

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

Echier Edition Afficher Outils Aide

Tableau de bord Paramètres État Mises à jour logicielles Alertes Analyse des rapports Installation Active Directory Opérations Exploration de données

Hôtes hors de l'arborescence de domaine

En attente (0)
Non gérés (0)

Arborescence de domaine

- Racine
- IBGC
 - Computers
 - Old Computers
 - Servers
 - No restriction
 - Proxy
 - fsecure-pmp-dmz
 - fsecure-pmp.ibgc

Racine > Tableau de bord

Tableau de bord

17 mars 2023
02:02:28

CPU: 0%

Hôtes en attente (0)
Hôtes non gérés (0)

- Notifications par e-mail
- Rapport planifié
- Transfert des alertes
- Active Directory
- Proxy Policy Manager

POLICY MANAGER 15.30

Version : 2023-03-16_16
Date de version : 17 mars 2023 00:36
[Afficher les détails](#)

16,4 Go

16,5 Go de libre

123 Go

Réinitialiser

Tous les Vendredi après 22:00
Dernière exécution le 10 mars 2023
[Configurer la sauvegarde](#)

10 mars 2023

ÉVÉNEMENTS DE SERVEUR, DERNIÈRES 24 H

définitions

- 01:30 Définitions de virus Nouveau F-Secure Aquarius 2023-03-16_16
- 01:00 Définitions de virus Nouveau F-Secure Aquarius 2023-03-16_15
- 21:30(-1) Définitions de virus Nouveau F-Secure Aquarius 2023-03-16_14
- 21:00(-1) Définitions de virus Nouveau F-Secure Aquarius 2023-03-16_13
- 19:40(-1) Définitions de virus Nouveau F-Secure Hydra 2023-03-16_02
- 19:10(-1) Définitions de virus Nouveau F-Secure Aquarius 2023-03-16_12
- 18:40(-1) Définitions de virus Nouveau F-Secure Aquarius 2023-03-16_11
- 16:50(-1) Définitions de virus Nouveau F-Secure HIPS-N 2023-03-16_01

Ne jamais modifier les paramètres de la racine

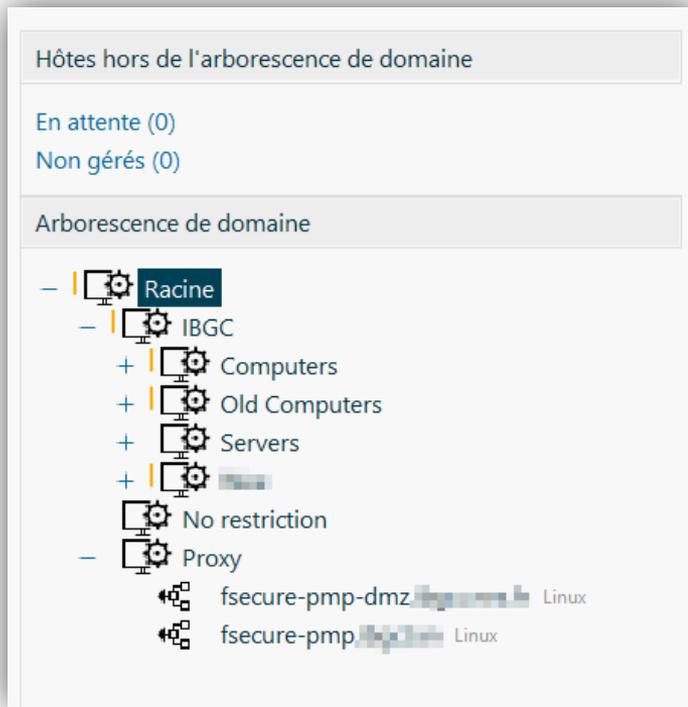
Toujours commencer par créer un nouveau domaine de stratégie à la racine

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

The screenshot displays the F-Secure management console interface. On the left, the 'Arborescence de domaine' (Domain tree) shows a hierarchy starting with 'Racine' (Root), followed by 'IBGC', and then sub-domains like 'Computers', 'Old Computers', 'Servers', 'No restriction', and 'Proxy'. A red arrow points to the 'IBGC' domain. The main panel shows the configuration for 'Analyse en temps réel' (Real-time analysis) under 'Paramètres' (Parameters) > 'Windows' > 'Analyse en temps réel'. The 'Généralités' (General) section includes checkboxes for 'Activer l'analyse en temps réel' (checked), 'Utiliser Security Cloud', and 'Activer l'interface d'analyse anti-programmes malveillants (AMS)'. Each checkbox has an 'Effacer' (Reset) button. A red arrow points to the 'Effacer' button for 'Activer l'analyse en temps réel'. The 'Fichiers à analyser' (Files to analyze) section shows a list of file extensions to be analyzed, with 'Effacer' buttons for each. A red arrow points to the 'Effacer' button for the first extension, 'BOO HLP TD0 TT6 MSG ASD JSE VBE WSC CHM EML PRC SHB LNK WSF (* PDF ZL? XML ANI BAT CMD DOC DOT JOB LSP MHT PHP PPT SWF WMA WMV WMF WRI XLS XLT CLASS DOXC DOCM DOTX DOTM DOCB XLSX XLSM XLTX XLTM XLSB XLAM PPTX PPTM POTX POTM PPAM PPSX PPSM SLDX SLDM PUB)'. The top navigation bar includes 'Tableau de bord', 'Paramètres', 'État', 'Mises à jour logicielles', 'Alertes', 'Analyse des rapports', 'Installation', 'Active Directory', 'Opérations', and 'Exploration de données'. The breadcrumb trail is 'Racine > IBGC > Paramètres > Windows > Analyse en temps réel'.

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 :

- Client F-Secure Security Cloud 1.25, 15.30
 - Paramètres
 - /// Autoriser une analyse approfondie = Non
 - /// Le client est activé = Oui
 - /// Proxy HTTP

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

The screenshot shows the 'Analyse en temps réel' (Real-time analysis) configuration window. At the top right, there are links for 'Autoriser les modifications utilisateur' and 'Interdire'. The 'Généralités' (General) section includes three checked options: 'Activer l'analyse en temps réel' (with an 'Effacer' button), 'Utiliser Security Cloud' (highlighted in yellow, with an 'Effacer' button), and 'Activer l'interface d'analyse anti-programmes malveillants (AMSI)' (with a 'Hôtes 15.x uniquement' label and an 'Effacer' button). The 'Fichiers à analyser' (Files to analyze) section has a dropdown for 'Fichiers à analyser' set to 'Fichiers avec ces extensions', and a list of 'Extensions incluses' including COM, EXE, SYS, OV?, BIN, SCR, DLL, SHS, HTM, HTML, HTT, VBS, JS, INF, VXD, DO?, XL?, RTF, CPL, WIZ, HTA, PP?, PWZ, POT, MSO, PIF, ACM, ASP, AX, CNV, CSC, DRV, INI, MDB, MPD, MPP, MPT, OBD, OCK, PCI, TLB, TSP, WBK, WBT, WPC, WSH, VWP, WML, BOO, HLP, TDO, TT6, MSG, ASD, JSE, VBE, WSC, CHM, EML, PRC, SHB, LNK, WSF, *. Below this is an unchecked option 'Ne pas analyser les fichiers portant les extensions suivantes' (with an 'Effacer' button) and an empty 'Extensions exclues' field (with an 'Effacer' button). The 'Fichiers et applications exclus de l'analyse' (Files and applications excluded from analysis) section has an unchecked option 'Ne pas analyser les fichiers et les applications suivants' (with an 'Effacer' button). Below this is a table with columns: 'Activé', 'Type', 'Exclusion', 'Étendue d'exclusion', and 'Ajouter'. The table is currently empty. At the bottom, there is an unchecked option 'Empêcher les utilisateurs d'ajouter des exclusions aux analyses' (with an 'Effacer' button).

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

Racine > IBGC > Paramètres > Windows > Analyse en temps réel

Windows

- Analyse en temps réel
- Analyse manuelle
- Contrôle des logiciels espions
- Gestion de la mise en quarantaine
- Pare-feu
- Contrôle d'accès réseau
- Contrôle des applications
- Software Updater
- DataGuard
- Analyse du trafic Web
- Protection de la navigation
- Contrôle du contenu Web
- Contrôle des appareils
- Envoi d'alertes
- Endpoint Detection & Response

Analyser les lecteurs réseau connectés

- Activer l'analyse des lecteurs réseau
- Mode d'analyse : Analyser les fichiers exécutés

Actions en cas de détection de programmes malveillants (postes de travail)

- Décider automatiquement
- Action personnalisée sur l'infection : Mettre automatiquement en quarantaine

Actions en cas de détection de logiciels espions/programmes à risque (postes de travail)

- Action personnalisée sur les programmes à risque : Mettre automatiquement en quarantaine
- Action personnalisée sur les logiciels espions : Mettre automatiquement en quarantaine

Actions en cas de détection de programmes malveillants (serveurs Windows)

- Décider automatiquement
- Action personnalisée sur l'infection : Mettre automatiquement en quarantaine

Actions en cas de détection de logiciels espions/programmes à risque (serveurs Windows)

- Action personnalisée sur les programmes à risque : Mettre automatiquement en quarantaine
- Action personnalisée sur les logiciels espions : Mettre automatiquement en quarantaine

DeepGuard

- Activer DeepGuard
- Bloquer les fichiers rares et suspects

Configuration

Analyse manuelle

Tableau de bord Paramètres État Mises à jour logicielles Alertes Analyse des rapports Installation Active Directory

Racine > IBGC > Computers > Paramètres > Windows > Analyse manuelle

Windows

- Analyse en temps réel
- > Analyse manuelle
- Contrôle des logiciels espions
- Gestion de la mise en quarantaine
- Pare-feu
- Contrôle d'accès réseau
- Contrôle des applications
- Software Updater
- DataGuard
- Analyse du trafic Web
- Protection de la navigation
- Contrôle du contenu Web

Analyse manuelle

Autoriser les m...

Analyse des fichiers

Fichiers à analyser : Fichiers avec extensions connues uniquement 

Extensions incluses : WMF WRI XLS XLT CLASS DOCX DOCM DOTX DOTM DOCB XLSX XLSM XLTX XLTM XLSB XLAM PPTX PPTM POTX POTM PPAM PPSX PPSM SLDX SLDM PUB A3X ? TBZ TBZ2 ACE UUE XZ Z R?? O?? CNM ZIP 7Z JAR ARJ LZH TAR TGZ GZ CAB RAR BZ2

Analyser le contenu des fichiers compressés (zip, arj, lzh,...) 

Activer les extensions exclues 

Extensions exclues : 

Activer les dossiers et les fichiers exclus 

Configurer les fichiers et les dossiers exclus de l'analyse manuelle

Action sur l'infection : Mettre automatiquement en quarantaine 

Demander aux utilisateurs d'analyser les périphériques USB Hôtes 15.x uniquement 

Analyse planifiée

Nom	Paramètres de planification	Type de tâche	Paramètres spéc
Schedu...	/t18:00 /ti30 /b2022-20-06 /rweekly	Analyser les lecteurs locaux	

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

Tableau de bord Paramètres État Mises à jour logicielles Alertes Analyse des rapports Installation Active Directory Opérations Exploration de données

Racine > IBGC > Paramètres > Windows > Gestion de la mise en quarantaine

Vue standard Vue avancée

Windows

- Analyse en temps réel
- Analyse manuelle
- Contrôle des logiciels espions
- > Gestion de la mise en quarantaine
- Pare-feu
- Contrôle d'accès réseau

Gestion de la mise en quarantaine

Autoriser les modifications utilisateur | **Interdire les modifications utilisateur**

Généralités

Permettre aux utilisateurs de libérer des éléments de la quarantaine Effacer

Mot de passe de libération :

Définir le mot de passe Supprimer le mot de passe

Contenu mis en quarantaine

Type de logiciel malveillant	Nom du logiciel malveillant ▲	Chemin d'accès au fichier
(Empty area circled in red)		

Libérer
Supprimer

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)

Racine > IBGC > Paramètres > Windows > Pare-feu

Windows

- Analyse en temps réel
- Analyse manuelle
- Contrôle des logiciels espions
- Gestion de la mise en quarantaine
- > Pare-feu**
- Contrôle d'accès réseau
- Contrôle des applications
- Software Updater
- DataGuard
- Analyse du trafic Web
- Protection de la navigation
- Contrôle du contenu Web
- Contrôle des appareils
- Envoi d'alertes
- Endpoint Detection & Response
- Protection centralisée

Profil d'hôte de la station de travail : Office, NO file and printer sharing between computers (Effacer)

Profil d'hôte du serveur : Server (Effacer)

Sélectionner automatiquement le profil du pare-feu pour les stations de travail (Effacer)

Configurer la sélection automatique des profils du pare-feu pour les stations de travail

Profil en cours de modification : Office, NO file and printer sharing between computers (Mon étendue) (Cloner) (Renommer) (Supprimer)

Modification : Office, NO file and printer sharing between computers

Informer l'utilisateur lorsque le pare-feu bloque une nouvelle application

Ignorer toutes les règles de pare-feu qui ne sont pas répertoriées dans ce profil

Règles par défaut

Bloquer toutes les connexions entrantes

Connexions entrantes inconnues : Bloquer

Connexions sortantes inconnues : Bloquer

Règles de pare-feu

Activé	Nom	Type	Services	Hôtes distants
<input checked="" type="checkbox"/>	Allow all outbound traffic	Autoriser	[sortant] : TCP (6) [sortant] : UDP (17)	Tout hôte distant
<input checked="" type="checkbox"/>	Allow commonly needed ICMP messages	Autoriser	[sortant] : Ping [entrant] : ICMP restricted [entrant] : ICMPv6 restricted in [sortant] : ICMPv6 restricted out	Tout hôte distant
<input checked="" type="checkbox"/>	Block inbound computer browsing and file sharing	Bloquer	[entrant] : SMB (TCP) [entrant] : SMB (UDP) [entrant] : Windows Networking (1) [entrant] : Windows Networking (2)	Tout hôte distant

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

Racine > IBGC > Paramètres > Windows > Contrôle des applications

Vue standard

Windows

- Analyse en temps réel
- Analyse manuelle
- Contrôle des logiciels espions
- Gestion de la mise en quarantaine
- Pare-feu
- Contrôle d'accès réseau
- > Contrôle des applications
- Software Updater
- DataGuard
- Analyse du trafic Web
- Protection de la navigation

Contrôle des applications

Hôtes 14.x/15.x uniquement

Autoriser les modifications utilisateur | Interdire les modifications

Activer le contrôle des applications Effacer

Profil d'hôte : Default Effacer

Afficher les alertes de contrôle des applications

Profil en cours de modification : Default (Prédéfinie) Cloner Renommer Supprimer

Modification : Default

Règle par défaut appliquée aux applications non approuvées: Autoriser

Règles d'exclusion

Actif	Nom	Action	Événement	Conditions	
<input type="checkbox"/>	Block potentially unwanted applications in Temp folder	Bloquer	Exécuter l'application	Chemin d'accès de la cible, Ré...	Preven...
<input type="checkbox"/>	Block rare and unknown applications in Temp folder	Bloquer	Exécuter l'application	Chemin d'accès de la cible, Ré...	Preven...
<input type="checkbox"/>	Block potentially unwanted applications in Downloads folder	Bloquer	Exécuter l'application	Chemin d'accès de la cible, Ré...	Preven...
<input type="checkbox"/>	Block rare and unknown applications in Downloads folder	Bloquer	Exécuter l'application	Chemin d'accès de la cible, Ré...	Preven...
<input type="checkbox"/>	Block batch scripts started by Microsoft Office applications	Bloquer	Démarrer le process...	Chemin d'accès parent, Ligne ...	Preven...
<input type="checkbox"/>	Block powershell scripts started by Microsoft Office	Bloquer	Démarrer le process...	Chemin d'accès parent, Ligne ...	Preven...

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

Racine > IBGC > Paramètres > Windows > Software Updater

Windows

- Analyse en temps réel
- Analyse manuelle
- Contrôle des logiciels espions
- Gestion de la mise en quarantaine
- Pare-feu
- Contrôle d'accès réseau
- Contrôle des applications
- > Software Updater**
- DataGuard
- Analyse du trafic Web
- Protection de la navigation
- Contrôle du contenu Web

Software Updater

Autoriser les modifications utilisateur | Interdire

Généralités

- Activer Software Updater [Effacer](#)
- Télécharger les mises à jour logicielles depuis Policy Manager : Si possible [Effacer](#)
- Priorité d'analyse : Arrière-plan [Hôtes 15.x uniquement](#) [Effacer](#)
- Afficher les options de Software Updater aux utilisateurs [Hôtes 15.x uniquement](#) [Effacer](#)
- Action lorsque l'application est en cours d'exécution : Annuler l'installation
- M'informeur de l'installation

Installation automatique

- Installer les mises à jour automatiquement : Toutes celles de sécurité [Effacer](#)
- Installer tous les : Jour [Effacer](#)
- Heure d'installation : 13:00 [Effacer](#)
- Redémarrer après installation : Demander à l'utilisateur
- Forcer le redémarrage dans : 1 jours 0 heures 0 min. 0 s
- Exécuter la tâche même si un démarrage planifié est manqué [Effacer](#)
- Autoriser la poursuite de l'installation des mises à jour logicielles avant le redémarrage [Effacer](#)

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

- **DataGuard**
- DataGuard activé = Activée
- Dossiers protégés
- Afficher les icônes F-Secure sur les dossiers protégés = Désactivée
- + Accès restreint

DataGuard

Autoriser les modifications utilisateur | Interdire les modifications utilisateur

Activer la protection DataGuard

Dossiers de données protégés

Activée	Dossier	
<input checked="" type="checkbox"/>	Bureau	Inclut tous les fichiers et les sous-dossiers contenu
<input checked="" type="checkbox"/>	Documents	Inclut tous les fichiers et les sous-dossiers contenu
<input checked="" type="checkbox"/>	Favoris	Inclut tous les fichiers et les sous-dossiers contenu
<input checked="" type="checkbox"/>	Musique	Inclut tous les fichiers et les sous-dossiers contenu
<input checked="" type="checkbox"/>	Images	Inclut tous les fichiers et les sous-dossiers contenu
<input checked="" type="checkbox"/>	Vidéos	Inclut tous les fichiers et les sous-dossiers contenu

Interdire les modifications utilisateur

Surveiller l'accès aux données utilisateur

Surveiller les applications modifiant les fichiers et les dossiers protégés par DataGuard

Action pour les applications non approuvées :

[Afficher les alertes DataGuard](#)

Applications approuvées

Identifier automatiquement les applications approuvées

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 ».

Racine > IBGC > Paramètres > Windows > Analyse du trafic Web

Windows

- Analyse en temps réel
- Analyse manuelle
- Contrôle des logiciels espions
- Gestion de la mise en quarantaine
- Pare-feu
- Contrôle d'accès réseau
- Contrôle des applications
- Software Updater
- DataGuard
- > Analyse du trafic Web**
- Protection de la navigation

Analyse du trafic Web

Autoriser les modifications utilisateur | Interdire

Analyse HTTP

Analyse HTTP activée : Uniquement les types de contenu inclus Effacer

Configurer les types de contenu inclus en vue avancée

Configurer les types de contenu exclus en vue avancée

Bloqueur de botnets

Filtrage des requêtes DNS : Bloquer les demandes non sécurisées

Alerte de filtrage des requêtes DNS : Informations Hôtes 13.x uniquement

Configurer les applications exclues en vue avancée

Protection avancée

Bloquer le contenu Web : Désactivé

Types de contenu inclus :

Active	Type de contenu	Nom de fichier/Extension(s)	
<input checked="" type="checkbox"/>	*	*.SWF *.JAR *.EXE *.DLL *.OCX *.XAP *.PDF *.DOC *.X...	Block conte...
<input checked="" type="checkbox"/>	application/*java-*	*	Block Java...

Ajout...

Éditi...

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 entraîne de nombreux faux positifs

Racine > IBGC > Paramètres > Windows > Protection de la navigation

Windows

- Analyse en temps réel
- Analyse manuelle
- Contrôle des logiciels espions
- Gestion de la mise en quarantaine
- Pare-feu
- Contrôle d'accès réseau
- Contrôle des applications
- Software Updater
- DataGuard
- Analyse du trafic Web
- > Protection de la navigation
- Contrôle du contenu Web

Protection de la navigation

Autoriser l

Généralités

- Protection de la navigation activée 

Protection en fonction de la réputation

- Bloquer les sites Web dangereux 
- Bloquer les sites Web suspects Hôtes 14.x/15.x uniquement 
- Bloquer les sites Web interdits Hôtes 14.x/15.x uniquement 
- Activer le mode SafeSearch Hôtes 15.x uniquement 
- Afficher les classements des résultats de moteur de recherche (Google, Yahoo, etc.) 
- Autoriser les utilisateurs à accéder aux pages bloquées 

Contrôle de la connexion

- Contrôle de la connexion activé 
- Déconnecter les applications non approuvées 
- Déconnecter les outils de scripts et en ligne de commande Hôtes 15.x uniquement 
- Effacer le contenu du Presse-papiers après les sessions bancaires 
- Bloquer l'accès à distance pendant une session de banque en ligne Hôtes 15.x uniquement 



Protection de la navigation par F-Secure 

Extension pour protéger la navigation chiffrée avec les produits de sécurité F-Secure.



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

Racine > IBGC > Computers > Paramètres > Windows > Contrôle du contenu Web

Windows

- Analyse en temps réel
- Analyse manuelle
- Contrôle des logiciels espions
- Gestion de la mise en quarantaine
- Pare-feu
- Contrôle d'accès réseau
- Contrôle des applications
- Software Updater
- DataGuard
- Analyse du trafic Web
- Protection de la navigation
- > Contrôle du contenu Web
- Contrôle des appareils
- Envoi d'alertes
- Endpoint Detection & Response

Contrôle du contenu Web

Contrôle des catégories

Contrôle du contenu Web activé

Catégories de sites non autorisés

Non autori...	Catégorie de site ▲
<input type="checkbox"/>	Alcool et tabac
<input type="checkbox"/>	Armes
<input type="checkbox"/>	Arnaque
<input type="checkbox"/>	Avortement
<input type="checkbox"/>	Blogs
<input type="checkbox"/>	Contenu adulte
<input type="checkbox"/>	Courrier indésirable
<input type="checkbox"/>	Divertissement
<input type="checkbox"/>	Drogue
<input type="checkbox"/>	Enchères

Interdire les modifications utilisateur

Sites de confiance

Activée	Adresse
<input checked="" type="checkbox"/>	https://www.f-s.com
<input checked="" type="checkbox"/>	https://espaceclient.gazdebordeaux.fr
<input checked="" type="checkbox"/>	https://fs.com

Configuration

Contrôle des appareils

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

Racine > IBGC > Paramètres > Windows > Contrôle des appareils

Vue standard

Windows

- Analyse en temps réel
- Analyse manuelle
- Contrôle des logiciels espions
- Gestion de la mise en quarantaine
- Pare-feu
- Contrôle d'accès réseau
- Contrôle des applications
- Software Updater
- DataGuard
- Analyse du trafic Web
- Protection de la navigation
- Contrôle du contenu Web
- > Contrôle des appareils

Contrôle des appareils

Autoriser les modifications utilisateur | Interdire les modifications

Généralités

- Contrôle des appareils activé [Effacer](#)
- Envoyer des alertes lorsque les appareils sont connectés : Uniquement lorsqu'un nouvel appareil se connecte [Hôtes 15.x uniquement](#)
- Envoyer des alertes en cas de blocage d'appareils : Informations [Hôtes 13.x uniquement](#)

Périphériques de stockage amovibles

- Autoriser l'accès en écriture [Effacer](#)
- Autoriser les exécutables [Effacer](#)

Configurer les périphériques de stockage amovibles sur lesquels les autorisations d'exécution et d'écriture sont octroyées

Règles d'accès aux appareils

Active	Nom d'affichage	HardwareID	Niveau
<input checked="" type="checkbox"/>	DVD/CD-ROM drives	gencdrom	Accès complet
<input checked="" type="checkbox"/>	Wireless devices	USB\Class_E0	Accès complet
<input checked="" type="checkbox"/>	Media Transfer Protocol (MTP)	USB\MS_COMP_MTP	Accès complet
<input checked="" type="checkbox"/>	Picture Transfer Protocol (PTP)	USB\MS_COMP_PTP	Accès complet
<input checked="" type="checkbox"/>	USB Mass Storage Devices	USBSTOR\GenDisk	Accès complet
<input checked="" type="checkbox"/>	Windows CE ActiveSync devices	{25dbce51-6c8f-4a72-8a6d-b54c2b4fc835}	Accès complet
<input checked="" type="checkbox"/>	Modems	{4d36e96d-e325-11ce-bfc1-08002be10318}	Accès complet
<input checked="" type="checkbox"/>	COM & LPT ports	{4d36e978-e325-11ce-bfc1-08002be10318}	Accès complet

[Ajouter](#)
[Edition](#)
[Effacer une ligne](#)
[Forcer la ligne](#)

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

Effacer	Ctrl+Maj-X
Forcer la valeur...	Ctrl+Maj-Z
Afficher les valeurs du domaine...	Ctrl+Maj-S
Afficher dans la vue avancée	Ctrl+Maj-G

Racine > IBGC > Paramètres > Windows > Gestion centralisée

- Windows
 - Analyse en temps réel
 - Analyse manuelle
 - Contrôle des logiciels espions
 - Gestion de la mise en quarantaine
 - Pare-feu
 - Contrôle d'accès réseau
 - Contrôle des applications
 - Software Updater
 - DataGuard
 - Analyse du trafic Web
 - Protection de la navigation
 - Contrôle du contenu Web
 - Contrôle des appareils
 - Envoi d'alertes
 - Endpoint Detection & Response
 - > Gestion centralisée**
- Linux
- Atlant
- Mac
- Microsoft Exchange
- Microsoft SharePoint

Neighborcast

- Activer le client Neighborcast **Hôtes 15.x uniquement** Effacer
- Activer le serveur Neighborcast **Hôtes 15.x uniquement** Effacer
- Port Neighborcast : 12110
- Adresse de découverte Neighborcast :

Connexions Internet

- Utiliser le proxy HTTP : A partir des paramètres du navigateur
- Adresse du proxy HTTP :
- Activer la découverte réseau **Hôtes 15.x uniquement** Effacer

Interface utilisateur locale

- Afficher l'interface utilisateur locale **Hôtes 15.x uniquement** Effacer
- Afficher les notifications de poste de travail à : Tous les utilisateurs
- Afficher les notifications serveur à : Administrateurs uniquement

Journalisation

- Niveau de journalisation du client : Info **Hôtes**

Contourner la sécurité des produits

- Autoriser les utilisateurs à désinstaller les produits F-Secure Effacer
- Mot de passe de désinstallation :
- Définir le mot de passe
- Non autorisé
- Autoriser les utilisateurs à télécharger les produits :
- Activer la protection contre la falsification **Hôtes 15.x uniquement** Effacer

Identification de l'hôte

- Mettre à jour automatiquement l'identité de l'hôte client **Hôtes 15.x uniquement** Effacer

Opérations de groupe

- Autoriser les utilisateurs à modifier tous les paramètres
- Ne pas autoriser les utilisateurs à modifier tous les paramètres**

Liens web

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

<https://securite-si.cnrs.fr/consignes/systemes/antimalware/>



Rejoignez le Groupe de travail antivirus de RAISIN !

www.cnrs.fr