

MISE EN SERVICE

Équipements numériques — Dell Pro Slim QCS1250

Pôle Sud — Direction des Systèmes d'Information — Ville de Toulon / TPM

Champ	Valeur
Auteur	Zoughlami Mohamed
Structure	Pôle Sud — Ville de Toulon / TPM Métropole
Responsable	Sophie Vaccaro
Contexte	Mission en entreprise — BTS SIO SISR
Matériel	Dell Pro Slim QCS1250 (Service Tag : DZGF7G4)
Système	Windows 11 Professionnel — Version 25H2
Domaine	si.tpmed.org

1. Contexte de la mission

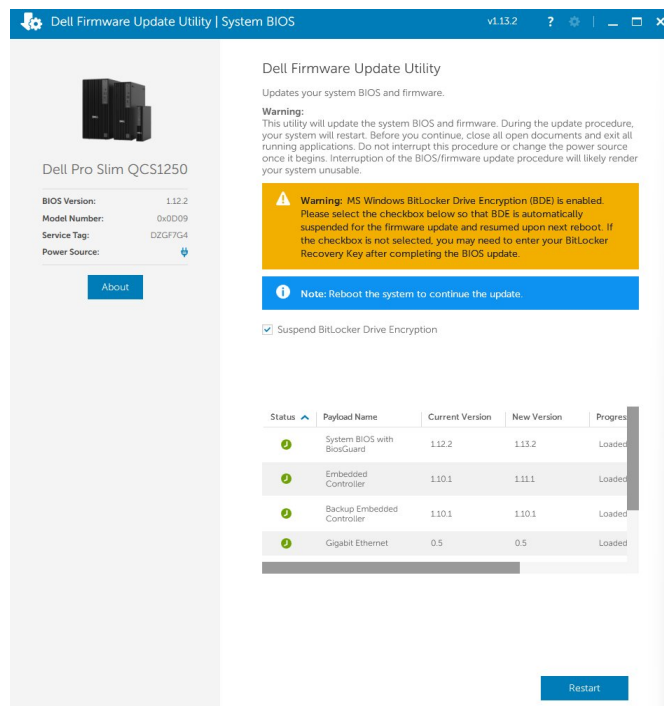
Dans le cadre de mon alternance à Pôle Sud (Direction des Systèmes d'Information de la Ville de Toulon et de TPM Métropole), j'ai été chargé de la mise en service de nouveaux équipements numériques. Cette procédure décrit les étapes de vérification et de validation à effectuer après la masterisation d'un poste, avant sa remise à l'utilisateur final.

La mise en service garantit que le poste est opérationnel, sécurisé, à jour et correctement intégré dans l'infrastructure informatique de la collectivité.

Étape	Outil utilisé	Objectif
1 — Vérification Windows	Paramètres système	Confirmer la version et la licence
2 — Mise à jour BIOS/firmware	Dell Command Update / Firmware Utility	Mettre à jour les composants Dell
3 — Vérification logiciels	Explorateur Windows	Contrôler les applications installées
4 — Vérification navigateur	Google Chrome	Confirmer la version à jour
5 — Test prise en main	BMC Software	Valider la télémaintenance helpdesk

2. Vérification de la version Windows 11

Après la masterisation, vérifier que Windows 11 est correctement installé et sous licence. Aller dans **Paramètres** → **Système** → **À propos** ou faire **Win + Pause**.



Capture — Windows 11 Professionnel — Version 25H2 (build 26200.8117) — licencié sous AdminTemp / IT

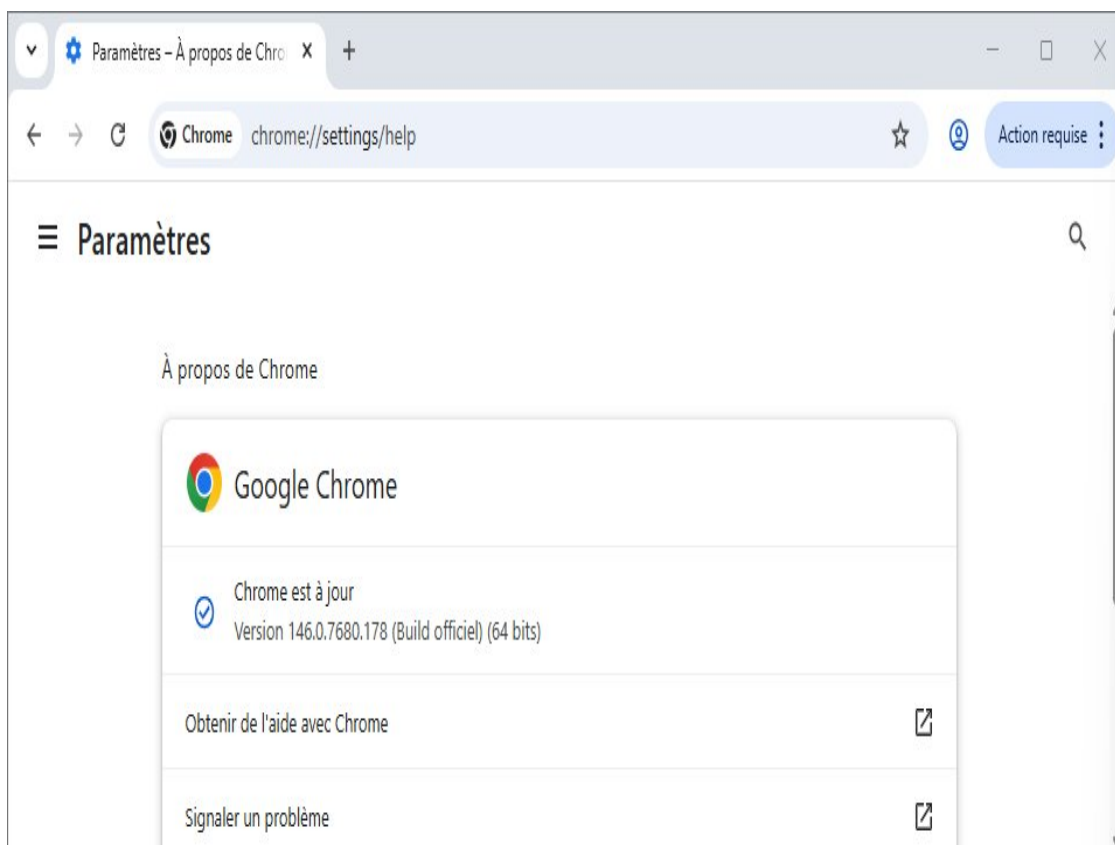
La version déployée est **Windows 11 Professionnel — Version 25H2** (build 26200.8117). La licence est attribuée à l'organisation **IT** via le compte **AdminTemp**, conformément aux licences Microsoft de la collectivité.

■ INFO

Windows 11 25H2 est la version standard déployée en production sur les postes Pôle Sud / TPM. Vérifier que le numéro de build correspond bien à la version attendue par le service informatique.

3. Mise à jour BIOS et firmwares Dell

Ouvrir **Dell Command | Update** (version 5.6.0) pour rechercher et installer les mises à jour du BIOS et des firmwares disponibles pour le poste Dell Pro Slim QCS1250.



Capture — Dell Command Update v5.6.0 — Dell Pro Slim QCS1250 (DZGF7G4) — Échec mise à jour BIOS : mot de passe BIOS non configuré

Dans cet exemple, Dell Command Update signale un **échec de la mise à jour du BIOS** car le mot de passe BIOS n'est pas encore configuré. Pour résoudre ce problème : accéder au BIOS (F2) → Security → Passwords → Admin Password, définir un mot de passe, sauvegarder, puis relancer Dell Command Update.

■ ATTENTION

Ne jamais ignorer une mise à jour BIOS disponible. Le BIOS embarque des correctifs de sécurité critiques (BiosGuard, Embedded Controller). S'assurer que le poste est branché sur secteur avant toute mise à jour firmware.

Mise à jour via Dell Firmware Update Utility

En alternative, utiliser le **Dell Firmware Update Utility** pour mettre à jour le BIOS et les firmwares. Cet outil détecte automatiquement les composants à mettre à jour.



Capture — Dell Firmware Update Utility v1.13.2 — BIOS 1.12.2 → 1.13.2, Embedded Controller 1.10.1 → 1.11.1 — Suspend BitLocker coché

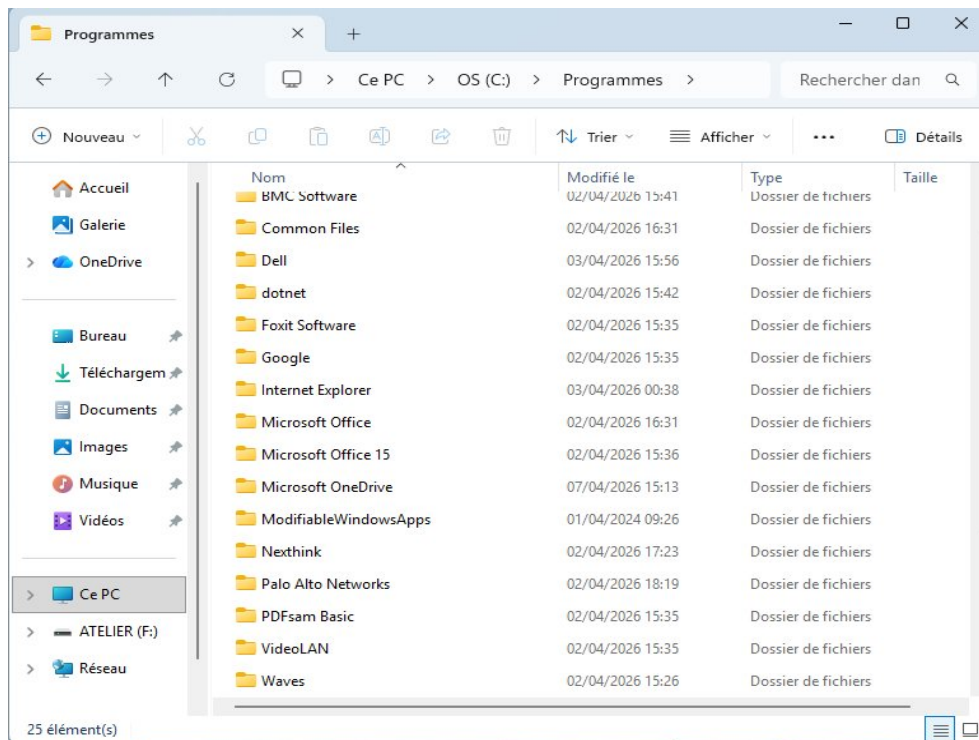
Les mises à jour disponibles pour ce poste sont :

- **System BIOS with BiosGuard** : 1.12.2 → 1.13.2
- **Embedded Controller** : 1.10.1 → 1.11.1
- **Backup Embedded Controller** : 1.10.1 → 1.10.1 (déjà à jour)
- **Gigabit Ethernet** : 0.5 → 0.5 (déjà à jour)

Cocher **Suspend BitLocker Drive Encryption** pour éviter tout problème de déchiffrement après redémarrage, puis cliquer sur **Restart**.

4. Vérification des logiciels installés

Ouvrir l'explorateur Windows et naviguer vers **C:\Programmes** pour vérifier que tous les logiciels standards ont bien été installés par le script de déploiement.



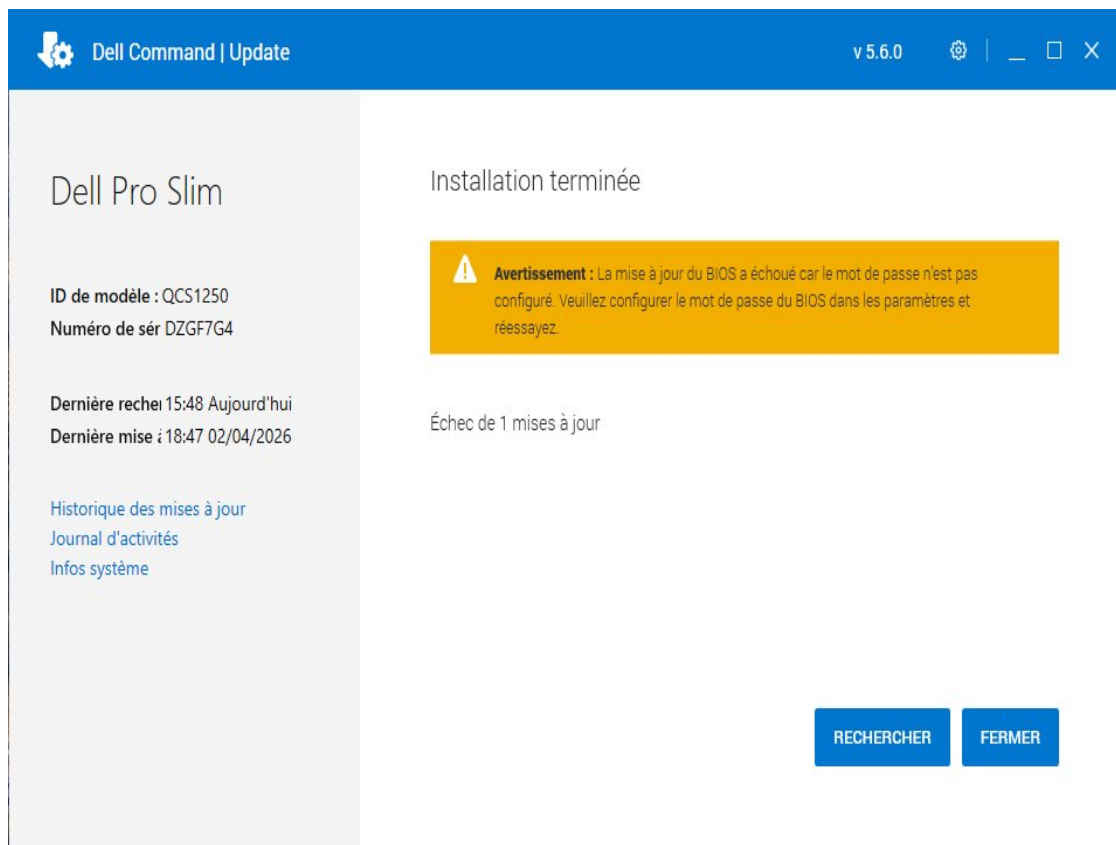
Capture — C:\Programmes : 25 dossiers — BMC Software, Foxit, Google, Microsoft Office, Nexthink, Palo Alto Networks, PDFsam, VideoLAN, Waves...

Les 25 dossiers présents confirment que le déploiement des logiciels s'est bien déroulé. Vérifier en particulier :

- **Microsoft Office** — suite bureautique de la collectivité
- **Palo Alto Networks** (Cortex XDR) — antivirus et EDR
- **Nexthink** — supervision et télémétrie du poste
- **BMC Software** — gestion de parc et prise en main à distance
- **Google Chrome** — navigateur web standard
- **Foxit Software** — lecteur PDF
- **VideoLAN VLC** — lecteur multimédia
- **PDFsam Basic** — manipulation de fichiers PDF

5. Vérification de Google Chrome

Ouvrir Google Chrome et aller dans **Paramètres** → **À propos de Chrome** (raccourci : taper **chrome://settings/help** dans la barre d'adresse) pour vérifier que le navigateur est bien à jour.



Capture — Google Chrome — Version 146.0.7680.178 (Build officiel) 64 bits — Chrome est à jour

Chrome version **146.0.7680.178** est installé et à jour. Le navigateur se met à jour automatiquement via les GPO du domaine.

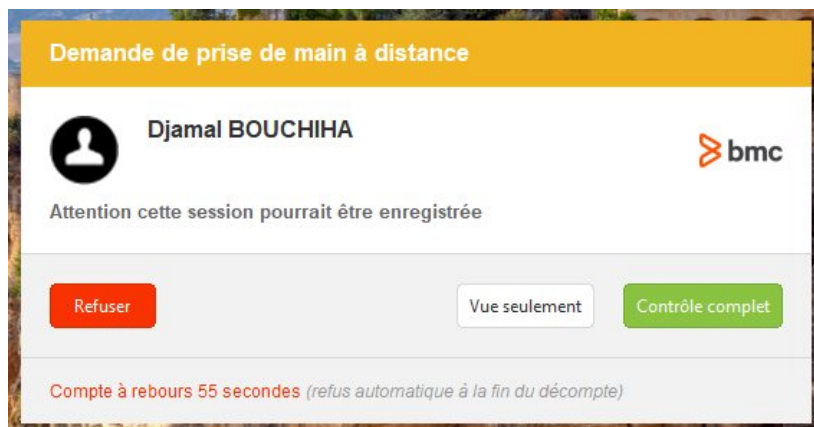
6. Test de prise en main à distance — BMC

La solution **BMC Software** (Helix Client Management) est utilisée par le service informatique pour la télémaintenance des postes du parc. Une fois l'agent BMC installé et le poste joint au domaine, tester la prise en main à distance depuis la console helpdesk.

Lors d'une demande de connexion, une notification s'affiche sur le poste avec trois options :

- **Refuser** — l'utilisateur peut refuser la connexion entrante
- **Vue seulement** — le technicien voit l'écran sans pouvoir interagir
- **Contrôle complet** — le technicien prend le contrôle total du poste

Un compte à rebours de **55 secondes** s'affiche. Si aucune action n'est effectuée, la session est automatiquement refusée.



Capture — Demande de prise de main à distance BMC par Djamal BOUCHIHA — Refuser / Vue seulement / Contrôle complet — 55 secondes

■ INFO

La prise en main BMC permet au helpdesk d'assister les utilisateurs à distance sans déplacement physique. L'utilisateur est toujours notifié et peut refuser la session. La session peut être enregistrée.

7. Checklist de mise en service

Avant de remettre le poste à l'utilisateur, valider chaque point de la checklist :

Vérification	Statut attendu
Windows 11 Pro version 25H2 installé	✓ Confirmé dans Paramètres → À propos
Poste joint au domaine si.tpmed.org	✓ Paramètres → Système → Domaine
Nom du poste conforme (PCW-TOU-XXXXXX)	✓ Paramètres → Système → Nom du PC
Mises à jour Windows appliquées	✓ Windows Update — aucune mise à jour en attente
BIOS/Firmware Dell à jour	✓ Dell Command Update ou Firmware Utility
Logiciels standards présents dans C:\Programmes	✓ 25 dossiers vérifiés
Google Chrome à jour	✓ Version vérifiée via chrome://settings/help
Agent Cortex (Palo Alto) actif	✓ Visible dans les services Windows
Agent Nexthink actif	✓ Visible dans les services Windows
Agent BMC actif — prise en main testée	✓ Test validé depuis la console helpdesk
Logs de déploiement exportés sur srv-mdt	✓ \\srv-mdt.si.tpmed.org\Partage\Logos

✓ RÉSULTAT

Le poste Dell Pro Slim QCS1250 est entièrement vérifié, à jour et opérationnel. Il peut être remis à l'utilisateur final avec son profil Active Directory sur le domaine si.tpmed.org.