. *Android: Default activation email*
 - ii. *iOS: Apple DEP activation email*

Android :

✕

Définir le mot de passe d'activation du terminal

Activation du terminal

Option d'activation *

Activation du terminal par défaut
▼

Mot de passe d'activation *

Définir le mot de passe d'activation du terr
▼

Mot de passe d'activation du terminal *

.....
👁

Expiration de la période d'activation *

2

jours

▼

La période d'activation expire à l'issue de l'activation du premier terminal

Modèle d'e-mail d'activation

Default activation email
▼

Annuler

Appliquer

iOS :

The screenshot shows a dialog box titled "Définir le mot de passe d'activation du terminal" with a close button (X) in the top right corner. The dialog contains the following fields and options:

- Activation du terminal**
 - Option d'activation *: "Activation du terminal par défaut" (dropdown)
- Mot de passe d'activation *: "Définir le mot de passe d'activation du tei" (dropdown)
- Mot de passe d'activation du terminal *: A text input field with three dots and a toggle icon.
- Expiration de la période d'activation *
 - Input: "2" (text), "jours" (dropdown)
 - La période d'activation expire à l'issue de l'activation du premier terminal
- Modèle d'e-mail d'activation: "Apple DEP activation email" (dropdown)

At the bottom of the dialog are two buttons: "Annuler" and "Appliquer".

- 4) Sélectionnez **Appliquer** pour définir le mot de passe d'activation. Un courrier électronique sera envoyé à l'utilisateur avec les informations (mot de passe d'activation, par exemple) nécessaires à l'activation de l'appareil.

4.7 Redémarrer l'appareil à distance (iOS seulement)

L'appareil doit être connecté à un réseau cellulaire ou Wifi afin de le redémarrer à distance.

Vous pouvez redémarrer à distance un appareil iOS à partir de la console d'administrateur de la GAME.

- 1) Recherchez l'utilisateur et ouvrez leur compte de la GAME
- 2) Sous le compte de l'utilisateur, sélectionnez l'appareil iOS de l'utilisateur (par exemple, Apple iPhone 8).

EMDM-GAME - LP2

https://emdm-game-4a.prod.global.gc.ca/admin/index.jsp?locale=fr

EMDM-GAME - LP2

Se déconnecter | Aide

< MAYOTTE, ANDREW (DND/MDN) >

All users | Dept - DND-MDM | Global - Certificats (Indirect) | Global - Distribution (Indirect)

TERMINAUX GÉRÉS | ENTERPRISE IDENTITY

Synthèse des données utilisateur | **Apple iPhone 8 (GSM)** | Samsung Galaxy S7

Terminal activé

Appareil
Apple iPhone 8 (GSM)

SUPERVISÉ

Opérateur local
Rogers

IMEI
35 608709 440504 7

Numéro de téléphone
+13439613202

Version logicielle
ios 12.1.4

Propriété
Work: Modifier

Type d'activation
Contrôles MDM

Date et heure de l'activation
Février 13, 2019, 12:05 PM (-05:00)

Gérer le terminal

Afficher le rapport de terminal | Afficher les actions du terminal | Verrouiller le terminal | Déverrouiller le terminal et effacer le mot de passe | Supprimer toutes les données du terminal

Supprimer uniquement les données professionnelles | Mettre à jour les informations sur le terminal | Redémarrer le terminal | Supprimer le terminal

Stratégie informatique et profils

Applications

Applications BlackBerry Dynamics

3) Sous Gérer le terminal, sélectionnez **Redémarrer le terminal**

The screenshot shows the EMDM-GAME - LP2 administrator console. The user profile is MAYOTTE, ANDREW (DND/MDN). The device being managed is an Apple iPhone 8 (GSM). The 'Gérer le terminal' section is expanded, showing various actions: 'Afficher le rapport de terminal', 'Afficher les actions du terminal', 'Verrouiller le terminal', 'Déverrouiller le terminal et effacer le mot de passe', 'Supprimer toutes les données du terminal', 'Supprimer uniquement les données professionnelles', and 'Redémarrer le terminal'. The 'Redémarrer le terminal' option is highlighted with a yellow box.

4) Dans la fenêtre Redémarrer le terminal, sélectionnez **Redémarrer**

The screenshot shows a dialog box titled 'Redémarrer le terminal' for an Apple iPhone 8 (GSM). The dialog asks 'Voulez-vous redémarrer le terminal ?' and has two buttons: 'Annuler' and 'Redémarrer'.

5) En l'espace d'une minute ou deux, l'appareil iOS redémarrera.

4.8 Afficher le rapport de l'appareil (Android et iOS)

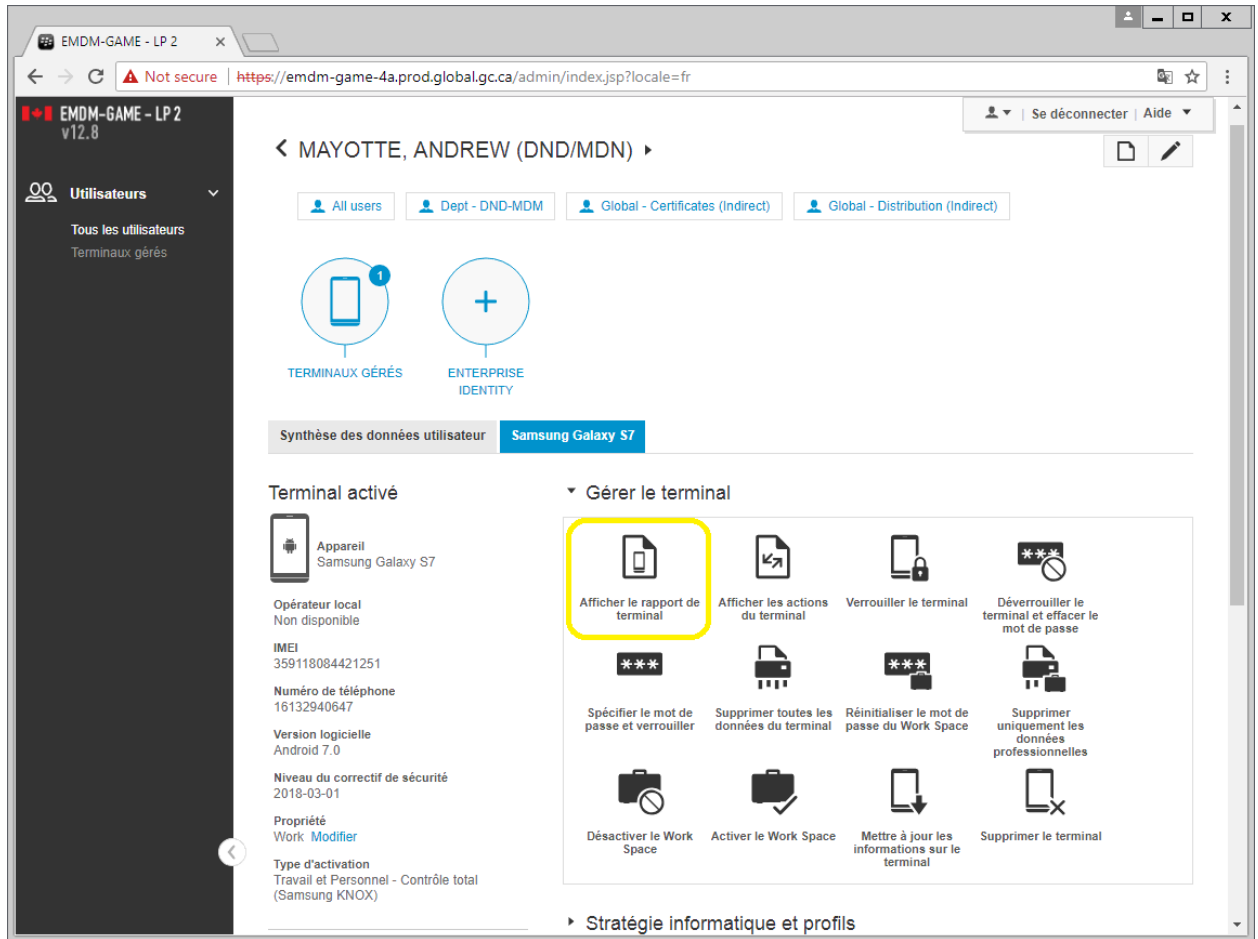
Vous pouvez afficher des informations détaillées sur l'appareil d'un utilisateur (par exemple, l'heure du dernier contact, le numéro de téléphone, la version du système d'exploitation, etc.) à partir de la console d'administrateur de la GAME.

- 1) Recherchez l'utilisateur et ouvrez leur compte de la GAME
- 2) Sous le compte de l'utilisateur, sélectionnez l'appareil l'utilisateur (par exemple, Samsung Galaxy S7 ou Apple iPhone 8).

The screenshot shows the EMDM-GAME administrator console. The user profile for 'MAYOTTE, ANDREW (DND/MDN)' is displayed. The 'TERMINAUX GÉRÉS' section shows 'Samsung Galaxy S7' as the active device. The 'Stratégie informatique et profils' section lists various profiles and their status.

Profil attribué	Attribution	État
WP-04 Stratégie informatique	Groupe	
DND E-mail	Groupe	
Work and Personal Activation	Groupe	
MDM Connectivity Connectivité d'entreprise	Groupe	
Default Conformité		Par défaut
Default BlackBerry Dynamics		Par défaut

- 3) Sous Gérer le terminal, sélectionnez **Afficher le rapport de terminal**



- 4) Une fenêtre apparaît affichant les informations détaillées de l'appareil. Vous pouvez extraire le rapport dans un fichier .csv en sélectionnant la flèche dans le coin supérieur droit.

BlackBerry UEM - Google Chrome

Not secure | <https://emdm-game-4a.prod.global.gc.ca/admin/device/viewDeviceReport.do?deviceId=52&userId=101...>

Rapport de terminal

MAYOTTE, ANDREW (DNDVMDN)
ANDREW.MAYOTTE@forces.gc.ca

Samsung Galaxy S7

Violations de conformité définies par le profil de conformité attribué

Violation du système d'exploitation	Faux
Une application non attribuée est installée	Faux
L'application requise n'est pas installée	Faux
L'application restreinte est installée sur le terminal	Faux
La version restreinte du SE est installée sur le terminal	Faux
Modèle de terminal restreint	Faux
Le niveau de correctif de sécurité requis n'est pas installé	Faux

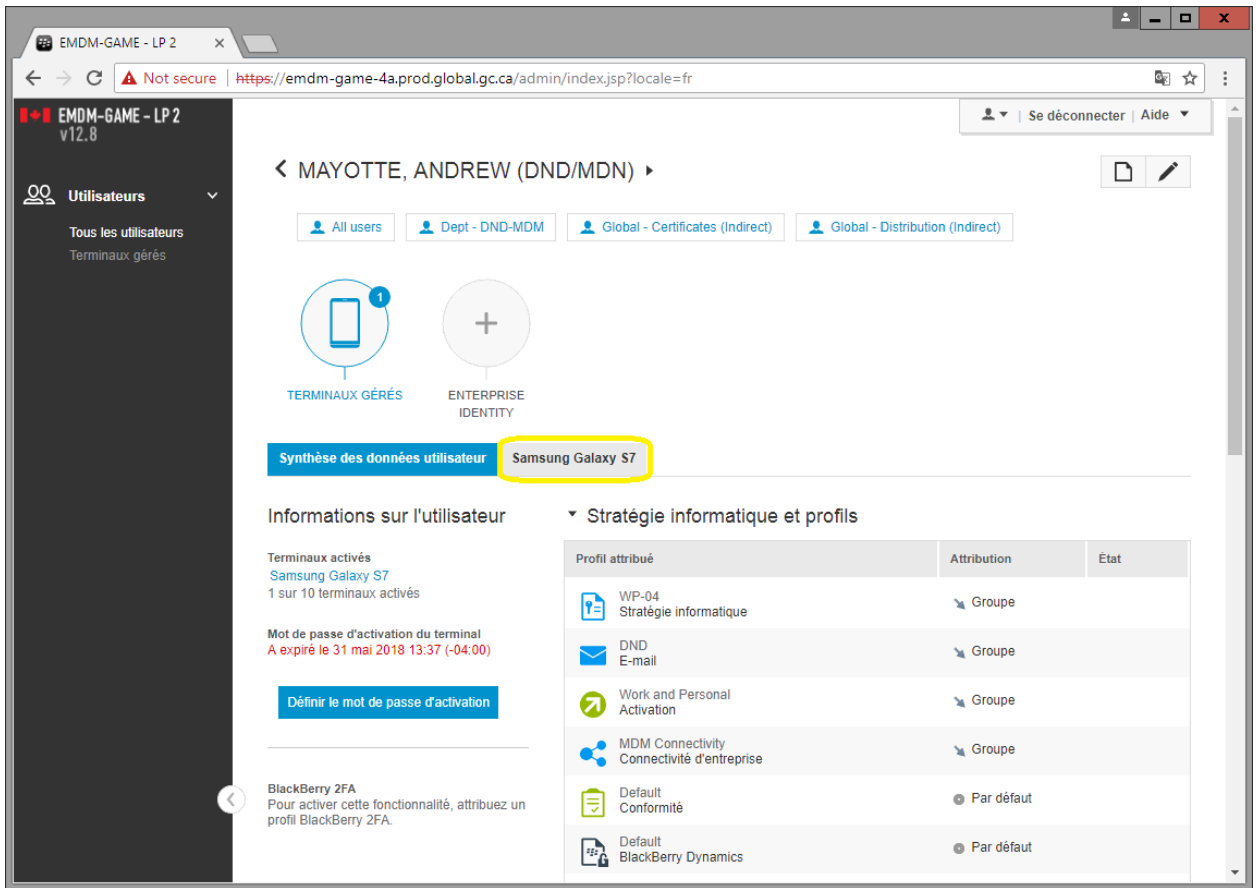
Général

Nom du fournisseur de matériel	Samsung Electronics
ID de modèle	heroltebmc
Numéro de modèle	Galaxy S7
Facteur de forme du terminal	Terminal mobile
Version du système d'exploitation	Android 7.0
Propriété du terminal	Professionnel
État de l'activation	Le terminal est activé.
Date et heure de l'activation	mai 29, 2018 2:12:22 PM (-04:00)
Dernier contact	juin 4, 2018 8:50:35 AM (-04:00)
Niveau de la batterie	80.0
UDID	146e16ef9a7d0e142b9891413ded8f6e88afe53150643f77769feac37fde833d
Langue	en_CA
IMEI	359118084421251
UUID du périmètre	279544ca-a71b-4c3f-a097-01e2d37fe6dd
Nombre de réactivations	0
Dernière modification de l'état du périmètre	mai 29, 2018 2:15:26 PM (-04:00)

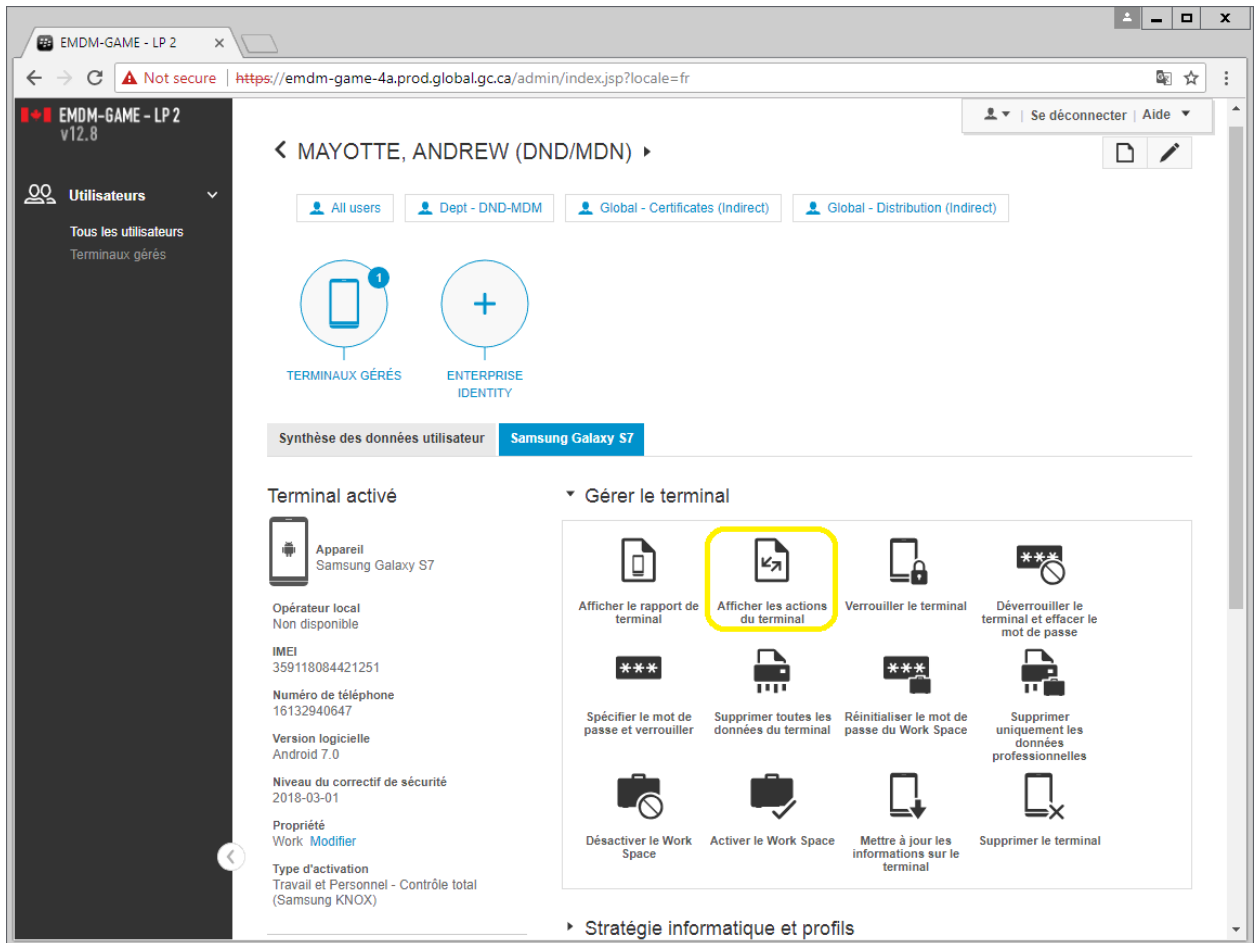
4.9 Afficher les actions de l'appareil (Android et iOS)

Cette fonction affiche les actions entreprises ou en cours sur un appareil à la suite de commandes envoyées à partir de la console d'administrateur de la GAME, telles que le déverrouillage, la réinitialisation du mot de passe de l'espace de travail Knox ou la suppression des données de l'appareil.

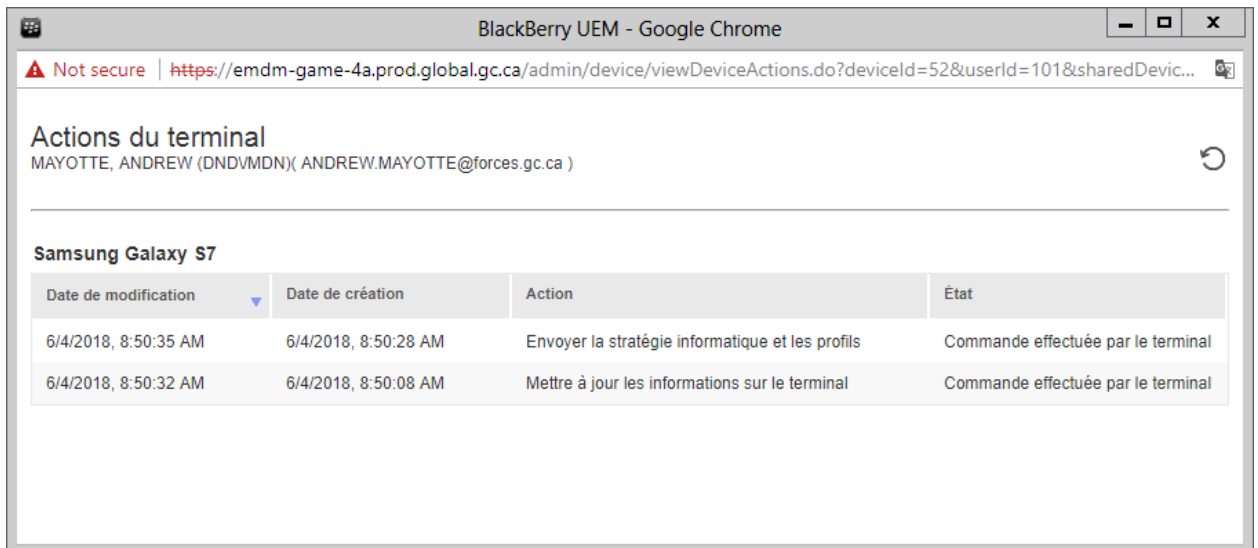
- 1) Recherchez l'utilisateur et ouvrez leur compte de la GAME
- 2) Sous le compte de l'utilisateur, sélectionnez l'appareil l'utilisateur (par exemple, Samsung Galaxy S7 ou Apple iPhone 8).



3) Sous Gérer le terminal, sélectionnez **Afficher les actions du terminal**



- 4) Une fenêtre apparaît affichant les actions entreprises ou en cours sur l'appareil à la suite de commandes envoyées à partir de la console d'administrateur de la GAME.

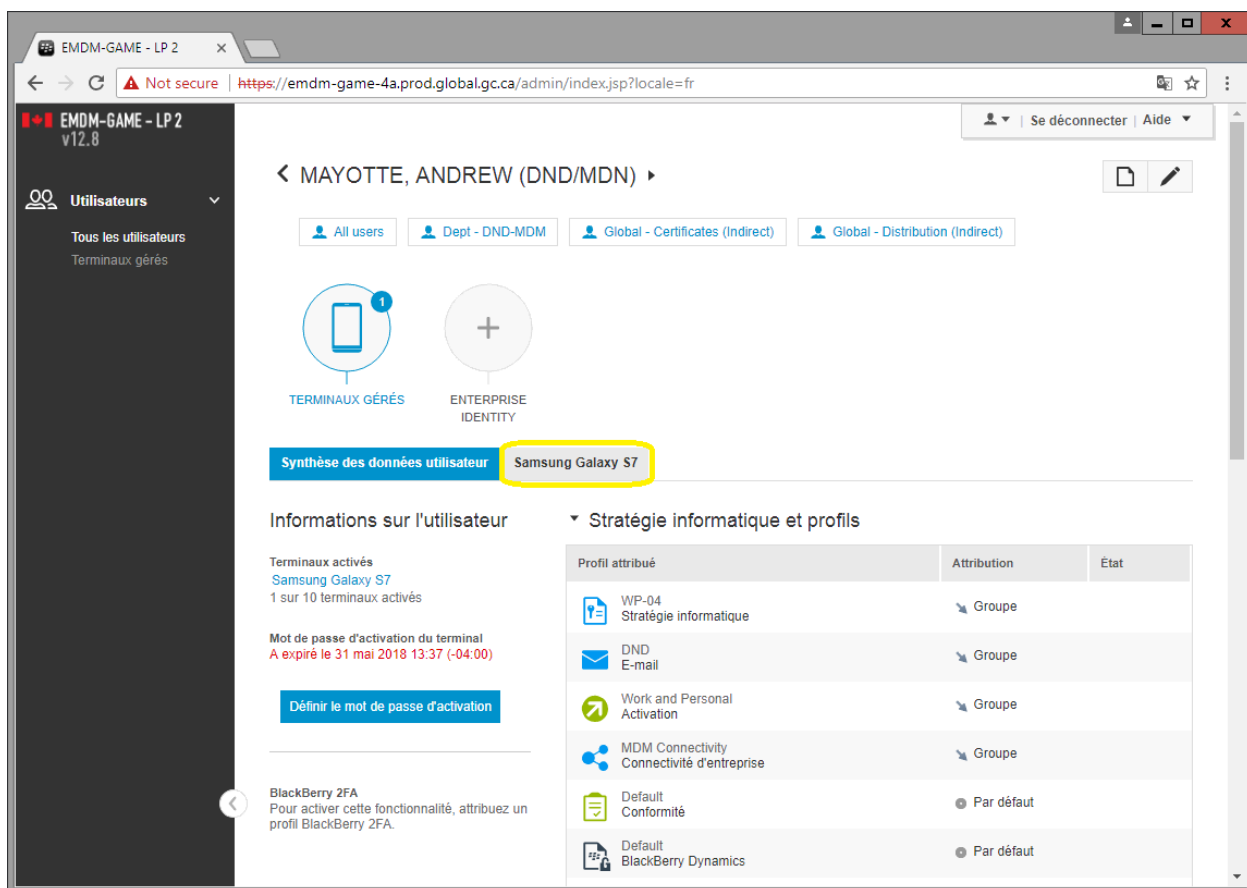


4.10 Mettre à jour les informations de l'appareil (Android et iOS)

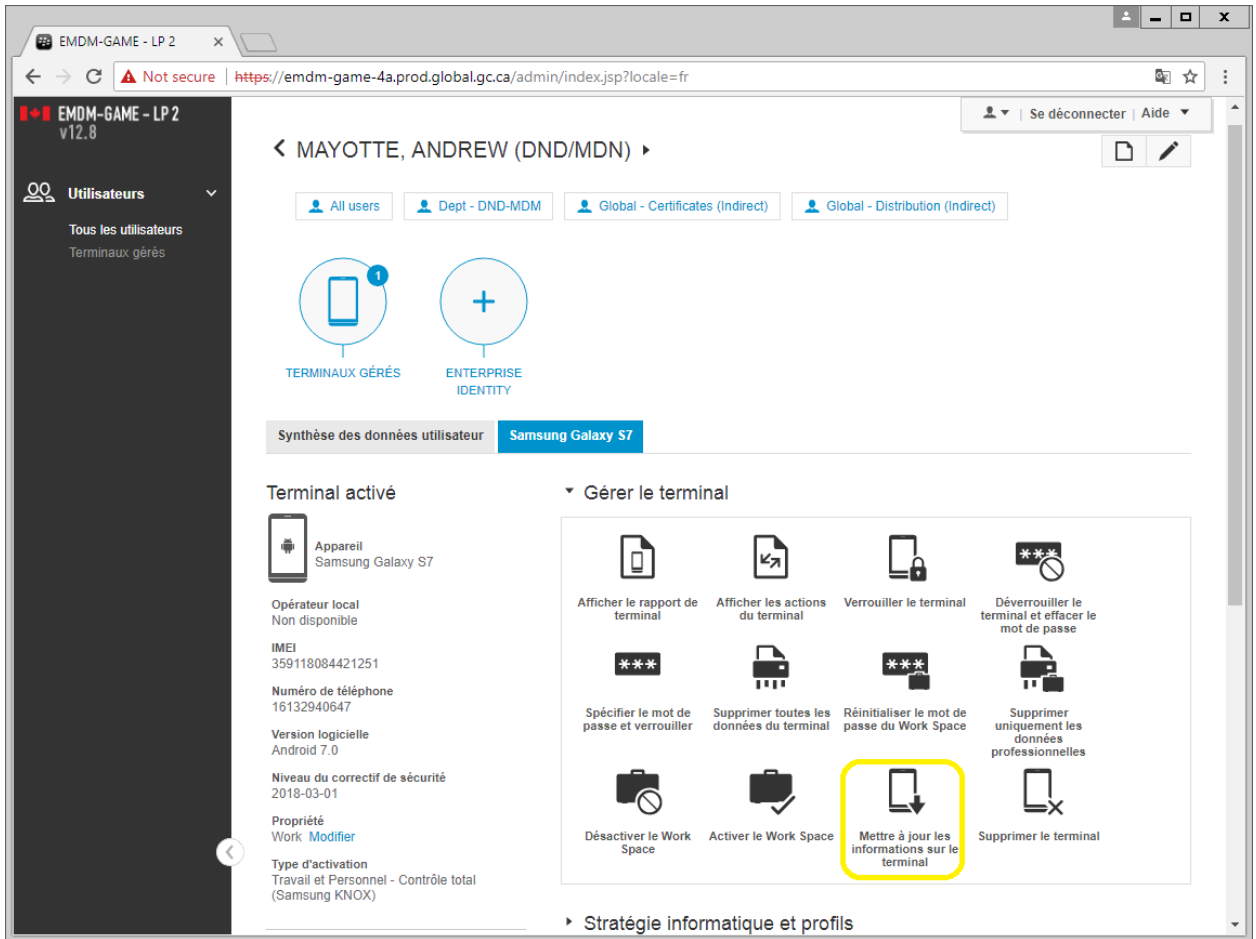
L'appareil doit être connecté à un réseau cellulaire ou Wifi afin de mettre à jour les informations de l'appareil.

Cette fonction envoie et reçoit des informations en temps réel sur l'appareil, telles que la version du système d'exploitation, l'opérateur actuel ou le niveau de la batterie.

- 1) Recherchez l'utilisateur et ouvrez leur compte de la GAME
- 2) Sous le compte de l'utilisateur, sélectionnez l'appareil l'utilisateur (par exemple, Samsung Galaxy S7 ou Apple iPhone 8).



- 3) Sous Gérer le terminal, sélectionnez **Mettre à jour les informations sur le terminal**



- 4) Un message de succès apparaît si le service de la GAME réussit à communiquer avec l'appareil afin de recevoir une mise à jour des informations.

The screenshot shows the EMDM-GAME administration interface. The browser address bar indicates the URL: <https://emdm-game-4a.prod.global.gc.ca/admin/index.jsp?locale=fr>. The user is logged in as MAYOTTE, ANDREW (DND/MDN). The interface displays a sidebar with 'Utilisateurs' and 'Tous les utilisateurs' options. The main content area shows filters for 'All users', 'Dept - DND-MDM', 'Global - Certificates (Indirect)', and 'Global - Distribution (Indirect)'. There are two main sections: 'TERMINAUX GÉRÉS' (1 terminal) and 'ENTREPRISE IDENTITY'. Below this is a 'Synthèse des données utilisateur' for a 'Samsung Galaxy S7'. The 'Terminal activé' section lists details for the device: Appareil Samsung Galaxy S7, Opérateur local Non disponible, IMEI 359118084421251, Numéro de téléphone 16132940647, Version logicielle Android 7.0, Niveau du correctif de sécurité 2018-03-01, Propriété Work (with a 'Modifier' link), and Type d'activation Travail et Personnel - Contrôle total (Samsung KNOX). The 'Gérer le terminal' section contains a grid of 12 actions: 'Afficher le rapport de terminal', 'Afficher les actions du terminal', 'Verrouiller le terminal', 'Déverrouiller le terminal et effacer le mot de passe', 'Spécifier le mot de passe et verrouiller', 'Supprimer toutes les données du terminal', 'Réinitialiser le mot de passe du Work Space', 'Supprimer uniquement les données professionnelles', 'Désactiver le Work Space', 'Activer le Work Space', 'Mettre à jour les informations sur le terminal', and 'Supprimer le terminal'. A 'Réussi' notification is visible over the first action. The bottom right corner shows 'Stratégie informatique et profils'.

- 5) Vous pouvez par la suite [Afficher le rapport de l'appareil](#) afin d'obtenir les plus récentes informations de l'appareil.

4.11 Supprimer uniquement les données professionnelles (Android et iOS)

N'utilisez pas cette fonction!

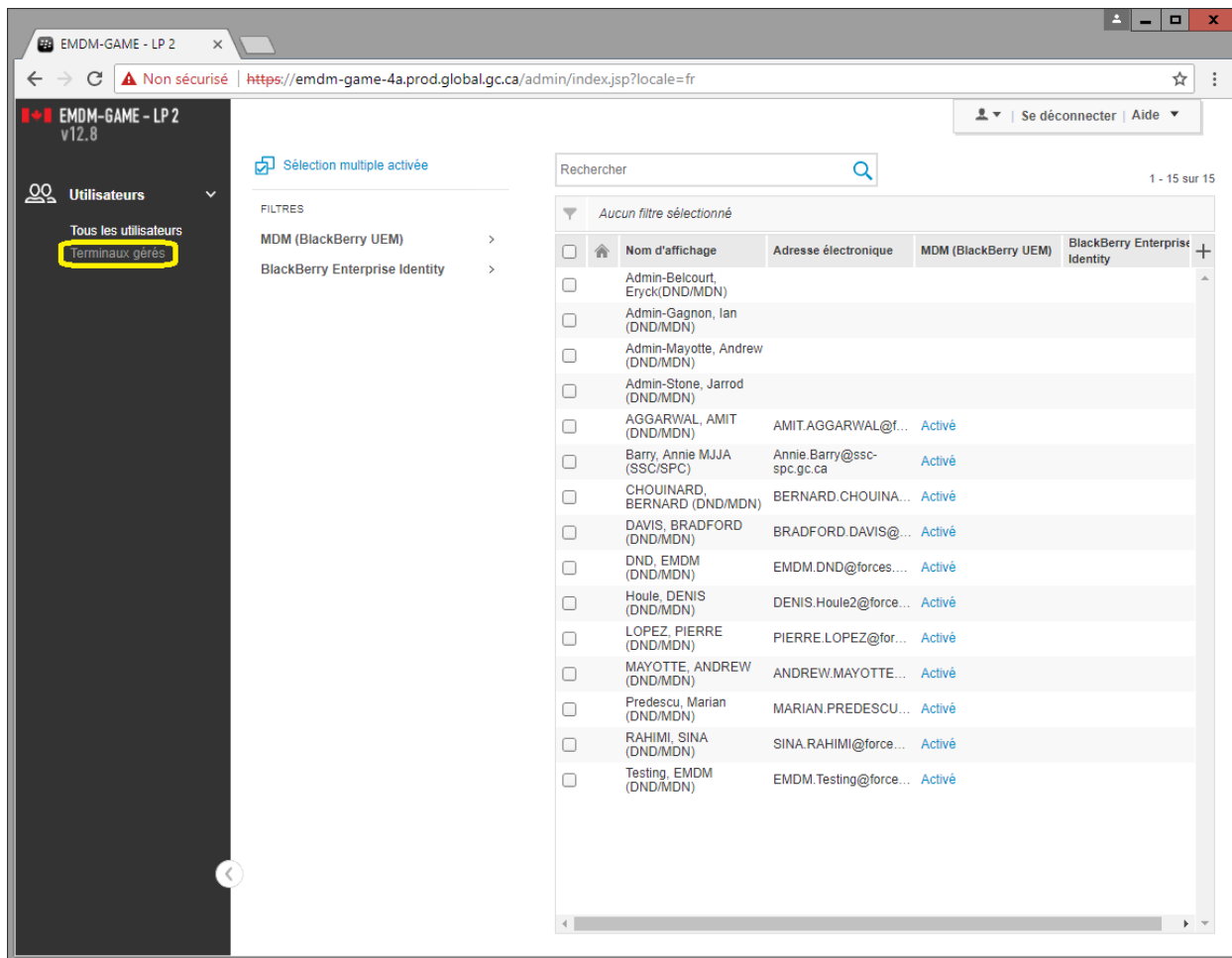
Les appareils Android sont enregistrés avec « Knox Mobile Enrollment (KME) » et les appareils iOS sont enregistrés avec « Apple Device Enrollment Program (DEP) ». Cette fonction brise la gestion de ces appareils et nécessite une réinitialisation complète de l'appareil afin de le réactiver. Donc, veuillez ne pas utiliser cette fonction.

5. Administration générale

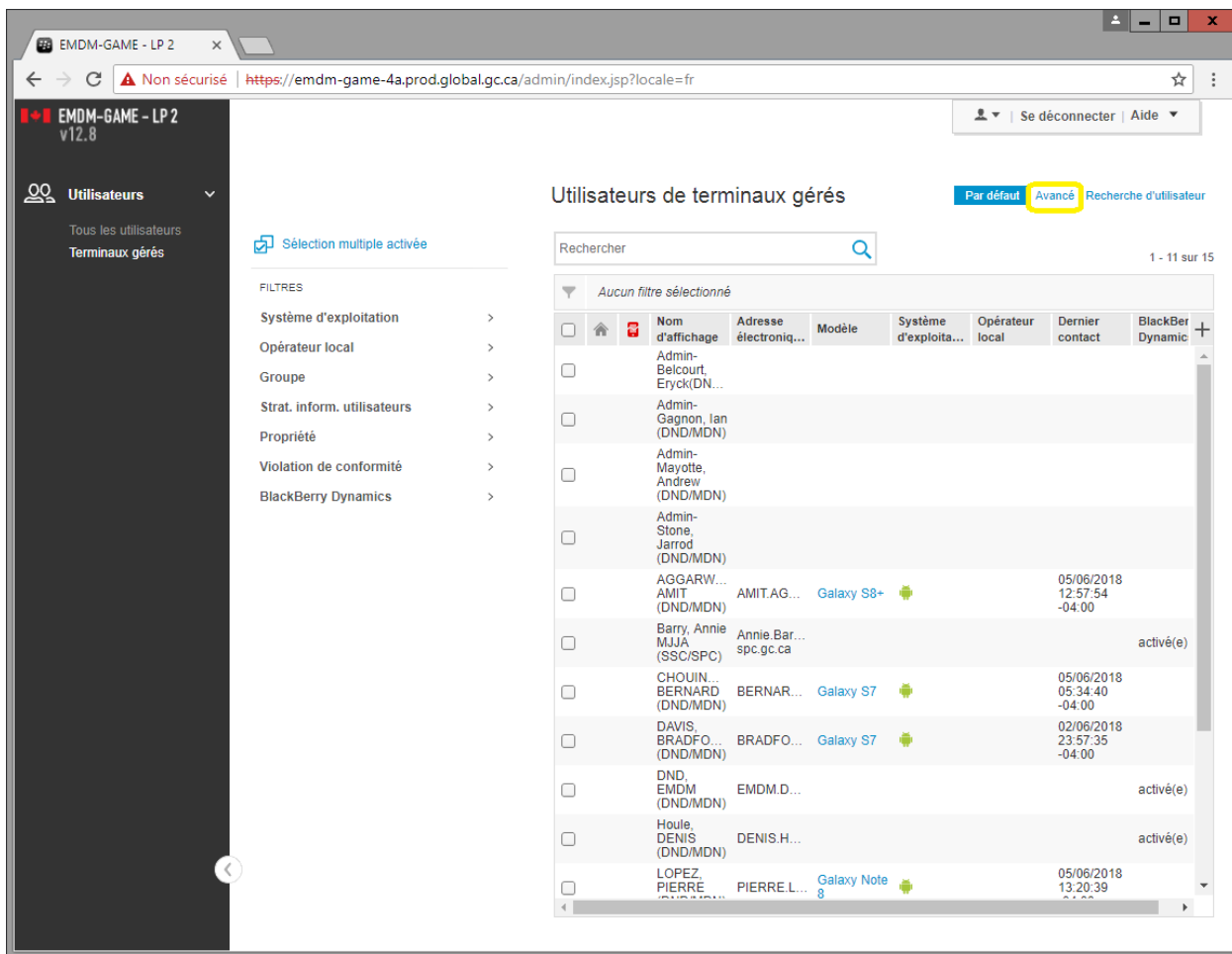
5.1 Exporter la liste des utilisateurs et appareils

Cette fonction permet de exporter la liste des utilisateurs et appareils gérés par le service de la GAME.

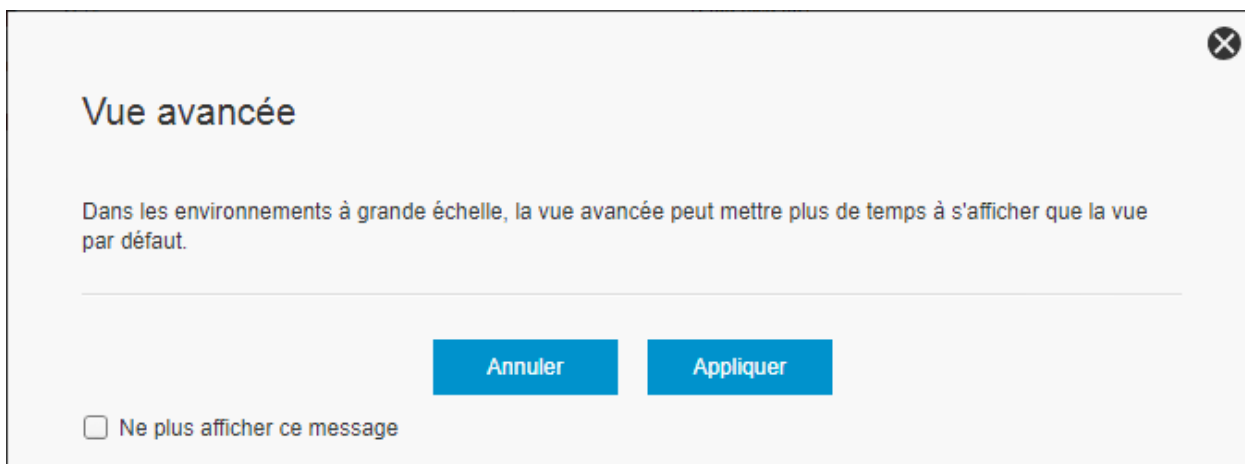
- 1) Dans la colonne de gauche, sous Utilisateurs, sélectionnez **Terminaux gérés**



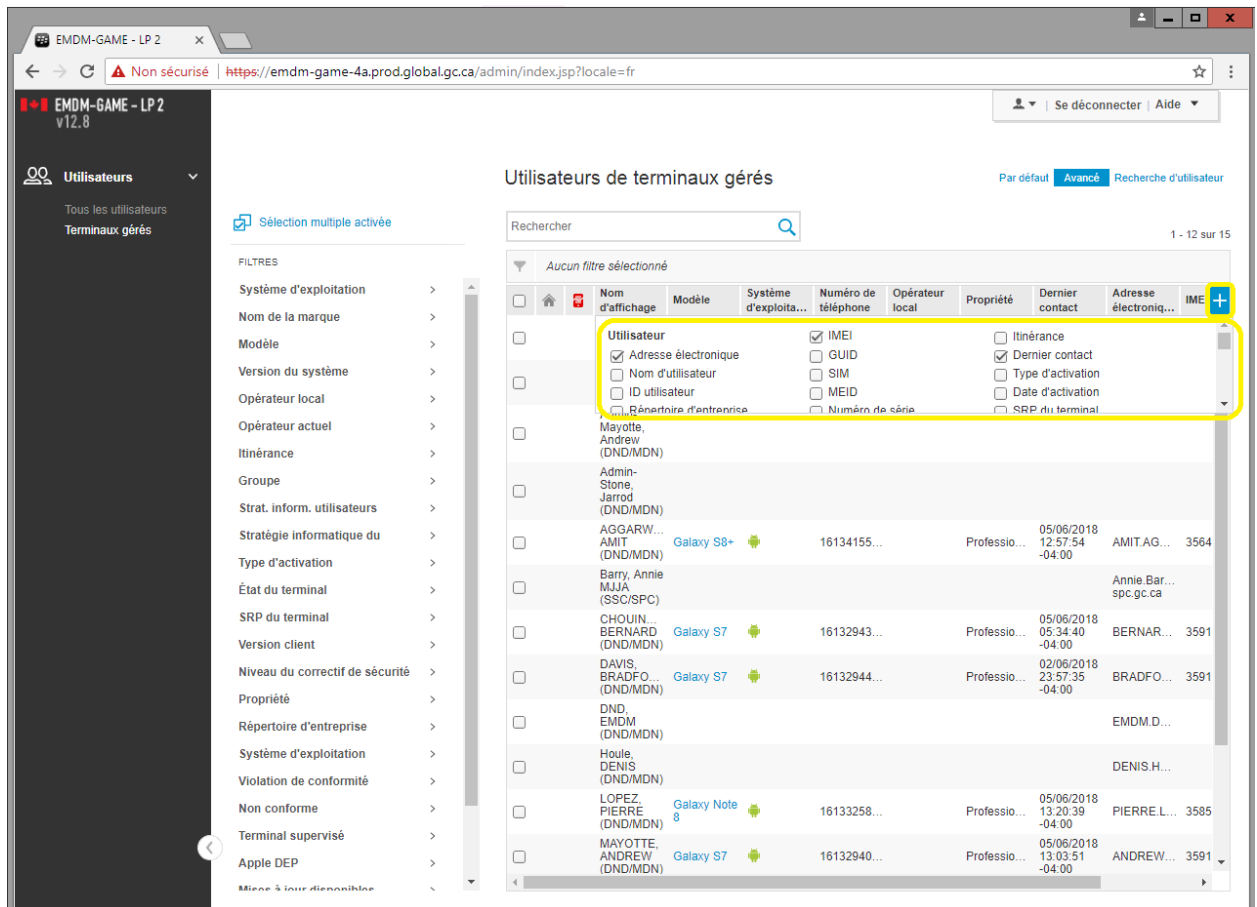
- 2) Dans le coin supérieur droit, sélectionnez **Avancé**



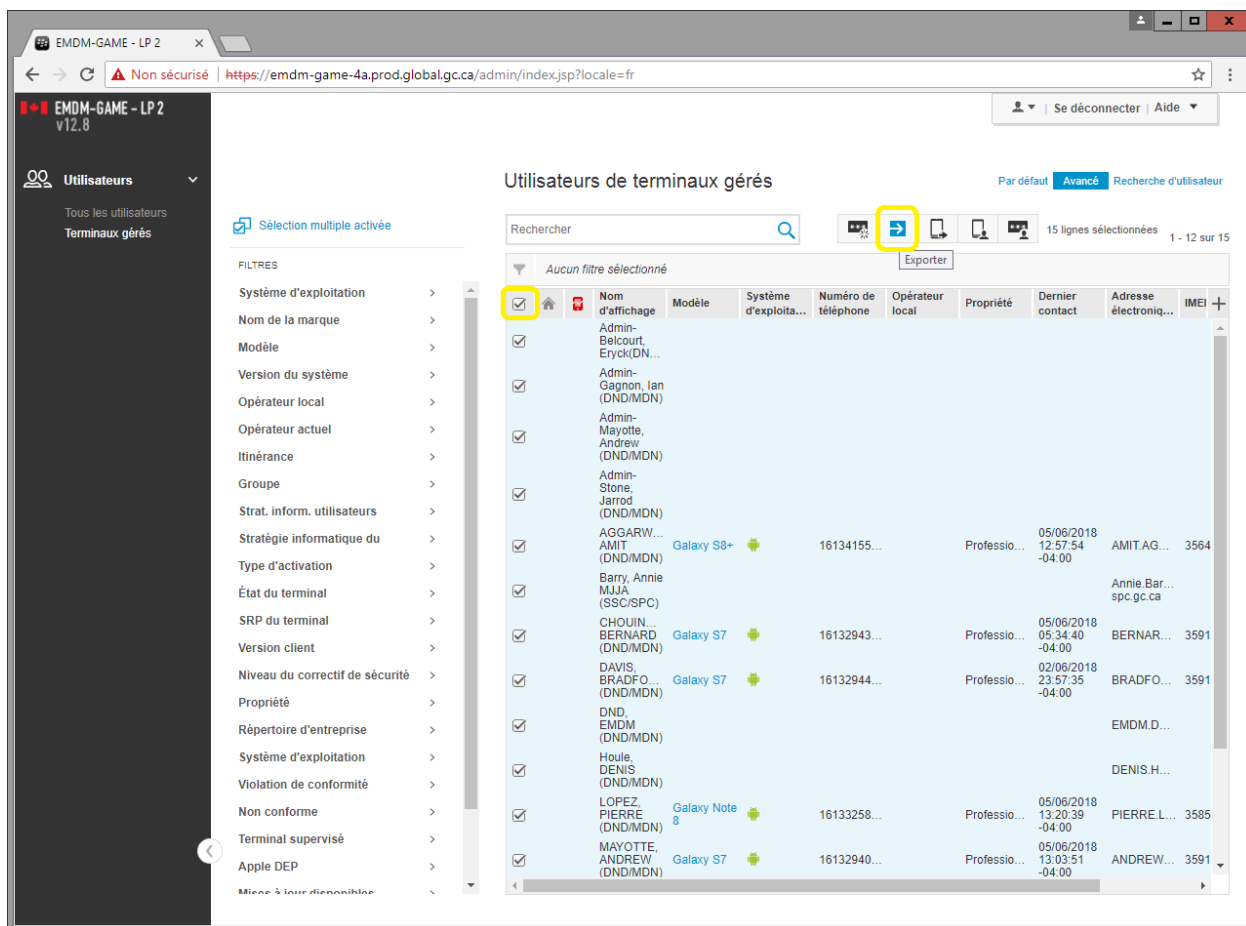
3) Dans la fenêtre Vue avancée, sélectionnez **Appliquer**



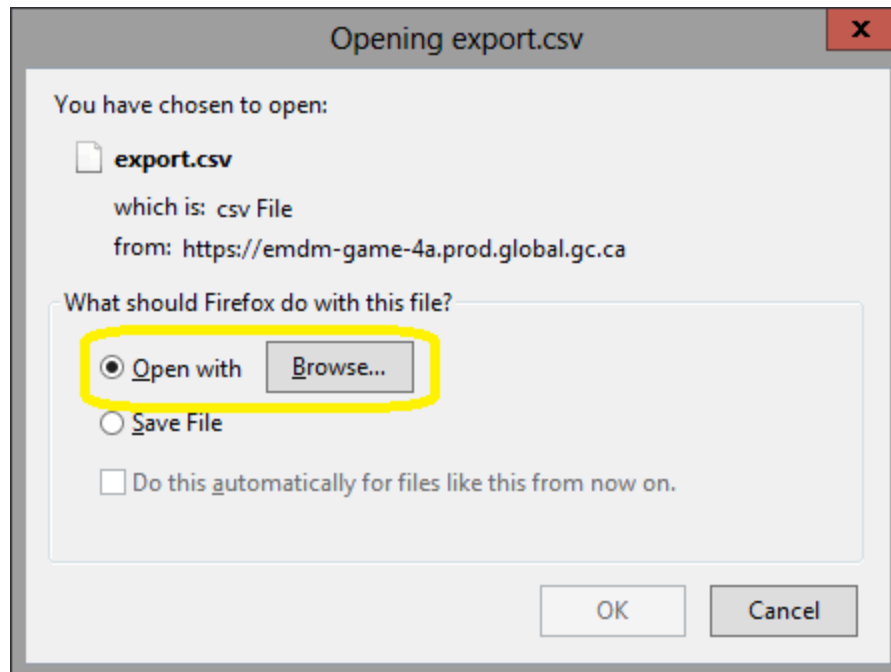
4) Dans le coin supérieur droit de la liste, sélectionnez le symbole (+) et sélectionnez les informations que vous voulez exporter (numéro IMEI, numéro de téléphone, adresse électronique, etc.)



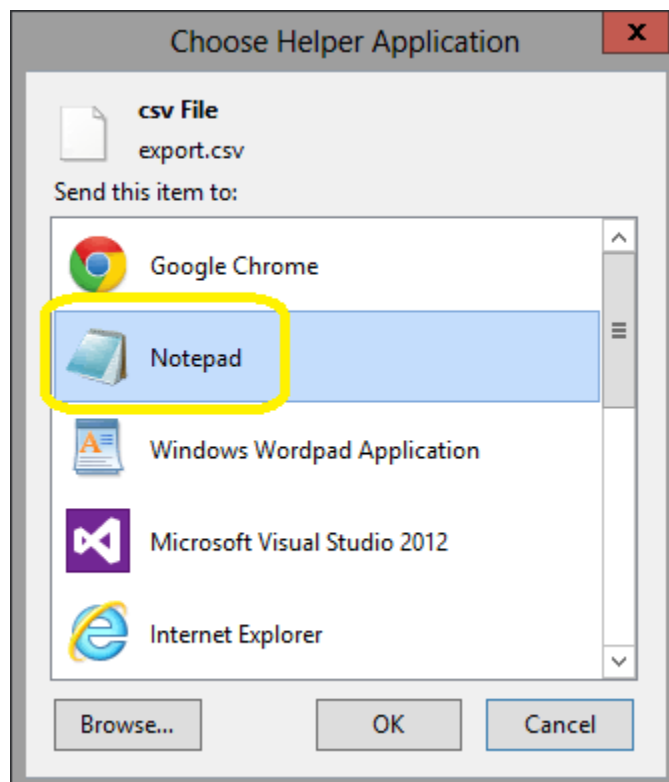
- 5) Dans le coin supérieur gauche de la liste, sélectionnez tous les utilisateurs. Ensuite, en haut de la liste, sélectionnez la fonction Exporter (bouton avec une flèche)



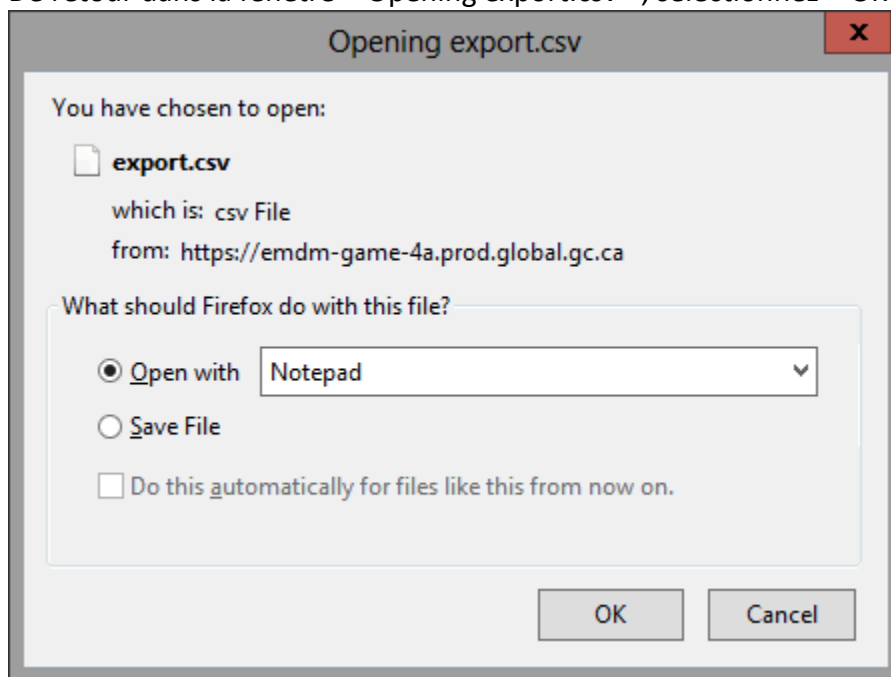
- 6) La liste des utilisateurs et appareils sera exportée dans un fichier .csv. Toutefois, ce fichier .csv est contenu dans l'environnement Citrix de SPC. Voici comment transférer les données sur votre ordinateur du RED :
 - a. Dans la fenêtre « Opening export.csv », sélectionnez « Open with... » et ensuite « Browse... »



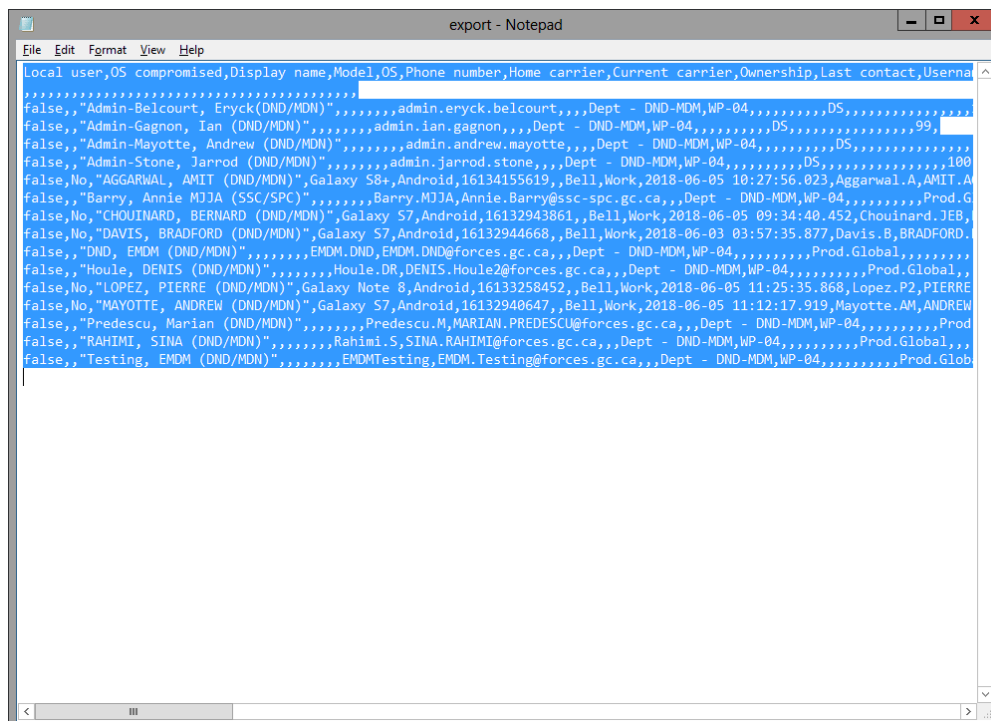
- b. Dans la fenêtre « Choose Helper Application », sélectionnez « Notepad » et ensuite sélectionnez « OK »



- c. De retour dans la fenêtre « Opening export.csv », sélectionnez « OK »



- d. La liste des utilisateurs et appareils s’affiche dans Notepad dans l’environnement Citrix de SPC. Sélectionnez et copiez toutes les données (Ctrl-A, ensuite Ctrl-C)



- e. Sur votre ordinateur du RED (DWAN), ouvrez le logiciel Notepad (menu Démarrer -> Recherche -> Notepad)
- f. Collez (Ctrl-V) les données dans le logiciel Notepad

- g. Sauvegardez les données dans un fichier .csv
- h. Vous pouvez ensuite importer ce fichier .csv dans Excel à l'aide de la fonction d'importation de données d'Excel. La fonction d'importation de données d'Excel assure que les données sont correctement importées dans Excel. N'ouvrez pas le fichier CSV directement dans Excel, car certaines des données (numéros IMEI par exemple) seront corrompues. Toujours utiliser la fonction d'importation de données Excel.

5.2 Modifier les informations du compte d'un utilisateur

Le service de la GAME est synchronisé avec Active Directory du RED (DWAN). De ce fait, si un utilisateur requiert une modification du nom d'utilisateur et / ou de l'adresse électronique, la modification doit d'abord avoir lieu dans Active Directory du RED. Le délai de synchronisation est de 24 à 48 heures.