LOSTE TRADI-FRANCE

Renforcement de l'Authentificationvia Windows Hello for Business

Procédure de déploiement

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

1. Contexte et objectifs

Dans le cadre du renforcement de la sécurité des accès au système d'information de Loste Tradi-France (~1 700 collaborateurs), la direction informatique a décidé de déployer Windows Hello for Business (WHfB). Cette solution remplace l'authentification par mot de passe traditionnel par une authentification forte à deux facteurs : un geste utilisateur (PIN, empreinte digitale ou reconnaissance faciale) combiné à une clé cryptographique stockée dans le TPM du poste.

WHfB offre une résistance aux attaques de type phishing, pass-the-hash et credential stuffing, car les credentials ne transitent jamais sur le réseau.

1.1 Comparatif authentification classique / WHfB

Critère	Mot de passe classique	Windows Hello for Business
Transmission réseau	Hash/mot de passe transmis	**Jamais — clé privée locale**
Résistance phishing	Faible	**Très élevée**
Résistance pass-the-hash	Vulnérable	**Immunisé**
Expérience utilisateur	Saisie manuelle à chaque session	Rapide (PIN court ou biométrie)
Réinitialisation oubliée	Support IT requis	PIN réinitialisable en autonomie
Prérequis matériel	Aucun	TPM 2.0 obligatoire

1.2 Mode de déploiement choisi : Hybrid Azure AD Join

Loste Tradi-France dispose d'un Active Directory on-premise synchronisé avec Azure AD via Azure AD Connect. Le mode retenu est le déploiement hybride (Hybrid Azure AD Joined), qui permet d'utiliser WHfB sur des postes membres du domaine AD tout en bénéficiant de la confiance Azure AD.

Composant	Version / Détail
Active Directory	Windows Server 2022 — Niveau fonctionnel domaine 2016+
Azure AD Connect	Version 2.x — Synchronisation UPN + appareils
PKI interne	Autorité de certification (CA) Active Directory Certificate Services
Postes clients	Windows 10 Pro/Entreprise 21H2+ ou Windows 11
TPM	TPM 2.0 requis sur tous les postes cibles
Licences	Azure AD Premium P1 (ou Microsoft 365 Business Premium)

2. Prérequis et vérifications préalables

2.1 Vérification du TPM sur les postes

```
# Vérifier la présence et l'état du TPM (PowerShell)
Get-Tpm

# Résultat attendu :
# TpmPresent     : True
# TpmReady       : True
# TpmEnabled     : True
# TpmActivated   : True
# ManufacturerVersion : (version >= 2.0)

# Si TPM non activé : l'activer dans le BIOS/UEFI du poste
# Paramètre BIOS : Security > TPM > Enabled
```

2.2 Vérification du Hybrid Azure AD Join

```
# Vérifier l'état de jonction Azure AD du poste
dsregcmd /status

# Valeurs attendues :
# AzureAdJoined     : YES
# DomainJoined      : YES
# AzureAdPrt        : YES  (token d'authentification Azure AD présent)
```

2.3 Vérification de la PKI

- L'autorité de certification (AD CS) doit être opérationnelle
- Le modèle de certificat « Kerberos Authentication » doit être publié
- Les contrôleurs de domaine doivent posséder un certificat d'authentification Kerberos

```
# Vérifier les certificats des contrôleurs de domaine
certutil -dcinfo verify
```

3. Configuration de la PKI pour WHfB

3.1 Modèle de certificat pour les contrôleurs de domaine

1. Ouvrir la console « Autorité de certification » (certsrv.msc)
2. Clic droit sur « Modèles de certificats » > Gérer
3. Dupliquer le modèle « Kerberos Authentication »
4. Onglet Général : nommer « WHfB-DC-Auth », période 1 an
5. Onglet Sécurité : ajouter le groupe « Contrôleurs de domaine » avec droits Inscrire et Inscription automatique
6. Onglet Extensions > Stratégies d'application : vérifier la présence de « Authentification du client » et « Authentification Kerberos »
7. Publier le modèle : dans certsrv.msc > Modèles de certificats > Nouveau > Modèle de certificat à délivrer

3.2 Inscription automatique des certificats DC

Via GPO (Configuration ordinateur > Paramètres Windows > Paramètres de sécurité > Stratégies de clé publique > Client des services de certificats) :

- Activer : Inscription automatique des certificats
- Cocher : Renouveler les certificats expirés, mettre à jour les certificats en attente
- Cocher : Mettre à jour les certificats qui utilisent des modèles de certificats

4. Déploiement de Windows Hello for Business

4.1 Enregistrement des appareils dans Azure AD

> **i** Les postes doivent être enregistrés dans Azure AD (Hybrid Join) avant de pouvoir utiliser WHfB. Cette étape est normalement effectuée automatiquement par Azure AD Connect.

```
# Forcer l'enregistrement Hybrid Azure AD Join sur un poste
dsregcmd /join

# Vérifier l'enregistrement dans le portail Azure
# Azure Active Directory > Appareils > Tous les appareils
# Le poste doit apparaître avec le type 'Hybrid Azure AD Joined'
```

4.2 Activation de WHfB via GPO

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

Paramètre GPO	Valeur	Description
Utiliser Windows Hello for Business	**Activé**	Active WHfB sur les postes
Utiliser un périphérique TPM	**Activé**	Oblige le stockage dans le TPM
Utiliser des certificats pour l'authentification	**Activé**	Mode certificat (hybride)
Longueur minimale du PIN	6 chiffres	Sécurité minimale PIN
PIN complexe requis	**Activé**	Lettres + chiffres obligatoires
Utiliser la biométrie	Activé	Empreinte / Face ID si capteur présent
Exclure les cartes à puce	Non configuré	Coexistence avec smartcard possible

4.3 Déploiement progressif par phases

Phase	Population cible	Action	Durée
1 — Pilote	Équipe IT (10 postes)	Déploiement GPO sur OU IT	2 semaines
2 — Services admin	RH, Compta, Direction (200 postes)	Extension GPO aux OU admin	3 semaines
3 — Production	Opérateurs et techniciens (1 490 postes)	Extension GPO + guide utilisateur	4 semaines

5. Enrôlement utilisateur

Lors de la première connexion après application de la GPO, Windows guide l'utilisateur pour configurer son PIN WHfB :

8. L'utilisateur se connecte avec son mot de passe AD habituel
9. Windows affiche le message : « Votre organisation requiert la configuration de Windows Hello »
10. L'utilisateur clique sur « OK » et entre son mot de passe AD pour confirmer son identité
11. L'utilisateur choisit un PIN (minimum 6 caractères, complexe)
12. Optionnel : l'utilisateur configure la reconnaissance faciale ou l'empreinte digitale
13. WHfB est opérationnel : les connexions suivantes utilisent le PIN ou la biométrie

> ⚠ **En cas de perte ou d'oubli du PIN, l'utilisateur peut le réinitialiser via : Paramètres > Comptes > Options de connexion > PIN Windows Hello > J'ai oublié mon PIN.**

6. Vérification post-déploiement

N°	Vérification	Résultat attendu	Statut
1	dsregcmd /status : NgcSet = YES	YES	[ ] OK / [ ] KO
2	Connexion Windows avec PIN WHfB réussie	Session ouverte	[ ] OK / [ ] KO
3	Accès aux ressources réseau (partages, intranet) sans resaisie	Accès transparent (SSO)	[ ] OK / [ ] KO
4	Certificat WHfB visible dans le magasin personnel du poste	Certificat présent	[ ] OK / [ ] KO

5	Journaux événements : Event 5382 (WHfB credential enregistré)	Event présent	[ ] OK / [ ] KO

```
# Vérifier l'état WHfB complet sur un poste
dsregcmd /status | Select-String -Pattern
'NgcSet|HelloSet|AzureAdJoined|DomainJoined'
```