Installation EDR Automatique avec GPO

A) Placer l'exécutable dans un répertoire accessible depuis l'ensemble des postes

1. Récupérez l'exécutable Crowdstrike (c.f. Préalable)
2. Placez le fichier sur un serveur accessible de tous les postes, par exemple le serveur de fichiers.

Notez le chemin d'accès, par exemple
`\\NomDuServeur\DossierPartage\Crowdstrike\<nom du fichier Crowdstrike>.exe`

B) Créer le script l'installation

1. Créez un nouveau fichier texte, avec par exemple Notepad++, et enregistrez-le sous le nom `InstallCrowdStrike.bat.`
2. Entrez les commandes à exécuter, telles qu'indiquées dans la partie Console.

Attention, il faut bien indiquer tout le chemin d'accès à l'exécutable.
Par exemple, la commande peut être :
`\\NomDuServeur\DossierPartage\Crowdstrike\<nom du fichier Crowdstrike>.exe /install /quiet /norestart CID=code_client` en remplaçant `code_client` par votre identifiant client.

C) Créez une GPO pour exécuter le script

1. Ouvrez la console de gestion des stratégies de groupe (GPMC) : `Wind. + R > gpmc.msc` et appuyez sur `Entrée`.
2. Faites un clic droit sur le conteneur où vous souhaitez appliquer la GPO (exemple : le domaine ou une OU spécifique).
3. Cliquez sur "**Créer un objet de stratégie de groupe dans ce domaine et le lier ici"**, et donnez-lui un nom (par exemple : `Déploiement CrowdStrike`).
4. Ajoutez le script :
    a. Copiez le script de l'étape B dans le dossier `\\<nom serveur>\SysVol\<nom domaine>\Policies\<GUID de la GPO>\Machine\Scripts\Startup` pour qu'il soit accessible à tous.
    b. Retournez dans la console de gestion des stratégies de groupe (GPMC), faites un clic droit sur la nouvelle GPO et sélectionnez **Modifier**.
    c. Accédez à **Configuration de l'ordinateur > Stratégies > Paramètres Windows > Scripts (Démarrage/Arrêt)**.
    d. Double-cliquez sur **Démarrage**, puis cliquez sur **Ajouter**.

e. Dans la fenêtre qui s'ouvre, cliquez sur **Parcourir**, puis sélectionnez le script préalablement rédigé InstallCrowdStrike.bat.

D) Appliquez la GPO

1. Assurez-vous que la GPO est bien liée au bon conteneur (domaine ou OU contenant les machines cibles).
2. Utilisez `gpupdate /force` sur un contrôleur de domaine pour forcer la mise à jour des stratégies.
3. Vérifiez l'application :

a. Redémarrez une machine cible pour déclencher le script.
b. Lancez la commande `gpresult /h gpresults.html` et vérifiez que votre nouvelle GPO est bien sur présente sur la machine
c. Vérifiez que CrowdStrike est installé et opérationnel sur cette machine.

En cas de problèmes : consultez le fichier journal des scripts de démarrage sur les machines clientes `C:\Windows\Debug\StartupLog.txt`

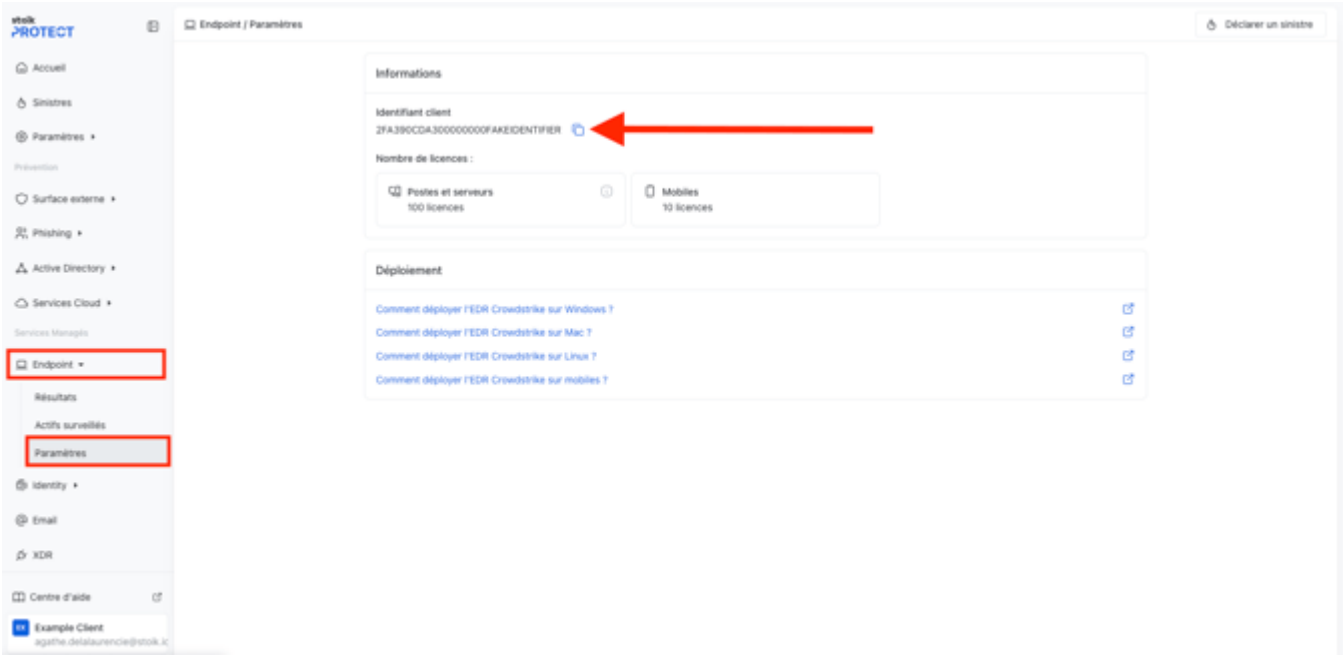
Comment déployer l'EDR CrowdStrike sur Windows ?

Deux méthodes sont possibles pour installer l'EDR CrowdStrike sur Windows : manuelle via interface graphique ou automatique via ligne de commande.

Si vous souhaitez déployer l'EDR à large échelle par la méthode automatique, Stoïk vous recommande de débuter par une installation manuelle test sur quelques postes.

1. Préalable : exécutable et identifiant

- Télécharger l'exécutable (aussi appelé "binaire d'installation") depuis ce lien.
- Trouver votre identifiant client : disponible depuis votre espace **Stoïk Protect** 👉 **Onglet "MDR" > "Paramètres"**



⚠️ L'exécutable n'est plus valide pour les postes de travail ayant une version Windows strictement inférieures à W7.

Cet exécutable (aussi appelé Falcon Legacy) est à utiliser pour les systèmes d'ancienne génération suivants :

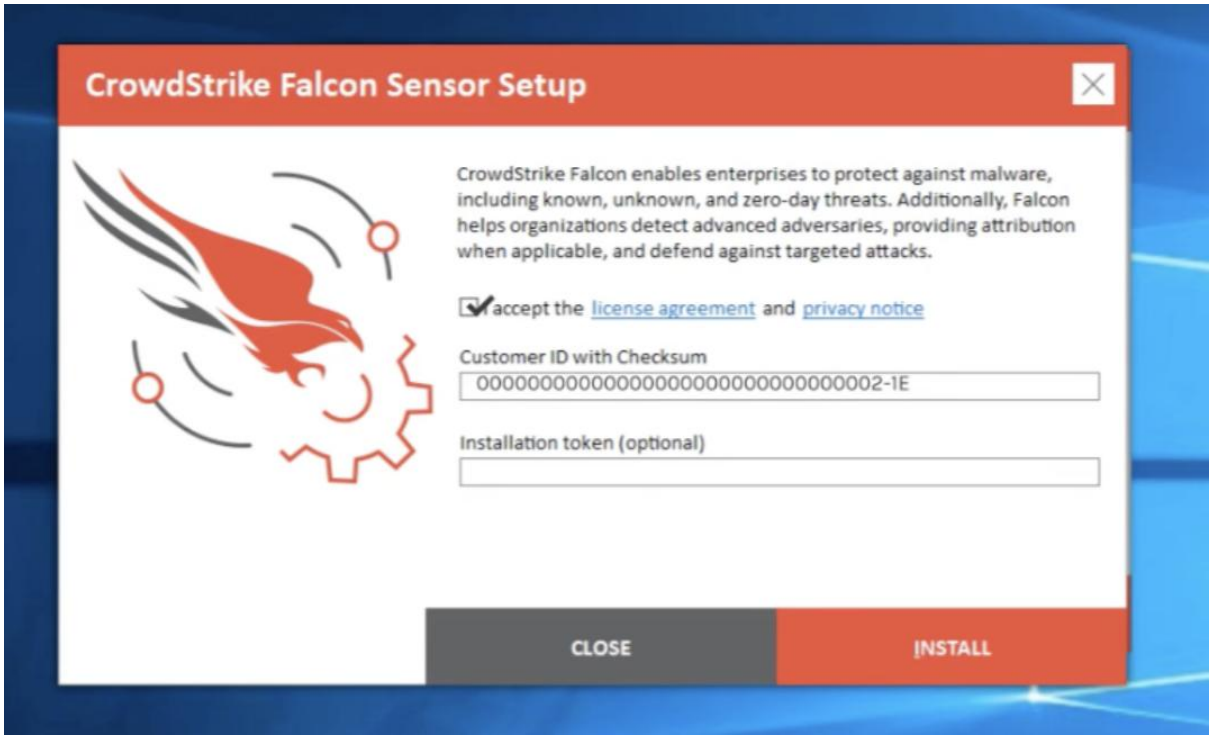
- Windows XP 32 bits - Service Pack 3
- Windows XP 64 bits - Service Pack 2
- Windows Server 2003 32 et 64 bits - Service Pack 2
- Windows Server 2003 R2 32 et 64 bits - Service Pack 2
- Windows Vista 32 et 64 bits - Service Pack 2
- Windows Server 2008 32 et 64 bits - Service Pack 2
- Windows Embedded POSReady 2009
- Windows 8 32 et 64 bits
- Windows 8.1 32 et 64 bits

Le cas échéant, ce message d'erreur risque d'apparaître :

2. Méthode manuelle

2.1. Graphique

1. Lancez l'exécutable sur le poste concerné depuis ce lien.
2. Renseignez l'identifiant client dans le champ **Customer ID with Checksum**
3. Cliquez sur **Install**



CrowdStrike **remplace votre antivirus actuel**. Il est donc nécessaire de **le désinstaller complètement avant d'installer CrowdStrike**.

⚠️ **Gestion du pare-feu :**

- Si le pare-feu est géré par la même solution que l'antivirus et que vous souhaitez la conserver, **ne désactivez pas entièrement cette solution et gardez le pare-feu tel quel.**
- A l'inverse, si vous souhaitez vous séparer de cette solution, pensez à **retranscrire les règles personnalisées** dans le pare-feu Windows local.

2.2. Console

1. Ouvrez une console sur votre endpoint.

2. Entrez la commande suivante : `<nom_du_fichier>.exe /install /quiet /norestart CID=code_client` en remplaçant `code_client` par votre identifiant client.

Cas particuliers

1. **Ajout de tags**
   a. Vous pouvez choisir d'ajouter un ou plusieurs **tags** pour organiser vos installations (par site, pays, entité, etc.), dans ce cas utilisez plutôt la commande suivante : `<nom du fichier crowdstrike>.exe /install /quiet /norestart CID=code_client GROUPING_TAGS="INSERER_ICI_LES_TAGS"`
   b. Il vous est possible de spécifier plusieurs tag en les séparant par des virgules.
2. **Déployer l'EDR sur un poste temporairement hors-ligne**
   a. Vous devez rajouter l'option `ProvNoWait=1` . La ligne de commande ressemblera alors à ceci : `<nom du fichier crowdstrike>.exe /install /quiet /norestart ProvNoWait=1 CID=code_client`
   b. Attention, l'EDR Crowdstrike a tout de même besoin d'une connexion internet pour fonctionner correctement, et notamment remonter les alertes détectées.

3. Méthode automatique

3.1 Par GPO

A) Placer l'exécutable dans un répertoire accessible depuis l'ensemble des postes

1. Récupérez l'exécutable Crowdstrike (c.f. Préalable)
2. Placez le fichier sur un serveur accessible de tous les postes, par exemple le serveur de fichiers.
   Notez le chemin d'accès, par exemple `\\NomDuServeur\DossierPartage\Crowdstrike\<nom du fichier Crowdstrike>.exe`

B) Créer le script l'installation

1. Créez un nouveau fichier texte, avec par exemple Notepad++, et enregistrez-le sous le nom `InstallCrowdStrike.bat` .
2. Entrez les commandes à exécuter, telles qu'indiquées dans la partie Console.
   Attention, il faut bien indiquer tout le chemin d'accès à l'exécutable.
   Par exemple, la commande peut être : `\\NomDuServeur\DossierPartage\Crowdstrike\<nom du fichier Crowdstrike>.exe /install /quiet /norestart CID=code_client` en remplaçant `code_client` par votre identifiant client.

C) Créez une GPO pour exécuter le script

1. Ouvrez la console de gestion des stratégies de groupe (GPMC) : `Wind. + R > gpmc.msc` et appuyez sur `Entrée`.

2. Faites un clic droit sur le conteneur où vous souhaitez appliquer la GPO (exemple : le domaine ou une OU spécifique).
3. Cliquez sur "**Créer un objet de stratégie de groupe dans ce domaine et le lier ici"**, et donnez-lui un nom (par exemple : `Déploiement CrowdStrike`).
4. Ajoutez le script:
    a. Copiez le script de l'étape B dans le dossier `\\<nom serveur>\SysVol\<nom domaine>\Policies\<GUID de la GPO>\Machine\Scripts\Startup` pour qu'il soit accessible à tous.
    b. Retournez dans la console de gestion des stratégies de groupe (GPMC), faites un clic droit sur la nouvelle GPO et sélectionnez **Modifier**.
    c. Accédez à **Configuration de l'ordinateur > Stratégies > Paramètres Windows > Scripts (Démarrage/Arrêt)**.
    d. Double-cliquez sur **Démarrage**, puis cliquez sur **Ajouter**.
    e. Dans la fenêtre qui s'ouvre, cliquez sur **Parcourir**, puis sélectionnez le script préalablement rédigé `InstallCrowdStrike.bat`.

D) Appliquez la GPO

1. Assurez-vous que la GPO est bien liée au bon conteneur (domaine ou OU contenant les machines cibles).
2. Utilisez `gpupdate /force` sur un contrôleur de domaine pour forcer la mise à jour des stratégies.
3. Vérifiez l'application :

    a. Redémarrez une machine cible pour déclencher le script.
    b. Lancez la commande `gpresult /h gpresults.html` et vérifiez que votre nouvelle GPO est bien sur présente sur la machine
    c. Vérifiez que CrowdStrike est installé et opérationnel sur cette machine.

En cas de problèmes : consultez le fichier journal des scripts de démarrage sur les machines clientes `C:\Windows\Debug\StartupLog.txt`

3.3 Par MDM (Intune ou NinjaOne)

Intune

1. Téléchargez les éléments nécessaires

1. Téléchargez l'outil (interface graphique) **Win32 Content Prep Tool**
2. Télécharger l'exécutable CrowdStrike depuis **ce lien**

2. Ouvrez Win32 Content Prep Tool

1. Ajoutez le fichier `.exe`
2. Renseignez la commande suivante : nom_du_fichier.exe /install /quiet /norestart CID=code_client
   Il s'agit du script de démarrage préalablement rédigé (cf. 2.2 Console).

3. Remplacez `nom_du_fichier.exe` par le nom réel du fichier et `code_client` par votre CID CrowdStrike

3. Téléchargez le fichier généré nommé `.intunewin`

4. Déployez

1. Connectez-vous à **Intune Admin Center** (intune.microsoft.com)
2. Importez le fichier `.intunewin`
3. Assignez-le à vos groupes d'ordinateurs
4. L'installation sera effectuée automatiquement sur les postes cibles

NinjaOne

Voici le lien vers une procédure pour l'intégration de Crowdstrike via NinjaOne : Lien procédure Crowdstrike avec NinjaOne