AvePoint®

AvePoint Compliance Guardian
FAQs for Technical Users

AvePoint Compliance Guardian

A comprehensive risk management solution ensuring information is available and accessible to the people who should have it and protected from the people who should not.

Questions	Answers
What services are used for this product? How is it installed/deployed?	Refer to this Visio diagram for architecture overview, services, exe processes, port numbers, and more.
How many install packages are there for the product? What components are part of each install package?	There will be two packages, Manager and Agent. If you are going to scan SharePoint Server, the Compliance Guardian Agent is required to be installed on all SharePoint Web-front-end servers.
What are the pre-requisites and system requirements for the install packages?	Please refer to the AvePoint Compliance Guardian Installation and Administration User Guide (Section: Preparations before the Installation).
What portion of the architecture gives us the GUI?	Compliance Guardian GUI is built based on Silverlight technology.
Does DocAve need to be installed when using Compliance Guardian?	The services of Compliance Guardian are completely separate from DocAve, and it does not require DocAve to be installed unless you are going to get SharePoint Auditor information from Risk Report in the Compliance Report.
Can Compliance Guardian, DocAve, and/or Governance Automation be installed on the same server?	Yes, Compliance Guardian can be installed on the server which is hosting DocAve or Governance Automation. There is no conflict between these products.
What is the basic communication path and method between the services?	Compliance Guardian services use WCF to communicate with each other.
How do we secure communication in Compliance Guardian?	All communications are encrypted using SSL.
What service is responsible for scanning content of the document?	The Compliance Guardian Engine is responsible for scanning the document based on the Test Suite.
What service is responsible for adding tags into the document?	Compliance Guardian Scanner adds tags into the document based on the scan results from the Compliance Guardian Engine.

Questions	Answers
What service is responsible for taking actions on the document?	The Compliance Guardian Scanner take actions on the document based on the Action Policy.
What databases does Compliance Guardian use and what is their purpose? Do you have any database sizing estimates?	There are three types of database roles used in Compliance Guardian. ● Control Database: It is created when installing Compliance Guardian Manager, and each Compliance Guardian Manager only has one Control Database. It is targeted to store all related scan job settings information (such as plan settings, schedule settings, job reports, and license file) and Test Suite files. If the Control Database is corrupt, the Compliance Guardian GUI cannot be opened and all scan jobs will fail. The database size depends on how many plans have been set up; how many scan jobs have been performed; how many Test Suites have been created and the frequency of accessing Compliance Manager GUI. Generally speaking, job reports take up a large proportion of database space. By enabling the Job Pruning feature, Compliance Guardian can remove the expired job reports from its Control Database for space saving purposes. ● Compliance Report Database: It is used to store detailed scan results from the Compliance Scan job, such as how many files failed on the Test Suite; the name and location of the files; and which Check(s) the file violated. All the information loaded from the Compliance Report GUI are from the Compliance Report Database. Compliance Guardian allows you to use different Compliance Report Databases for different Compliance Scan plans. If the database is corrupt, there would be no information from the Compliance Report GUI. The database size mainly depends how many items have been scanned; how many Checks were used to scan each item and how many violations Compliance Guardian detected. The following equation can be used to estimate how much space that one scan job takes up: *Number of scanned items * (1.2KB * Number of used Test Suites + 0.12KB * Number of detected violations).* ● Classification Report Database: It stores all detailed information about the Classification Scan job such as how many files have taken action in the given scope; what action Compliance Guardian did take on the file; basic information about the scanned file; and what tag value Compliance Guardian has added to the scanned files. All the information loaded from the Classification Report GUI are from the Classification Report Database. Compliance Guardian allows you to use different Classification Report Databases for different Classification Scan plans. If the database is corrupt, there would be no information from the Classification Report GUI. The database size is mainly dependent on how many items have been scanned, how many tags Compliance Guardian added into each item, and what kind of actions and how many actions Compliance Guardian has taken on each item. The following equation can be used to estimate how much space that one scan job takes up: *If taking Quarantine or Encryption Action:* (796B + 232B * Number of tags + 792B * Number of actions + 1852B) * Number of scanned items *If not taking Quarantine or Encryption Action:* (796B + 232B * Number of tags + 792B * Number of actions) * Number of scanned items As a rough estimate, if Compliance Guardian has scanned 10,000 items, added 3 tags and taken 2 actions on each item, the total size of Classification Report Database is around 25MB.
How does Compliance Guardian real time scanning work? Why does it require that an Agent is installed on each SharePoint WFE server?	The Compliance Guardian Real-Time Scan module uses SharePoint Event Receivers to monitor end-users' actions and to trigger jobs to scan content. The scan job will be executed by a process called RTS.exe and the specific Event Receiver is deployed by the Compliance Guardian Real-Time Classification Scan Solution in SharePoint. The SharePoint WFE server is used to handle requests from end-users, and multiple application servers running the same service applications are load balanced by default. Due to this SharePoint behavior, if the Compliance Guardian Agent is not installed on each SharePoint WFE server, when an end-user's request is sent to a server which does not have the process RTS.exe, the real-time scan job would not be executed and the content would not be scanned.

Questions	Answers
For a scheduled scan job, how can we improve the job performance?	Compliance Guardian supports load-balancing scans in a schedule job. If multiple Compliance Guardian Agents are being used in a scan job, the documents will be distributed to multiple Agents for scanning, which can improve the job performance.
What types of SharePoint metadata is supported (e.g. standard columns, managed metadata, content types)?	Compliance Guardian can use SharePoint columns for storing the tag value. It will use pre-defined columns (in content type or using Managed Metadata Services) if they already exist, or create whatever is needed if it cannot find a column in SharePoint with the same name as the one defined in the Test Suite.
Can item-level permissions be assigned to documents, and if so, will it have any kind of negative effect on performance?	Compliance Guardian can assign item-level permissions with no performance decrease. And Compliance Guardian can also take quarantine, encrypt, redact, or move actions to further secure or isolate documents.
What are the standards of encryption in Compliance Guardian Encrypt Action?	In Compliance Guardian, there are three encryption methods: AES (Advanced Encryption Standard) 128 or 256-bit, DES (Data Encryption Standard) 64-bit, and Blowfish 256-bit. You can use any one of these encryption methods to create a key to encrypt the content.
Are public/private keys used?	In the built-in Compliance Guardian package, we have a default security key generated based on AES Encryption for encrypting the content. You can create your own key in Compliance Guardian to encrypt the documents as well.
Where are the keys stored?	Compliance Guardian stores the encryption key in its Manager Control Database (an MS SQL server database). All keys are encrypted in the database as well.
Who can encrypt and decrypt the files?	Compliance Guardian does the encryption and decryption jobs. You can define an Action Policy to tell Compliance Guardian what document should be encrypted, then Compliance Guardian will make the encryption job accordingly. After the job finishes, documents can only be decrypted and viewed in the Compliance Guardian Incident Manager. This provides security for content even if it is removed from its original environment.