



National Défense
Defence nationale

Assistant Deputy Minister (Information Management)



Enterprise Mobile Device Management (EMDM) Administration Console

Version: 2.1
Date: 14 February, 2019
Created by: DIMCD

Revision History

Date	Version	Amendment	Author
13 May 2018	0.a	First draft	Andrew Mayotte
17 May 2018	0.b	Edits and screenshots	Andrew Mayotte
25 May 2018	0.c	Additional edits and screenshots	Andrew Mayotte
30 May 2018	1.0	First release	Andrew Mayotte
4 June 2018	1.1	Minor edits and formatting	Andrew Mayotte
5 June 2018	1.2	Clarified password resets, expanded user extract instructions, added disable/enable work space instructions	Andrew Mayotte
7 June 2018	1.3	Clarified account modification, changed SSC browser recommendation, formatted certain screenshots, tested device wipe	Andrew Mayotte
9 February 2019	2.0	Added iOS EMDM Admin console instructions	Andrew Mayotte
14 February 2019	2.1	Clarified Knox work space only deletion section, removed Entrust token Annexes, instead linking to SSC's documents	Andrew Mayotte

Table of Contents

1. Introduction.....	4
2. Prerequisites to access the EMDM Administration Console.....	4
2.1 Administrator account	4
2.2 Entrust IdentityGuard Token.....	4
2.3 Citrix Client installation	5
3. Accessing the EMDM Administration Console	8
3.1 Connect to the SSC portal	8
3.2 Connect to the EMDM Administration Console.....	9
4. Managing mobile devices	17
4.1 Quick user search (Android & iOS).....	17
4.2 Reset device unlock password (Android & iOS)	18
4.3 Reset Knox work space password (Android only).....	22
4.4 Remote device wipe (Android & iOS).....	24
4.5 Disable/Re-enable Knox work space (Android only)	28
4.6 Set device re-activation password (Android & iOS).....	31
4.7 Remote restart device (iOS only)	34
4.8 View device information (Android & iOS).....	37
4.9 View device actions (Android & iOS)	40
4.10 Update device information (Android & iOS).....	43
4.11 Delete work space only data (Android & iOS)	45
5. General administration.....	46
5.1 Extract EMDM user list	46
5.2 Modify a user's EMDM account information.....	53

1. Introduction

Intended Audience

This document is intended to be used by the following personnel:

- Service Management Centres (SMC)
- Defence Service Operations Centre (DEFSOC)
- EMDM Partner Administrators

EMDM Service Description

Shared Services Canada's (SSC) EMDM service provides a controlled and secure management of Android and iOS mobile devices for the Government of Canada.

In addition, Android devices are registered with "Knox Mobile Enrollment" and iOS devices are registered with "Apple Device Enrollment Program" to streamline the activation of devices and ensure devices cannot be used outside the EMDM service.

The EMDM services utilises the BlackBerry Unified Endpoint Management (UEM) v12.9 platform.

2. Prerequisites to access the EMDM Administration Console

2.1 Administrator account

EMDM partner administrators will receive the following information from SSC:

- Username and password
- Entrust Self-Service One-Time Password (OTP) to configure their security token (see section 2.2 below)

2.2 Entrust IdentityGuard Token

A token, also called "hard token" or "soft token", is required in order to access the EMDM Administration Console. The token is obtained either by using the Entrust IdentityGuard application installed on an Android or iOS smartphone or by using an Entrust hard token device. Follow the steps in one the documents below to complete this requirement:

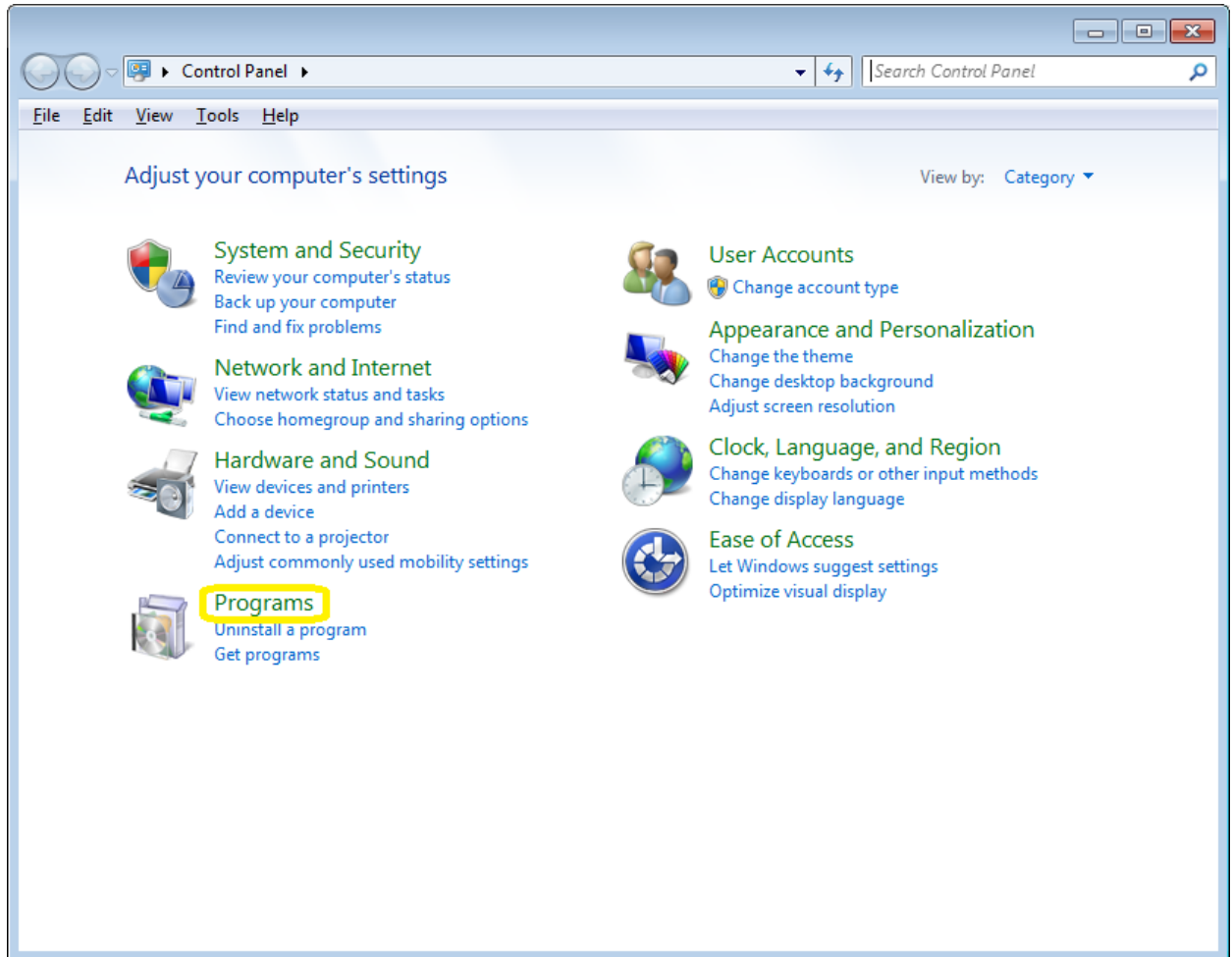
- [Entrust IdentityGuard Self-Service User Guide for Android Soft Token - SSC \(EDC\)](#)
- [Entrust IdentityGuard Self-Service User Guide for iOS Soft Token - SSC \(EDC\)](#)
- [Entrust IdentityGuard Self-Service User Guide for Hard Token - SSC \(EDC\)](#)

Note: The above documents from SSC are hosted on GCPedia. In order to access those documents, you must be on the DWAN. In addition, it's possible that you may have to copy/paste the hyperlink into a web browser in order to access the documents.

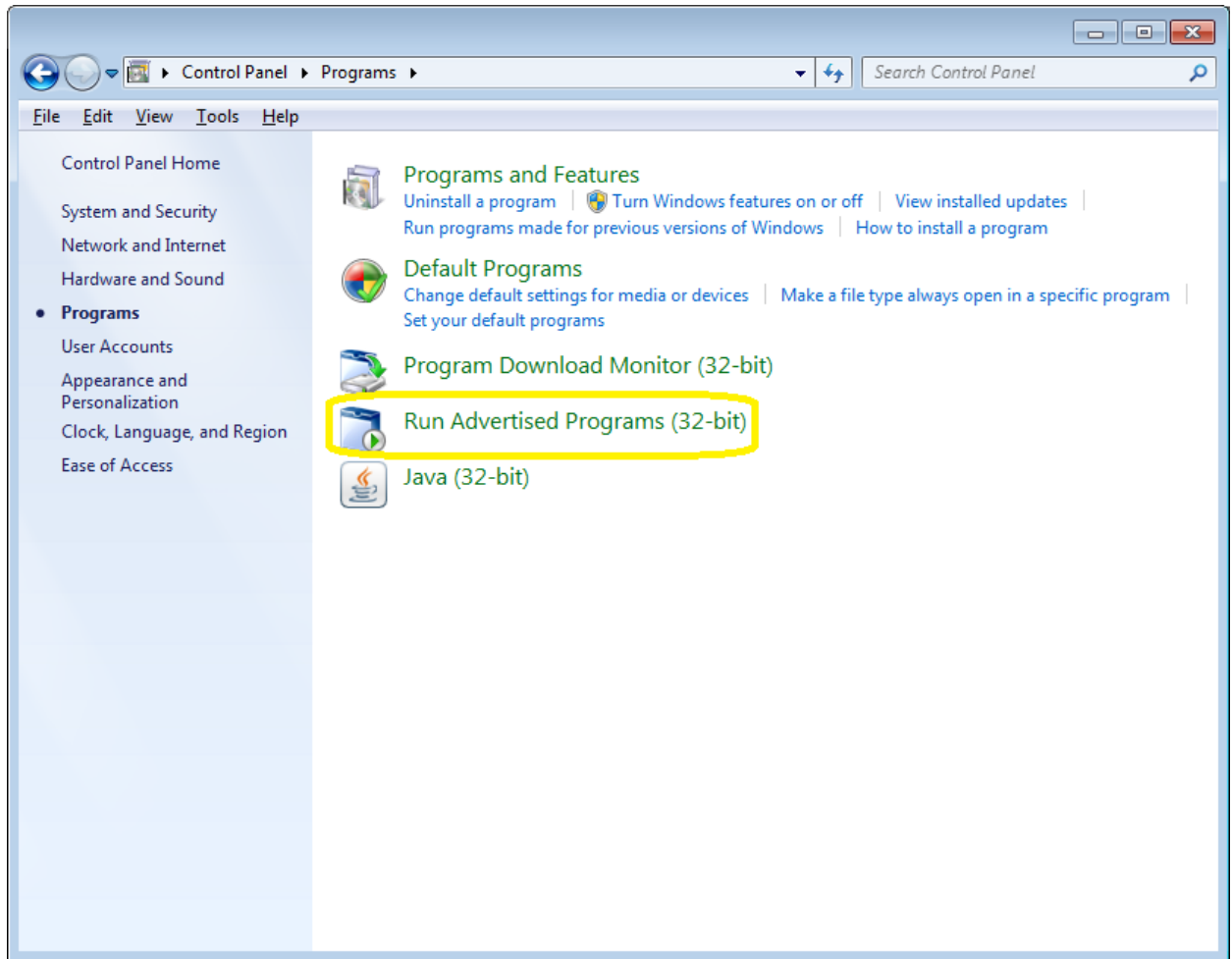
2.3 Citrix Client installation

The EMDM Administration Console is a web application that runs in a Citrix container hosted on a SSC server. The Citrix client must be installed prior to accessing the EMDM Administration Console. Follow the steps below to install the Citrix Client on a DWAN PC:

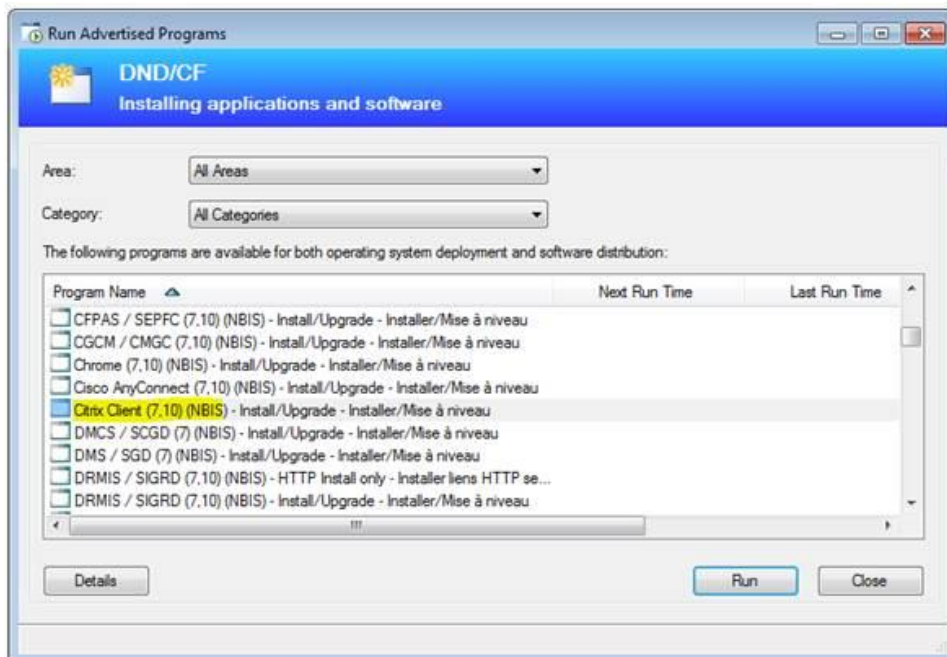
1. Go to the **Control Panel** (Start button -> Control Panel) and select **Programs**.



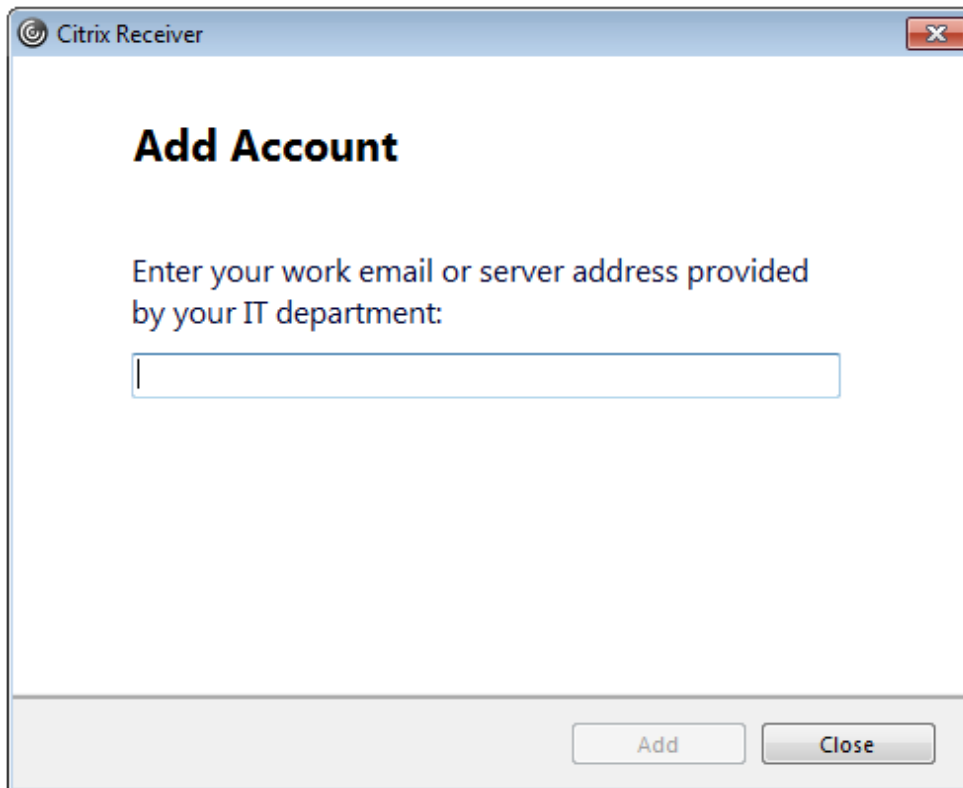
2. Click **Run Advertised Programs (32-bit)**



3. Navigate to **Citrix Client (7, 10) (NBIS) Install/Upgrade** and click the **Run** button.



- 4. Once the Citrix Client installation has completed, the Citrix Receiver Add Account screen may appear. If it does, click the Close button.



3. Accessing the EMDM Administration Console

3.1 Connect to the SSC portal

1. In a web browser, go to <https://appadmin-dev1.ssc-spc.gc.ca/vpn/index.html> and enter your administrator username (admin.firstname.lastname) and password and click Log On.



CDOQ - EDC/CDE

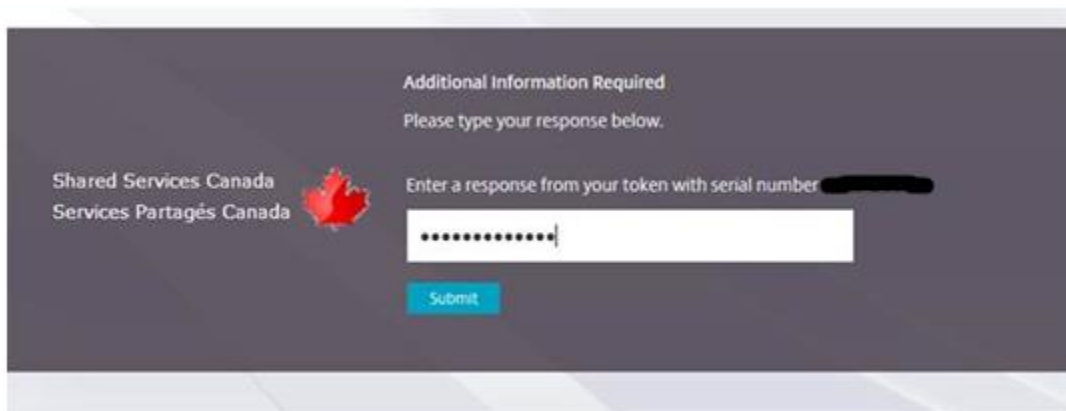
Shared Services Canada
Services Partagés Canada

User name: admin.bradford.davis

Password:

Log On

2. At the next screen, enter the hard or soft token value from Entrust IdentityGuard, and click Submit:



Additional Information Required

Please type your response below.

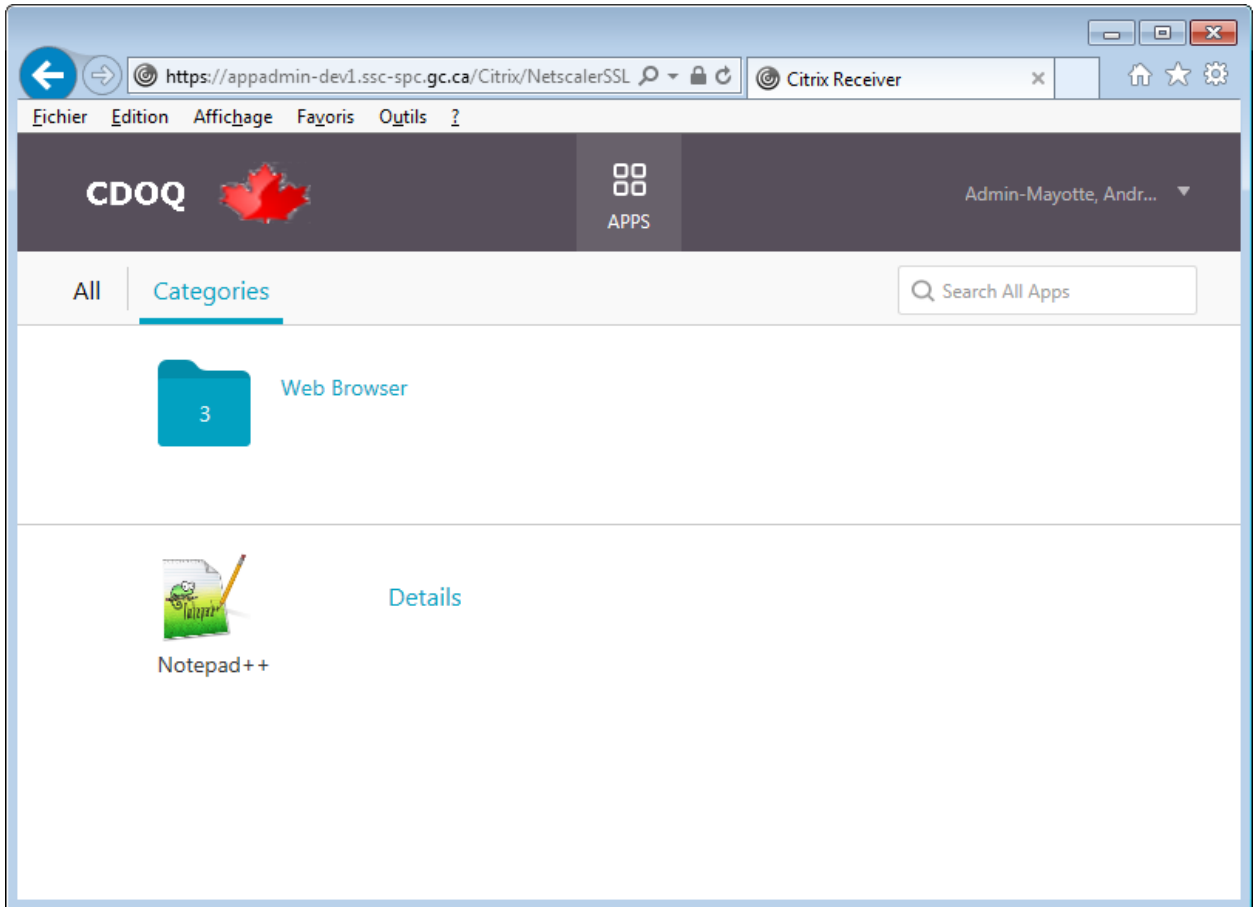
Shared Services Canada
Services Partagés Canada

Enter a response from your token with serial number [REDACTED]

.....

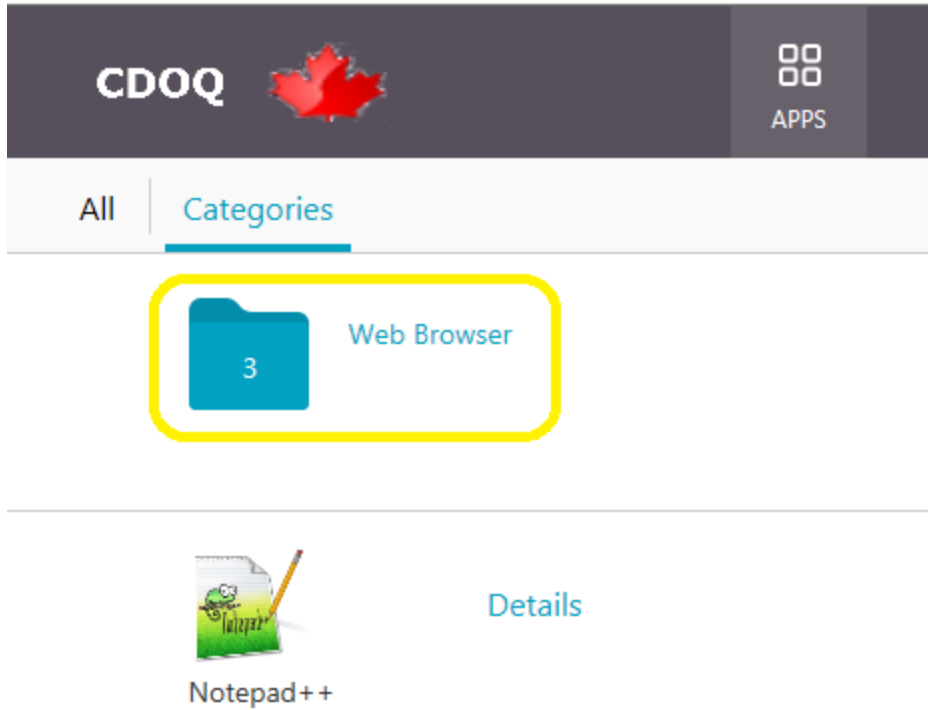
Submit

3. You should be presented with the following page

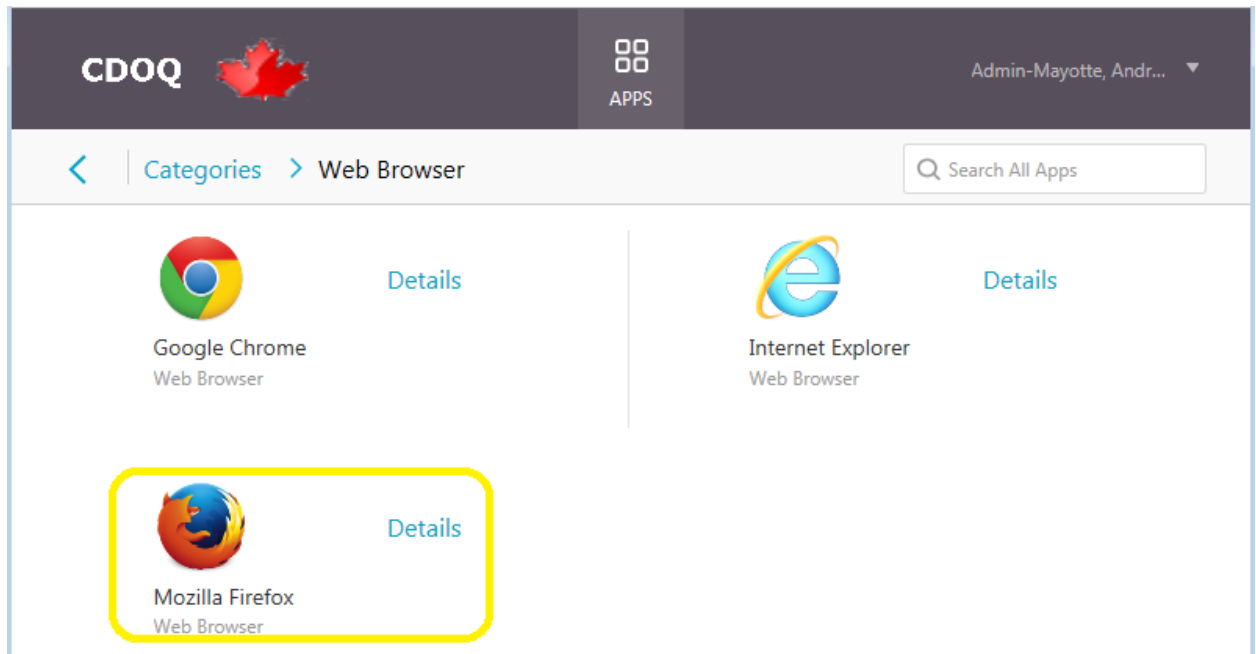


3.2 Connect to the EMDM Administration Console

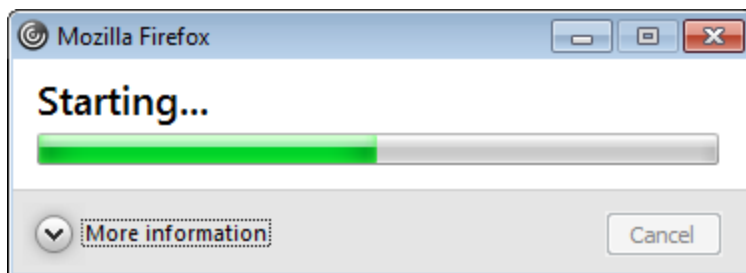
- 1) Click the Web Browser icon



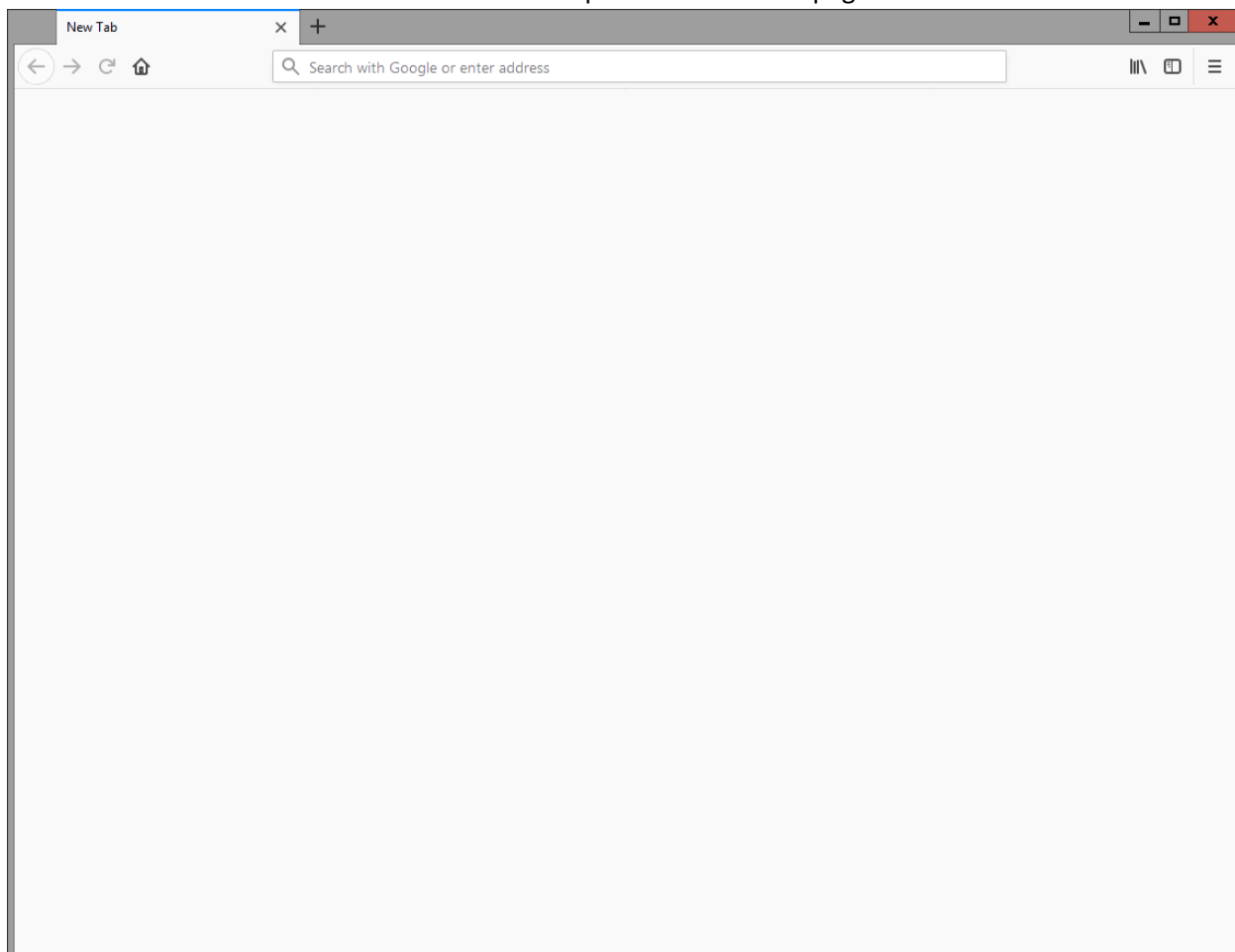
- 2) Click the Firefox browser icon to launch Firefox through Citrix. *Note: Do not use Internet Explorer or Google Chrome as those browsers have technical issues with the EMDM administration console.*



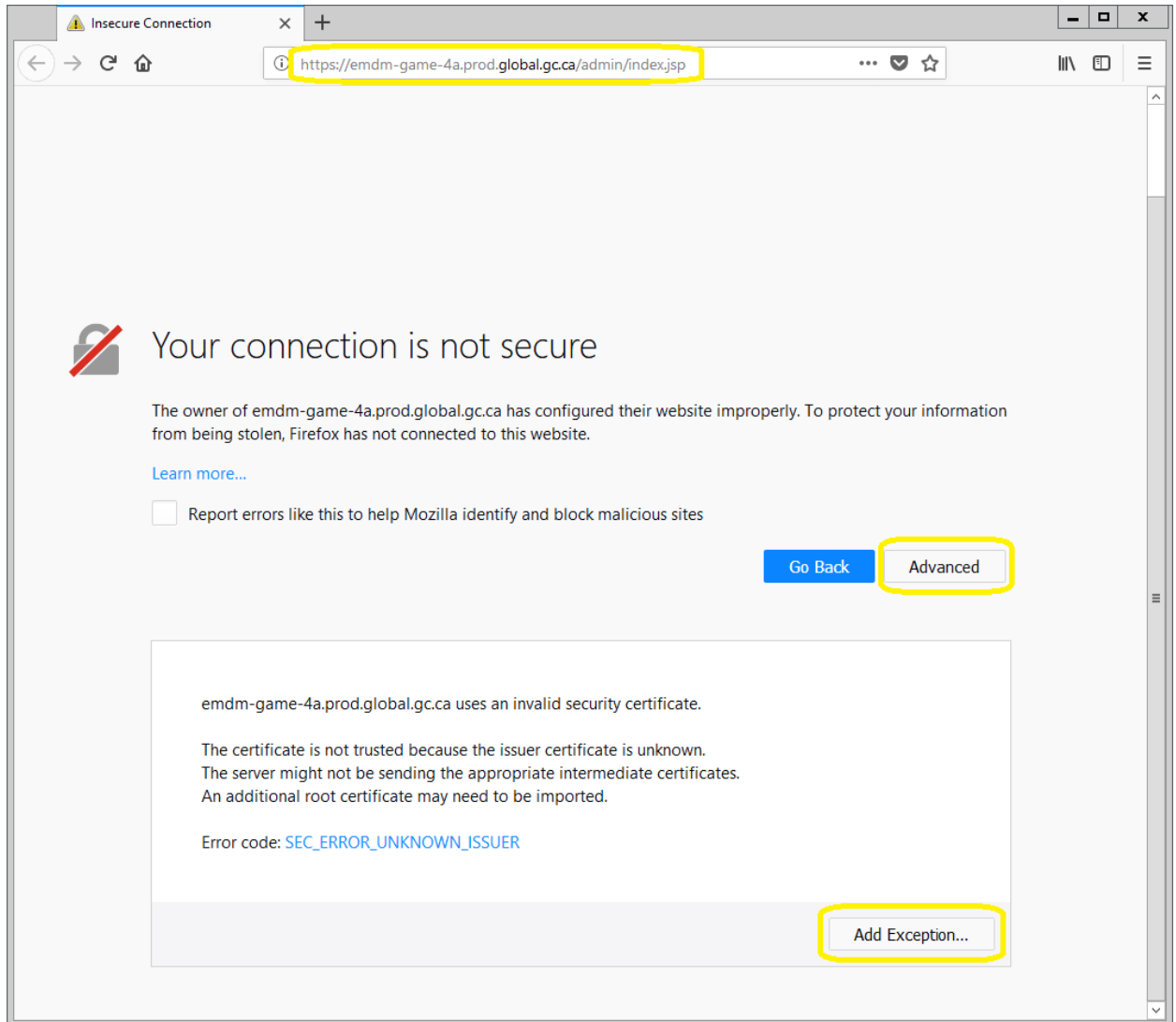
- 3) Firefox will launch within the Citrix environment



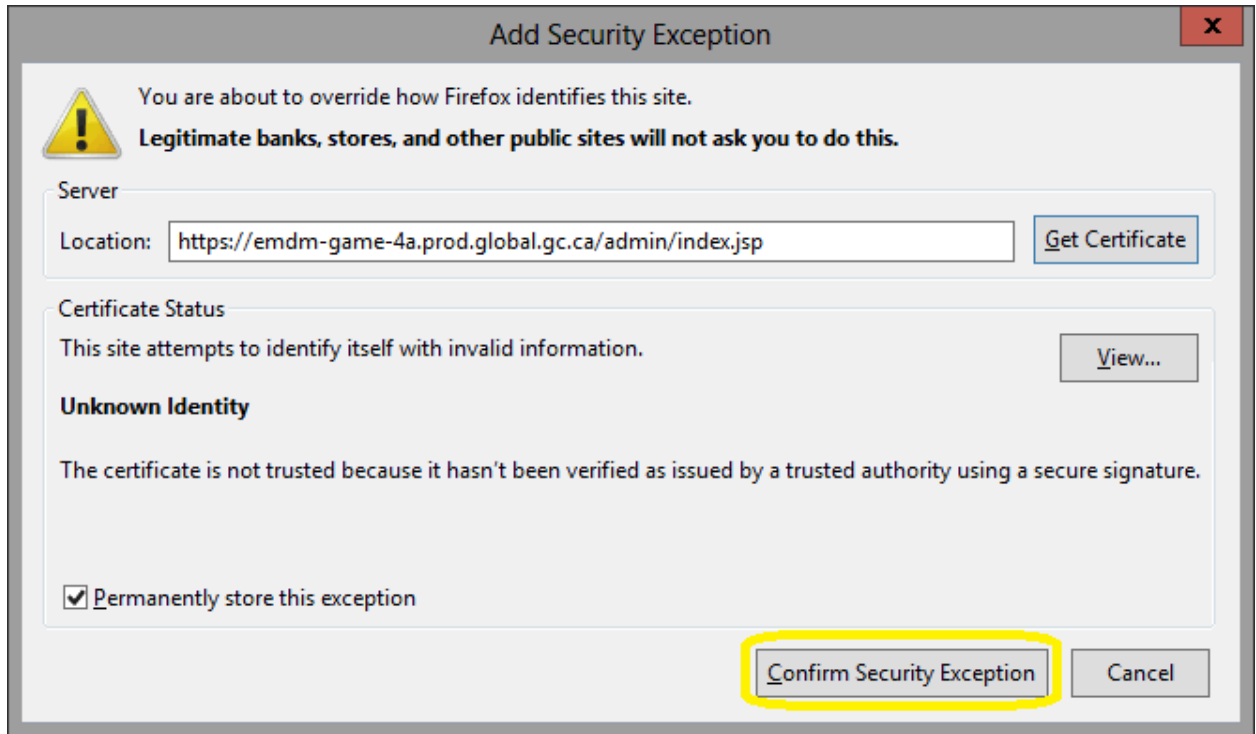
- 4) If asked “How do you want to open this HTTP link”, choose Firefox from the list.
- 5) You should now be in Firefox within the SSC EDC portal with a blank page:



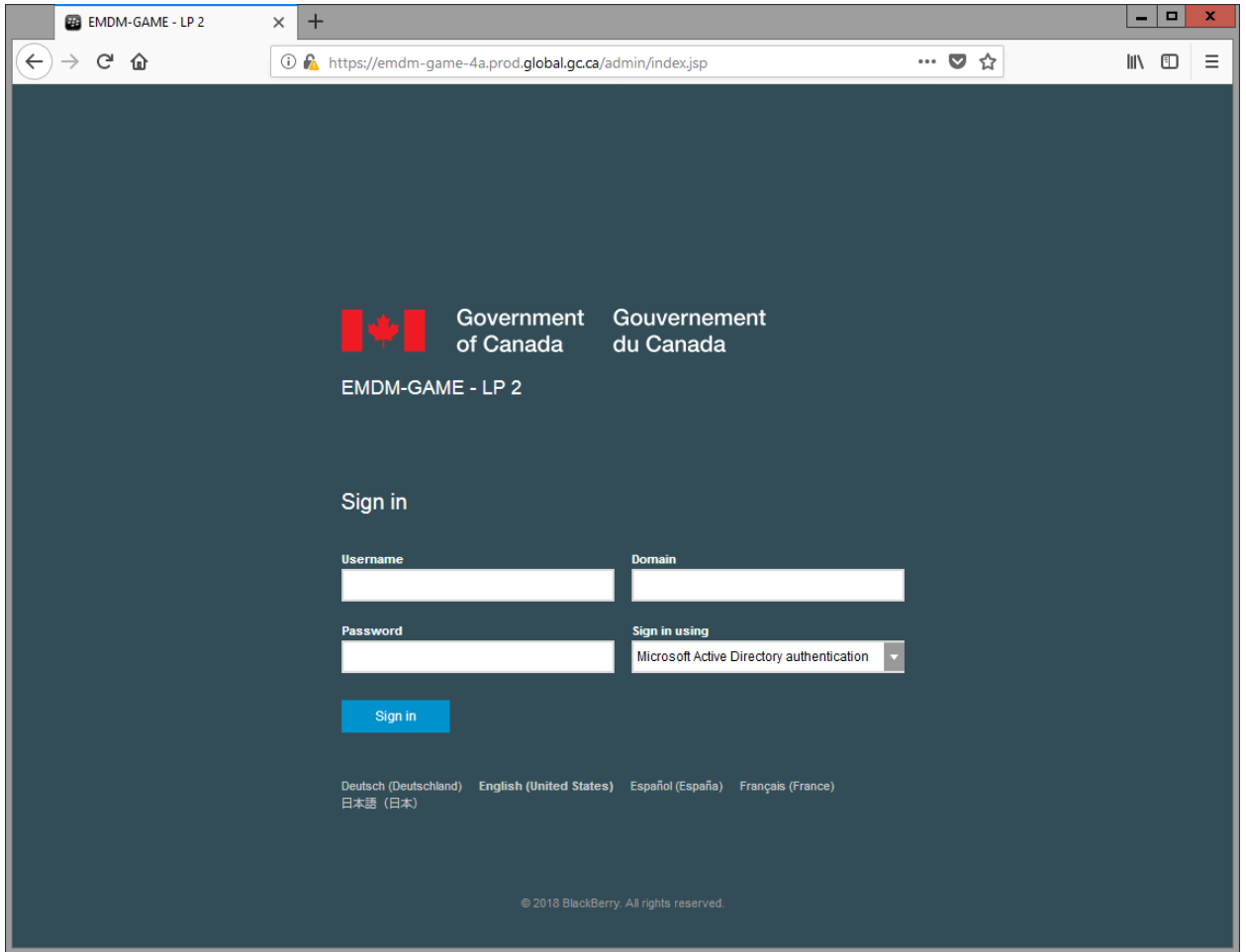
- 6) In the Firefox address bar copy and paste the following address <https://emdm-game-4a.prod.global.gc.ca/admin/index.jsp> which is the EMDM Administration Console link for DND/CAF.
- 7) You will likely get a connection is not secure warning page on the next screen, if so click the “Advanced” button, and then click the “Add Exception...” button



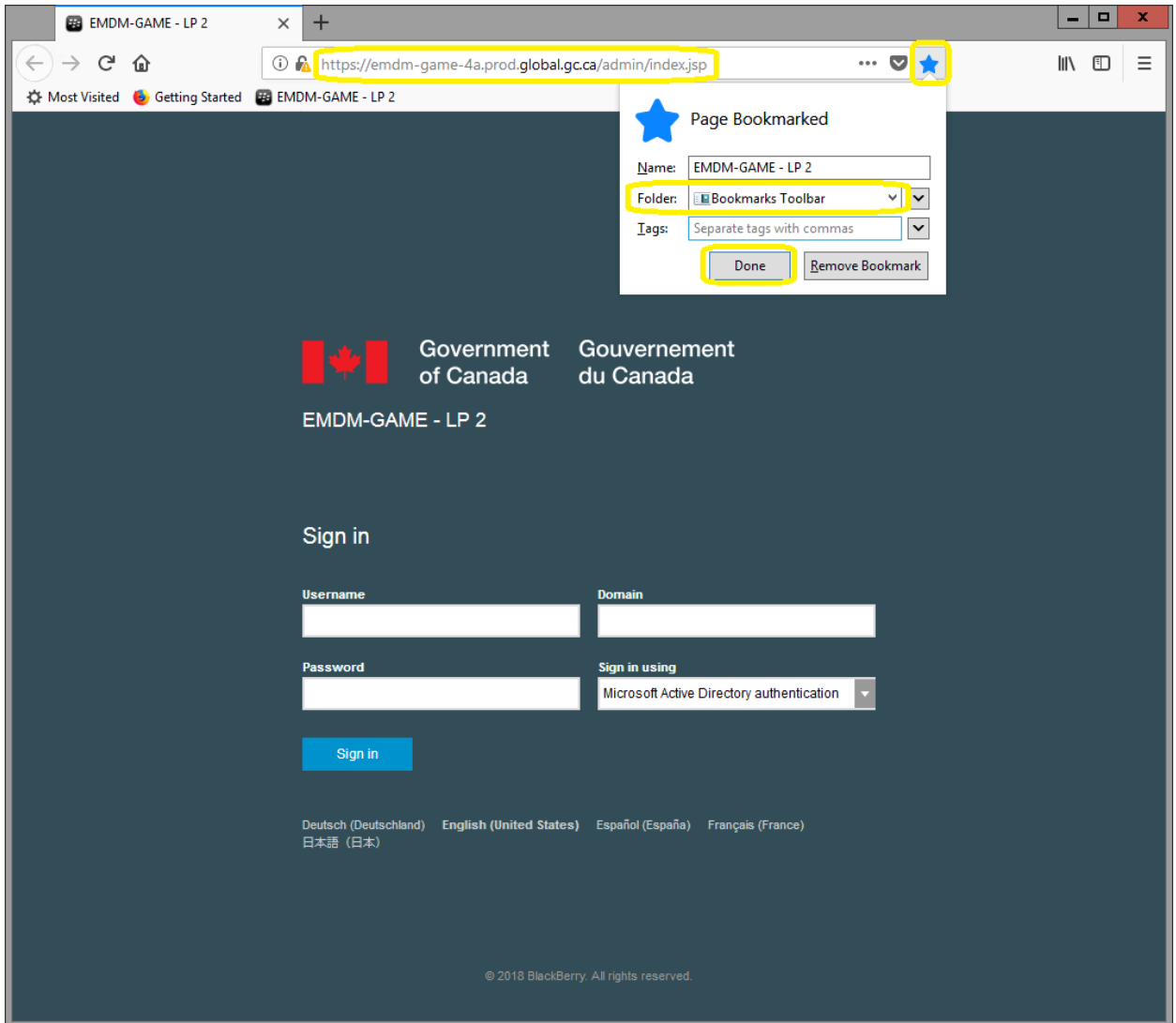
8) Click the “Confirm Security Exception” button



- 9) This will take you to the EMDM Administration Console sign in page.



10) Add the EMDM Administration Console as a Bookmark in Firefox for quicker access in the future



- 11) Enter your Admin username (admin.firstname.lastname) and password. Next click Sign In. *Note: Do not touch the Domain or Sign in using fields.*



Government of Canada / Gouvernement du Canada

EMDM-GAME - LP 2

Sign in

Username: admin.andrew.mayotte

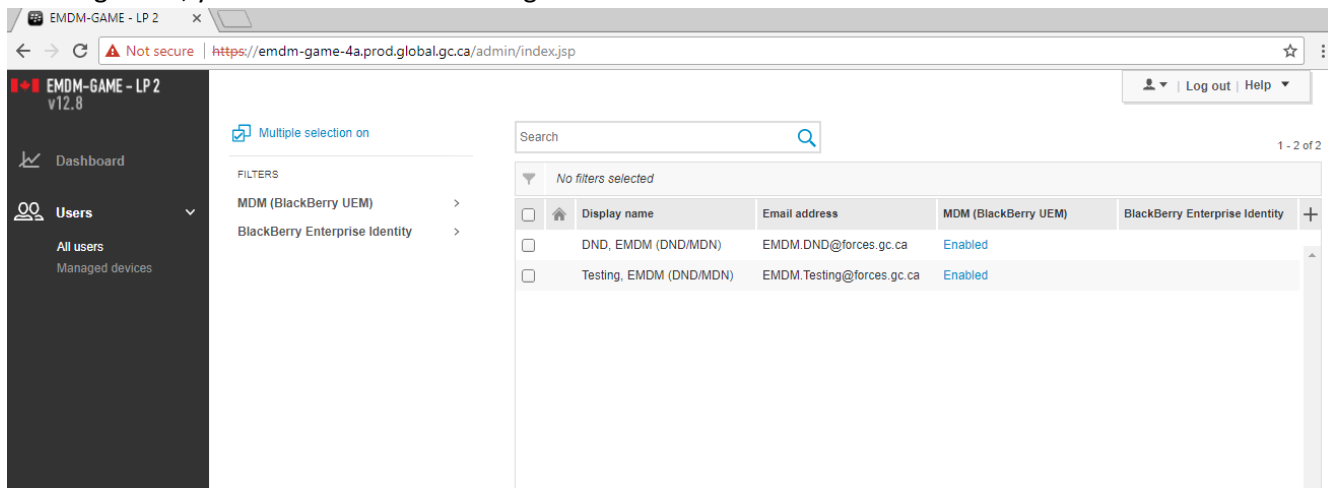
Domain: DS

Password: [masked]

Sign in using: Microsoft Active Directory authentication

Sign in

12) Once signed in, you should see the following:



EMDM-GAME - LP 2 v12.8

Dashboard

Users

- All users
- Managed devices

Multiple selection on

FILTERS

- MDM (BlackBerry UEM)
- BlackBerry Enterprise Identity

Search

No filters selected

	Display name	Email address	MDM (BlackBerry UEM)	BlackBerry Enterprise Identity
<input type="checkbox"/>	DND, EMDM (DND/MDN)	EMDM.DND@forces.gc.ca	Enabled	
<input type="checkbox"/>	Testing, EMDM (DND/MDN)	EMDM.Testing@forces.gc.ca	Enabled	

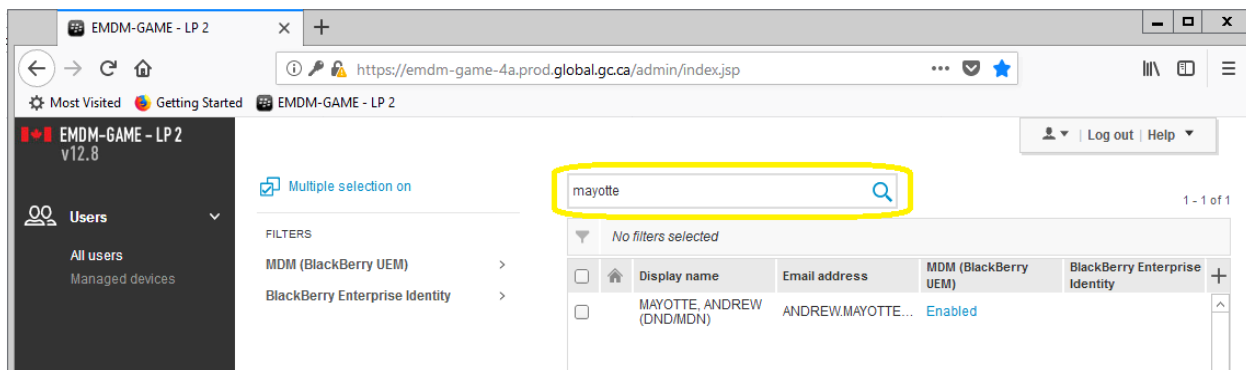
1 - 2 of 2

4. Managing mobile devices

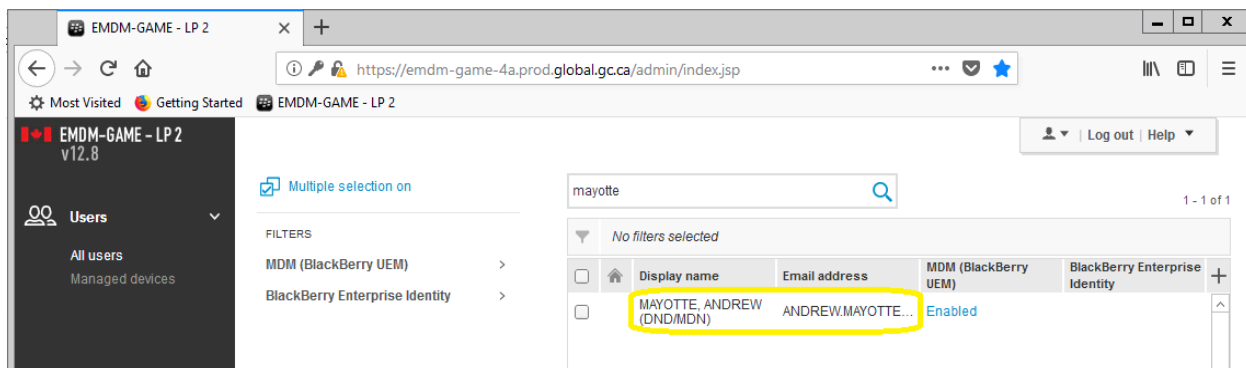
4.1 Quick user search (Android & iOS)

Before you can manage a user’s device, you first need to find the user and open their EMDM user account.

1. To search for an EMDM user, type a user’s name into the Quick Search field located near the top of the EMDM Administration Console



2. Click on the user to open their EMDM user account



3. You should now be viewing the user’s EMDM user account information

EMDM-GAME - LP 2

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

EMDM-GAME - LP 2 v12.8

Users

All users
Managed devices

< MAYOTTE, ANDREW (DND/MDN) >

All users Dept - DND-MDM Global - Certificates (Indirect) Global - Distribution (Indirect)

MANAGED DEVICES ENTERPRISE IDENTITY

Summary Samsung Galaxy S7

Activation details

Activated devices
Samsung Galaxy S7
1 of 10 devices activated

Device activation password
Expires on July 4, 2018, 09:27 AM (-04:00)
Default activation email
[View activation email](#)
[Expire](#)

[Set activation password](#)

BlackBerry 2FA
To enable this feature, assign a BlackBerry 2FA profile.

IT policy and profiles

Assigned profile	Assignment	Status
WP-04 IT policy	Group	
DND Email	Group	
Work and Personal Activation	Group	
MDM Connectivity Enterprise connectivity	Group	
Default Compliance	Default	
Default BlackBerry Dynamics	Default	
Default BlackBerry Dynamics connectivity	Default	
Default Enterprise Management Agent	Default	

4.2 Reset device unlock password (Android & iOS)

The device must have network connectivity for this command to be successful.

Note for Android devices: Android devices have 2 different passwords, one to unlock the device itself and one to access the Knox workspace. The user can choose to use the same password for both. If they do, they will likely require a [Knox work space password reset](#) in addition to a device unlock password reset.

Note for iOS devices: iOS devices use one password to both unlock the device and access the work apps.

- 1) Search for the user and open their EMDM user account
- 2) Under the user's profile, select the user's mobile device (e.g. Samsung Galaxy S7 or Apple iPhone 8)

EMDM-GAME - LP 2 v12.8

Users

- All users
- Managed devices

< MAYOTTE, ANDREW (DND/MDN) >

All users Dept - DND-MDM Global - Certificates (Indirect) Global - Distribution (Indirect)

MANAGED DEVICES ENTERPRISE IDENTITY

Summary Samsung Galaxy S7

Activation details

Activated devices
Samsung Galaxy S7
1 of 10 devices activated

Device activation password
Expired on May 23, 2018, 07:03 PM (-04:00)

Set activation password

BlackBerry 2FA
To enable this feature, assign a BlackBerry 2FA profile.

IT policy and profiles

Assigned profile	Assignment	Status
WP-04 IT policy	Group	
DND Email	Group	
Work and Personal Activation	Group	
MDM Connectivity Enterprise connectivity	Group	
Default Compliance	Default	
Default BlackBerry Dynamics	Default	
Default BlackBerry Dynamics connectivity	Default	
Default Enterprise Management Agent	Default	
Entrust Root CA (L1K-G2-cf)	Group	

3) Under Manage Device, select **Unlock device and clear password**

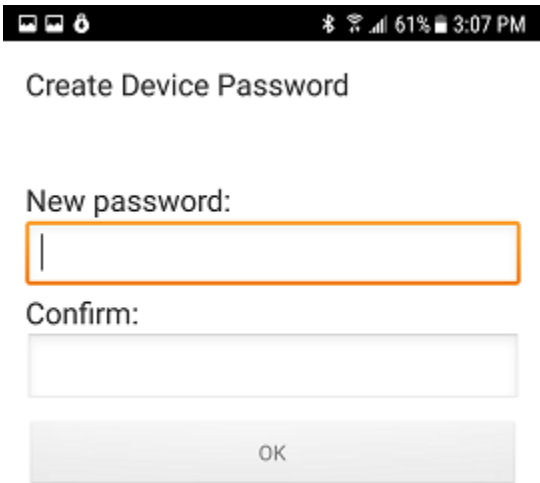
The screenshot shows the EMDM Administration Console interface. The browser address bar displays `https://emdm-game-4a.prod.global.gc.ca/admin/index.jsp`. The user is logged in as MAYOTTE, ANDREW (DND/MDN). The page shows a list of managed devices, with the selected device being a Samsung Galaxy S7. The 'Manage device' section contains several actions, with 'Unlock device and clear password' highlighted by a yellow box. Other actions include 'View device report', 'View device actions', 'Lock device', 'Specify device password and lock', 'Delete all device data', 'Reset work space password', 'Delete only work data', 'Disable work space', 'Enable work space', 'Update device information', and 'Remove device'. The 'Activated device' section provides details for the Samsung Galaxy S7, including IMEI, phone number, software version, and ownership information.

- 4) In the Unlock device and clear password window click on **Unlock and clear**

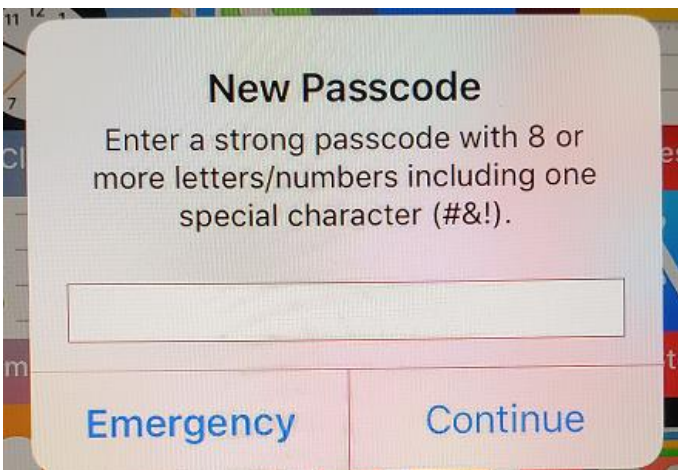
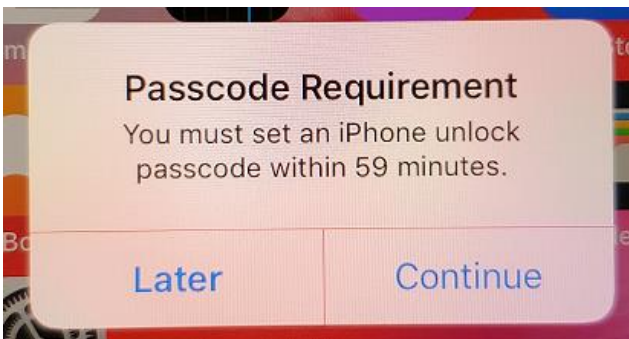
The dialog box titled 'Unlock device and clear password' for a Samsung Galaxy S7 is shown. It contains the question 'Do you want to unlock the device and clear the password?' and two buttons: 'Cancel' and 'Unlock and clear'.

- 5) Within a minute or two, the user's device will unlock and prompt them to create a new device unlock password

Android device screen:



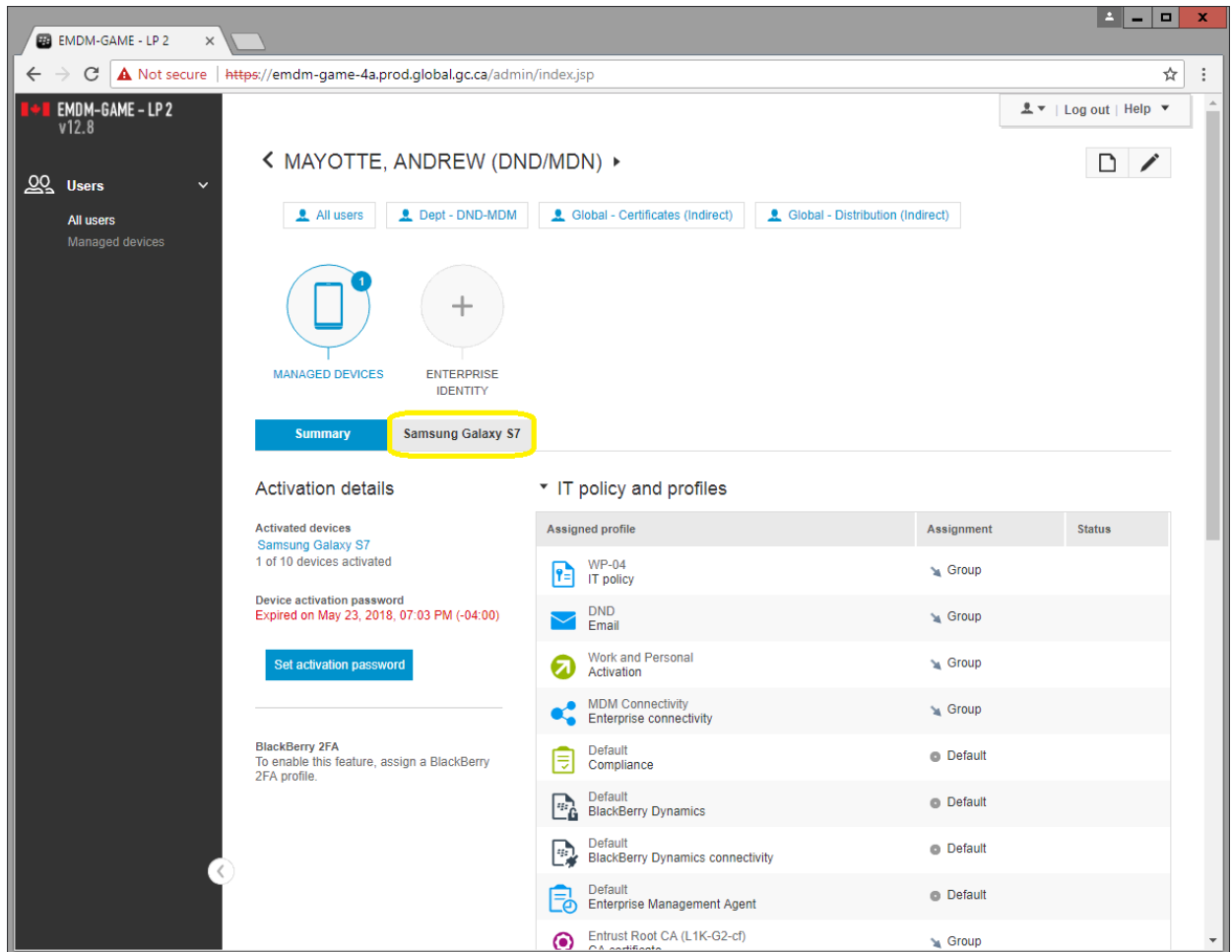
iOS device screen:



4.3 Reset Knox work space password (Android only)

This command resets the Android Knox work space password, prompting the user to create a new password. The device must have network connectivity for this command to be successful.

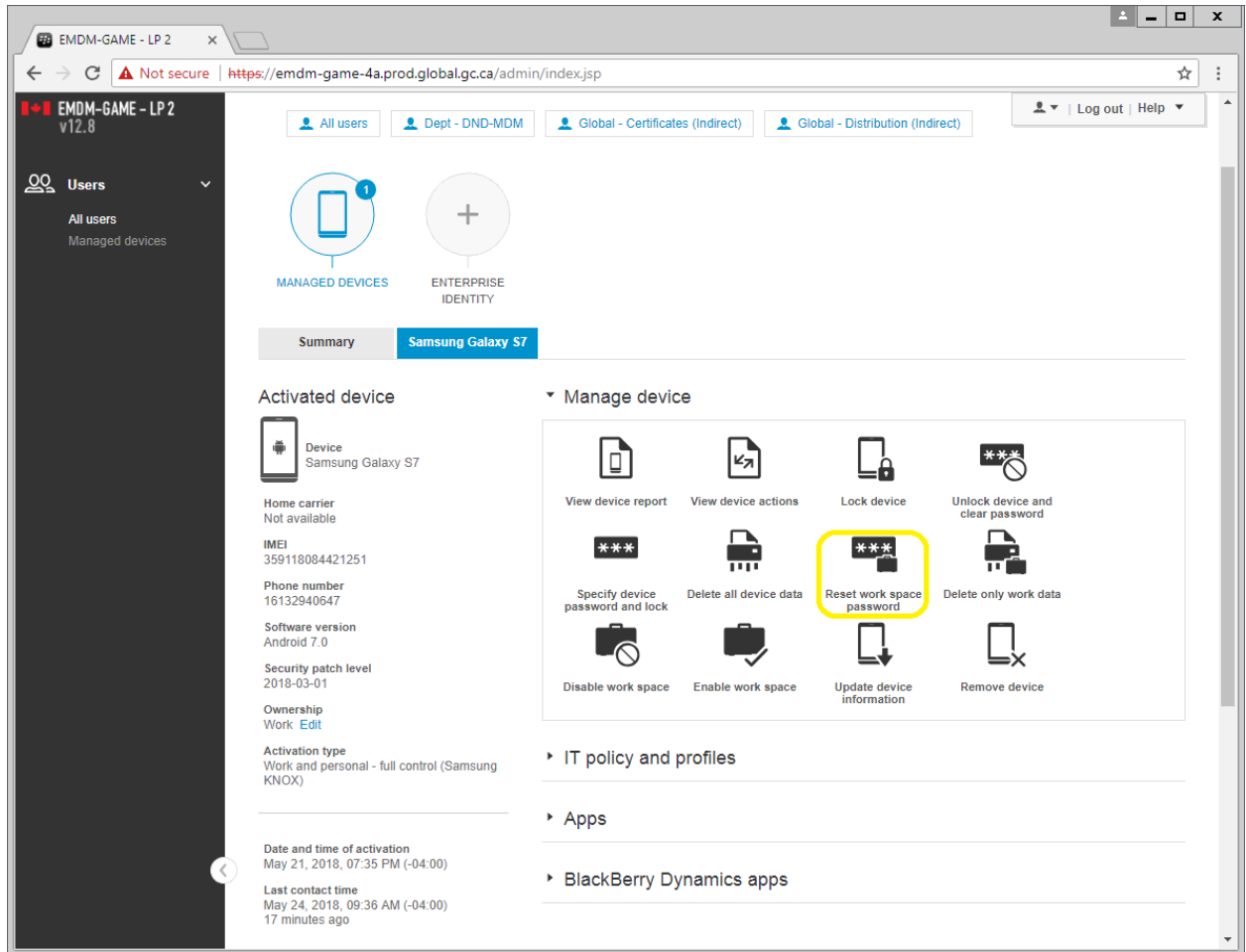
- 1) Search for the user and open their EMDM user account
- 2) Under the user's profile, select the user's Android device (e.g. Samsung Galaxy S8)



The screenshot displays the EMDM Administration Console interface. The user profile for MAYOTTE, ANDREW (DND/MDN) is shown. The 'Managed Devices' section is highlighted, showing a 'Samsung Galaxy S7' device. The 'Activation details' section shows the device is activated and the activation password has expired. The 'IT policy and profiles' section lists various profiles assigned to the device.

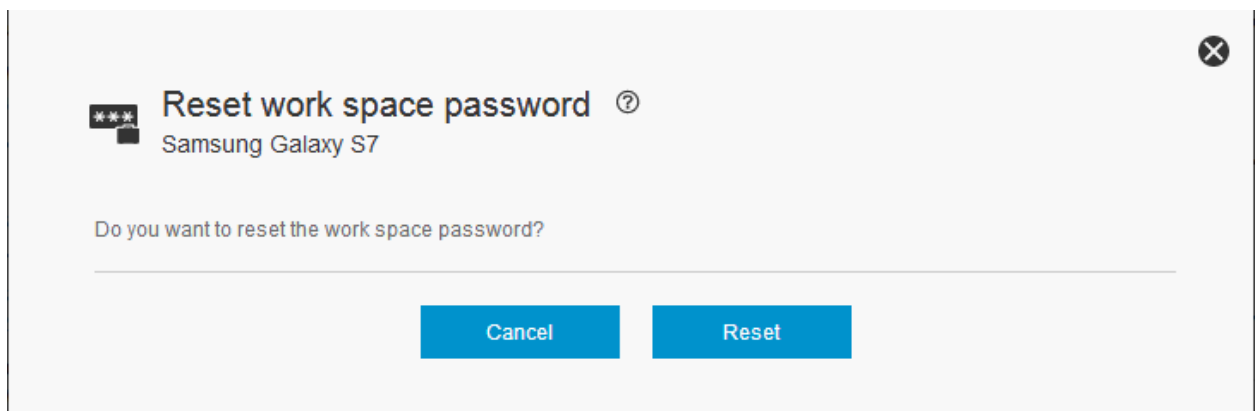
Assigned profile	Assignment	Status
WP-04 IT policy	Group	
DND Email	Group	
Work and Personal Activation	Group	
MDM Connectivity Enterprise connectivity	Group	
Default Compliance	Default	
Default BlackBerry Dynamics	Default	
Default BlackBerry Dynamics connectivity	Default	
Default Enterprise Management Agent	Default	
Entrust Root CA (L1K-G2-cf) CA certificate	Group	

- 3) Under Manage Device, select **Reset work space password**



The screenshot shows the EMDM-GAME - LP 2 administration console. The left sidebar contains 'Users' and 'Managed devices'. The main content area displays 'MANAGED DEVICES' and 'ENTERPRISE IDENTITY'. A 'Summary' tab is selected for a 'Samsung Galaxy S7'. The 'Activated device' section shows details for the device, including Home carrier, IMEI, Phone number, Software version, Security patch level, Ownership, and Activation type. The 'Manage device' section contains a grid of actions: View device report, View device actions, Lock device, Unlock device and clear password, Specify device password and lock, Delete all device data, **Reset work space password** (highlighted), Delete only work data, Disable work space, Enable work space, Update device information, and Remove device. Below this are expandable sections for 'IT policy and profiles', 'Apps', and 'BlackBerry Dynamics apps'.

- 4) In the Reset work space password window, click on **Reset**



The dialog box is titled 'Reset work space password' with a question mark icon. Below the title is the device name 'Samsung Galaxy S7'. The main text asks 'Do you want to reset the work space password?'. At the bottom, there are two buttons: 'Cancel' and 'Reset'.

- 5) Within a minute or two, the user's Knox work space will prompt them to create a new Knox work space password

4.4 Remote device wipe (Android & iOS)

This command wipes all data from the device and returns the device to its factory settings and deactivates it from EMDM. The device must have network connectivity for this command to be successful.

Note for Android devices: This command also disables the Android Factory Reset Protection.

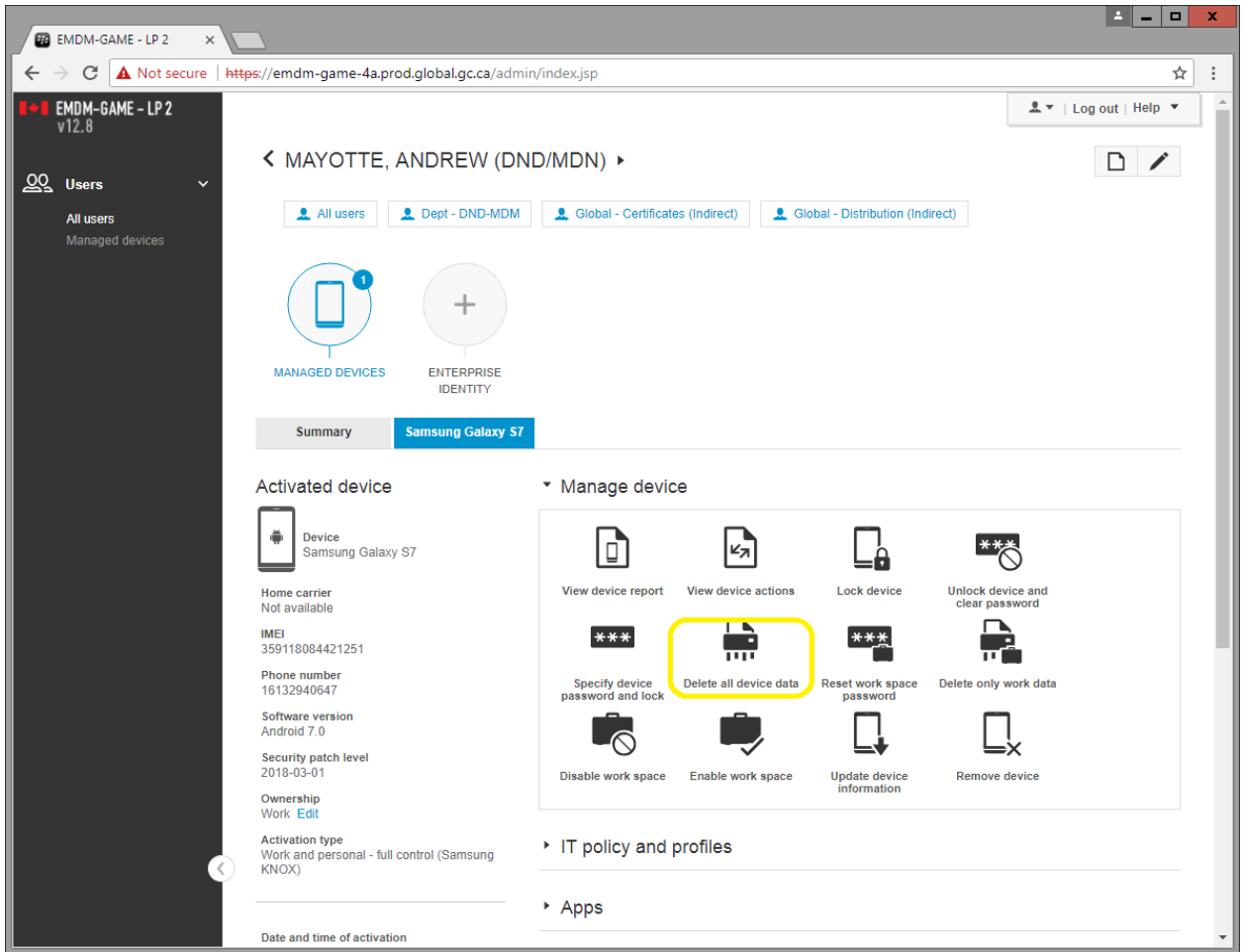
Note for Apple devices: This command does **NOT** remove the Apple Activation Lock feature. If a user was logged into the device with an iCloud / Apple ID, the device will prompt for that account after wiping.

- 1) Search for the user and open their EMDM user account
- 2) Under the user's profile, select the user's mobile device (e.g. Samsung Galaxy S8 or Apple iPhone 8)

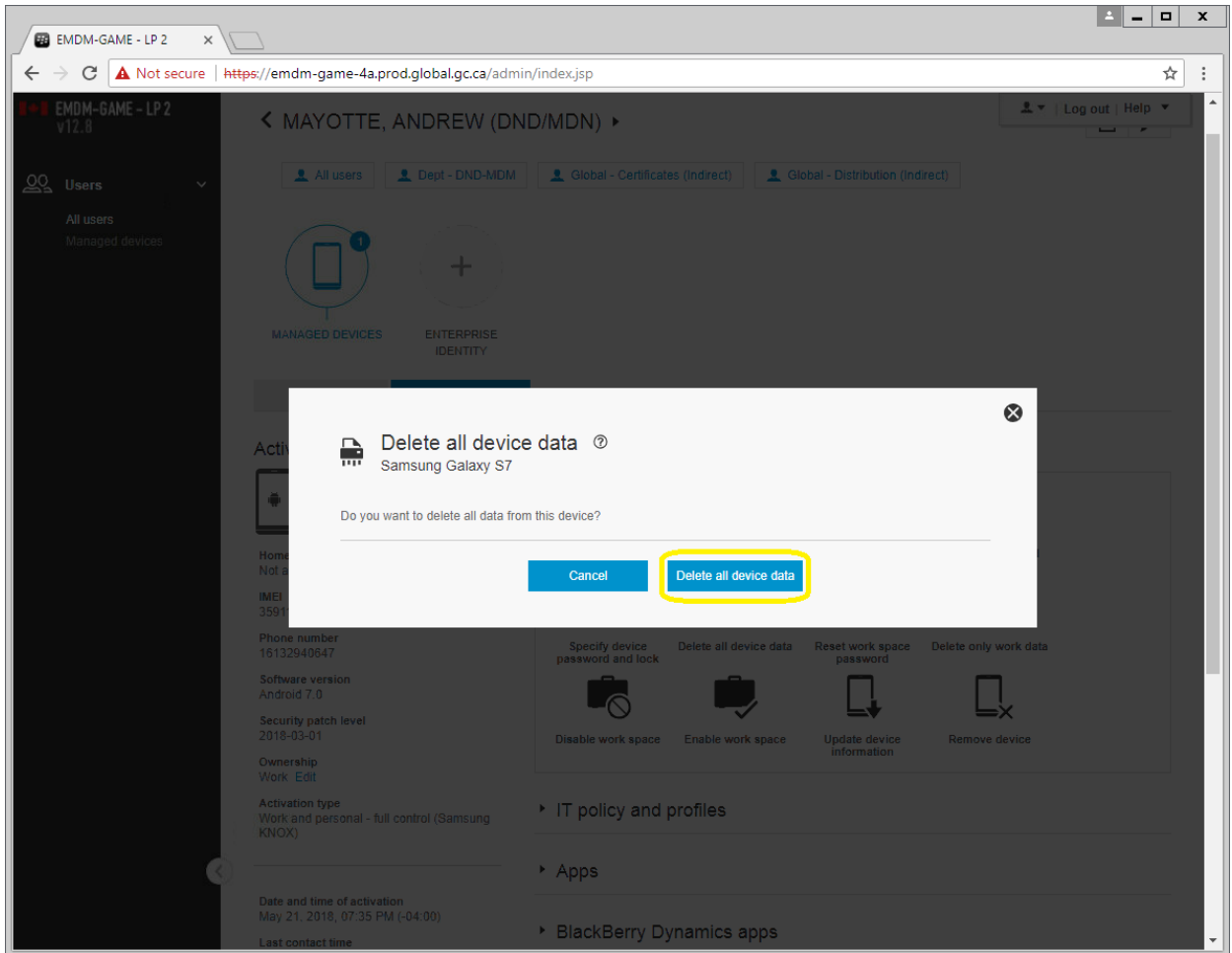
The screenshot displays the EMDM Administration Console interface. The user profile for MAYOTTE, ANDREW (DND/MDN) is shown. The 'Managed Devices' section is highlighted, showing a 'Samsung Galaxy S7' device. The 'Activation details' section shows the device is activated and provides the activation password expiration date. The 'IT policy and profiles' section lists various profiles assigned to the device.

Assigned profile	Assignment	Status
WP-04 IT policy	Group	
DND Email	Group	
Work and Personal Activation	Group	
MDM Connectivity Enterprise connectivity	Group	
Default Compliance	Default	
Default BlackBerry Dynamics	Default	
Default BlackBerry Dynamics connectivity	Default	
Default Enterprise Management Agent	Default	
Entrust Root CA (L1K-G2-cf)	Group	

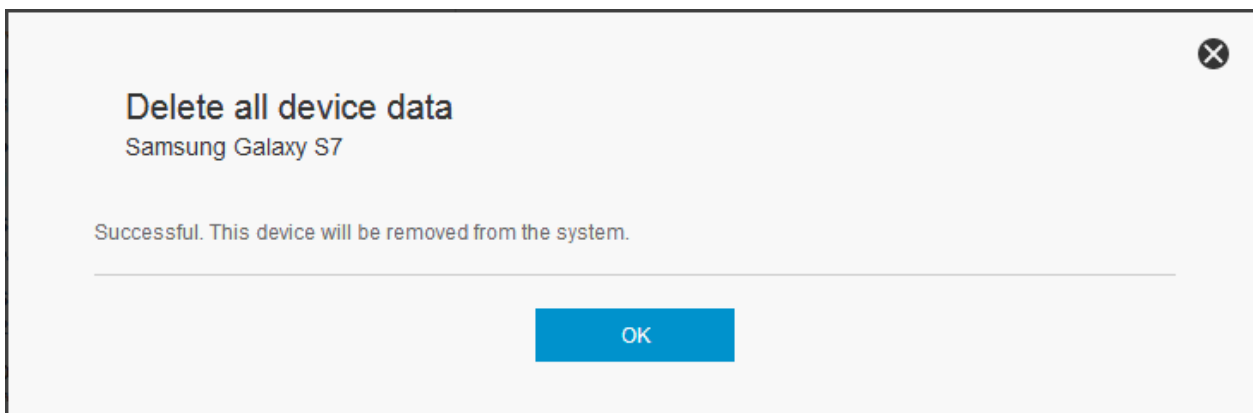
- 3) **Important:** If the device was lost or stolen, capture any pertinent device information (make, model, IMEI, phone number, carrier, etc.) as this will be required for the military police investigation as well as to request a replacement device.
- 4) Under Manage Device, select **Delete all device data**



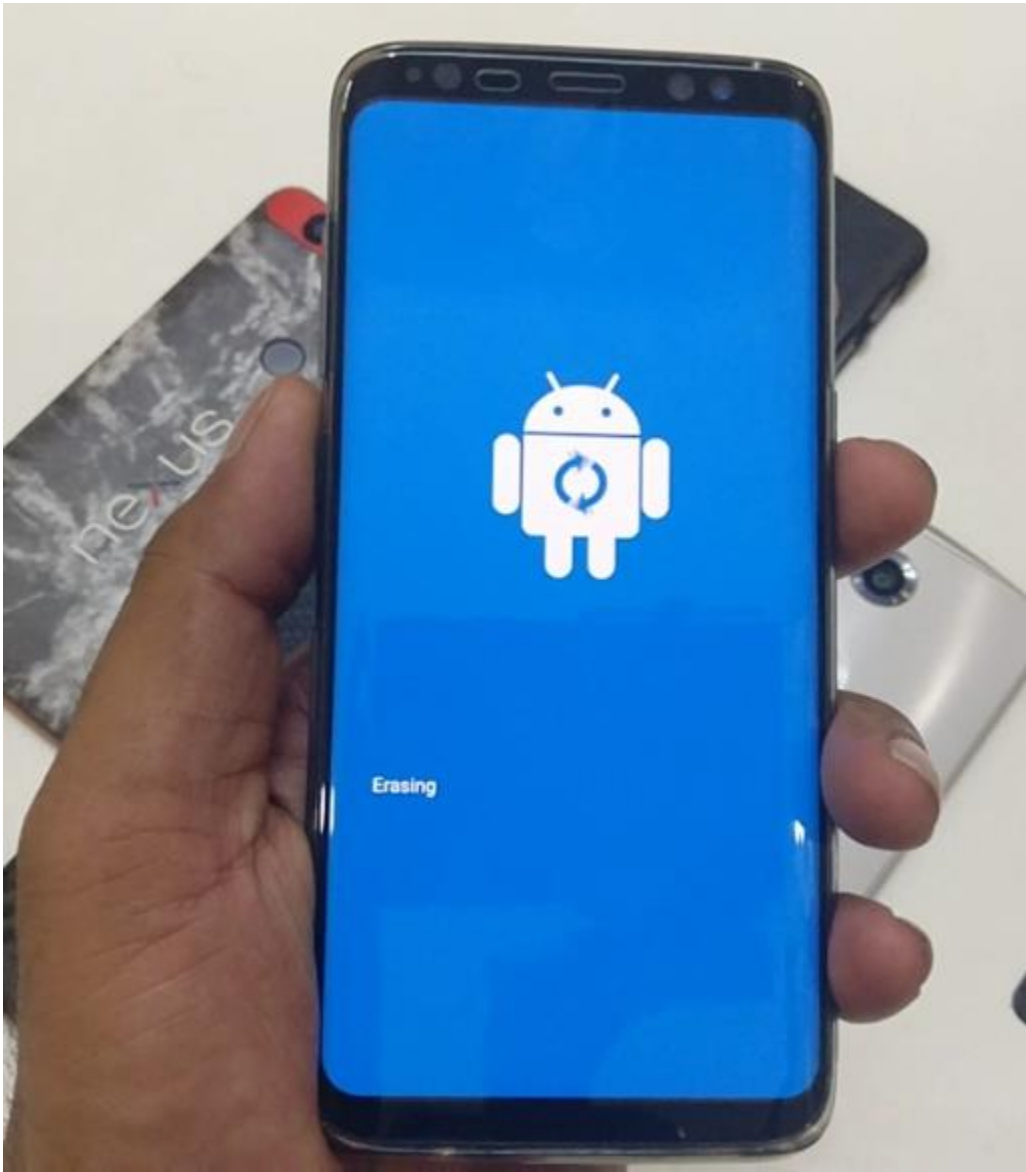
5) In the Delete all device data window, click on **Delete all device data**



- 6) Within a minute or two, the device will perform a factory reset, wiping all data in the process. The EMDM Administration console will display a confirmation when the remote device wipe has been initiated



Android device:



iOS device:



4.5 Disable/Re-enable Knox work space (Android only)

This command disables or re-enables a user's access to the Android Knox work space on the device. This command does not delete the work space. The device must have network connectivity for this command to be successful.

- 1) Search for the user and open their EMDM user account
- 2) Under the user's profile, select the user's Android device (e.g. Samsung Galaxy S8)

EMDM-GAME - LP 2

Not secure | https://emdm-game-4a.prod.global.gc.ca/admin/index.jsp

EMDM-GAME - LP 2
v12.8

Users

All users
Managed devices

< MAYOTTE, ANDREW (DND/MDN) >

All users Dept - DND-MDM Global - Certificates (Indirect) Global - Distribution (Indirect)

MANAGED DEVICES ENTERPRISE IDENTITY

Summary Samsung Galaxy S7

Activation details

Activated devices
Samsung Galaxy S7
1 of 10 devices activated

Device activation password
Expired on May 23, 2018, 07:03 PM (-04:00)

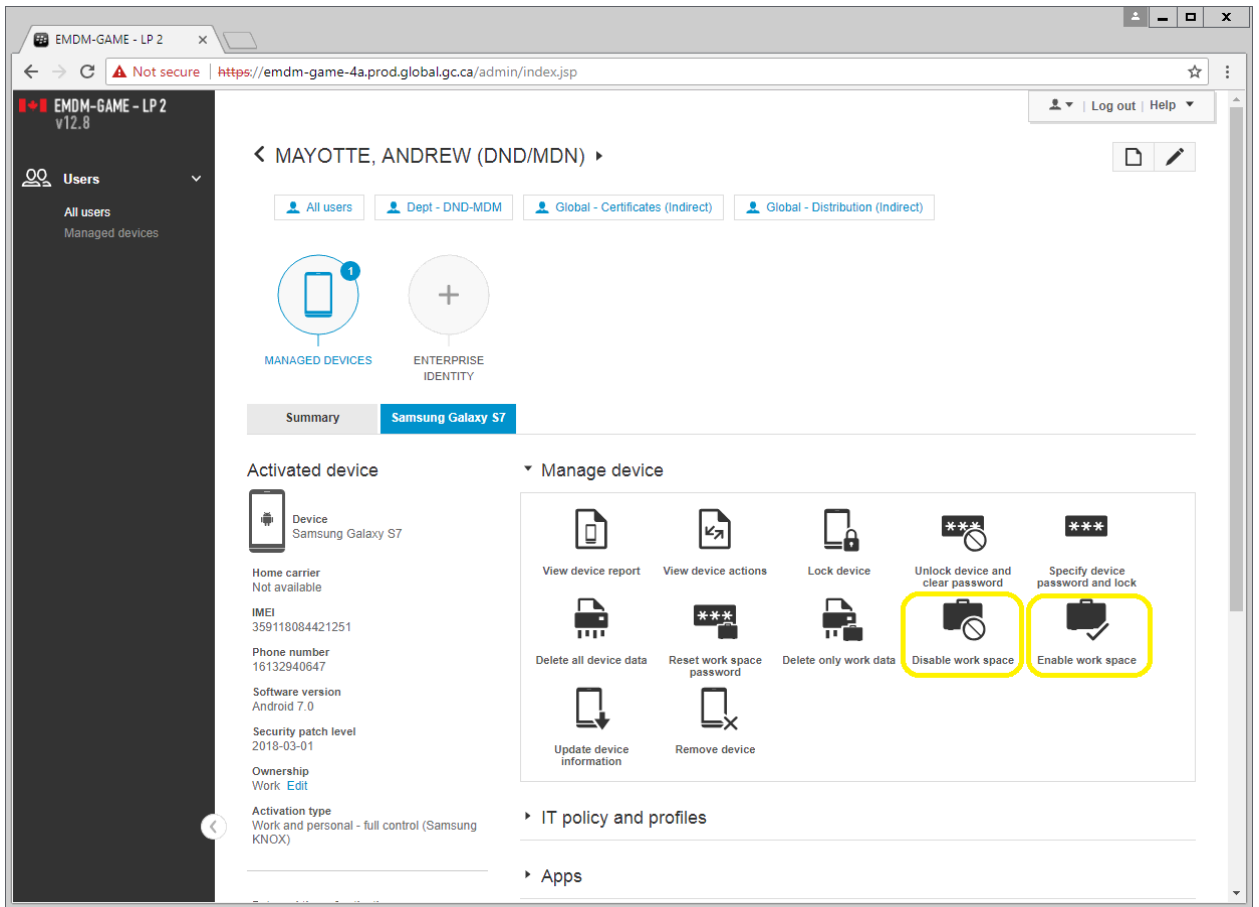
Set activation password

BlackBerry 2FA
To enable this feature, assign a BlackBerry 2FA profile.

IT policy and profiles

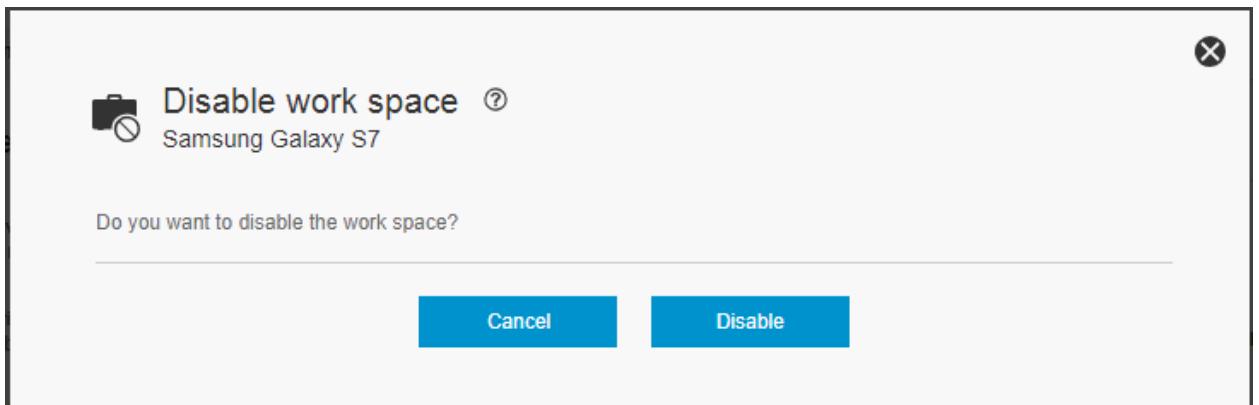
Assigned profile	Assignment	Status
WP-04 IT policy	Group	
DND Email	Group	
Work and Personal Activation	Group	
MDM Connectivity Enterprise connectivity	Group	
Default Compliance	Default	
Default BlackBerry Dynamics	Default	
Default BlackBerry Dynamics connectivity	Default	
Default Enterprise Management Agent	Default	
Entrust Root CA (L1K-G2-cf)	Group	

3) Select **Disable work space** or **Enable work space** depending on the circumstance

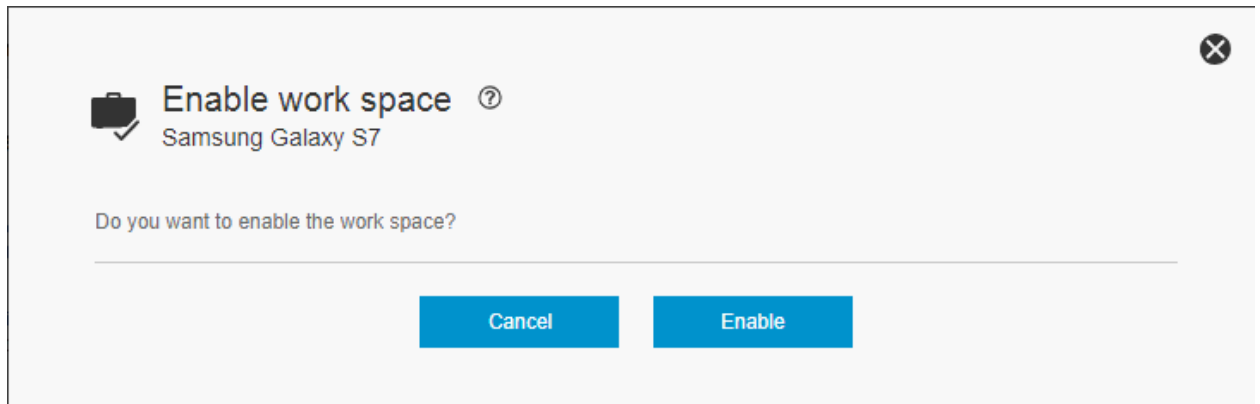


4) Confirm the command

Disable:



Re-enable:



Note: When the Knox workspace is disabled, the following message will appear on the device when the user attempts to access the workspace:



4.6 Set device re-activation password (Android & iOS)

This command creates a device activation password in order to activate a new device or reactivate an existing device.

Note: Instructions on how to activate a mobile are available separately from this document.

- 1) Search for the user and open their EMDM user account

2) Under the user's profile, select **Set activation password**

The screenshot displays the user profile page for MAYOTTE, ANDREW (DND/MDN). The page includes a navigation sidebar on the left with 'Users' and 'Managed devices' options. The main content area shows the user's profile with tabs for 'All users', 'Dept - DND-MDM', 'Global - Certificates (Indirect)', and 'Global - Distribution (Indirect)'. Below the profile, there are sections for 'MANAGED DEVICES' (showing 1 device) and 'ENTERPRISE IDENTITY'. The 'Summary' tab is selected, showing details for a 'Samsung Galaxy S7'. The 'Activation details' section indicates that 1 of 10 devices are activated and shows the device activation password expiration date. A yellow box highlights the 'Set activation password' button. The 'IT policy and profiles' section lists various assigned profiles such as 'WP-04 IT policy', 'DND Email', 'Work and Personal Activation', and 'MDM Connectivity Enterprise connectivity'.

3) In the Set activation password window:

- a. **Activation option:** *Default device activation*
- b. **Activation password:** *Set device activation password*
- c. **Device activation password:** *<set a device activation password of your choosing (e.g. Canada150)>*
- d. **Activation period expiration:** *<set a device activation password expiry period of your choosing (e.g. 2 days)>*
- e. **Activation period expires after the first device is activated:** *Optional*
- f. **Activation email template:**
 - i. *Android: Default activation email*
 - ii. *iOS: Apple DEP activation email*

Android:

Set device activation password

Device activation

Activation option*
Default device activation

Activation password*
Set device activation password

Device activation password*
●●●

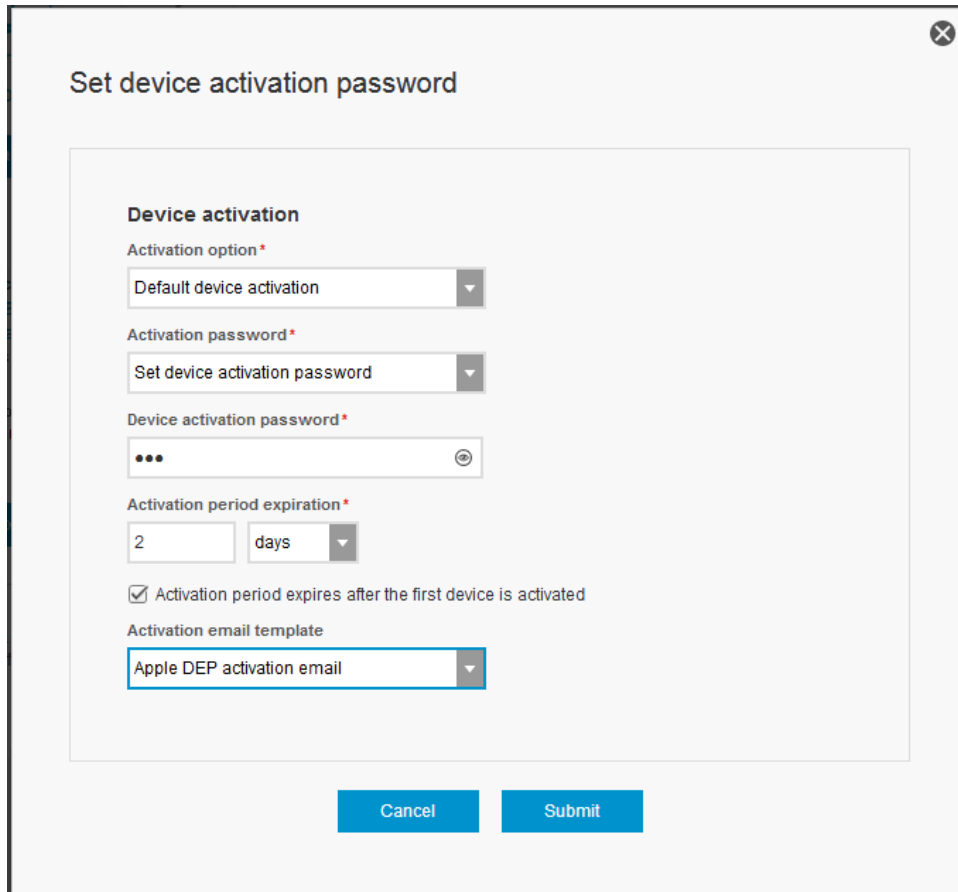
Activation period expiration*
2 days

Activation period expires after the first device is activated

Activation email template
Default activation email

Cancel Submit

iOS:



The screenshot shows a dialog box titled "Set device activation password" with a close button (X) in the top right corner. The dialog contains the following fields and options:

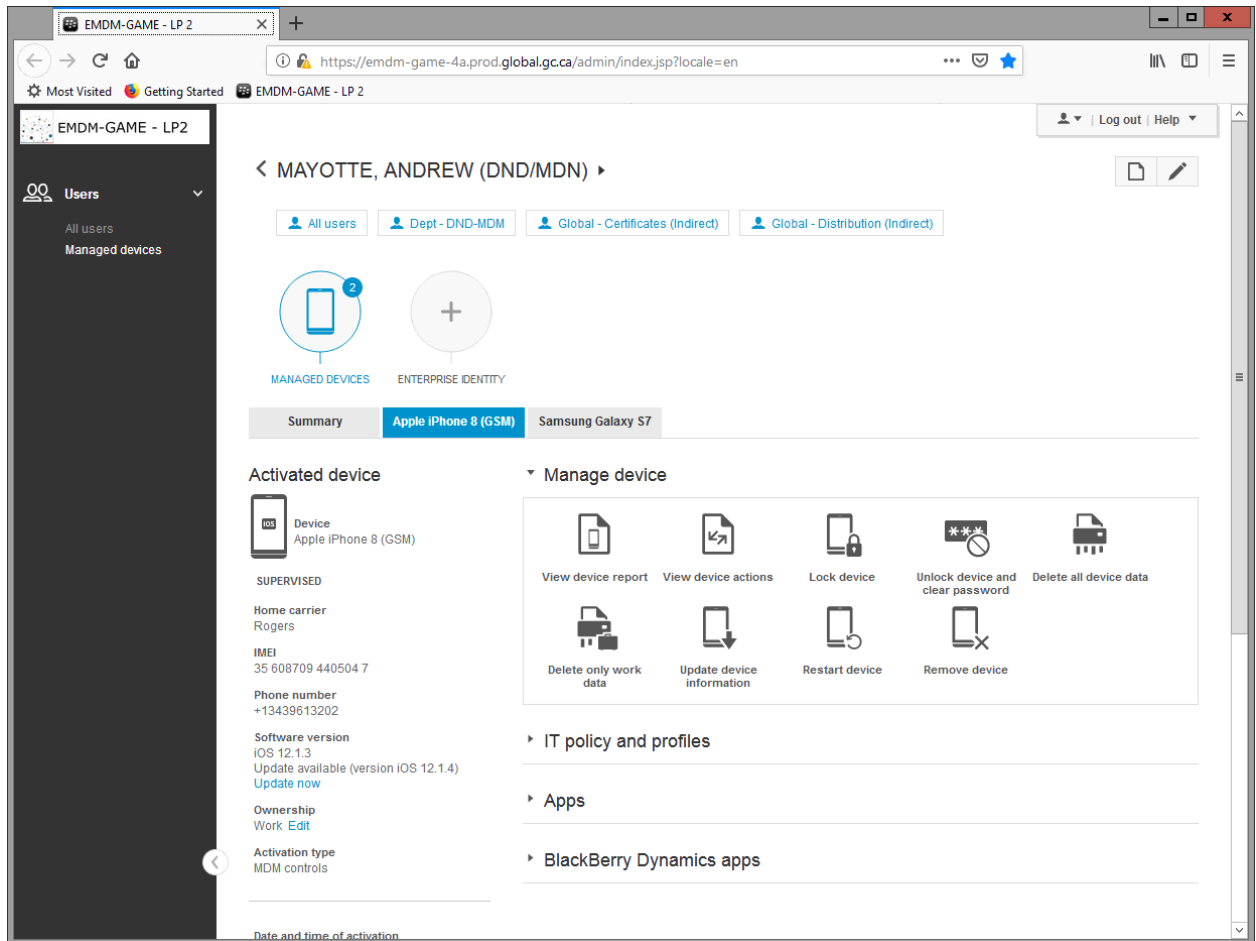
- Device activation**
 - Activation option *: Default device activation (dropdown)
 - Activation password *: Set device activation password (dropdown)
 - Device activation password *: [masked with dots] (password field with toggle icon)
 - Activation period expiration *: 2 days (input field and dropdown)
 - Activation period expires after the first device is activated
 - Activation email template: Apple DEP activation email (dropdown)
- Buttons: Cancel and Submit

- 4) Click **Submit** to set a device activation password and send the user an email with information (i.e. activation password) they will require to activate their device

4.7 Remote restart device (iOS only)

You can remote restart an iOS device from within the EMDM administration console. The device must have network connectivity for this command to be successful.

- 1) Search for the user and open their EMDM user account
- 2) Under the user's profile, select the user's iOS device (e.g. Apple iPhone 8)



The screenshot displays the Enterprise Mobile Device Management Administration Console interface. The browser address bar shows the URL: <https://emdm-game-4a.prod.global.gc.ca/admin/index.jsp?locale=en>. The page title is "EMDM-GAME - LP2".

The main content area is titled "MAYOTTE, ANDREW (DND/MDN)". Below the title, there are navigation tabs: "All users", "Dept - DND-MDM", "Global - Certificates (Indirect)", and "Global - Distribution (Indirect)".

There are two main sections: "MANAGED DEVICES" (with a notification badge '2') and "ENTERPRISE IDENTITY".

The "Activated device" section shows details for an "Apple iPhone 8 (GSM)". The device is supervised and managed by Rogers. Key details include:

- IMEI: 35 608709 440504 7
- Phone number: +13439613202
- Software version: iOS 12.1.3 (Update available: version iOS 12.1.4)
- Ownership: Work
- Activation type: MDM controls

The "Manage device" section provides various actions:

- View device report
- View device actions
- Lock device
- Unlock device and clear password
- Delete all device data
- Delete only work data
- Update device information
- Restart device
- Remove device

Below the "Manage device" section, there are expandable sections for "IT policy and profiles", "Apps", and "BlackBerry Dynamics apps".

3) Under Manage device, select **Restart device**

The screenshot shows the EMDM-GAME Administration Console interface. The browser address bar displays `https://emdm-game-4a.prod.global.gc.ca/admin/index.jsp?locale=en`. The main content area is titled "Managed devices" and shows a list of devices. The "Apple iPhone 8 (GSM)" device is selected, and its details are displayed. The "Restart device" option is highlighted with a yellow box in the "Manage device" section. The details for the selected device include:

- Device: Apple iPhone 8 (GSM)
- SUPERVISED
- Home carrier: Rogers
- IMEI: 35 608709 440504 7
- Phone number: +13439613202
- Software version: iOS 12.1.3 (Update available (version iOS 12.1.4) [Update now](#))
- Ownership: Work [Edit](#)
- Activation type: MDM controls
- Date and time of activation: October 19, 2018, 11:17 AM (-04:00)
- Last contact time: February 9, 2019, 04:02 PM (-05:00)

The "Restart device" option is highlighted in a yellow box in the "Manage device" section. Other options include "View device report", "View device actions", "Lock device", "Unlock device and clear password", "Delete all device data", "Delete only work data", "Update device information", and "Remove device".

4) In the Restart device window, confirm the command by selecting **Restart**

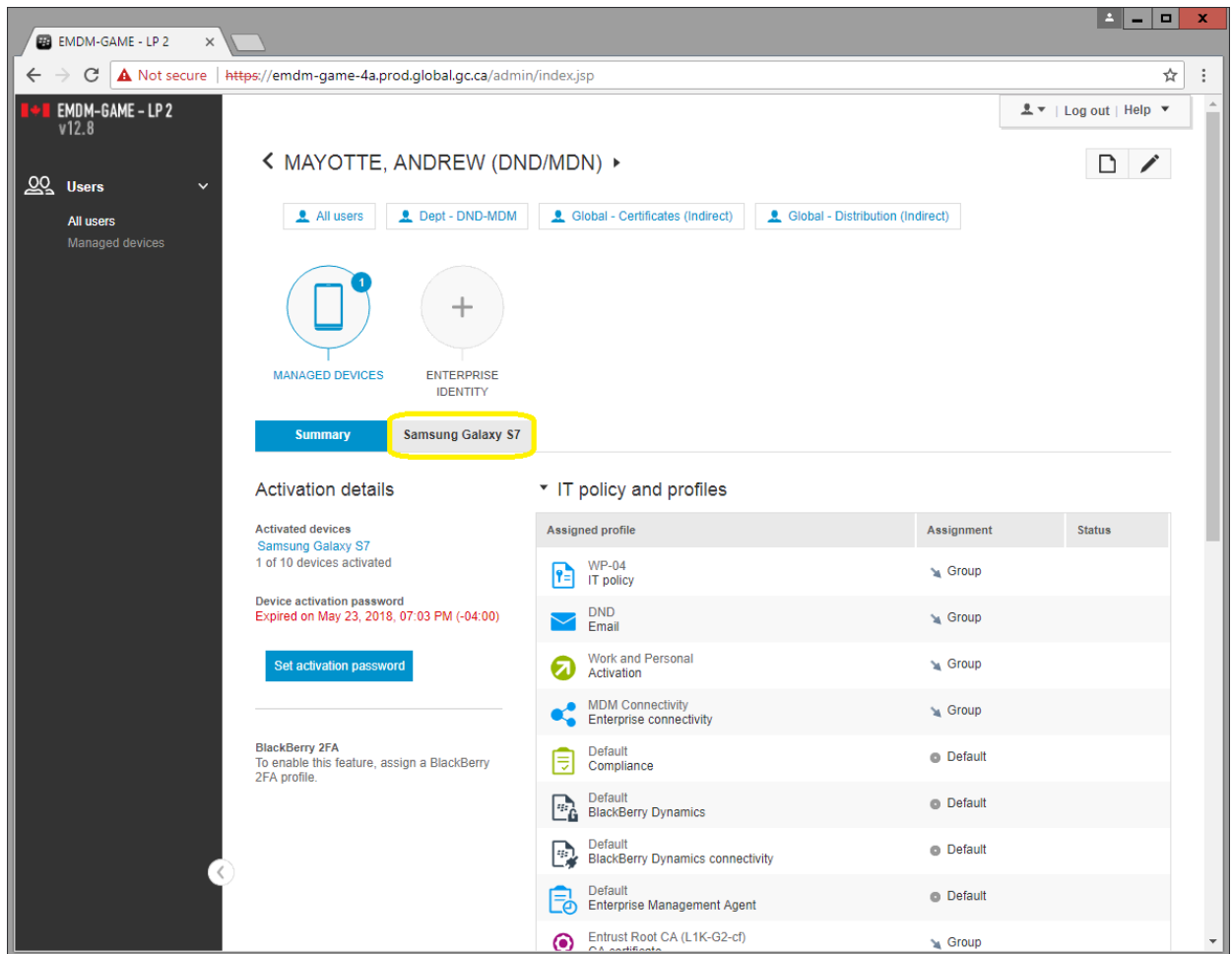
The screenshot shows a confirmation dialog box titled "Restart device" for the device "Apple iPhone 8 (GSM)". The dialog asks "Do you want to restart the device?" and provides two buttons: "Cancel" and "Restart".

5) Within a minute or two, the device will restart.

4.8 View device information (Android & iOS)

You can view detailed information about a user's device (e.g. Last contact time, phone number, OS version, etc.) from within the EMDM administration console.

- 1) Search for the user and open their EMDM user account
- 2) Under the user's profile, select the user's mobile device (e.g. Samsung Galaxy S8 or Apple iPhone 8)



The screenshot displays the EMDM administration console interface. The user profile for MAYOTTE, ANDREW (DND/MDN) is shown. The 'Managed Devices' section is highlighted, showing a 'Samsung Galaxy S7' device. The 'Activation details' section shows the device is activated and the activation password has expired. The 'IT policy and profiles' section lists various profiles assigned to the device.

Assigned profile	Assignment	Status
WP-04 IT policy	Group	
DND Email	Group	
Work and Personal Activation	Group	
MDM Connectivity Enterprise connectivity	Group	
Default Compliance	Default	
Default BlackBerry Dynamics	Default	
Default BlackBerry Dynamics connectivity	Default	
Default Enterprise Management Agent	Default	
Entrust Root CA (L1K-G2-0f)	Group	

- 3) Under Manage Device, select **View device report**

The screenshot displays the EMDM-GAME - LP 2 v12.8 interface. The user profile for MAYOTTE, ANDREW (DND/MDN) is shown, with tabs for All users, Dept - DND-MDM, Global - Certificates (Indirect), and Global - Distribution (Indirect). The device list shows 1 Managed Device and Enterprise Identity. The selected device is a Samsung Galaxy S7. The 'Activated device' section provides details: Device (Samsung Galaxy S7), Home carrier (Not available), IMEI (359118084421251), Phone number (16132940647), Software version (Android 7.0), Security patch level (2018-03-01), Ownership (Work), and Activation type (Work and personal - full control (Samsung KNOX)). The 'Manage device' section includes options: View device report (highlighted), View device actions, Lock device, Unlock device and clear password, Specify device password and lock, Delete all device data, Reset work space password, Delete only work data, Disable work space, Enable work space, Update device information, and Remove device. Below are sections for IT policy and profiles, and Apps.

- 4) A window will open with a full hardware/software report of that user's device. You can export the report to a .csv file by clicking on the arrow in the top right hand corner of the report.

BlackBerry UEM - Google Chrome

Not secure | <https://emdm-game-4a.prod.global.gc.ca/admin/device/viewDeviceReport.do?deviceId=49&userId=101&sharedDeviceGroupId=0>

Device report

MAYOTTE, ANDREW (DND/MDN)
ANDREW.MAYOTTE@forces.gc.ca

Samsung Galaxy S7

Compliance violations defined by the assigned compliance profile

OS violation	False
Non-assigned app is installed	False
Required app is not installed	False
Restricted app is installed on the device	False
Restricted OS version is installed on the device	False
Restricted device model	False
Required security patch level is not installed	False

General

Hardware vendor name	Samsung Electronics
Model ID	herollebmc
Model number	Galaxy S7
Device form factor	Handheld
OS version	Android 7.0
Device ownership	Work
Activation state	The device is activated.
Date and time of activation	May 21, 2018 7:35:06 PM (-04:00)
Last contacted	May 24, 2018 12:03:06 PM (-04:00)
Battery level	60.0
UDID	146e16ef9a7d0e142b9891413ded8f6e88afe53150643f7769feac37fde833den_CA
Language	en_CA
IMEI	359118084421251
Perimeter UUID	dffd031e-8ab1-453d-a188-1fdd539f4dfd
Reactivation count	0
Last perimeter state changed	May 21, 2018 7:37:35 PM (-04:00)
Workspace password configured	True
Personal hotspot	False
Organization information	True

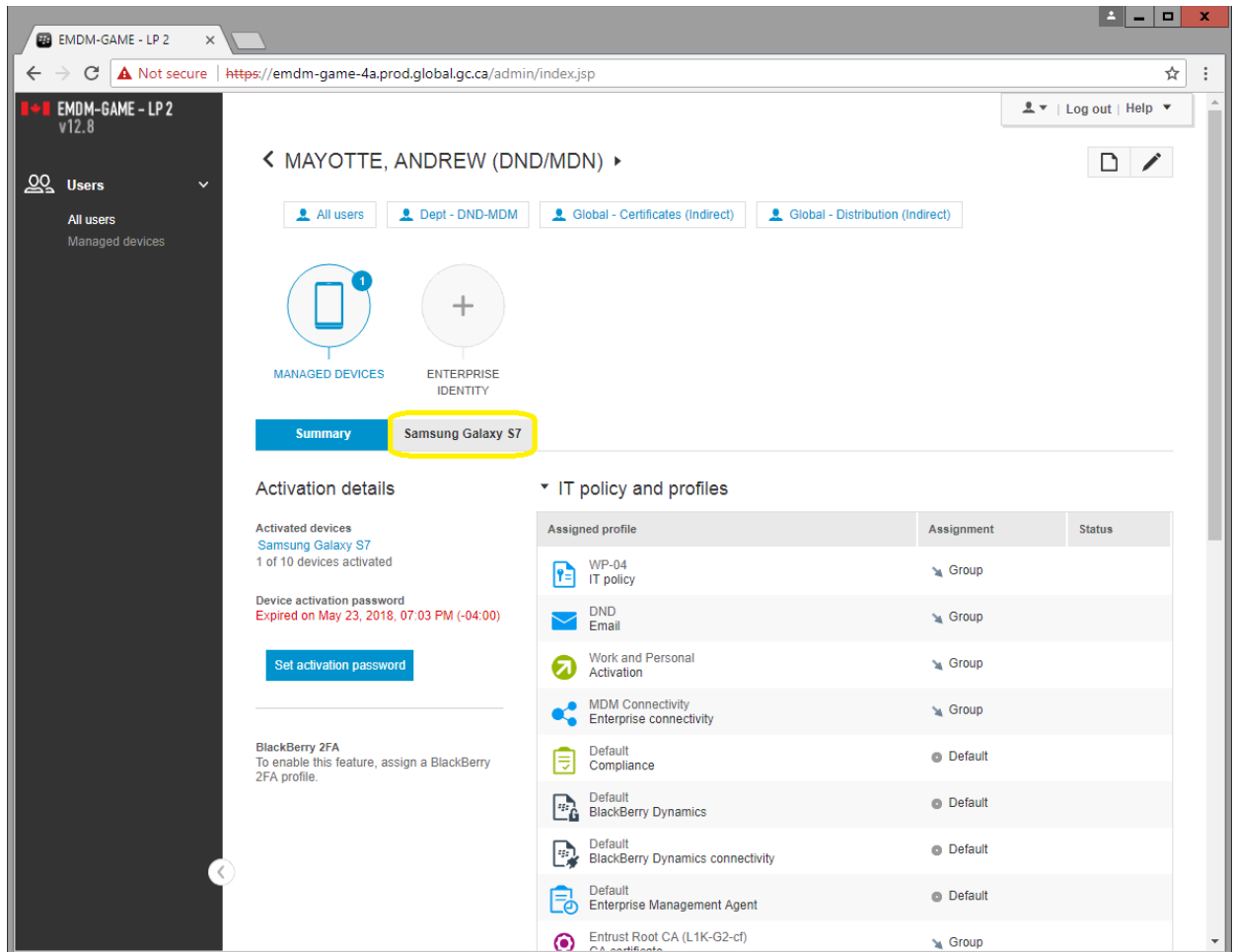
Device status and specifications

Bluetooth enabled	True
Bluetooth type supported	v4.2, A2DP, LE, apt-X
Bluetooth MAC address	14:9F:3C:A2:26:3A
Wi-Fi enabled	True
Wi-Fi networks supported	Wi-Fi 802.11 a/b/g/n/ac
Wi-Fi SSID	Blocked
Wi-Fi IP address	Blocked

4.9 View device actions (Android & iOS)

This function displays the actions that were taken or are in progress on a device as a result of commands sent from the EMDM Administration Console, such as locking a device, resetting the Knox work space password, or deleting device data.

- 1) Search for the user and open their EMDM user account
- 2) Under the user's profile, select the user's mobile device (e.g. Samsung Galaxy S8 or Apple iPhone 8)



The screenshot displays the EMDM Administration Console interface. The user profile for MAYOTTE, ANDREW (DND/MDN) is shown. The 'Managed Devices' section is highlighted, indicating one device is managed. The 'IT policy and profiles' section is also visible, listing various profiles and their assignments.

Assigned profile	Assignment	Status
WIP-04 IT policy	Group	
DND Email	Group	
Work and Personal Activation	Group	
MDM Connectivity Enterprise connectivity	Group	
Default Compliance	Default	
Default BlackBerry Dynamics	Default	
Default BlackBerry Dynamics connectivity	Default	
Default Enterprise Management Agent	Default	
Entrust Root CA (L1K-G2-cf) CA certificate	Group	

- 3) Under Manage Device, select **View device actions**

The screenshot displays the EMDM Administration Console interface. The browser address bar shows the URL <https://emd-game-4a.prod.global.gc.ca/admin/index.jsp>. The page title is "EMDM-GAME - LP 2 v12.8". The left sidebar shows "Users" and "Managed devices". The main content area is titled "Summary" and "Samsung Galaxy S7". Under "Activated device", the device details are listed: Device (Samsung Galaxy S7), Home carrier (Not available), IMEI (359118084421251), Phone number (16132940647), Software version (Android 7.0), Security patch level (2018-03-01), Ownership (Work), Activation type (Work and personal - full control (Samsung KNOX)), Date and time of activation (May 21, 2018, 07:35 PM (-04:00)), Last contact time (May 25, 2018, 06:59 AM (-04:00)), Battery level (80.0%), and Internal storage (19456.0 MB free / 65536.0 MB total). The "Manage device" section contains a grid of icons for various actions: View device report, View device actions (highlighted with a yellow box), Lock device, Unlock device and clear password, Specify device password and lock, Delete all device data, Reset work space password, Delete only work data, Disable work space, Enable work space, Update device information, and Remove device. Below the grid are sections for "IT policy and profiles", "Apps", and "BlackBerry Dynamics apps".

- 4) A window will appear displaying the actions that were taken or are in progress on a device as a result of commands sent from the EMDM Administration Console

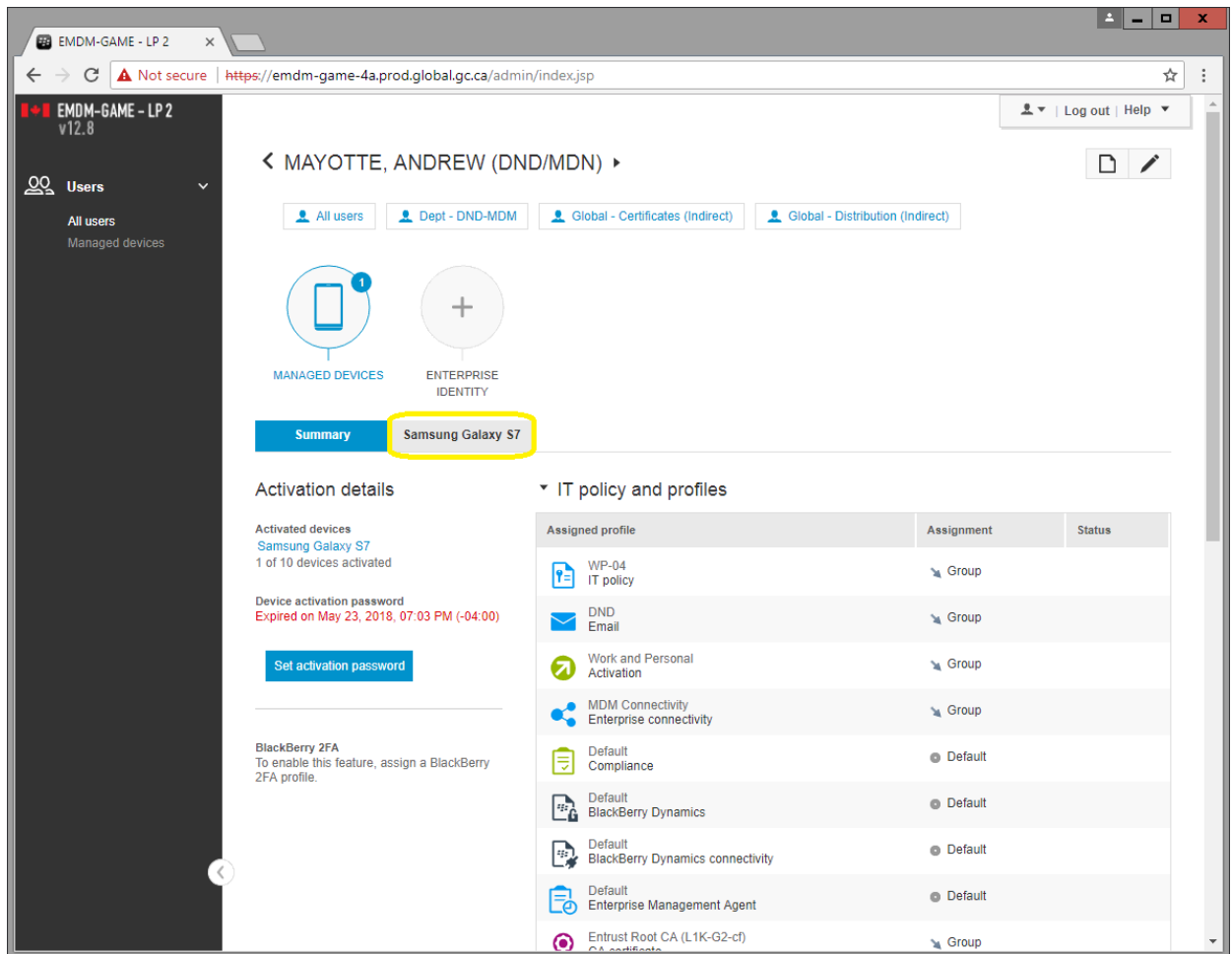
The screenshot shows a web browser window titled "BlackBerry UEM - Google Chrome". The address bar displays a "Not secure" warning and the URL <https://emdm-game-4a.prod.global.gc.ca/admin/device/viewDeviceActions.do?deviceId=...>. The page content includes a header "Device actions" with a refresh icon and the user name "MAYOTTE, ANDREW (DNDVMDN)(ANDREW.MAYOTTE@forces.gc.ca)". Below this, a section titled "Samsung Galaxy S7" contains a table with the following data:

Date modified	Date created	Action	Status
5/23/2018, 10:00:08 AM	5/23/2018, 9:58:34 AM	Send IT policy and profiles	Command completed by device

4.10 Update device information (Android & iOS)

This command polls the device for updated information, such as OS version, current carrier or battery level. The device must have network connectivity for this command to be successful.

- 1) Search for the user and open their EMDM user account
- 2) Under the user's profile, select the user's mobile device (e.g. Samsung Galaxy S8 or Apple iPhone 8)



The screenshot displays the EMDM Administration Console interface. The user profile for MAYOTTE, ANDREW (DND/MDN) is shown. The 'Managed Devices' section is highlighted, showing a 'Samsung Galaxy S7' device. The 'Activation details' section shows the device is activated and the activation password has expired. The 'IT policy and profiles' section lists various profiles assigned to the device.

Assigned profile	Assignment	Status
WP-04 IT policy	Group	
DND Email	Group	
Work and Personal Activation	Group	
MDM Connectivity Enterprise connectivity	Group	
Default Compliance	Default	
Default BlackBerry Dynamics	Default	
Default BlackBerry Dynamics connectivity	Default	
Default Enterprise Management Agent	Default	
Entrust Root CA (L1K-G2-0f)	Group	

- 3) Under Manage Device, select **Update device information**

The screenshot displays the EMDM Administration Console interface. The browser address bar shows the URL <https://emdm-game-4a.prod.global.gc.ca/admin/index.jsp>. The user profile for MAYOTTE, ANDREW (DND/MDN) is visible at the top. Below the profile, there are tabs for 'All users', 'Dept - DND-MDM', 'Global - Certificates (Indirect)', and 'Global - Distribution (Indirect)'. The main content area shows 'MANAGED DEVICES' and 'ENTERPRISE IDENTITY' icons. A 'Summary' tab is selected, showing details for a 'Samsung Galaxy S7' device. The device is listed as an 'Activated device' with the following information:

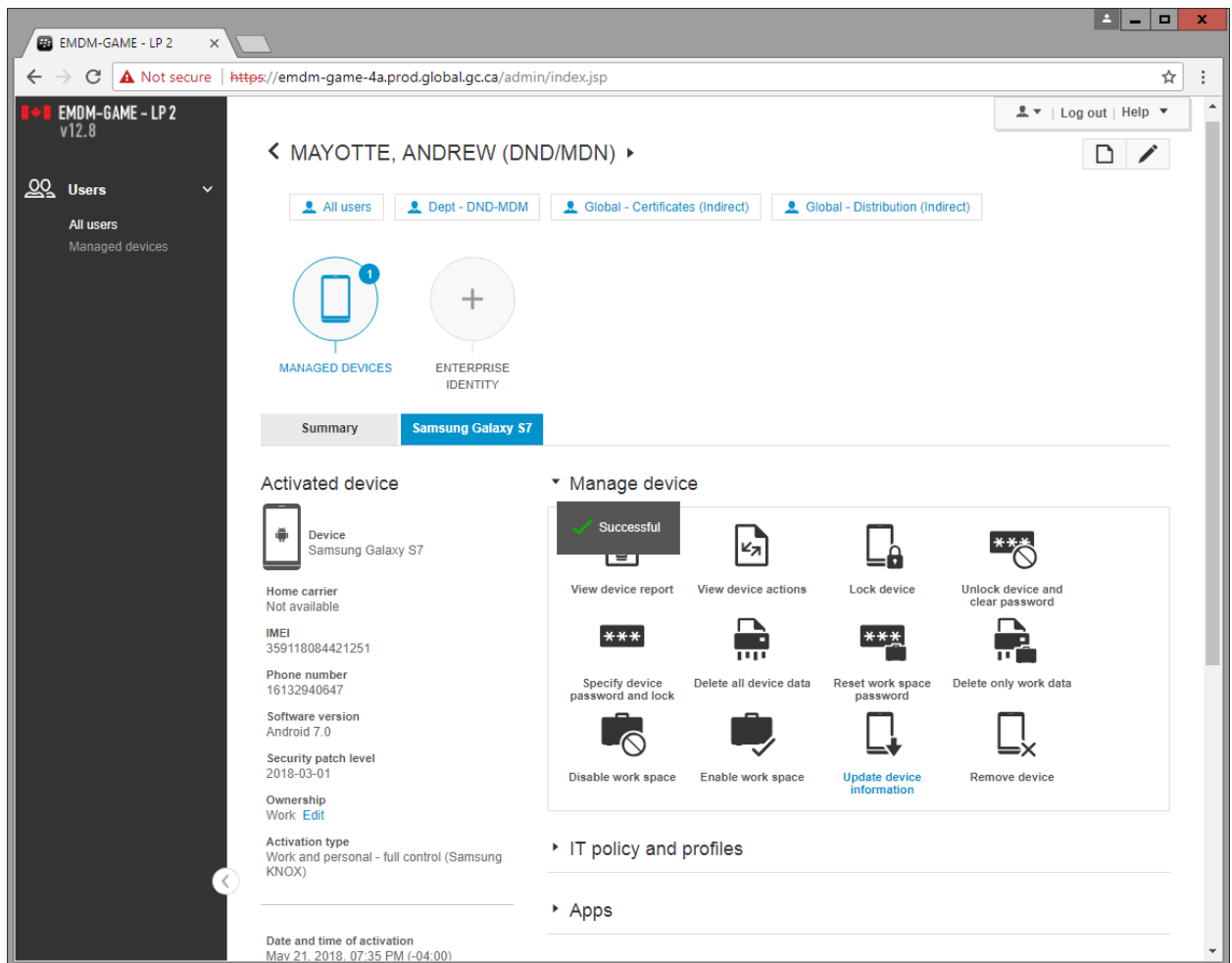
- Device: Samsung Galaxy S7
- Home carrier: Not available
- IMEI: 359118084421251
- Phone number: 16132940647
- Software version: Android 7.0
- Security patch level: 2018-03-01
- Ownership: Work Edit
- Activation type: Work and personal - full control (Samsung KNOX)

The 'Manage device' section contains several actions, with 'Update device information' highlighted in yellow:

- View device report
- View device actions
- Lock device
- Unlock device and clear password
- Specify device password and lock
- Delete all device data
- Reset work space password
- Delete only work data
- Disable work space
- Enable work space
- Update device information
- Remove device

Below the 'Manage device' section, there are expandable sections for 'IT policy and profiles' and 'Apps'.

- 4) A Successful message will appear if the EMDM Administration Console is able to contact the device and poll information from it.



- 5) You can then run the [View device information](#) command to get an up to date information report of the device.

4.11 Delete work space only data (Android & iOS)

Do not use this command!

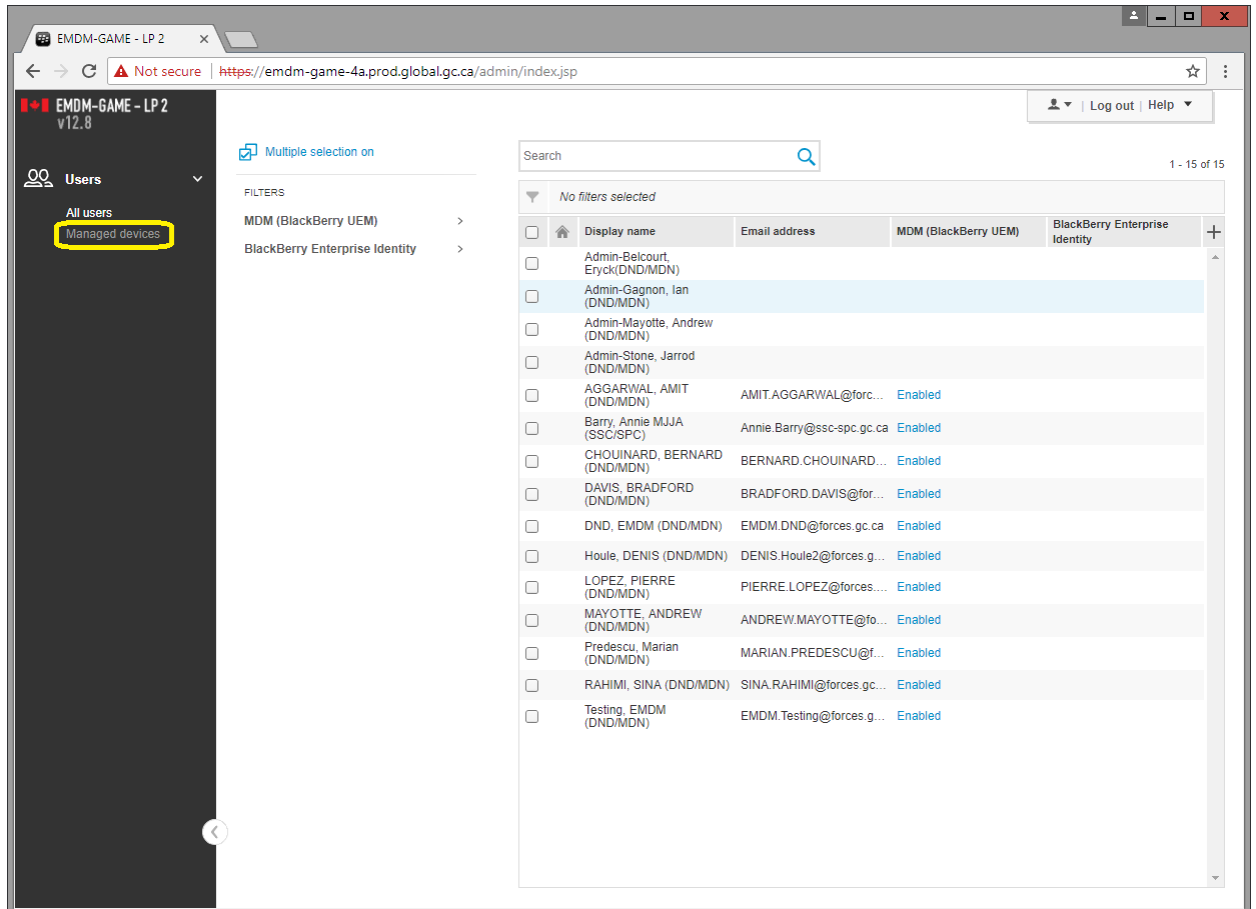
Android devices are registered with "Knox Mobile Enrollment" and iOS devices are registered with "Apple Device Enrollment Program". This command breaks the management of those devices and requires a factory reset in order to activate them again. As such, do not use this command.

5. General administration

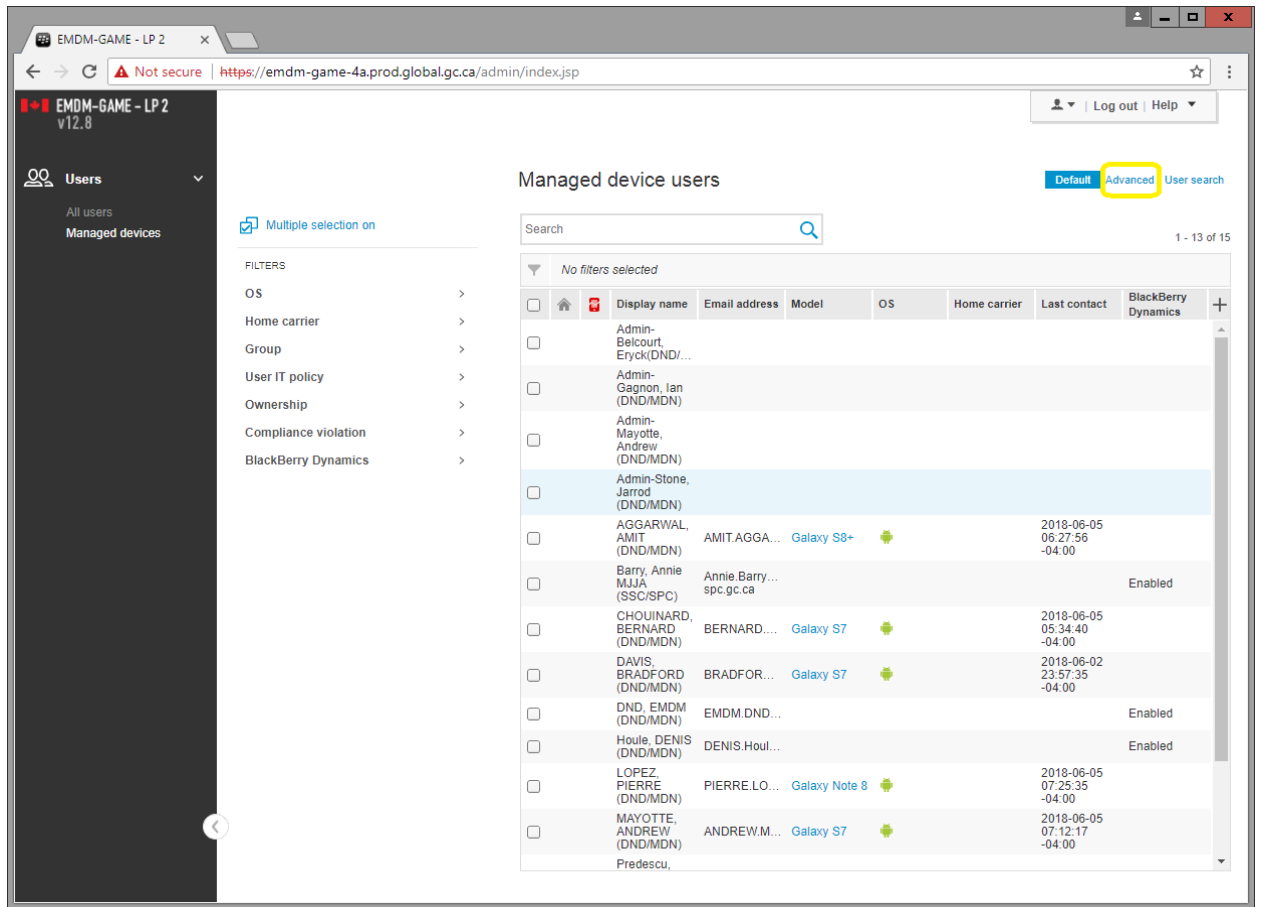
5.1 Extract EMDM user list

This function allows exporting of user and device information into a .csv file format document.

- 1) From the left hand side menu, select Managed devices



- 2) In the top right of the screen, select Advanced



3) Select Submit to access Advanced view

The screenshot shows the 'Managed device users' interface. A modal dialog titled 'Advanced view' is open, with the following text: 'In larger environments, the advanced view might take longer to display than the default view.' Below the text are two buttons: 'Cancel' and 'Submit'. The 'Submit' button is highlighted with a yellow circle. At the bottom of the dialog, there is a checkbox labeled 'Do not show this again' which is currently unchecked. The background shows a table of users with columns for 'Display name', 'Email address', 'Model', 'OS', 'Home carrier', 'Last contact', and 'BlackBerry Dynamics'. The table contains several rows of user data, including names like CHOUINARD, BERNARD, DAVIS, BRADFORD, DND, EMDM, Houle, DENIS, LOPEZ, PIERRE, MAYOTTE, ANDREW, and Predescu.

- 4) At the top right of the user/device list, select the (+) sign and then select the information you want included in the report

The screenshot shows the 'Managed device users' interface. On the left is a sidebar with 'Users' and 'Managed devices' sections. The main area contains a table of users and a search bar. A yellow box highlights the 'Export' button (a right-pointing arrow) at the top right of the user list. A modal window is open, showing various filters and options for user and device management.

<input type="checkbox"/>	Display name	Model	OS	Phone number	Home carrier	Ownership	Last contact	Email address	<input type="checkbox"/>
<input type="checkbox"/>	Admin-Belcourt, Eryck(DN...								<input type="checkbox"/>
<input type="checkbox"/>	Admin-Gagnon, Ian (DND/MDN)								<input type="checkbox"/>
<input type="checkbox"/>	Admin-Mayotte, Andrew (DND/MDN)								<input type="checkbox"/>
<input type="checkbox"/>	Admin-Stone, Jarrod (DND/MDN)								<input type="checkbox"/>
<input type="checkbox"/>	AGGARW... AMIT (DND/MDN)	Galaxy S8+							<input type="checkbox"/>
<input type="checkbox"/>	Barry, Annie MJA (SSC/SPC)								<input type="checkbox"/>
<input type="checkbox"/>	CHOUIN... BERNARD (DND/MDN)	Galaxy S7							<input type="checkbox"/>
<input type="checkbox"/>	DAVIS, BRADFO... (DND/MDN)	Galaxy S7							<input type="checkbox"/>
<input type="checkbox"/>	DND, EMDM (DND/MDN)							EMDM.D...	<input type="checkbox"/>
<input type="checkbox"/>	Houle, DENIS (DND/MDN)							DENIS.H...	<input type="checkbox"/>
<input type="checkbox"/>	LOPEZ, PIERRE (DND/MDN)	Galaxy Note 8		16133258...		Work	2018-06-05 07:25:35 -04:00	PIERRE.L...	<input type="checkbox"/>

- 5) Select all the users by clicking on the top left box. Once all users are selected, click on the Export button at the top of the list (right pointing arrow)

EMDM-GAME - LP 2

Users

All users

Managed devices

Multiple selection on

Filters

- OS
- Brand name
- Model
- OS version
- Home carrier
- Current carrier
- Roaming
- Group
- User IT policy
- Device IT policy
- Activation type
- Device status
- Device SRP
- Client version
- Security patch level
- Ownership
- Company directory
- OS compromised
- Compliance violation
- Out of compliance
- Supervised device

Managed device users

Default Advanced User search

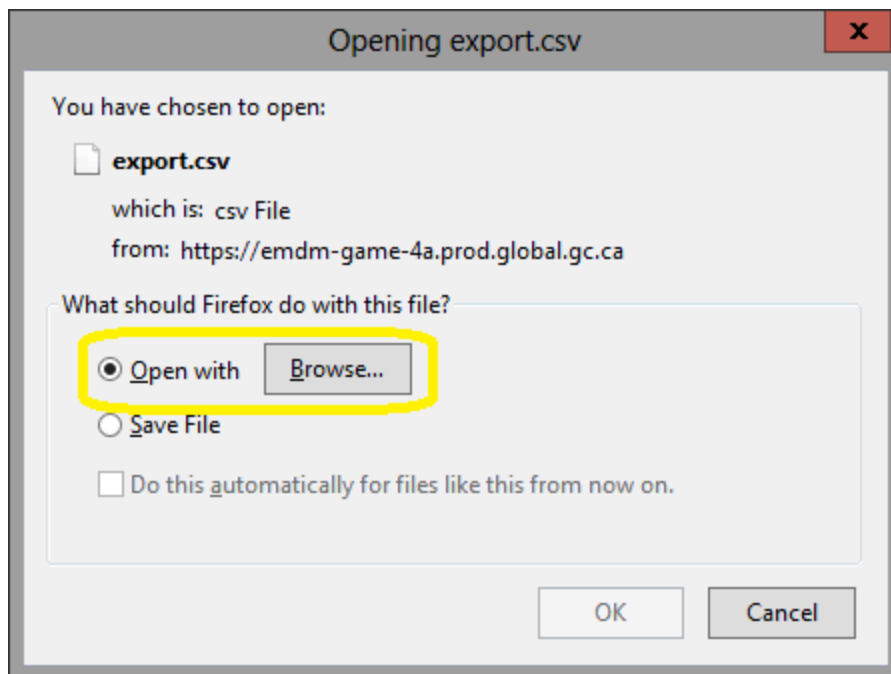
Search

15 rows selected 1 - 12 of 15

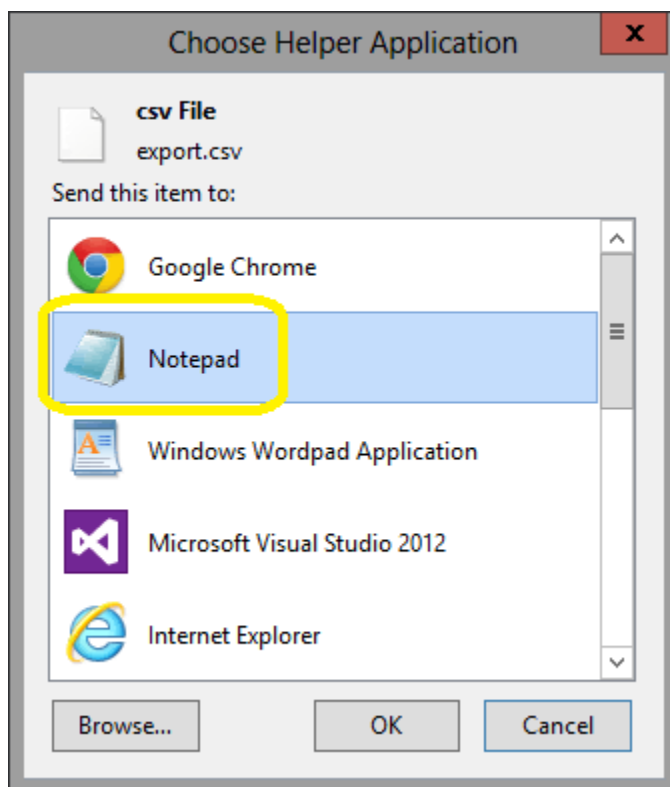
No filters selected

<input checked="" type="checkbox"/>	Display name	Model	OS	Phone number	Home carrier	Ownership	Last contact	Username
<input checked="" type="checkbox"/>	Admin-Belcourt, Eryck(DN...							admin.ery...
<input checked="" type="checkbox"/>	Admin-Gagnon, Ian (DND/MDN)							admin.ian...
<input checked="" type="checkbox"/>	Admin-Mayotte, Andrew (DND/MDN)							admin.an...
<input checked="" type="checkbox"/>	Admin-Stone, Jarrod (DND/MDN)							admin.jarr...
<input checked="" type="checkbox"/>	AGGARW... AMIT (DND/MDN)	Galaxy S8+		16134155...		Work	2018-06-05 06:27:55 -04:00	Aggarwal.A
<input checked="" type="checkbox"/>	Barry, Annie MJJA (SSC/SFC)							Barry.MJJA
<input checked="" type="checkbox"/>	CHOUIN... BERNARD (DND/MDN)	Galaxy S7		16132943...		Work	2018-06-05 05:34:40 -04:00	Chouinar...
<input checked="" type="checkbox"/>	DAVIS, BRADFO... (DND/MDN)	Galaxy S7		16132944...		Work	2018-06-02 23:57:35 -04:00	Davis.B
<input checked="" type="checkbox"/>	DND, EMDM (DND/MDN)							EMDM.DND
<input checked="" type="checkbox"/>	Houle, DENIS (DND/MDN)							Houle.DR
<input checked="" type="checkbox"/>	LOPEZ, PIERRE (DND/MDN)	Galaxy Note 8		16133258...		Work	2018-06-05 07:25:35 -04:00	Lopez.P2

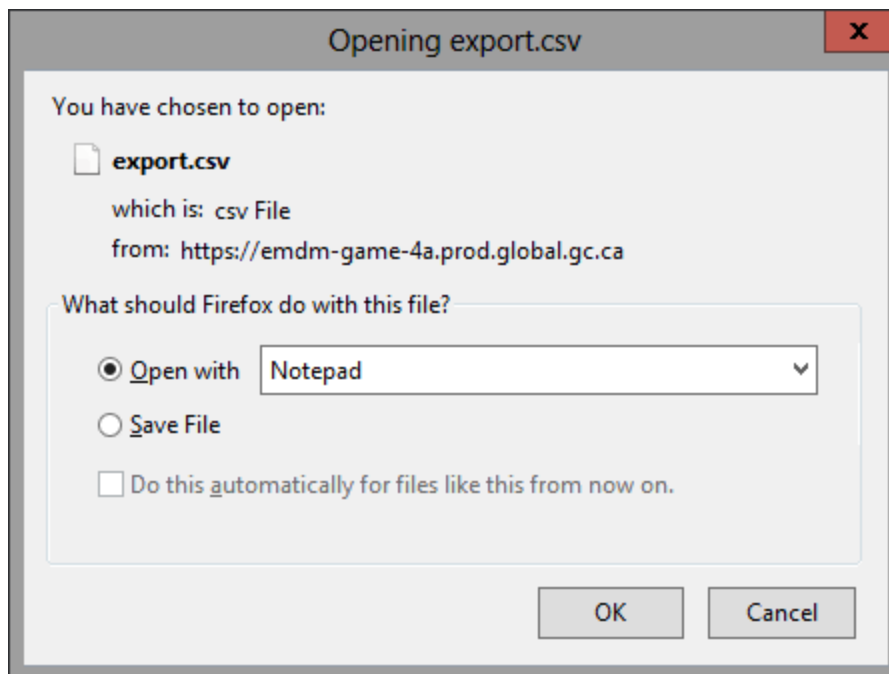
- 6) The user list will be exported to a .csv file. However, this .csv file is contained within the SSC Citrix environment. Here is how you bring the data over to your DWAN PC:
 - a. In the Opening export.csv window, select Open with... and click the Browse... button



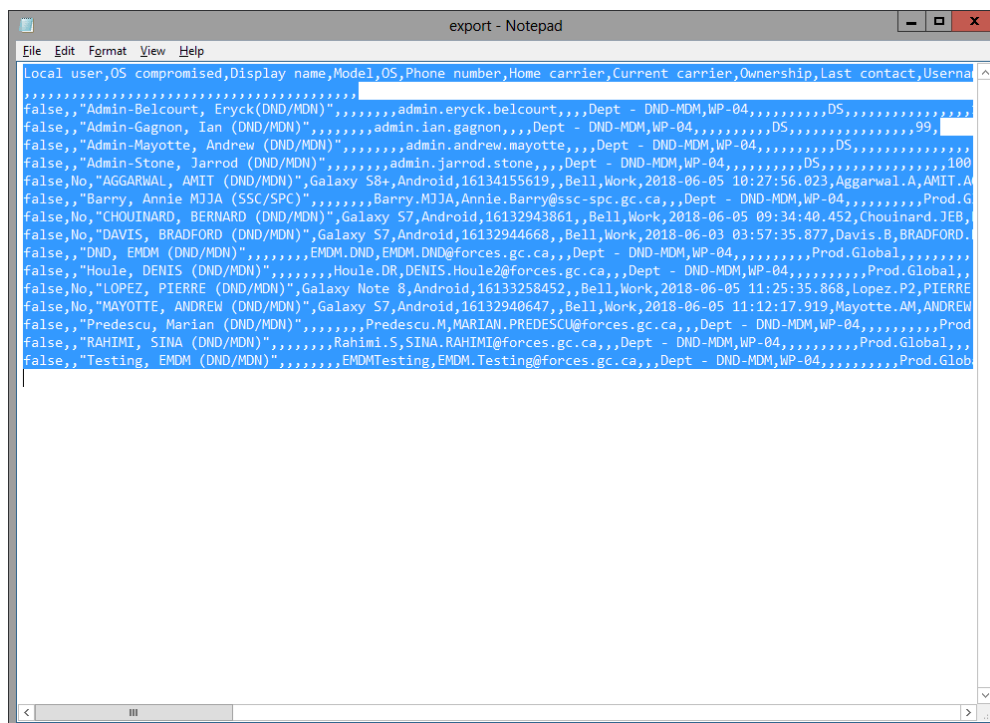
b. Select Notepad, then click OK



c. Click OK



- d. With the extract now open in Notepad (within the SSC EDC Citrix environment), select all the data (Ctrl-A) and copy it (Ctrl-C)



- e. On your DWAN PC, open Notepad (Start -> search for Notepad -> select Notepad)
- f. Paste the data into the new Notepad window.
- g. Save the Notepad as a .csv file

- h. You can then import that .csv file into Excel using Excel's Data Import feature. Excel's Data Import feature will ensure the data is properly imported into Excel. Do not open the CSV directly into Excel as some of the data (i.e. IMEI numbers) will become corrupt. Always use the Excel Data Import feature.

5.2 Modify a user's EMDM account information

The EMDM service is synchronized with the DWAN Active Directory. As such, if a user requires a username and/or email address modification, the change must first occur in the DWAN Active Directory. The synchronization delay is 24 to 48 hours.