PSB & PM BEST PRATICES #1

F-SECURE DEEPGUARD AND EXTENSIONS

F-Secure Business Suite and Protection Service for Business can offer the best protection in the market – if they are configured correctly. Two common questions relate to setting DeepGuard and file extensions to ensure that efficient malware protection is available and that proper files are examined.

1. Ensure that DeepGuard is set properly

The importance of keeping **DeepGuard** enabled cannot be stressed enough. DeepGuard is extremely sophisticated technology, relying on heuristic, behavior, and reputation analysis to provide an exceptionally important layer of security, and disabling it or is components should never be the valid choice.

You can enable DeepGuard in the **Profiles** (PSB Portal) or **Policy Settings** (PM):

1) In **Policy Manager**, or **PSB Portal**, edit the used policy or profile.
2) Open **Real-Time Scanning**. (Ensure that **Real-time scanning** is enabled.)
3) Enable **DeepGuard**.
4) Preferably set **Action on system…** to **Automatic: Do Not Ask**.
5) Enable **Use Server Queries to Improve Detection Accuracy**. This setting is essential for the functioning of DeepGuard, allowing DeepGuard to check file reputations from F-Secure Security Cloud. The queries are anonymous and encrypted.
6) Ensure that **Advanced Process Monitoring** is enabled. Advanced Process Monitoring provides extremely important functionalities for DeepGuard, enhancing its reliability severely. In some rare cases, software such as some DRM applications may be incompatible with Advanced Process Monitoring, but in all other cases it should be turned on.

Important: Remember to **lock** the settings so that users cannot disable **DeepGuard**.

2. In Policy Manager, check that extensions are not locked at root

In Business Suite environments, in many cases, the extensions that define files included in real-time scanning have been locked on the **root** level in **Policy Manager**.

However, this should not be done, as locking the settings on the root level prevents the **Client Security** installers from updating the list with new extensions.

Instead, the setting should be locked on the **policy domain** level. That is, one level from the default or root level.

To ensure that you have not locked the included extensions on the root level:

1) In **Policy Manager**, select **root** and **Settings**.
2) Open **Real-Time Scanning**. (Ensure that **Real-time scanning enabled** is checked.)
3) Check that **Files to scan** is marked as **Files with These Extensions**.
4) Check that the lock icon next to **Included extensions** is marked as **Allow user changes**.

Important: After unlocking the **Included extensions** at the root level, remember to lock them on the policy domain level!

Note: Note that this applies only to Business Suite environments; in Protection Service for Business environments, file extensions cannot be locked on the root (or *default.ser*) level.