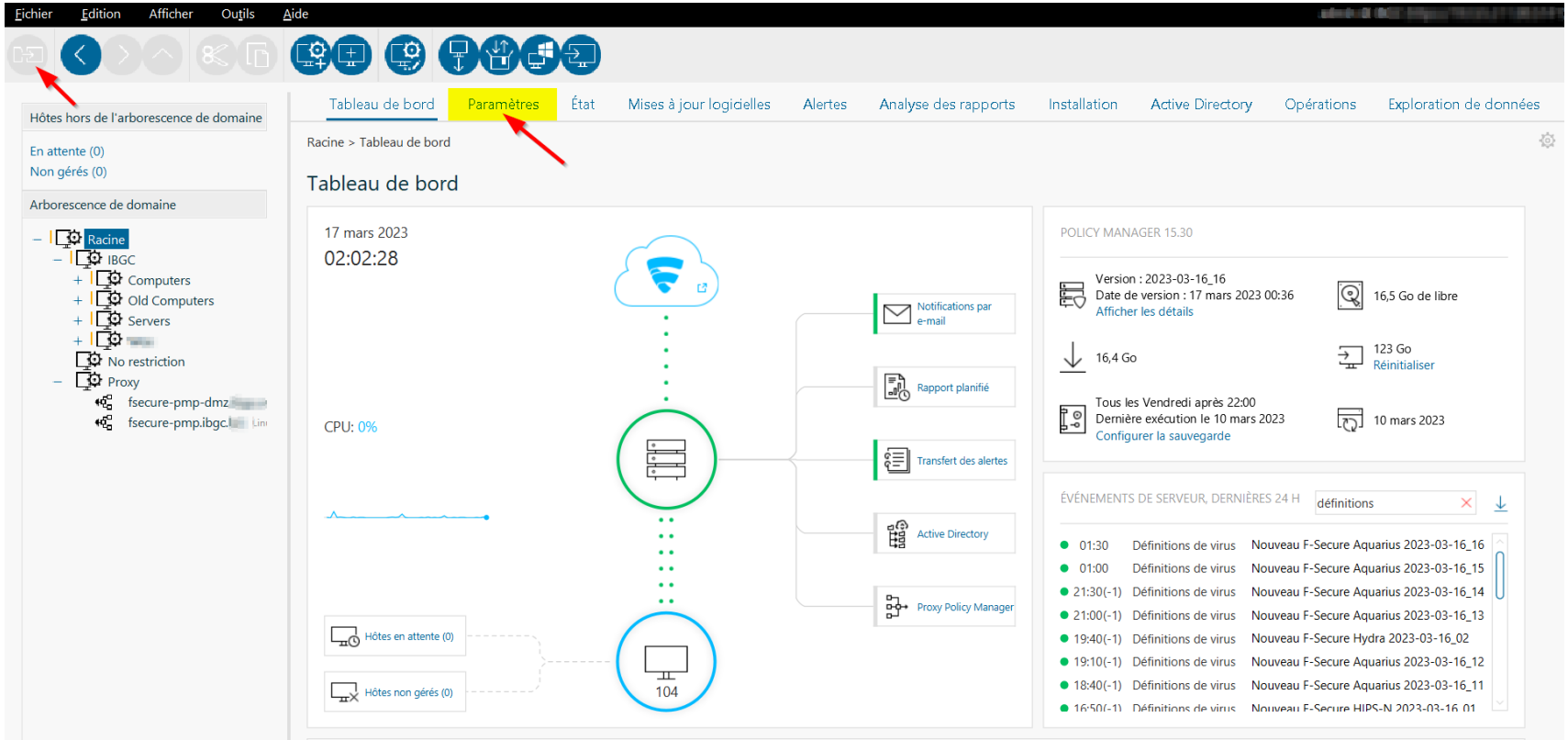
# Tableau de bord
# F-Secure Policy Manager Console (PMC)



# Configuration Racine

**Ne jamais modifier les paramètres de la racine**

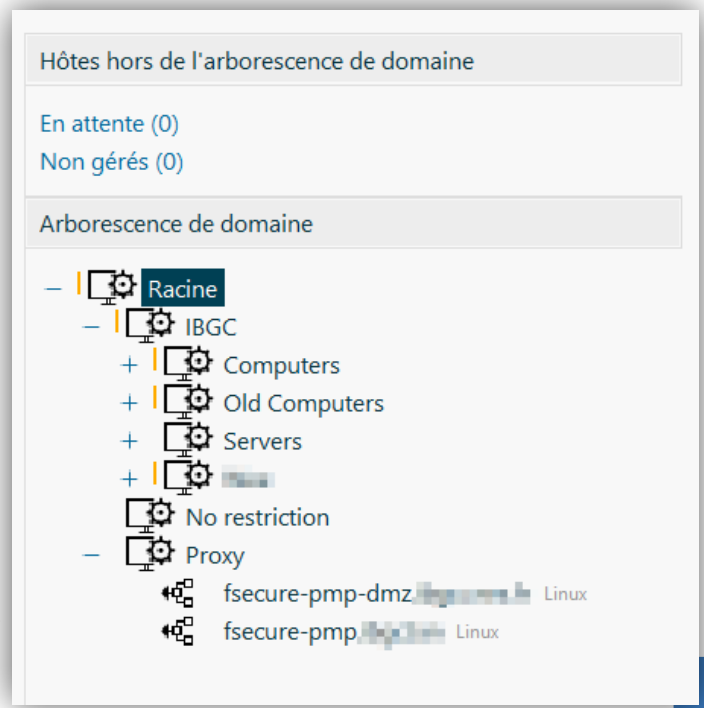
**Toujours commencer par créer un nouveau domaine de stratégie à la racine**

**Ne jamais importer l'AD dans la racine**

**En cas de synchro AD avec un domaine de stratégie il sera impossible d'y ajouter manuellement une machine**

**Seuls les postes Windows de l'AD sont gérés**

**Les Linux et Mac devront être intégrés manuellement dans un autre domaine de stratégie**



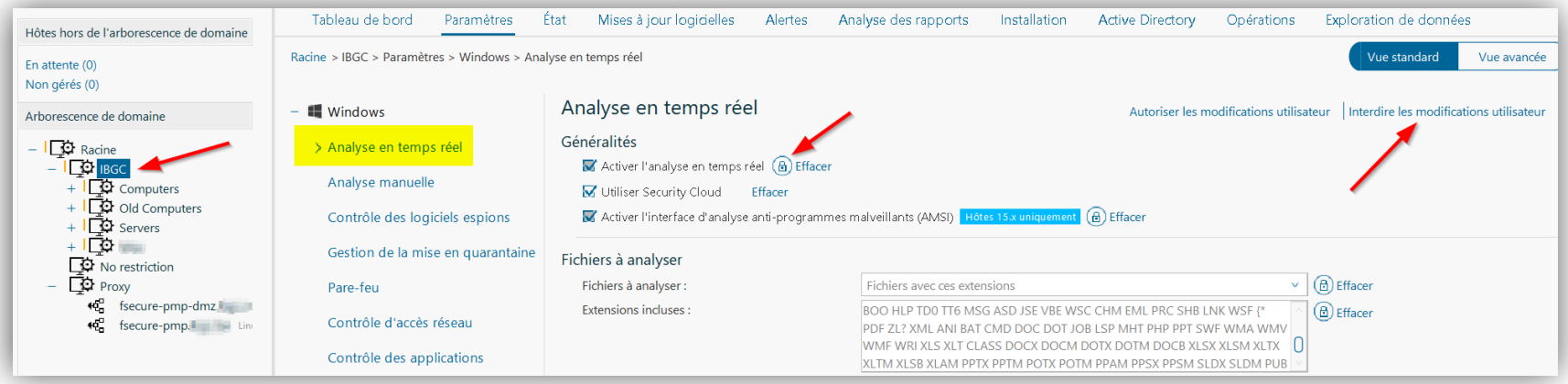
# Configuration
# Domaine de stratégie – Bonnes pratiques

1. Créer un nouveau domaine de stratégie pour sa structure qui héritera des paramètres par défaut (racine)

2. Créer un domaine « Proxy » à la racine (si nécessaire)

3. Interdire toutes les modifications utilisateur sur sa structure et fermer tous les cadenas qui seraient restés ouverts

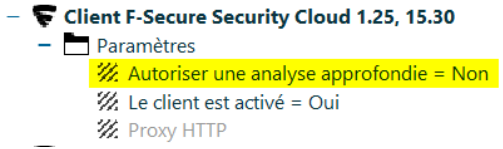
4. Modifier les paramètres du domaine « structure » en fonction de ses besoins



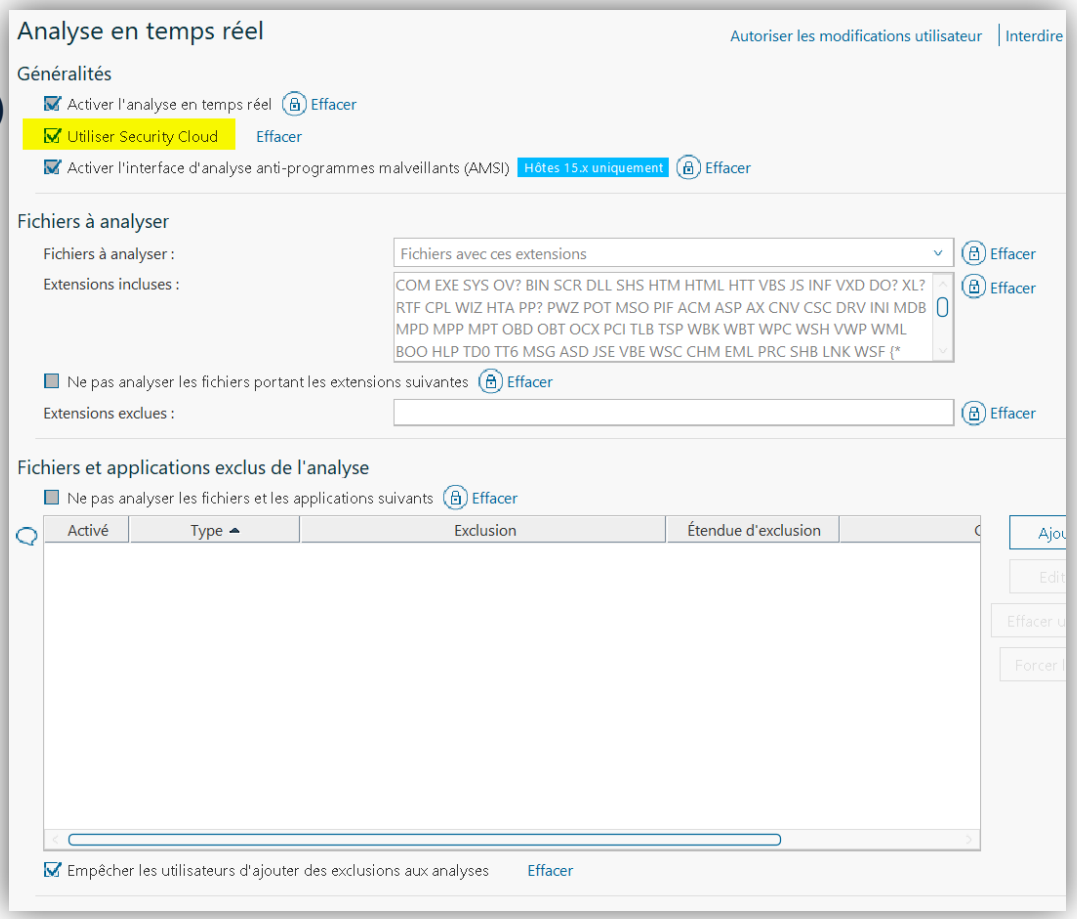
# Configuration
# Analyse en temps réel (1/2)

**« Security Cloud » est recommandé en environnement non sensible**

**A condition de désactiver l'analyse approfondie via la vue avancée, accessible avec un clic droit :**




**« Security Cloud » est interdit en Zone à régime restrictif (ZRR)**

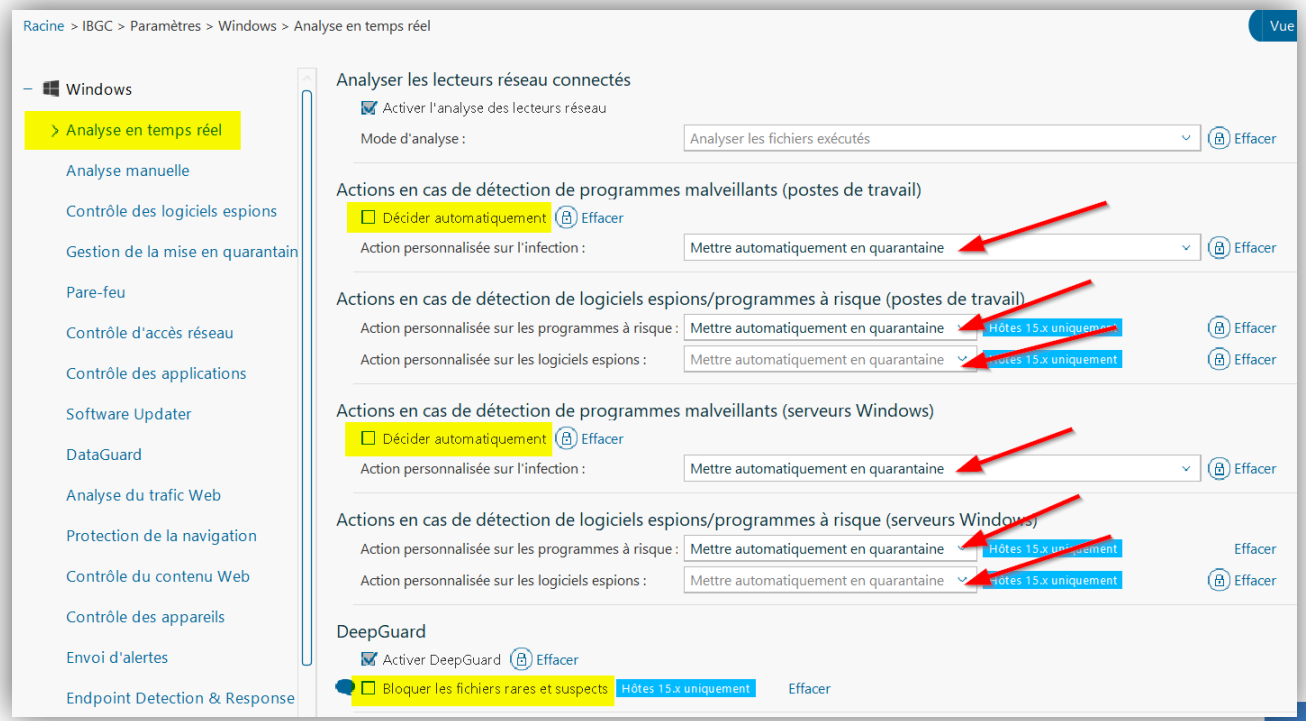


# Configuration
# Analyse en temps réel (2/2)

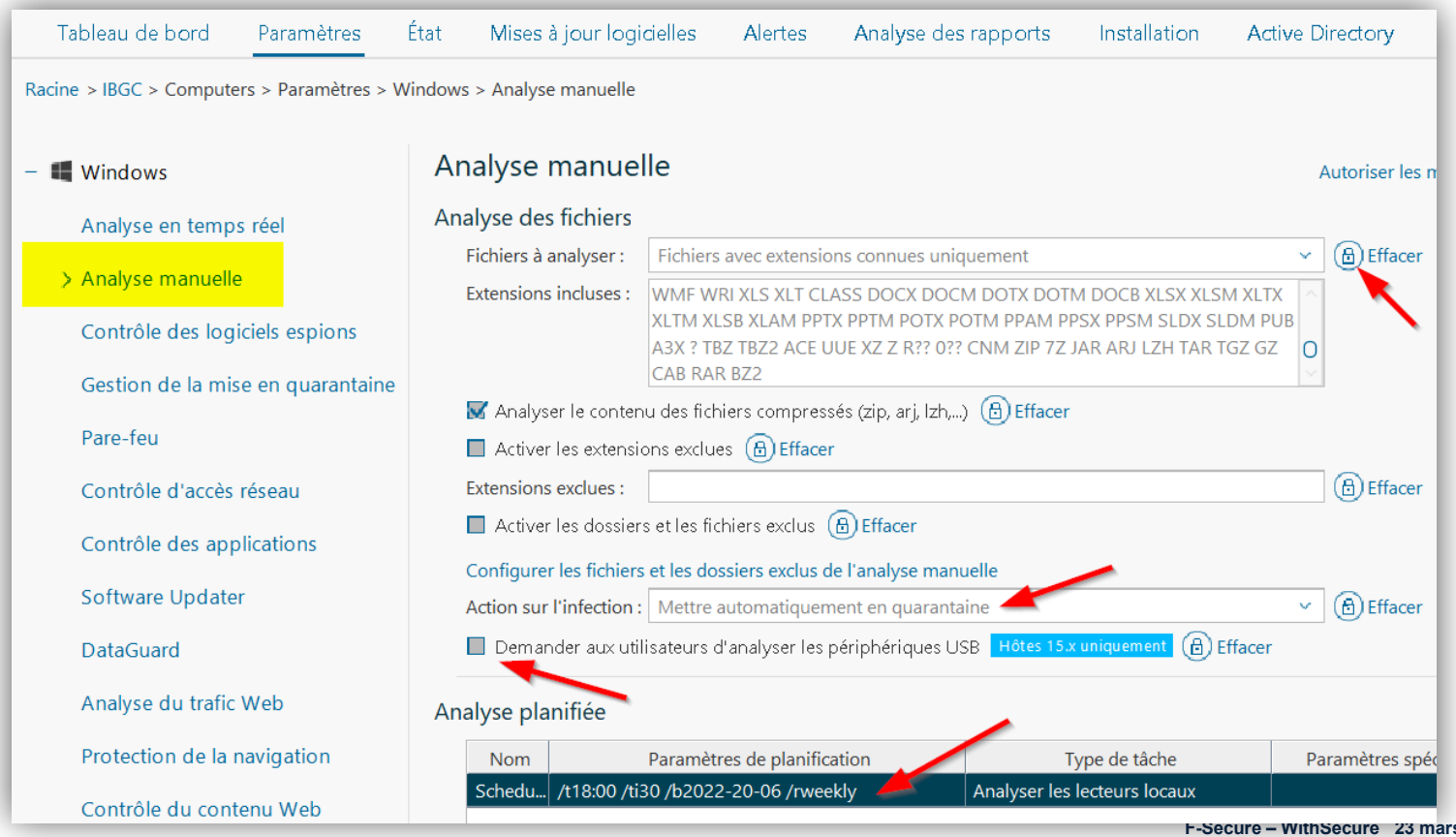
**En cas de détection de menace, il faut la mettre en quarantaine automatiquement**

**Toute décision automatique doit être désactivée**

**Décocher « Bloquer les fichiers rares et suspects » de DeepGuard car cette option nécessite de nombreux ajustements**



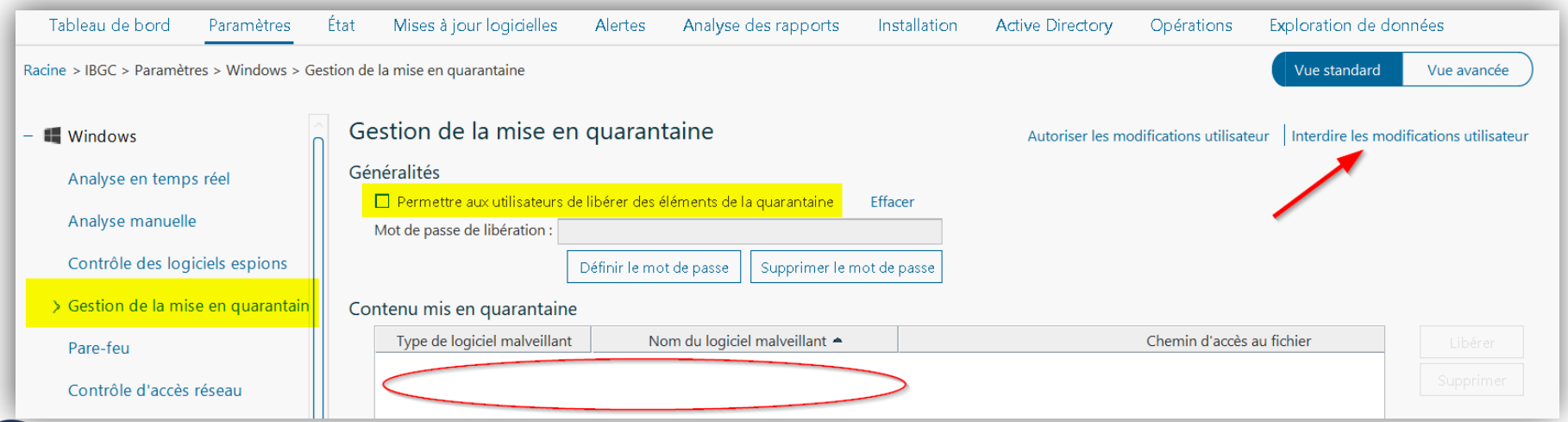
# Configuration
# Analyse manuelle



# Configuration
# Gestion de la mise en quarantaine

## Interdire aux utilisateurs de libérer des éléments de la quarantaine

## Possibilité de libérer / supprimer / nettoyer le contenu mis en quarantaine

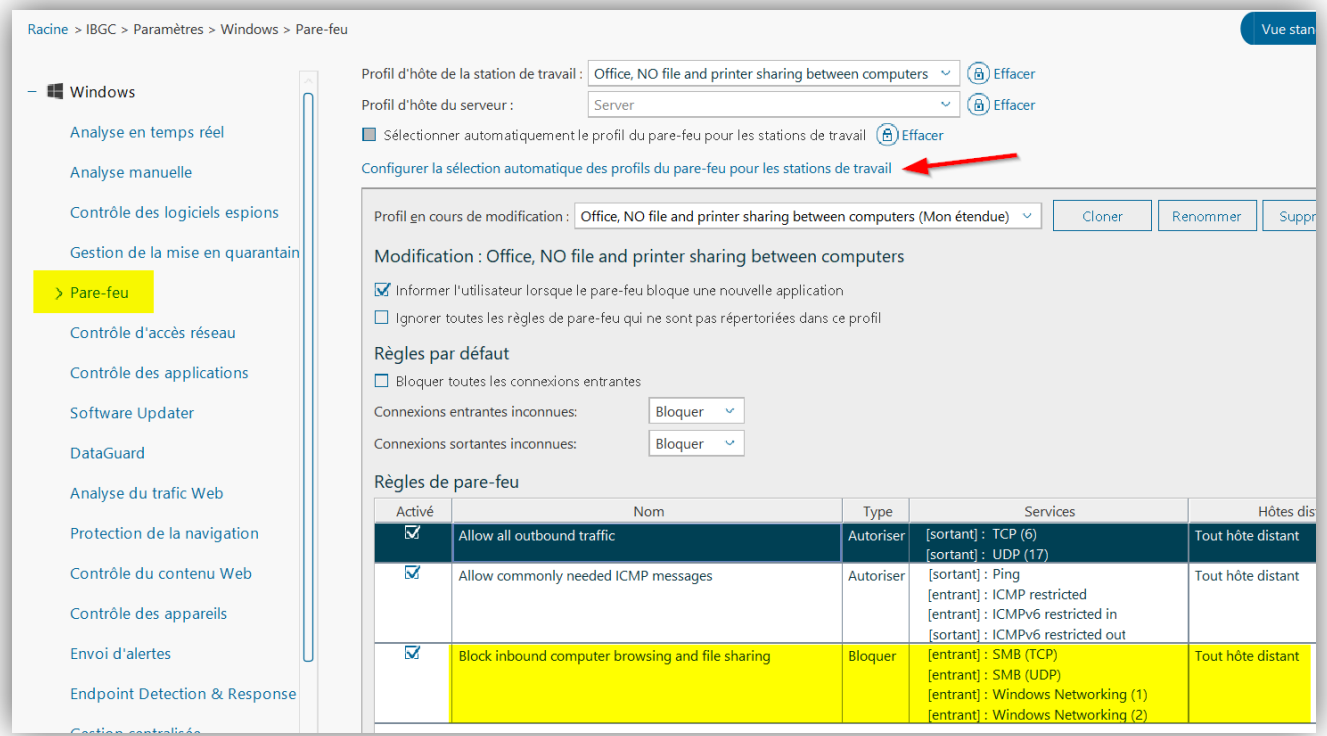


# Configuration Pare-feu

**Le profil par défaut « Office, file and printer sharing » est trop permissif**

**Dans l'exemple les partages SMB sont désactivés**

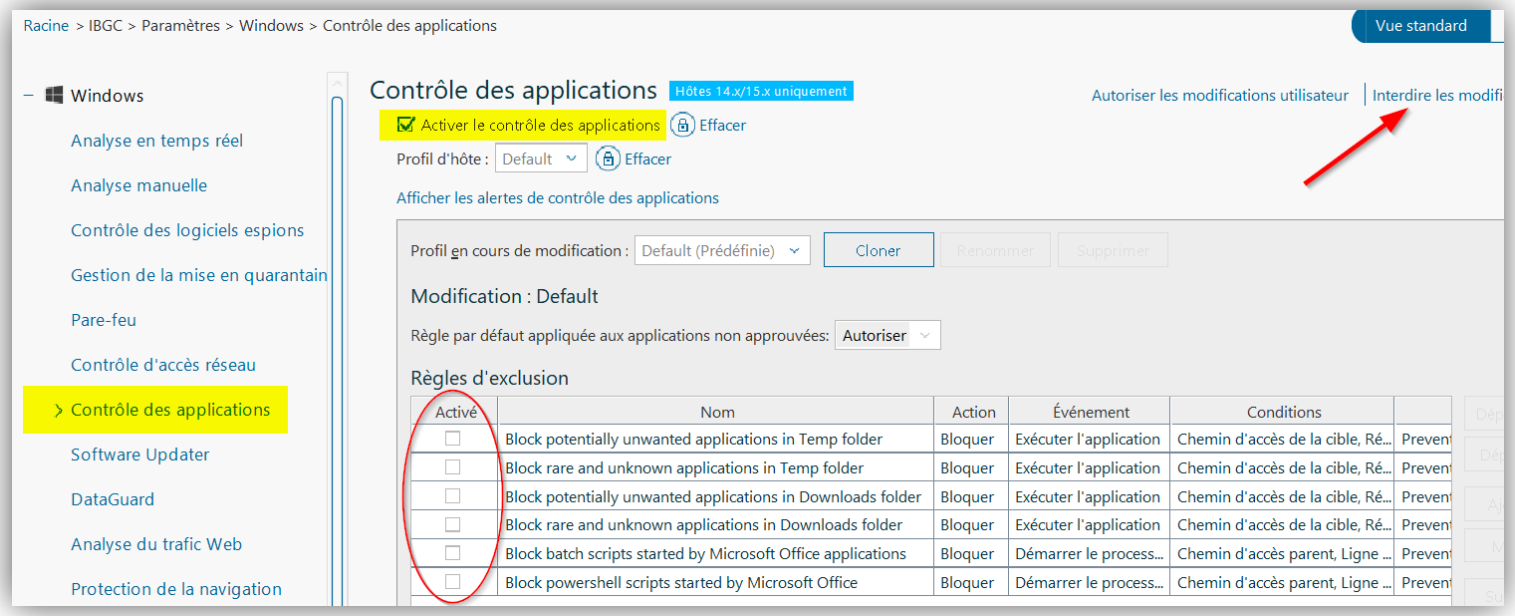
**Les règles de pare-feu peuvent être changées dynamiquement en fonction de critères réseaux choisis (IP)**



# Configuration
# Contrôle des applications

## Il est recommandé d'activer le contrôle des applications

## Activez et testez les règles d'exclusion sur des cobayes avant de les appliquer à tout votre parc



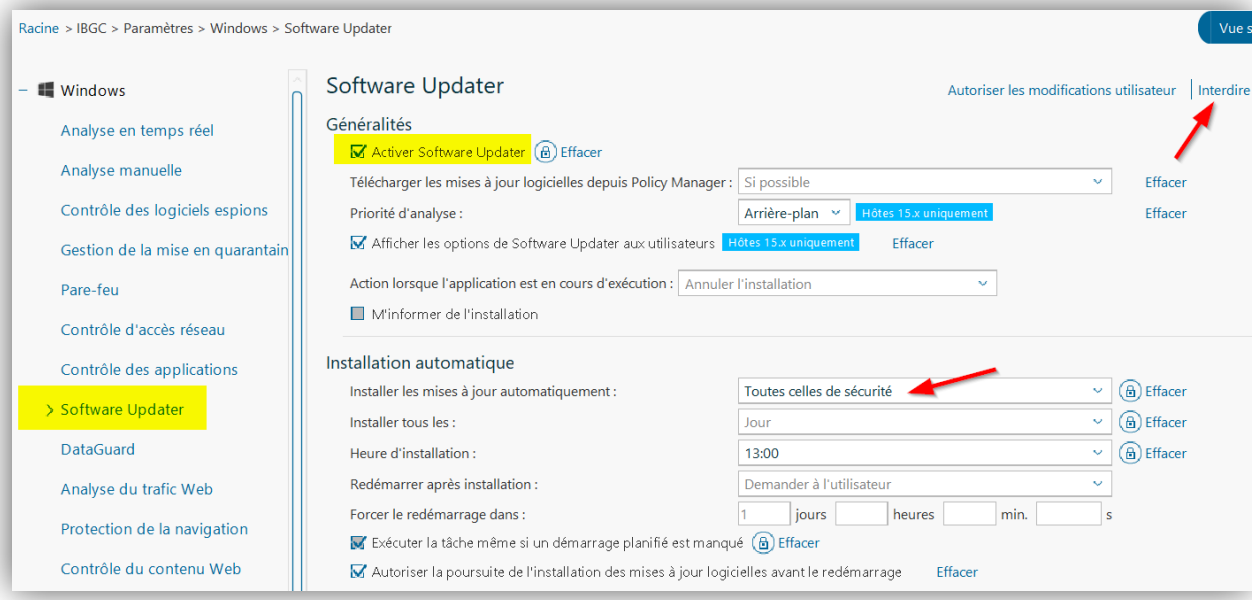
# Configuration Software Updater

**« Software Updater » permet de visualiser l'obsolescence des postes (OS et logiciels)**

**Activation recommandée si aucun autre outil de gestion des mises à jour n'existe déjà**

**L'installation automatique des mises à jour doit être testée avant un déploiement global**

**Remplace WSUS pour les màj systèmes et assure la màj des logiciels**




**Attention aux postes lents**

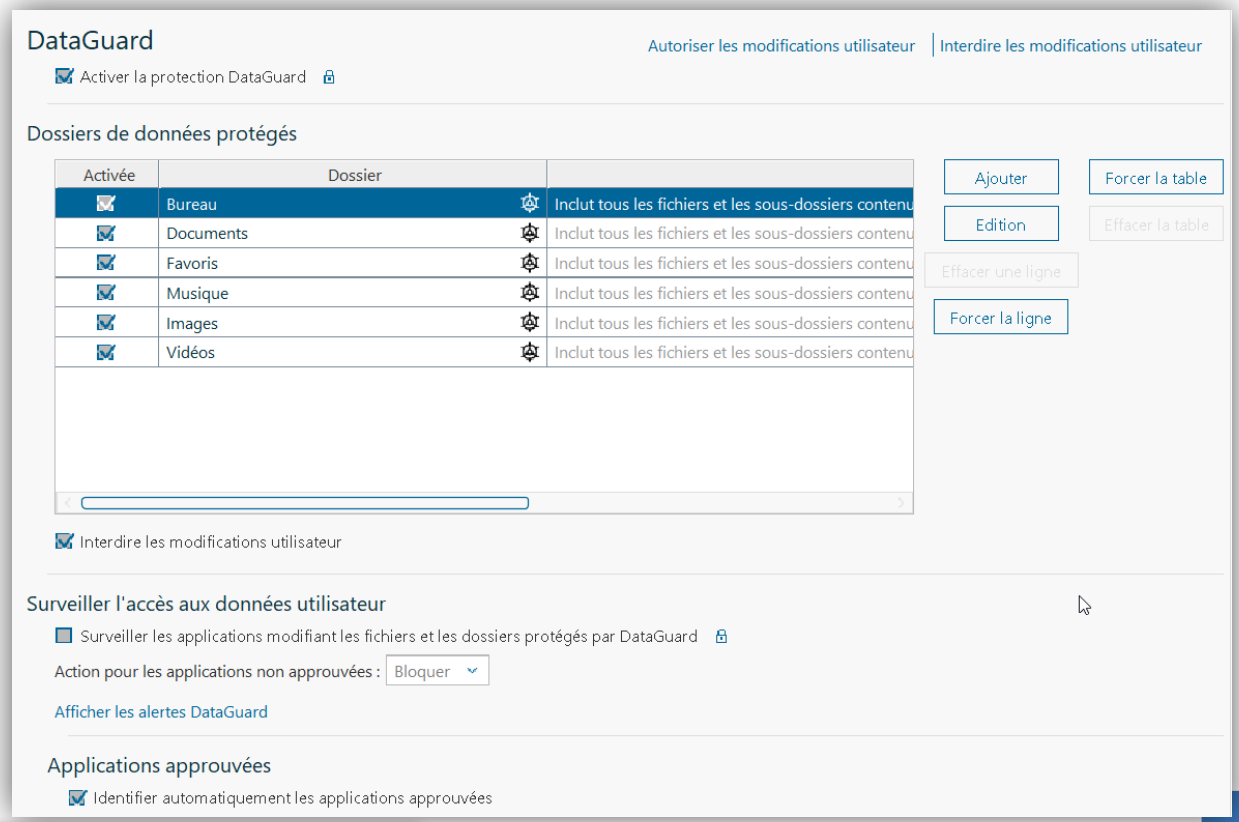
# Configuration DataGuard

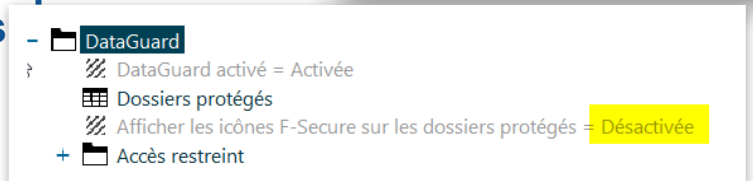
**« DataGuard » bloque les ransomwares inconnus**

**En environnement non sensible (hors ZRR), DataGuard peut être activé**

**Cette fonctionnalité repose sur « DeepGuard » et « Security Cloud ». L'utilisation est donc à adapter en conséquence**

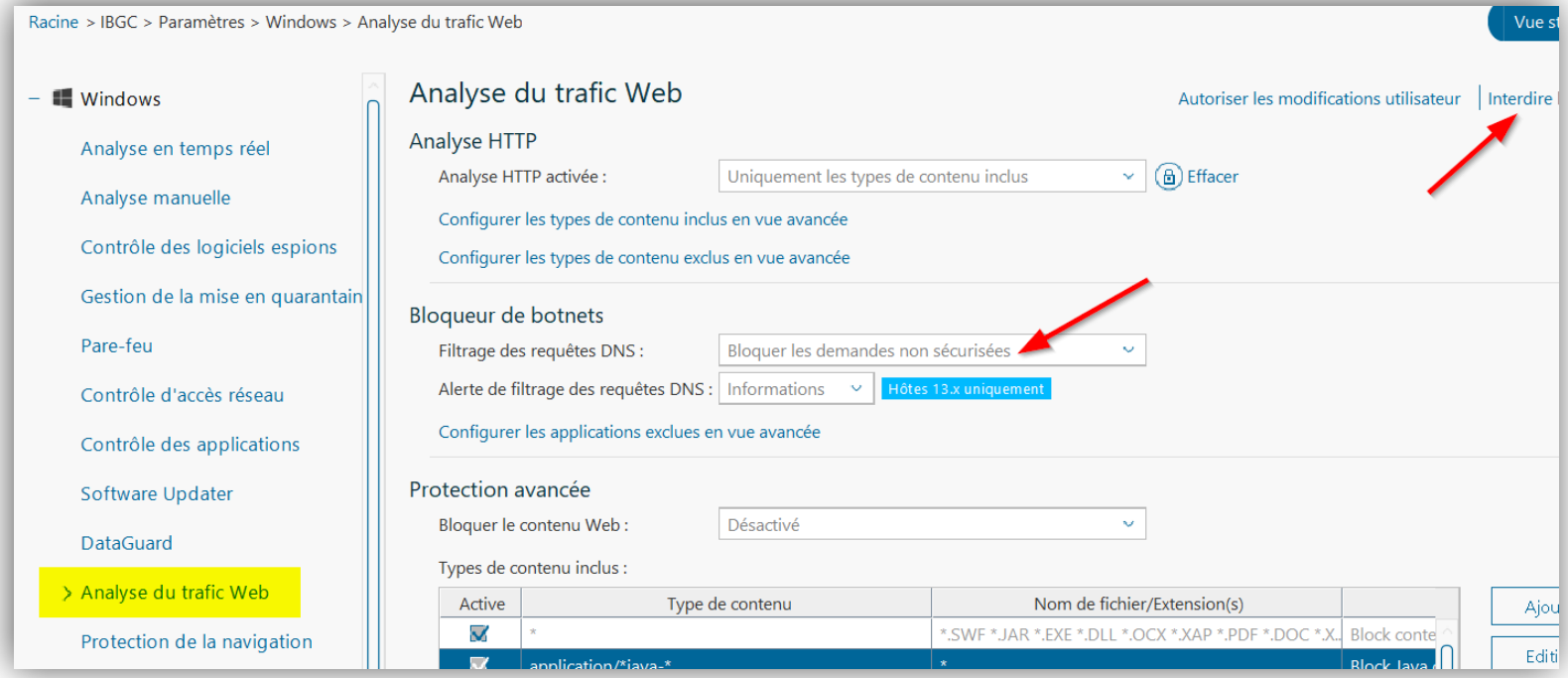
**En vue avancée décochez les icônes sur les dossiers pour ne pas perturber les utilisateurs**



# Configuration
# Analyse du trafic Web

**L'activation du « bloqueur de botnets » est recommandée dans les environnements non sensibles car celle-ci est dépendante de l'activation de « Security Cloud ».**

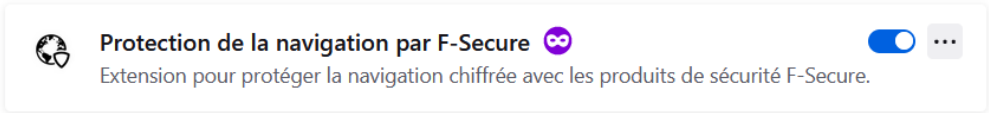


# Configuration
# Protection de la navigation

**Cette fonctionne repose sur l'installation de plugins navigateurs web**

**Ces plugins ne peuvent pas être déployés au travers de la solution WithSecure**

**Le blocage des sites web suspects entraine de nombreux faux positifs**

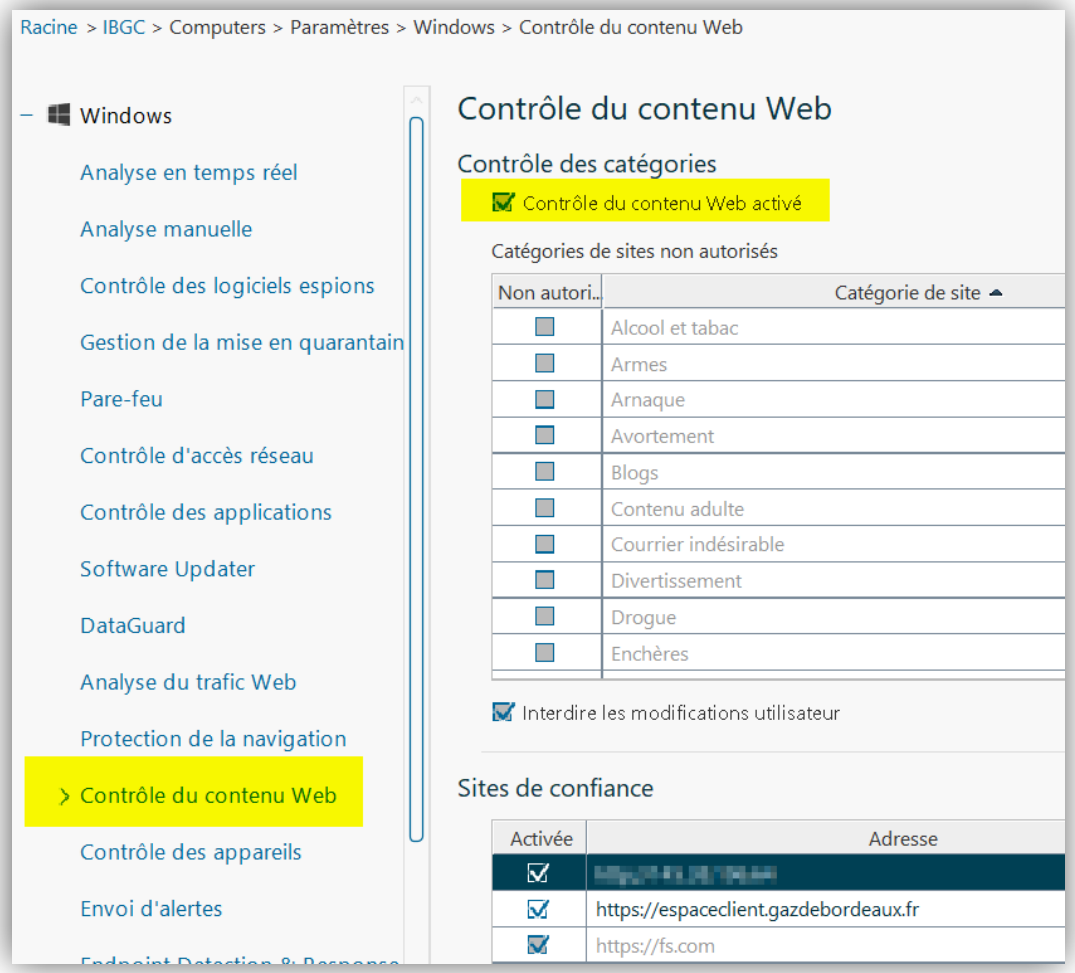



# Configuration
# Contrôle du contenu Web

**Le contrôle du contenu Web utilise les données d'analyse de réputation F-Secure pour classer les sites par catégories et bloquer l'accès en cas de contenu défini dans la stratégie.**

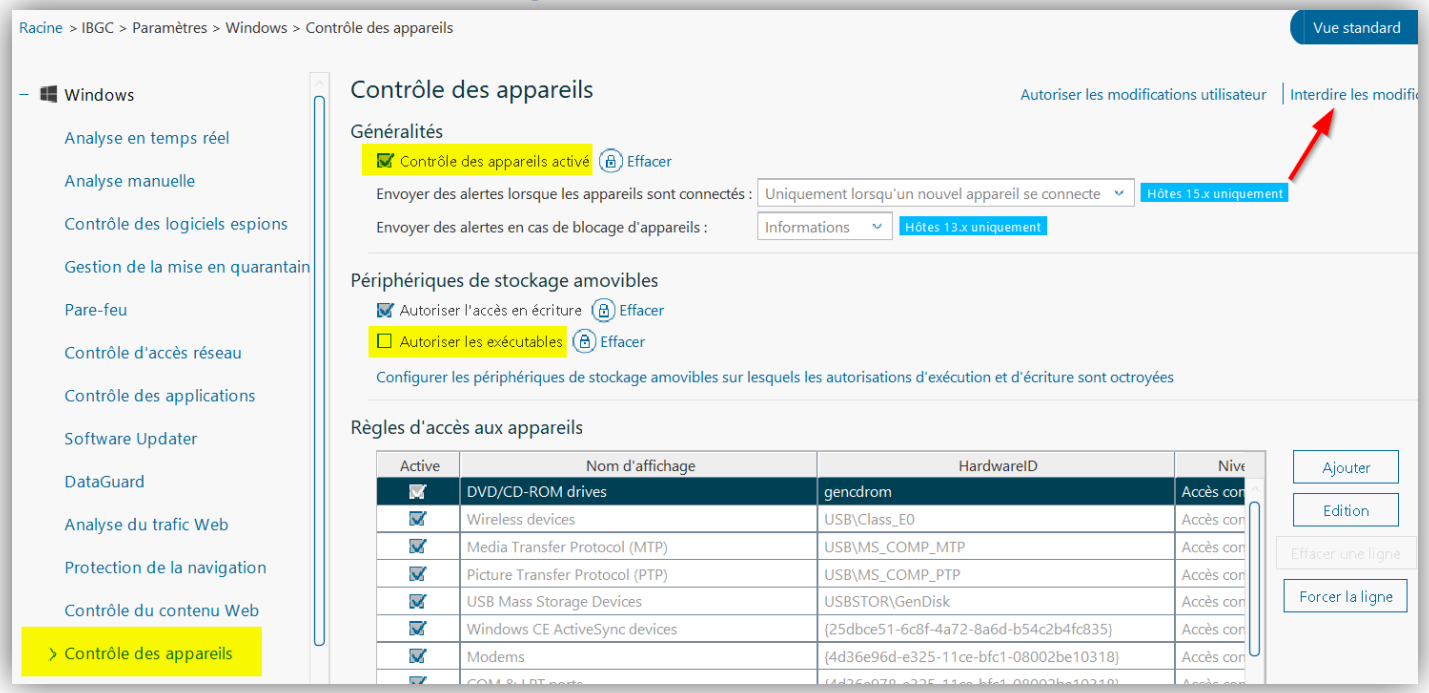
**Lorsque des sites sont bloqués sans raison valable, vous pouvez ajouter une exception « Site de confiance ».**

**Débloque aussi dans la protection de la navigation**



# Configuration
# Contrôle des appareils

**Il est recommandé d'activer le contrôle des appareils et d'interdire le lancement d'exécutables depuis un stockage amovible**

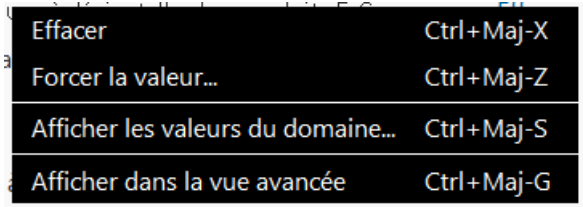


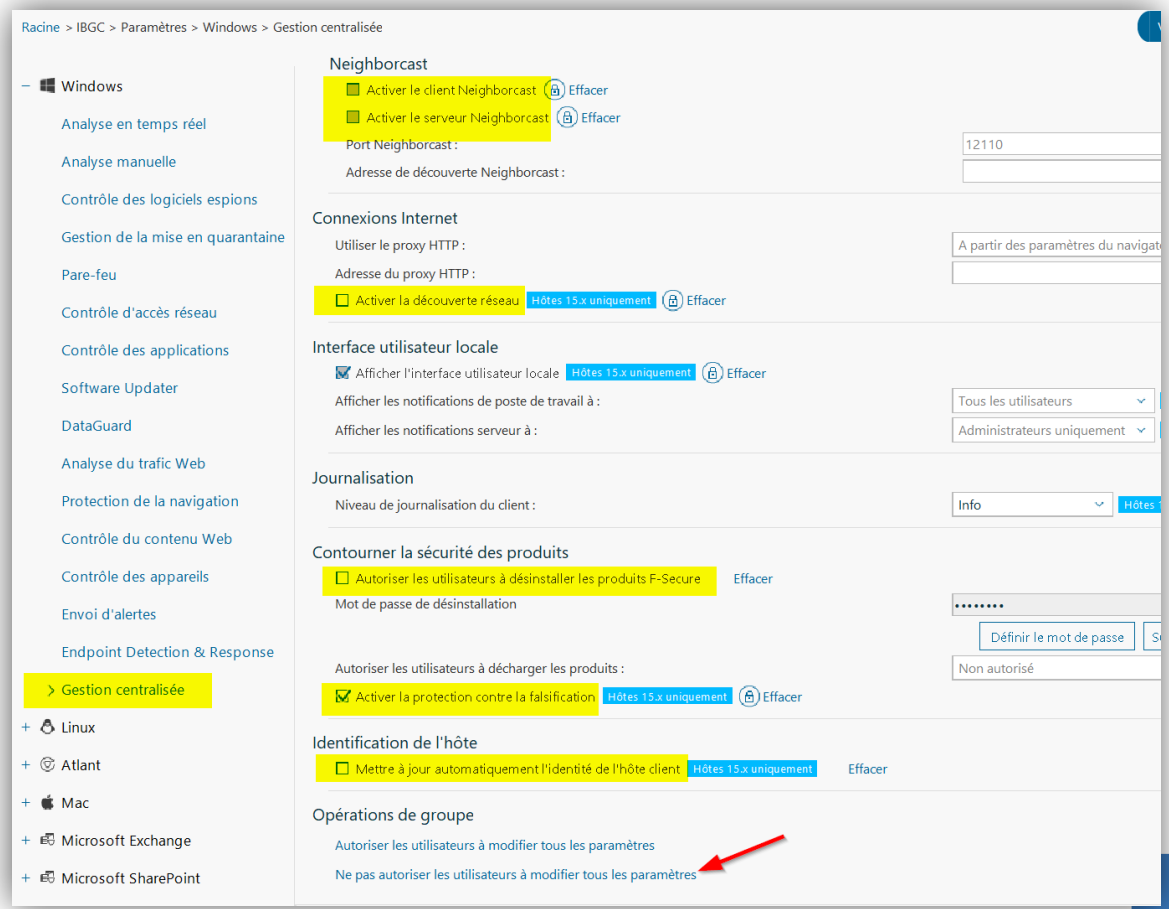
# Configuration
# Gestion centralisée

**Neighborcast doit être désactivé sur recommandation du CNRS.**

**Il permet aux hôtes gérés de télécharger leurs mises à jour entre eux, outre le téléchargement depuis les serveurs ou proxys existants**

**Un clic droit permet d'afficher un menu contextuel**



## Liens web

https://help.f-secure.com/product.html#business/policy-manager/15.30/fr/

https://securite-si.cnrs.fr/consignes/systèmes/antimalware/

**Rejoignez le Groupe de travail antivirus de RAISIN !**

**www.cnrs.fr**