Délivrer automatiquement un certificat via une GPO

Cours | 🌐 Admin sys réseaux

Avant de commencer, vérifie que :

- **AD CS** est bien installé sur une **autorité de certification d'entreprise** ;
- le poste cible est **joint au domaine** ;
- la machine peut contacter l'AC ;
- tu disposes des droits nécessaires pour gérer les **modèles de certificats** et les **GPO**. Microsoft indique aussi qu'il faut avoir une AC d'entreprise configurée et un modèle prêt pour l'auto-inscription.

Ordinateur

1. Créer le modèle de certificat

Sur le serveur de certification :

1. Ouvre la console **Autorité de certification**.
2. Fais un clic droit sur **Modèles de certificats** puis **Gérer**.
3. Dans la console des modèles, repère le modèle **Ordinateur**.
4. Fais **clic droit > Dupliquer le modèle**. Le tutoriel IT-Connect part bien du modèle **Ordinateur** pour créer un modèle personnalisé destiné aux machines.

2. Configurer les permissions du modèle

Dans le modèle dupliqué :

1. Va dans l'onglet **Sécurité**.
2. Ajoute le groupe qui doit recevoir le certificat :
    - soit **Ordinateurs du domaine** pour toutes les machines ;

- soit un groupe AD plus restreint si tu veux cibler seulement certaines machines.

3. Donne **trois autorisations** :
   - **Lecture**
   - **Inscrire**
   - **Inscription automatique**

Ces trois droits sont précisément ceux indiqués dans le tutoriel IT-Connect, et Microsoft confirme que l'auto-inscription repose sur les permissions **Read / Enroll / Autoenroll** du modèle.

3. Vérifier que le modèle peut construire automatiquement le certificat

Toujours dans le modèle, il faut que les informations nécessaires à la génération du certificat soient **récupérées automatiquement depuis Active Directory**. Le tutoriel précise que sans ce point, **l'inscription automatique ne peut pas fonctionner**.

En pratique, évite de configurer un modèle qui exigerait des informations saisies manuellement ou une validation qui bloquerait l'auto-enrôlement. Je ne peux pas confirmer un réglage universel unique pour tous les modèles, car cela dépend aussi des autres onglets du template, mais pour un certificat ordinateur standard basé sur **Ordinateur**, il faut rester sur une configuration compatible avec l'auto-inscription.

4. Publier le modèle sur l'autorité de certification

Une fois le modèle configuré :

1. Reviens dans la console **Autorité de certification**.
2. Clic droit sur **Modèles de certificats**.
3. Choisis **Nouveau > Modèle de certificat à délivrer**.
4. Sélectionne ton modèle personnalisé.

Cette publication du modèle sur l'AC est nécessaire pour qu'il puisse être demandé par les clients. Microsoft la mentionne aussi dans sa procédure de configuration des templates.

5. Créer ou modifier une GPO d’auto-inscription

Depuis la console **Gestion de stratégie de groupe (GPMC)** :

1. Crée une nouvelle GPO, ou modifie une GPO existante.
2. Lie-la à l’OU contenant les **ordinateurs** ciblés.
3. Ouvre la GPO en modification.

6. Désactiver la partie “Utilisateur” dans la GPO

Comme il s’agit ici d’un **certificat ordinateur** :

1. Ouvre les **propriétés** de la GPO.
2. Désactive les **paramètres de configuration de l’utilisateur**.

Le tutoriel le fait explicitement, car la stratégie ne concerne que le **compte ordinateur**.

7. Activer l’auto-inscription dans la GPO

Dans l’éditeur de GPO, va ici :

Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégie de clé publique

Puis ouvre :

Clients des services de certificats – Inscription automatique

Configure :

- **Activé**
- coche **Renouveler les certificats expirés, mettre à jour les certificats en attente et supprimer les certificats révoqués**
- coche **Mettre à jour les certificats utilisant des modèles de certificat**

Le chemin GPO et les deux cases à cocher sont donnés à la fois par IT-Connect et par Microsoft.

8. Forcer l’application de la GPO sur le poste client

Sur le poste cible :

- soit tu **redémarres** la machine ;

- soit tu exécutes `gpupdate /force` en invite de commandes ou PowerShell administrateur, puis redémarrage si besoin.

Le tutoriel IT-Connect indique qu'un poste déjà allumé devra être **redémarré** pour appliquer la GPO dans ce scénario.

9. Vérifier que le certificat a bien été délivré

Sur le poste client :

1. Lance **certlm.msc**
2. Va dans :**Certificats (ordinateur local) > Personnel > Certificats**
3. Vérifie qu'un certificat issu de ton **AC interne** est présent.

IT-Connect indique que le certificat doit apparaître dans le **magasin personnel de la machine**, ce qui confirme que l'opération s'est faite automatiquement.

Utilisateur

1. Modèle de certificat

🔁 Au lieu de :

- **Modèle : Ordinateur**

👉 Utilise :

- **Modèle : Utilisateur**

➡️ Tu dois :

- Dupliquer le modèle **Utilisateur** (au lieu de Ordinateur)

➡️ Dans propriété du modèle utilisateur > Nom du sujet, il faut décocher **Inclure le nom de compte de messagerie dans le nom du sujet** car dans notre cas il y'a pas de mail de messagerie configuré

---

2. Permissions du modèle

🔁 Au lieu de :

- Groupe : **Ordinateurs du domaine**

👉 Utilise :

- Groupe : **Utilisateurs du domaine** (ou un groupe spécifique d'utilisateurs)

➡️ Droits à donner (inchangés) :

- Lecture
- Inscrire
- Inscription automatique

---

3. Portée de la GPO

🔁 Au lieu de :

- GPO liée à une **OU contenant des ordinateurs**

👉 Utilise :

- GPO liée à une **OU contenant des utilisateurs**

---

4. Configuration dans la GPO

🔁 Au lieu de configurer :

```
Configuration ordinateur
```

👉 Tu dois configurer :

```
Configuration utilisateur
```

Puis :

```
Stratégies
→ Paramètres Windows
→ Paramètres de sécurité
→ Stratégie de clé publique
→ Client des services de certificats – Inscription automatique
```

➡️ Paramètres (identiques) :

- Activer
- Cocher :

- Renouveler les certificats expirés
- Mettre à jour les certificats
- Supprimer les certificats révoqués

---

5. Paramètre GPO à ne PAS faire

🔁 Au lieu de :

- Désactiver la partie utilisateur (cas ordinateur)

👉 Ici :

- ❌ **NE PAS désactiver la configuration utilisateur**
- ✔️ C'est elle qui est utilisée

---

6. Application de la GPO

🔁 Au lieu de :

- Redémarrage machine

👉 Ici :

- Déconnexion / reconnexion de l'utilisateur
  OU
- `gpupdate /force`

---

7. Vérification du certificat

🔁 Au lieu de :

- `certlm.msc` (certificat machine)

👉 Utilise :

- `certmgr.msc` (certificat utilisateur)

Puis :

```
Certificats - Utilisateur actuel
→ Personnel
→ Certificats
```

Vérifications utiles si ça ne fonctionne pas

A. Contrôler que la GPO est bien appliquée

Sur le poste client :

```
gpresult/r
```

ou

```
gpresult/hc:\temp\gpresult.html
```

Tu dois voir la GPO appliquée au **compte ordinateur**. Microsoft précise que la configuration se fait bien dans **Computer Configuration** pour les certificats machine.

B. Contrôler les droits du modèle

Le problème le plus fréquent est un oubli sur le modèle :

- **Lecture**
- **Inscrire**
- **Inscription automatique**

Sans ces droits, l'auto-enrollment ne se fait pas. C'est confirmé par IT-Connect et par la documentation Microsoft sur les permissions des templates.

C. Vérifier que le modèle est bien publié sur l'AC

Même si le modèle est correctement configuré, il ne sera pas délivré s'il n'a pas été **ajouté aux modèles à délivrer** sur l'autorité de certification.

D. Vérifier que le certificat est bien un certificat ordinateur

La GPO ici agit côté **ordinateur**, donc il faut :

- viser la bonne OU ;
- cibler les bons objets ordinateurs ;

- vérifier que tu ne cherches pas le certificat dans **certmgr.msc** côté utilisateur au lieu de **certlm.msc** côté machine. Le tutoriel IT-Connect montre bien une vérification via **certlm.msc**.

E. Vérifier les journaux d'événements

En cas d'échec, consulte l'Observateur d'événements sur le poste client, notamment les journaux liés à la stratégie de groupe et aux certificats. Microsoft recommande l'usage des journaux d'événements pour surveiller l'enrôlement et diagnostiquer les problèmes d'auto-enrollment.

Version très courte des étapes

1. Dupliquer le modèle **Ordinateur**.
2. Donner **Lecture + Inscrire + Inscription automatique** au bon groupe.
3. Vérifier que le modèle est compatible avec une génération automatique depuis l'AD.
4. Publier le modèle sur l'AC.
5. Créer/lier une GPO sur l'OU des ordinateurs.
6. Activer **Certificate Services Client – Auto-Enrollment** dans **Configuration ordinateur > Stratégie de clé publique** avec les **2 cases cochées**.
7. Forcer la GPO / redémarrer.
8. Vérifier le certificat dans **certlm.msc > Personnel > Certificats**.