Enabling and Using CryptoSafeGuard

CryptoSafeGuard is a new security feature in BackupAssist, designed to protect your backups from 'Crypto' variants of malware (widely known as 'ransomware'). This new feature is only available to installations with valid 'BackupCare' licensing. If your 'BackupCare' term has expired, CryptoSafeGuard will stop functioning.

The first time you run a job with CryptoSafeGuard enabled, it will scan files modified in the last 3 months looking for signs of a Crypto malware infection. Please be aware that this scan may take some time depending on the amount of data being backed up. Subsequent scans will be incremental and a lot faster, with minimal impact on the jobs' run times.

CryptoSafeGuard also has a per-job grace period to assist in the transition to ransomware detection. During the grace period, if a job detects possible ransomware, a warning will be displayed but the backup jobs will not be blocked. The grace period for a job lasts until the job has 3 consecutive clean scans.

Configuring CryptoSafeGuard in BackupAssist

To access the CryptoSafeGuard settings:

- Launch BackupAssist
- Select Settings
- Select CryptoSafeGuard

Important Note: *When your backup destination is a NAS or network share, it should be secured using best practice data security. This means only machines running BackupAssist and CryptoSafeGuard should have access to the folders that the backups are in, and those folders should only allow access to the Backup User Identity.*

Enabling or Disabling CryptoSafeGuard

CryptoSafeGuard is enabled by default and runs each time a backup job starts. You can disable or enable CryptoSafeGuard using the Settings tab.

Untick the box beside Enable CryptoSafeGuard protection to disable CryptoSafeGuard. Ticking this box will enable CryptoSafeGuard protection.

If CryptoSafeGuard is disabled, all jobs will be automatically unblocked, if they are currently blocked due to a potential ransomware infection.

SMS notifications

If you set up SMS notifications, SMS alerts will be sent when CryptoSafeGuard detects a possible ransomware infection.

SMS Number

Enter the phone number that is to receive the notifications into this field using the standard international phone number format "+<country code><mobile phone number>".

Detection Message

Enter an identifier or description for this machine. This is especially useful if you manage a lot of servers and need to know exactly which server the message has come from.

SMS Test

The SMS test button will become active once a phone number has been entered in the correct format. Click Test and a test message will be sent to that phone.

Manage Whitelist

The Manage Whitelist sections allow you to add, modify and delete whitelisted files, directories, and file extensions. Any files whitelisted in the CryptoSafeGuard alert dialog will automatically appear here.

If you respond to a CryptoSafeGuard alert by whitelisting files, you can review and change your whitelist using the Manage Whitelist section of the CryptoSafeGuard Settings dialog. You can also use this dialog to add to your whitelist without an alert, but it is recommended that you use the alert list to inform your whitelisting decisions.

Ignored File Paths

This field is used to manage **whitelisted files**. Use the Add button to browse to the file and add it, and the Remove button to remove the selected file from the list. Selecting Edit will allow you to manually edit the entry, or browse from the entries location. Select Save after making manual changes.

Ignored Directories

This field is used to manage **whitelisted directories**, which excludes all files inside the directory from the CryptoSafeGuard scan. Use the Add button to browse to the directory and add it, and the Remove button to remove the selected directory from the list. Selecting Edit will allow you to manually edit the entry, or browse from the entries location. Select Save after making manual changes.

Ignored File Extensions

This field is used to manage **whitelisted file extensions**, which excludes all files with that extension from the CryptoSafeGuard scan.

To add a file extension:

- Select Add
- Type the file extension. (**Do NOT include periods or wildcard symbols**. E.g. enter txt. Not .txt or *.txt.)

- Select Add.
- Repeat this process for each file extension. Do not enter multiple extensions as a single entry.
- Use the Remove button to remove the selected file extension from the list and the Edit option to edit an existing entry. Select Save after making manual changes.

Important Note: *Adding files and folders to the whitelist means they are excluded from CryptoSafeGuards' scan when a backup job starts. It is important to only whitelist files that create, or are expected to create, false positive responses when the scan runs.*