LOSTE TRADI-FRANCE

Renforcement de l'Authentificationvia Windows Hello for Business

Documentation configuration GPO — Authentification forte

Rédacteur	Paul Barrault-Gautier
Entreprise	Loste Tradi-France
Poste	Administrateur Réseau & Systèmes
Date	Avril 2026
Version	1.0
Classification	Usage interne — Confidentiel

1. Introduction

Ce document décrit en détail les stratégies de groupe (GPO) configurées pour le déploiement et le renforcement de l'authentification forte via Windows Hello for Business chez Loste Tradi-France. Il couvre la GPO principale WHfB, les politiques de PIN, les restrictions d'accès complémentaires et les paramètres de sécurité associés.

2. Structure des GPO déployées

Nom de la GPO	OU liée	Rôle
WHfB-Enable-Policy	OU=Computers,DC=loste,DC=local	Activation et configuration WHfB
WHfB-PIN-Policy	OU=Computers,DC=loste,DC=local	Complexité et durée de vie du PIN
WHfB-Biometric-Policy	OU=Computers,DC=loste,DC=local	Gestion de la biométrie
WHfB-PKI-Autoenroll	OU=Domain Controllers	Inscription auto certificats DC
Password-Lockout-Policy	Default Domain Policy	Verrouillage compte (complément)

3. GPO « WHfB-Enable-Policy »

3.1 Paramètres Windows Hello for Business

Chemin : Configuration ordinateur > Modèles d'administration > Composants Windows > Windows Hello for Business

Paramètre	Valeur	Justification
Utiliser Windows Hello for Business	**Activé**	Activation obligatoire du WHfB
Utiliser un périphérique TPM	**Activé**	Clé privée stockée dans le TPM uniquement
Utiliser des certificats pour l'authentification en local	**Activé**	Nécessaire pour le mode hybride AD/Azure AD
Ne pas démarrer l'approvisionnement WHfB après connexion	Désactivé	Lancer l'enrôlement dès la première connexion
Utiliser Windows Hello for Business comme méthode d'authentification principale	**Activé**	Priorité WHfB sur le mot de passe

3.2 Paramètres complémentaires — Credential Guard

Chemin : Configuration ordinateur > Modèles d'administration > Système > Device Guard

Paramètre	Valeur	Justification
Activer la sécurité basée sur la virtualisation	**Activé**	Isole les credentials dans un enclave sécurisé
Credential Guard	**Activé avec verrouillage UEFI**	Protège les hashes NTLM et tickets Kerberos

4. GPO « WHfB-PIN-Policy »

4.1 Politique de PIN

Chemin : Configuration ordinateur > Modèles d'administration > Composants Windows > Windows Hello for Business > PIN Complexity

Paramètre	Valeur configurée	Justification
Longueur minimale du PIN	6 caractères	Équilibre sécurité / ergonomie
Longueur maximale du PIN	20 caractères	Permet des PIN longs pour les admins
Exiger des chiffres	**Activé**	Renforcement du PIN
Exiger des minuscules	**Activé**	Empêche les PIN trop simples
Exiger des majuscules	**Activé**	Renforcement supplémentaire
Exiger des caractères spéciaux	Non configuré	Trop contraignant pour opérateurs prod.
Expiration du PIN (jours)	180 jours	Renouvellement semestriel
Historique du PIN	5 PIN précédents	Empêche la réutilisation immédiate
Autoriser la récupération du PIN	**Activé**	Autorise la réinitialisation en autonomie

> **i** Pour les opérateurs de production (environnement industriel, gants), la longueur minimale est maintenue à 6 caractères pour faciliter la saisie. Voir le guide utilisateur (DOC-WHB-03).

5. GPO « WHfB-Biometric-Policy »

5.1 Paramètres biométrie

Chemin : Configuration ordinateur > Modèles d'administration > Composants Windows > Biométrie

Paramètre	Valeur	Justification
Autoriser l'utilisation de la biométrie	**Activé**	Confort utilisateur postes équipés
Autoriser les utilisateurs à se connecter avec la biométrie	**Activé**	Empreinte ou reconnaissance faciale
Configurer la détection de présence améliorée	**Activé**	Verrouillage auto si l'utilisateur s'éloigne
Autoriser la biométrie en mode dégradé de réseau	**Activé**	Fonctionnement hors connexion AD

6. GPO complémentaire — Politique de verrouillage

6.1 Verrouillage du compte et de l'écran

Chemin : Configuration ordinateur > Paramètres Windows > Paramètres de sécurité > Stratégies de compte

Paramètre	Valeur	Justification
Seuil de verrouillage du compte	5 tentatives	Limite les attaques par force brute PIN
Durée de verrouillage du compte	15 minutes	Auto-déverrouillage sans IT
Réinitialisation compteur après	15 minutes	Cohérent avec la durée de verrouillage

Chemin : Configuration ordinateur > Modèles d'administration > Panneau de configuration > Personnalisation

Paramètre	Valeur	Justification
Activer l'écran de verrouillage	Activé	Verrouillage automatique à l'inactivité
Délai d'inactivité avant verrouillage (secondes)	300 s (5 min)	Adapté à l'environnement de production

7. Commandes de diagnostic

```
# État WHfB complet
dsregcmd /status

# Vérifier les GPO appliquées
gpresult /h C:\Temp\gpo-report.html /f

# Journaux d'événements WHfB
Get-WinEvent -LogName 'Microsoft-Windows-HelloForBusiness/Operational' | Select
-First 20

# Lister les credentials WHfB enregistrés
certutil -user -store My

# Forcer l'application des GPO
gpupdate /force
```