

Déverrouillage des périphériques Qualcomm EDL

Table of Contents

- Déverrouillage des périphériques Qualcomm EDL
 - Câble EDL
 - JTAG / Test Pin
 - ADB
- Déverrouillage avec ADB
 - Préparation de Windows
 - Installation de fastboot et adb
 - Installation des drivers ADB
 - Installer TWRP & ROOT:
 - Activer le mode développeur/débogage USB
 - Fastboot et déverrouillage OEM:
 - Installer la récupération TWRP:
 - Réinitialisation d'usine/tout essuyer:
 - Activer le mode développeur/débogage USB
- Mettre à niveau la ROM
 - Sauvegarde QCN (IMEI)
 - Mettre le téléphone en mode EDL
 - Premier téléchargement
 - Deuxième téléchargement
 - Redémarrage du téléphone

L'utilisation du mode **EDL** sont l'une des nombreuses façons de contourner les codes d'accès et d'accéder physiquement à de nombreux appareils Android avec des chipsets basés sur Qualcomm. Le mode de téléchargement d'urgence (**EDL**) est une fonctionnalité Qualcomm qui peut vous permettre de récupérer les données d'un appareil et d'effectuer des tâches telles que le débranchement ou le flashage de l'appareil. Sur les appareils pris en charge, on peut utiliser **EDL** pour extraire une image complète.

La méthode pour mettre un appareil en mode **EDL** peut varier en fonction du modèle. Il existe trois façons de mettre un appareil en mode **EDL** et aucune méthode ne fonctionne sur tous les téléphones. Sur certains appareils, on peut utiliser un câble spécial, tandis que d'autres peuvent obliger à démonter l'appareil. Enfin, si l'appareil est déverrouillé, on peut utiliser **ADB** ou **fastboot** pour redémarrer le téléphone en mode **EDL**.

Câble EDL

L'utilisation d'un câble spécial pour mettre le téléphone en mode EDL est probablement la méthode la

plus simple. Le câble est conçu avec un interrupteur à bascule pour court-circuiter la broche de données correcte et forcer le téléphone en mode EDL.

Pour passer en mode EDL:

1. brancher simplement le câble sur l'ordinateur,
2. maintenir le bouton bascule enfoncé et le brancher au téléphone.
3. Après avoir relâché le bouton bascule, le téléphone doit démarrer en mode EDL.

Pour s'assurer que le téléphone est en mode EDL, rechercher dans le Gestionnaire de périphériques Windows tous les périphériques Qualcomm répertoriés sous Ports COM, ce qui devrait confirmer que l'appareil est en mode EDL et prêt à fonctionner. Une fois que le téléphone est en mode EDL.

JTAG / Test Pin

Si la méthode du câble ne fonctionne pas, une autre méthode utile consiste à court-circuiter la broche CMD sur les ports de test pour diriger le périphérique vers le démarrage en mode EDL. Tous les appareils n'ont pas de ports de test JTAG, mais s'ils l'ont, cette méthode fonctionne très bien.

Pour passer en mode EDL:

1. Ouvrir l'appareil et trouver les ports de test nécessaires
2. les court-circuiter avec une paire de pincettes ou autre chose métallique tout en insérant le câble USB dans l'appareil.

Cette méthode fonctionne assez bien sur de nombreux appareils sensibles à l'exploit EDL, mais comme mentionné précédemment, ne fonctionnera pas sur tous les appareils.

ADB

Enfin, la dernière méthode disponible est limitée aux appareils sur lesquels l'accès ADB est activé. Cela signifie que le téléphone doit être allumé, déverrouillé et que le débogage USB doit être activé pour que l'on puisse envoyer et recevoir des commandes ADB vers le téléphone. Ce ne sera pas toujours le cas si on a affaire à un téléphone verrouillé, mais la méthode fonctionne assez bien dans les scénarios où le téléphone est déjà déverrouillé.

Une fois que l'on a accès à ADB, il suffit d'envoyer simplement la commande `adb reboot edl` sur la ligne de commande et le téléphone redémarrera en mode EDL.

Déverrouillage avec ADB

Android Debug Bridge (adb) est un outil de ligne de commande polyvalent qui permet de communiquer avec un appareil. La commande **adb** facilite une variété d'actions sur l'appareil, telles que l'installation et le débogage d'applications, et elle donne accès à un shell Unix que l'on peut utiliser pour exécuter une variété de commandes sur un appareil. C'est un programme client-serveur qui comprend trois composants:

- Un client, qui envoie des commandes. Le client s'exécute sur la machine de développement. On peut appeler un client à partir d'un terminal de ligne de commande en émettant une commande **adb**.
- Un démon (adbd), qui exécute des commandes sur un périphérique. Le démon s'exécute en tant que processus d'arrière-plan sur chaque périphérique.
- Un serveur, qui gère la communication entre le client et le démon. Le serveur s'exécute en tant que processus d'arrière-plan sur la machine de développement.

adb est inclus dans le package Android SDK Platform-Tools. On peut télécharger le package Android SDK Platform-Tools autonome.

Préparation de Windows

Installation de fastboot et adb

Les binaires **ADB/fastboot** téléchargés depuis le site [Android SDK Platform Tools](#) doivent être placés dans le PATH système

Installation des drivers ADB

Il existe 2 pilotes USB disponibles pour les périphériques, le pilote **Qualcomm** et le pilote **ADB**:

- Le Pilote Qualcomm: est compatible avec l'outil Qualcomm Flash et l'outil Qualcomm IMEI et permet d'installer le micrologiciel (ROM) sur l'appareil.
- Le Pilote ADB: est utilisé pour connecter un mobile (sous Android) à l'ordinateur et transférer des données entre le mobile et l'ordinateur.

Pour installer manuellement un pilote USB (le périphérique ne doit pas être attaché à l'ordinateur):

- Télécharger et extraire le pilote USB sur l'ordinateur.
- Ouvrir le Gestionnaire de périphériques (devmgmt.msc) et accéder à **[Nom de l'ordinateur]>Action>Ajouter du matériel hérité**.
- Cliquer sur le bouton Suivant.
- Cocher la case **Installer un matériel que je sélectionne manuellement dans une liste** et cliquer sur le bouton Suivant.
- Encore une fois, cliquer sur le bouton Suivant.
- Cliquer sur **Disque fourni> Parcourir>** pour Rechercher le fichier **.inf** (trouvé dans le dossier du pilote extrait) et cliquer sur le bouton Ouvrir.
- Cliquer sur le bouton Terminer pour terminer l'installation.
- Déconnecter et reconnecter le téléphone sur un port usb¹⁾.

Installer TWRP & ROOT:

Il faut rooter le téléphone pour sauvegarder QCN.

Activer le mode développeur/débogage USB

- Aller dans **Paramètres, À propos du téléphone** → appuyer sur le numéro de build 7 fois pour activer le mode développeur
- Aller dans **Paramètres → Paramètres avancés → Options du développeur**
 - Activer le débogage USB
 - Activer le déverrouillage OEM

Fastboot et déverrouillage OEM:

- Éteindre, déconnecter de l'USB
- Appuyer sur le bouton de réduction du volume + d'alimentation pendant 5 s
- Ouvrir Windows → CMD et exécuter

```
fastboot flashing unlock  
fastboot oem unlock
```

Installer la récupération TWRP:

- Maintenir **power** pour arrêter, attendre que le symbole de chargement de la batterie disparaisse le cas échéant
- Maintenir **power** et le **vol** - pendant 10 s

```
fastboot flash recovery rec.img  
fastboot flash recoverybp rec.img  
fastboot boot rec.img
```



Avant de redémarrer, il faut s'assurer que l'option **Agressive Stock Recovery** dans le menu system soit coché afin qu'à l'avenir, appuyer sur **Volume +** et **power** amène à la récupération TWRP.

Réinitialisation d'usine/tout essayer:

- **Option n° 1:** réinitialisation d'usine Android
 - Accéder aux paramètres Android et effectuer une réinitialisation d'usine
- **Option n° 2:** utiliser TWRP pour essayer
 - Utilisateur TWRP pour effacer le stockage interne et les données (mode avancé)
 - Ignorer tous les échecs (échecs de montage, etc.)
 - TWRP Redémarre le système

Activer le mode développeur/débogage USB

- Aller dans **Paramètres, À propos du téléphone** → appuyer sur le numéro de build 7 fois pour activer le mode développeur
- Aller dans **Paramètres → Paramètres avancés → Options du développeur**
 - Activer le débogage USB
 - Activer le déverrouillage OEM
- Connecter le Yota3 à Windows
- Attendre que les pilotes ADB soient installés le cas échéant
- Ouvrir Windows CMD et exécuter

adb devices

- Déverrouiller le Yota3 et autoriser/accepter la demande de débogage USB
- Installer MagiskManager via l'installation ADB dans Windows CMD, exécuter `adb install MagiskManager-v7.0.0.apk`
- Installer Magisk-v20.3 depuis TWRP Recover avec `adb sideload`
 - Éteindre Yota3, déconnecter l'USB
 - Maintenir le bouton d'alimentation + Volume Up to TWRP Recovery
 - Une fois TWRP chargé, Aller dans **Paramètres avancés>Transfert** via ADB et faire glisser pour débiter le transfert.
 - Attendre que les pilotes soient installés sur le Windows ²⁾
 - Dans windows CMD exécuter `adb sideload Magisk-v20.3.zip`
 - Redémarrer le système. Après le redémarrage de Yota3, accéder à l'application **Magisk Manager** pour vérifier si **Magisk** est installé

Mettre à niveau la ROM

Yota3 + a une amélioration significative de l'expérience utilisateur par rapport à Yota3 (version chinoise), prend en charge toutes les applications de l'écran arrière (écran E-ink), exécutant Android 8.1.0 qui est plus sûr.

Mises en garde

- Tout dans le téléphone sera effacé (perdu)
- Il y a une chance que le téléphone soit endommagé (brique)

Sauvegarde QCN (IMEI)

Fondamentalement, le fichier QCN intégré dans tous les derniers téléphones mobiles Android est le fichier principal et sensible du réseau, caché dans le noyau le plus profond du système de fichiers de la mémoire interne du téléphone mobile (dans le dossier `efs`, où toutes les informations de `imei`³⁾

Tous les téléphones basés sur Qualcomm ont pris en charge le fichier QCN.

Si le dossier `efs` est effacé, le téléphone ne verra plus le réseau 3g/2g/LTE.

Il faut donc sauvegarder le fichier QCN (IMEI) en cas de perte, sinon le téléphone ne pourra plus se connecter à la 4G. Comme suit.

- Dans le Windows
 - Installer **QPST_2.7.474China**
 - Installer **QDLoader HS-USB Driver_64bit_Setup**
 - Redémarrer Windows comme demandé après l'installation du pilote
- Activer les diagnostics Qualcomm
 - Après le redémarrage de Windows, connecter le Yota3 rooté à Windows 10 via USB
 - dans Windows CMD exécuter,

```
adb shell
su
```

- Autoriser SuperSU
 - Accéder à Yota3 pour l'autoriser dans SuperSU (déjà installé dans Magisk)
 - Après avoir autorisé SU, dans Windows CMD exécuter

```
setprop sys.usb.config diag
```

- Attendre que les pilotes **Qualcomm USB Diagnostics** soient installés sur le Windows⁴⁾
- Cliquer avec le bouton droit sur l'icône **Démarrer** de Windows, ouvrir le Gestionnaire de périphériques
- Vérifier dans les ports (COM et LPT) que **Qualcomm HS-USB Diagnostics 900E (COM *)** est affiché
- Accéder à l'icône **Démarrer de Windows → QPST → Configuration QPST**, on peut voir qu'un nouveau port est ajouté, affiché comme suit:

```
Port: COM3, Phone: MSM8953(*****)
```

- Si rien ne s'affiche, cela signifie que le Yota3 n'est pas enraciné correctement ou que `setprop sys.usb.config diag` a échoué ou que la connexion USB est instable
 - Il faut abandonner la mise à niveau si on ne peut pas sauvegarder NV, ou si on risque de briser le Yota3.
- Cliquer sur **Menu → Start Clients → Software Download**
- Aller dans l'onglet **Backup**; Sélectionner un emplacement dans xQCN File:, cliquer sur **Start**.
- Attendre que la barre d'état du fichier soit à 100%. Peut prendre quelques minutes. Une fois terminé, quitter.

Mettre le téléphone en mode EDL

Le mode **EDL** ou **E**mergency **D**ownload est un mode de démarrage spécial dans les appareils Android Qualcomm qui permet aux OEM de forcer le flash des fichiers du micrologiciel. Ce mode de fonctionnement spécial est également couramment utilisé par les utilisateurs expérimentés pour débrider leurs appareils.

- Activer et désactiver le débogage USB
 - Accéder aux **paramètres → Paramètres avancés → Options pour les développeurs**, désactiver, puis réactiver le déverrouillage OEM et le débogage USB
- Mettre le Yota 3 en mode 9008 (mode edl)
 - **Option n° 1**: utiliser la commande adb : `adb reboot edl`

- **Option n° 2:** Éteindre et déconnecter de l'USB puis appuyer sur les boutons **Vol + + Vol**
- Cliquer sur **Load XML** et sélectionner uniquement les fichiers **Rawprogram0.xml** et **patch0.xml**
- Connecter le câble USB ⁵⁾
- Cliquer à nouveau sur le bouton **Download**
- Attendre que Windows ait terminé l'installation des pilotes.

Premier téléchargement

Le téléphone n'est pas reconnu pendant le téléchargement en tant que périphérique USB inconnu/non reconnu, procéder comme suit:

- Utiliser l'adaptateur secteur pour le charger pendant plus de 2 heures.
- Décompresser la rom téléchargée new9008-0112.zip
- Après 2 heures, déconnecter le téléphone de l'USB du PC
- Fermer la configuration QPST (serveur QPST)
- * Appuyer ensuite sur Vol + + Vol - + Power et maintenir pendant 20 secondes (on n'entendra aucune vibration)
- Exécuter Windows **Démarrer → QPST → QFil.exe**, aller dans **Configuration → Configuration**
-  **Firehose**
- Connecter le téléphone à l'USB
- Cocher **Reset After Download** (Réinitialiser après le téléchargement)
- Il devrait afficher Qualcomm HS-USB QLoader 9008 (COM *) dans le Gestionnaire de périphériques. Si ce n'est pas le cas, essayer de maintenir les 3 boutons enfoncés pendant que l'USB est connecté pendant 20 secondes
- Sélectionner **Flat build** dans **Select Build type**
- Cliquer sur le bouton **Browse ...** à droite pour sélectionner le programmeur
- Sélectionner le fichier **mbn** de la rom dans le dossier
- Une fois le mode 9008 activé, redémarrer à partir de l'étape Cliquer sur Charger XML...
- Cliquer sur **Charger XML...** et sélectionner les deux fichiers xml (**rawprogram0.xml** et **rawprogram0_BLANK.xml**), puis **open** après cela
- Et puis cliquer sur le bouton **Download**
- Attendre 2 minutes jusqu'à voir **Download Success** et **Download Finished**

Redémarrage du téléphone

Après le téléchargement, le téléphone redémarrera. et affichera un écran «Décryptage échoué». Maintenant cliquer deux fois sur le bouton **Réinitialiser le téléphone**.

Attendre que le téléphone redémarre plusieurs fois. Il ira à l'écran de cryptage.

Enfin, le Yota3 + sera démarré.

1) 2) 4)

Si windows ne détecte pas corectement le pilote:

- ouvrir le Gestionnaire de périphériques (devmgmt.msc)
- accéder au périphérique ajouter automatiquement
- cliquer sur **Mettre à jour le pilote**
- Cliquer rechercher un pilote sur mon ordinateur
- Cliquer sur Choisir parmi une liste des périphériques sur mon ordinateur
- Cliquer sur Android device
- Choisir Android ADB interface dans la liste des modèles
- cliquer sur suivant
- Cliquer sur le bouton Terminer pour terminer l'installation

³⁾ IMEI (International **M**obile **E**quipment **I**ntity) est un numéro unique permettant d'identifier un appareil sur un réseau mobile. Il comporte 15 chiffres et est attribué à chaque téléphone GSM.

⁵⁾

Un câble deep flash est un câble spécial pour relier un appareil mobile à un PC. Normalement, lorsque l'appareil est à l'état OFF, le PC le reconnaîtra comme un appareil rechargeable et l'appareil sera donc chargé avec un peu d'alimentation du PC. Ce câble Deep Flash rendra l'appareil reconnu comme appareil flashable à la place

From:

<http://www.ouarte.garden/> - **dwndoc**

Permanent link:

<http://www.ouarte.garden/doku.php?id=prive:yota3-firmware>

Last update: **2025/02/19 10:59**

