AvePoint® User Guide

Compliance Guardian 3

Installation and Administration User Guide

Service Pack 1, Cumulative Update 1

Revision D

Issued August 2013

Table of Contents

About Compliance Guardian 10

Complementary Products 10

Submitting Documentation Feedback to AvePoint 10

Accessibility Information for Screen Reading Software 11

Preparations Before the Installation 12

- Ports Used by Compliance Guardian 12
- Compliance Guardian Manager System Requirements 13
  - System Requirements for Control Service Installation 13
- Compliance Guardian Agent System Requirements 16
- Where to Install Compliance Guardian Agent 16
  - System Requirements for Agent Service Installation 17
  - SQL Server Requirements for Compliance Guardian Databases 17
  - SharePoint Environment Requirements for Compliance Guardian Agents 17
- Overview of Compliance Guardian Manager and Agent Services 18

Installing Compliance Guardian 18

- Compliance Guardian Manager 18
  - Installing Compliance Guardian Manager 19
- Compliance Guardian Agent 21
  - Installing Compliance Guardian Agent 21
- Accessing the Compliance Guardian GUI 24
- Internet Explorer Setup 25
- Logging In to Compliance Guardian 28
- How to Use Your Keyboard in Compliance Guardian 28
- Compliance Guardian Manager and Agent Maintenance 29

Uninstalling Compliance Guardian 29

- Uninstalling Compliance Guardian Manager 29
- Uninstalling Compliance Guardian Agent 30
- Resolve Issues Occurred During the Compliance Guardian Installation 30

Navigation Bar 31

Control Panel 31
Getting Started 31
Launching Control Panel 31
Understanding the Control Panel 33
Accessing the Control Panel 33
Monitor 33
Using the Manager Monitor 34
Using the Agent Monitor 34
System Options 37
Configuring General Settings 37
Configuring Security Settings 38
Viewing Security Information 40
Authentication Manager 40
Configuring Windows Authentication 41
Configuring AD Integration 41
Configure ADFS Integration 43
Account Manager 45
Managing Permission Levels 45
Managing User Groups 47
Managing Users 50
My Settings 53
License Manager 54
Viewing License Information 54
Importing and Exporting the License File 56
Configuring License Renewal Notifications 56
Configuring Server Usage 58
Update Manager 58
Configuring Update Settings 59
Checking for Updates 60
Managing Updates 61
Reviewing the Installation History of Updates 62
Agent Groups 63

Managing Agent Groups 63
User Notification Settings 65
Configuring Send E-Mail Settings 65
Configuring Receive E-Mail Settings 66
Configuring Receive E-Mail Notification 66
Managing Receive E-Mail Notification 67
Configuring E-mail Templates 67
Job Pruning 68
Configuring Pruning Rules 68
Configuring Settings 69
Configuring a Schedule 69
Log Manager 71
Configuring Log Settings 71
Collecting Logs 72
Solution Manager 72
Managing Solutions 72
Solution Description 74
Database Manager 75
Report Database 75
Report Database Policy 76
Test Suite Manager 77
Background Information 77
Managing Test Suites 78
Create a New Check or Test Suite 79
Upload Checks and Test Suites 81
Download a Test Suite 81
View Details about a Test Suite 81
Edit a Previously Configured Check or Test Suite 81
Delete a Check or Test Suite 84
Risk Formula 84
Report Configuration 86
Managing Report Settings 86

Configuring Report Settings 86
Allowed Location 87
Configuring Allowed Location 87
Export Location 88
Managing Export Locations 88
Configuring Export Locations 89
Filter Policy 89
Managing Filter Policies 90
Configuring Filter Policies 90
Editing Filter Policies 92
Website Scanner Settings 92
Configuring Authentication Profile 92
Configuring User Agent Profile 93
Compliance Manager 96
Pre-Configurations 96
Configuring Scan Policies 96
Configuring Filter Policies 98
Configuring Database Policies 98
Configuring the Account Manager 98
Configuring Connections for File System 98
Compliance Scanner 100
Launching Compliance Scanner 101
Home Page Overview 102
Selecting Mode 102
Managing Compliance Guardian Scanner Plans 102
Compliance Guardian Scanner for SharePoint 104
Launching Compliance Guardian Scanner SharePoint Mode 104
Selecting the Scan Scope 104
Using Plan Builder to Perform a Compliance Guardian Scanner Plan for SharePoint 104
Compliance Guardian Scanner for File System 109
Launching Compliance Guardian Scanner File System Mode 109
Selecting the Scan Scope 109

Using Plan Builder to Perform a Compliance Guardian Scanner Plan for File System 109
Compliance Guardian Scanner for Website 113
Launching Compliance Guardian Scanner in Website Mode 113
Using Plan Builder to Perform a Compliance Guardian Scanner Plan for Website 113
Compliance Reports 116
Getting Started 116
Launching Compliance Report 116
User Interface Overview 118
Classification Manager 119
Real-Time Classification Scanner 119
Pre-Configurations 119
Configuring Scan Policies 119
Configuring Filter Policies 121
Configuring Action Policies 121
Getting Started 131
Launching Real-Time Classification Scanner 131
Home Page Overview 132
Using Real-Time Classification Scanner Rules 133
Creating Real-Time Classification Scanner Rules 133
Applying Real-Time Classification Scanner Rules 135
Inheriting and Stop Inheriting Parents' Rule 135
Scheduled Classification Scanner 136
Pre-Configurations 136
Configuring Scan Policies 136
Configuring Filter Policies 136
Configuring Action Policies for SharePoint 137
Configuring Action Policies for File System 137
Configuring Connections for File System 139
Getting Started 141
Launching Scheduled Classification Scanner 141
Home Page Overview 143
Selecting Mode 143

Managing Scheduled Classification Scanner Plans 143
Scheduled Classification Scanner for SharePoint 145
Launching Compliance Guardian Scanner SharePoint Mode 145
Performing a Scheduled Classification Scanner Plan in Wizard Mode 145
Performing a Scheduled Classification Scanner Plan in Form Mode 149
Scheduled Classification Scanner for File System 149
Launching Compliance Guardian Scanner File System Mode 149
Performing a Scheduled Classification Scanner Plan in Wizard Mode 149
Performing a Scheduled Classification Scanner Plan in Form Mode 152
Using Compliance Guardian Features in SharePoint 152
Using Compliance Guardian Tag Assist Manager in SharePoint 152
Using Compliance Guardian Quarantine Manager in SharePoint 155
Job Monitor 160
Getting Started 160
Launching Job Monitor 160
Understanding Job Monitor 161
Job Monitor Interface 161
Job Monitor vs. Scheduled Job Monitor 162
Configuring the Viewing Pane 162
The View Toolbar 162
The Filter Toolbar 163
Searching Jobs 163
Managing Jobs 164
Operations in the Job Monitor Tab 164
The Manage Toolbar 164
The Actions Toolbar 165
The Settings Toolbar 165
Operations in the Scheduled Job Monitor Tab 166
The Actions Toolbar 166
The Filter Toolbar 166
Appendix A: Accessing Hot Key Mode 167
Compliance Scanner Page 167

Scheduled Classification Scanner Page 170
Real-Time Classification Scanner page 172
Job Monitor Page 173
Scheduled Job Monitor Page 174
Control Panel Page 174
Appendix B: Configuring Checks and Test Suites 175
Configuring Check Type Attributes 175
Element Type Check 176
EnhancedElement Type Check 182
MatchedElement Type Check 189
FindText Type Check 194
ComplexFindText Type Check 196
RegularExpression Type Check 199
ComplexRegEx Type Check 201
Dictionary Type Check 206
Cookie Type Check 210
SSL Type Check 212
WebBeacons Type Check 213
FindFile Type Check 216
LinkValidation Type Check 217
FileProperty Type Check 220
Configuring CCC or MCC File Attributes 223
Content Compliance Collection (CCC) File Body Configuration 223
Metadata Compliance Collection File Body Configuration 225
Appendix C: Supported File Types in Compliance Guardian 227
Appendix D: Using the Scan Engine API 228
Initialize the ScanEngine Class 228
Parameters of the ScanEngine.Scan Method 228
Usage Example 229
Scan Files Using CCC 229
Scan Files Using MCC 233
Scan Metadata 236

CCE.EngineWorker.exe Mode 238
Appendix E: Using Check Validator Tool 240
Related Configuration File 242
Appendix F: Generate Detailed Risk Report of a File 243
Before You Begin 243
Appendix G: Compliance Guardian Configuration File 245
Appendix H: Using CustomCheck in Compliance Guardian 246
Using CustomCheck 246
Method 246
Configuration 246
Example 246
Related Configuration File 247
Appendix I: Using Compliance Guardian Transaction Capture 248
Installing Compliance Guardian Transaction Capture 248
Using the Tool 249
Appendix J: Using Detailed Risk Report Analysis Tool 251
Generating the Report 251
Information Included in the Exported Excel File 252
Appendix K: Using Compliance Guardian Report Database Upgrade Tool 253
Using the Tool 253
Appendix L: Displaying Only Violations in the Error Highlight Report 254
Index 255
Notices and Copyright Information 262

About Compliance Guardian

Compliance Guardian is designed to ensure that information is available and accessible to the people who should have it and protected from the people who should not. Compliance Guardian helps Chief Privacy Officers, Chief Information Security Officers, Compliance Managers, Records Managers, SharePoint Administrators, and Company Executives proactively protect their IT environments from harmful information leaks, contamination, or misuse while simultaneously ensuring that all activities and content residing in their environments are compliant, accessible, and manageable.

Compliance Guardian is designed to empower organizations to comply with regulatory, statutory, or organization specific requirements to manage and oversee access to sensitive data.

Compliance Guardian works with AvePoint's extended Compliance Solutions to provide a "heat map" that provides additional actionable context about the document including: how old is the document, who authored it, how many times has it been accessed, who can access it, who has accessed it, and what have they done with it. In this way, organizations can take specific steps to protect and mitigate their risk.

By identifying, classifying, and taking action on compliance risks, and presenting this information in easily digestible formats for various stakeholders, organizations can more effectively build and maintain a compliant framework.

Complementary Products

Many products and product suites on the Compliance Guardian platform work in conjunction with one another. The DocAve Auditor Reports are recommended for use with Compliance Guardian. Auditor Reports are available in DocAve 6 Report Center under Compliance Reports.

Submitting Documentation Feedback to AvePoint

AvePoint encourages customers to provide feedback regarding our product documentation. You can Submit Your Feedback on our website.

Accessibility Information for Screen Reading Software

Ensure that the following requirements are met before you use Job Access with Speech (JAWS) or NonVisual Desktop Access (NVDA) to read Microsoft Silverlight:

1. JAWS does not read ActiveX controls by default. In order to enable JAWS to read Silverlight, the following text must be added to the **FsDomSrv.ini** file, and JAWS must be restarted.

   Add this text to the **FsDomSrv.ini** file:

   [MS Silverlight Embedded in Internet Explorer using OBJECT Tag with type]
   DLLName=SDomNodeMSAA
   ; TagNameMatch | ParamAndValueMatch
   MappingFlags=96
   Param=application/x-silverlight-2
   TagName=OBJECT
   StartString=Silverlight application start
   EndString=Silverlight application end
   ImplementationFlags=7
   InteractionModeFlags=3

   The user must disable the Virtual Cursor by pressing **Ins + Z** after the page containing the Silverlight application (Compliance Guardian interface) has loaded.

2. For the NVDA screen reader, the following step must be performed in order to enable NVDA to read Silverlight:

   The user must enable NVDA **Virtual Buffer Pass-through** using **Ins + Space** after the page containing the Silverlight application (Compliance Guardian interface) has loaded.

Preparations Before the Installation

Refer to the following sections for the prerequisites before installing Compliance Guardian.

Ports Used by Compliance Guardian

Before the installation, make sure the ports required for Compliance Guardian Manager and Agents are able to be accessed through the firewall software installed on the corresponding machines. For example, if the **Windows Firewall** is enabled on the servers which have installed Compliance Guardian, you must make sure the 14100 and 14104 ports are allowed in the **Inbound Rules** on the corresponding servers.

The port numbers may vary according to the settings configured when installing Compliance Guardian in your environments. In the following example of configuring the **Inbound Rules**, the default ports are used:

***Note**: If there are multiple Compliance Guardian services installed on the same server, make sure all of the required ports are enabled on that server.

1. Remotely connect to the server where the **Compliance Guardian Timer Service** is installed.
2. Navigate to **Start** > **Administrative Tools** > **Windows Firewall with Advanced Security**.
3. Select **Inbound Rules** under **Windows Firewall with Advanced Security on Local Computer** and select **New Rule**.
4. In the **Rule Type** step, select **Port** to configure the inbound rule for the ports used by **Compliance Guardian Timer Service**, and then select **Next**.
5. In the **Protocol and Ports** step, specify the rule to be applied to **TCP**, and then select **Specific local ports** option. Enter **14100** in the textbox, and then select **Next**.
6. In the **Action** step, select the **Allow the connection** option to allow the connection to port 14100, and then select **Next**.
7. In the **Profile** step, keep the default selection so that all three options are selected, and then select **Next**.
8. In the **Name** step, enter the **Name** and an optional **Description** for this inbound rule.
9. Select **Finish** to complete the inbound rule creation.
10. Repeat the same steps on all of the other servers that have Compliance Guardian Agents installed and have **Windows Firewall** enabled. The port used by the Compliance Guardian Agent is 14104.

Compliance Guardian Manager System Requirements

Compliance Guardian Manager consists of one service called the Compliance Guardian Timer Service (a control service). You can either run it on the same server as your Compliance Guardian Agent or on a separate server. For more information on Compliance Guardian Manager, refer to Installing Compliance Guardian Manager.

While it is possible to have the Compliance Guardian Manager and Compliance Guardian Agent on a single server, it is not recommended. For the best performance, install the Manager Service on a separate server, and install only the necessary agents on the agent servers.

Refer to System Requirements for Control Service Installation for the system requirements of the Compliance Guardian Control Service.

System Requirements for Control Service Installation

Rules		Requirements
Operating System Edition: Windows Server 2008, Windows Server 2008 R2, Windows 7, Windows Server 2012	Total Physical Memory	Required: 512MB or above Recommended: 2GB
	Available Disk Space	Required: 1GB or above
	.Net Framework Version	.NET Framework 3.5 SP1 or above (excluding .NET Framework 4.0)
	.Net Framework Features	The Windows features, including WCF Activation, HTTP Activation and Non-HTTP Activation must be installed
	Net.Tcp Port Sharing Service	Net.Tcp Port Sharing Service is started
	Windows Process Activation Service	• Windows Process Activation Service is started • Process Model, .NET Environment and Configuration APIs are installed
	World Wide Web Publishing Service	World Wide Web Publishing Service is started

Rules		Requirements
	Web Server (IIS) Role	The following Windows features are installed: • Web Server • Common HTTP Features (Static Content, Default Document) • Application Development (ASP.NET, .NET Extensibility, ISAPI Extensions and ISAPI Filters) • Management Tools (IIS Management Console, IIS 6 Management Compatibility and IIS 6 Metabase Compatibility)
Operating System Edition: Windows Server 2003, Windows Server 2003 R2	Total Physical Memory	Required: 512MB or above Recommended: 2GB
	Available Disk Space	Required: 1GB or above
	.Net Framework Version	.NET Framework 3.5 SP1 or above (excluding .NET Framework 4.0)
	Net.Tcp Port Sharing Service	Net.Tcp Port Sharing Service is started
	World Wide Web Publishing Service	World Wide Web Publishing Service is started
	ASP.NET	ASP .Net 2.0.50727 or above
	Application Server	• Network COM+ access is enabled. • Internet Information Services (IIS) is started, including the following installed features: Common Files, IIS Manager, and World Wide Web Service
	IIS Service	IIS Admin Service is started IIS version must be 6.0 or above
	HTTP SSL	HTTP SSL Service is started

Required Application Pool Settings

The following application pool settings are required by Compliance Guardian Control Service Installation whether you choose to use an existing application pool or create a new one. If you choose to create a new application pool, Compliance Guardian will automatically configure these settings. If you choose to use an existing application pool, you must configure the application pool according to the following table:

IIS Version	IIS Setting	Value	Note
IIS7	Advanced Settings > General > .NET Framework Version	v2.0 / v4.0	**No Managed Code** is not supported.
	Advanced Settings > General > Enable 32-bit Applications	False	**False** is required since Compliance Guardian must load some third-party dlls which are 64-bit ones.
	Advanced Settings > General > Managed Pipeline Mode	Integrated / Classic	It is not supported to use **Classic** together with **.NET Framework v4.0**.
	Process Model > Load User Profile	True	**True** is required by Compliance Guardian SSO, and **False** is not supported.
	Advanced Settings > General > Start Automatically	True / False	**True** is strongly recommended because if you set the value to **False**, the application pool requires manual start up.

Required Application Pool Account Permissions

The application pool account for connecting an existing IIS website or creating a new IIS website must have the following local system permissions. The specified application pool account will be granted Full Control permission to the following groups and folders automatically during Compliance Guardian Manager installation:

- IIS_WPG (for IIS 6.0) or IIS_IUSRS (for IIS 7.0)
- Full Control to HKEY_LOCAL_MACHINE\SOFTWARE\AvePoint\ComplianceGuardian
- Full Control to Compliance Guardian Manager folder
- Member of the Performance Monitor Users group
- Full Control to Compliance Guardian Certificate private keys
- Full Control (or Read, Write, Modify, and Delete) to C:\WINDOWS\Temp (only for Windows 2003 environment)

You can add the application pool account to the local **Administrators** group to meet the required permission.

Compliance Guardian Agent System Requirements

Compliance Guardian Agent has one service named the Compliance Guardian Agent Service. A Compliance Guardian Agent communicates with SharePoint based on the commands it receives from the Compliance Guardian Manager's Control Service. Multiple agent setups provide redundancy as well as scalability for large environments by allowing you to specify different accounts for different farms where multiple farms exist. The Compliance Guardian Agent can be installed on different machines according to the role of the machine, and the Compliance Guardian modules and functionalities you want to use. For more information on where to install the Compliance Guardian Agents, refer to Where to Install Compliance Guardian Agent.

***Note:** In order to scan Microsoft Office files that are in a 2003 or earlier format, you must download a compatibility pack, and then install the compatibility pack on the server where Compliance Guardian Agent is installed. Once you install the compatibility pack, Compliance Guardian will support scans of these files, but the software does not support tagging of Microsoft Office 2003 files even though they can be scanned and classified after installing the compatibility pack.

Where to Install Compliance Guardian Agent

In order to install Compliance Guardian Agents, the following basic requirements must be met to make all of the functions and configurations of the corresponding product available:

- All of the installed Compliance Guardian Agents must be properly licensed in the modules and functions you want to use.
- In order to use Compliance Scanner, Compliance Guardian Agent must be installed on at least one of the front-end Web servers.
- In order to use the Scheduled Classification Scanner, Compliance Guardian Agent must be installed on at least one of the front-end Web servers.
- In order to use the Real-Time Classification Scanner, Compliance Guardian Agents must be installed on all of the front-end Web servers.

System Requirements for Agent Service Installation

Rules		Requirements
Operating System Edition: Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012	Total Physical Memory	Required: 512MB or above Recommended: 2GB
	Available Disk Space	Required: 1GB or above
	.NET Framework Version	.NET Framework 3.5 SP1 or above (excluding .NET Framework 4.0)
	.Net Framework Features (only in **Windows Server 2008, Windows Server 2008 R2** and **Windows Server 2012** environments)	The Windows features, including HTTP Activation and Non-HTTP Activation are installed.
	Net.Tcp Port Sharing Service	Net.Tcp Port Sharing Service has started.
	SharePoint Version	SharePoint Server 2007 or SharePoint Server 2010 is installed.

SQL Server Requirements for Compliance Guardian Databases

Databases	SQL Server Edition
Control Database	• Microsoft SQL Server 2005 • Microsoft SQL Server 2008 R2 • Microsoft SQL Server 2012 RTM
Report Database	

SharePoint Environment Requirements for Compliance Guardian Agents

Compliance Guardian Agents can be installed and used in the following SharePoint 2010 environments:

- Microsoft Office SharePoint Server 2007 with SP2
- Windows SharePoint Services 3.0 with SP2
- Microsoft SharePoint Server 2010 with SP1
- Microsoft SharePoint Foundation 2010 with SP1
- Microsoft SharePoint Server 2010 RTM
- Microsoft SharePoint Foundation 2010 RTM

Overview of Compliance Guardian Manager and Agent Services

After properly installing all of the services, including Compliance Guardian Manager Service and Compliance Guardian Agent Service, you are able to manage the compliance of your SharePoint data via the Compliance Guardian product.

Control Service receives the request from Compliance Guardian Manager GUI, and then sends the request to Agent Services which retrieve data from SharePoint. Agent Services then send the retrieved data to the Control Service for analyzing. If some actions should be performed on the SharePoint contents that are considered not compliant by Compliance Guardian, those actions will be performed by the Agent Services. The Agent Services will also be used to export the compliance reports from the report database.

Installing Compliance Guardian

The Compliance Guardian Installation Wizard is there to guide you through the installation process. By following the steps below, you will have Compliance Guardian up-and-running on your environment very quickly. In order to complete the installation successfully, a local administrator account must be used to run the Installation Wizard.

***Note:** Install Compliance Guardian in the following order:

1. Install the Compliance Guardian Manager with the Manager Installation Wizard.
2. Install the Compliance Guardian Agents with the Agent Installation Wizard.
3. Log in to Compliance Guardian to make sure the Manager and Agent are able to communicate with each other properly.

Compliance Guardian Manager

Make sure the system requirements are met before starting installation for Compliance Guardian Manager. For more information, refer to System Requirements for Control Service Installation.

***Note**: When running the Manager Installation Wizard on the server running Windows Server 2003/Windows Server 2003 R2, make sure the Windows components are not being added or removed during the rule scanning; otherwise, the scanning result will be affected.

***Note**: When running the Manager Installation Wizard on the server running Windows Server 2008/Windows Server 2008 R2/Windows 7, make sure the Server Manager is not being used to add or remove Windows features during the rule scanning; otherwise, the scanning result will be affected.

Installing Compliance Guardian Manager

To install Compliance Guardian Manager, complete the following steps:

1. Download the Manager ZIP file, either by requesting a demo version or by contacting an AvePoint representative for links to this package.
2. Unzip the package, and then open the unpacked Compliance Guardian Manager directory. Run the **Setup.exe** file.
3. After the welcome screen appears, select **Next**.
4. Enter your **Name** and **Organization** into the provided fields. Select **Next**.
5. Carefully review the Compliance Guardian License Agreement. After you have read the agreement, check the **I accept the terms in the license agreement** checkbox, and select **Next**.
6. Select **Browse**, and then select the location for the Manager installation. By default, the installation location is **C:\Program Files\AvePoint**. Select **Next**.
7. Select the Compliance Guardian Manager Service you want to install by checking the corresponding checkbox. There is only one service to install.

   Control Service – Manage all Compliance Guardian operations and achieve the Web-based Compliance Guardian platform, allowing users to interact with the software. All agents can communicate with the manager through the Control Service, so it is imperative that the machine you install the control service on is accessible by all agent machines.

   Select **Next**.

8. Compliance Guardian will perform a brief pre-scan of the environment to ensure that all rules meet the requirements. The status for each rule will be listed in the **Status** column. Select the hyperlink of the status, and the detailed information about the scan result will be listed in the pop-up window. You may select **Details** to view the detailed information of all of the requirements.

   If any rules have failed the pre-scan, update your environment to meet the requirements, and then select the **Rescan** button to check your environment again. Once all the rules pass, select **Next**.

9. Set up the Control Service Configuration:
   - **Control Service Address** – Specify the current machine's hostname or IP address. The Control Service manages internal configuration data, user access control, scheduling, and job monitoring.
   - **IIS Website Settings** – Configure the IIS website settings for the Control Service. You can select to use an existing IIS website or create a new IIS website. The IIS website is used to access Compliance Guardian Manager.
     - **Use an existing IIS website** – Select an existing IIS website from the drop-down list, and if necessary, you can adjust the **Website Port** used to access the Compliance Guardian Control Service.

- **Create a new IIS website** – Enter the website name and create a new IIS website for the Control Service. The default **Website Port** used to access Compliance Guardian Control Service is 14100; you do not need to change it unless a known port conflict exists.
- **Website Port** – Control Service communication port. The default port is 14100.

- **Application Pool Settings** – Configure the IIS application pool settings for the corresponding website. You can select to use an existing application pool or create a new application pool. The application pool is used to handle the requests sent to the corresponding website. The following settings can be configured:
  - **Use an existing application pool (not recommended)** – Select an existing application pool from the drop-down list. If you choose to use an existing application pool, the Application Pool Account settings are greyed out and cannot be changed.
  - **Create a new application pool** – Enter the application pool name and application pool account settings to create a new IIS application pool for the corresponding website. By default, the new application pool's name is **ComplianceGuardian**.

Select **Next** to continue to configure the database settings for Control Service.

10. In this page, **MS SQL** is selected in the **Database Type** drop-down menu. The following information must be configured for the MS SQL database:
    - **Database Server** – The MS SQL server name.
    - **Control Service Database Name** – Enter a database name for the Control Service, if the database does not exist, it will be created in the provided MS SQL server.
    - **Database Credentials** – Select the credentials for this Control Service database.
      - **Windows Authentication** (the default option) – Use this method when you want the user identity to be confirmed by Windows. The specified account must have permission to access the SQL Server machine where you want to create the Control Service Database.
      - **SQL Authentication** – SQL server will confirm the user identity itself according to the specified account and password. The specified account must have the following permission: DB Owner of the existing Compliance Guardian Control Database or DB Creator of the newly created Compliance Guardian Control Database.
    - **Passphrase Settings** – Enter the passphrase you want to use for protecting Compliance Guardian Manager data.
    - **Advanced Database Settings** – You can choose to associate the Compliance Guardian Control database with a specific failover SQL server that is used in conjunction with SQL Server database mirroring.

    Select **Next**.

11. Set up the Advanced Configuration.
    - **SSL Certification** – Specify the method for encrypting information and providing authentication for Compliance Guardian:
        - **Built-in Certificate** – Uses the certificate provided by Compliance Guardian. No additional configuration is necessary.
        - **User-defined Certificate** – Enabling this option allows you to select a certificate from your local machine. It will use the Certificate Authentication server of the current machine to check whether the certificate is revoked. After the certificates are filtered, only the certificates that are not revoked will be displayed.

    Select **Next**.

12. In the **Ready to install Compliance Guardian Manager** page, all of the information configured in the previous steps is listed. Select **Install** to begin the installation. Select **Back** to change any of the previous settings. Select **Cancel** to abandon all of the configurations and exit the installation wizard.
13. When the Manager installation is completed, the Manager Passphrase you specified to protect Compliance Guardian Manager data will be displayed on the **Install Completed** page. Save this passphrase to enter it during the Agent installation.

After the installation is complete, select **Finish** to exit the installation wizard.

Compliance Guardian Agent

Make sure the system requirements are met before starting the Compliance Guardian Agent installation. For more information, refer to System Requirements for Agent Service Installation.

Check that the Compliance Guardian Manager services have started before installing the Compliance Guardian Agents.

Installing Compliance Guardian Agent

After the Manager's services have started, complete the following steps to install the Compliance Guardian Agent:

1. Download the Agent ZIP file, either by requesting a demo version or by contacting an AvePoint representative for links to this package.
2. Unzip this package and navigate to the Compliance Guardian Agent directory. Run the **Setup.exe** file.
3. From the welcome screen, select **Next**.
4. Enter your **Name** and **Organization** into the provided fields, and then select **Next**.
5. Carefully review the Compliance Guardian License Agreement.

After you have read the terms in the license agreement, check the **I accept the terms in the license agreement** checkbox, and then select **Next**.

6. Select **Browse**, and then select the location for the Agent installation. By default, the installation location is **C:\Program Files\AvePoint**. Select **Next**.
7. Compliance Guardian will perform a brief pre-scan of the environment to ensure that all rules meet the requirements. The status for each rule will be listed in the **Status** column. Select the hyperlink of the status, and the detailed information about the scan result will be listed in the pop-up window.
8. Select **Details to** view the detailed information of all of the requirements. Update your environment to meet the requirements if there are some checked rules that failed.
9. Select the **Rescan** button to check your environment again. Once all rules pass, select **Next**.
10. Set up the Communication Configuration.

    - **Compliance Guardian Agent Host** – Specify the current server's hostname, IP address, or fully qualified domain name (FQDN).
    - **Compliance Guardian Agent Port** – The port specified here is used by the Manager or other Agents for communication. The default port number is 14104.
    - **Control Service Host** – The hostname or IP address of the machine where the Control Service is installed.
    - **Control Service Port** – This is the port used for communication with Control Service and should match the information provided during the Manager configuration. The default port number is 14100.
    - **SSL Certification** – Specify the SSL Certification used for the specified Compliance Guardian Manager.

    Select **Next**.

11. Set up the Agent Configuration:

    - **Agent Authentication** – Enter the Manager Passphrase specified when configuring the Compliance Guardian Manager installation. If you forget the passphrase, you can view it by navigating to **DocAve** > **Control Panel** > **System Options** > **Security Settings**. For more information, refer to Viewing Security Information.
    - **Agent Account** – Specify the Agent Account under which the agent activities are performed. For more information on the permissions required for each Compliance Guardian module, refer to the section of that module in this user guide. The ideal account permissions for all Compliance Guardian products are listed below:

Local System Permissions

The specified Agent Account will be granted Full Control permission to the following groups and folders during Compliance Guardian Agent installation:

***Note**: The **local administrator** permission is required for the Agent Account when you are installing the Compliance Guardian solutions using the Agent Account in Solution Manager.

- IIS_WPG (for IIS6.0) or IIS_IUSRS (for IIS7)
- Performance Monitor Users
- Compliance Guardian Users (the group is created by Compliance Guardian automatically and it has the following permissions):
  - Full Control to the Registry of HKEY_LOCAL_MACHINE\SOFTWARE\AvePoint\ComplianceGuardian.
  - Full Control to the Registry of HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\services\eventlog.
  - Full Control to the Communication Certificate.
  - Permission of **Log on as a batch job** (it can be found within Control Panel\Administrative Tools\Local Security Policy\Security Settings\Local Policies\User Rights Assignment)
  - Full Control Permission of Compliance Guardian Agent installation directory

SharePoint Permissions for SharePoint 2007

- Member of the Farm Administrators group
- Full Control permission to all zones of all Web applications via the User Policy for Web Applications

SharePoint Permissions for SharePoint 2010

- Member of the Farm Administrators group
- Full Control permission to all zones of all Web applications via the User Policy for Web Applications
- User Profile Service Application permissions:
  - Use Personal Features
  - Create Personal Site
  - Use Social Features
- Managed Metadata Service: Term Store Administrator
- Business Data Connectivity Service: Full Control

- Search Service: Full Control

SharePoint Permissions for SharePoint 2013

- Member of the Farm Administrators group
- Full Control permission to all zones of all Web applications via the User Policy for Web Applications
- User Profile Service Application permissions:
  - Use Personal Features
  - Create Personal Site
  - Use Social Features
- Managed Metadata Service: Term Store Administrator
- Business Data Connectivity Service: Full Control
- Search Service: Full Control

SQL Server Permissions

- Database role of **db_owner** for all of the databases related with SharePoint, including content databases, SharePoint configuration database, and Central Admin database.
- Database role of **dbcreator** and Security Admin to SQL Server.

Select **Next**.

12. In the **Ready to install Compliance Guardian Agent** Page, review the customer information you defined, and then select **Install** to begin the installation. Select **Back** to change any of the previous settings. Select **Cancel** to abandon all configurations and exit the installation wizard.
13. After the installation is complete, select **Finish** to exit the installation wizard.

Congratulations! Compliance Guardian is now installed and configured. Once you have completed the product installation, you can begin to configure the report database needed to store the report data.

Accessing the Compliance Guardian GUI

The following table displays the supported browsers and their requirements on the Silverlight version if you want to access the Compliance Guardian GUI in a Windows Server 2008 R2 Enterprise SP1 environment.

Rules	Requirement
Silverlight Version	5.0 or above
Internet Explorer	IE 7 or above
Google Chrome	19.0.1084.52

Rules	Requirement
Mozilla Firefox	14.0.1

Internet Explorer Setup

When first accessing Compliance Guardian using Microsoft Internet Explorer (IE), some initial security settings must be configured. Run Compliance Guardian's server application found in the Start menu on the machine where the Compliance Guardian Control Service is installed, and complete the following steps:

1. When you access Compliance Guardian by IE, the browser will display a security certificate prompt. Select the **Continue to this website** option listed next to the shield.

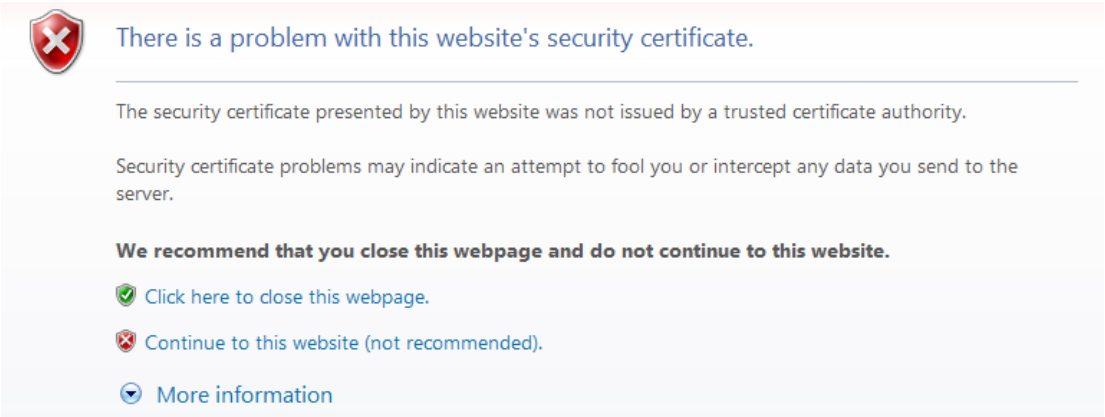

Figure 1: Security certificate prompt.

2. Select the **Certificate Error** button next to the address bar.

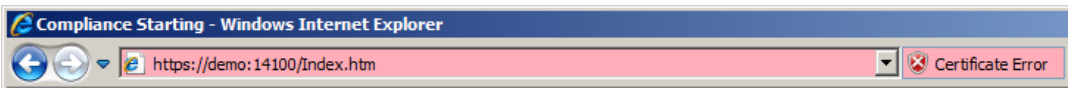

Figure 2: Certificate Error button.

3. Select **View certificates** in the pop-up. The Certificate window appears.

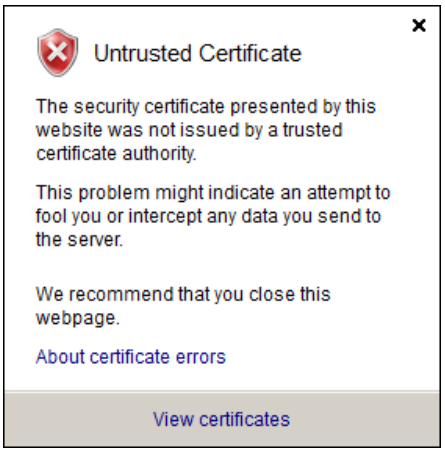

Figure 3: View certificates link.

4. Select the **Install Certificate…** button to install the Compliance Guardian certificate. The name of this certificate is the same as the hostname of the server that has Compliance Guardian Control Service installed.

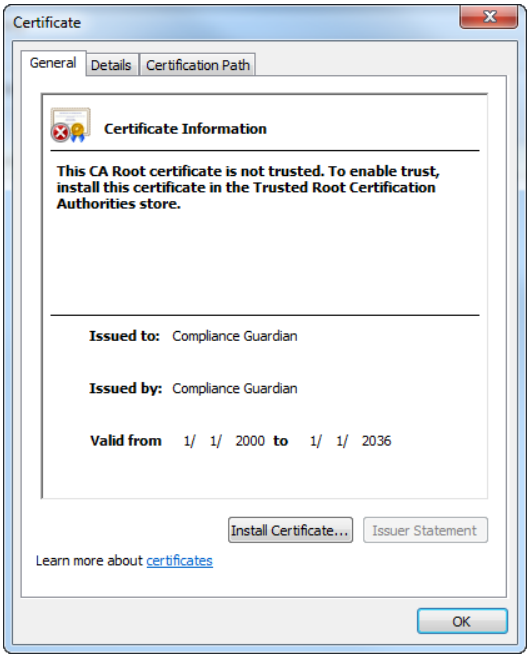

Figure 4: Install Certificate button.

5. Select **Next** to continue installing the certificate.

6. Select the **Place all certificates in the following store** option and select **Browse** to browse to the **Trusted Root Certification Authorities** folder. Select **OK** to confirm the selection and select **Next**.

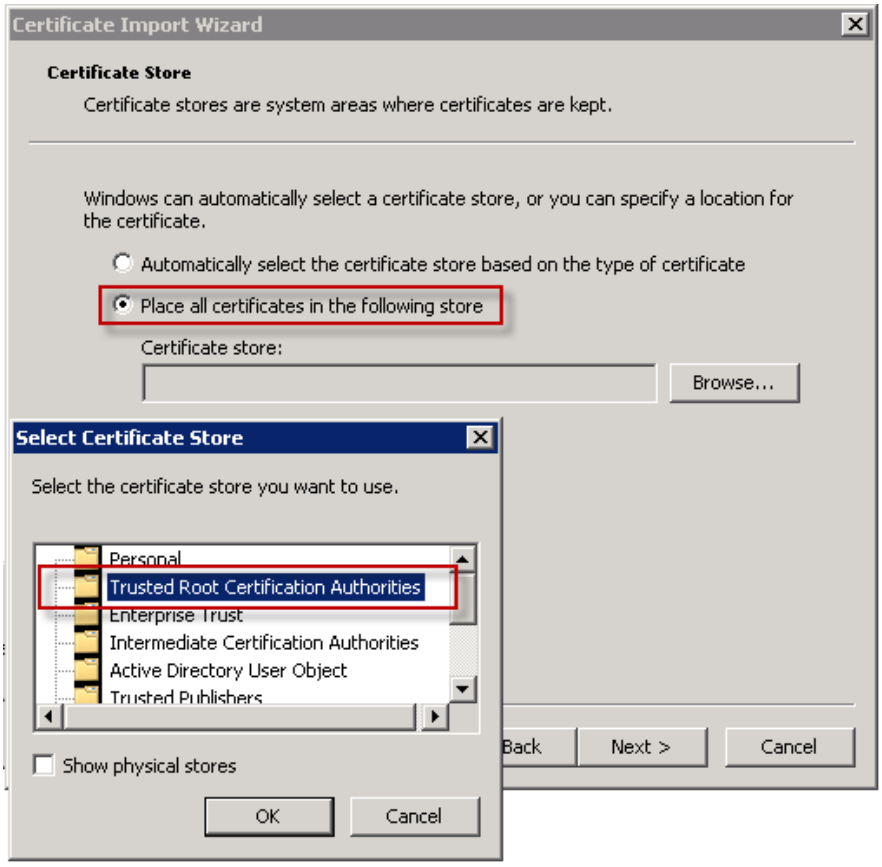

Figure 5: Certificate Import Wizard.

7. Select **Finish** to complete the certificate import.
8. Select **OK** in the prompt window to acknowledge the successful import.
9. Choose to temporarily allow the Compliance Guardian GUI pop-up window or to always allow the Compliance Guardian GUI in the prompt window.

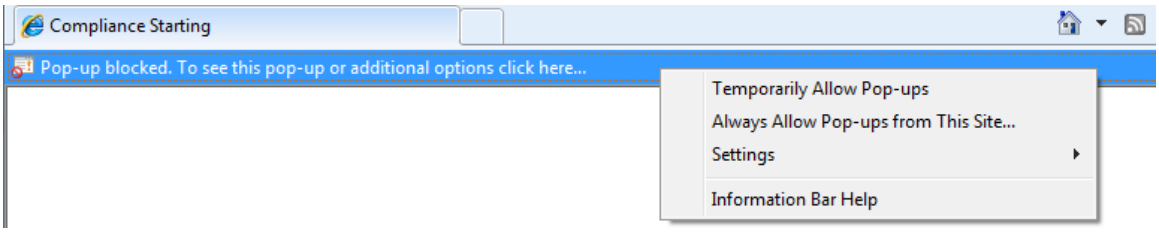

Figure 6: Choose how to allow the pop-ups.

You can now log into Compliance Guardian from Internet Explorer.

Logging In to Compliance Guardian

The Compliance Guardian GUI can be launched from Web browsers within the same network as the Compliance Guardian Manager. Refer to Accessing the Compliance Guardian GUI for the supported Web browsers. Connect to the interface using the IP/hostname for the Compliance Guardian Manager Control Service, as well as the Control Service Port if it was changed.

1. Open an Internet Explorer window and enter **https://<machine>:14100** where <machine> is the hostname or IP address of the machine running the Compliance Guardian Control Service. If the default port number has been changed from 14100, enter the new port number.

   ***Note**: If the hostname of the machine running the Compliance Guardian Control Service contains the underline (_), use the IP address of the corresponding machine to access Compliance Guardian.

2. The Compliance Guardian login screen pops up. Select **Local System** from the **Log on to** drop-down list and enter the default login account information:

   - **Login ID:** admin
   - **Password:** admin

3. Select **Login**.

   ***Note**: When you log on to Compliance Guardian for the first time, it is strongly recommended that you back up the Compliance Guardian security keys for protection. For more information, refer to Viewing Security Information.

You can also log on Compliance Guardian using the integration with other authentication methods. For more information, refer to Authentication Manager.

How to Use Your Keyboard in Compliance Guardian

Please refer to the following table for instructions on using the keyboard in Compliance Guardian.

Keyboard Key	When to Use
Tab	Switch among all of the functions in one page.
Enter	Select one button.
Space	Select one check box/radio button/button.
F2	Gain focus in one cell of a table.
↑↓←→	Switch among options in one list box, options in one combo box, or among cells in one table.

Compliance Guardian Manager and Agent Maintenance

If you want to modify the configuration of Compliance Guardian Manager/Agent after the installation, open the **Start Menu** in Windows on the Compliance Guardian Manager/Agent server, and navigate to **All Programs** > **AvePoint Compliance Guardian**. Then, open the **Compliance Guardian Manager Tools**/ **Compliance Guardian Agent Tools** folder and select **Manager Configuration Tool**/**Agent Configuration Tool**.

Select the items listed on the left part of the tool and you can modify the corresponding settings.

Refer to Installing Compliance Guardian Manager and Installing Compliance Guardian Agent for detailed information about the settings.

Uninstalling Compliance Guardian

The Compliance Guardian Uninstallation Wizard is there to guide you through this uninstallation process. By following the steps below, you will have Compliance Guardian removed from your environment very quickly. In order to complete the uninstallation successfully, the Uninstallation Wizard must be run by a local administrator.

Uninstalling Compliance Guardian Manager

In order to uninstall Compliance Guardian Manager, please ensure the Manager Service being removed is not in use by another process. To uninstall Compliance Guardian Manager, complete the following steps:

***Note:** Once the uninstallation is in progress, it cannot be cancelled and the uninstallation interface cannot be closed.

1. Open the **Start Menu** in Windows on the Compliance Guardian Manager Server, and navigate to **All Programs** > **AvePoint Compliance Guardian**.
2. Open the **Compliance Guardian Manager Tools** folder, and then select **Manager Uninstall**.
3. Select the **Remove** option, and then select **Next**.
4. In the **Ready to Remove Compliance Guardian Manager** page, configure the **Remove configuration file** option. Select this option if you want to remove all of the folders and configuration files generated by the Compliance Guardian Manager installation.

   ***Note:** The Logs folder will not be removed whether you select the **Remove configuration file** option or not.

5. Select **Remove** to start the Manager uninstallation process.

If the application pool created by Compliance Guardian Manager installation is still useful, it will not be deleted during the Manager uninstallation. If the application pool created by Compliance Guardian Manager installation is not used by any other applications, it will be deleted during the Manager uninstallation.

***Note:** The Manager uninstallation will not delete the Manager databases.

6. Select **Finish** to complete the uninstallation.

Uninstalling Compliance Guardian Agent

In order to uninstall Compliance Guardian Agent, please ensure there are no current jobs running on the agent. To uninstall Compliance Guardian Agent, complete the following steps:

***Note:** Once the uninstallation is in progress, it cannot be cancelled and the uninstallation interface cannot be closed.

1. Open the **Start Menu** in Windows on the Compliance Guardian Agent server, and navigate to **All Programs** > **AvePoint Compliance Guardian.**
2. Open the **Compliance Guardian Agent Tools** folder, and then select **Agent Uninstall**.
3. Select the **Remove** option, and then select **Next**.
4. In ready to Remove Compliance Guardian Agent page, configure the **Remove configuration file** option. Select this option if you want to remove all of the folders and configuration files generated by the Compliance Guardian Agent installation.

   ***Note**: The Logs folder will not be removed whether you select the **Remove configuration file** option or not.

5. Select **Remove** and the Agent uninstallation process starts.
6. Select **Finish** to complete the uninstallation.

Resolve Issues Occurred During the Compliance Guardian Installation

If you encounter other issues when installing the Compliance Guardian Manager or Agents, follow the prompt messages to resolve the issue, and run the installation program again.

If the issue persists, refer to the AvePoint Technical Support site for additional help.

Navigation Bar

After you login to Compliance Guardian, select **Report** or **Administration** on the top-left corner of the home page. The navigation bar appears. You can navigate to your desired module by selecting the corresponding tab in the navigation bar.

Control Panel

The Compliance Guardian Control Panel is the central interface for managing Compliance Guardian and how it interacts with your SharePoint environments.

Control Panel is also integrated into other Compliance Guardian products, enabling you to configure relevant settings without having to leave the interface of the module you are using.

Getting Started

Refer to the following sections for important information on getting started with Control Panel.

Launching Control Panel

To launch Control Panel and access its functionality, complete the following steps:

1. Log in to Compliance Guardian. If you are already in the software, select the home page button ( ) on the top-left corner to go back to the home page.
2. From the **Compliance Guardian** home page, select **Control Panel** to launch the Control Panel.
3. Alternatively, you can select **Administration** on the top-left corner, and select the **Control Panel** tab on the appeared navigation bar to launch Control Panel.

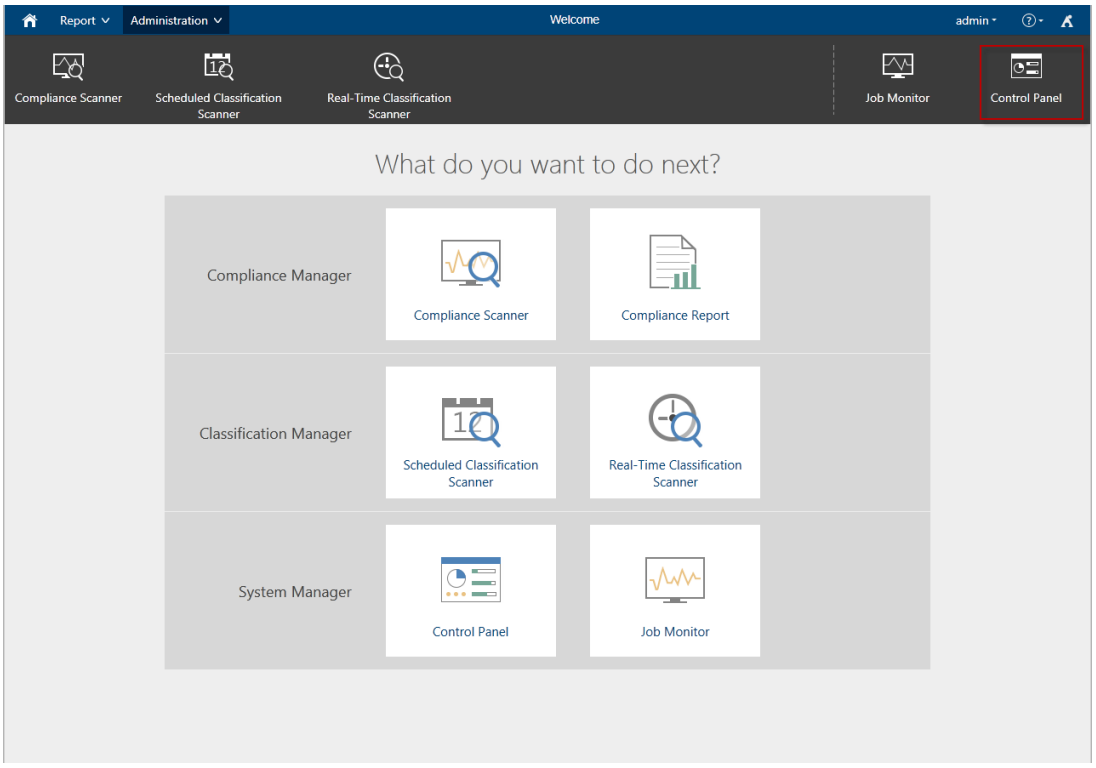

Figure 7: Control Panel tab on the navigation bar.

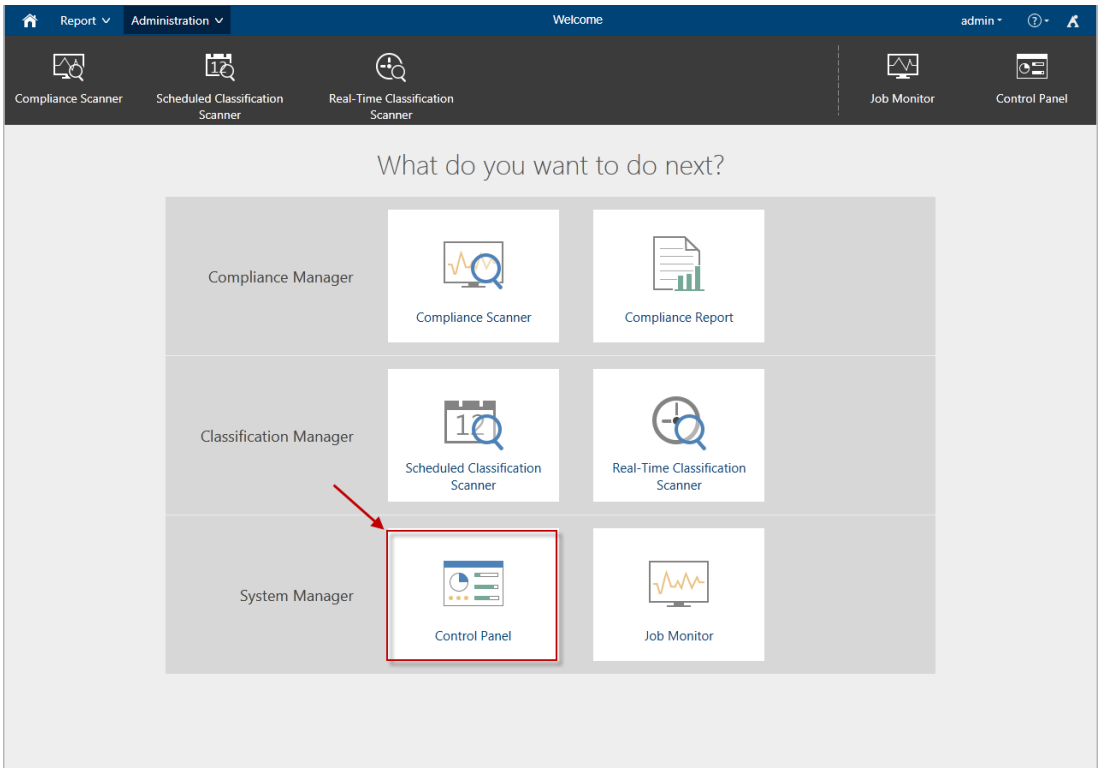

Figure 8: Compliance Guardian module launch window.

Understanding the Control Panel

Control Panel has three key groups of components:

- **General System Settings** – View and manage your Compliance Guardian settings, managers, agents, authentication, licenses, and product version. All of these functions are performed in Control Panel so that you can easily access them without leaving the interface for your current task in Compliance Guardian.
- **Common Application Settings** – Configure settings affect common tasks performed by all Compliance Guardian products. All of these settings are configured in Control Panel so that you can easily access them without leaving the interface for your current task in Compliance Guardian.
- **Specific Products Settings** – Certain products in Compliance Guardian use preset configurations for certain functionalities. While these settings may not affect all Compliance Guardian products, all of these settings are configured in Control Panel because they can be leveraged by more than one product.

Accessing the Control Panel

Since features in Control Panel overlap with so many products, it is important that it is easily accessible, but not disruptive of your current task. For this reason, while there are many ways to access Control Panel, the interface opens as a pop-up window so that you can remain on whichever page you are on, and when you are finished configuring settings in Control Panel, closing it will return you to the page you were on.

To access Control Panel, select the **Compliance Guardian** tab, and then select **Control Panel**. At any point while in Compliance Guardian, select the **Control Panel** button ( ) in the upper left hand corner to launch Control Panel. While in the interface of a certain product, if the product utilizes a feature in Control Panel, selecting on that feature on the ribbon of the product page will bring up the Control Panel pop-up window with the appropriate tab open. Whenever you are finished configuring settings in Control Panel, close the window to return to the previous screen you were on.

Monitor

The monitor features in the Control Panel of Compliance Guardian allow you to view and manage Compliance Guardian Control Service and Compliance Guardian Agents:

- **Manager Monitor** – Here you can view details about your Compliance Guardian Control Service.
- **Agent Monitor** – Here you can view and configure your Compliance Guardian Agents currently installed on your SharePoint environment. This can be useful if there is a change in personnel, and the SharePoint account that the Agent uses to communicate with SharePoint needs to be changed. With Agent Monitor, you can also perform basic

maintenance operations on your agents if an agent ever becomes unresponsive or is having issues, or temporarily disable the Compliance Guardian Agent Service to perform server maintenance.

Using the Manager Monitor

To access Manager Monitor in the Control Panel interface, select **Manager Monitor** under the Monitor heading. In Manager Monitor, you will see the Compliance Guardian Control Service.

You can select the Control Service by checking the checkbox next to the service name, then select **View Details** on the ribbon to bring up the **View Details** page with information about the selected Manager Service. When you are finished viewing the information about the Control Service, select **Close** on the ribbon to close the Manager Monitor tab and return to the Control Panel main page.

Using the Agent Monitor

To access Agent Monitor, open the Control Panel interface, and then select **Agent Monitor** under the Monitor heading. In Agent Monitor, you will see a list of Compliance Guardian Agents which have been registered to the current Compliance Guardian Control Service. You can customize how your agents are displayed in the following ways:

- **Search** – Filter the agents displayed by the keyword you designate; the keyword must be contained in a column value. At the top of the Agent Monitor viewing pane, enter the keyword for the agents you want to display. You can select to **Search all pages** or **Search current page**.
- **Manage columns** (( ) – Manage which columns are displayed in the list so that only the information you want to see will be shown. Select the manage columns button ( ), and then check the checkbox next to the column name to have that column shown in the list.
- **Hide the column** ( ) – Hover over a column name, and then select the hide the column button ( ) in the column name to hide the column.
- **Filter the column** ( ) – Filter which item in the list is displayed. Unlike Search, you can filter whichever item you want, rather than search based on a keyword. Hover over a column name, and then select the filter the column button ( ) of the column you want to filter, and then check the checkbox next to the item name to have that item shown in the list. To remove all of the filters, select **Clear Filter**.

Once your Compliance Guardian Agents are appropriately displayed, you can select an agent by checking the checkbox next to the Agent Name, and then select:

- **Configure** – Once you select an agent, this button will become available. Select **Configure** on the ribbon to access the Agent Configuration interface. Here you can configure the SharePoint Account for the agent as well as the agent type.
    - **SharePoint Account**– The SharePoint Account is used by the Compliance Guardian Agent to provide Compliance Guardian with access and control to your

SharePoint environment. The account configured here must have the required permissions for the Compliance Guardian products that are enabled. To configure the SharePoint account, enter the **Username** and **Password** for the desired account into the corresponding text box.

- **Agent Type Configuration** – In order to use a certain product, the corresponding agent type must first be configured. Before selecting the product, the necessary agents for that product must already be installed.

  To configure the agent type for the agent, check the checkbox next to the corresponding product. You can navigate through the different product suites that are enabled by selecting on the name of the suite. The configuration of the agent type is on your local environment.

- **Job Restriction** – Limit the maximum number of jobs that are allowed to run simultaneously by this agent by enabling the **Restrict the simultaneously running job count** option and enter a positive integer into the text box.

Once you are finished configuring the agent, select **OK** to save the configurations and return to the Agent Monitor interface, or select **Cancel** to return to the Agent Monitor interface without saving any changes.

- **Configuration File** – Upload agent configuration files to the Manager Server and change them for the specified agents. Select the desired Compliance Guardian Agents in Agent Monitor and select **Configuration File** on the ribbon to change the configuration file for them. In the pop-up window, select **OK** to confirm the modification action and you will be redirected to the configuration page. Refer to the instructions below to change the configuration file.

  ***Note**: Since modifying the agent configuration files can be risky, it is not recommended for end-users to do it.

  - **Agent Information** – In this field, you can view the agents you have selected previously.
  - **Browse Configuration File** – Upload the configuration file to the Manager Server. Select **Browse** to find the specified **.config** file and select **Open** to upload it. You are able to upload multiple configuration files.

    ***Note:** The name of the configuration file you upload must have the same name as the existing one, and then you are able to apply the configuration file to destination.

  - **Destination Path** – Enter the place where you want to upload the configuration file. Compliance Guardian supports configuration file change in **Agent\Bin** and **Agent\data** paths.
  - **Conflict Resolution** – Select a resolution when two configuration files have the same name.

- **Merge** – The content of the newly uploaded configuration file will be merged into the old one.
- **Replace** – The newly uploaded configuration file will replace the old one.

Select **OK** to change the configuration files as you have configured or select **Cancel** to exit the interface without saving the configuration. If you select **OK**, you will be asked to restart the Agent Service. Select **Auto** to automatically restart the Agent Service immediately or select **Manual** to manually restart the Agent Service later.

- **View Details** – Select **View Details** on the ribbon to bring up the View Details page with information about the selected Compliance Guardian Agent.
- **Restart** – Select **Restart** on the ribbon to restart the selected Compliance Guardian Agent. This is useful in situations where the agent is sluggish, or if a job it is running hangs. You can restart the agent and try again.

  ***Note**: Any jobs that are running when you restart the agent will fail.

- **Remove** – Select **Remove** on the ribbon to remove the selected Compliance Guardian Agent from the Agent Monitor. The removed agent will no longer be used by the Control Service. You can only remove agents that have a down arrow ( ) in the **Status** column. Removing an agent does not uninstall the agent.

  ***Note**: When removing the last agent of one farm in Agent Monitor, the associated farm and plans will also be deleted from the Compliance Guardian databases.

- **Deactivate** – Select **Deactivate** on the ribbon to deactivate the selected Compliance Guardian Agent. Once the agent is deactivated, it is marked as **Inactive***,* and will not be used by the current control service. However, the deactivated service will still run normally. This is useful when you want to perform maintenance on a specified Compliance Guardian Agent.

  ***Note**: Any jobs that are running when you deactivate the agent will fail.

- **Activate** – Select **Activate** on the ribbon to activate the selected Compliance Guardian Agent. Once the agent is activated, it is marked as **Active***,* and will be used by the current control service.

When you are finished viewing and managing your Compliance Guardian Agents, select **Close** on the ribbon to close the Agent Monitor tab and return to the Control Panel main page.

System Options

System Options allow you to customize the Compliance Guardian software interface itself. Within the System Options tab, you can access Compliance Guardian General Settings, Security Settings, and Advanced Settings:

- **General Settings** – These settings affect Compliance Guardian's interface, which includes settings for Appearance and SharePoint Farm Settings. You can display Compliance Guardian in the language of your preference, use date and time format that you are comfortable with, insert a custom logo for your reports and e-mail templates, and rename your SharePoint farms so that it is easier for you to recognize them.
- **Security Settings** – These settings affect access to Compliance Guardian, which includes settings for System Security Policy and System Password Policy. This way, you have control over the users that are able to access Compliance Guardian.

Configuring General Settings

To access General Settings for Compliance Guardian, open the Control Panel interface, and then select **General Settings** under the System Options heading.

The following settings can be configured in this page:

- **Language Preference** – Specify a language for Compliance Guardian to be displayed in, or allow users to utilize a translation engine to have Compliance Guardian displayed in the language of the user's browser.
    - **Display … for all users** – Select this option to display Compliance Guardian in the language specified here. To change the display language, select the drop-down menu, and select your desired language.
    - **Change to the end user browser used language** – Select this option to allow Compliance Guardian to be displayed in the language used by the user's browser. Then select a language for Compliance Guardian to default to in the **If the language does not change successfully, please select to use a default language** drop-down menu. This way, if Compliance Guardian does not properly display in the user's browser language, Compliance Guardian will be displayed in the language specified here.
- **Date and Time Format** – Set the system location by selecting a location from the **Locale (Location)** drop-down menu. Set the format for all date and time displayed in Compliance Guardian by selecting a date format from the **Date format** drop-down menu, and selecting a time format from the **Time format** drop-down menu.
- **Customize Logo** – Customize the logo for Compliance Guardian system reports and e-mail templates. Select **Browse** to find the desired logo file in the pop-up, then select the logo, and select **Open** to open it. Select **Preview** to view the logo in the Show Preview area. To hide the Show Preview area, select **Hide Preview.**

Select and drag the logo in the display field to change its placement. Select the zoom in button (), the zoom out button (), or the reset button () to reset the settings of the new logo. Select **Restore to Default** button to roll back to the default logo.

- **Farm Name Mapping** – Customize the display names for your farms in Compliance Guardian. To find a specific farm, enter the farm name in the search text box, and select the search button (). For each farm, enter the desired display name in the corresponding **Display Name in Compliance Guardian** text field.

  ***Note:** The search function is not case sensitive.

When you are finished configuring Compliance Guardian General Settings, select **Save** to save all changes, then **Close** to exit the System Options interface. If you select **Close** without saving first, any changes you have made will be lost.

Configuring Security Settings

To access Security Settings for Compliance Guardian, open the Control Panel interface, and then select **General Settings** under the System Options heading. Select **Security** on the ribbon. There are two tabs under Security Settings, System Security Policy, and System Password Policy.

System Security Policy

In the **System Security Policy** tab, the following options can be configured:

- **Maximum User Session** – Configure the number of simultaneous logons allowed for Compliance Guardian. For any new sessions that surpass the designated number, the earliest session will be terminated.
- **Session Timeout** – Configure how long a user can be inactive before being automatically logged off. Enter an integer into the **Logon will expire in:** text box, and then select either **Minute(s)** or **Hour(s)** in the drop-down menu.
- **Failed Logon Limitation** – Specify the maximum number of failed logon attempts allowed in one day. If a specific account fails to provide the correct login information in a single day, it will be locked. To unlock the specified account, refer to Account Manager.

  ***Note**: The default **admin** account cannot be locked.

- **Inactive Period** – Configure how long a user can be inactive before the account is automatically disabled. Enter an integer into the **Deactivate the account when the inactive period reaches:** text box, then select either **Day(s)** or **Month(s)** in the drop-down menu. Once deactivated, a Compliance Guardian administrator must activate the account before the user can log onto Compliance Guardian.

- **Network Security** – Configure the IP addresses to have the desired level of access to Compliance Guardian. To access these settings, check the **Enable network security** checkbox, and then select either:
    - **Trusted network** – If selected, only the IP addresses added to this field can access Compliance Guardian. To add an IP address as a trusted network, enter the IP address in the **Equals** text box, and then select **Add**. Repeat these steps to add additional IP addresses.
    - **Restricted network** – If selected, the IP addresses added to this field cannot access Compliance Guardian. To add an IP address as a restricted network, enter the IP address in the **Equals** text box, and then select **Add**. Repeat these steps to add additional IP addresses.

System Password Policy

In the **System Password Policy** tab, the following options can be configured:

- **Default Password Settings** – Specify the rules to be applied on the password after it has been saved. Select **Account is inactive** if you would like to manually activate the account before it can be used.

  ***Note:** If no option is selected in this field, the password does not need to be modified at first login, and it will never expire.

- **Maximum and Minimum Password Length** – Enter an integer for the maximum and minimum number of characters allowed in a password.
- **Password Rule** – Configure the requirements for the password.
    - **Minimum number of alpha** – Enter a positive integer. There must be at least the specified number of letters in the password.
    - **Minimum number of numeric** – Enter a positive integer. There must be at least the specified number of numbers in the password.
    - **Minimum number of special characters** – Enter a positive integer, there must be at least the specified number of special characters in the password. The special characters include !, @, #, $, %, ^, &, and *.
    - **Password cannot contain user ID** – Select this option and the password cannot contain the user's name.
    - **Password cannot contain space** – Select this option and the password cannot contain spaces.
- **Password Expiration Warning** – Send out warnings if the password of a user will expire in the specified time period. Set the period by entering a positive integer using the **Day(s)** or **Month(s)** option. You can choose the forms of the warning by selecting the **Pop-up message** or **E-mail notification**.

Viewing Security Information

Compliance Guardian uses a passphrase to protect the Compliance Guardian databases and secure the communication. Before connecting to the Compliance Guardian Manager when installing the Compliance Guardian Agents, the passphrase must be entered to verify the access.

The default passphrase is generated automatically at the end of the Manager's Installation. To manage the passphrase, open the System Options tab, and then select **Security Information** on the ribbon to perform the following actions:

- **Back Up** – Select this button to back up the passphrase to the following path: **…\AvePoint\Compliance Guardian\Manager\KeysBak.** It is strongly recommended that you back up the security keys and save the backup in a safe place.
- **Manage Passphrase** – Select this button to view and modify the passphrase. The **Modify** option will be displayed. By default, the password cannot be modified. You can select this button to enable the modification of the default password. Enter a new passphrase in the corresponding text box and select **OK** to save it.

  ***Note**: Only the users of Administrators group have the permission to modify the passphrase. For details of adding users into Administrators group, refer to Managing Users.

Authentication Manager

Authentication Manager allows you to view and manage integrated authentication methods usable by Compliance Guardian. This means that Compliance Guardian can leverage your pre-existing authentication methods, and customize it for access to Compliance Guardian. These authentication methods include:

- Windows Authentication – Allows the users to log onto Compliance Guardian using their Windows Authentication credentials.
- AD Integration – Allows the users to log onto Compliance Guardian using their Active Directory authentication credentials.
- ADFS Integration – Allows the users to access Compliance Guardian as long as they have logged into the local machine using their ADFS credentials.

To access Authentication Manager for Compliance Guardian, open the Control Panel interface, select **Authentication Manager** under the Authentication Manager heading. Select **Close** on the ribbon to close the Authentication Manager interface.

Configuring Windows Authentication

To leverage Windows Authentication credentials to access Compliance Guardian, complete the following steps:

1. In the Authentication Manager interface, select **Windows Authentication** on the ribbon.
2. Select the **Authentication Type** from the drop-down menu:
    - NTLM
    - Negotiate (Kerberos)

      ***Note**: Kerberos authentication method must be previously configured in the operating system before you select the **Negotiate (Kerberos)** option when enabling the integration with Windows Authentication. Otherwise, the **NTLM** authentication method will be enabled.
3. Select **OK** to save any changes made and close the Windows Authentication interface, or select **Cancel** to close the Windows Authentication interface without saving any changes made.

Configuring AD Integration

To leverage Active Directory authentication credentials to access Compliance Guardian, configure your Active Directories in the AD Integration interface.

To access your Active Directory integration configurations, open the Authentication Manager interface, and then select **AD Integration** on the ribbon. In the AD Integration configuration interface, you will see a list of previously configured Active Directories. You can customize how these Active Directories are displayed in the following ways:

- **Search** – Filter the Active Directories displayed by the keyword you designate; the keyword must be contained in a column value. At the top of the viewing pane, enter the keyword for the Active Directory you want to display. You can select to **Search all pages** or **Search current page**.
- **Manage columns** (( ) – Manage which columns are displayed in the list so that only the information you want to see will be shown. Select the manage columns button ( ), and then check the checkbox next to the column name to have that column shown in the list.
- **Hide the column** ( ) – Hover over a column name, and then select the hide the column button ( ) in the column name to hide the column.
- **Filter the column** ( ) – Filter which item in the list is displayed. Unlike Search, you can filter whichever item you want, rather than search based on a keyword. Hover over a column name, and then select the filter the column button ( ) of the column you want to filter, and then check the checkbox next to the item name to have that item shown in the list. To remove all of the filters, select **Clear Filter**.

To manage your integrated Active Directories, you can perform the following actions:

- **Add** - To add a new Active Directory, select **Add** on the ribbon, then enter the **Domain**, **Username** and **Password** in the corresponding text box. Select **Validation Test** to see if the values you entered are valid, and then select **OK** to save the configurations for the new Active Directory and return to the AD Integration interface, or select **Cancel** to return to the AD Integration interface without saving the configurations.
- **Edit** – To make changes to a previously configured integrated Active Directory, select the Active Directory by checking the corresponding checkbox, then select **Edit** on the ribbon. Make the necessary changes, and then select **OK** to save the changes and return to the AD Integration interface, or select **Cancel** to return to the AD Integration interface without saving any changes.
- **Delete** – To delete a previously configured Active Directory, select the Active Directory by checking the corresponding checkbox, then select **Delete** on the ribbon. You will be presented with a pop-up window notifying you that "**The user(s) associated with the selected domain(s) will be disabled. The user(s) can be enabled only by adding the selected domain(s) again. Are you sure you want to proceed?"**. There is also an option to remove all of the users that are associated with the selected Active Directories from Compliance Guardian; to do so, check the **Remove all users associated with the selected domain(s)** checkbox. Select **OK** to confirm the deletion, or select **Cancel** to return to the AD Integration interface without deleting the selected Active Directories.
- **Enable** – Select **Enable** to allow the use of credentials from the corresponding Active Directory to access Compliance Guardian.
- **Disable** – Select **Disable** to not allow the use of credentials from the corresponding Active Directory to access Compliance Guardian. This option is useful during the maintenance of the Domain Controller machine. You can disable the integration with the domain to be maintained and enable the integration again after the maintenance.

After one Active Directory has been integrated with Compliance Guardian, it will be shown in the **Domain** text box after you select **AD Integration** in the **Log on to** drop-down list of the Compliance Guardian login page. If a domain has father domain, sub domain or trust domain, when a user from these domains has been added to Compliance Guardian, the corresponding domain will also be added into Compliance Guardian and you will be able to view this domain in Compliance Guardian login page.

Configure ADFS Integration

To leverage Active Directory Federation Services (ADFS) authentication credentials to access Compliance Guardian, configure your ADFS integration in the ADFS Integration interface.

To access your ADFS integration configurations, in the Authentication Manager interface, select **ADFS Integration** on the ribbon, then select **ADFS Integration** in the drop-down menu. You will be brought to the **ADFS Integration Configure Wizard**. Complete the following steps in the wizard to set up ADFS integration:

1. **ADFS Information** – Specify the following general information of the ADFS you want to integrate:
    - ADFS Integration Method – Select **Manually** to configure the settings yourself, or select **Automatically** to get the required information by using a federation metadata trust XML file.
        - Manual configuration – Enter the URL of the security token service (STS) in the **ADFS Issuer** text box in the following format: **https://full qualified domain name/adfs/ls**
        - Automatic configuration – Enter the URL of the federation metadata trust XML file in the **Federation Metadata Trust** text box in the following format: **https://full qualified domain name/FederationMetadata/2007-06/FederationMetadata.xml**
    - Relying Party Identifier – Enter Compliance Guardian's Relying Party Identifier, which must first be configured in ADFS in the **Relying Party Identifier** text box.

    When you are finished configuring the ADFS Information, select **Next** to configure the Security Token Settings.

2. **Security Token Settings** – Configure the certificates used in the ADFS integration:
    - Token-signing – Choose **Select.** A new Select Certificate pop-up window will appear for you to specify a token-signing certificate to communicate with ADFS. This certificate must be the same as the one configured in ADFS. Alternatively, you may also select **Find Certificate** to search for the desired certificate. Select a **Find in:** parameter from the drop-down menu, enter the keywords in the **Contains:** text box, select a **Look in field:** parameter from the drop-down menu, then select **Find Now** to start the search. Select **Stop** to stop the search. Once you have selected your desired certificate, select **OK** to save and exit the Select Certificate interface, or select **Cancel** to exit the Select Certificate interface without saving specifying a certificate.

        ***Note**: The certificate specified here must be the same as the one configured in ADFS.

    - Token-decrypting (optional) – Choose **Select.** A new Select Certificate pop-up window will appear for you to specify a token-decrypting certificate to protect the communication between Compliance Guardian and ADFS. This certificate must be the same as the one configured in ADFS. Alternatively, you may also select **Find Certificate** to search for the desired certificate. Select a **Find in:** parameter from the drop-down

menu, enter the keywords in the **Contains:** text box, select a **Look in field:** parameter from the drop-down menu, then select **Find Now** to start the search. Select **Stop** to stop the search. Once you have selected your desired certificate, select **OK** to save and exit the Select Certificate interface, or select **Cancel** to exit the Select Certificate interface without saving specifying a certificate.

When you are finished configuring the Security Token Settings, select **Next** to configure the Claim Configuration.

3. **Claim Configuration** – Configure the mappings between the Claim Name displayed in Compliance Guardian and the Claim Type displayed in ADFS. You can perform the following actions to your claims:

   - You can change the order of the claims in the **Order** column of the table. If a user can be identified using several claims, Compliance Guardian will use the Claim Name of the first claim listed here as the display name for each respective user.
   - Select to delete the selected claim.
   - Select **Automatically** to have the claim type be specified automatically after you select the claim name from the **Claim Name** drop-down menu. Select **Manu** to add the claims manually. Select **Auto** to switch back to the default option.

4. **Overview** – Review the settings you have configured in the previous steps. To make changes, select **Edit** in the corresponding section, and you will be brought back to that step so you can make changes.

5. **Finish** – Provides you with three options to import the relying party data for Compliance Guardian in ADFS (using the **Add Relying Party Trust Wizard**).

   - **Option 1** – Select the link to import relying party data that is published online from the local network Federation metadata address.
   - **Option 2** – Select the link to download the Federation metadata XML file, then upload the downloaded file to the ADFS server. Follow the wizard to configure other settings.
   - **Option 3** – Enter the relying party data and the relying party identifier manually in the ADFS configuration wizard.

   In this step, you can also choose to export the current ADFS configuration information to a specified location by selecting **Export** on the ribbon, then explore to the location you want to save the XML file to.

   Select **Finish** to save your configurations, and return to the Authentication Manager interface, or select **Cancel** to return to the Authentication Manager interface without saving any of the configurations made.

Once you have configured an ADFS integration for Compliance Guardian, the **Add Federation Trust** option will become available**. Add Federation Trust** allows you to integrate another trusted ADFS with the ADFS you have already configured for Compliance Guardian.

To add integration with another trusted ADFS, open the Authentication Manager interface, select **ADFS Integration** on the ribbon, and then select **Add Federation Trust** from the drop-down menu. In the Add Federation Trust interface, enter the following information:

- **Name** – The name entered here will be displayed in the **Server** drop-down menu on the login page. You can select the corresponding name to log on Compliance Guardian using the trusted ADFS.
- **URL** – The identifier of the trusted ADFS.

  Select **Add** to add the new record or select ✕ to delete a selected ADFS trust.

Account Manager

Account Manager allows you to view and manage users and configure user groups with custom permission levels for Compliance Guardian. This module allows you to give specific people, or groups of people your desired level of access to Compliance Guardian.

In Account Manager you can give specified permissions to Compliance Guardian users to limit which Compliance Guardian module a user is able to access and which farms specific Compliance Guardian users can access. A user can belong to multiple groups.

***Note:** If you would like to leverage authentication credentials from Windows Authentication, AD or ADFS, you must first configure the relevant integration settings in the Authentication Manager.

To access Account Manager for Compliance Guardian, open the Control Panel interface, and then select **Account Manager** under the Account Manager heading. Select **Close** on the ribbon to close the Account Manager interface.

Managing Permission Levels

The Permission Level module allows you to create pre-configured permissions that can be applied to user groups or users to quickly and easily apply the same permission configuration for multiple users.

To configure permission levels for Compliance Guardian, open the Account Manager interface, and then select **Permission Level** on the ribbon. In the Permission Level interface, previously configured Permission Levels will be displayed.

You can customize how these permission levels are displayed in the following ways:

- **Search** – Filter the permission levels displayed by the keyword you designate; the keyword must be contained in a column value. At the top of the viewing pane, enter the keyword for the permission level you want to display. You can select to **Search all pages** or **Search current page**.

- **Manage columns** (⊞) – Manage which columns are displayed in the list so that only the information you want to see is shown. Select the show column button (⊞), then check the checkbox next to the column name to have that column shown in the list.
- **Hide the column** (⊖) – Hover over a column name, and then select the hide the column button (⊖) in the column name to hide the column.
- **Filter the column** ( ) – Filter which item in the list is displayed. Hover over a column name, and then select the filter the column button ( )of the column you want to filter, and then check the checkbox next to the item name to have that item shown in the list. To remove all of the filters, select **Clear Filter**.

To manage your permission levels, you can perform the following actions:

- **Add** – To create a new permission level, select Add on the ribbon. After selecting to add the corresponding permission level, you will be redirected to the configuration page to perform the following actions:
  - **Name and Description** – Enter a name for the new system permission level and an optional **Description** for future reference.
  - **Module** – Select the modules you want to grant permission to for all groups and users using this permission level.

  Select **OK** to save the configuration. Select **Cancel** to return to the Permission Level Interface without saving changes.

- **Edit** – To edit a previously configured permission level, select the permission level you want to edit by checking the corresponding checkbox, then select **Edit** on the ribbon. In the Edit Permission Level interface, you can modify the **Name** and a **Description** of this Permission Level. In the Module section, you can select the modules you want to allow this permission level to access by checking the corresponding checkboxes. You can select a product suite name to modify the access to its modules.

  ***Note:** Unlicensed products have grayed out tabs and cannot be configured. Select **OK** to save the modifications for the permission level and return to the Permission Level interface, or select **Cancel** to return to the Permission Level interface without saving the modifications.

- **Delete** – To delete a previously configured permission level, select the permission level you want to delete by checking the corresponding checkbox, and then select **Delete** on the ribbon. A pop-up window will appear to confirm this action. Select **OK** to delete the selected permission level and return to the Permission Level interface, or select **Cancel** to return to the Permission Level interface without deleting the selected permission level.

When you are finished managing your permission levels, select **Cancel** on the ribbon to return to the Account Manager interface.

There are four permission levels configured in advance:

- **Real-Time Classification Scanner** – This permission level only enables the Real-Time Classification Scanner module.
- **Scheduled Classification Scanner** – This permission level only enables the Scheduled Classification Scanner module.
- **Compliance Report** – This permission level only enables the Compliance Report module.
- **Compliance Scanner** – This permission level only enables the Compliance Scanner module.

Managing User Groups

User groups allow you to apply the same permission levels to all users within the same user group. This way, you can change the permission levels of multiple users by editing your user group rather than individually configuring permission levels for each user. You can also change the permission levels of a user by changing the group they belong to with pre-configured permission levels.

To access your user group configurations, go the Account Manager interface and then select **Groups** on the ribbon. In the Groups configuration interface, you will see a list of previously configured user groups. The Administrators group comes pre-configured and users of this group have Full Control permissions for all modules.

You can customize how these user groups are displayed in the following ways:

- **Search** – Filter the user groups displayed by the keyword you designate; the keyword must be contained in a column value. At the top of the viewing pane, enter the keyword for the user group you want to display. You can select to **Search all pages** or **Search current page**.
- **Manage columns** (⊞) – Manage which columns are displayed in the list so that only the information you want to see is shown. Select the manage columns button (⊞), then check the checkbox next to the column name to have that column shown in the list.
- **Hide the column** (⊖) – Hover over a column name, and then select the hide the column button (⊖) in the column name to hide the column.
- **Filter the column** ( ) – Filter which item in the list is displayed. Unlike Search, you can filter whichever item you want, rather than search based on a keyword. Hover over a column name, and then select the filter the column button ( )of the column you want to filter, then check the checkbox next to the item name to have that item shown in the list. To remove all of the filters, select **Clear Filter**.

To manage your user groups, you can perform the following actions:

- **Add Group** – To add a new group, select **Add Group** on the ribbon. You will be directed to the configuration page accordingly, and then you can perform the following actions:
    - **Group Information** – Enter a **Group Name** for the new group, then enter an optional **Description** for future reference.
    - **Group Permissions** – In the Scope section, select **Global permission** to grant the users of this group access to all farms with the permission levels configured here or select **Permission for different farms** to grant users of this system group access to specific farms with the configured system permission levels. If **Global permission** is selected, choose which or all of the Permission Levels you want to associate with this Group. If **Permission for different farms** is selected, for each farm, choose which or all of the Permission Levels you want to associate with this group.

      ***Note:** At least one permission level must be assigned to the new group.

  When you are finished configuring the settings for the new group, select **OK** to save and return to the Account Manager interface, or select **Cancel** to return to the Account Manager interface without saving the configurations.

- **Edit Group** – To edit a group, select the group by checking the corresponding checkbox, then select **Edit Group** on the ribbon, or select the name of the desired group. You will be brought to the Edit Group interface. Here you can change the description for this group, as well as the permission scope and permission levels.

  ***Note**: If you have a group with **Full Control** permission configured in Compliance Guardian, after upgrading to Compliance Guardian, this group will maintain the **Full Control** permission but this will not show up on the interface by default. When you edit this group and change the permission, it will pop up a warning message that the **Full Control** permission of this group will be replaced by the newly granted permissions. You can select **OK** to continue the action and save the change or select **Cancel** to cancel the operation. In Compliance Guardian, only users of **Administrators** group have **Full Control** permission.

  When you have finished making changes to the configurations for this group, select **OK** to save and return to the Account Manager interface, or select **Cancel** to return to the Account Manager interface without saving any changes.

- **Show User(s)** – To view and manage the users in a group, select the group by checking the corresponding checkbox, then select **Show User(s)** on the ribbon. You will be brought to the Show User(s) interface. Here you will see a list of all of the users that belong to this group. You can customize how these users are displayed in the following ways:
    - **Search** – Filter the users displayed by the keyword you designate; the keyword must be contained in a column value. At the top of the viewing pane, enter the

keyword for the user you want to display. You can select to **Search all pages** or **Search current page**.

- **Manage columns** (⊞) – Manage which columns are displayed in the list so that only the information you want to see is shown. Select the manage columns button (⊞), then check the checkbox next to the column name to have that column shown in the list.
- **Hide the column** (⊖) – Hover over a column name, and then select the hide the column button (⊖) in the column name to hide the column.
- **Filter the column** ( ) – Filter which item in the list is displayed. Unlike Search, you can filter whichever item you want, rather than search based on a keyword. Hover over a column name, and then select the filter the column button ( ) of the column you want to filter, and then check the checkbox next to the item name to have that item shown in the list. To remove all of the filters, select **Clear Filter**.

You can perform the following actions on the users of this group:

- **Add User to Group** – To add users to this group, select **Add User to Group** on the ribbon. You will be brought to the Add User to Group interface. Enter the username of the user you want to add, and then select the check names button ( ) to verify that the username you entered is valid. Alternatively, you can select the browse button ( )to search for the desired user. In the pop-up window, enter the value to search for in the **Find** text box, and then select the search button ( )**.** Select the desired user, and then select **Add**. Select **OK** to add the users, or select **Cancel** to close the window without adding the users.
- **Remove User from Group** – To remove users from this group, select the desired users by checking the corresponding checkbox, then select **Remove User from Group** on the ribbon. A confirmation pop-up window will appear to confirm the remove operation. Select **OK** to delete the selected users, or select **Cancel** to return to the Show Users interface without deleting the users.

When you are finished, select **Cancel** to add the defined users to this group and return to the Show Users interface.

There are five groups are configured in advance:

- **Administrators** – The permission scope is Global permission. The users in this group have full control of all Compliance Guardian modules.
- **Real-Time_Classification_Scanner** – The permission scope is Global permission. The users in this group can only access the Real-Time Classification Scanner module.
- **Scheduled_Classification_Scanner** – The permission scope is Global permission. The users in this group can only access the Scheduled Classification Scanner module.
- **Compliance_Report** – The permission scope is Global permission. The users in this group can only access the Compliance Report module.

- **Compliance_Scan** – The permission scope is Global permission. The users in this group can only access the Compliance Scanner module.

Managing Users

***Note**: If a domain is integrated with Compliance Guardian and a user from its parent domain, subdomain or trust domain is added in Compliance Guardian Account Manager, the corresponding parent domain, subdomain or trust domain will be integrated into Compliance Guardian and added to the **Log on to** drop-down list in Compliance Guardian login page.

To view and manage users, go to the Account Manager interface, select **Users** on the ribbon. In the Users interface, you will see a list of previously added users. You can customize how these users are displayed in the following ways:

- **Search** – Filter the users displayed by the keyword you designate; the keyword must be contained in a column value. At the top of the viewing pane, enter the keyword for the user you want to display. You can select to **Search all pages** or **Search current page**.
- **Manage columns** (⊞) – Manage which columns are displayed in the list so that only the information you want to see is shown. Select manage columns button (⊞), then check the checkbox next to the column name to have that column shown in the list.
- **Hide the column** (⊖) – Hover over a column name, and then select the hide the column button (⊖) in the column name to hide the column.
- **Filter the column** ( ) – Filter which item in the list is displayed. Unlike Search, you can filter whichever item you want, rather than search based on a keyword. Hover over a column name, and then select the filter the column button ( ) of the column you want to filter, then check the checkbox next to the item name to have that item shown in the list. To remove all of the filters, select **Clear Filter**.

To manage users, you can perform the following actions:

- **Add User** – To add a user for Compliance Guardian, select **Add User** on the ribbon. You will be brought to the Add User interface. Select the **User Type** to configure the method for authentication:
    - **Local User** – Select **Local User** to manually enter the authentication credentials for this user. Configure the following settings to add a local user:
        - Enter the **Username** and **E-mail** of the user you are adding, as well as an optional **Description** for future reference.
        - Enter the desired password into the **Password** and **Confirm password** text boxes, and then configure the Password Settings. The password entered here must meet the **System Password Policy**. For more information, refer to System Password Policy.

          You can select to use the **Default** password settings, or select **Customized** to configure the password settings manually. Check the

corresponding checkbox next to the **User must change password at next logon**, **User cannot change password**, **Password never expires**, **Account is inactive** setting.

- Set the permissions for this user by adding the user to a previously configured Compliance Guardian user group or manually configure the user's permission levels. Select the **Add user to group(s)** option, and then select the desired user group from the drop-down menu. The user will have all of the permissions of the specified group.

- **Active Directory User/Group** – Select **Active Directory User/Group** to utilize the user's active directory authentication credentials for this new user. Configure the following settings to add an active directory user:
  - Enter the name of the user/group you want to add into the **AD User/Group Name** field, and then select the check names button ( ) to verify that the username you entered is valid. Alternatively, you can select the browse button ( ) to search for the desired user/group. In the pop-up window, enter the value to search for in the **Find** text box, then select the find names button ( )Select the desired user, then select **Add**. Select **OK** to add the users, or select **Cancel** to close the window without adding the users. Enter an optional description for future reference.
  - Set the permissions for this user by adding the user to a previously configured Compliance Guardian user group or, manually configure the user's permission levels. Select the **Add user to group(s)** option, and then select the desired user group from the drop-down menu. The user will have all of the permissions of the specified group.

- **Windows User/Group** – Select **Windows User/Group** to utilize the user's Windows authentication credentials for this new user. Configure the following settings to add a Windows user:
  - Enter the username of the user/group you want to add into the **Windows User/Group Name** field, and then select the check names button ( ) to verify that the username you entered is valid. The users/groups that are in the same domain as the Compliance Guardian Control server can be added to Compliance Guardian. Alternatively, you can select the browse button ( ) to search for the desired user/group; In the pop-up window, enter the value to search for in the **Find** text box, and then select the find name button ( )**.** Select the desired user, and then select **Add**. Select **OK** to add the users, or select **Cancel** to close the window without adding the users.
  - Enter an optional description for future reference.

***Note**: In order to log on Compliance Guardian using the added user, the corresponding user must have the permission to access the machine where the Compliance Guardian Control Service is installed.

- Set the permissions for this user by adding the user to a previously configured Compliance Guardian user group or, manually configure the user's permission levels. Select the **Add user to group(s)** option, and then select the desired user group from the drop-down menu. The user will have all of the permissions of the specified group.

- **ADFS Claim** – Select **ADFS Claim** to utilize the user's ADFS authentication credentials for this new user. Configure the following settings to add an ADFS user:
  - Select a **Claim name** from the drop-down menu. Claims are configured in Authentication Manager. Enter the username in the **Claim value** text box. The value entered in the **Claim value** text box will be displayed as the logon name for the user in Compliance Guardian.
  - Set the permissions for this user by adding the user to a previously configured Compliance Guardian user group or, manually configure the user's permission levels. Select the **Add user to group(s)** option, and then select the desired user group from the drop-down menu. The user then has all of the permissions of the specified group.

When you are finished, select **OK** to add the user and return to the Users interface, or select **Cancel** to return to the Users interface without saving the configurations for this new user.

- **Edit User** – To edit a user for Compliance Guardian, select the user by checking the corresponding checkbox, and then select **Edit User** on the ribbon, or select the username. You will be brought to the Edit User interface where you can configure the following settings for a user:
  - **Edit Information** – Edit the user information for the current user.
    - **E-mail** – Enter the e-mail address of the current logged-on user.
    - **Description** – Enter the optional description for future reference.
  - **Password** – Change the user password and configure the security settings for the logged-on user. Check the **Change my password** checkbox, supply the **New password**, and re-enter the new password in the **Confirm new password** field. Select the desired security settings by checking the corresponding checkboxes. If desired, select a deactivation method for the password:
    - **Never** – The password never expires.
    - **After __ day(s)** – Enter the number of days you wish the password to be valid for before it expires.

        - **On __** – Select the calendar button (15) to choose the date when you wish the password to expire.

    - **Group** – Change the group the logged-on user belongs to. Select the desired group from the drop-down menu. The user will have all of the permissions of the specified group. When you are finished, select **OK** to save your changes and return to the Users interface, or select **Cancel** to return to the Users interface without saving any changes made.

- **Delete User** – To delete previously configured users, select the users by checking the corresponding checkbox, then select **Delete User** on the ribbon. A confirmation window will pop up for this deletion. Select **OK** to delete the selected users, or select **Cancel** to return to the Account Manager interface without deleting the selected users.

- **Activate** – To activate the **Inactive** user, select the user by checking the corresponding checkbox, then select **Activate** on the ribbon.

  ***Note:** If a user fails to provide the correct credentials when attempting to log into Compliance Guardian, they will receive the following alert: **Sorry, the login ID or password is incorrect**. If the user receives this alert more times than the number of Failed Login Attempts, the user's account will become **Inactive**.

- **Deactivate** – To deactivate the **Active** user, select the user by checking the corresponding checkbox, then select **Deactivate** on the ribbon.

My Settings

In Compliance Guardian, some users do not have the permission to navigate to the Account Manager. **My Settings** allows the user to edit his/her own account information.

When you log into Compliance Guardian GUI, the currently logged-on user will be displayed at the top right corner of the Compliance Guardian interface. Select the current username and a drop-down list will appear. Select **My Settings** and enter the My Settings interface where you can view detailed information of the current logged-on user and the Compliance Guardian groups it belongs to. Select **Edit** on the ribbon and you can configure the settings. For details on how to configure the settings, refer to Managing Users. In addition, refer to the following information:

1. In the **Password** field, if one user does not have the permission to change the password, the password field will be grayed out. You must supply the **Old password** here.
2. In the **Group** field, refer to the following information:
    - Only users of **Administrators** group have the permission to change the Compliance Guardian groups it belongs to. If a user both belongs to **Administrators** group and the other groups, it also has the permission to change the Compliance Guardian groups it belongs to. If the user moves itself out of **Administrators** group, the action will take effect the next time that user logs in.
    - If the user is **admin** (Compliance Guardian default user), it can view that it belongs to the **Administrators** group but is not able to edit the **Group** setting.

- For users who do not belong to the **Administrators** group, they can only view the group names they belong to and are not able to edit the **Group** setting.

After you have saved the modifications, select **Cancel** to exit the My Settings interface and return to the previous Compliance Guardian interface you are in.

License Manager

Compliance Guardian licensing is based on different conditions:

- Compliance Guardian for SharePoint – Charged by the number of SharePoint servers (Web front-end severs + Application servers) per farm. The license for SharePoint 2007, the license for SharePoint 2010, and the license for SharePoint 2013 are separate.

  You can use both the Compliance Scanner and Classification Scanner modules and all built-in test suites if you have the license.

  ***Note:** SharePoint Fast Search servers and SQL Servers are not charged. The Incoming E-Mail server is not free. The **Not Configured** SharePoint servers are not included in the charged servers.

- Compliance Guardian for File System – Charged by Compliance Guardian Agent Service.

  You can use both the Compliance Scanner and Classification Scanner modules and all built-in test suites if you have the license.

- Compliance Guardian for Website – Charged by the number of Check Groups and Website Domains/Hosts.

License Manager provides you with information regarding your Compliance Guardian licenses. Here you are also able to import and export license files, generate license reports, set up expiration notifications, as well as monitor the number of servers you have used up in your license.

To access License Manager for Compliance Guardian, open the Control Panel interface and select **License Manager** under the License Manager heading. Select **Close** on the ribbon to close the License Manager interface.

Viewing License Information

In the License Manager interface, the License Details section displays the following information:

- **License Type** – Whether you have a Trial license or an Enterprise license.
- **Server Host/IP** – The host/IP of the server used to install Compliance Guardian Control Service.
- **Maintenance Expiration Details** – The start time and expiration date of the Compliance Guardian maintenance service you have purchased.

- **License Details** – The detailed license information for every SharePoint version in SharePoint mode, File System mode, or Website mode by selecting the corresponding tab under **License Details**.
    - **SharePoint** – Select the **SharePoint** tab under License Details to see every SharePoint version license information specific to:
        - **Source** – The SharePoint version.
        - **License Type** – The type of license purchased for the product.
        - **Number of Servers** – The number of servers you have bought.
        - **Registered Servers** – The number of servers you have used.
        - **Expiration Time** – The expiration time of the license for this SharePoint.
        - **Status** – The current status of the SharePoint which reflects proper licensing.

      If the **License Type** is **Trial**, the following two columns appear:

        - **Max Scanning Files** – The maximum number of files that can be scanned.
        - **Remaining Scanning Files** – The number of the files that can still be scanned.

      ***Note**: You are only able to view the SharePoint you are licensed for.

    - **File System** – Select the **File System** tab under **License Details** to see File System license information specific to:
        - **License Type** – The type of license purchased for the product.
        - **Number of Agents** – The number of agents you have bought.
        - **Registered Agents** – The number of agents you have used.
        - **Expiration Time** – The expiration time of the license for File System.
        - **Status** – The current status of the SharePoint which reflects proper licensing.

      If the **License Type** is **Trial**, the following two columns appear:

        - **Max Scanning Files** – The maximum number of files that can be scanned.
        - **Remaining Scanning Files** – The number of the files that can still be scanned.
    - **Website** – Select the **Website** tab under **License Details** to see Website license information specific to:
        - **License Type** – The type of license purchased for the product.
        - **Expiration Time** – The expiration time of the license for the website.

- **Status** – The current status of the SharePoint which reflects proper licensing.
- **Check Groups** – Display the Check groups.
- **Used Host** – The number of hosts you have used.
- **Remaining Host** – The number of hosts you have not used.
- **Used Domain** – The number of domains you have used.
- **Remaining Domain** – The number of domains you have not used.

If the **License Type** is **Trial**, the following two columns appear:

- **Max Scanning Files** – The maximum number of files that can be scanned.
- **Remaining Scanning Files** – The number of the files that can still be scanned.

Select **Details** to the right of **Check Groups** to view details about the used hosts, remaining hosts, used domains, and remaining domains.

Importing and Exporting the License File

In License Manager, you can import a license file to apply that new license. Since all of Compliance Guardian products are installed as a single platform, activating any product is as simple as applying the new license file.

To import a license file, select **Import** on the ribbon. In the Import License interface, select **Browse**. Find and choose the desired LIC file, then select **Open**. You will see a summary view of this license. Select **Apply** to apply this license, or select **Cancel** to return to the previous page without applying this license.

***Note**: Compliance Guardian will automatically log you off in order to use the new license upon logging in again.

Configuring License Renewal Notifications

Compliance Guardian can be configured to notify you before licenses or maintenance expires. You can set how many days prior to expiration and at what interval you want to be notified, as well as configure the method of notification to use.

To configure License Renewal Notifications, select **Settings** on the ribbon. You will be brought to the License Renewal Notification Settings interface. Here you can configure the following settings for Notification Schedule:

- **By expiration date** – Configure these settings for notifications of license expiration:
  - Enter a positive integer into the text box and select **Day**, **Week** or **Month** from the Remind me starting from __ before license expires for any modules drop-down menu.
  - Check the **Interval** checkbox to have the reminder repeat at a set interval. Enter a positive integer into the text box and select **Day**, **Week** or **Month** from the drop-down menu.
- **By maintenance expiration date** – Configure these settings for notifications of maintenance expiration:
  - Enter a positive integer into the text box and select **Day**, **Week** or **Month** from the **Remind me starting from __ before license maintenance expires** drop-down menu.
  - Check the **Interval** checkbox to have the reminder repeat at a set interval. Enter a positive integer into the text box and select **Day**, **Week** or **Month** from the drop-down menu.
- **By number of servers** – Configure these settings for notifications of the number of available servers left for any farm.
  - Enter a positive integer into the text box and Compliance Guardian will send you a notification when the number of servers left of any farm is less than the specified value.
  - Check the **Interval** checkbox to repeat the reminder at a set interval. Enter a positive integer into the text box and select **Day**, **Week**, or **Month** from the drop-down menu.

Configure the following settings for the Notification Method:

***Note:** You must select at least one of the options in order for License Renewal Notifications to work.

- **Pop-up message box when you login** – Select this option to have a message box pop up with a reminder for expiring licenses or maintenance.
- **E-mail notification** – Select this option to be notified of expiring licenses or maintenance by e-mail based on the Notification Schedule you configured above. A drop-down menu will appear where you can either select a previously configured Notification Profile or you can choose **New Notification Profile** to set up a new e-mail notification profile. For more information on how to configure the notification profile, refer to User Notification Settings.

When you are finished configuring License Renewal Notification Settings, select **OK** to save and return to the License Manager interface, or select **Cancel** to return to the License Manager interface without saving the new configurations.

Configuring Server Usage

In Server Usage, you can register a new farm/agent or remove a previously registered farm/agent.

Select **Server Usage** on the ribbon or the server number/agent number in the **Registered Servers/Registered Agents** column of the **License Details** area to enter the **Server Usage** interface. Refer to the instructions below to configure the settings.

Select a SharePoint/File System tab, and then modify its registered farms or agents. You can perform the following actions:

- Register a farm/agent – Select the farm or agent you want to register in the **Unregistered Farms/Unregistered Agents** list and select **Add>>**. The farm or agent will be moved to the **Registered Farms/Registered Agents** list.
- Unregister a farm – Select the farm or agent you want to unregister in the **Registered Farms/Registered Agents** list and select **<<Remove** button. The farm or agent will be moved to the **Unregistered Farms/Unregistered Agents** list.

***Note:** If the number of servers in the **Registered Farms/Registered Agents** list reaches the number of servers/agents for which the license you have purchased allows, Compliance Guardian will not allow you to register more farms or agents and the exclamation point ( ) will appear left of the SharePoint/File System name.

Select **OK** to save the changes or select **Cancel** to cancel the operation. You will then be redirected to the License Manager interface.

Update Manager

Compliance Guardian Update Manager provides you with information regarding Compliance Guardian versions. You can check whether you are running the most up to date version of Compliance Guardian, download updates, view download and installation history, and configure download and update settings. Update Manager allows you to update the current version of Compliance Guardian within the Compliance Guardian GUI to reduce the time and risk of a manual update.

Before performing an update, if multiple Compliance Guardian Control Services are installed in the Windows Network Load Balance environment, the **Download Location** must be configured before you can perform the update operation successfully.

To access Update Manager for Compliance Guardian, navigate to the Control Panel interface, and then select **Update Manager** under the Update Manager heading. Select **Close** on the ribbon to close the Update Manager interface.

Configuring Update Settings

In Update Manager, you can configure settings for custom locations to download updates, set Update Manager to download or check for updates automatically, and configure a proxy server for downloading Compliance Guardian updates. To configure these settings, select **Update Settings** on the ribbon. You will be brought to the Update Settings interface where you can configure the following settings:

- **Download Location** – Download Compliance Guardian updates to a net share path and store them for future use. To utilize this capability, check the **Use the Net Share path as the update storage location** checkbox, and then enter the **UNC path**, **Username**, and **Password** into the corresponding text boxes.

  ***Note**: The UNC path should be entered in the following format: **\\admin-PC\c$\data** or **\\admin-PC\c$\shared** folder.

  Select **Validation Test** to verify the access to the specified path.

  If you are changing the download location to a new one, you can perform the following two actions on the previously downloaded updates in the old path:

  - **Move the uninstalled update(s) to the new location** – All of the uninstalled updates whose versions are higher than the current Compliance Guardian version will be moved to the new location. The original update files in the old location will be deleted.
  - **Delete the installed update(s)** – All of the downloaded files of the installed updates will be deleted from the old path.

- **Automatic Update** – Configuring Automatic Update can save time and effort for Compliance Guardian administrators. Choose from the following options:

  ***Note**: Automatic Update settings can only be configured if you have purchased maintenance for Compliance Guardian.

  - Download the update for me, but let me choose when to install it – Compliance Guardian will download the available updates for you, and save them to the default installation path or the customized net share path. All of the updates will be ready for installation at your own discretion.
  - Please notify me of the new updates, but do nothing to the updates – Compliance Guardian will notify the configured users of available updates but will not download the updates automatically.

    ***Note**: The maintenance license must already have been applied in order to select this option.

    - Select an e-mail notification profile you previously configured from the drop-down list or select **New E-mail Notification** to set up a new e-mail notification. For more information about how to configure the notification, refer to User Notification Settings.

    - **Turn off automatic updates** – The automatic updates function will be turned off and you will not be notified about the Compliance Guardian updates.

- **Proxy** – Configure the settings of the proxy server you want to use to download Compliance Guardian updates. Enter the proxy port to use when updating Compliance Guardian Control Service in the **Update Port** text box. The default port is 14007. Select the proxy protocol you want to use from the **Proxy Type** drop-down menu:
    - **No Proxy** (default) – No proxy server will be used.
    - **HTTP Proxy** – Select this to use the HTTP proxy, then configure the following settings:
        - **Proxy host** – Host name or IP address of the proxy server.
        - **Proxy port** – Port used to access the proxy server.
        - **Username** – Username to log on the proxy server.
        - **Password** – Password to access the proxy server.
    - **SOCKS5 Proxy** – Select this to use the SOCKS5 proxy, then configure the following settings:
        - **Proxy host** – Host name or IP address of the proxy server.
        - **Proxy port** – Port used to access the proxy server.
        - **Username** – Username to log on the proxy server.
        - **Password** – Password to access the proxy server.

Checking for Updates

To check for the latest updates, select **Check for Updates**. You can only check for updates after having purchased maintenance for Compliance Guardian. If there are any new updates available, the following information will be displayed in the area to the right:

- **Update Name** – Name of the update.
- **Product Name** – Compliance Guardian.
- **Type** – Type of the update.
- **Size** – Size of the update. The unit of the size is megabyte.
- **Status** – Installation status of the update.
- **Version** – Version of the update.

Managing Updates

To manage available updates, select **Manage Updates** on the ribbon. All available updates found by using the **Check for Updates** function will be listed in this page. You can perform the following actions on these updates:

- **View History** – Select **View History** on the ribbon to view a list of previously installed Compliance Guardian updates. You can customize how the list is displayed in the following ways:
  - **Search** – Filter the updates displayed by the keyword you designate; the keyword must be contained in a column value. At the top of the viewing pane, enter the keyword for the update you want to display. You can select to **Search all pages** or **Search current page**.
  - **Manage columns** ( ) – Manage which columns are displayed in the list so that only the information you want to see is shown. Select manage columns button ( ), then check the checkbox next to the column name to have that column shown in the list.
  - **Hide the column** ( ) – Hover over a column name, and then select the hide the column button ( ) in the column name to hide the column.
  - **Filter the column** ( ) – Filter which item in the list is displayed. Unlike Search, you can filter whichever item you want, rather than search based on a keyword. Hover over a column name, and then select the filter the column button ( ) of the column you want to filter, then check the checkbox next to the item name to have that item shown in the list. To remove all of the filters, select **Clear Filter**.

  To see more information about an update, select the update by checking the corresponding checkbox, and then select **View Details** on the ribbon. In the pop-up window, you can perform the following actions:

  - **Uninstall** – Select **Uninstall** to uninstall the selected update. The following options can be configured in the pop-up window:

    ***Note**: Only hotfixes and feature packs can be uninstalled. Service packs and cumulative updates contain major important changes between different versions, so they cannot be uninstalled.

    - In the **Manager** tab, all of the installed Manager services will be displayed. Select **Uninstall the update from all the managers below** when uninstalling updates from the Compliance Guardian Manager services since all of the available manager services must be updated at the same time.
    - In the **Agent** tab, select a farm to remove the update from all Compliance Guardian Agents in that farm.

- **Browse** – Select **Browse** on the ribbon to look for the updates on your local server. Select the desired update, and then select **Open** to load the update file into Compliance Guardian. The hotfix will be stored in the UNC path you specified in **Update Settings**. If there is no UNC path configured, the hotfix will be stored under the default path: **…\AvePoint\Compliance Guardian\Manager\Work\patchFolder.**
- **Download** – Select **Download** to download the selected updates from Compliance Guardian update server.
- **Stop** – Select **Stop** to interrupt the selected downloading update.

  ***Note:** The download progress will be reset to 0%.

- **Install** – Select **Install** to install the selected updates. The following options can be configured in the pop-up window:
  - In the **Manager** tab, all of the installed Manager services will be displayed. Select **Install the update for all the managers below** when installing updates for the Compliance Guardian Manager services since all of the available manager services must be updated at the same time.
  - In the **Agent** tab, select a farm to update all Compliance Guardian Agents in that farm.
- **Delete** – Select **Delete** to delete the selected updates from Compliance Guardian. The downloaded/browsed update files will be deleted at the same time.

Reviewing the Installation History of Updates

To review the installation history of your Compliance Guardian updates, select **View History** on the ribbon. You will see a list of all of the previously installed Compliance Guardian updates. You can customize how the list is displayed in the following ways:

- **Search** – Filter the updates displayed by the keyword you designate; the keyword must be contained in a column value. At the top of the viewing pane, enter the keyword for the update you want to display. You can select to **Search all pages** or **Search current page**.
- **Manage columns** ( ) – Manage which columns are displayed in the list so that only the information you want to see is shown. Select manage columns button ( ), then check the checkbox next to the column name to have that column shown in the list.
- **Hide the column** ( ) – Hover over a column name, and then select the hide the column button ( ) in the column name to hide the column.
- **Filter the column** ( ) – Filter which item in the list is displayed. Unlike Search, you can filter whichever item you want, rather than search based on a keyword. Hover over a column name, and then select the filter the column button ( ) of the column you want to filter, then check the checkbox next to the item name to have that item shown in the list. To remove all of the filters, select **Clear Filter**.

To see more information about an update, check the corresponding checkbox next to the update, and then select **View Details** on the ribbon. In the pop-up window, you can select **Uninstall** if you want to uninstall the selected update. The following options can be configured in the pop-up window:

***Note**: Only hotfixes and feature packs can be uninstalled. Service packs (SP) and cumulated updates (CU) contain major important changes between different versions and cannot be uninstalled.

- In the **Manager** tab, all of the installed Manager services will be displayed. Select **Uninstall the update from all the managers below** when uninstalling updates from the Compliance Guardian Manager services since all of the available manager services must be updated at the same time.
- In the **Agent** tab, select a farm to remove the update from all Compliance Guardian Agents in that farm.

When you are finished, select **Close** to close the pop-up window, and then select **Cancel** to return to the Update Manager interface.

Agent Groups

Agent Groups allow you to assign specific agents for performing certain jobs. This way, you can maintain balanced work load for different agents, and not have certain agents perform slower due to poor load distribution.

To access Agent Groups for Compliance Guardian, open the Control Panel interface, and then select **Agent Groups** under the Agent Groups heading. Select **Close** on the ribbon to close the Agent Group interface. If you have several Agents enabled for an agent type, they will be displayed in different colors in the **Available Agents** table.

Managing Agent Groups

In the Agent Groups interface, you will see a list of previously configured Agent Groups. You can customize how these Agent Groups are displayed in the following ways:

- **Search** – Filter the Agent Groups displayed by the keyword you designate; the keyword must be contained in a column value. At the top of the viewing pane, enter the keyword for the Agent Group you want to display. You can select to **Search all pages** or **Search current page**.
- **Manage columns** (+) – Manage which columns are displayed in the list so that only the information you want to see is shown. Select manage columns button (+), then check the checkbox next to the column name to have that column shown in the list.
- **Hide the column** (⊖) – Hover over a column name, and then select the hide the column button (⊖) in the column name to hide the column.
- **Filter the column** ( ) – Filter which item in the list is displayed. Unlike Search, you can filter whichever item you want, rather than search based on a keyword. Hover over a

column name, and then select the filter the column button ( ) of the column you want to filter, then check the checkbox next to the item name to have that item shown in the list. To remove all of the filters, select **Clear Filter**.

The following settings can be configured in the Agent Groups interface:

- **Create** – Select **Create** on the ribbon to create a new Agent Group. In the Create interface, you can configure the following settings:
  - **Agent Group Name** – Enter a name for the new Agent Group, and then enter an optional description for future reference.
  - **Agent Group Type** – Select one of the three Agent Group Types: **SharePoint**, **File System,** and **Website**.

    If **SharePoint** is selected, you must select a farm where you want to create this new Agent Group.

  - **Available Agents** – Available agents will be displayed in the lower panel. In the Available Agents panel, the number of the available agents will be displayed on the top left corner above each product name, and the available products for each agent will be colored in blue. Select the desired agent by checking the corresponding checkbox, then select **Add** to add the agent to the Agent Group. To remove an agent from the Agent Group, select the desired agent in the **Agents in Group** column by checking the corresponding checkbox, then select **Remove**.

  When you are finished, select **OK** to save these configurations and return to the Agent Groups interface, or select **Cancel** to return to the Agent Groups interface without saving this new Agent Group.

- **View Details**– Select an Agent Group by checking the corresponding checkbox, then select **View Details** on the ribbon to view detailed information about the Agent Group. In the View Details interface, select **Edit** on the ribbon to make changes to the configurations of this Agent Group. Follow the instructions in the next bullet point to edit Agent Groups.

- **Edit** – Select an Agent Group by checking the corresponding checkbox, then select **Edit** on the ribbon to make changes to the configurations. In the Edit Agent Group interface, enter a new name for the Agent Group, and then enter a description for future reference. Select the farm where you want to create this Agent Group from the **Farm** drop-down menu. Available agents will be displayed in the lower panel. In the **Available Agents** column, the number of the available agents will be displayed on the top left corner above each product name, and the available products for each agent will be colored blue. Select the desired agent by checking the corresponding checkbox, and then select **Add** to add the agent to the Agent Group. To remove an agent from the Agent Group, select the desired agent in the **Agents in Group** column by checking the corresponding checkbox, then select **Remove**.

When you are finished, select **Save** to save all changes made to the configurations of this Agent Group, select **Save As** to save the new configurations as a new Agent Group, or select **Cancel** to return to the Agent Groups interface without saving any changes.

- **Delete** – Select an Agent Group by checking the corresponding checkbox, then select **Delete** to delete the selected Agent Group. A confirmation window will pop up to ask if you are sure you want to delete the selected Agent Groups. Select **OK** to delete the selected Agent Groups, or select **Cancel** to return to the Agent Groups interface without deleting the selected Agent Groups.

User Notification Settings

Certain Compliance Guardian products provide e-mail reports or notifications to provide you with information when a certain triggering event occurs. Currently, Compliance Guardian notifications are provided as a pop-up window within Compliance Guardian or as e-mails to designated recipients. We are working on providing you with additional notification options which will be configurable in the Integration Settings interface. Once the notification integration feature is activated, the **Integration Settings** button on the ribbon will become available.

To access User Notification Settings for Compliance Guardian, navigate to the Control Panel interface, and then select **User Notification Settings** under the User Notification Settings heading. Select **Close** on the ribbon to close the User Notification Settings interface.

Configuring Send E-Mail Settings

The outgoing e-mail server must be configured before Compliance Guardian can send out e-mail notifications. To configure the Outgoing e-mail server, complete the following steps:

1. Check the **Enable Sending E-Mail Servers Settings** checkbox in order to activate e-mail server settings.
2. **Send e-mail server (SMTP)** – Enter the address of the outgoing e-mail server.
3. **Secure password authentication** – Check this checkbox if you have this option enabled in your E-mail account configuration.
4. **Port** – Enter the SMTP port. The default SMTP port is 25. For SSL authentication, the default port is 587.
5. **Sender** – Enter the e-mail address for all Compliance Guardian e-mails to be sent from.
6. **Username on SMTP** – Enter the sender's username on the SMTP server.
7. **Password on SMTP** – Enter the sender's password to log onto the SMTP server.
8. **SSL authentication** – Configure this option according to your e-mail settings.
9. Select the **Validation Test** button to verify the information entered. If the information you entered is verified successfully, a test e-mail will be sent to the sender you configured.

10. Select **Save** to save your configurations and select **Close** to exit the interface.

Configuring Receive E-Mail Settings

In the Receive E-Mail Settings interface, you will see a list of previously configured e-mail notification profiles. You can customize how these notification profiles are displayed in the following ways:

- **Search** – Filter the notification displayed by the keyword you designate; the keyword must be contained in a column value. At the top of the viewing pane, enter the keyword for the notification you want to display. You can select to **Search all pages** or **Search current page**.
- **Manage columns** (⊞) – Manage which columns are displayed in the list so that only the information you want to see is shown. Select manage columns button (⊞), then check the checkbox next to the column name to have that column shown in the list.
- **Hide the column** (⊖) – Hover over a column name, and then select the hide the column button (⊖) in the column name to hide the column.
- **Filter the column** ( ) – Filter which item in the list is displayed. Unlike Search, you can filter whichever item you want, rather than search based on a keyword. Hover over a column name, and then select the filter the column button ( ) of the column you want to filter, then check the checkbox next to the item name to have that item shown in the list. To remove all of the filters, select **Clear Filter**.

Configuring Receive E-Mail Notification

The receive e-mail notification profile allows you to specify e-mail address to receive reports from Compliance Guardian plans and services. To configure a receive e-mail notification profile, complete the following steps:

1. **Type** – Select a type for the profile you are about to create:
   - **Alert** – An alert is sent to let you know that the file cannot be scanned, or operation has been made according to the action policy.
   - **Notification** – A notification is sent to let you know the job report information after the job finished.
2. **Name and Description** – Enter a **Name** for this Receive E-mail Notification profile and an optional **Description** for future reference.
3. **Notification Address** – Configure the recipients for this notification. Select **Add a Notification Address** and then follow the steps below to add a recipient:
   a. (**Only for Notification**) Choose the detail level for the notification from the drop-down menu in the **Report** column. Select either **Summary Report Recipient** or **Detailed Report Recipient**.
   b. Enter the notification recipient's e-mail address in the **Recipient** column.

c. Repeat the steps above to add more recipients.

4. **Report Setting** (**Only for Notification**) – Select the type of information to include for the report levels, the recipients of **the** corresponding report types must exist before you can configure the report levels. If **Notification** was selected, you can configure the following settings:

   - **Summary report level(s)** – Set when to send the summary report. By default, Success, Failure, and Warning are all selected. After the job completed, failed, or completed with exception, a summary report will be sent to the recipient.
   - **Detailed report level(s)** – Set when to send the detailed report. By default, **Success**, **Failure**, and **Warning** are all selected. After the job completed, failed, or completed with exception, a detailed report will be sent to the recipient.
   - **Send all logs to recipient according to status** – Select what kind of logs will be sent to recipient. You can select **Success**, **Failure**, or **Warning**. By default, Failure is selected.
   - **Message format** – Select the format which the message will be delivered in: **HTML** or **Plain text**.

Select **OK** on the ribbon to save the settings or select **Cancel** to return to the Receive E-mail Settings interface without saving the profile.

Managing Receive E-Mail Notification

To see the configurations of a notification profile, select a notification profile, and then select **View Details** on the ribbon. You will see the configuration details of this notification profile.

To change the configurations for a notification profile, select the notification profile from the list of previously configured notification profiles, and select **Edit** on the ribbon. For details on editing configurations for a notification, refer to Configuring Receive E-Mail Notification.

To set a notification profile as the default one, select the notification profile from the list of previously configured notification profiles, and select **Set as Default Profile** on the ribbon. The default notification profile will be selected by default when you build up plans or configure notification settings for the Compliance Guardian Manager services or Agent services.

To delete a notification profile which is no longer needed, select the notification profile from the list of previously configured notification profiles, and select **Delete** on the ribbon. Select **OK** to confirm the deletion or select **Cancel** to cancel the operation.

Configuring E-mail Templates

E-mail Template displays the e-mail templates that previously configured, and allows you to configure an e-mail template to be used when sending alert emails. To create a new e-mail template, select **Create** on the ribbon, and then complete the following steps:

- **Notification Name** – Enter a **Name** for this Notification profile and an optional **Description** for future reference.

- **E-mail Template** – Specify the **Subject** and **Body** of the e-mail template. There are three columns that can be added to the e-mail subject: Item Name, Item URL and Scanned Time. There are seven columns that can be added to the e-mail body: Job Name, Plan Name, Job Type, Item Name, Item URL, Scanned Time, and Reason. The values of these columns will be displayed in the e-mail is the columns are added in the e-mail template. Alternatively, you can customize the subject and body of the e-mail template with the desired content.

Job Pruning

Job pruning allows you to set up pruning rules for all job records across your farms. When a job record is pruned, it will be deleted from the Job Monitor and the Compliance Guardian Control database.

***Note:** It is highly recommended that you configure a Job Pruning policy if you are running scan jobs frequently to ensure your databases are not overloaded with job data.

In Job Pruning, you can configure Job Pruning Rules for Compliance Guardian modules to retain the desired number of jobs, or jobs within a desired time frame. Once you have configured the Job Pruning Rule for a module, you may configure a schedule in the **Settings** tab to have Compliance Guardian prune jobs according to the Job Pruning Rules at a specified time with a specified notification, or manually run pruning jobs by selecting a module by checking the corresponding checkbox, and select **Prune Now** on the ribbon to prune jobs for the selected module based on the Job Pruning Rules you have configured for each module.

Job Pruning has Job Monitor integrated within the interface. To see the progress of your pruning jobs, select **Job Monitor** on the ribbon. For more information about Job Monitor, refer to Job Monitor.

To access Job Pruning for Compliance Guardian in the Control Panel interface, select **Job Pruning** under the Job Pruning heading. Select **Save** on the ribbon to save any changes made in Job Pruning. Select **Close** on the ribbon to close the Job Pruning interface.

Configuring Pruning Rules

In the **Rules** tab, select a Compliance Guardian module by checking the corresponding checkbox, then select **Configure** on the ribbon, or select the corresponding Job Pruning Rule for a module. The Configure interface will open in a pop-up window. The following options can be configured:

- **No Pruning** – Select this option to not prune the job records of this module.
- When configuring pruning rules, you will be presented with the following options:
    - **Keep the last__ job(s)** – Select this option to keep only the desired number of most recent jobs for this module. Set the number of jobs to keep by entering a positive integer into the text box. For example, if you enter **5** in the text box, only the 5 most recent jobs for this module will be kept. All other job records for this module will be deleted.

- **Keep the last __ Day(s)/Week(s)/Month(s) of job(s)** – Select this option to keep only the jobs within the desired time frame for this module. Set the time frame for the jobs you want to keep by entering a positive integer into the text box, then select **Day(s)**, **Week(s)**, or **Month(s)** from the drop-down menu. For example, if you enter **7** in the text box, and select **Day(s)**, only jobs performed within the last 7 days by this module will be kept. All of the previous job records of this module will be deleted.

When you are finished, select **OK** to save your configurations and return to the Job Pruning interface, or select **Cancel** to return to the Job Pruning interface without saving any changes.

Configuring Settings

Once you have configured Job Pruning Rules for Compliance Guardian modules, you can set up a schedule for Compliance Guardian to run pruning jobs, and notify the designated users with reports about the pruning jobs. In the **Settings** tab of the Job Pruning interface, configure the following settings:

1. **Schedule Selection** – Set up a schedule for Compliance Guardian to run pruning jobs, or select to manually run pruning jobs.
    - **No Schedule** – Select this option if you want to manually run pruning jobs.
    - **Configure the schedule myself** – Select this option to have Compliance Guardian run pruning jobs at a designated time. If this is selected, the **Schedule Settings** configuration will appear. Here you will see a list of all of your previously configured schedules. To add a new schedule, select **Add Schedule**. To edit a previously configured schedule, select the text in the **Summary** column. To delete a schedule, select . To preview the added schedules in a calendar, select **Calendar View**. For more details on adding or editing a schedule, refer to Configuring a Schedule.
2. N**otification** – Select an e-mail notification profile you have previously configured, or select **New Notification** to set up a new e-mail notification profile. For more information about how to configure the notification profile, refer to User Notification Settings.

Configuring a Schedule

To add or edit a schedule, complete the following steps:

1. **Type** – Select the time unit of the time interval for this schedule.
    - **By hour** – Configure the schedule by hour.
    - **By day** – Configure the schedule by day.
    - **By week** – Configure the schedule by week.
    - **By month** – Configure the schedule by month.
2. **Schedule Settings** – Configure the frequency for this schedule by entering a positive integer in the text box. If you want to set up a more specific schedule, check the **Advanced** checkbox, more options will appear depending on the **Type** you have selected in step 1:

- If you selected **By hour**, select one of the following options and configure its settings:
    - **Specify production time**: **From __ to __** – Specify the production time, it will run the job pruning in the specified production time frame.

      ***Note:** All pruning jobs that started within this time frame will finish even if the end time is reached.

    - **Select time below** – Specify the time you want to run the job pruning. To add several time points, select **Add**.
- If you select **By week**, configure the following settings:
    - **Run every __ week(s)** – Enter the frequency in terms of weeks in the text box.
    - **On __** – Specify the days of the week to run the job pruning on.
- If you select **By month**, select one of the following options and configure its settings:
    - **On day __ of __** – Select the day of the specific months to run the pruning jobs. For example, if you select **On day 3 of January** and **July**, the pruning jobs will run on the third of January and July.
    - **Day __ of every __ month(s)** – Select the day of the month and frequency to run the pruning jobs on. For example, if you select **Day 3 of every 3 month(s)**, the pruning jobs will run every three months, on the third of the month.
    - **The __ __of every __ month(s)** – Specify on which occurrence of which days of the month, and the frequency to run the pruning jobs. For example, if you select **The First Monday of every 3 month(s)**, the pruning jobs will run every three months, on the first Monday of the month.
    - **The __ __of __** – Specify on which occurrence of which days of which month to run the pruning jobs. For example, if you select **The First Monday of January** and **July**, the pruning jobs will run on the first Monday of January and July.

3. **Range of Recurrence** – Specify the **Start time** for pruning jobs. Select one of the following options for the end time and configure its settings:
    - **No end date** – The pruning jobs will run on the configured schedule until you manually end it.
    - **End after __ occurrence(s)** – The pruning jobs will stop running after the number of times you specify here.
    - **End by __** – The pruning jobs will end on the date and time you specify here.
4. When you are finished configuring the new schedule you want to add, select **OK** to save, or select **Cancel** to close the Add Schedule interface without saving.

Log Manager

Log Manager allows you to manage the logs of all of the Compliance Guardian services. Logs provide the Compliance Guardian support staff with important information for quicker troubleshooting.

Log Manager has Job Monitor integrated within the interface. To see the progress of your log collection jobs, select **Job Monitor** on the ribbon. For more information about Job Monitor, refer to Job Monitor.

***Note**: A Report Location must be configured in Job Monitor before you can use the Log Manager when Compliance Guardian Control Service High Availability is used.

To access Log Manager for Compliance Guardian, go to the Control Panel interface, and then select **Log Manager** under the Log Manager heading. Select **Close** on the ribbon to close the Log Manager interface.

Configuring Log Settings

To configure the log settings, go to the Log Manager interface, and then select **Log Settings** on the ribbon. You can configure the log settings for the following services by selecting either the **Control Service** or **Agent** tab.

In each of the tabs, you will see the name of the service. For each service, the following options can be configured:

- **Log Level** – Logs could be configured to generate on each of the following levels.
  - **Information** (default) – Logs of this level record the basic information of Compliance Guardian, such as the jobs that you have run, the operations you have performed, and important processes of jobs. Information level logs also contain all of the logs from warning and error levels.
  - **Debug** – Logs of this level record the detailed information related to the internal operations such as the communication between Compliance Guardian Manager and Compliance Guardian Agent, the operations in the database, the output message of the data.

    Logs of this level are used for finding out all of the details of the jobs, and it is recommended that the level is set to **Debug** before troubleshooting. Debug level logs also contain all of the logs from information, warning, and error levels.
  - **Error** – Logs of this level record the error messages for jobs. Not all of the errors could lead to the failure of the jobs, some of the errors have already been dealt with and the logs will record the detailed information.
  - **Warning** – Logs of this level record exceptions for jobs. Warning level logs also contain all of the logs from error level.
- **Size of Each Log** –The default size for a log is 5 MB. You can adjust the size according to your requirements by entering a different number into the text box.

- **Total Log Count** – The maximum number of all the log files in the Logs folder under the installation folder of each Manager Service. For each Agent Server, the Total Log Count is the maximum number of all of the log files which can be generated by each .exe file. The Agent logs are stored in the Logs folder under the installation folder of each Agent. When the number of log files exceeds the threshold, the oldest log files will be deleted.

When you are finished configuring Log Settings, select **OK** to save all changes and return to the Log Manager interface, or select **Cancel** to return to the Log Manager interface without saving any changes.

Collecting Logs

In order to collect logs, you must first specify the Manager services or Agents that you want to collect the logs from in the Log Collection section of the Log Manager interface. Select **Collect** on the ribbon to begin collecting logs for the selected services or agents.

To receive e-mail notification containing the report, select a previously configured e-mail notification profile in the drop-down list or select **New Notification** to set up a new e-mail notification profile. For more information about how to configure the e-mail notification profile, refer to User Notification Settings.

Solution Manager

Solution Manager provides an interface for you to manage all of the Compliance Guardian solutions. To access Solution Manager for Compliance Guardian, go to the Control Panel interface, and then select **Solution Manager** under the Solution Manager heading. Select **Close** on the ribbon to close the Solution Manager interface.

***Note:** Be sure that you have Full Control of all zones of all Web applications via the User Policy for Web Applications in your SharePoint permissions.

Managing Solutions

When you first access Solution Manager, you will see two Compliance Guardian solutions. In order to see some of the information for these solutions, or to perform certain actions to these solutions, you must first select a farm.

Farm Selection

Select a farm from the **Farm** drop-down menu, the following information of the farm will be displayed in a table:

- **Number of Front-end Web Servers** – Number of the servers which have enabled the Microsoft SharePoint Foundation Web Application service.
- **Number of Available Agents** – Number of the Compliance Guardian Agents with an up ( ) and Active status.

- **Deployment Method** – Currently the solution can only be locally deployed. In other words, solution files are deployed only to the Compliance Guardian Agent Server from which the deployment operation was initiated.

Viewing the Solution's Information

You can view the following information of the solutions in the corresponding table:

- **Solution** – Name of the Compliance Guardian solution.
- **Module** – Name of the module this solution is intended for.

The following information is only available if you have a farm selected:

- **Version** – Version of the solution.
- **Status** – Deployment status of the solution file.
  - **N/A** – The solution is not installed.
  - **Not Deployed** – The solution is installed but not deployed.
  - **Deployed** – The solution is deployed to all of the Agent servers.
  - **Partially Deployed** – The solution is deployed to some of the Agent servers.
- **Last Refreshed Time** – Last modified time of the corresponding solution.
- **Message** – Detailed information about the solution deployment.

Operations on the Solutions

Select a solution from the table by checking the corresponding checkbox. You can perform the following actions:

- **Install** – Select **Install** on the ribbon to add a solution package to the farm's solution store, which is in the farm's configuration database. Use this button when you only want to add the solution to the specified farm and do not want to deploy it.
- **Deploy** – Select **Deploy** on the ribbon to unpack the solution package, and copy its elements to their appropriate places. This button can be used even when the solution has not been installed to the specified farm. In that case, the solution will be installed to the specified farm first and then be deployed.
- **Retract** – Reverse the deployment of the farm solution's components. The solution remains in the solution store and can be redeployed later.
- **Remove** – Deletes the solution package from the solution store. This button can be used even when the solution has not been retracted from the specified farm. In that case, the solution will be retracted from the specified farm first and then removed.

After a solution is installed, to view information about it, select the solution by checking the corresponding checkbox, and then select **Solution Properties** on the ribbon. You will be brought to the Solution Properties page. By default, the **Summary** tab is open, which shows an overall view of the

specified solution. Select the **Details** tab to view the solution's deployment status on each of the Web applications and other detailed information. In the Details tab, you can also select Web applications by checking the corresponding checkboxes, and then select to **Deploy** or **Retract** the solution from the selected Web applications. When you are finished, select **Cancel** on the ribbon to return to the Solution Manager interface.

Managing Solutions

To keep your Compliance Guardian solutions up to date, Solution Manager provides you tools to check for solution version, upgrade existing solutions, and repair deployed solutions. To perform any of these actions, select the solution by checking the corresponding checkbox, then select:

- **Retrieve Version** on the ribbon to retrieve version information about the selected solutions. The information displayed in the Version, Status, and Message columns will be refreshed.
- **Upgrade** on the ribbon to upgrade the selected solution to the latest version. A solution can be upgraded if the solution version is lower than the current agent version.
- **Repair** on the ribbon to repair the selected solution. You can repair a solution if it does not have the same version as the current agent version.

Solution Description

Refer to the descriptions below to get an overall view of all of the Compliance Guardian solutions.

CCS.QuarantineManager.wsp – This solution is used for the Real-Time Classification Scanner and Scheduled Classification Scanner. If you deploy this solution, you are able to use the Compliance Guardian Quarantine Manager in SharePoint.

CCS.AssistManager.wsp – This solution is only used for the Real-Time Classification Scanner module. After enabling this feature, you can manually scan the document in the specified scope defined in Compliance Guardian, and view the scanned results, or you can directly modify the tag values for the scanned document without modifying the checks.

CCS.InstallEventReceiver.wsp – This solution is only used for the Real-Time Classification Scanner module. If you deploy this solution, the **Compliance Guardian Newly Created Sites Real-Time Scan** feature will be enabled on the Web application automatically. The newly created site's corresponding **Compliance Guardian Real-Time Scan** feature will also be enabled, and then the newly created site will apply its parent's Real-Time Classification rule (if the parent has applied a rule).

Database Manager

Database Manager allows you to create and configure the databases for a Compliance Scan job and Classification Scan job to use.

A database policy is configured for a Compliance Scan job, you can select a previously configured database, and set up a retention policy for saving data in this database. In the Database Manager interface, you will see the Report Database and Report Database Policy tabs.

Report Database

Report Database allows you to store the scanned results of Compliance Scanner and Classification Scanner. To access Report Database settings for Compliance Guardian in the Control Panel interface, select **Database Manager** under the Common Settings heading. Select **Close** on the ribbon to close the Report Database interface.

Managing Report Database

In Report Database, you can create a report database, view details about a report database, edit a previously configured report database, or delete a previously configured report location. For details on creating or editing a report database, refer to Configuring Report Database.

To view details about a report database, select it from the list of previously configured report databases, select **View Details** on the ribbon, then select **Report Database** in the drop-down menu. You will see the previously configured settings for this report database.

Select **Edit** on the ribbon to change the configurations for this report database. For details on editing configurations for a report database, refer to Configuring Report Database.

To delete a report database from Compliance Guardian, select it from the list of previously configured report databases, and select **Delete** on the ribbon, and then select **Report Database** from the drop-down list. A confirmation window will appear and ask if you are sure you want to proceed with the deletion. Select **OK** to delete the selected report databases, or select **Cancel** to return without deleting it.

Configuring Report Database

To create a new report database, select **Create** on the ribbon, and then select **Report Database** in the drop-down menu. To modify a previously configured report database, select the report database, and select **Edit** on the ribbon, and then select **Report Database** in the drop-down list menu. In the Create Report Database or Edit Report Database interface, configure the following settings:

- **Configure Report Database** – Specify a report database. Enter a new **Database Server** and a **Database Name** in the corresponding fields.
- **Authentication** – Select the authentication mode for the report database.

If **Windows Authentication** is selected, the application pool account and the Compliance Guardian Agent Account must have the **db_owner** permission for the report database. If the report database does not exist and need to be created, the application pool account and the Compliance Guardian Agent Account must have the **dbcreator** permission for the report database. You can also validate the database account by selecting **Validation Test**. The **Validation Test** only runs if the application pool account has enough permissions to the report database.

If **SQL Authentication** is selected, the necessary information must be specified in the **Account** and **Password** fields. You can also validate the database account by selecting **Validation Test**.

- **Failover Database Server** – Specify a failover database server. In the event that the specified report database collapses, the data stored in the report database can be transferred to this standby database.

Alternatively, you can configure the authentication in **Advanced** settings by entering a connection string instead of configuring the settings. Select **Advanced**; the **Connection String** section appears. Check the **Edit Connection String directly** checkbox to activate this feature, and then enter the connection string according to the example listed in the left pane.

Select **OK** to finish and save the configuration, or select **Cancel** to return to the Report Database page without saving any configurations.

Report Database Policy

Report Database Policy allows you to apply report retention rule to the specified report database. A retention rule defines how to prune the reports stored in the report database.

To access Report Database Policy settings in the Control Panel interface, select **Database Manager** under the Common Settings heading. The Report Database tab is the default one. Select the **Report Database Policy** tab to launch the Report Database Policy page. Select **Close** on the ribbon to close the Report Database Policy interface.

Managing Report Database Policy

In Report Database Policy, you can create a report database policy, view details about a report database policy, edit a previously configured report database policy, or delete a previously configured report database policy. For details on creating or editing a report database policy, refer to Configuring Report Database Policy.

To view details about a report database policy, select it from the list of previously configured report database policies, select **View Details** on the ribbon, then select **Report Database Policy** in the drop-down menu. You will see the previously configured settings for this report database policy.

Select **Edit** on the ribbon to change the configurations for this report database policy. For details on editing configurations for a report database policy, refer to Configuring Report Database Policy.

To delete a report database policy from Compliance Guardian, select it from the list of previously configured report database policies, and select **Delete** on the ribbon, and then select Report Database Policy in the drop-down list. A confirmation window will pop up and ask if you are sure you want to proceed with the deletion. Select **OK** to delete the selected report database policies, or select **Cancel** to return without deleting it.

Configuring Report Database Policy

To create a new report database policy, select **Create** on the ribbon, and then select **Report Database Policy** in the drop-down menu. To modify a previously configured report database policy, select the report database policy, and select **Edit** on the ribbon, and then select Report Database Policy in the drop-down list. In the Create Report Database Policy or Edit Report Database Policy interface, configure the following settings:

- **Configure Report Database Policy Name** – Specify a name for the report database policy. Enter a **Report Database Policy Name** and a **Description** in the corresponding fields. The description is optional.
- **Report Database** – Select an existing report database or create a new one.
- **Report Retention Rule** – Check the **Enable report retention** checkbox to activate this feature, and then enter an integer in the right pane to define how to prune the reports in the specified report database.

Select **OK** to finish and save the configuration, or select **Cancel** to return to the Report Database Policy page without saving any configurations.

Test Suite Manager

Test Suite Manager allows you to manage test suites and create checks and test suites. To access the Test Suite Manager in the Control Panel interface, select **Test Suite Manager** under the Common Settings heading. Select **Close** on the ribbon to close the **Test Suite Manager** interface.

Background Information

In order to provide a flexible and customizable compliance solution, AvePoint developed the AvePoint Testing Language (ATL) to provide organizations with the ability to rapidly respond to new compliance threats and requirements. ATL is an XML structured language that is used to validate and classify content related to compliance to standards or guidelines, including but not limited to security, privacy, accessibility, and content classification. Because it is open and modifiable, ATL allows for coverage to specifically match an organization's needs. ATL uses test definition files (checks) to match your environment and standards, test your framework and repair issues, validate that your content complies

with organizational standards, and identify all content that requires user review and distribute a list of items to the appropriate parties.

A check is an XML file that defines the logic that Compliance Guardian uses to check files. Checks identify the purpose for the check (the type of check to run, such as a pattern of characters), the condition for the check (such as social security number pattern), and the possible result of the check (true or false). Users can change the values in the checks to determine the check conditions, but the elements' specific format defined by Compliance Guardian in the checks must stay the same.

A test suite is a logical grouping of test definition files, or a set of checks, that define how to present the scanned data. test suites allow you to build scan plans for your specific regulations and requirements. These collections are the basis of Compliance Guardian scans. A test suite contains one or more checks and a configuration file that is used to define how to combine these checks and set risk levels for scan results. The two types of configuration files are:

- Content Compliance Collection (CCC) (.ccc) – CCC files flag specific instances where content fails or violates an associated check in a check. Each violation is then assigned a relative risk score defined by the CCC file.
- Metadata Compliance Collection (MCC) (.mcc) – MCC files define what tags should be created as a result of a check against checks, where the tags should be applied, and if the Compliance Guardian applied tags should override user applied tags.

Managing Test Suites

In the **Test Suite Manager** interface, you will see a list of the configured test suites (including the built-in test suites). You can customize how these test suites are displayed in the following ways:

- **Sort** – Select the header row of each column to sort all of the values in the specified column according to the ascending/descending order.
- **Search** – Filter the test suites and display them by the keyword you designate; the keyword must be contained in a column value. At the top right corner of the test suite viewing pane, enter the keyword for the test suites you want to display. You can select **to Search all pages** or **Search current page**.
- **Manage columns** (⊞) – Manage which columns are displayed in the list so that only the information you want to see is shown. Select manage columns button (⊞), then check the checkbox next to the column name to have that column shown in the list.
- **Hide the column** (⊖) – Hover over a column name, and then select the hide the column button (⊖) in the column name to hide the column.
- To change the number of test suites displayed per page, select the desired number from **5**, **8**, **10**, **15** (default value), **20**, **25**, **50**, **100** in the **Show rows** drop-down menu at the lower right corner.
- To go to the specified page, enter the page number in the **Go to …** of text box at the lower right corner and press **Ente**r.

- To go to the next page, select the **>** button at the lower right corner; to return to the previous page, select the **<** button at the lower right corner.

***Note:** You can view the version of a test suite. When a test suite is uploaded to Compliance Guardian or created through Compliance Guardian, Compliance Guardian will automatically assign a version for this test suite. If a test suite is updated via Test Suite Manager, Compliance Guardian will also automatically update its version when it is saved.

In the **Test Suite Manager** interface, you can create, upload, download, view details about, edit, or delete checks and test suites. Review the following sections for details on each of these available actions.

Create a New Check or Test Suite

Review the following two procedures for details on creating either a new check or test suite.

Creating Checks

To create a new check, select **Create** on the ribbon of the **Test Suite Manager** interface. When the drop-down menu appears, select **Check** from the drop-down menu. To create a new check, complete the following steps:

1. In the **Check Template** screen, select the desired check template in the check template list by selecting the radio button before the check template.
2. Select **Next** on the ribbon or on the lower right corner of the screen. The Report Text screen appears.
3. Configure the following settings in the **Report Text** screen:
    - **Name and Description** – Enter a name for the check. The description is optional.
    - **URL** – Enter a hyperlink to provide additional information about this check, including any official rules or articles of law that specify how the check will test files. This field is optional.
    - **True Result and Message** – Select the returning status and message for this check when the checking result is True. The checking logic determines whether a check result is false or true.
    - **False Result and Message** – Select the returning status and message for this check when the checking result is False. The checking logic determines whether a check result is false or true.
4. Select **Next** on the ribbon or on the lower right corner of the screen. The check attributes configuration screen appears.
5. Configure the attributes for the check. The attributes that are required to be configured for each type of check are different. For details on configuring attributes for each type of check, refer to Configuring Check Type Attributes in Appendix B.
6. Select **Save** on the ribbon or on the lower right corner of the screen to save the check.

If you want to preview the check before saving it, select **Preview** on the ribbon or on the lower right corner of the screen. A pop-up window appears. Enter the file name in the pop-up window, and select **Save**. The check will be saved. You can view the configuration information on the check, and then save the check in Compliance Guardian after you have previewed the check and confirmed the check information.

Creating Test Suites

To create a new test suite, select **Create** on the ribbon of the Test Suite Manager interface. When the drop-down menu appears, select **Test Suite** from the drop-down menu. To create a new test suite, complete the following steps:

1. In the **Test Suite Type** screen, select the test suite type:
   - **Test Suite for Compliance Reporting** – Found in Compliance Manager, this type of test suite is used to identify and report any instances of non-compliance to defined rules and then identify the associated risks.
   - **Test Suite for Classification and Tagging** – Found in Classification Manager, this type of test suite is used for content classification with a variety of related actions such as embedding metadata, quarantining documents, and reacting content.
2. After selecting the test suite type, select **Next** on the ribbon or on the lower right corner of the screen. The **Test Suite for Compliance Reporting** or **Test Suite for Classification and Tagging** screen appears.
3. Configure the following settings:
   - **Name and Description** – Enter a name for the test suite. The description is optional.
   - **DepthScan** – If the file types that will be scanned are the supported types in Compliance Guardian, this function is not required to be used no matter if the **True** option or the **False** option is selected. If the files that will be scanned are the unsupported types in Compliance Guardian, and the **True** option is selected, the exception message will be thrown and displayed in Compliance Guardian Report. If the **False** option is selected, the **IFilter** will be used for the scan.

     For more information on the supported file types in Compliance Guardian, refer to Appendix C: Supported File Types in Compliance Guardian.

   If **Test Suite for Compliance Reporting** type is selected, you need to configure the **Check Accessibility** setting. Select whether or not to check the file accessibility. If **Yes** is selected, the file will be scanned keeping its formatting. If **No** is selected, the file will be scanned, stripping out its formatting. If the file that will be scanned is the unsupported type in Compliance Guardian, the function will not be used no matter the **Yes** option or the **No** option is selected.
4. Select **Next** on the ribbon or on the lower right corner of the screen. The File Body Configuration screen appears.

5. Configure the attributes for the content compliance collection (CCC) or metadata compliance collection (MCC) file. For details on configuring the file attributes, refer to Configuring CCC or MCC File Attributes in Appendix B.
6. Select **Save** on the ribbon or on the lower-right corner of the screen to save the test suite.

   If you want to preview the **Test Suite for Compliance Reporting** or **Test Suite for Classification and Tagging** file before saving it, select **Preview** on the ribbon or on the lower right corner of the screen, a pop-up window appears. Enter the file name in the pop-up window, and select **Save** to save the file. You can view configuration information on the file, and then save the test suite in Compliance Guardian after you have previewed the file and confirmed the file information.

Upload Checks and Test Suites

Select **Upload** on the ribbon. A window will pop up, and then you can select the desired test suite or check. The uploaded test suite will display in the test suite list in the Test Suite Manager interface; the uploaded check will be loaded when you create a test suite. You can upload multiple test suites or checks at one time. Before uploading the test suites or checks, you must zip the test suites to one file, or zip the checks to one file first, and then select the ZIP file to upload them to Compliance Guardian.

Download a Test Suite

Select a test suite from the list of previously configured test suites, and then select **Download** on the ribbon.

View Details about a Test Suite

Select a test suite from the list of previously configured test suites, and then select **View Details** on the ribbon.

Edit a Previously Configured Check or Test Suite

In the **Test Suite Manager** interface, select the collection that you want to edit, and then select **Edit** on the ribbon. A drop-down menu appears. Choose one of the following options:

- **Check and Test Suite** – Edit the test suite by enabling or disabling checks and removing checks. You can also edit the checks in the test suite. Refer to Editing Checks and Test Suites for details.
- **CCC or MCC File** – Edit the selected test suites' content compliance collection (CCC) or metadata compliance collection (MCC) file. Refer to Editing CCC or MCC Files for details.

Editing Checks and Test Suites

If selecting **Check and Test Suite** from the **Edit** drop-down menu, you will be brought to the Edit Check and Test Suite interface where you can configure the following settings:

- **Name and Description** – Edit the test suite's name and description.
- **Check Selection** – All the checks that are included in the selected test suite will be loaded here. Refer to the description field for an overview of each check. Perform the following actions as needed:
    - In the **Status** column, you can select the down arrow ( ), and then select **Enable** or **Disable** to enable or disable a check. If you disable a check, the check will not be used in the test suite.

      ***Note:** The **Status** column only appears if you are editing a Test Suite for Compliance Reporting. It will not appear if you are editing a Test Suite for Classification and Tagging.
    - To delete one or more checks from the test suite, select the checkboxes before the checks, and select **Delete** on the ribbon.
    - To edit a single check, select the checkbox to the left of the check, and then select **Edit** on the ribbon of this interface. Refer to Editing a Check.

  You can also perform the following additional actions when selecting the checks in the **Check Selection** section:

    - **Sort** – Select the header row of each column to sort all of the values in the specified column according to the ascending/descending order.
    - To change the number of checks displayed per page, select the desired number from **5**, **8**, **10**, **15** (default value), **20**, **25**, **50**, **100** in the **Show rows** drop-down menu at the lower right corner.
    - To go to the specified page, enter the page number in the **Go to …** of text box at the lower right corner and press **Enter**.
    - To go to the next page, select the **>** button at the lower right corner; to return to the previous page, select the **<** button at the lower right corner.

Editing a Check

After selecting a check and selecting **Edit** on the ribbon, you will be brought to the check **Edit** interface. Complete the following steps as needed:

1. Edit the following settings in the **Report Text** screen:
    - **Name and Description** – Enter a name for the check. The description is optional.
    - **URL** – Enter a hyperlink to provide additional information about this check, including any official rules or articles of law that specify how the check will test files. This field is optional.

- **True Result and Message** – Select the returning status and message for this check when the checking result is True. The checking logic determines whether a check result is false or true.
- **False Result and Message** – Select the returning status and message for this check when the checking result is False. The checking logic determines whether a check result is false or true.

2. Select **Next** on the ribbon or on the lower right corner of the screen. The check attributes configuration screen appears.
3. Configure the attributes for the check. The attributes that are required to be configured for each type of check are different. For details on configuring attributes for each type of check, refer to Configuring Check Type Attributes in Appendix B.
4. Select **Save** on the ribbon or on the lower right corner of the screen to save the check. Alternatively, select **Save As** and enter a check name to save it as another check.

   If you want to preview the check before saving it, select **Preview** on the ribbon or on the lower right corner of the screen. A pop-up window appears. Enter the file name in the pop-up window, and select **Save**. The check will be saved. You can view the configuration information on the check, and then save the check in Compliance Guardian after you have previewed the check and confirmed the check information.

Editing CCC or MCC Files

If selecting **CCC or MCC File**, you will be brought to the Test Suite Manager Edit interface where you can edit the following settings:

1. Edit the **Name and Description** in the **Test Suite for Compliance Reporting** or **Test Suite for Classification and Tagging** screen. The description is optional.

   If you're editing a test suite for Compliance Reporting, you need to configure the **Check Accessibility** setting. Select whether or not to check the file accessibility.

2. Select **Next** on the ribbon or on the lower right corner of the screen. The File Body Configuration screen appears.
3. Configure the attributes for the content compliance collection (CCC) or metadata compliance collection (MCC) file. For details on configuring the file attributes, refer to Configuring CCC or MCC File Attributes in Appendix B.
4. Select **Save** on the ribbon or on the lower right corner of the screen to save the test suite. Alternatively, select **Save As** and enter a test suite name to save it as another test suite.

   If you want to preview the **Test Suite for Compliance Reporting** or **Test Suite for Classification and Tagging** file before saving it, select **Preview** on the ribbon or on the lower right corner of the screen. A pop-up window appears. Enter the file name in the pop-up window, and select **Save** to save the file. You can view configuration information on the file, and then save the test suite in Compliance Guardian after you have previewed the file and confirmed the file information.

Delete a Check or Test Suite

Select a check or test suite from the list of previously configured checks or test suites, and then select **Delete** on the ribbon. A confirmation window will pop up and ask if you are sure you want to proceed with the deletion. Select **OK** to delete, or select **Cancel** to return without deleting it.

Risk Formula

Risk Formula provides the user with a method to measure level of risk in proportion to the risk type. It allows users to grow risk at a specified factor, providing an accurate look at risk by occurrence.

Managing Risk Formulas

Select Risk Formula on the ribbon of the Test Suite Manager interface, you will be brought to the Risk Formula interface. In the Risk Formula interface, you will see a list of the created Formula. There are three default Formulas: Weighted, Stepped, and Raw.

You can customize how these formulas are displayed in the following ways:

- **Sort** – Select the header row of each column to sort all of the values in the specified column according to the ascending/descending order.
- **Search** – Filter the Formulas and display them by the keyword you designate; the keyword must be contained in a column value. At the top right corner of the Formula viewing pane, enter the keyword for the Formulas you want to display. You can select **to Search all pages** or **Search current page**.
- **Manage columns** (+) – You can manage which columns are displayed in the list so that only the information you want to see will be shown. Select the plus button (+), then check the checkbox next to the column name to have that column shown in the list.
- **Hide the column** (⊖) – Hover over a column name, and then select the hide the column button (⊖) in the column name to hide the column.
- To change the number of formulas displayed per page, select the desired number from **5**, **8**, **10**, **15** (default value), **20**, **25**, **50**, **100** in the **Show rows** drop-down menu at the lower-right corner.
- To go to the specified page, enter the page number in the **Go to …** of text box at the lower right corner and press **Ente**r.
- To go to the next page, select the **>** button at the lower right corner; to return to the previous page, select the **<** button at the lower right corner.

In the Risk Formula interface, you can create, view details about, edit, or delete the created Formulas.

- To view details about a Formula, select the Formula, and select **View Details** on the ribbon.
- To edit a previously created Formula, select the Formula, and select **Edit** on the ribbon.

- To delete a previously created Formula, select the Formula, and select **Delete** on the ribbon.
- To create a new Formula, select **Create** on the ribbon, you will be brought to the Create Risk Formula interface, configure the following settings:
    - **Name and Description** – Enter a name for the new formula. The description is optional.
    - **Formula** – Define a new formula.

Detailed Information on the Formula

There are three default risk formulas: Weighted, Stepped, and Raw.

- The formula for Weighted is: r1+r2*r3*(n-1).
- The formula for Stepped is: r1+r2*(n-1).
- The formula for Raw is: r1*n.

User can also create a new risk formula. Refer to the following section for the introduction about r1, r2 and r3:

- **r1** – Item Initial Risk value, this is the value assigned on the initial occurrence of the compliance failure (related to the check being tested for) in the document or stream.

  Allowed Values for r1 are 1-10.

- **r2** – Item Additional Risk Level factor (Step) that the risk level grows at for every additional failure at the check level (for the same type) found in the document or stream. This number is optional where the integer "-1" means ignore the value (allowing to use the third value). If the value is -1 then the factor will be 1.

  Allowed Values are -1 to 10.

- **r3** – Item risk in relation to other checks. This Item is optional. If this number is missing then it is assumed that its value is "1".

  Allowed Values are 1-10.

  In addition, the r3 value allows us to define importance of an item in a check against other checks allowing us to look at a document with 100 images with missing alternative text quite differently than a document that has 100 social security numbers. In addition, if we considered alt text errors and SSN numbers as errors that should grow risk at the same value for every new occurrence we could then define importance at a higher level for a specified test suite. These two additional risk factors allow us to more accurately show risk against checks or test suites and based on importance of repetitive failure in a document.

Report Configuration

Report Configuration allows you to configure the report settings. To access Report Configuration settings for Compliance Guardian in the Control Panel interface, select **Report Configuration** under the Common Settings heading. Select **Close** on the ribbon to close the Report Configuration interface.

Managing Report Settings

In Report Configuration, you can specify a default report location, specify the maximum number of files to display in the report interface, connect to DocAve Auditor Database, configure the authentication and advanced settings. For details on configuring the report settings, see the Configuring Report Settings section of this guide.

Configuring Report Settings

In the Report Configuration interface, configure the following settings:

1. **Default Report Location**– Specify a **Report Location as the default location** for storing reports, and then configure the pruning rule. The following options can be configured:
    - **No Pruning** – Select this option to choose not to prune the reports in the report location.
    - Depending on the report location you are configuring pruning rule for, you will be presented with different options:
        - **Keep the last__ report(s)** – Select this option to keep only the desired number of most recent reports in this report location. Set the number of reports to keep by entering a positive integer into the text box. For example, if you enter **5** in the text box, only the 5 most recent reports in this report location will be kept. All other reports will be deleted.
        - **Keep the last __ Minute(s)/Hour(s)/Day(s)/Week(s)/Month(s) of report(s)** – Select this option to keep only the reports within the desired time frame in this report location. Set the time frame for the reports you want to keep by entering a positive integer into the text box, then select **Minute(s), Hour(s), Day(s)**, **Week(s)** or **Month(s)** from the drop-down menu. For example, if you enter **7** in the text box, and select **Day(s)**, only reports generated within the last 7 days in this report location will be kept. All of the previous reports will be deleted.
2. **Maximum Number of Files** – Set the maximum number of files to display in the report interface by entering a positive integer into the text box. For example, if you enter **500** in the text box, only 500 reports will be stored in the report location.
3. **Connect to DocAve Auditor Database** – Specify a **Database Server** where the DocAve Auditor database resides and a **Database Name** in the corresponding fields to connect to the specified DocAve Auditor database. The DocAve Auditor information will be used with the risk analysis from Compliance Guardian to generate the Risk Report export.

***Note:** Since any changes to the database server or database name may lead to loss, it is strongly recommended not to change them once configured.

4. **Authentication** – Select the authentication mode for the report database. The necessary information must be specified in the **Account** and **Password** fields. You can also validate the database account by selecting **Validation Test**.

   Alternatively, you can configure the report settings in the **Advanced** settings by entering a connection string instead of configuring the settings. Select **Advanced**, and the **Connection String** section will appear. Check the **Edit Connection String directly** checkbox to activate this feature, and then enter the connection string according to the example listed in the left pane.

5. Select **OK** to save the configurations and return to the Control Panel interface, or select **Back** to return to the Control Panel interface without saving any changes.

Allowed Location

Allowed Location allows you to configure a destination location where the scanned file is moved. To access Allowed Location settings for Compliance Guardian in the Control Panel interface, select **Allowed Location** under the Common Settings heading. Select **Close** on the ribbon to close the Allowed Location interface.

Configuring Allowed Location

In Allowed Location, you can create a new allowed location, edit a previously configured allowed location, or view the information of the previously configured allowed locations.

To create a new allowed location, select a scope (you can configure an allowed location either in the site level or the list level). Select **Configure** and the **Configure** window will pop up and ask you to enter a full URL to specify the destination folder within the site. You can also validate the full URL by selecting **Test**.

***Note**: Only the full URL of a document library or a folder can be specified as the allowed location.

Inheritance Status

For site level, there are two types of inheritance status: **N/A** and **Not Inherit**. For list level, there are three types of inheritance status: **N/A**, **Not Inherit**, and **Inherit**.

1. When there is no allowed location configured for a site, the site inheritance status is **N/A**. The inheritance statuses of the lists that inherit the site are **N/A**; the inheritance statuses of the lists that do no inherit the site are **Not Inherit**.
2. When there is an allowed location that has been configured for the site, the site inheritance status is **Not Inherit**. The inheritance statuses of the lists that inherit the site are **Inherit**; the inheritance statuses of the lists that do not inherit the site are **Not Inherit**.

Inherit or Not Inherit

After configuring an allowed location in a site, the lists under this site automatically inherit the destination folder that is configured for the site. If you configure an allowed location in the lists that are under this site, these lists are regarded as stopping inheriting from the site. If files are moved after scanning according to the action policy, the files in these lists will be moved to the list destination folders; the files in this site except this list will be moved to the site destination folder.

If some lists have configured allowed locations, and the site does not configure one. The files in these lists that are moved according to the action policy will be moved to the list destination folders; the files in the site but not in these lists will not be moved even if they should be.

The files in sites or lists that do not configure allowed locations will not be moved.

Helpful Notes

Review the following helpful notes on configuring the Allowed location:

- By default, the Allowed Location configured for the site level is inherited by the list levels.
- You can configure a new destination folder in list level to break the inheritance from the site level.
- **Not Inherit** logically separates the destination folder in list level from the site level.
- When configuring destination folders for the first time, you can configure destination folders directly at either the site level or the list level. After one destination folder has been configured for a list level, you can still configure destination folders directly to the site levels.
- The inherited destination folder cannot be removed; it can only be edited.
- The target library where the allowed location is must contain a content type that matches with the source file's content type, and the matched content type must contain all the source's files columns.

Export Location

Export Location allows you to export SharePoint data to a specified location. To access Export Location settings for Compliance Guardian in the Control Panel interface, select **Export Location** under the Export Location heading. Select **Close** on the ribbon to close the Export Location interface.

Managing Export Locations

In Export Location, you can create a new export location, view details about an export location, edit a previously configured export location, or delete a previously configured export location. For details on creating or editing an export location, refer to Configuring Export Locations.

To view details about an export location, select it from the list of previously configured export locations, then select **View Details** on the ribbon. You will see the previously configured settings for this export location.

Select **Edit** on the ribbon to change the configurations for this export location. For details on editing configurations for an export location, refer to Configuring Export Locations.

To delete an export location from Compliance Guardian, select it from the list of previously configured export locations, and then select **Delete** on the ribbon. A confirmation window will appear and ask if you are sure you want to proceed with the deletion. Select **OK** to delete the selected export locations, or select **Cancel** to return without deleting it.

Configuring Export Locations

To create a new export location, select **Create** on the ribbon. To modify a previously configured export location, select the export location, and then select **Edit** on the ribbon. In the Create Export Location or Edit Export Location interface, configure the following settings:

1. **Name and Description** – Enter a **Name** for this export location, and then enter an optional **Description** for this export location for future reference.
2. **Path** – The export location can be a file share, storage area network (SAN), or network-attached storage (NAS).
    - Enter the **UNC Path** in the following format: **\\admin-PC\c$\data** or **\\admin-PC\shared** folder.

      *__Note:__ The path you specified must already exist.

    - Enter the **Username** and **Password** in the corresponding text boxes, and then select **Validation Test**. Compliance Guardian will test the path and user information to make sure they are valid.
3. Select **OK** to save the configurations and return to the Export Location interface, or select **Back** to return to the Export Location interface without saving any changes.

Filter Policy

Filter Policy allows you to set up filter rules so you can control what objects and data appear so that you can target content more precisely. By setting up and saving filter policies, you can apply the same filter policies to different plans without having to recreate them each time.

To access Filter Policy for Compliance Guardian in the Control Panel interface, select **Filter Policy** under the Filter Policy heading. Select **Close** on the ribbon to close the Filter Policy interface.

In the Filter Policy interface, you will see a list of previously configured filter policies. You can customize how these filter policies are displayed in the following ways:

- **Search** – Filter the filter policies displayed by the keyword you designate; the keyword must be contained in a column value. At the top of the viewing pane, enter the keyword for the filter policy you want to display. You can select to **Search all pages** or **Search current page**.
- **Manage columns** (⊞) – Manage which columns are displayed in the list so that only the information you want to see is shown. Select manage columns button (⊞), then check the checkbox next to the column name to have that column shown in the list.
- **Hide the column** (⊖) – Hover over a column name, and then select the hide the column button (⊖) in the column name to hide the column.
- **Filter the column** ( ) – Filter which item in the list is displayed. Unlike Search, you can filter whichever item you want, rather than search based on a keyword. Hover over a column name, and then select the filter the column button ( ) of the column you want to filter, then check the checkbox next to the item name to have that item shown in the list. To remove all of the filters, select **Clear Filter**.

Managing Filter Policies

In Filter Policy, you can create a new filter policy, view details about a filter policy, edit a previously configured filter policy, or delete a previously configured filter policy. For details on creating a filter policy, refer to Configuring Filter Policies. For details on editing configurations for filter policy, refer to Editing Filter Policies.

To view a filter policy for Compliance Guardian, select it from the list of previously configured filter policies, and then select **View Details** on the ribbon. To delete a filter policy for Compliance Guardian, select it from the list of previously configured filter policies, and then select **Delete** on the ribbon. A confirmation window will pop up and ask if you are sure you want to proceed with the deletion. Select **OK** to delete the selected filter policy, or select **Cancel** to return without deleting it.

***Note**: There are three default filter policies (Common File Types and Items is used for Compliance Guardian Scanner for SharePoint and Classification Scanner for SharePoint; File System Common File Types is used for Compliance Guardian Scanner for File System and Classification Scanner for File Systems; Common Website Content is used for Compliance Guardian Scanner for Website) configured in advance. The default filter policies will be selected if no other filter policies are configured.

Configuring Filter Policies

To create a new filter policy, select **Create** on the ribbon. In the Create Filter Policy interface, configure the following settings:

1. **Name** – Enter a **Name** for the filter policy.
2. **Description** – Enter an optional **Description** for future reference.

3. **Type** – Select a filter policy type. There are three kinds of filter policy types: SharePoint, File System, and Website:

   - **SharePoint** – This type of filter policy is used in Compliance Guardian Scanner for SharePoint and Classification Scanner for SharePoint. If this type is selected, then select specific objects or data within each SharePoint level (from site collection down to attachment). Each level has a unique set of rules that can be applied to enhance configurations.
   - **File System** – This type of filter policy is used in Compliance Guardian Scanner for File System and Classification Scanner for File System. If this type is selected, then select the level. Each level has a unique set of rules that can be applied to enhance configurations.
   - **Website** – This type of filter policy is used in Compliance Guardian Scanner of Website.

   After selecting the filter policy type, configure the following settings:

   a. Select a criterion, and then select **Add a Filter Level Group** to add a new rule of the specified level. Select the delete button ( ) to delete the rule that is no longer needed.

      - **Rule** – Select the new rule you want to create from the drop-down list.
      - **Condition** – Select the condition for the rule.
      - **Value** – Enter a value you want the rule to use in the text box.

      ***Note:** The **File Content** criterion for the SharePoint type filter policy and File System type filter policy is only for the HTML file, you can specify which lines or columns are excluded in this scan by using the filter policy.

   b. To add more filters to the filter policy, repeat the previous step.

      ***Note:** Depending on the filters you enter, you can change the logical relationships between the filter rules. There are currently two logical relationships: **And** and **Or**. By default, the logic is set to **And**. To change the logical relationship, select the logical relationship link. The **And** logical relationship means that the content which meets all of the rules will be filtered and included in the result. The **Or** logic means that the content which meets any one of the rules will be filtered and included in the result.

      You can view the logical relationship of the filter rules in the **Basic Filter Condition** area.

   For example, if the logical relationship is ((1 And 2) Or 3) in the Basic Filter Condition area, the contents that meet both the filter rule 1 and filter rule 2, or meet the filter rule 3, will be filtered out.

Select **Save** to save the configurations and return to the **Filter Policy** interface, or select **Cancel** to return to the Filter Policy interface without saving any changes.

Editing Filter Policies

To modify a previously configured filter policy, select the filter policy, and then select **Edit** on the ribbon. In the **Edit Filter Policy** interface, edit the related settings according to your own requirement. For details on how to configure settings for filter policies, refer to Configuring Filter Policies.

After finishing editing settings of the selected filter policy, select **Save** to save the configurations and return to the **Filter Policy** interface. Alternatively, select **Save As** and enter a filter policy name to save it as a new filter policy. Select **Cancel** to return to the **Filter Policy** interface without saving any changes.

Website Scanner Settings

Configure the Authentication Profile and the User Agent Profile for using Compliance Guardian Scanner for Website.

Configuring Authentication Profile

An authentication profile is used to connect to the website. To configure authentication profiles in the Control Panel interface, select Authentication Profile under the Website Scanner Settings heading. Select **Close** on the ribbon to close the Authentication Profile interface.

Managing Authentication Profile

In the **Authentication Profile** interface, you will see a list of previously configured Authentication profiles. You can customize how these profiles are displayed in the following ways:

- **Sort** – Select the header row of each column to sort all of the values in the specified column according to the ascending/descending order.
- **Search** – Filter the profiles and display them by the keyword you designate; the keyword must be contained in a column value. At the top right corner of the profile viewing pane, enter the keyword for the profiles you want to display. You can select to **Search all** pages or **Search current page**.
- **Manage columns** (⊞) – Manage which columns are displayed in the list so that only the information you want to see will be shown. Select the manage columns button (⊞), and then check the checkbox next to the column name to have that column shown in the list.
- **Hide the column** (⊖) – Hover over a column name, and then select the hide the column button (⊖) in the column name to hide the column.
- To change the number of profiles displayed per page, select the desired number from **5**, **8**, **10**, **15** (default value), **20**, **25**, **50**, **100** in the **Show rows** drop-down menu at the lower right corner.
- To go to the specified page, enter the page number in the **Go to … of** text box at the lower right corner and press **Enter**.

- To go to the next page, select the **>** button at the lower right corner; to return to the previous page, select the **<** button at the lower right corner.

In the **Authentication Profile** interface, you can create a new authentication profile, view details about an authentication profile, edit a previously configured authentication profile, or delete a previously configured authentication profile. For details on creating or editing an authentication profile, refer to Creating and Editing Authentication Profile.

Select **Edit** on the ribbon to change the configurations for the selected authentication profile. For details on editing configurations for the authentication profile, refer to Creating and Editing Authentication Profile.

To view an Authentication profile, select it from the list of previously configured profiles, and then select **View Details** on the ribbon. To delete an authentication profile, select it from the list of previously configured profiles, and then select **Delete** on the ribbon. A confirmation window will pop up and ask if you are sure you want to proceed with the deletion. Select **OK** to delete the selected authentication profile, or select **Cancel** to return without deleting it.

Creating and Editing Authentication Profile

To create a new authentication profile, select **Create** in the **Manage** group of the Authentication Profile page. To modify a previously configured authentication profile, select the authentication profile, and then select **Edit** on the ribbon. In the Create Authentication Profile or Edit Authentication Profile interface, configure the following settings:

- **Name and Description** – Enter a name and an optional description for the profile.
- **Authentication Method** – Select an authentication method: **Username and Password Only** or **Certificate**.

  If **Username and Password Only** is selected, then enter the specified username and password for accessing the web site. Compliance Guardian supports Basic, Digest, NTLM, Negotiation Authentications.

  If **Certificate** is selected, then upload a Certificate, and then specify the username and password for accessing the website.

Configuring User Agent Profile

A user agent profile is used for the backend web server when scanning the website. To configure user agent profiles in the **Control Panel** interface, select **User Agent Profile** under the **Website Scanner Settings** heading. Select **Close** on the ribbon to close the **User Agent Profile** interface.

Managing User Agent Profile

In the **User Agent Profile** interface, you will see a list of previously configured User Agent profiles. You can customize how these profiles are displayed in the following ways:

- **Sort** – Select the header row of each column to sort all of the values in the specified column according to the ascending/descending order.
- **Search** – Filter the profiles and display them by the keyword you designate; the keyword must be contained in a column value. At the top right corner of the profile viewing pane, enter the keyword for the profiles you want to display. You can select to **Search all** pages or **Search current page**.
- **Manage columns** (⊞) – You can manage which columns are displayed in the list so that only the information you want to see will be shown. Select the show column button (⊞), then check the checkbox next to the column name to have that column shown in the list.
- **Hide the column** (⊖) – Hover over a column name, and then select the hide column button (⊖) in the column name to hide the column.
- To change the number of profiles displayed per page, select the desired number from **5**, **8**, **10**, **15** (default value), **20**, **25**, **50**, **100** in the **Show rows** drop-down menu at the lower right corner.
- To go to the specified page, enter the page number in the **Go to … of** text box at the lower right corner and press **Enter**.
- To go to the next page, select the **>** button at the lower right corner; to return to the previous page, select the **<** button at the lower right corner.

In the **User Agent Profile** interface, you can create a new user agent profile, view details about an user agent profile, edit a previously configured user agent profile, or delete a previously configured user agent profile. For details on creating or editing a user agent profile, refer to Creating and Editing User Agent Profile.

Select **Edit** on the ribbon to change the configurations for the selected user agent profile. For details on editing configurations for the user agent profile, refer to Creating and Editing User Agent Profile.

To view a user agent profile, select it from the list of previously configured profiles, and then select **View Details** on the ribbon. To delete a user agent profile, select it from the list of previously configured profiles, and then select **Delete** on the ribbon. A confirmation window will pop up and ask if you are sure you want to proceed with the deletion. Select **OK** to delete the selected user agent profile, or select **Cancel** to return without deleting it.

Creating and Editing User Agent Profile

To create a new user agent profile, select **Create** in the **Manage** group of the User Agent Profile page. To modify a previously configured user agent profile, select the user agent profile, and then select **Edit** on

the ribbon. In the Create User Agent Profile or Edit User Agent Profile interface, configure the following settings:

- **Name and Description** – Enter a name and an optional description for the profile.
- **User Agent String** – Specify the user agent string.

Compliance Manager

Compliance Manager enables you to retrieve compliance information about all of the files in the specified scope through performing Compliance Scanner jobs. It displays the scan results through different kinds of Compliance Reports so users can easily view the compliance status of the files in the specified scopes.

***Note:** In order to scan Microsoft Office files that are in a 2003 or earlier format, you must download a compatibility pack. Once you install the compatibility pack, Compliance Guardian will support scans of these files, but the software does not support tagging of Microsoft Office 2003 files even though they can be scanned and classified after installing the compatibility pack.

Pre-Configurations

Make sure the settings in the following sections have been configured prior to creating a Compliance Scanner plan.

Configuring Scan Policies

A scan policy defines the compliance rules to be used when scanning the contents in the specified scope. To configure the scan policies, select **Scan Policy** on the ribbon of the Compliance Scanner page to enter the Scan Policy interface.

Managing Scan Policies

In the Scan Policy interface, you will see a list of previously configured scan policies. You can customize how these scan policies are displayed in the following ways:

- **Sort** – Select the header row of each column to sort all of the values in the specified column according to the ascending/descending order.
- **Search** – Filter the scan policies and display them by the keyword you designate; the keyword must be contained in a column value. At the top right corner of the scan policy viewing pane, enter the keyword for the scan policies you want to display. You can select to **Search all** pages or **Search current page**.
- **Manage columns** (⊞) – Manage which columns are displayed in the list so that only the information you want to see will be shown. Select the manage columns button (⊞), and then check the checkbox next to the column name to have that column shown in the list.
- **Hide the column** (⊖) – Hover over a column name, and then select the hide column button (⊖) in the column name to hide the column.
- To change the number of scan policies displayed per page, select the desired number from **5**, **8**, **10**, **15** (default value), **20**, **25**, **50**, **100** in the **Show rows** drop-down menu at the lower right corner.

- To go to the specified page, enter the page number in the **Go to … of** text box at the lower right corner and press **Enter**.
- To go to the next page, select the **>** button at the lower right corner; to return to the previous page, select the **<** button at the lower right corner.

In the Scan Policy interface, you can create a new scan policy, view details about a scan policy, edit a previously configured scan policy, delete a previously configured scan policy, or export the check information for the test suites included in the selected scan policy. For details on creating or editing a scan policy, refer to Configuring Scan Policies.

Select **Edit** on the ribbon to change the configurations for the selected scan policy. For details on editing configurations for the scan policy, refer to Configuring Scan Policies.

Select **Export** on the ribbon to export the check information for the test suites in the selected scan policy.

To view a scan policy, select it from the list of previously configured scan policies, and then select **View Details** on the ribbon. To delete a scan policy, select it from the list of previously configured scan policies, and then select **Delete** on the ribbon. A confirmation window will pop up and ask if you are sure you want to proceed with the deletion. Select **OK** to delete the selected scan policy, or select **Cancel** to return without deleting it.

Creating or Editing Scan Policies

To create a new scan policy, select **Create** in the **Manage** group of the Scan Policy page. To modify a previously configured scan policy, select the scan policy, and then select **Edit** on the ribbon. In the Create Scan Policy or Edit Scan Policy interface, configure the following settings:

- **Name and Description** – Enter a name for this scan policy. You can also enter an optional description to distinguish this scan policy from the others.
- **Select the Test Suites** – Specify the test suites that you want to include in this scan policy. There are some predefined test suites in this page, you can refer to the description of each test suite for the introduction of its usage. To add more desired test suites, select **Test Suite Manager** in the **Settings** group on the ribbon. For more information on configuring test suites, refer to Test Suite Manager.

  After selecting some test suites, if you want to clear the selection status, select the **Clear Selection** link and then specify your desired test suites again.

You can also perform the following actions when selecting the test suites:

- **Sort** – Select the header row of each column to sort all of the values in the specified column according to the ascending/descending order.
- **Search** – Filter the test suites and display them by the keyword you designate; the keyword must be contained in a column value. At the top right corner of the test suite

viewing pane, enter the keyword for the test suites you want to display. You can select to **Search all** pages or **Search current page**.

- **Manage columns** (⊞) – You can manage which columns are displayed in the list so that only the information you want to see will be shown. Select the manage columns button (⊞), then check the checkbox next to the column name to have that column shown in the list.
- **Hide the column** (⊖) – Hover over a column name, and then select the hide column button (⊖) in the column name to hide the column.
- To change the number of test suites displayed per page, select the desired number from **5**, **8**, **10**, **15** (default value), **20**, **25**, **50**, **100** in the **Show rows** drop-down menu at the lower right corner.
- To go to the specified page, enter the page number in the **Go to … of** text box at the lower right corner and press **Enter**.
- To go to the next page, select the **>** button at the lower right corner; to return to the previous page, select the **<** button at the lower right corner.

After you are satisfied with the configuration of the scan policy, select **OK** to save this scan policy. If you do not want to save the current configuration, select **Cancel** to cancel the configuration.

Configuring Filter Policies

For more information, refer to Filter Policy.

Configuring Database Policies

For more information, refer to Database Manager.

Configuring the Account Manager

For more information, refer to Account Manager.

Configuring Connections for File System

A connection is used in the Compliance Guardian Scanner File System Mode. Configure a connection with the file system, then the files in the connected file system are supported to be scanned in Compliance Guardian.

Navigate to **Compliance Scanner** > **Create** > **File System**, and select **Configure Connection** on the ribbon to enter the **Configure Connection** interface.

Managing Connections

In the **Configure Connection** interface, you will see a list of previously configured connections. You can customize how these connections are displayed in the following ways:

- **Sort** – Select the header row of each column to sort all of the values in the specified column according to ascending/descending order.
- **Search** – Filter the connections and display them by the keyword you designate; the keyword must be contained in a column value. At the top right corner of the connection viewing pane, enter the keyword for the connections you want to display. You can select to **Search all pages** or **Search current page**.
- **Manage columns** (⊞) – Manage which columns are displayed in the list so that only the information you want to see will be shown. Select the manage columns button (⊞), and then check the checkbox next to the column name to have that column shown in the list.
- **Hide the column** (⊖) – Hover over a column name, and then select the hide column button (⊖) in the column name to hide the column.
- To change the number of connections displayed per page, select the desired number from **5**, **8**, **10**, **15** (default value), **20**, **25**, **50**, **100** in the **Show rows** drop-down menu at the lower right corner.
- To go to the specified page, enter the page number in the **Go to … of** text box at the lower right corner and press **Enter**.
- To go to the next page, select the **>** button at the lower right corner; to return to the previous page, select the **<** button at the lower right corner.

In the **Configure Connection** interface, you can create a new connection, view details about a connection, edit a previously configured connection, or delete a previously configured connection. For details on creating or editing a connection, review Creating and Editing Connections.

Select **Edit** on the ribbon to change the configurations for the selected connection. For details on editing configurations for the connection, review Creating and Editing Connections.

To view a connection, select it from the list of previously configured connections, and then select **View Details** on the ribbon. To delete a connection, select it from the list of previously configured connections, and then select **Delete** on the ribbon. A confirmation window will pop up and ask if you are sure you want to proceed with the deletion. Select **OK** to delete the selected connection, or select **Cancel** to return without deleting it.

Creating and Editing Connections

To create a new connection, select **Create** in the **Manage** group on the **Configure Connection** page. To modify a previously configured connection, select the connection, and then select **Edit** on the ribbon. In the Create Connection or Edit Connection interface, configure the following settings:

- **Name and Description** – Enter a name for this connection. You can also enter an optional description to distinguish this connection from the others.
- **Type** – Select the file system type for the connection.
- **Connection** – Configure the following settings:
  - **Agent Group** – Select the agent group that will perform the Compliance Scanner File System job.
  - **UNC Path** – Specify a path in the format *\\admin-PC\c$\data or \\admin-PC\shared folder*. The files in the specified location are supported to be scanned.
  - **Username** – Specify a username that can access the specified location.
  - **Password** – Specify a password.

    ***Note:** The specified user must have the following permissions:

    If the path is specified in the format *\\admin-PC\c$\data*:

    - The specified user must have the **local administrator** permission to the connected server.

    If the path is specified in the format *\\admin-PC\shared folder*:

    - The specified user must have the **Log on as a batch job** permission to the connected server, or the user must be the member of the **Backup Operators** group of the connected server.
    - The specified user must have the **Read** and **Change** permissions to the shared folder.

After you are satisfied with the configuration of the connection, select **OK** to save this connection. If you do not want to save the current configuration, select **Cancel** to cancel the configuration.

Compliance Scanner

Compliance Scanner enables you to perform a scan job using the defined scan policy and generate the compliance scan results of all of the scanned files. The users in the specified Report Group can then view the compliance scan results in the Compliance Report module.

Refer to the following sections for important information on getting started with Compliance Scanner.

Launching Compliance Scanner

To launch Compliance Scanner, complete the following steps:

1. Log in to Compliance Guardian. If you are already in the software, select the home page button ( ) go to the home page. From the home page, all of the products are displayed.
2. Select **Compliance Scanner** to launch its interface.
3. Alternatively, you can select **Administration** on the top-left corner, and select the **Compliance Scanner** tab on the appeared navigation bar to launch Compliance Scanner.

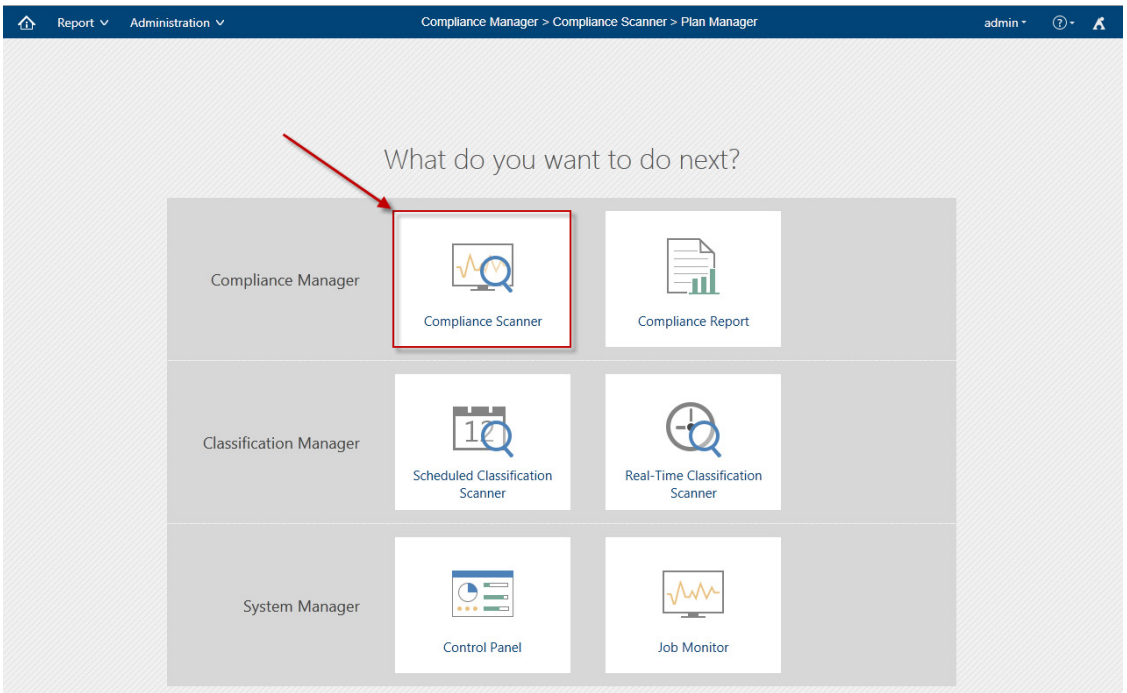

Figure 9: Compliance Guardian module launch window.

Home Page Overview

The Compliance Scanner home page displays a list of all of your previously created Compliance Guardian Scanner plans. You can also select **Create** to select the Compliance Guardian Mode: SharePoint, File System, or Website, and then create a plan.

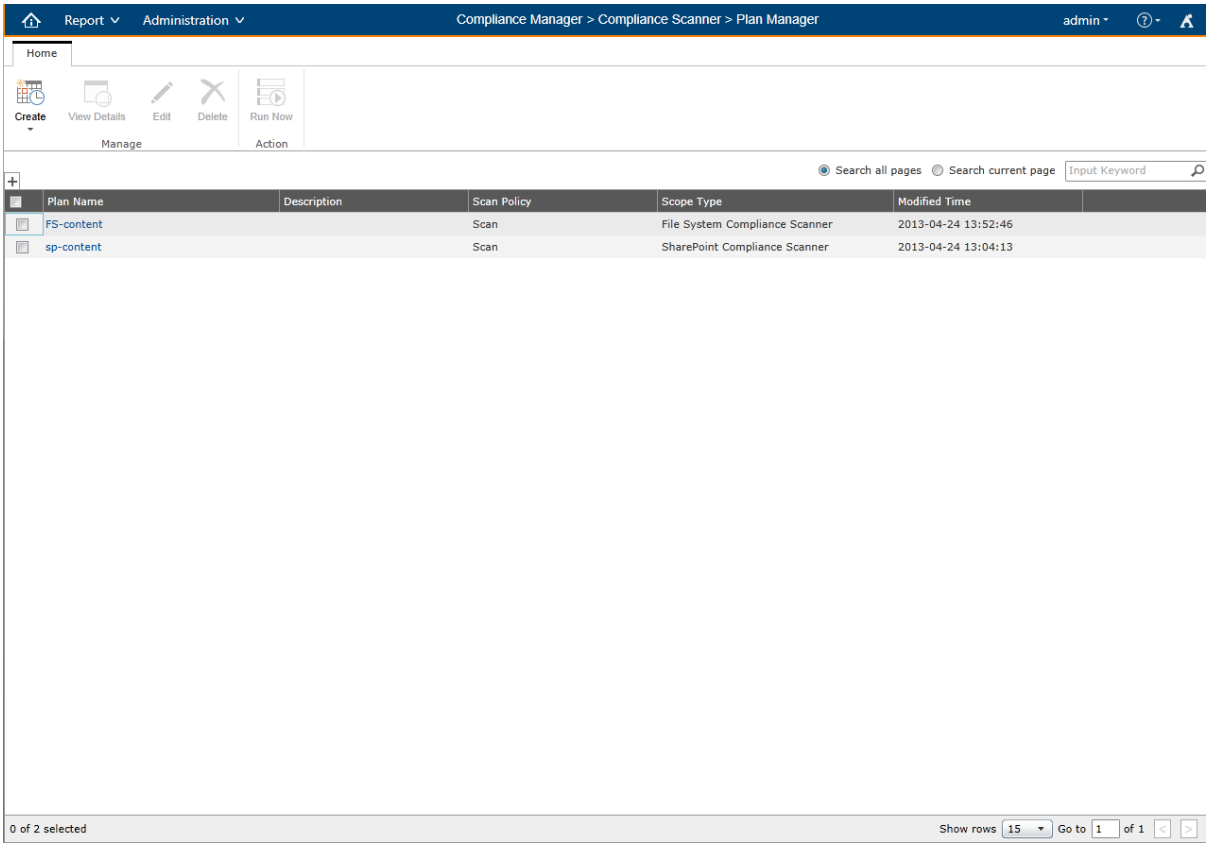

Figure 10: Compliance Scanner home page.

Selecting Mode

Select **Create** on the ribbon. A drop-down list appears. Select the corresponding mode from the drop-down list: **SharePoint**, **File System**, or **Website**. Then you can enter the corresponding mode, and configure a plan to scan objects in SharePoint, a file system, or a website.

Managing Compliance Guardian Scanner Plans

The Compliance Scanner home page displays a list of all of your previously created Compliance Guardian Scanner plans. Also it displays the scan policy that is selected in the plan. You can also see the plan type in the **Scope Type** column.

You can customize how these plans are displayed in a number of different ways:

- **Search** – Filters the plans displayed by the keyword you designate. The keyword must be contained in a column value. At the top of the viewing pane, type in the keyword for the plan you want to display. You can select to **Search all pages** or **Search current page**.

  ***Note:** The search function is not case sensitive.

- **Manage columns** (⊕) – Manages which columns are displayed in the list so that only the information you want to see is displayed. Select the manage columns button (⊕), and then select the checkbox next to the column name to have that column shown in the list.

- **Hide the column** (⊖) – Hover over a column name, and then select the hide column button (⊖) of any column you want to hide.

- **Filter the column** ( ) – Filters which item in the list is displayed. You can filter whichever item you want, rather than search based on a keyword. Hover over a column name, and then select the filter button ( ) of the column you want to filter, then select the checkbox next to the item name to have that item shown in the list.

You may perform any of the following actions on a selected plan:

- **View Details** – Select **View Details** on the ribbon to see the details of the selected plan. Here you can also select **Edit** on the ribbon to make changes to the plan's settings. You will be brought to the **Edit** page where you can change the settings for this plan. After editing the settings, select **Save** on the ribbon to save the plan. To save a changed plan as a new one, select **Save As** on the ribbon. At any time, select **Cancel** on the ribbon to return to the **Plan Manager** without saving any of your changes.

- **Edit** – Select **Edit** on the ribbon to make changes to the selected plan's settings. You will be brought to the **Edit** page where you can change the settings for this plan. Select **Save** on the ribbon to save the plan. To save a changed plan as a new one, select **Save As** on the ribbon. At any time, select **Cancel** on the ribbon to return to the **Plan Manager** without saving any of your changes.

  ***Note:** If you change the scan policy when editing a Compliance Scanner plan, or change the database policy when editing a Compliance Scanner plan, after you save the changes, the next time the plan will mandatorily run a full job although you select to run an incremental job, thus to guarantee that the job can perform correctly, as well as guarantee the job data is generated correctly.

- **Delete** – Select **Delete** on the ribbon to delete the selected plan. A warning message will appear to confirm the deletion. Select **OK** to delete the selected plan, or select **Cancel** to return to **Plan Manager** without deleting the selected plan.

- **Run Now** – Select **Run Now** on the ribbon to execute the plan immediately. After you select **Run Now**, a pop-up window appears, you can select to run a full job or an incremental job. If **Incremental Scan** is selected, the **Reference Time** option is enabled.

- **Reference Time** – Choose whether to scan contents created or modified at a specified interval. If you choose to use a reference time, specify the time to scan contents created or modified. Enter an integer into the textbox and select **Month(s)**, **Day(s)**, **Hour(s)**, or **Minute(s)** from the drop-down list.

  ***Note**: It is recommended that you specify a reference time when the recurrence schedule configured in **Range of Recurrence** is **End after 1 occurrence**.

You can see the review details about the plan's execution in Job Monitor.

Compliance Guardian Scanner for SharePoint

The SharePoint Mode allows you to define a SharePoint scope and then perform a scan job using the defined scan policy to generate the compliance scan results of all of the files within that SharePoint scope. The users in the specified Report Group can then view the compliance scan results in the Compliance Report module.

Launching Compliance Guardian Scanner SharePoint Mode

On the Compliance Guardian Scanner Home interface, select **Create** on the ribbon, a drop-down list appears. Select **SharePoint** from the drop-down list, and you will be brought to the Compliance Guardian Scanner SharePoint Mode.

Selecting the Scan Scope

After launching the Compliance Scanner SharePoint mode, the **Scope** panel on the left of the screen displays the root node of the farm. To select the scan scope, complete the following steps:

1. Select the farm node to expand the tree. The tree can be loaded down to the list level.
2. Select the scope where you want to perform the scan job on the tree.

Using Plan Builder to Perform a Compliance Guardian Scanner Plan for SharePoint

Use the **Plan Builder** to set up a Compliance Scanner plan. To use Plan Builder, complete the following steps:

1. After selecting the scope for the compliance scan, select **Plan Builder** on the ribbon of Compliance Scanner page.
2. From the drop-down menu, select **Wizard Mode** for step-by-step guidance during configuration, or select **Form Mode** (recommended for advanced users only) to set up a plan quickly.

Refer to the following section that is applicable to your choice for details on performing a Compliance Scanner plan.

Performing a Compliance Scanner Plan in Wizard Mode

Wizard Mode provides you with step-by-step guidance on how to configure a new plan. To configure a plan using Wizard Mode, complete the following steps:

***Note:** An asterisk (*) in the user interface indicates a mandatory field or step.

1. Enter a **Plan Name** and an optional **Description** if desired. Select **Next**. The **Report Settings** page appears.
2. Configure the report settings:
   - **Database Policy** – Select a database policy from the drop-down list to store the result data of the Compliance Scanner job. If you want to set up a new database policy, select the **New Database Policy** link in the drop-down list. Refer to Configuring Report Database Policy for more information.
   - **Report Group** – Select a Compliance Guardian group from the drop-down list. Once a group is specified as the **Report Group**, all of the users in the specified group will be able to view and download the reports in the Compliance Report module. Multiple groups can be specified here; choose **Select All** to select all of the listed groups.

   Select **Next**. The **Scan Settings** page appears.
3. Configure the scan settings:
   - **Scan Policy** – Select a scan policy from the drop-down list and it will be used to scan the contents in the specified scope. Only one scan policy can be selected here.
   - **Content Option** – Specify the contents that will be scanned within the specified scope.
     - **Include user content** – This checkbox is selected by default, and only the documents and items that are created by the end users will be scanned in the specified scope.
     - **Include system content** – Select this checkbox to also scan the system built-in contents in the specified scope.
   - **Scan File/Item Versions** – Specify the method of scanning file/item versions:
     - **Scan the current version** – Only the current versions of the files/items defined in the job scope are supported to be scanned.
     - **Scan all versions** – The files/items and all their previous versions defined in the job scope are supported to be scanned. If this option is selected, the scan result of each file/item version will be reported in the Compliance Guardian report separately.
   - **Filter Policy** – Specify a filter policy to filter the contents that will be scanned. By default, the default filter policy is used, and all of the types of documents/items supported by Compliance Guardian are included in this default filter policy. If you want to set up a new filter policy, select the **New Filter Policy** link in the drop-down list. Refer to Configuring Filter Policies for more information.

- **Alert** – Specify whether to send out an alert e-mail when an unsupported type of embedded file is found. An embedded file is one file that is inserted to another file. If the type of the embedded file is supported by Compliance Scanner, it can be scanned as usual. However, if the type of the embedded file is not supported by Compliance Scanner, it cannot be scanned.

  If you choose to send out alert e-mails when unsupported embedded files are found, configure the recipients by selecting the corresponding checkboxes in the **Send e-mail to** field:

  - **Creator** – Select this checkbox to send an alert e-mail to the creator of the specified file where unsupported embedded files are found.
  - **Modifier** – Select this checkbox to send an alert e-mail to the last modifier of the specified file where unsupported embedded files are found.
  - **User who is specified in the following notification file** – Select this checkbox to send an alert e-mail to the recipients configured in the selected alert notification profile. If this option is selected, you must select an alert notification profile from the appeared drop-down list. You can also select the **New Notification Profile** link to create a new notification profile. For more information, refer to User Notification Settings.

  ***Note**: Even though there may be more than one embedded file in one file, the alert e-mail will only be sent when the first unsupported embedded file is found. The rest of the content in the file where the embedded file resides will be skipped and will not be scanned.

After configuring the recipients, choose one e-mail template from the **E-mail template** drop-down list; you can also select the **New E-mail template** link to create a new e-mail template. For more information, refer to Configuring E-mail Templates.

Select **Next**. The **Schedule** page appears.

4. Configure the schedule settings:

   - **No schedule** – Select this option to run the plan immediately and save the plan in Plan Manager.
   - **Configure the schedule myself** – Select this option to configure a customized schedule, and run the Compliance Scanner job by schedule. Select **Add Schedule** to set up a schedule. The **Add Schedule** window appears. In the **Options** section, select a scan type from the drop-down list. For more information, refer to Scan Schedule.
     - **Full Scan –** Run a full scan of all of the documents and items in the specified scope. Unlike incremental scan, all full scans are independent of one another and do not have any dependencies on the other's scan results. However, because each of the full scans is comprehensive, full scan jobs take the longest to complete of the two available options.
     - **Incremental Scan –** Run a fractional scan. It scans only the updated documents and items since the last successful full scan or incremental scan. This kind of

scan requires less storage than a full scan and it reduces the execution time of the scan job. However, it is important to note that for each incremental scan, the latest full scan job in the full scan cycle must be available. If the incremental scan is based on a former incremental scan job, the former incremental scan must also be available.

If selecting Incremental Scan, the Reference Time option is enabled.

- **Reference Time** – Choose whether to scan contents created or modified at a specified interval. If you choose to use a reference time, specify the time to scan contents created or modified. Enter an integer into the textbox and select **Minute(s)**, **Hour(s)**, **Day(s),** or **Month(s)** from the drop-down list.

  ***Note**: It is recommended that you specify a reference time when the recurrence schedule configured in **Range of Recurrence** is **End after 1 occurrence**.

After configuring the schedule for the Compliance Scanner plan, select **Calendar View** to view the scheduled jobs by **Day**, **Week**, or **Month**. All of the schedules will be displayed in the **Summary** table. Select **X** to delete a schedule.

Select **Next**. The **Advanced** page appears.

5. Configure the advanced settings:

   - **Agent Group** – Select the agent group that will perform the Compliance Scanner job.
   - **Notification** – Configure the e-mail notification settings. Select a previously-configured notification profile from the **Select a profile with address only** drop-down list, or choose to create a new e-mail notification profile by selecting the **New Notification Profile** link. Select **View** to view the detailed configuration of the selected notification profile. For more information on configuring the e-mail notification profiles, refer to Configuring Receive E-Mail Settings.

   Select **Next**. The **Overview** page appears.

6. Review and edit the plan configurations. To make changes, select the **Edit** button next to the name of the each configuration field to jump to the corresponding setting page and edit the configuration.
7. Once you are satisfied with the plan settings, choose one finishing option at the lower-right section of the screen. Select **Finish** to save the configuration of the plan without running it or **Finish and Run Now** to save the configuration and then run the saved plan immediately.

Scan Schedule

Configure the following settings to build a new Compliance Scanner schedule in the Add Schedule pop-up window:

- **Options** – Select a scan type from the drop-down list.

- **Full Scan** – Run a full scan of all of the documents and items in the specified scope. Unlike incremental scan, all full scans are independent of one another and do not have any dependencies on the other's scan results. However, because each of the full scans is comprehensive, full scan jobs take the longest to complete of the two available options.
- **Incremental Scan** – Run a fractional scan. It scans only the updated documents and items since the last successful full scan or incremental scan. This kind of scan requires less storage than a full scan and it reduces the execution time of the scan job. However, it is important to note that for each incremental scan, the latest full scan job in the full scan cycle must be available. If the incremental scan is based on a former incremental scan job, the former incremental scan must also be available.

  If selecting Incremental Scan, the Reference Time option is available for configuration.

  - **Reference Time** – Choose whether to scan contents created or modified at a specified interval. If you choose to use a reference time, specify the time to scan contents created or modified. Enter an integer into the textbox and select **Minute(s)**, **Hour(s)**, **Day(s)**, or **Month(s)** from the drop-down list.

  ***Note**: It is recommended that you specify a reference time when the recurrence schedule configured in **Range of Recurrence** is **End after 1 occurrence**.

- **Schedule Settings** – Set up the frequency for the scheduled Compliance Scanner job. Select one time unit from **Minute(s)**, **Hour(s)**, **Day(s)**, **Week(s)**, and **Month(s)**, and then enter an integer into the text box. The scheduled Compliance Scanner job will be run according to the interval configured here.
- **Range of Recurrence** – Select the start time and end time for the schedule.
  - **Start time** – Set up the time to start the Compliance Scanner plan and modify the time zone as required.

    ***Note**: The start time cannot be earlier than the current time.

  - **No end date** – Select this option to repeat running the plan until being stopped manually.
  - **End after specified occurrence(s)** – Select this option to stop the plan automatically after the specified occurrences that you configure in the text box.
  - **End by** – Set up the time to end the recurrence of scheduled Compliance Scanner plans.

Performing a Compliance Scanner Plan in Form Mode

Form Mode is recommended for users who are familiar with building Compliance Scanner plans. To build a Compliance Scanner plan in Form Mode, select the scan scope, and then select **Plan Builder** >

Form Mode. Refer to Performing a Compliance Scanner Plan in Wizard Mode for detailed information regarding each option.

***Note**: If this is your first time building a plan, or if you think you would benefit from descriptions of each plan component, it is recommended that you use the Wizard Mode.

Compliance Guardian Scanner for File System

The File System Mode allows you to configure a connection with a location and then perform a scan job using the defined scan policy to generate the compliance scan results of all of the files within that specified location. The users in the specified Report Group can then view the compliance scan results in the Compliance Report module.

Launching Compliance Guardian Scanner File System Mode

On the Compliance Guardian Scanner Home interface, select **Create** on the ribbon. A drop-down list appears. Select **File System** from the drop-down list, and you will be brought to the Compliance Guardian Scanner File System Mode.

Selecting the Scan Scope

After launching the Compliance Scanner File System mode, the **Scope** panel on the left of the screen displays all of the pre-configured connections. Select one or more connections. The files in the connected locations will be scanned.

Using Plan Builder to Perform a Compliance Guardian Scanner Plan for File System

Use the Plan Builder to set up a Compliance Scanner plan. To use Plan Builder, complete the following steps:

1. After selecting the connections for the compliance scan, select **Plan Builder** on the ribbon of Compliance Scanner page.
2. From the drop-down menu, select **Wizard Mode** for step-by-step guidance during configuration, or select **Form Mode** (recommended for advanced users only) to set up a plan quickly.

See the section below that is applicable to your choice for details on performing a Compliance Scanner plan.

Performing a Compliance Scanner Plan in Wizard Mode

Wizard Mode provides you with step-by-step guidance on how to configure a new plan. To configure a plan using Wizard Mode, complete the following steps:

***Note:** An asterisk (*) in the user interface indicates a mandatory field or step.

1. Enter a **Plan Name** and an optional **Description** if desired. Select **Next**. The **Report Settings** page appears.
2. Configure the report settings:
   - **Database Policy** – Select a database policy from the drop-down list to store the result data of the Compliance Scanner job. If you want to set up a new database policy, select the **New Database Policy** link in the drop-down list. Refer to Configuring Report Database Policy for more information.
   - **Report Group** – Select a Compliance Guardian group from the drop-down list. Once a group is specified as the **Report Group**, all of the users in the specified group will be able to view and download the reports in the Compliance Report module. Multiple groups can be specified here; choose **Select All** to select all of the listed groups.

   Select **Next**. The **Scan Settings** page appears.
3. Configure the scan files settings:
   - **Scan Policy** – Select a scan policy from the drop-down list and it will be used to scan the contents in the specified scope. Only one scan policy can be selected here.
   - **Scan Hidden Files Option** – Select whether or not to scan the hidden files in the specified file system.
   - **Filter Policy** – Specify a filter policy to filter the contents that will be scanned. By default, the default filter policy is used, and all of the types of documents/items supported by Compliance Guardian are included in this default filter policy. If you want to set up a new filter policy, select the **New Filter Policy** link in the drop-down list. Refer to Configuring Filter Policies for more information.
   - **Alert** – If you want Compliance Guardian to send an e-mail when an error occurs during the file scan, then select an e-mail profile to specify the users who will receive the e-mail. And then select an e-mail template. You can also select the **New E-mail Template** link to create a new e-mail template. Refer to Configuring E-mail Templates for more information.

     ***Note:** Even though there may be more than one error when scanning a file, the alert e-mail will only be sent when the first error occurs.

   Select **Next**. The **Schedule** page appears.
4. Configure the schedule settings:
   - **No schedule** – Select this option to run the plan immediately and save the plan in Plan Manager.

- **Configure the schedule myself** – Select this option to configure a customized schedule, and run the Compliance Scanner job by schedule. Select **Add Schedule** to set up a schedule. The **Add Schedule** window appears. In the **Options** section, select a scan type from the drop-down list. For more information, review to Scan Schedule.
    - **Full Scan** – Run a full scan of all of the documents and items in the specified scope. Unlike incremental scan, all full scans are independent of one another and do not have any dependencies on the other's scan results. However, because each of the full scans is comprehensive, full scan jobs take the longest to complete of the two available options.
    - **Incremental Scan** – Run a fractional scan. It scans only the updated documents and items since the last successful full scan or incremental scan. This kind of scan requires less storage than a full scan and it reduces the execution time of the scan job. However, it is important to note that for each incremental scan, the latest full scan job in the full scan cycle must be available. If the incremental scan is based on a former incremental scan job, the former incremental scan must also be available.

      If selecting Incremental Scan, the Reference Time option is enabled.

        - **Reference Time** – Choose whether to scan contents created or modified at a specified interval. If you choose to use a reference time, specify the time to scan contents created or modified. Enter an integer into the textbox and select **Minute(s)**, **Hour(s)**, **Day(s),** or **Month(s)** from the drop-down list.

          ***Note**: It is recommended that you specify a reference time when the recurrence schedule configured in **Range of Recurrence** is **End after 1 occurrence**.

After configuring the schedule for the Compliance Scanner plan, select **Calendar View** to view the scheduled jobs by **Day**, **Week**, or **Month**. All of the schedules will be displayed in the **Summary** table. Select **X** to delete a schedule.

Select **Next**. The **Advanced** page appears.

5. Configure the advanced settings:

    - **Notification** – Configure the e-mail notification settings. Select a previously-configured notification profile from the **Select a profile with address only** drop-down list, or choose to create a new e-mail notification profile by selecting the **New Notification Profile** link. Select **View** to view the detailed configuration of the selected notification profile. For more information on configuring the e-mail notification profiles, refer to Configuring Receive E-Mail Settings.

Select **Next**. The **Overview** page appears.

6. Review and edit the plan configurations. To make changes, select the **Edit** button next to the name of the each configuration field to jump to the corresponding setting page and edit the configuration.
7. Once you are satisfied with the plan settings, choose one finishing option at the lower-right section of the screen. Select **Finish** to save the configuration of the plan without running it or **Finish and Run Now** to save the configuration and then run the saved plan immediately.

Scan Schedule

Configure the following settings to build a new Compliance Scanner schedule in the Add Schedule pop-up window.

- **Options** – Select a scan type from the drop-down list.
  - **Full Scan** – Run a full scan of all of the documents and items in the specified scope. Unlike incremental scan, all full scans are independent of one another and do not have any dependencies on the other's scan results. However, because each of the full scans is comprehensive, full scan jobs take the longest to complete of the two available options.
  - **Incremental Scan** – Run a fractional scan. It scans only the updated documents and items since the last successful full scan or incremental scan. This kind of scan requires less storage than a full scan and it reduces the execution time of the scan job. However, it is important to note that for each incremental scan, the latest full scan job in the full scan cycle must be available. If the incremental scan is based on a former incremental scan job, the former incremental scan must also be available.

    If selecting Incremental Scan, the Reference Time option is available for configuration.

    - **Reference Time –** Choose whether to scan contents created or modified at a specified interval. If you choose to use a reference time, specify the time to scan contents created or modified. Enter an integer into the textbox and select **Minute(s)**, **Hour(s)**, **Day(s)**, or **Month(s)** from the drop-down list.

    ***Note**: It is recommended that you specify a reference time when the recurrence schedule configured in **Range of Recurrence** is **End after 1 occurrence**.

- **Schedule Settings** – Set up the frequency for the scheduled Compliance Scanner job. Select one time unit from **Minute(s)**, **Hour(s)**, **Day(s)**, **Week(s)**, and **Month(s)**, and then enter an integer into the text box. The scheduled Compliance Scanner job will be run according to the interval configured here.
- **Range of Recurrence** – Select the start time and end time for the schedule.
  - **Start time –** Set up the time to start the Compliance Scanner plan and modify the time zone as required.

***Note**: The start time cannot be earlier than the current time.

- **No end date** – Select this option to repeat running the plan until being stopped manually.
- **End after specified occurrence(s)** – Select this option to stop the plan automatically after the specified occurrences that you configure in the text box.
- **End by** – Set up the time to end the recurrence of scheduled Compliance Scanner plans.

Performing a Compliance Scanner Plan in Form Mode

Form Mode is recommended for users who are familiar with building Compliance Scanner plans. To build a Compliance Scanner plan in Form Mode, select the scan scope, and then select **Plan Builder** > **Form Mode**. Refer to Performing a Compliance Scanner Plan in Wizard Mode for detailed information regarding each option.

***Note**: If this is your first time building a plan, or if you think you would benefit from descriptions of each plan component, it is recommended that you use the Wizard Mode.

Compliance Guardian Scanner for Website

Launching Compliance Guardian Scanner in Website Mode

On the Compliance Guardian Scanner Home interface, select **Create** on the ribbon, and a drop-down list appears. Select **Website** from the drop-down list, and you will be brought to the Compliance Guardian Scanner Website **Create Plan** interface.

Using Plan Builder to Perform a Compliance Guardian Scanner Plan for Website

In the **Create Plan** interface, configure the following settings for creating a Compliance Guardian Website Scanner plan.

In the **What do you want to scan?** field:

- **Start From** – Enter a URL, Compliance Guardian will scan the objects from this URL. Optionally, you can select to use the Compliance Guardian Transaction Capture tool to save a transaction file, and select the **Use Compliance Guardian Transaction Capture. Export the following transaction file for the scan** radio button in this interface to import a transaction file, then the recorded URLs in the transaction file will be the start URLs. For more information on the Compliance Guardian Transaction Capture tool, refer to Appendix I: Using Compliance Guardian Transaction Capture.
- **Maximum Depth** – It's used to specify the depth level needed to crawl. For example: If you enter **1**, Compliance Guardian will only crawl the start URL specified and scan the

objects in the URL. If you enter **3**, Compliance Guardian will crawl the start URL specified, the linked pages on the start URL page, and the linked pages from the pages one level deeper. If you want to scan all the pages of an entire website, you can enter **0**.

- **Maximum Pages** – Specify the maximum pages allowed to crawl in a single job. **0** means unlimited. If you enter **100**, Compliance Guardian will stop the job after it scans **100** pages in the website.
- **Filter Policy** – Specify a defined filter policy to limit the scope of the scan job. Filter policies are defined in Control Panel.

  ***Note**: The filter policy still takes effect on scanning the recorded results in the transaction file.

- **Follow Robot Exclusion Protocol** – Select whether or not to follow Robot Exclusion Protocol. By default, the checkbox is selected, which means that Compliance Guardian will not crawl any link that is forbidden to access in **Robot.txt**.
- **Allow crawling redirections--Maximum Redirections allowed []** – Select whether or not to allow crawling redirections. If you want to allow crawling redirections, specify the maximum redirections allowed for one page. By default, the checkbox is selected, and the default maximum allowed redirections are **10**.

In the **What policy do you want to use for scanning this website?** field:

- **Select a Predefined Scan Policy** – Specify a scan policy for scanning the defined site. Select **View** beside the drop-down list to view details of the scan policy, or select **New Scan Policy** from the drop-down list. For information on creating a scan policy, refer to Creating or Editing Scan Policies.

In the **How do you want to scan this website?** field:

- **User Agent** – Select the saved user agent profile to specify the user agent for the backend web server when scanning the website. A pre-defined user agent profile can be used directly. Select **New User Agent** to create a new user agent profile.
- **Authentication Method** – Select the Authentication Profile used to connect to the website.
- **Maximum Concurrent Threads** – Allow user to specify the maximum concurrent threads that can be used during the crawling job for the scan. If you select **Breadth-first** in **Crawl Mode**, the default value of **Maximum Concurrent Threads** is 2; if you select **Depth-first** in **Crawl Mode**, the default value of **Maximum Concurrent Threads** is 1.
- **Time out of one scan** – Specify the maximum time of one entire scan job. The default value is **24 hours**.
- **Time out of link** – Specify the maximum time of waiting for a response from a link before skipping it during a crawl. The default value is **100 seconds**.

  ***Note**: By default, the crawl mode is Depth First. If you want to change the crawl mode, you can go to the machines with Compliance Guardian Manager installed and open

the …*Compliance Guardian**Manager**Control**Config* directory to find the **ComplianceSetting.config** file. In the configuration file, find the **DepthFirst="true"** node. **True** means Depth First (scans child nodes from the current node first). **False** means Breadth First (scans sibling nodes from the current node, and the scan will only continue to a lower level after the scan finishes on all the pages of one level).

In the **Where do you want to output the report data and who do you want to share the reports with?** field:

- **Select a predefined Database policy** – Select a database policy to store the scan job data. Database policy also includes the retention settings for the scan data.
- **Report Group** – Select a Compliance Guardian report group from the drop-down list. Once a group is specified as the Report Group, all of the users in the specified group will be able to view and download the reports in the Compliance Report module. Multiple groups can be specified here; choose **Select All** to select all of the listed groups.

In the **How do you want to execute the scan?** field:

- **Set a start time and/or intervals to return the scan automatically** – Optionally, select this checkbox and then choose a scheduling option:
  - **No schedule** – Select this option to configure the job to not run on a schedule (the job must be manually initiated).
  - **Configure the schedule myself** – Configure a customized schedule, and run the plan by schedule.

    Select **Add Schedule** and the Add Schedule window pops up. Configure the following settings for the schedule:

    - **Options** – Select the type of the scan for this plan: **Full Scan** or **Incremental Scan**. Full Scan scans all of the content in the scope defined in the plan, while Incremental Scan only scans the content that has been modified since the last incremental or full scan job.

      If selecting **Incremental Scan**, the **Reference Time** option is enabled.

    - **Reference Time** – Choose whether to scan contents created or modified at a specified interval. If you choose to use a reference time, specify the time to scan contents created or modified. Enter an integer into the textbox and select **Minute(s)**, **Hour(s)**, or **Day(s)** from the drop-down list.

      ***Note**: It is recommended specifying a reference time when the recurrence schedule configured in Range of Recurrence is End after 1 occurrence.

    - **Schedule Settings** – Specify the frequency to run the rerunning schedule. Enter an integer into the text box and select **Minute(s)**, **Hour(s)**, **Day(s)**, **Week(s)**, or **Month(s)** from the drop-down list.

- **Range of Recurrence** – Specify when to start and end the running recurring schedule.
  - **Start time** – Set up the time to start the plan and Time Zone can be changed under the Start time.

    ***Note:** The start time cannot be earlier than the current time.
  - **No end date** – Select this option to repeat running the plan until being stopped manually.
  - **End after specified occurrence(s)** – Select this option to stop the plan after specified occurrences that you configure in the text box.
  - **End by** – Set up the time to end the recurrence of plans.

Select **OK** to save the settings. After configuring the schedule for this replication job, select **Calendar View** to view the job in a calendar view.

- **Select an agent group to allow the system to select a free agent to execute the scan job** – Select an agent group, or select **New Agent Group** to create an agent group.

In the **What do you want to name the plan and do you want to be notified by e-mail?** field:

- **Plan Name** – Enter a name for the plan.
- **Description** – Enter an optional description for this plan.

  Then select whether or not to receive the job report after a scan job finishes. If you want to receive the job report, select the checkbox before **E-mail me the job report and scan results**, and then select a notification profile. Select **New Notification Profile** to create to new notification profile.

Compliance Reports

For details about Compliance Guardian reports and procedures for how to use them, refer to the Compliance Guardian User Guide.

Getting Started

Refer to the sections below for important information on getting started with Compliance Report.

Launching Compliance Report

To launch Compliance Report, complete the following steps:

1. Log in to Compliance Guardian. If you are already in the software, select the home page button ( ) on the top left corner go to the home page. From the home page, all of the products are displayed.

2. Select the Compliance Report to launch its interface.
3. Alternatively, you can select **Report** on the top-left corner, and select the corresponding Report tab on the appeared navigation bar to launch Compliance Scanner.

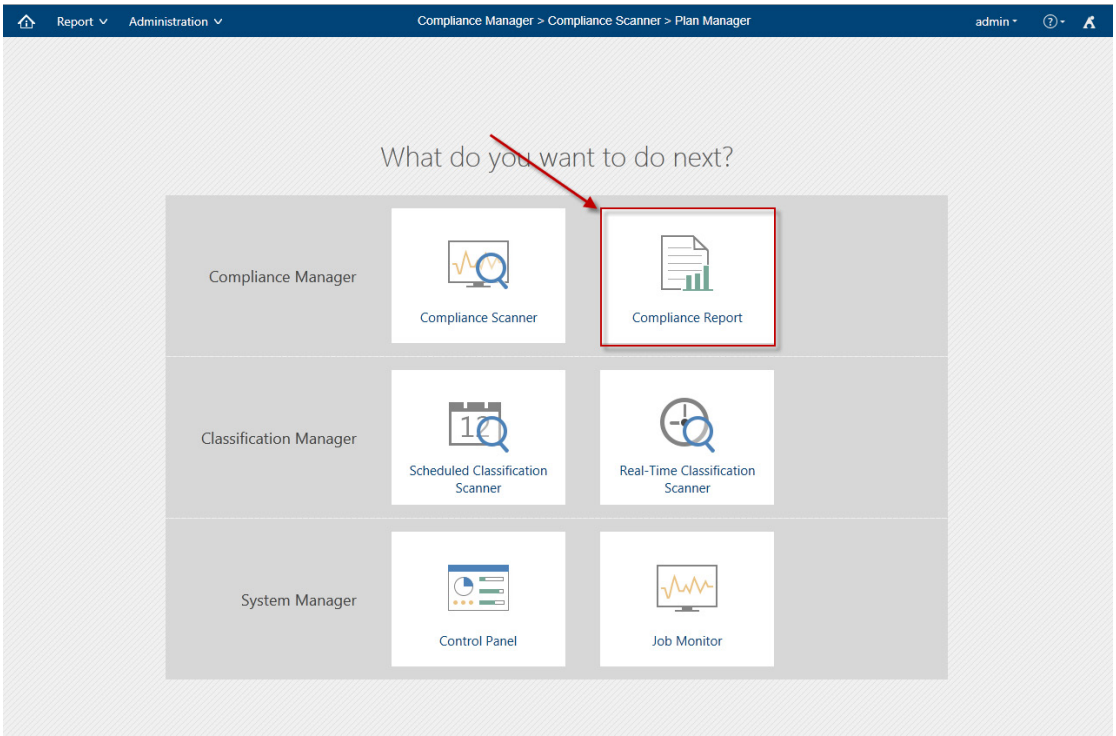

Figure 11: Compliance Guardian module launch window.

User Interface Overview

The Compliance Report user interface launches with the **Compliance Reports** tab active. This tab displays the scan results, risk report, violation report, and other reports after selecting a plan.

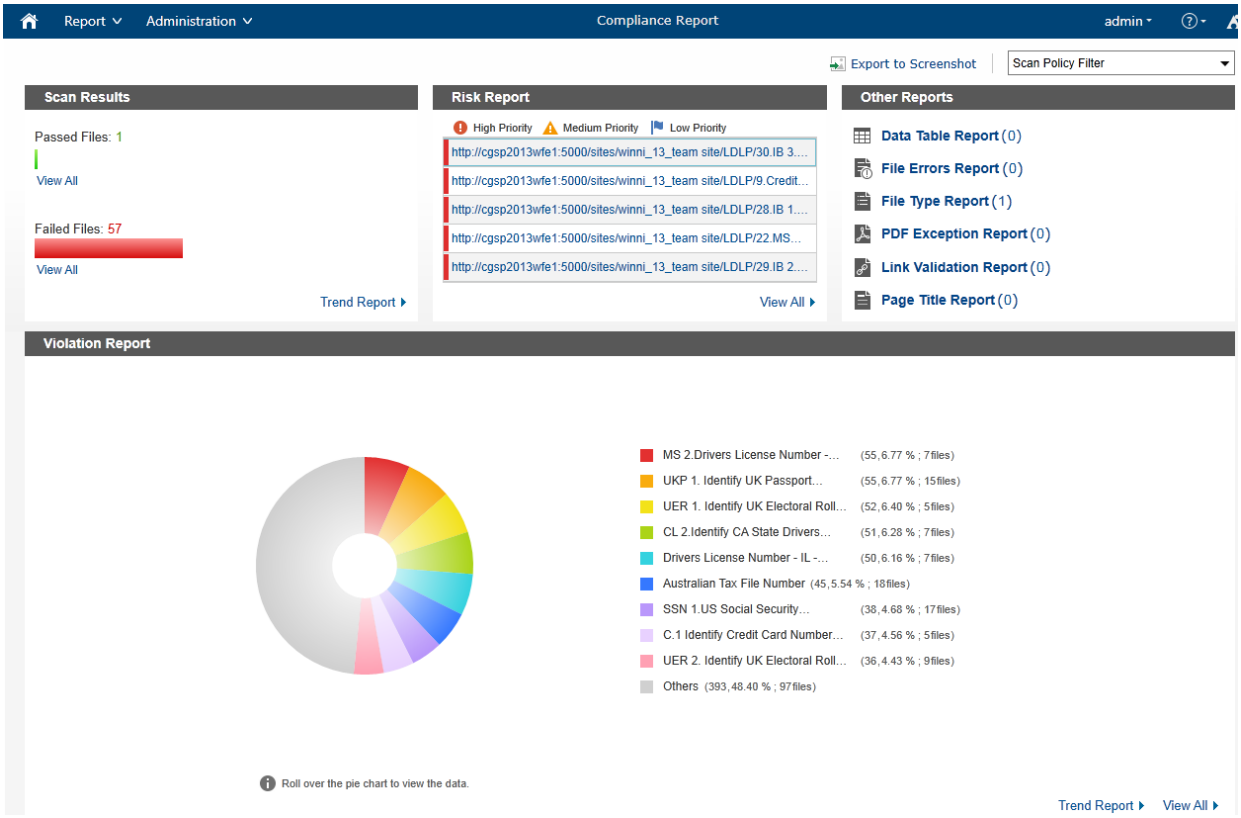

Figure 12: Compliance Report user interface.

This interface shows the scan results of the selected plan. This content is dynamic; it will often change depending on what kind of report is selected.

You can select **Report** on the left corner of the page, and then select the kind of report that you want to view on the appeared navigation bar.

Classification Manager

Classification Manager enables you to define a scan scope, and then it performs a job to scan out the related contents according to the scan policy, at last it will perform the specified actions to the contents scanned out.

***Note:** In order to scan Microsoft Office files that are in a 2003 or earlier format, you must download a compatibility pack. Once you install the compatibility pack, Compliance Guardian will support scans of these files, but the software does not support tagging of Microsoft Office 2003 files even though they can be scanned and classified after installing the compatibility pack.

Classification Manager includes the Real-Time Classification Scanner and Scheduled Classification Scanner. Refer to Real-Time Classification Scanner and Scheduled Classification Scanner for more information.

Real-Time Classification Scanner

The Real-Time Classification Scanner is used to scan contents, classify them, and then perform actions to the scanned contents in real time. The Real-Time Classification Scanner rule must first be applied on the desired scope before using Real-Time Classification Scanner to scan contents in the specified scope. For more information, refer to Creating Real-Time Classification Scanner Rules. After you apply the Real-Time Classification Scanner rule, the updated content in the defined scope will be scanned and dealt with according to the specified rule in real time.

Pre-Configurations

Configuring Scan Policies

A scan policy defines the compliance rules to be used when scanning the contents in the specified scope. To configure the scan policies, select **Scan Policy** on the ribbon of the Real-Time Classification Scanner page to go to the **Scan Policy** interface.

Managing Scan Policies

The **Scan Policy** interface displays all of the scan policies that you have previously created. In the **Scan Policy** interface, you can change the number of scan policies displayed per page and the order in which they are displayed.

To change the number of scan policies displayed per page, select the desired number from the **Show rows** drop-down menu in the lower right-hand corner. To sort the action policies, select a column heading such as **Scan Policy Name**, **Description**, or **Last Modified Time**.

You can customize how these scan policies are displayed in the following ways:

- **Search** – Filter the scan policies to be displayed by the keyword you designate. The keyword must be contained in a column value. At the top of the viewing pane, enter the keyword for the action policy you want to display. You can select **Search all pages** or **Search current page** to define the search scope. **Search all pages** means that the scan policies in all of the pages whose names or descriptions contain the keywords will be displayed; while **Search current page** means that only the scan policies in the current page whose names or descriptions contain the keywords will be displayed.

  ***Note:** The search function is not case sensitive.

- **Manage columns** (⊞) – Manage which columns are displayed in the list so that only information you want to see is shown. Select the manage columns button (⊞), and then check the checkbox next to the column name to have that column shown in the list.
- **Hide the column** (⊖) – Hover over a column name, and then select the hide column button (⊖) of the column you want to hide, and the column will be hidden.

Perform the following actions in the **Scan Policy** interface:

- **Create** – Select **Create** on the ribbon to create a new scan policy. For details on creating a new action policy, refer to Creating and Editing Scan Policies.
- **View** – Select **View** on the ribbon and you will see the previously configured settings for the selected action policy. Here you can also select **Edit** on the ribbon to make changes to the scan policy's settings. You will be brought to the **Edit** Scan Policy interface where you can change this scan policy.
- **Edit** – Select **Edit** on the ribbon to change the configurations for the selected scan policy. For details on editing configurations for a scan policy, refer to Creating and Editing Scan Policies.
- **Delete** – Select **Delete** on the ribbon. A confirmation window will pop up and ask if you are sure you want to proceed with the deletion. Select **OK** to delete the selected scan policies, or select **Cancel** to return to the **Scan Policy** interface without deleting the selected scan policies.
- **Export** – Export the check information for the test suites included in the selected scan policy.

Creating and Editing Scan Policies

To create a new scan policy, select **Create** in the Manage group of the Scan Policy page. To modify a previously configured scan policy, select the scan policy, and then select **Edit** on the ribbon. In the **Create Scan Policy** or **Edit Scan Policy** interface, configure the following settings:

- **Name and Description** – Enter a name for this scan policy. You can also enter an optional description to distinguish this scan policy from the others.
- **Select the Test Suites** – Specify the test suites that you want to include in this scan policy. There are some predefined test suites in this page. You can refer to the

description of each test suite for the introduction of its usage. To add more desired test suites, select **Test Suite Manager** in the Settings group on the ribbon. For more information on configuring the test suites, refer to Test Suite Manager.

After selecting some test suites, if you want to clear the selection status, select the **Clear Selection** link and then specify your desired test suites again.

To change the number of test suites displayed per page, select the desired number from the **Show rows** drop-down menu in the lower right-hand corner. To sort the test suites, select a column heading such as **Test Suite** or **Description**.

You can also perform the following actions when selecting the test suites:

- **Search** – Filter the test suites to be displayed by the keyword you designate. The keyword must be contained in a column value. At the top of the viewing pane, enter the keyword for the action policy you want to display. You can select **Search all pages** or **Search current page** to define the search scope. **Search all pages** means that the test suites in all of the pages whose names or descriptions contain the keywords will be displayed; while **Search current page** means that only the test suites in the current page whose names or descriptions contain the keywords will be displayed.

  ***Note:** The search function is not case sensitive.

- **Manage columns** (⊞) – Manage which columns are displayed in the list so that only information you want to see is shown. Select the manage columns button (⊞), and then check the checkbox next to the column name to have that column shown in the list.
- **Hide the column** (⊖) – Hover over a column name, and then select the hide column button (⊖) of the column you want to hide, and the column will be hidden.

After you are satisfied with the configuration of the scan policy, select **OK** to save this scan policy. If you do not want to save the current configuration, select **Cancel** to cancel the configuration.

Configuring Filter Policies

For more information, refer to Filter Policy.

Configuring Action Policies

Action policies allow you to define the actions to be performed on the scanned contents in the specified scope. To configure the action policies, select **Action Policy** on the ribbon of the Real-Time Classification Scanner page to go to the Action Policy interface.

Managing Action Policies

The **Action Policy** interface displays all of the action policies that you have previously created. In this interface, you can change the number of action policies displayed per page and the order in which they are displayed.

To change the number of action policies displayed per page, select the desired number from the **Show rows** drop-down menu in the lower right-hand corner. To sort the action policies, select a column heading such as **Action Policy Name**, **Description**, or **Last Modified Time**.

You can customize how these connections are displayed in a number of different ways:

- **Search** – Filter the action policies to be displayed by the keyword you designate. The keyword must be contained in a column value. At the top of the viewing pane, enter the keyword for the action policy you want to display. You can select **Search all pages** or **Search current page** to define the search scope. **Search all pages** means that the action policies in all of the pages whose names or descriptions contain the keywords will be displayed; while **Search current page** means that only the action policies in the current page whose names or descriptions contain the keywords will be displayed.

  ***Note:** The search function is not case sensitive.

- **Manage columns** (⊞) – Manage which columns are displayed in the list so that only information you want to see is shown. Select the manage columns button (⊞), and then check the checkbox next to the column name to have that column shown in the list.
- **Hide the column** (⊖) – Hover over a column name, and then select the hide column button (⊖) of the column you want to hide, and the column will be hidden.

Perform the following actions in the **Action Policy** interface:

- **Create** – Select **Create** on the ribbon to create a new action policy. For details on creating a new action policy, refer to Creating and Editing Action Policies.
- **View** – Select **View** on the ribbon and you will see the previously configured settings for the selected action policy. Here you can also select **Edit** on the ribbon to make changes to the action policy's settings. You will be brought to the **Edit Action Policy** interface where you can change this action policy.
- **Edit** – Select **Edit** on the ribbon to change the configurations for the selected action policy. For details on editing configurations for an action policy, refer to Creating and Editing Action Policies.
- **Delete** – Select **Delete** on the ribbon. A confirmation window will appear and ask if you are sure you want to proceed with the deletion. Select **OK** to delete the selected action policies, or select **Cancel** to return to the **Action Policy** interface without deleting the selected action policies.

Creating and Editing Action Policies

To create a new action policy, select **Create** on the ribbon. To modify a previously-configured action policy, select the action policy, and then select **Edit** on the ribbon.

1. In the Create Action Policy interface or Edit Action Policy interface, configure the following settings:

    - **Name and Description** – Enter a **Name** for the action policy connection. Then enter an optional **Description** for this action policy for future reference.
    - **Actions** – Choose an action to handle the not compliant files which are found by performing the classification jobs.
        - **Move to the specified allowed location (only for files in document library)** – The scanned files that are not compliant will be moved to the specified allowed location configured beforehand.

          ***Note:** Only the files in the document library can be moved. For more detailed information on how to configure the allowed location, refer to Configuring Allowed Location.

          If you check this checkbox, the option **If the files(s) failed to move, it/they will be quarantined** will be shown. With this option enabled, the files that are failed to be moved will then be quarantined. For more information on managing the quarantined files, refer to Using Compliance Guardian Quarantine Manager in SharePoint. The following conditions will lead to the failure of moving files:

            - There is no content type that matches the source file's content type in the target library.
            - The matched content type of the target library (where the allowed location is) does not contain all of the source file's columns.
            - Other unknown system issues.

          Uncheck the **If the files fail to move, it/they will be quarantined** checkbox if you want to ignore to deal with the files that are failed to be moved.

          The **Enable Actions Configuration** area appears below after checking the **Move to the specified allowed location (only for files in document library)** checkbox. For detailed information on the action configuration, refer to Actions Configuration.

        - **Quarantine files/items** – The scanned files or items that are not compliant will be quarantined, they will be deleted to the Site Collection Recycle Bin, and you can **manage these files** or items through the **Compliance Guardian Quarantine Manager** feature in SharePoint. For more information on how to use **Compliance Guardian Quarantine Manager**, refer to Using Compliance Guardian Quarantine Manager in SharePoint.

***Note:** Items or files will be automatically deleted after 30 days in the Site Collection Recycle Bin. You must manage the items or files in 30 days after they are quarantined to the Recycle Bin, or you can adjust the schedule for deleting items in the Recycle Bin by navigating to SharePoint 2010 > **Central Administration** > **Manage Web Applications**, selecting the corresponding Web application, and then selecting **General Settings** (in SharePoint 2007, you can adjust the schedule for deleting items in the Recycle Bin by navigating to **SharePoint 2007** > **Central Administration** > **Web application general settings**).

The **Enable Actions Configuration** area appears below after checking the **Quarantine files** checkbox. For detailed information on the action configuration, refer to Actions Configuration.

- **Delete files/items** – The scanned files or items that are not compliant will be deleted to the Site Collection Recycle Bin.

  The **Enable Actions Configuration** area appears below after checking the **Delete files/items** checkbox. For detailed information on the action configuration, refer to Actions Configuration.

- **Change permissions** – The permissions of the files or items that are not compliant will be changed to be what you have configured in the **Enable Actions Configuration** section.

  The **Enable Actions Configuration** area appears below after checking the **Change permissions** checkbox. For detailed information on the action configuration, refer to Actions Configuration.

2. Select **OK** to save the configurations and return to the **Action Policy** interface, or select **Cancel** to return to the **Action Policy** interface without saving any changes.

Actions Configuration

Configure the following settings corresponding to the actions you selected:

- Action Configuration for **Move to the specified allowed location (only for files in document library)** – Configure the following settings:
  - Configure action policy filter rules to define the files that will be moved to the allowed location. Refer to the following steps to configure the action policy filter rules:
    - Select a category, select **Add a Filter Level Group** to add a new rule of the specified category level, and then select the delete button ( ) to delete the rule that is no longer needed. Configure the following fields for the rule:
      - **Rule** – Select the new rule you want to create from the drop-down list.

- **Condition** – Select the condition for the rule.
- **Value** – Enter a value you want the rule to use in the text box.

The filter rule for **Move to the specified allowed location (only for files in document library)** contains two category levels:

- **Document** – Based on the SharePoint Document property value you specified here to define the scope in which the files that are not compliant will be moved.

  ***Note**: Under this category, the filter rules Modified Time and Created Time will not be applied to define the scope for Real-Time Classification Scanner.

- **Classification Result** – Based on the tag value you specified here to define the scope in which the files that are not compliant will be moved. To add more filters, repeat the previous step.

***Note**: Depending on the filters you enter, you can change the order of the rules by selecting ˅ before the Rule value, and then select the order of the rule from the appeared drop-down list to determine the priority of the rule.

You can also change the logical relationships between the rules. There are currently two logical relationships: **And** and **Or**. By default, the logic is set to **And**. To change the logical relationship, select the logical relationship link. The **And** logical relationship means that the content which meets all of the rules will be filtered and included in the result. The **Or** logic means that the content which meets any one of the rules will be filtered and included in the result.

- **Manage Quarantine Files** – If you select the action **If the files fail to move, it/they will be quarantined** above, this option appears. It allows you to manage the quarantined files that are failed to be moved.

  Specify a **SharePoint Group Name** and specify the **Group Permissions** for the SharePoint Group. Users in this group have permissions to manage these quarantined files.

  ***Note:** If the specified SharePoint group does not exist in SharePoint, then the group with the specified permissions will be created for managing the files; if the group already exists in SharePoint, then the permissions of this group will not be changed to what you specified here.

- **Alert** – Specify whether to send out an alert e-mail when a file is moved to the allowed location or is quarantined by checking the **If the action successfully executed** checkbox. Specify whether to send out an alert e-mail when the file is

failed to move to the allowed location or failed to be quarantined by checking the **If the action failed to execute** checkbox.

If you choose to send out alert e-mails, configure the recipients by selecting the corresponding checkboxes in the **Send e-mail to** field:

- **Creator** – Select this checkbox to send an alert e-mail to the creator of the specified file that is moved or quarantined.
- **Modifier** – Select this checkbox to send an alert e-mail to the last modifier of the specified file that is moved or quarantined.
- **User who is specified in the following notification file** – Select this checkbox to send an alert e-mail to the recipients configured in the selected alert notification profile. If this option is selected, you must select an alert notification profile from the appeared drop-down list. You can also select the **New Notification Profile** link to create a new notification profile. For more information, refer to Configuring Receive E-Mail Settings.

- Action Configuration for **Quarantine files/items** – Configure the following settings:
  - Configure action policy filter rules to define the files or items that will be quarantined. Refer to the following steps to configure the action policy filter rules:
    - Select a category, select **Add a Filter Level Group** to add a new rule of the specified category level, and then select the delete button ( ) to delete the rule that is no longer needed. Configure the following fields for the rule:
      - **Rule** – Select the new rule you want to create from the drop-down list.
      - **Condition** – Select the condition for the rule
      - **Value** – Enter a value you want the rule to use in the text box.

      The filter rule for **Quarantine files/items** contains three category levels:

      - **Document** – Based on the SharePoint Document property value you specified here to define the scope in which the files that are not compliant will be quarantined.
      - **Item** – Based on the SharePoint Item property value you specified here to define the scope in which the items that are not compliant will be quarantined.

        ***Note**: Under the **Document** category and the **Item** category, the filter rules **Modified Time** and **Created Time** will not be applied to define the scope for **Real-Time Classification Scanner**.

- **Classification Result** – Based on the tag value you specified here to define the scope in which the files that are not compliant will be quarantined.

To add more filters, repeat the previous step.

***Note**: Depending on the filters you enter, you can change the order of the rules by selecting the change order button ( ) before the rule value, and then select the order of the rule from the appeared drop-down list to determine the priority of the rule.

You can also change the logical relationships between the rules. There are currently two logical relationships: **And** and **Or**. By default, the logic is set to **And**. To change the logical relationship, select the logical relationship link. The **And** logical relationship means that the content which meets all of the rules will be filtered and included in the result. The **Or** logic means that the content which meets any one of the rules will be filtered and included in the result.

- **Manage Quarantine Files/Items** – Specify a **SharePoint Group Name** and specify the **Group Permissions** for the SharePoint Group. Users in this group have permissions to manage these quarantined files or items.

  ***Note:** If the specified SharePoint group does not exist in SharePoint, then the group with the specified permissions will be created for managing the files or items; if the group already exists in SharePoint, then the permissions of this group will not be changed to what you specified here.

- **Alert** – Specify whether to send out an alert e-mail when a file or an item is quarantined by checking the **If the action successfully executed** checkbox. Specify whether to send out an alert e-mail when the file or item is failed to be quarantined by checking the **If the action failed to execute** checkbox.

  If you choose to send out alert e-mails, configure the recipients by selecting the corresponding checkboxes in the **Send e-mail to** field:

  - **Creator** – Select this checkbox to send an alert e-mail to the creator of the specified file that is quarantined.
  - **Modifier** – Select this checkbox to send an alert e-mail to the last modifier of the specified file that is quarantined.
  - **User who is specified in the following notification file** – Select this checkbox to send an alert e-mail to the recipients configured in the selected alert notification profile. If this option is selected, you must select an alert notification profile from the appeared drop-down list. You can also select the **New Notification Profile** link to create a new notification profile. For more information, refer to Configuring Receive E-Mail Settings.

- Action Configuration for **Delete files/items**
  - Configure action policy filter rules to define the files or items that will be deleted.
    - Select a category and then select **Add a Filter Level Group** to add a new rule of the specified category level. And select the delete button ( ) to delete the rule that is no longer needed. Configure the following fields for the rule:
      - **Rule** – Select the new rule you want to create from the drop-down list.
      - **Condition** – Select the condition for the rule
      - **Value** – Enter a value you want the rule to use in the text box

      The filter rule for **Delete files/items** contains two category levels:

      - **Document** – Based on the SharePoint Document property value you specified here to define the scope in which the files that are not compliant will be deleted.
      - **Item** – Based on the SharePoint Document property value you specified here to define the scope in which the items that are not compliant will be deleted.

        ***Note**: Under the **Document** category and the **Item** category, the filter rules **Modified Time** and **Created Time** will not be applied to define the scope for **Real-Time Classification Scanner**.

      - **Classification Result** – Based on the tag value you specified here to define the scope in which the files that are not compliant will be deleted. To add more filters, repeat the previous step.

    ***Note**: Depending on the filters you enter, you can change the order of the rules by selecting before the rule value, and then select the order of the rule from the appeared drop-down list to determine the priority of the rule.
    You can also change the logical relationships between the rules. There are currently two logical relationships: **And** and **Or**. By default, the logic is set to And. To change the logical relationship, select the logical relationship link. The **And** logical relationship means that the content which meets all of the rules will be filtered and included in the result. The **Or** logic means that the content which meets any one of the rules will be filtered and included in the result.

  - Alert – Specify whether to send out an alert e-mail when a file or an item is deleted by checking the **If the action successfully executed** checkbox. Specify whether to send out an alert e-mail when the file or item is failed to be deleted by checking **If the action failed to execute** checkbox.

If you choose to send out alert e-mails, configure the recipients by selecting the corresponding checkboxes in the **Send e-mail to** field:

- **Creator** – Select this checkbox to send an alert e-mail to the creator of the specified file that is deleted.
- **Modifier** – Select this checkbox to send an alert e-mail to the last modifier of the specified file that is deleted.
- **User who is specified in the following notification file** – Select this checkbox to send an alert e-mail to the recipients configured in the selected alert notification profile. If this option is selected, you must select an alert notification profile from the appeared drop-down list. You can also select the **New Notification Profile** link to create a new notification profile. For more information, refer to Configuring Receive E-Mail Settings.

- Action Configuration for **Change permissions**
  - Configure action policy filter rules to define the files or items that will be changed permissions.
    - Select a category and then select **Add a Filter Level Group** to add a new rule of the specified category level. And select the delete button ( ) to delete the rule that is no longer needed. Configure the following fields for the rule: .
      - **Rule** – Select the new rule you want to create from the drop-down list.
      - **Condition** – Select the condition for the rule
      - **Value** – Enter a value you want the rule

      The filter rule for **Change permissions** contains three category levels:

      - **Document** – Based on the SharePoint Document property value you specified here to define the scope in which the files that are not compliant will be changed permissions.
      - **Item** – Based on the SharePoint Document property value you specified here to define the scope in which the items that are not compliant will be changed permissions.

        ***Note**: Under the **Document** category and the **Item** category, the filter rules **Modified Time** and **Created Time** will not be applied to define the scope for **Real-Time Classification Scanner**.

      - **Classification Result** – Based on the tag value you specified here to define the scope in which the files that are not compliant will be changed permissions.

***Note**: Depending on the filters you enter, you can change the order of the rules by selecting the change order button ( ) before the rule value, and then select the order of the rule from the appeared drop-down list to determine the priority of the rule.
You can also change the logical relationships between the rules. There are currently two logical relationships: **And** and **Or**. By default, the logic is set to And. To change the logical relationship, select the logical relationship link. The **And** logical relationship means that the content which meets all of the rules will be filtered and included in the result. The **Or** logic means that the content which meets any one of the rules will be filtered and included in the result.

- **Change Permissions** – Specify a **SharePoint Group Name** and specify the **Group Permissions** for the SharePoint Group. The permissions of the scanned files or items that are not compliant will be changed to what you have configured here.

  ***Note**: If the specified SharePoint group does not exist in SharePoint, then the group with the specified permissions will be created for managing the files or items; if the group already exists in SharePoint, then the permissions of this group will not be changed to what you specified here.

- **Alert** – Specify whether to send out an alert e-mail when a file or an item's permissions are changed by checking **If the action successfully executed** checkbox. Specify whether to send out an alert e-mail when the file or item's permissions are failed to be changed by checking **If the action failed to execute** checkbox.

  If you choose to send out alert e-mails, configure the recipients by selecting the corresponding checkboxes in the **Send e-mail to** field:

  - **Creator** – Select this checkbox to send an alert e-mail to the creator of the specified file whose permissions are changed.
  - **Modifier** – Select this checkbox to send an alert e-mail to the last modifier of the specified file whose permissions are changed.
  - **User who is specified in the following notification profile** – Select this checkbox to send an alert e-mail to the recipients configured in the selected alert notification profile. If this option is selected, you must select an alert notification profile from the appeared drop-down list. You can also select the **New Notification Profile** link to create a new notification profile. For more information, refer to Configuring Receive E-Mail Settings.

If you select more than one action in the Actions field, all of the action configurations for each action must be configured. You can change the order of the action configuration by selecting the textbox on the top of **Scan Settings** to determine the priority of the action. For example, if you select **Quarantined files/items** action and **Move to the specified allowed location (only for files in document library)** action in the **Actions** field of this screen, the action configurations of both the two actions will display. Set the

order of **Move to the specified allowed location (only for files in document library)** action to be **1**, and set the order of **Quarantined files** order to be **2**: The scanned files that are not compliant will not be quarantined, they will be moved to the target allowed location directly instead.

Getting Started

Refer to the sections below for important information on getting started with Real-Time Classification Scanner.

Launching Real-Time Classification Scanner

To launch Real-Time Classification Scanner, complete the following steps:

1. Log in to Compliance Guardian. If you are already in the software, select the home page button ( ) to go to the home page. From the home page, all of the products are displayed.
2. Select the **Real-Time Classification Scanner** to launch its interface.
3. Alternatively, you can select **Administration** on the top-left corner, and select the **Real-Time Classification Scanner** tab on the appeared navigation bar to Real-Time Classification Scanner.

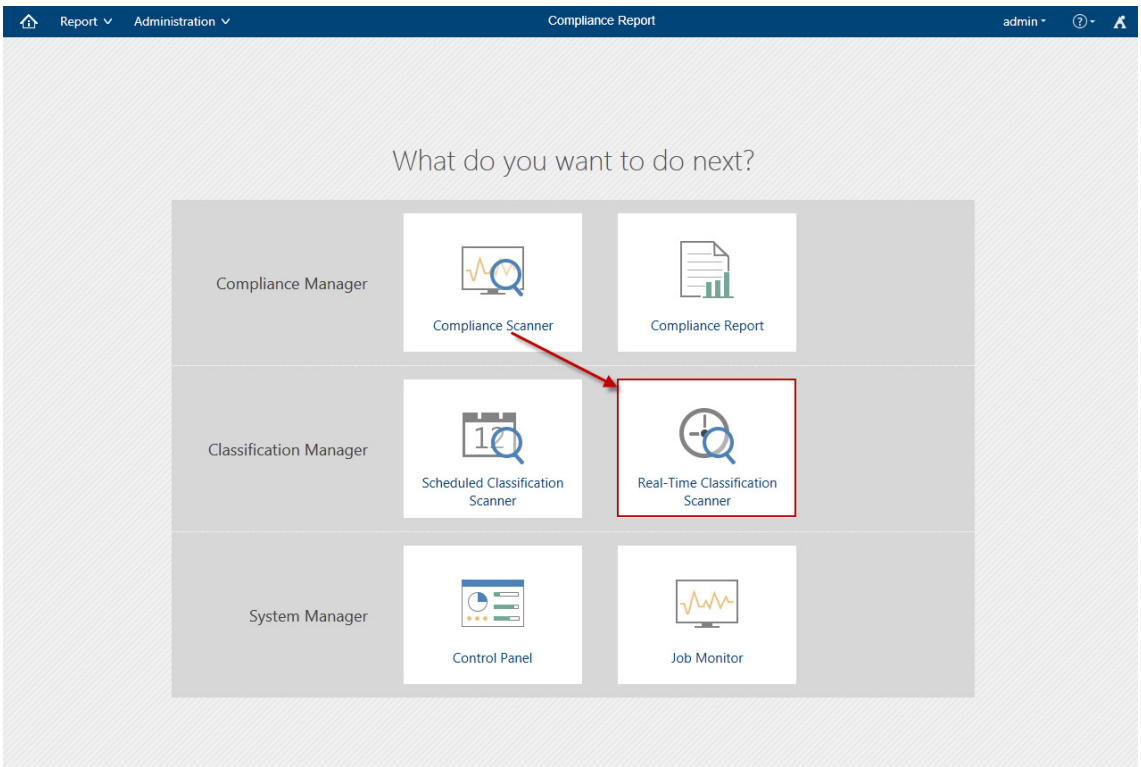

Figure 13: Compliance Guardian module launch window.

Home Page Overview

The Real-Time Classification Scanner home page displays a list of all of your previously configured nodes, which have applied the Real-Time Classification Scanner rules. Also you can select **Create** to enter the **Create Rule** page to create and apply a rule.

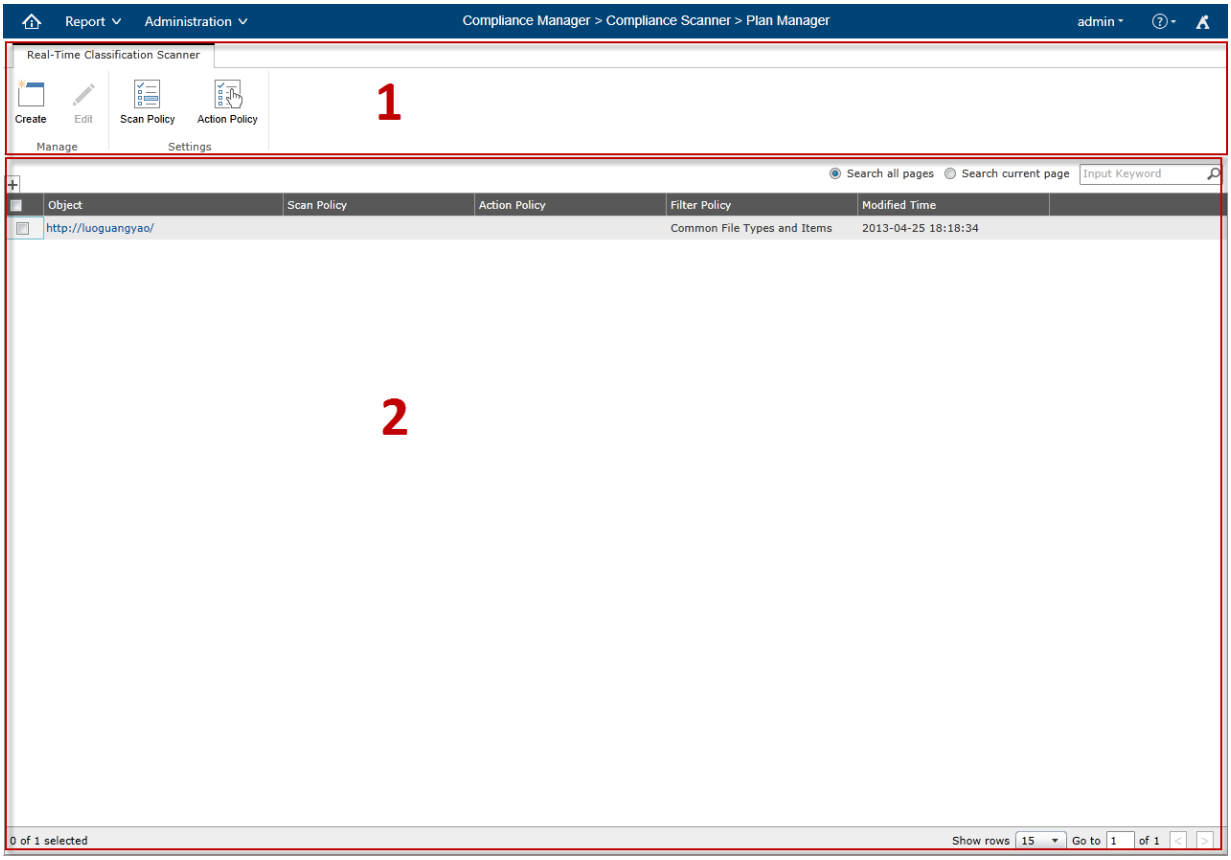

Figure 14: Real-Time Classification Scanner home page.

1. **Ribbon** – Shows the available actions.
    - **Create** – Select **Create**. You will be brought to the **Create Rule** page.
    - **Edit** – Select **Edit** on the ribbon to make changes to the rule of the selected node. You will be brought to the **Edit** page where you can change the rule settings for the node. Select **Apply** on the ribbon to save the changes and apply the rule. Select **Cancel** on the ribbon to return to the home page without saving any of your changes.
    - **Scan Policy** – Create a new scan policy or manage the previously configured scan policies by selecting **Scan Policy**.
    - **Action Policy** – Create a new action policy or manage the previously configured action policies by selecting **Action Policy**.
2. **Managing Nodes** – Display the nodes that have applied Real-Time Classification Scanner rules, but the node that has an inherited rule is not displayed in this field. This field also displays the Scan Policy, **Action** Policy, and Filter Policy that are selected in the corresponding rule.

You can customize how these nodes are displayed in a number of different ways:

- **Search** – Filters the nodes displayed by the keyword you designate. The keyword must be contained in a column value. At the top of the viewing pane, type in the keyword for the plan you want to display. You can select to **Search all pages** or **Search current page**.

  ***Note:** The search function is not case sensitive.

- **Manage columns** (⊕) – Manages which columns are displayed in the list so that only the information you want to see is displayed. Select the manage columns button (⊕) , and then select the checkbox next to the column name to have that column shown in the list.

- **Hide the column** (⊖) – Hover over a column name, and then select the hide column button (⊖) of any column you want to hide.

- **Filter the column** ( ) – Filters which item in the list is displayed. You can filter whichever item you want, rather than search based on a keyword. Hover over a column name, and then select the filter button ( ) of the column you want to filter, then select the checkbox next to the item name to have that item shown in the list.

Using Real-Time Classification Scanner Rules

On the Real-Time Classification Scanner Home interface, select **Create** on the ribbon and you will be brought to the **Create Rule** page.

Creating Real-Time Classification Scanner Rules

To create a Real-Time Classification Scanner rule, complete the following steps:

1. Select the scope of the content you want to scan:

   a. From the **Scope** panel on the left, select the farm that contains the relevant SharePoint content. You can input a keyword into the Search box above the farm tree to filter out the relevant SharePoint content.

   b. Select the relevant content from which you want to perform further operations by selecting the radio button to the left of the content.

2. Select **Create Rule** from the **Rule Management** group on the ribbon.

3. Configure the following rule settings:

   - **Report Database** – Select a **Report Database** for storing the Real-Time Classification Scanner result.

   - **Scan Policy** – Select a scan policy from the drop-down list or create a new scan policy to define the scan rules for scanning content. For more information on working with scan policies, refer to Configuring Scan Policies.

If selecting the **For assist panel only checkbox** below the **Scan Policy** selection drop-down box, the **Action Policy** and **Filter Policy** will be grayed out in this screen. Instead, in SharePoint, through activating the **Compliance Guardian Tag Assist Manager** feature, you can manually scan the selected content based on the scan policy defined in Compliance Guardian, you can change the search results according to your requirements.

***Note:** Only used for scanning documents. For more detailed about using the **Compliance Guardian Tag Assist Manager** feature in SharePoint, refer to Using Compliance Guardian Tag Assist Manager in SharePoint.

- **Action Policy** – Select an action policy from the drop-down list or create a new action policy to define the actions to the content that will be scanned out. For more information on working with action policies, refer to Configuring Action Policies.
- **Alert** – Specify whether to send out an alert e-mail when an error occurs during the process of scanning a file or when a tag fails to be added to a file. If you choose to send out alert e-mails when an error occurs, configure the recipients by selecting the corresponding checkboxes in the Send e-mail to field:
    - **Creator** – Select this checkbox to send an alert e-mail to the creator of the specified file.
    - **Modifier** – Select this checkbox to send an alert e-mail to the last modifier of the specified file.
    - **User who is specified in the following notification file** – Select this checkbox to send an alert e-mail to the recipients configured in the selected alert notification profile. If this option is selected, you must select an alert notification profile from the appeared drop-down list. You can also select the New Notification Profile link to create a new notification profile. For more information, refer to User Notification Settings.

  ***Note:** Even though there may be more than one error when scanning a file, the alert e-mail will only be sent when the first error occurs.
  After configuring the recipients, choose one e-mail template from the E-mail template drop-down list; you can also select the New E-mail template link to create a new e-mail template. For more information, refer to Configuring E-mail Templates.

- **Filter Policy** – Select a filter policy from the drop-down list or create a new policy to limit the scope of the job. For more information on working with filter policies, refer to Configuring Filter Policies.

Applying Real-Time Classification Scanner Rules

After creating a Real-Time Classification Scanner rule on the selected node, select **Apply** on the ribbon or on the right-lower section of the screen to apply the rule.

***Note**: By default, the newly created site will not inherit its parent's Real-Time Classification Scanner rule. You must first deploy the CCS.InstallEventReceiver.wsp solution on SharePoint. For more information on deploying the solution, refer to Solution Manager.

After the CCS.InstallEventReceiver.wsp solution is deployed, the **Compliance Guardian Newly Created Sites Real-Time Scan** feature will be enabled on the Web application automatically. The newly created site's corresponding **Compliance Guardian Real-Time Scan** feature will also be enabled, then the newly created site will apply its parent's Real-Time Classification rule (if the parent has applied a rule).

Inheriting and Stop Inheriting Parents' Rule

After applied a Real-Time Classification Scanner rule on the selected node, the sub-nodes automatically inherit this rule.

On the SharePoint tree, if a node inherits its parent node's rule, only the inherit button ( ) is displayed before this node; if a node does not inherit its parent node's rule, but has its own rule, the stop inherit button ( ) icon is also displayed before this node.

Stop Inheriting Parents Rule

Stop Inheriting logically separates the rule in the lower level-node from the upper-level node. After one rule has been applied for a particular level (Level A), you can still configure rules directly to levels that are higher than Level A. However, if you want to configure rules at levels that are lower than Level A, you must first break the rule inheritance. To break this inheritance, select **Stop Inheriting** in the **Manage** group on the ribbon.

Some helpful notes on the Stop Inheriting Parents rule:

- When breaking the rule's inheritance at a specified level, the inheritance is only broken at this level. The rule's inheritance of the lower levels is not broken.
- After the rule's inheritance is broken, you can apply new rules and edit the corresponding rule settings at the lower level.

Inheriting Parents' Rule

Use the inheriting feature after you have stopped a node's rule inheritance from its parent node. To manually apply a rule inheritance to a node, select the node that will inherit the parent node's rule, and select **Inheriting** in the **Manage** group on the ribbon. After selecting **Inheriting**, this button changes to **Stop Inheriting**.

Some following helpful notes on the Inheriting rule:

- By default, the Real-Time Classification Scanner rule configured for a higher level is inherited by the lower levels.
- You cannot create a new rule on a node if it inherits the rules of the higher level. Inheritance must first be broken.
- The inherited Real-Time Classification Scanner rule cannot be edited; it can only be viewed.
- Once you have broken the rule inheritance on a node, if you choose to inherit the rules of the higher level again, all of the rules that are added after breaking the inheritance on this node will be removed from the following nodes:
    - The node that inherits the higher level rules again.
    - The nodes that inherit the rules from the node above.

Scheduled Classification Scanner

Scheduled Classification Scanner enables you to define a scan scope, and then it performs a scheduled or immediate job to scan out the related content according to the scan policy, at last take the specified actions to the scanned content.

Pre-Configurations

Configuring Scan Policies

Scan policies define the compliance rules to be used when scanning the contents in the specified scope. To configure the scan policies, select **Scan Policy** on the ribbon of the Scheduled Classification Scanner page to go to the **Scan Policy** interface.

Managing Scan Policies

For details on how to manage scan policies, refer to Managing Scan Policies in the Real-Time Classification Scanner section of this guide.

Creating and Editing Scan Policies

For details on how to create and edit scan policies, refer to Managing Scan Policies in the Real-Time Classification Scanner section of this guide.

Configuring Filter Policies

For more information, refer to Filter Policy.

Configuring Action Policies for SharePoint

Action policies for SharePoint allow you to define the actions to the scanned contents in the specified SharePoint scope. To configure the action policies, navigate to **Scheduled Classification Scanner** > **Create** > **SharePoint**, under the **SharePoint** tab, and select **Action Policy** on the ribbon to go to the **Action Policy** interface.

Managing Action Policies

For details on how to manage action policies, refer to Managing Action Policies in the Real-Time Classification Scanner section of this guide.

Creating and Editing Action Policies

For details on how to create and edit action policies, refer to Creating and Editing Action Policies in the Real-Time Classification Scanner section of this guide.

Configuring Action Policies for File System

Action policies for File System allow you to define the actions to the scanned contents in the specified file system. To configure the action policies, navigate to **Scheduled Classification Scanner** > **Create** > **File System**. Under the **File System** tab, select **Action Policy** on the ribbon to go to the **Action Policy** interface.

Managing Action Policies

For details on how to manage action policies, refer to Managing Action Policies in the Real-Time Classification Scanner section of this guide.

Creating and Editing Action Policies

To create a new action policy, select **Create** on the ribbon of the **Action Policy** interface. To modify a previously-configured action policy, select the action policy, and then select **Edit** on the ribbon of the **Action Policy** interface.

In the Create Action Policy interface or Edit Action Policy interface, configure the following settings:

- **Name and Description** – Enter a **Name** for the action policy connection. Then enter an optional **Description** for this action policy for future reference.
- **Actions** – Select the **Move to the specified allowed location** checkbox, and then specify whether or not to send an alert:
    - **If the action failed to execute** – Specify whether to send out an alert e-mail when a file failed to be moved to the specified location. If you select the checkbox, you must select an alert e-mail profile from the appeared drop-down list. You can also select the **New Notification Profile** link to create a new notification profile, also you must select an e-mail template from the appeared

drop-down list. You can also select the **New E-mail Template** to create a new e-mail template. For more information, refer to User Notification Settings.

- **If the action successfully executed** – Specify whether to send out an alert e-mail when a file is successfully to be moved to the specified location. If you select the checkbox, you must select an alert e-mail profile from the appeared drop-down list. You can also select the **New Notification Profile** link to create a new notification profile, also you must select an e-mail template from the appeared drop-down list. You can also select the **New E-mail Template** to create a new e-mail template. For more information, refer to User Notification Settings.

Once you select the **Move to the specified location** checkbox, the **Set up the scan action rules** field appears. Configure the following settings under this field:

- Configure a location where the non-compliant files will be moved in the **Move to the specified location** field. Enter a UNC path according to the format: *\\admin-PC\c$\data or \\admin-PC\shared folder*.

  If the path is specified in the format *\\admin-PC\c$\data*:

  - The agent account must have the **local administrator** permission to the server where the specified location resides.

  If the path is specified in the format *\\admin-PC\shared folder*:

  - The specified user must have the **Log on as a batch job** permission to the server where the specified location resides, or the user must be the member of the **Backup Operators** group of the server where the specified location resides.
  - The specified user must have the **Full Control** permission to the shared folder.

- Configure action rules to define the files that will be moved to the allowed location. Refer to the following steps to configure the rules:

  Select a category, select **Add an Action Level Group** to add a new filter rule of the specified category level, and then select the delete button (✕) in the **Delete** field to delete the rule that is no longer needed. Configure the following fields for the rule:

  - **Rule** – Select the new rule you want to create from the drop-down list.
  - **Condition** – Select the condition for the rule.
  - **Value** – Enter a value you want the rule to use in the text box.

  The rule contains two category levels:

  - **Document** – Based on the file property value you specified here to define the scope in which the files that are not compliant will be moved.

- **Classification Result** – Based on the tag value you specified here to define the scope in which the files that are not compliant will be moved. To add more filters, repeat the previous step.

***Note**: Depending on the filters you enter, you can change the order of the rules by selecting the change order button ( ) before the rule value, and then select the order of the rule from the appeared drop-down list to determine the priority of the rule.

You can also change the logical relationships between the rules. There are currently two logical relationships: **And** and **Or**. By default, the logic is set to **And**. To change the logical relationship, select the logical relationship link. The **And** logical relationship means that the content which meets all of the rules will be filtered and included in the result. The **Or** logic means that the content which meets any one of the rules will be filtered and included in the result.

Select **Add an Action Group** to add another action rule. If you add more than one action rule, you can change the order of the action rules by selecting the textbox under **Set up the scan action rules** to determine the priority of the action rule. For example, if you add two action rules and the non-compliant file A fulfills both of the two action rules, then it will be moved to the location specified in the action rule whose priority is 1.

Select the delete button ( ) to delete the action rule. Select the retract button ( ) or the expand button ( ) before the action rule order to retract or expand the action rule.

Configuring Connections for File System

A connection is configured to be used in the Scheduled Classification Scanner File System Mode. Configure a connection with the file system, then the files in the connected file system are supported to be scanned and taken actions in Compliance Guardian.

Navigate to **Scheduled Classification Scanner** > **Create** > **File System**, and select **Configure Connections** on the ribbon to enter the **Configure Connection** interface.

Managing Connections

In the **Configure Connection** interface, you will see a list of previously configured connections. You can customize how these connections are displayed in the following ways:

- **Sort** – Select the header row of each column to sort all of the values in the specified column according to the ascending/descending order.
- **Search** – Filter the connections and display them by the keyword you designate; the keyword must be contained in a column value. At the top right corner of the connection

viewing pane, enter the keyword for the connections you want to display. You can select to **Search all** pages or **Search current page**.

- **Manage columns** (⊞) – Manage which columns are displayed in the list so that only the information you want to see will be shown. Select the manage columns button (⊞), and then check the checkbox next to the column name to have that column shown in the list.
- **Hide the column** (⊖) – Hover over a column name, and then select the hide column button (⊖) in the column name to hide the column.
- To change the number of connections displayed per page, select the desired number from **5**, **8**, **10**, **15** (default value), **20**, **25**, **50**, **100** in the **Show rows** drop-down menu at the lower right corner.
- To go to the specified page, enter the page number in the **Go to … of** text box at the lower right corner and press **Enter**.
- To go to the next page, select the **>** button at the lower right corner; to return to the previous page, select the **<** button at the lower right corner.

In the **Configure Connection** interface, you can create a new connection, view details about a connection, edit a previously configured connection, or delete a previously configured connection. For details on creating or editing a connection, see the Configuring Connections for File System section of this guide.

Select **Edit** on the ribbon to change the configurations for the selected connection. For details on editing configurations for the connection, see the Configuring Connections for File System section of this guide.

To view a connection, select it from the list of previously configured connections, and then select **View Details** on the ribbon. To delete a connection, select it from the list of previously configured connections, and then select **Delete** on the ribbon. A confirmation window will pop up and ask if you are sure you want to proceed with the deletion. Select **OK** to delete the selected connection, or select **Cancel** to return without deleting it.

Creating and Editing Connections

To create a new connection, select **Create** in the **Manage** group of the **Configure Connection** page. To modify a previously configured connection, select the connection, and then select **Edit** on the ribbon. In the Create Connection or Edit Connection interface, configure the following settings:

- **Name and Description** – Enter a name for this connection. You can also enter an optional description to distinguish this connection from the others.
- **Type** – Select the file system type for the connection.
- **Connection** – Configure the following settings:
    - **Agent Group** – Select the agent group that will perform the Scheduled Classification Scanner job.

- **UNC Path** – Specify a path in the format *\\admin-PC\c$\data or \\admin-PC\shared folder*, the files in the specified location are supported to be scanned.
- **Username** – Specify a username that can access the specified location.
- **Password** – Specify a password.

  ***Note:** The user must have the following permissions

  If the path is specified in the format *\\admin-PC\c$\data*:

  - The specified user must have the **local administrator** permission to the connected server.

  If the path is specified in the format *\\admin-PC\shared folder*:

  - The specified user must have the **Log on as a batch job** permission to the connected server, or the user must be the member of the **Backup Operators** group of the connected server.
  - The specified user must have the **Full Control** permission to the shared folder.

After you are satisfied with the configuration of the connection, select **OK** to save this connection. If you do not want to save the current configuration, select **Cancel** to cancel the configuration.

Getting Started

Refer to the sections below for important information on getting started with Scheduled Classification Scanner.

Launching Scheduled Classification Scanner

To launch Scheduled Classification Scanner, complete the following steps:

1. Log in to Compliance Guardian. If you are already in the software, go to the welcome page. From the welcome page, all of the products are displayed.
2. Select the Scheduled Classification Scanner to launch its interface.
3. Alternatively, you can select **Administration** on the top-left corner, and select the **Scheduled Classification Scanner** tab on the appeared navigation bar to Scheduled Classification Scanner.

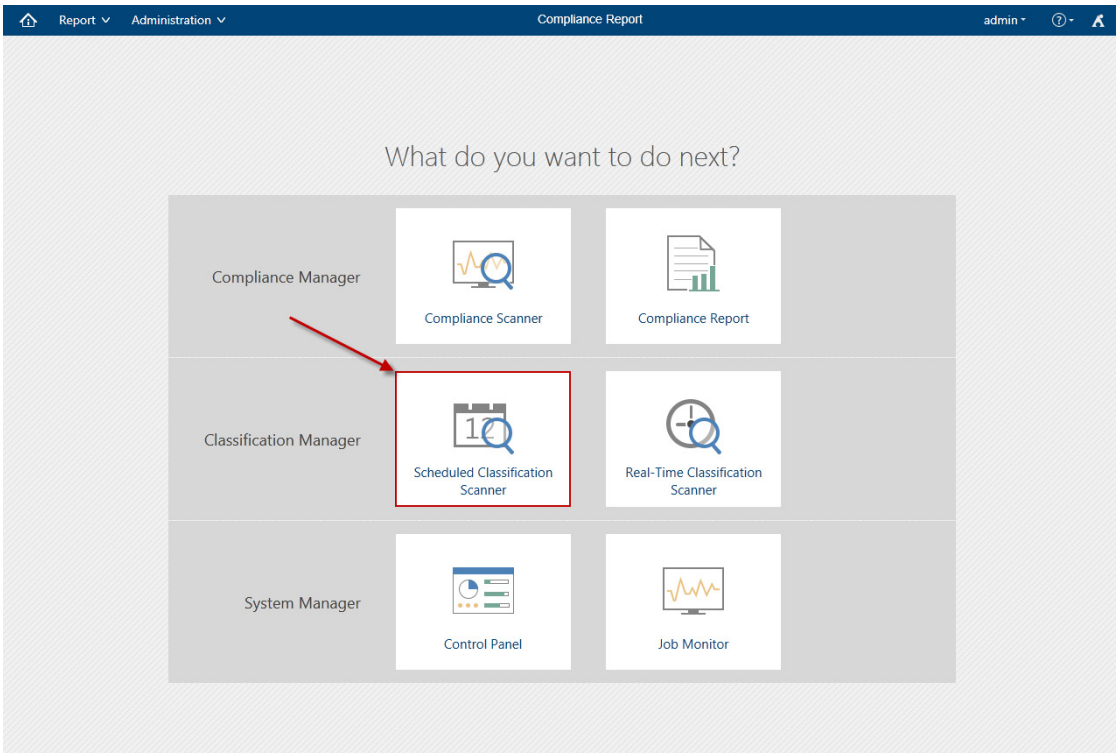

Figure 15: Compliance Guardian module launch window.

Home Page Overview

The Compliance Scanner home page displays a list of all of your previously created Scheduled Classification Scanner plans. Also you can select **Create** to select the Scheduled Classification Scanner Mode: SharePoint or File System, and then create a plan.

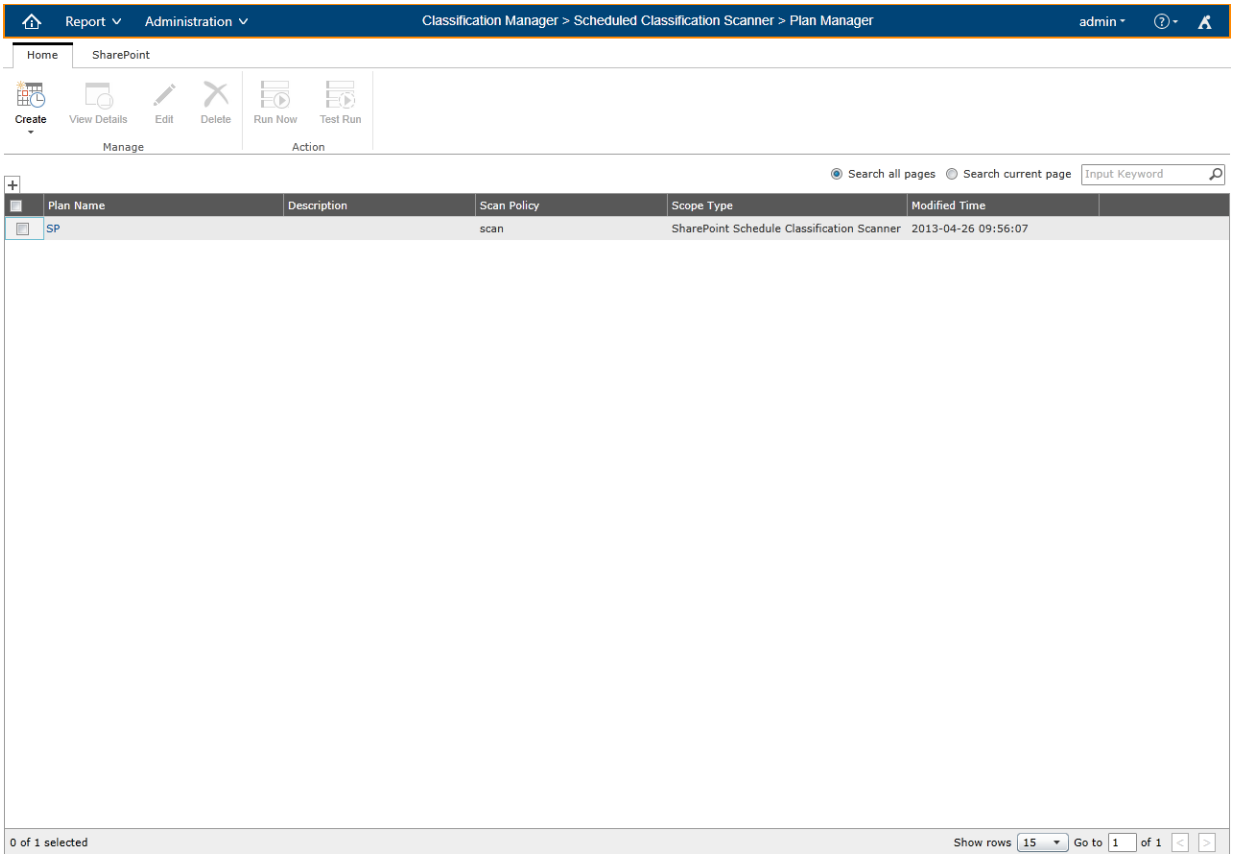

Figure 16: Scheduled Classification Scanner home page.

Selecting Mode

Select **Create** on the ribbon, a drop-down list appears. Select the corresponding mode from the drop-down list: SharePoint or File System. Then you can enter the corresponding mode, and configure a plan to scan objects in SharePoint or file system, and then perform the specified actions to the files in SharePoint or file system.

Managing Scheduled Classification Scanner Plans

The Scheduled Classification Scanner home page displays a list of all of your previously created Scheduled Classification Scanner plans. Also it displays the scan policy and action policy that are selected in the plan. You can also see the plan type in the **Scope Type** column.

You can customize how these plans are displayed in a number of different ways:

- **Search** – Filters the plans displayed by the keyword you designate. The keyword must be contained in a column value. At the top of the viewing pane, type in the keyword for the plan you want to display. You can select to **Search all pages** or **Search current page**.

  ***Note:** The search function is not case sensitive.

- **Manage columns** (⊕) – Manages which columns are displayed in the list so that only the information you want to see is displayed. Select the manage columns button (⊕), and then select the checkbox next to the column name to have that column shown in the list.

- **Hide the column** (⊖) – Hides the column. Select the hide the column button (⊖) of any column you want to hide.

- **Filter the column** ( ) – Filters which item in the list is displayed. You can filter whichever item you want, rather than search based on a keyword. Select the filter the column button ( ) of the column you want to filter, then select the checkbox next to the item name to have that item shown in the list.

You may perform any of the following actions on a selected plan:

- **View Details** – Select **View Details** on the ribbon to see the details of the selected plan. Here you can also select **Edit** on the ribbon to make changes to the plan's settings. You will be brought to the **Edit** page where you can change the settings for this plan. After editing the settings, select **Save** on the ribbon to save the plan. To save a changed plan as a new one, select **Save As** on the ribbon. At any time, select **Cancel** on the ribbon to return to the **Plan Manager** without saving any of your changes.

- **Edit** – Select **Edit** on the ribbon to make changes to the selected plan's settings. You will be brought to the **Edit** page where you can change the settings for this plan. Select **Save** on the ribbon to save the plan. To save a changed plan as a new one, select **Save As** on the ribbon. At any time, select **Cancel** on the ribbon to return to the **Plan Manager** without saving any of your changes.

  ***Note:** If you change the scan policy when editing a Scheduled Classification Scanner plan, or change the database policy when editing a Scheduled Classification Scanner plan, after you save the changes, the next time the plan will mandatorily run a full job although you select to run an incremental job, thus to guarantee that the job can perform correctly, as well as guarantee the job data is generated correctly.

- **Delete** – Select **Delete** on the ribbon to delete the selected plan. A warning message will appear to confirm the deletion. Select **OK** to delete the selected plan, or select **Cancel** to return to **Plan Manager** without deleting the selected plan.

- **Test Run** – Select **Test Run** on the ribbon to simulate the execution of the selected plan. After you select **Test Now**, a pop-up window appears. You can select to run a full job or an incremental job. If **Incremental Scan** is selected, the **Reference Time** option is enabled.

- **Reference Time** – Choose whether to scan contents created or modified at a specified interval. If you choose to use a reference time, specify the time to scan contents created or modified. Enter an integer into the textbox and select **Minute(s)**, **Hour(s)**, **Day(s),** or **Month(s)** from the drop-down list.

  ***Note**: It is recommended that you specify a reference time when the recurrence schedule configured in **Range of Recurrence** is **End after 1 occurrence**.

You can see the review details about the plan's execution in Job Monitor.

- **Run Now** – Select **Run Now** on the ribbon to execute the plan immediately. After you select **Run Now**, a pop-up window appears. You can select to run a full job or an incremental job. If **Incremental Scan** is selected, the **Reference Time** option is enabled.
  - **Reference Time** – Choose whether to scan contents created or modified at a specified interval. If you choose to use a reference time, specify the time to scan contents created or modified. Enter an integer into the textbox and select **Minute(s)**, **Hour(s)**, **Day(s),** or **Month(s)** from the drop-down list.

    ***Note**: It is recommended that you specify a reference time when the recurrence schedule configured in **Range of Recurrence** is **End after 1 occurrence**.

You can see the review details about the plan's execution in Job Monitor.

Scheduled Classification Scanner for SharePoint

The SharePoint Mode allows you to define a scan scope in SharePoint, and then it performs a scheduled or immediate job to scan out the related content according to the scan policy, at last take the specified actions to the scanned content.

Launching Compliance Guardian Scanner SharePoint Mode

On the Scheduled Classification Scanner Home interface, select **Create** on the ribbon, a drop-down list appears. Select **SharePoint** from the drop-down list, then you will be brought to the Scheduled Classification SharePoint Mode.

Performing a Scheduled Classification Scanner Plan in Wizard Mode

To configure a Scheduled Classification Scanner plan using Wizard Mode, complete the following steps:

1. Select the scope of the content you want to scan:
   a. From the **Scope** panel on the left, select the farm that contains the relevant SharePoint content. You can enter a keyword into the **Search** box above the farm tree to filter out the relevant SharePoint content.

a. Select the relevant content from which you want to perform further operations by selecting the checkboxes to the left of the content.

2. Select **Plan Builder** from the **Plan Management** group on the ribbon, select **Wizard Mode** from the drop-down menu. Or you can directly select **Start with Wizard Mode** on the landing page.
3. Enter a **Plan Name** for the plan and an optional **Description**.
4. Select **Next** on the ribbon or on the lower-right section of the screen. The **Report Settings** screen appears, select a **Report Database** for storing the job result.
5. Select **Next** on the ribbon or on the lower-right section of the screen. The **Scan Settings** screen appears.
6. Configure the following scan settings:
   - **Action Policy** – Select an action policy from the drop-down list or create a new action policy to define the actions to the content that will be scanned out. For more information on working with action policies, refer to Managing Action Policies.
   - **Scan Policy** – Select a scan policy from the drop-down list or create a new scan policy to define the scan rules for scanning content. For more information on working with scan policies, refer to Configuring Scan Policies.
   - **Scan File/Item Versions** – Specify the method for scanning file/item versions:
     - **Scan the current version** – Only the current versions of the files/items defined in the job scope are supported to be scanned. The files/items that are not compliant will be treated according to actions defined in the action policy.
     - **Scan all versions** – The files/items and all their previous versions defined in the job scope are supported to be scanned. If the current version of a scanned file/item or one of its previous versions is not compliant, the entire file/item (the current version of the file/item along with its previous versions) will be treated according to actions defined in the action policy.
   - **Alert** – Specify whether to send out an alert e-mail when an error occurs during the process of scanning a file or when a tag fails to be added to a file. If you choose to send out alert e-mails when an error occurs, configure the recipients by selecting the corresponding checkboxes in the **Send e-mail to** field:
     - **Creator** – Select this checkbox to send an alert e-mail to the creator of the specified file.
     - **Modifier** – Select this checkbox to send an alert e-mail to the last modifier of the specified file.
     - **User who is specified in the following notification file** – Select this checkbox to send an alert e-mail to the recipients configured in the selected alert notification profile. If this option is selected, you must select an alert notification profile from the appeared drop-down list. You can also select the New Notification Profile link to create a new notification profile. For more information, refer to User Notification Settings.

***Note:** Even though there may be more than one error when scanning a file, the alert e-mail will only be sent when the first error occurs.

After configuring the recipients, choose one e-mail template from the E-mail template drop-down list. You can also select the New E-mail template link to create a new e-mail template. For more information, refer to Configuring E-mail Templates.

- **Filter Policy** – Select a filter policy from the drop-down list or create a new policy to limit the scope of the job. For more information on working with filter policies, refer to Filter Policy.

7. Select **Next** on the ribbon or on the lower-right section of the screen. The **Schedule** screen appears.
8. Select a scheduling option:
    - **No schedule** – Select this option to configure the job to not run on a schedule (the job must be manually initiated).
    - **Configure the schedule myself** – Configure a customized schedule, and run the plan by schedule.

      Select **Add Schedule** and the **Add Schedule** window pops up. Configure the following settings for the schedule:

      - **Options** – Select the type of the scan for this plan: **Full Scan** or **Incremental Scan**. Full Scan scans all of the content in the scope defined in the plan, while Incremental Scan only scans the content that has been modified since the last incremental or full scan job.

        If selecting **Incremental Scan**, the **Reference Time** option is enabled.

        - **Reference Time** – Choose whether to scan contents created or modified at a specified interval. If you choose to use a reference time, specify the time to scan contents created or modified. Enter an integer into the textbox and select **Minute(s)**, **Hour(s)**, or **Day(s)** from the drop-down list.

          ***Note**: It is recommended specifying a reference time when the recurrence schedule configured in **Range of Recurrence** is **End after 1 occurrence**.

      - **Schedule Settings** – Specify the frequency to run the rerunning schedule. Enter an integer into the text box and select **Minute(s)**, **Hour(s)**, **Day(s)**, **Week(s)**, or **Month(s)** from the drop-down list.
      - **Range of Recurrence** – Specify when to start and end the running recurring schedule.
        - **Start time** – Set up the time to start the plan and Time Zone can be changed under the Start time. Note that the start time cannot be earlier than the current time.

- **No end date** – Select this option to repeat running the plan until being stopped manually.
- **End after specified occurrence(s)** – Select this option to stop the plan after specified occurrences that you configure in the text box.
- **End by** – Set up the time to end the recurrence of plans.

Select **OK** to save the settings. After configuring the schedule for this replication job, select **Calendar View** to view the job in a calendar view.

9. Select **Next** on the ribbon or on the lower-right section of the screen. The **Advanced** screen appears.
10. Configure the following advanced settings:
    - **Agent Group** – Select the agent group for the Scheduled Classification Scan Plan. For more information on working with agent groups, refer to Agent Groups.
    - **Notification** – Allow you to choose the type of notification report, and designate which user will receive an e-mail notification report. Select a Notification Profile you previously created from the drop-down menu. Select **View** beside the drop-down menu to view details of the Notification Profile or select **New Notification Profile** from the drop-down menu. For information on creating a notification profile, refer to User Notification Settings.
11. Select **Next** on the ribbon or on the lower-right section of the screen. The Overview screen appears.
12. Review and edit the plan selections on the Overview screen. To make changes, select **(Edit)**. This link takes you to the corresponding setting page, and allows you to edit the configuration.
13. Select **Finish or Finish and Run Now** on ribbon or on the lower-right section of the screen. The plan is now listed in Plan Manager.

    If you select **Finish and Run Now**, the **Run Now** interface pops up to allow you to choose **Options**:

    - **Full Scan** – Scans all of the content in the scope defined in the plan.
    - **Incremental Scan** – Scans the content that has been modified (**Add**, **Delete**, and **Modify**) since the last incremental or full scan job. If selecting **Incremental Scan**, the **Reference Time** option is enabled.
        - **Reference Time** – Choose whether to replicate contents created or modified at a specified interval. If you choose to use a reference time, specify the time to replicate contents created or modified. Enter an integer into the text box and select **Minute(s)**, **Hour(s)**, or **Day(s)** from the drop-down list.

    ***Note:** The default maximum storage time of a SharePoint change log is 60 days. If the reference time you configure is greater than 60 days, Compliance Guardian only runs an incremental scan for the modifications within 60 days. For the modifications exceed 60 days, Compliance Guardian runs full replication.

Select **OK** to run the job.

Performing a Scheduled Classification Scanner Plan in Form Mode

Form Mode offers the ability to run a quick scan job by providing a truncated version of all of the Scheduled Classification Scan Plan Wizard screens on one page. Select the Scope of the content you want to scan, select **Plan Builder** from the **Plan Management** group on the ribbon, and then select **Form Mode** from the drop-down menu. Or, you can directly select **Start with Form Mode** on the landing page. For detailed information about how to configure the Scheduled Classification Scan Plan settings, refer to Performing a Scheduled Classification Scanner Plan in Wizard Mode.

***Note:** If you are unfamiliar with this plan creation process, it is not recommended that you use this mode to configure settings.

Scheduled Classification Scanner for File System

The File System Mode allows you to configure connection with a location, and then perform a scheduled or immediate job to scan out the related content according to the scan policy, at last take the specified actions to the scanned content in the location.

Launching Compliance Guardian Scanner File System Mode

On the Scheduled Classification Scanner Home interface, select **Create** on the ribbon, a drop-down list appears. Select **File System** from the drop-down list, then you will be brought to the Scheduled Classification File System Mode.

Performing a Scheduled Classification Scanner Plan in Wizard Mode

To configure a Scheduled Classification Scanner plan using Wizard Mode, complete the following steps:

1. From the **Scope** panel on the left, select one or more connections. You can enter a keyword into the **Search** box above the connections to filter out the relevant connections.
2. Select **Plan Builder** from the **Plan Management** group on the ribbon, select **Wizard Mode** from the drop-down menu. Or you can directly select **Start with Wizard Mode** on the landing page.
3. Enter a **Plan Name** for the plan and an optional **Description**.
4. Select **Next** on the ribbon or on the lower-right section of the screen. The **Report Settings** screen appears. Select a **Report Database** for storing the job result.
5. Select Next on the ribbon or on the lower-right section of the screen. The **Scan Settings** screen appears.

6. Configure the following scan settings:

    - **Filter Policy** – Select a filter policy from the drop-down list or create a new policy to limit the scope of the job. For more information on working with filter policies, refer to Filter Policy.
    - **Scan Policy** – Select a scan policy from the drop-down list or create a new scan policy to define the scan rules for scanning content. For more information on working with scan policies, refer to Configuring Scan Policies.
    - **Scan Hidden Files Option** – Select whether or not to scan the hidden files in the specified file system.
    - **Alert** – If you want Compliance Guardian to send an e-mail when an error occurs during the file scan, then select an e-mail profile to specify the users who will receive the e-mail. And then select an e-mail template. You can also select the **New E-mail Template** link to create a new e-mail template. For more information, refer to the Configuring E-mail Templates section in this user guide.

      ***Note:** Even though there may be more than one error when scanning a file, the alert e-mail will only be sent when the first error occurs.

    - **Action Policy** – Select an action policy from the drop-down list or create a new action policy to define the actions to the content that will be scanned out. For more information on working with action policies, refer to Managing Action Policies.

7. Select **Next** on the ribbon or on the lower-right section of the screen. The **Schedule** screen appears.

8. Select a scheduling option:

    - **No schedule** – Select this option to configure the job to not run on a schedule (the job must be manually initiated).
    - **Configure the schedule myself** – Configure a customized schedule, and run the plan by schedule.

      Select **Add Schedule** and the **Add Schedule** window pops up. Configure the following settings for the schedule:

        - **Options** – Select the type of the scan for this plan: **Full Scan** or **Incremental Scan**. Full Scan scans all of the content in the scope defined in the plan, while Incremental Scan only scans the content that has been modified since the last incremental or full scan job.

          If selecting **Incremental Scan**, the **Reference Time** option is enabled.

            - **Reference Time** – Choose whether to scan contents created or modified at a specified interval. If you choose to use a reference time, specify the time to scan contents created or modified. Enter an integer into the textbox and select **Minute(s)**, **Hour(s)**, or **Day(s)** from the drop-down list.

***Note**: It is recommended specifying a reference time when the recurrence schedule configured in **Range of Recurrence** is **End after 1 occurrence**.

- **Schedule Settings** – Specify the frequency to run the rerunning schedule. Enter an integer into the text box and select **Minute(s)**, **Hour(s)**, **Day(s)**, **Week(s)**, or **Month(s)** from the drop-down list.
- **Range of Recurrence** – Specify when to start and end the running recurring schedule.
  - **Start time** – Set up the time to start the plan and Time Zone can be changed under the Start time. Note that the start time cannot be earlier than the current time.
  - **No end date** – Select this option to repeat running the plan until being stopped manually.
  - **End after specified occurrence(s)** – Select this option to stop the plan after specified occurrences that you configure in the text box.
  - **End by** – Set up the time to end the recurrence of plans.

Select **OK** to save the settings. After configuring the schedule for this replication job, select **Calendar View** to view the job in a calendar view.

9. Select **Next** on the ribbon or on the lower-right section of the screen. The **Advanced** screen appears.
10. Configure the following advanced settings:
    - **Notification** – Allow you to choose the type of notification report, and designate which user will receive an e-mail notification report. Select a Notification Profile you previously created from the drop-down menu. Select **View** beside the drop-down menu to view details of the Notification Profile or select **New Notification Profile** from the drop-down menu. For information on creating a notification profile, refer to User Notification Settings.
11. Select **Next** on the ribbon or on the lower-right section of the screen. The Overview screen appears.
12. Review and edit the plan selections on the Overview screen. To make changes, select **(Edit)**. This link takes you to the corresponding setting page, and allows you to edit the configuration.
13. Select **Finish or Finish and Run Now** on ribbon or on the lower-right section of the screen. The plan is now listed in Plan Manager.

    If you select **Finish and Run Now**, the **Run Now** interface pops up to allow you to choose **Options**:

    - **Full Scan** – Scans all of the content in the scope defined in the plan.

- **Incremental Scan** – Scans the content that has been modified (**Add**, **Delete**, and **Modify**) since the last incremental or full scan job. If selecting **Incremental Scan**, the **Reference Time** option is enabled.
    - **Reference Time** – Choose whether to replicate contents created or modified at a specified interval. If you choose to use a reference time, specify the time to replicate contents created or modified. Enter an integer into the text box and select **Minute(s)**, **Hour(s)**, or **Day(s)** from the drop-down list.

***Note:** The default maximum storage time of a SharePoint change log is 60 days. If the reference time you configure is greater than 60 days, Compliance Guardian only runs an incremental scan for the modifications within 60 days. For the modifications exceed 60 days, Compliance Guardian runs full replication.

Select **OK** to run the job.

Performing a Scheduled Classification Scanner Plan in Form Mode

Form Mode offers the ability to run a quick scan job by providing a truncated version of all of the Scheduled Classification Scan Plan Wizard screens on one page. Select the Scope of the content you want to scan, select **Plan Builder** from the **Plan Management** group on the ribbon, and then select **Form Mode** from the drop-down menu. Or, you can directly select **Start with Form Mode** on the landing page. For detailed information about how to configure the Scheduled Classification Scan Plan settings, refer to Performing a Scheduled Classification Scanner Plan in Wizard Mode.

***Note:** If you are unfamiliar with this plan creation process, it is not recommended that you use this mode to configure settings.

Using Compliance Guardian Features in SharePoint

Compliance Guardian provides two features in SharePoint: **Compliance Guardian Tag Assist Manager** feature and **Compliance Guardian Quarantine Manager** feature. Refer to the following sections for details about the two features.

Using Compliance Guardian Tag Assist Manager in SharePoint

Compliance Guardian Tag Assist Manager is used in combination with the **For Compliance Guardian Tag Assist Manager only** option in Real-Time Classification Scanner. It allows you to manually scan the file in the specified scope defined in Compliance Guardian and view the scanned results, or you can directly modify the tag values for the scanned file without modifying the checks. Ensure that the CCS.AssistManager.wsp is deployed before using this feature. For more information on deploying the solution, refer to Solution Manager.

***Note:** This feature is supported in both SharePoint 2007 and SharePoint 2010.

Refer to the following steps to use Compliance Guardian Tag Assist Manager in SharePoint 2007:

1. Navigate to the corresponding SharePoint site (where the content you want to scan is) > **Site Settings** > **Site features**, and activate the **Compliance Guardian Tag Assist Manager** feature. ***Note:** At a minimum, to use the **Compliance Guardian Tag Assist Manager** feature in a site, the user must have the following required six site permissions assigned:

    - Manage Lists
    - Edit Items
    - View Items
    - View Application Pages
    - View Pages
    - Open

2. Navigate to the corresponding document library. Select the down arrow button ( ) before the file you want to scan, and select **Compliance Guardian Tag Assist Manager** from the appeared drop-down list. The Compliance Guardian Tag Assist Manager interface appears. There are three columns in the table of this interface:

    - **Tag Name** – Display the tag names defined in the corresponding checks. The values in this column cannot be changed.
    - **Original Value** – Display the tag values that are added for the file in the last scan. If you have not added any tag values in the last scan, there will be no value in this column.
    - **Current Value** – Display the file's current tag value based on the checks. The current values can be modified according to your own requirements.

    You can select to check the checkbox to the right of the tag value to determine which tag (include the tag name and tag value) can be added to this file. Selecting the checkbox after the **Current Value** column will select all of the tags.

3. Select **OK** or **Cancel**, and the Compliance Guardian Tag Assist Manager window will be closed.

    - If you select **OK**, the current tags will be added in the locations that are defined in the corresponding checks. There are three locations where the tags will be:
        - In SharePoint – The single line of text column named Tag Name will be added for the file in SharePoint, the tag values will be added in this column; If a single line of text column named Tag Name already exists in SharePoint, then the tag values will be added in this column; If a column named Tag Name already exists in SharePoint, but it is not a single line of text column, then a single line of text column named Tag Name will also be created in SharePoint for displaying the tag values.
        - In the file – The tags will be added in the file.

- In both the Tag Name column and the file – The tags will be added in both the file and SharePoint.

  ***Note**: Tags can only be added into the following file types: DOCX, XLSX, PPTX, HTM, HTML, PDF, and ASPX.

  If you define to add tags in the file in the check, but the file type is not one of the above file types, select **OK**, and the tags will not be added.

- If you select **Cancel**, the current tag names and tag values will not be added.

***Note**: If you do not have the **Manage Lists** or **Edit Items** permission to the corresponding site, you can only view the scanned results, the **OK** button will be greyed out.

Refer to the following steps to use Compliance Guardian Tag Assist Manager in SharePoint 2010:

1. Navigate to the corresponding SharePoint site (where the content you want to scan is) > **Site Settings** > **Site features** and activate the **Compliance Guardian Tag Assist Manager** feature.

   ***Note:** At a minimum, to use the **Compliance Guardian Tag Assist Manager** feature in a site, the user must have the following required six site permissions assigned:

   - Manage Lists
   - Edit Items
   - View Items
   - View Application Pages
   - View Pages
   - Open

2. Select the corresponding document library in Quick Launch Bar, and then select the **Documents** tab. The button **Compliance Guardian Tag Assist Manager** appears in the **Compliance Guardian Tool** group on the ribbon.

3. Check the checkbox in front of the file that you want to scan. Select **Compliance Guardian Tag Assist Manager** on the ribbon.

   The **Compliance Guardian Tag Assist Manager** window pops up, and the message **Please wait while the page is loading…** appears. After the file is finished scanning, the scan results will appear in this window.

   There are three columns in the table of this window:

   - **Tag Name** – Display the tag names defined in the corresponding checks. The values in this column cannot be changed.
   - **Original Value** – Display the tag values that are added for the file in the last scan. If you have not added any tag values in the last scan, there will be no value in this column.

- **Current Value** – Display the file's current tag value based on the checks. The current values can be modified according to your own requirements.

You can select to check the checkbox to the right of the tag value to determine which tag (include the tag name and tag value) can be added to this file. Selecting the checkbox after the **Current Value** column will select all of the tags.

Select **OK** or **Cancel**, and the Compliance Guardian Tag Assist Manager window will be closed.

- If you select **OK**, the current tags will be added in the locations that are defined in the corresponding checks. There are three locations where the tags will be:
  - In SharePoint – If a Managed Metadata type/Choice type/Single line of text type column named Tag Name exists in SharePoint, the tag value will be added into this column (if the three kinds of columns all exist in SharePoint, and the name is Tag Name, the priority of the column being added tag is Metadata type column, Choice type column and then single line of text type column). If there is no column (Managed Metadata type/Choice type/single line of text type column) named Tag Name in SharePoint, a single line of text type column named Tag Name will be created for adding the tag value.
  - In the file – The tags will be added in the file.
  - In both the Tag Name column and the file – The tags will be added in both the file and SharePoint.

    ***Note:** Tags can only be added into the following file types: DOCX, XLSX, PPTX, HTM, HTML, PDF, and ASPX. If you define to add tags in the file in the check, but the file type is not one of the above file types, select **OK**, the tags will not be added.

- If you select **Cancel**, the current tag names and tag values will not be added.

***Note**: If you do not have the **Manage Lists** or **Edit Items** permission to the corresponding site, you can only view the scanned results, the **OK** button will be greyed out.

Using Compliance Guardian Quarantine Manager in SharePoint

Compliance Guardian Quarantine Manager allows you to manage the quarantined files. Ensure that CCS.QuarantineManager.wsp is deployed before using this feature. For more information on deploying the solution, refer to Solution Manager. This feature is supported in both SharePoint 2007 and SharePoint 2010.

To use this feature in SharePoint 2007, complete the following steps:

1. Navigate to the corresponding SharePoint site > **Site Settings** > **Site features**, activate the **Compliance Guardian Quarantine Manager** feature.

***Note:** At a minimum, to use the **Compliance Guardian Tag Assist Manager** feature in a site, the user must have the following required seven site permissions assigned:

- Manage Lists
- Edit Items
- View Items
- View Application Pages
- View Pages
- Open
- Browse User Information

2. Return to the **Site Settings**, and then select **Compliance Guardian Quarantine Manager** in the **Compliance Guardian Tools and Services** group. You will be brought to the **Compliance Guardian Quarantine Manager** interface.
3. In the **Compliance Guardian Quarantine Manager** interface, select **Quarantine Manager** tab, you will see the following areas:
    - **Tool Field** – Use the Tool Field to manage the quarantined files. You can download the files' details, restore the files or delete the files in bulk through the corresponding buttons in this field.
        - **View Content** – View the file's content in the webpage.
        - **View Properties** – View the file's properties.
        - **Download Details** – Download the selected files.
        - **Restore** – Restore the quarantined files from the site collection Recycle Bin to the original locations of the files.
        - **Delete** – Delete the quarantined files permanently.
    - **Scope** – Define the scope of the files you want to manage.
    - **Files Field** – View the files in the selected nodes.
    - **File Details** – Display a file's detailed information.

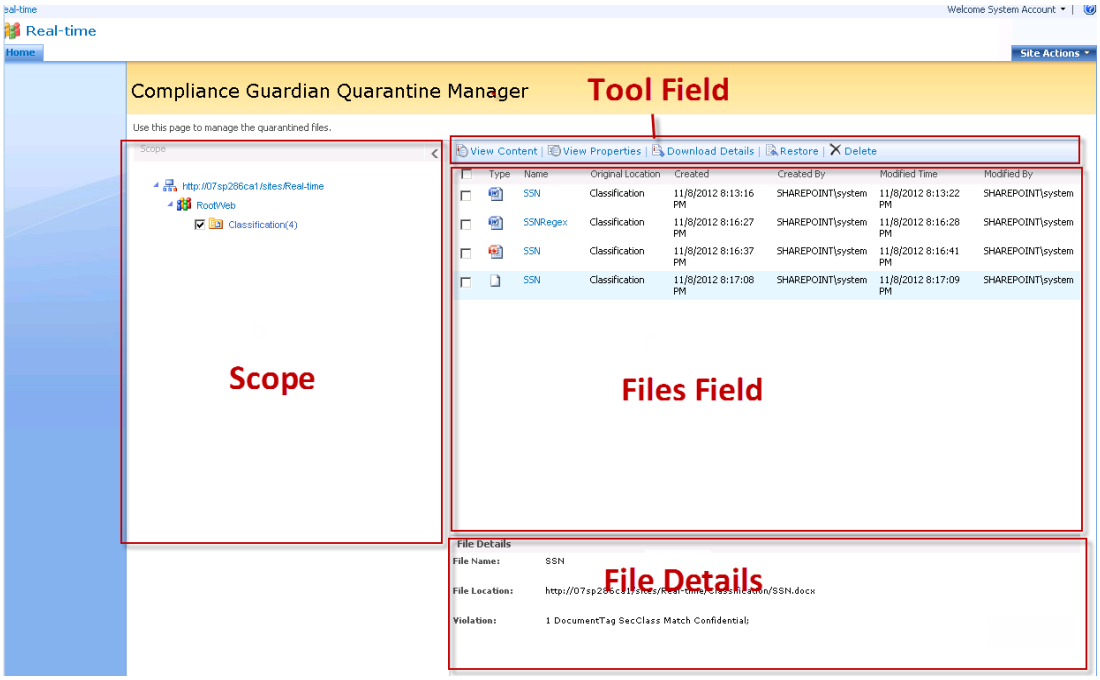

Figure 17: SharePoint 2010 Compliance Guardian Quarantine Manager Interface.

4. Refer to the following steps to manage the quarantined files:
    a. In the scope area of the screen, select the site collection to expand to the node in which the files you want to manage are.
    b. Select the node, and you will see all of the files listed in the **Files** field to the right of the **Scope** field.
    c. Select the specific files by checking the checkbox in front of the file in the Files field. The file details will display in the **File Details** field.

    ***Note:** In the **File Details** field, only one file's details can be displayed. If you select several files, only the last selected file's details can display in the screen. If you want to view all of the selected files' detailed information, you must download the details to a CSV file using **Download Details**.

    d. Select the checkbox next to the file you want to manage. Select next to the file name, and a drop-down list appears. You can choose how to manage the file by selecting the corresponding action (View Content, View Properties, Download Details, Restore and Delete).

To use this feature in SharePoint 2010, complete the following steps:

1. Navigate to the corresponding SharePoint site collection > Site Settings > Manage site features, and activate the Compliance Guardian Quarantine Manager feature.

***Note:** At a minimum, to use the **Compliance Guardian Tag Assist Manager** feature in a site, the user must have the following required seven site permissions assigned:

- Manage Lists
- Edit Items
- View Items
- View Application Pages
- View Pages
- Open
- Browse User Information

2. Return to the Site Settings, and then select **Compliance Guardian Quarantine Manager** in the **Compliance Guardian Tools and Services** group. You will be brought to the Compliance Guardian Quarantine Manager interface.
3. In the Compliance Guardian Quarantine Manager interface, select **Quarantine Manager** tab, you will see the following areas:
   - **Tabs** – Switch between the **Browse** tab, and the **Quarantine Manager** tab.
   - **Ribbon** – Use the ribbon to manage the quarantined files. You can download the files' details, restore the files or delete the files in bulk through the ribbon.
     - **View Content** – View the file's content in the Web page.
     - **View Properties** – View the file's properties.
     - **Download Details** – Download the selected files.
     - **Restore** – Restore the quarantined files from the Site Collection Recycle Bin to the original locations of the files.
     - **Delete** – Delete the quarantined files permanently.
   - **Scope** – Define the scope of the files you want to manage.
   - **Files Field** – View the files in the selected nodes.
   - **File Details** – Display a file's detailed information.

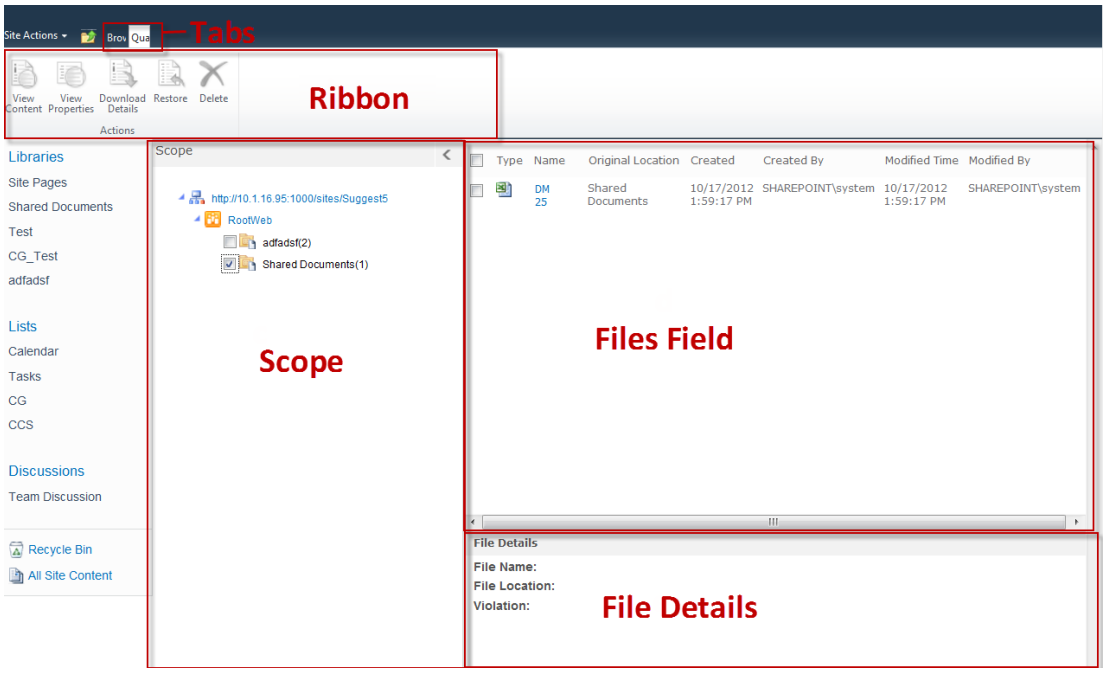

Figure 18: SharePoint 2010 Compliance Guardian Quarantine Manager Interface.

4. To manage the quarantined files, complete the following steps:

   a. In the scope field of the screen, select the site collection to expand to the node in which the files you want to manage are.

   b. Select the node, and then you will see all of the files will list in the **Files** field to the right of the **Scope** field.

   c. Select the specific files by checking the checkbox in front of the file in the **Files** field. The file details will display in the **File Details** field.

      ***Note:** The **File Details** field can only display information on one file at a time. If you select several files, only the last selected file's details can display on the screen. If you want to view details on all of the selected files, you must download the details to a CSV file using **Download Details**.

   d. Select the checkbox before the file you want to manage, select ▾ next to the file name, a drop-down list appears, and then you can select how to manage the file by selecting the corresponding action (View Content, View Properties, Download Details, Restore, and Delete).

Job Monitor

Job Monitor allows you to view the status or details of jobs, download reports, and manage the jobs all from a central interface.

Job Monitor is also integrated into other Compliance Guardian products, which enables you to manage the jobs inside its corresponding modules with additional features specific to the product itself. These additional features are also available in the stand-alone Job Monitor module.

Getting Started

Refer to the following sections for important information on getting started with Job Monitor.

Launching Job Monitor

To launch Job Monitor and access its functionality, complete the following steps:

1. Log in to Compliance Guardian. If you are already in the software, select the home page button ( ) on the left corner to go the home page.
2. From the home page, select **Job Monitor** to launch the module.

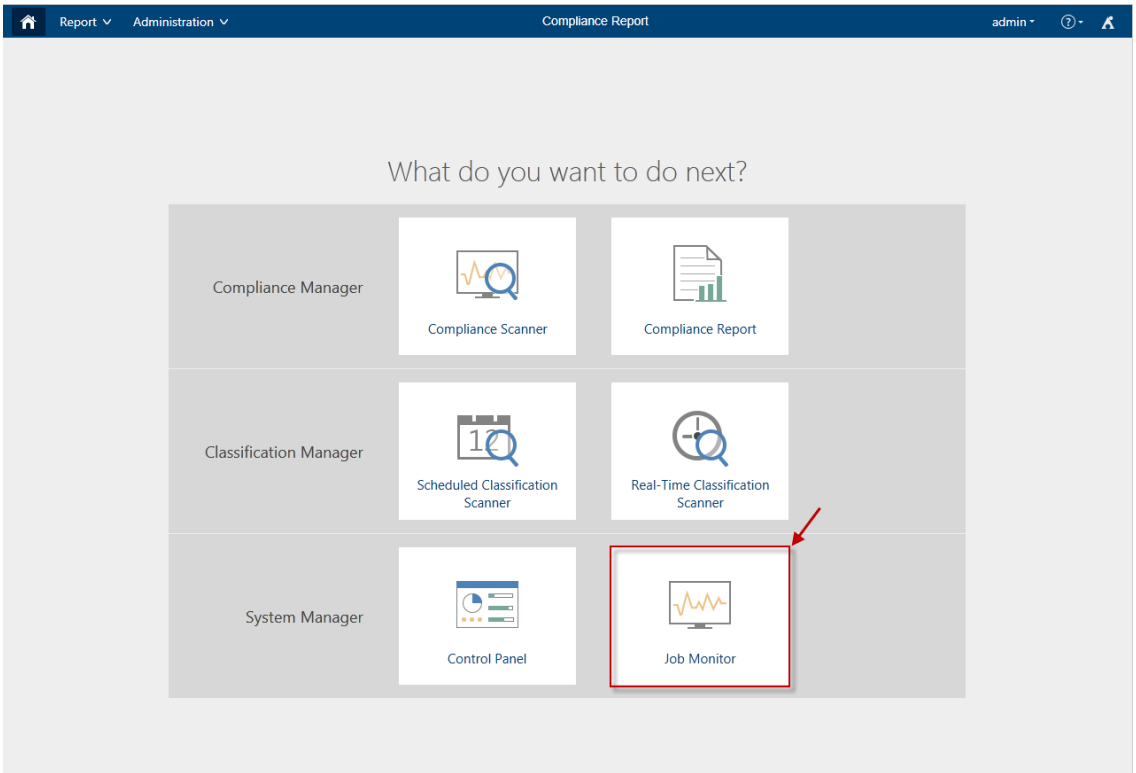

Figure 19: Compliance Guardian module launch window.

3. Alternatively, you can select **Administration** on the top-left corner, and select the **Job Monitor** tab on the appeared navigation bar to launch Control Panel.

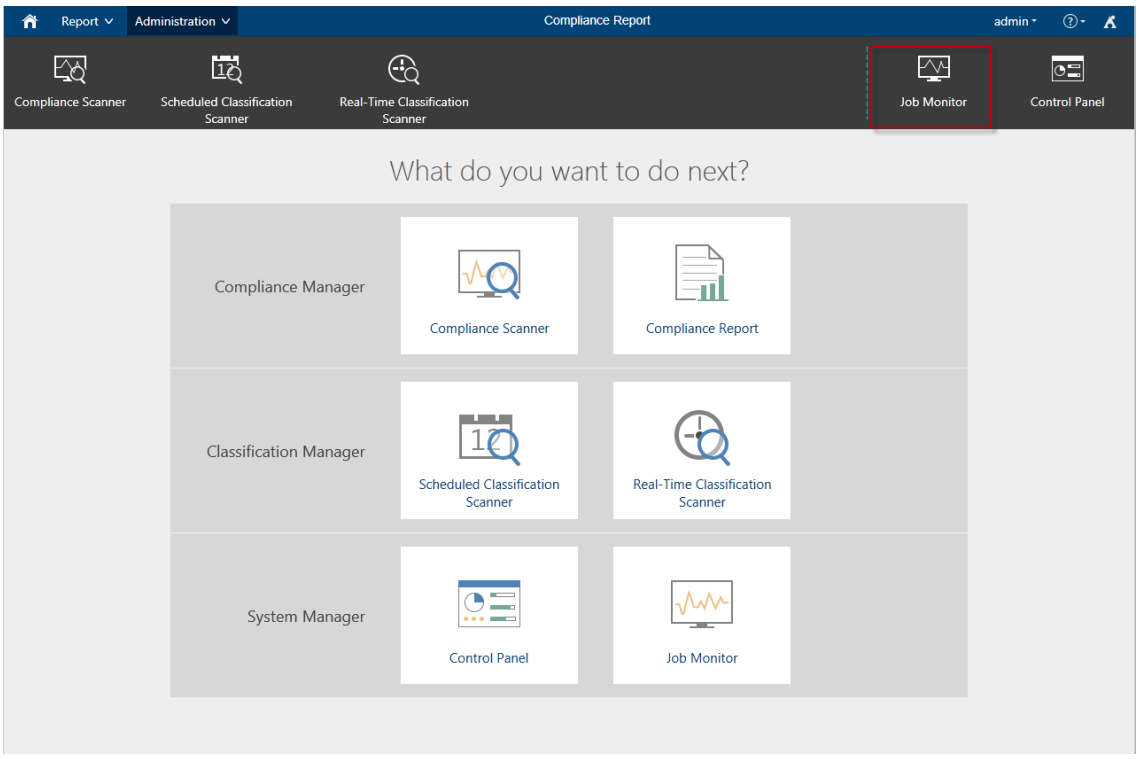

Figure 20: Job Monitor tab on the navigation bar.

Understanding Job Monitor

Job Monitor allows you to customize the way your jobs are displayed so you can more efficiently manage them. The following two sections will cover the different viewing options.

Job Monitor Interface

The interface in Job Monitor contains the following four areas:

1. **Tabs** – Switch between the Job Monitor and Scheduled Job Monitor interface.
2. **Ribbon** – Toolbar where you can customize the view, perform actions on selected jobs, and configure report location settings.
3. **Search** – Search tool for filtering the displayed jobs.
4. **Viewing pane** – List of jobs displayed according to the filters you configure.

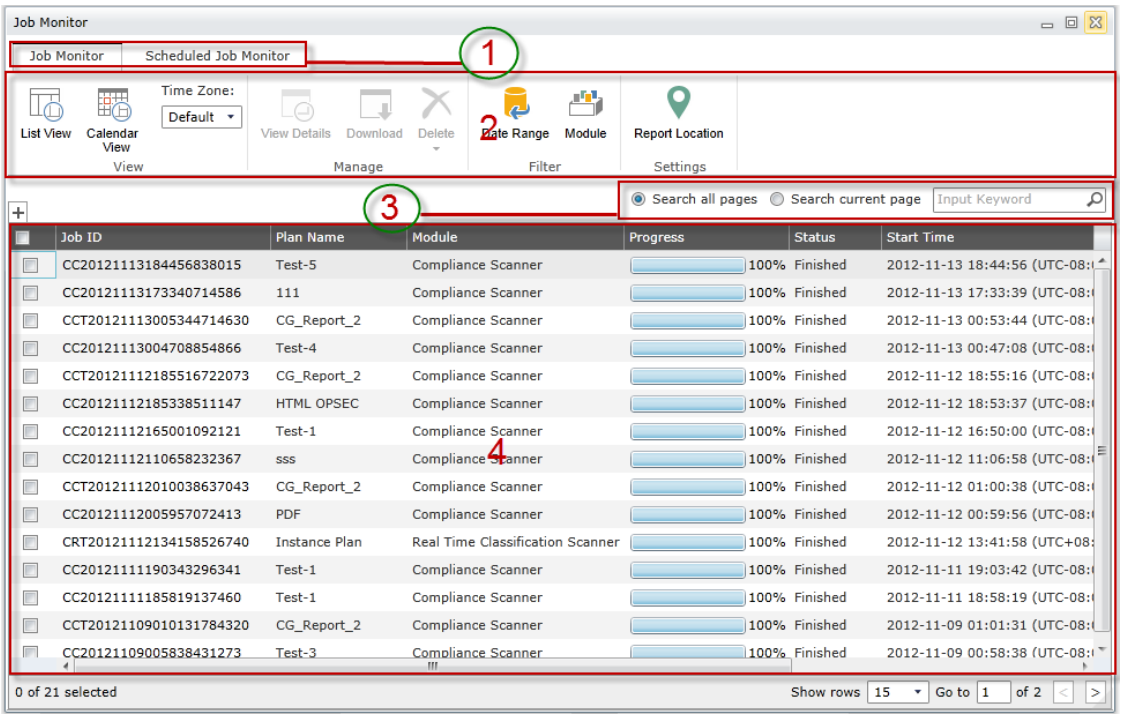

Figure 21: Job Monitor user interface.

Job Monitor vs. Scheduled Job Monitor

The Job Monitor module interface contains two tabs:

- **Job Monitor** – Allows you to access all of the current and previous jobs.
- **Scheduled Job Monitor** – Allows you to exclusively access jobs that are scheduled to run in the future.

***Note:** Differentiate between scheduled jobs (jobs scheduled to run in the future) and recurring jobs. Scheduled jobs will only show up on the Scheduled Job Monitor tab. Recurring jobs will show up on both tabs.

Configuring the Viewing Pane

In both the Job Monitor and Scheduled Job Monitor tabs, there is a View toolbar and a Filter toolbar on the ribbon with further configurable options to help you more efficiently manage your current and previous jobs.

The View Toolbar

This toolbar allows you to choose to have your jobs displayed in List View or Calendar View:

- **List View** – Displays your jobs in a table. You can add or remove a column to customize your view by selecting the manage columns button (+). Select the desired column for

this view by checking the checkbox next to its name in the drop-down menu. Select **OK** to save your choices, or select **Cancel** to close the drop-down menu without saving your choices.

- **Calendar View** – Displays your jobs in a calendar. You can configure Calendar View to display in **Day**, **Week**, or **Month** format by selecting the respective button in the upper right-hand corner. To see detailed information about a job, place your mouse cursor over its time slot.

You can also configure the Time Zone in this toolbar by specifying one of the options below to display in the job information.

- **Default** – Displays the time zone of the machine where the control service is installed. In the Scheduled Job Monitor tab, the default time zone is based on the time zone configured for each schedule.
- **Local** – Displays the time zone that the Internet Explorer (IE) browser used to access Compliance Guardian.

By default, the time zone of the job information is set to **Default**.

***Note:** In Calendar View, the time zone is set to Local and cannot be altered. To change the time zone, select the drop-down menu, and select **Local.**

The Filter Toolbar

This toolbar allows you to filter the jobs listed in the viewing pane by Date Range or Module.

- **Date Range** – Allows you to limit the jobs displayed by specifying a time frame.
- **Module** – Allows you to limit the jobs displayed by specifying the module where the jobs are run.

Searching Jobs

Job Monitor also allows you to search for jobs to further customize which jobs are displayed to you. The search interface is located under the toolbar ribbon. Select the corresponding radio button to either **Search all pages** or **Search current page**. Placing your cursor over the Search text box will bring up a tooltip informing you of the searchable parameters.

***Note:** The search function is not case sensitive.

Since the Job ID includes the start time for the job, you can search for a job by start time. Enter the time as a numerical string in the text box, then select the magnifying glass ( ) (for example, search for 2011-01-01 17:05:10 by typing 20110101170510 in the search text box).

Managing Jobs

The Job Monitor tab and the Scheduled Job Monitor tab offer different sets of tools more suitable for managing the different types of jobs.

***Note:** If one tool is not supported for the selected job of the specified product, the corresponding button of this tool will be greyed out and not available to select.

Operations in the Job Monitor Tab

The Job Monitor tab provides you with a number of tools that allow you to perform actions to jobs you are currently running or have run in the past.

The Manage Toolbar

This toolbar provides you with the following functionality:

- **View Details** – Allows you to view a job report of the selected job. Select the job by checking the corresponding checkbox. Select **View Details** on the ribbon. The Job Details tab appears with the job report displayed in the viewing pane with the Summary tab selected. The Summary tab displays general information about the job. For more in-depth information, select the **Details** tab in the viewing pane. Select **Download** to download the job report. Select **TXT**, **CSV**, or **XLS** as the format for the report, then select to download the **Current columns** or **All columns** from the Details tab, and then select **OK** to download the report, or **Cancel** to return to the Job Details tab.
- **Delete** – Deletes job information without sending a notification to anyone. Select the checkboxes before the jobs, and then select **Delete**. A confirmation pop-up window will appear to confirm the operation. Select **OK** to delete the selected jobs, or select **Cancel** to return to the interface without deleting the jobs.
- **Download** – Allows you to download the job report of the selected jobs to a specified location. You have the option to set the **Report Format** to download in TXT, CSV, or XLS format. Here you can only choose to download **All columns** from the Details tab.

  ***Note**: Prior to downloading the job report, make sure the Internet Explorer (IE) download settings are configured properly.

You can configure the download settings for IE by following the steps below.

1. Navigate to **Internet Explorer > Tools > Internet Options**.
2. Switch to the **Security** tab and select a zone.
3. Select the Custom level button inside the Security level for this zone field.
4. Scroll down to the **Downloads** setting.

5. Change the detailed settings according to the screenshot below.

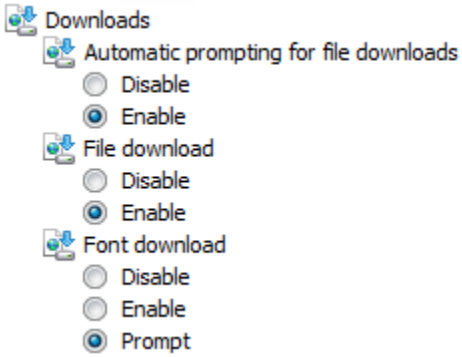

Figure 22: IE security settings.

The Actions Toolbar

When you select one or more jobs, the toolbar appears. This toolbar provides you with the **Stop** action to stop the selected in-progress job immediately. The job status will change to **Stopped**, but the job information will be retained, as well as any data aggregated by the job.

***Note**: Once a job is stopped, in order to run it again, you must launch the respective module you used to run that job. Select the **Plan Manager** tab, and then select the plan by checking the checkbox, and select **Run Now**. When you run the same job again, it will be considered a new job, so the previous data is retained.

The Settings Toolbar

This toolbar provides access to the Report Location tool that allows you to specify a location for storing the reports generated after running the jobs. If you do not configure this tool, the job reports will be stored in the default location (**...\AvePoint\Compliance Guardian\Manager\work**).

To store the job reports on a network share:

1. Check the **Use the Net Share path as the report location** checkbox.
2. Enter the **UNC Path**.
3. Enter the **Username**.
4. Enter the **Password**.
5. Select **OK**.

Operations in the Scheduled Job Monitor Tab

The Scheduled Job Monitor tab provides you with two toolbars that allow you to perform actions to jobs that you have scheduled to run in the future. The following sections explain what these tools do in detail.

The Actions Toolbar

This toolbar provides the following actions for a scheduled job:

- **Enable** – If the status of the selected jobs is disabled, you will have the option to select this button to enable it.
- **Disable** – If the status of the selected jobs is enabled, you will have the option to select this button to disable it.

The Filter Toolbar

This toolbar provides the following filter options for a scheduled job:

- **Date Range** – Allows you to limit the jobs displayed by specifying a time frame.
- **Module** – Allows you to limit the jobs displayed by specifying the module where the jobs are run.

Appendix A: Accessing Hot Key Mode

In order to work faster and improve your productivity, Compliance Guardian supports hot key mode for you to perform corresponding actions quickly using your keyboard. To access hot key mode in the Compliance Guardian interface, press **Ctrl** + **Alt** + **Z** on your keyboard.

The following table provides a list of hot keys for the top level. Each time you want to go back to the top level after accessing the lower level interface, press **Ctrl** + **Alt** + **Z**.

Operation Interface	Hot Key
Compliance Guardian	1
Report	2
Administration	3
User: admin	4
Help and About Information	5
Compliance Guardian Official Website	6

Compliance Scanner Page

The following table provides a list of hot keys for the functionalities on the ribbon of the Compliance Scanner page.

Functionality Name and Hot Key											
Compliance Guardian						1					
Report						2					
Administration						3					
Home	P	Create	C	SharePoint	S	SharePoint Tab	H				
						Plan Builder	C	Wizard Mode	M	Back	B
										Next	N
										Finish	R
										Finish and Run Now	O
										Cancel	C
								Form Mode	L	Save	R
										Save and Run Now	O
										Cancel	C
						Scan Policy	S	Create		C	
								View Details		V	
								Edit		E	
								Delete	D		
								Close	X		
						Filter Policy	F	Create	N		
								View Details	V		
								Edit	E		

Functionality Name and Hot Key												
								Delete	D			
								Close	X			
						Database Manager	D	Create	C			
								View Details	V			
								Edit	E			
								Delete	D			
								Close	X			
						Account Manager	A	Groups	G	Add Group	AD
										Edit Group	E
										Show Users	S
										Delete Group	D
										Permission Level	P
										Authentication Manager	AM
										Close	X
								Users	U	Add User	AU
										Edit User	E
										Delete User	DU
										Activate	AC
										Deactivate	DA
										Permission Level	P
										Authentication Manager	AM
										Close	X
						Job Monitor	J				
						Close	X				
				File System	F	File System Tab	F				
						Plan Builder	C	Wizard Mode	M	Back	B
										Next	N
										Finish	R
										Finish and Run Now	O
										Cancel	C
								Form Mode	L	Save	R
										Save and Run Now	O
										Cancel	C
						Configure Connection	N	Create	C		
								View Details	V		
								Edit	E		
								Delete	D		
								Close	X		

Functionality Name and Hot Key											
						Scan Policy	S	Create	C		
								View Details	V		
								Edit	E		
								Delete	D		
								Export	W		
								Close	X		
						Filter Policy	F	Create	N		
								View Details	V		
								Edit	E		
								Delete	D		
								Close	X		
						Database Manager	D	Create	C		
								View Details	V		
								Edit	E		
								Delete	D		
								Close	X		
						Account Manager	A	Groups	G	Add Group	AD
										Edit Group	E
										Show Users	S
										Delete Group	D
										Permission Level	P
										Authentication Manager	AM
										Close	X
								Users	U	Add User	AU
										Edit User	E
										Delete User	DU
										Activate	AC
										Deactivate	DA
										Permission Level	P
										Authentication Manager	AM
										Close	X
						Job Monitor	J				
						Close	X				
				Website	W	Create Plan Tab	W				
						Scan Policy	S	Create	C		
								View Details	V		
								Edit	E		

Functionality Name and Hot Key									
								Delete	D
								Export	W
								Close	X
						Filter Policy	F	Create	N
								View Details	V
								Edit	E
								Delete	D
								Close	X
						Database Manager	D	Create	C
								View Details	V
								Edit	E
								Delete	D
								Close	X
						Save	R		
						Save and Run Now	O		
						Cancel	C		
		View Details	V						
		Edit	E						
		Delete	D						
		Run Now	R						

Scheduled Classification Scanner Page

The following table provides a list of hot keys for the functionalities on the ribbon of the Scheduled Classification Scanner page.

Functionality Name and Hot Key											
Compliance Guardian							1				
Report							2				
Administration							3				
Home	P	Create	C	SharePoint	S	SharePoint Tab	H				
						Plan Builder	C	Wizard Mode	M	Back	B
										Next	N
										Finish	R
										Finish and Run Now	O
										Cancel	C
								Form Mode	L	Save	R
										Save and Run Now	O
										Cancel	C

Functionality Name and Hot Key											
						Scan Policy	S	Create		C	
								View Details		V	
								Edit		E	
								Delete		D	
								Close		X	
						Filter Policy	F	Create		N	
								View Details		V	
								Edit		E	
								Delete		D	
								Close		X	
						Action Policy	A	Create		C	
								View Details		V	
								Edit		E	
								Delete		D	
								Close		X	
						Job Monitor	J				
						Close	X				
				File System	F	File System Tab	F				
						Plan Builder	C	Wizard Mode	M	Back	B
										Next	N
										Finish	R
										Finish and Run Now	O
										Cancel	C
								Form Mode	L	Save	R
										Save and Run Now	O
										Cancel	C
						Configure Connection	N	Create		C	
								View Details		V	
								Edit		E	
								Delete		D	
								Close		X	
						Scan Policy	S	Create		C	
								View Details		V	
								Edit		E	
								Delete		D	

Functionality Name and Hot Key									
								Export	W
								Close	X
						Filter Policy	F	Create	N
								View Details	V
								Edit	E
								Delete	D
								Close	X
						Action Policy	A	Create	C
								View Details	V
								Edit	E
								Delete	D
								Close	X
						Job Monitor	J		
						Close	X		
		View Details	V						
		Edit	E						
		Delete	D						
		Run Now	R						

Real-Time Classification Scanner page

The following table provides a list of hot keys for the functionalities on the ribbon of the Real-Time Classification Scanner page. For example, continue pressing **H** on your keyboard to enter the **Real-Time Classification Scanner** interface.

Functionality Name and Hot Key					
Compliance Guardian	1				
Control Panel	3				
Job Monitor	4				
Real-Time Classification Scanner	H	Stop Inheriting/ Inheriting	T		
		Scan Policy	S	Create	C
				View Details	V
				Edit	E
				Delete	D
				Close	X

Functionality Name and Hot Key					
		Filter Policy	F	Create	N
				View Details	V
				Edit	E
				Delete	D
				Close	X
		Action Policy	A	Create	C
				View Details	V
				Edit	E
				Delete	D
				Close	X
		Apply	P		
		Create Rule	R		
		Job Monitor	J		

Job Monitor Page

The following table provides a list of hot keys for the functionalities on the ribbon of the Job Monitor page. For example, continue pressing **M** on your keyboard to enter the **Module** interface.

Functionality Name and Hot Key							
List View	LV						
Calendar View	CV						
Time Zone	TZ						
View Details	VD	Job Details Page	V	Download	D	OK	O
						Cancel	C
				Close	X		
Download	DL			OK	O		
				Cancel	C		
Pause	P						
Resume	RE						
Stop	SP						
Start	ST						
Delete	DE			Delete without Notification	D		
Date Range	DR						
Module	M						
Report Location	RL			OK	O		
				Back	B		

Scheduled Job Monitor Page

To access the Scheduled Job Monitor page by using hot keys from within the Job Monitor interface, press **Ctrl** + **Alt** + **Z** on your keyboard to access the hot key mode, and then press **S** on the keyboard to enter the **Scheduled Job Monitor** page.

The following table provides a list of hot keys for the functionalities on the ribbon of the Scheduled Job Monitor page. For example, continue pressing **L** to enter the **List View** interface.

Functionality Name and Hot Key	
List View	L
Calendar View	C
Time Zone	TZ
Enable	E
Disable	D
Date Range	R
Module	M

Control Panel Page

The following table provides a list of hot keys for the functionalities on the ribbon of the Control Panel page. For example, continue pressing **P** on your keyboard to enter the **Control Panel** interface.

Functionality Name and Hot Key	
Control Panel	P

Appendix B: Configuring Checks and Test Suites

When editing checks and test suites in the Test Suite Manager in Compliance Guardian, you will use detailed configuration screens to set the attributes and values.

- If you are editing a single check (per the Editing a Check section earlier in this document), refer to Configuring Check Type Attributes in this Appendix to configure the details according to the specific test definition file type.
- If you are editing a CCC or MCC file (per the Editing CCC or MCC Files section earlier in this document), refer to Configuring CCC or MCC File Attributes in this Appendix to configure the details according to the specific type of Content Compliance Collection (CCC) and Metadata Compliance Collection (MCC) file.

Configuring Check Type Attributes

Based on the different kinds of checks you can run, there are the following types of checks:

- Element Type
- EnhancedElement Type
- MatchedElement Type
- FindText Type
- ComplexFindText Type
- RegularExpression Type
- ComplexRegEx Type
- Dictionary Type
- Cookie Type
- SSL Type
- WebBeacons Type
- FindFile Type
- LinkValidation Type
- FileProperty Type

Details about configuring each of these check types are provided in the following sections.

Element Type Check

The Element type check is used to validate whether HTML/XML elements have particular settings on attributes or contents. The following section provides a general introduction about configuring attributes for this type of check, as well as a test example for you to understand the test logic.

Configuring Attributes for Element Type Check

Configure the attributes for the Element type check according to the instructions in the following sections.

Element

Configure the following attributes under the **Element** section:

- **Name** – Specify the element name that will be tested.
- **CaseSensitive** – Specify if the element name being tested for must match the case exactly.
- **ResultNA** – Specify a result when the specified element is not found. If **TrueResult** is selected, then if the specified element is not found, the True result will be returned. If **FalseResult** is selected, then if the specified element is not found, the False result will be returned. If **NAResult** is selected, then if the specified element is not found, the status of the tested file will be **Not Applicable**, which will be displayed in the Compliance Guardian report. In other words, you have the option to set the result to **Not Applicable** if none of the elements are found.
- **TrueIf** – There are two values for this attribute: **All** and **One**. If **One** is selected, the scan will stop when one instance is found (to save scan time). If **All** is selected, the scan will only stop when all instances are found.
- **ValidWhen** – This is used to indicate if the result is valid when the condition is one of two values: True or False.

ListLoc

Configure the following attributes under the **ListLoc** section:

- **Type** – There are two values for this attribute, **Valid** and **Invalid**. All elements that are considered valid or invalid are stored to the database (the Location).
- **Status** – This is used to indicate the disposition of the element and the severity selected by the user. Note that in the **Report Text** step, if the status set for True Result or False Result is **Failed**, the value for the **Status** attribute will be **Fail**, and the value cannot be changed.

ElementRepeat

If you want to configure the **ElementRepeat** section, select the checkbox before the element (this section is optional):

- **Alert** – Specify whether to check for repeating elements.
- **Value** – Specify the maximum times the element can repeat before the check is determined False.

TextCompare

If you want to configure the **TextCompare** section, select the checkbox before the element (this section is optional):

- **CompareType** – Specify a compare type. The attributes for CompareType are **MustContain**, **MustNotContain**, **MustEqual**, and **MustNotEqual**.
- **Separator** – Specify a separator if multiple values are specified.
- **CaseSensitive** – Specify if the element being tested for must match the case exactly.
- **Value** – Define one or more values for the test, use the separator specified before to separate the values.

Attributes

If you want to configure the **Attributes** section, select the checkbox before the element (this section is optional):

- **Name** – Specify attribute name that will be tested.
- **CaseSensitive** – Specify if the attribute name being tested for must match the case exactly.
- **AllowNull** – Specify whether the attribute that has no value will be tested.
- **MustExist** – Specify whether or not the attribute has to exist. If it is set to **True**, then the test will fail if the specified attribute does not exist.

Select the delete button ( ) to delete this check rule.

The following elements with specific attributes appear within the optional **Attributes** section:

- **Length** – This element is optional. Select the checkbox before this element, and the following attributes appear:
    - **CompareType** – Specify a compare type for this length compare. The attributes for CompareType are **GreaterThan**, **LessThan**, **GreaterOrEqualThan**, **LessOrEqualThan**, **Equal**, and **NotEqual**.
    - **Characters** – Specify the number of the characters used for the compare.

Select the delete button ( ) to delete this check rule. Select **Add Another Length** to add another rule.

- **TextCompare** – This element is optional. Select the checkbox before this element, and the following attributes appear:
  - **CompareType** – Specify a compare type. The attributes for CompareType are **MustContain**, **MustNotContain**, **MustEqual**, and **MustNotEqual**.
  - **Separator** – Specify a separator if multiple values are specified.
  - **CaseSensitive** – Specify if the attribute values being tested for must match the case exactly.
  - **Value** – Define one or more values for the test, use the separator specified before to separate the values.

  Select the delete button ( ) to delete this check rule. Select **Add Another TextCompare** to add another rule.

- **WordsRepeat** – This element is optional. Select the checkbox before this element, the following attribute appears:
  - **Number** – Define the number of times that words can repeat in the attribute value before the test fails.

Select **Add Another Attribute** to add another Attributes check rule.

ElementContent

If you want to configure the **ElementContent** section, select the checkbox before the element (this section is optional):

- **ContentReq** – Specify whether the specified element must contain content. If **Yes** is selected, then the element must contain content, or the check for this section will be False.

The following elements with specific attributes are within the optional **ElementContent** section:

- **Length** – This section is optional. Select the checkbox before this element, the following attributes appear:
  - **CompareType** – Specify a compare type for this length compare. The attributes for CompareType are GreaterThan, LessThan, GreaterOrEqualThan, LessOrEqualThan, Equal and NotEqual.
  - **Characters** – Specify the number of the characters used for the compare.

  Select the delete button ( ) to delete this check rule. Select **Add Another Length** to add another rule.

- **TextCompare** – This section is optional. Select the checkbox before this element, the following attributes appear:
    - **CompareType** – Specify a compare type. The attributes for CompareType are **MustContain**, **MustNotContain**, **MustEqual** and **MustNotEqual**.
    - **Separator** – Specify a separator if multiple values are specified.
    - **CaseSensitive** – Specify if the content being tested for must match the case exactly.
    - **Value** – Define one or more values for the test, use the separator specified before to separate the values.

  Select the delete button ( ) to delete this check rule. Select **Add Another TextCompare** to add another rule.

ChildElement

If you want to configure the **ChildElement** section, select the checkbox before the element (this section is optional):

- **Name** – Specify the name of the child element that will be tested.
- **CaseSensitive** – Specify if the element name being tested for must match the case exactly.
- **MustExist** – Specify whether or not the child element must exist. If **True** is selected, then the test will fail if there is No child element.

The following elements with specific attributes are within the optional **ChildElement** section:

- **ElementRepeat** – This section is optional. Select the checkbox before this element, the following attributes appear:
    - **Alert** – Specify whether to check for repeating elements.
    - **Value** – Specify the maximum times the element can repeat before the check is determined False
- **Attributes** – This section is optional. Select the checkbox before this element, the following attributes appear:
    - **Name** – Specify the attribute name that will be tested.
    - **CaseSensitive** – Specify if the attribute name being tested for must match the case exactly.
    - **AllowNull** – Specify whether the attribute that has no value will be tested.
    - **MustExist** – Specify whether or not the attribute has to exist. If True is selected, then the test will fail if the specified attribute does not exist.

The following elements with specific attributes are within the optional **Attributes** section:

- **Length** – This section is optional. Select the checkbox before this element, the following attributes appear:
  - **CompareType** – Specify a compare type for this length compare. The attributes for **CompareType** are **GreaterThan**, **LessThan**, **GreaterOrEqualThan**, **LessOrEqualThan**, **Equal** and **NotEqual**.
  - **Characters** – Specify the number of the characters used for the compare.

  Select the delete button ( ) to delete this check rule. Select **Add Another Length** to add another rule.

- **TextCompare** – This section is optional. Select the checkbox before this element, the following attributes appear:
  - **CompareType** – Specify a compare type. The attributes for CompareType are **MustContain**, **MustNotContain**, **MustEqual**, and **MustNotEqual**.
  - **Separator** – Specify a separator if multiple values are specified.
  - **CaseSensitive** – Specify if the attribute being tested for must match the case exactly.
  - **Value** – Define one or more values for the test, use the separator specified before to separate the values.

  Select the delete button ( ) to delete this check rule. Select **Add Another TextCompare** to add another check rule.

- **WordsRepeat** – This section is optional. Select the checkbox before this element, the following attribute appears:
  - **Number** – Define the number of times that words can repeat in the attribute value before the test fails.

- **ElementContent** – This section is optional. Select the checkbox before this element, the following attribute appears:
  - **ContentReq** – Specify whether the specified element must contain content. If **Yes** is selected, then the element must contain content, or the check for this section will be False.

  The following elements with specific attributes are within the optional **ElementContent** section:

  - **Length** – This section is optional. Select the checkbox before this element, the following attributes appear:

- **CompareType** – Specify a compare type for this length compare. The attributes for CompareType are **GreaterThan**, **LessThan**, **GreaterOrEqualThan**, **LessOrEqualThan**, **Equal** , and **NotEqual**.
- **Characters** – Specify the number of the characters used for the compare.

Select the delete button ( ) to delete this check rule. Select **Add Another Length** to add another check rule.

- **TextCompare** – This section is optional. Select the checkbox before this element, the following attributes appear:
  - **CompareType** – Specify a compare type. The attributes for CompareType are **MustContain**, **MustNotContain**, **MustEqual**, and **MustNotEqual**.
  - **Separator** – Specify a separator if multiple values are specified.
  - **CaseSensitive** – Specify if the attribute being tested for must match the case exactly.
  - **Value** – Define one or more values for the test, use the separator specified before to separate the values.

  Select the delete button ( ) to delete this check rule. Select **Add Another TextCompare** to add another check rule.

Element Check Test Logic Example

Refer to the following example to better understand the test logic of the Element type check.

The selected file A will be tested. It contains two nodes:

**
**

Create and configure the Element Type check test logic:

1. Create an Element type check. In the **Report Text** step, in the **False Result and Message** field, select **User Review Required** in the False Result drop-down list.
2. Configure the **Element** section:
   - Specify the element name **IMG** for the **Name** attribute.
   - Select **No** in the drop-down list under the **CaseSensitive** attribute.
   - Select **ResultNA** in the drop-down list under the **ResultNA** attribute.
   - Select **One** in the drop-down list under the **TrueIf** attribute.
   - Select **False** in the drop-down list under the **ValidWhen** attribute.

3. Configure the **ListLoc** section:
    - Select **Invalid** in the drop-down list under the **Type** attribute.
    - Select **Warn** in the drop-down list under the **Status** attribute.
4. Select the checkbox before the **ElementRepeat** element, and then select **Yes** in the drop-down list under the **Alert** attribute. Enter **2** in the **Value** field.
5. Select the checkbox before the **TextCompare** element:
    - Select **MustContain** in the drop-down list under the **CompareType** attribute.
    - Enter **;** as the separator.
    - Select **No** in the drop-down list under the **CaseSensitive** attribute.
    - Enter **A** in the **Value** field.
6. Save the check.
7. Run a Compliance Scanner job. The test suite used in this job contains the check configured above.

Review the check test logic:

- See the **ElementRepeat** section. The element **IMG** is continuously repeated 2 times in the file A, so the check in the **ElementRepeat** section is False;
- See the **TextCompare** section. The node in the file contains the value **A**, so the check in the **TextCompare** section is True.
- From the above, the check result of this check is False (any of the check results is False, the check result of this check is False). According to the settings in **False Result and Message** in the **Report Text** step, the returning status is **User Review Required**, which will be displayed in the Compliance Guardian report.
- See the attributes under **Element**: **True** has been selected in the drop-down list under **ValidWhen**, but the check result of this check is False, so the result for ValidWhen attribute is Invalid.
- See the **ListLoc** section. The result for **ValidWhen** is Invalid, so the check status will be **Warn**, and this check status will be recorded in the Compliance Guardian database, users cannot see the status in the Compliance Guardian GUI.

EnhancedElement Type Check

The EnhancedElement type check is used to validate two kinds of elements in one check during the scanning progress. The functionality of the EnhancedElement type check is similar to the Element type check. The following section provides a general introduction about configuring attributes for this type of check, as well as a test example for you to understand the test logic.

Configuring Attributes for EnhancedElement Type Check

Configure the attributes for the EnhancedElement type check according to the instructions in the following sections.

EnhancedElement

There are the five attributes under this element. For the details about the five attributes, refer to the Configuring Attributes for Element Type section.

ListLoc

There are the two attributes under this element. For the details about the two attributes, refer to the Configuring Attributes for Element Type section.

ElementRepeat

This section is optional. For the details about the attributes under this element, refer to the Configuring Attributes for Element Type section.

TextCompare

This section is optional. For the details about the attributes under this element, refer to the Configuring Attributes for Element Type section.

Attributes

This section is optional. For the details about the attributes under this element, refer to the Configuring Attributes for Element Type section.

ElementContent

This section is optional. For the details about the attributes under this element, refer to the Configuring Attributes for Element Type section.

ChildElement

This section is optional. For the details about the attributes under this element, refer to the Configuring Attributes for Element Type section.

SecondaryElement

This section is optional. Select the checkbox before this element, the following attributes appear:

- **Name** – Specify the secondary element that will be tested.
- **CaseSensitive** – Specify if the element name being tested for must match the case exactly.
- **MustExist** – Specify whether the secondary element must exist.

- **TrueIf** – There are two values for this attribute: **All** and **One**. If **One** is selected, the scan will stop when one instance is found (to save scan time). If **All** is selected, the scan will only stop when all instances are found.
- **MustNext** – Specify whether the secondary element must be next to the primary element (the element you specified above in this check). If you select **Yes** in the drop-down list under this attribute, only the secondary element that is next to the primary element will be checked. If you select **No** in the drop-down list under this attribute, then all the specified secondary elements will be checked.

The following elements with specific attributes are within the optional **SecondaryElement** section:

- **ElementRepeat** – This section is optional. Select the checkbox before this element, the following attributes appear:
  - **Alert** – Specify whether to check for repeating elements.
  - **Value** – Specify the maximum times the element can repeat before the check is determined False.
- **Attributes** – This section is optional. Select the checkbox before this element, the following attributes appear:
  - **Name** – Specify the attribute name that will be tested.
  - **CaseSensitive** – Specify if the attribute name being tested for must match the case exactly.
  - **AllowNull** – Specify whether the attribute that has no value will be tested.
  - **MustExist** – Specify whether or not the attribute has to exist. If True is selected, then the test will fail if the specified attribute does not exist.

  Select the delete button ( ) to delete this **Attributes** check rule.

  The following elements with specific attributes are within the optional **Attributes** section:

  - **Length** – This section is optional. Select the checkbox before this element, the following attributes appear:
    - **CompareType** – Specify a compare type for this length compare. The attributes for **CompareType** are **GreaterThan**, **LessThan**, **GreaterOrEqualThan**, **LessOrEqualThan**, **Equal**, and **NotEqual**.
    - **Characters** – Specify the number of the characters used for the compare.

    Select the delete button ( ) to delete this check rule. Select **Add Another Length** to add another rule.

- **TextCompare** – This section is optional. Select the checkbox before this element, the following attributes appear:
    - **CompareType** – Specify a compare type. The attributes for CompareType are **MustContain**, **MustNotContain**, **MustEqual**, and **MustNotEqual**.
    - **Separator** – Specify a separator if multiple values are specified.
    - **CaseSensitive** – Specify if the attribute being tested for must match the case exactly.
    - **Value** – Define one or more values for the test, use the Separator specified before to separate the values.

  Select the delete button ( ) to delete this check rule. Select **Add Another TextCompare** to add another rule.

- **WordsRepeat** – This section is optional. Select the checkbox before this element, the following attribute appears.
    - **Number** – Define the number of times that words can repeat in the attribute value before the test fails.

- **ElementContent** – This section is optional. Select the checkbox before this element, the following attribute appears:
    - **ContentReq** – Specify whether the specified element must contain content. If **Yes** is selected, then the element must contain content, or the check for this section will be False.

  The following elements with specific attributes are within the optional **ElementContent** section:

    - **Length** – This section is optional. Select the checkbox before this element, the following attributes appear:
        - **CompareType** – Specify a compare type for this length compare. The attributes for CompareType are **GreaterThan**, **LessThan**, **GreaterOrEqualThan**, **LessOrEqualThan**, **Equal**, and **NotEqual**.
        - **Characters** – Specify the number of the characters used for the compare.

      Select the delete button ( ) to delete this check rule. Select **Add Another Length** to add another rule.

    - **TextCompare** – This **section** is optional. Select the checkbox before this element, the following attributes appear:
        - **CompareType** – Specify a compare type. The attributes for CompareType are **MustContain**, **MustNotContain**, **MustEqual**, and **MustNotEqual**.
        - **Separator** – Specify a separator if multiple values are specified.

        - **CaseSensitive** – Specify if the attribute being tested for must match the case exactly.
        - **Value** – Define one or more values for the test, use the separator specified before to separate the values.

    Select the delete button ( ) to delete this check rule. Select **Add Another TextCompare** to add another rule.

- **ChildElement** – This section is optional. Select the checkbox before this element, the following attributes appear:
    - **Name** – Specify the name of the child element that will be tested.
    - **CaseSensitive** – Specify whether the element name being tested for must match the case exactly.
    - **MustExist** – Specify whether or not the child element must exist. If True is selected, then the test will fail if there is No child element.

    The following elements with specific attributes are within the optional **ChildElement** section:

    - **ElementRepeat** – This section is optional. Select the checkbox before this element, the following attributes appear:
        - **Alert** – Specify whether to check for repeating elements.
        - **Value** – Specify the maximum times the element can repeat before the check is determined False.
    - **Attributes** – This section is optional. Select the checkbox before this element, the following attributes appear:
        - **Name** – Specify the attribute name that will be tested.
        - **CaseSensitive** – Specify if the attribute name being tested for must match the case exactly.
        - **AllowNull** – Specify whether the attribute that has no value will be tested.
        - **MustExist** – Specify whether or not the attribute has to exist. If True is selected, then the test will fail if the specified attribute does not exist.

        The following elements with specific attributes are within the optional **Attributes** section:

    - **Length** – This section is optional. Select the checkbox before this element, the following attributes **appear**:
        - **CompareType** – Specify a compare type for this length compare. The attributes for CompareType are **GreaterThan**, **LessThan**, **GreaterOrEqualThan**, **LessOrEqualThan**, **Equal**, and **NotEqual**.

- **Characters** – Specify the number of the characters used for the compare.

Select the delete button ( ) to delete this check rule. Select **Add Another Length** to add another rule.

EnhancedElement Check Test Logic Example

Refer to the following example to better understand the test logic of the EnhancedElement type check. The following nodes are contained in the selected file A that will be tested:

<a href="http://www.google.com <http://www.google.com/> >google
**
**

Create and configure the EnhancedElement check test logic:

1. Create an EnhancedElement type check. In the **Report Text** step, in the **False Result and Message** field, select **User Review Required** in the **False Result** drop-down list.
2. Configure the **Element** section:
   - Specify the element name **A** for the **Name** attribute.
   - Select **No** in the drop-down list under the **CaseSensitive** attribute.
   - Select **ResultNA** in the drop-down list under the **ResultNA** attribute.
   - Select **One** in the drop-down list under the **TrueIf** attribute.
   - Select **False** in the drop-down list under the **ValidWhen** attribute.
3. In the **ListLoc** section:
   - Select **Valid** in the drop-down list under the **Type** attribute.
   - Select **Warn** in the drop-down list under the **Status** attribute.
4. Select the checkbox before **TextCompare**, and configure the following attributes:
   - Select **MustContain** in the drop-down list under the **CompareType** attribute.
   - Enter **;** as the separator.
   - Select **Yes** in the drop-down list under the **CaseSensitive** attribute.
   - Enter **google** in the **Value** field.
5. Select the checkbox before **SecondaryElement**, and configure the following attributes:
   - Specify the element name **IMG** for the Name attribute.
   - Select **No** in the drop-down list under the **CaseSensitive** attribute.
   - Select **Yes** in the drop-down list under the **MustExist** attribute.
   - Select **One** in the drop-down list under the **TrueIf** attribute.

- Select **Yes** in the drop-down list under the **MustNext** attribute.
- Select the checkbox before **Attributes**, and configure the following attributes:
    - Specify the attribute name **alt** for the **Name** attribute.
    - Select **No** in the drop-down list under the **CaseSensitive** attribute.
    - Select **Yes** in the drop-down list under the **AllowNull** attribute.
    - Select **Yes** in the drop-down list under the **MustExist** attribute.
    - Select the checkbox before the **WordsRepeat** element, and then enter **2** in the **Number** field.

6. Save the check.
7. Run a Compliance Scanner job. The test suite used in this job contains the check configured above.

Review the check test logic:

- See the **TextCompare** section: the node <a href="http://www.google.com <http://www.google.com/> >google in the file contains the value **google**, so the check result in the **TextCompare** section is True.
- See the attributes under **Element**: **True** has been selected in the drop-down list under **ValidWhen**, and the check result for the element **A** in this check is True, so the result for **ValidWhen** section is Valid.
- See the **ListLoc** section: the result for **ValidWhen** is **Valid**, so the location of the node <a href="http://www.google.com <http://www.google.com/> >google will be temporarily recorded (the location of the node is TEMPORARILY recorded, but is NOT really recorded in the Compliance Guardian database. For this type of check, only the location of the instance found by the **SecondaryElement** check can be recorded).
- See the **SecondaryElement** section: because we have set **Yes** for the **MustNext** attribute, the node in file A will be checked, the node will not be checked:
    - See the **Attributes** section under **SecondaryElement**: we have specified **2** in the **Number** field under the **WordsRepeat** attribute, the value in the node contains two repeated words: **test**, so the check for **Attributes** is False.
    - See the attributes under **Element**: **True** has been selected in the drop-down list under **ValidWhen**, but the check result of this check is False, so the result for **ValidWhen** field is **Invalid**.
    - See the **ListLoc** section: the result for **ValidWhen** is **Invalid**, so the check status is **Warn**, and this check status will be recorded in the Compliance Guardian database, users cannot see the status in the Compliance Guardian GUI.

- For this type of check, if there are nothing temporarily recorded in the **EnhancedElement** check section, the **SecondaryElement** check will not start, and the check result of this check will be True. If there are something that are recorded in the **EnhancedElement** check section, the **SecondaryElement** check will start. If there are something recorded based on the **SecondaryElement** check, the result of this check will be False. On the contrary, if there are nothing recorded based on the **SecondaryElement** check, the result of this check will be True.
- Since there is something recorded in the Compliance Guardian database in this use case, the check result of this check is False. According to the setting in **False Result and Message** in the **Report Text** step, the returning status is **User Review Required**, which will be displayed in the Compliance Guardian report.

MatchedElement Type Check

The MatchedElement type check is used to validate the matching relationship between two elements.

The following section provides a general introduction about configuring attributes for this type of check, as well as a test example for you to understand the test logic.

Configuring Attributes for MatchedElement Type Check

Configure the attributes for the MatchedElement type check according to the instructions in the following sections.

MatchElement

There are the five attributes under this element. For the details about the five attributes, refer to the Configuring Attributes for Element Type section.

ListLoc

There are two attributes under this element. For the details about the two attributes, refer to the Configuring Attributes for Element Type section.

Attributes

This section is optional. For the details about the attributes under this element, refer to the Configuring Attributes for Element Type section.

ElementContent

This section is optional. The details about the attributes under this element, refer to the Configuring Attributes for Element Type section.

ChildElement

This section is optional. The details about the attributes under this element, refer to the Configuring Attributes for Element Type section.

SecondaryMatch

This section is optional. Select the checkbox before the element, and configure the following attributes:

- **SecondaryMatch** – Configure the following attributes for this element:
  - **Name** – Specify the element that will be tested.
  - **CaseSensitive** – Specify if the element name being tested for must match the case exactly.
  - **ResultNA** – Specify a result when the specified element is not found. If **TrueResult** is selected, then if the specified element is not found, the True result will be returned. If **FalseResult** is selected, then if the specified element is not found, the False result will be returned. If **NAResult** is selected, then if the specified element is not found, the status of the tested file will be **Not Applicable**, which will be displayed in the Compliance Guardian report. This is basically stating that you have the option to set the result to **Not Applicable** if none of the elements are found.
  - **TrueIf** – There are two values for this attribute: **All** and **One**. If **One** is selected, the scan will stop when one instance is found (to save scan time). If **All** is selected, the scan will only stop when all instances are found.
  - **ValidWhen** – This is used to indicate if the result is valid when the condition is one of two values: True or False.
- **Attribute** – Configure the following attributes for this element:
  - **Name** – Specify the name of the attribute to be tested.
  - **CaseSensitive** – Specify if the attribute name being tested for must match the case exactly.
  - **AllowNull** – Specify whether the attribute that has no value will be tested.
  - **MustExist** – Specify whether or not the attribute has to exist. If **True** is selected, then the test will fail if the specified attribute does not exist.
- **TextCompare** – Configure the following attributes for this element:
  - **MatchElementValue** – If the **Attributes** element under the **MatchElement** section has been configured, this radio button will be selectable. If this radio button is selected, configure the following attributes:
    - **Name** – All the attribute names configured under the **MatchElement** section will be loaded. Select a name from the drop-down list for the test.
    - **CaseSensitive** – Specify if the attribute name being tested for must match the case exactly.
    - **CompareType** – There are two values for this attribute: **MustContain** and **MustNotContain**. If **MustContain** is selected, the test condition is: the value of the attribute under the **SecondaryMatch** section must

contain the value of the attribute under the **MatchElement** section, or the check will be failed; If **MustNotContain** is selected, the test condition is: the value of the attribute under the **SecondaryMatch** section must not contain the value of the attribute under the **MatchElement** section, or the check will be failed.

- **TextCompare** – If this radio button is selected, configure the following **attributes**:
  - **CompareType** – Specify a compare type. The attributes for **CompareType** are **MustContain**, **MustNotContain**, **MustEqual**, and **MustNotEqual**.
  - **Separator** – Specify a separator if multiple values are specified.
  - **CaseSensitive** – Specify if the attribute being tested for must match the case exactly.
  - **Value** – Define one or more values for the test, use the separator specified before to separate the values.

MatchedElement Check Test Logic Example

Refer to the following example to better understand the test logic of the MatchedElement type check.

The selected file A that will be tested contains the following nodes:

<Input id="search-keyword"/>
<Input id=".docx">
<label For=".docx">
<label For="keyword"/>

Create and configure the MatchedElement check test logic:

1. Create a **MatchedElement** type check. In the **Report Text** step, in the **True Result and Message** field, select **Passed** in the True Result drop-down list.
2. Configure the **Element** section:
   - Specify the element name **Input** for the **Name** attribute.
   - Select **No** in the drop-down list under the **CaseSensitive** attribute.
   - Select **ResultNA** in the drop-down list under the **ResultNA** attribute.
   - Select **One** in the drop-down list under the **TrueIf** attribute.
   - Select **True** in the drop-down list under the **ValidWhen** attribute.
3. Configure the **ListLoc** section:
   - Select **Valid** in the drop-down list under the **Type** attribute.
   - Select **Note** in the drop-down list under the **Status** attribute.

4. Select the checkbox before **Attributes**, and configure the following attributes:
    - Specify the attribute name **ID** for the **Name** attribute
    - Select **No** in the drop-down list under the **CaseSensitive** attribute.
    - Select **Yes** in the drop-down list under the **AllowNull** attribute.
    - Select **True** in the drop-down list under the **MustExist** attribute.
    - Select the checkbox before **Length**, and configure the following attributes:
        - Select **GreaterThan** in the drop-down list under the **CompareType** attribute.
        - Enter **5** as the value of the **Characters** attribute.
5. Select the checkbox before **SecondaryMatch**:
    - Configure the following attributes:
        - Specify the element name **Label** for the **Name** attribute.
        - Select **No** in the drop-down list under the CaseSensitive attribute.
        - Select **ResultNA** in the drop-down list under the **ResultNA** attribute.
        - Select **One** in the drop-down list under the **TrueIf** attribute.
        - Select **False** in the drop-down list under the **ValidWhen** attribute.
    - In the **Attributes** section:
        - Specify the attribute name **FOR** for the **Name** attribute.
        - Select **No** in the drop-down list under the **CaseSensitive** attribute.
        - Select **Yes** in the drop-down list under the **AllowNull** attribute.
        - Select **True** in the drop-down list under the **MustExist** attribute.
    - In the **TextCompare** section, select the **MatchElementValue** radio button:
        - Select the attribute name **ID** for the **Name** attribute.
        - Select **No** in the drop-down list under the **CaseSensitive** attribute.
        - Select **MustContain** in the drop-down list under the **CompareType** attribute.
6. Save the check.
7. Run a Compliance Scanner job, the test suite used in this job contains the check configured above.

Review the check test logic:

- See the **Attributes** section under **MatchElement**: under the **Length** element: we have set **GreaterThan** for the **CompareType** attribute, and set **5** for the **Characters** attribute, that means the check for the node **<Input id="keyword"/>** in file A is True, while the check for the node **<Input id=".docx">** is False. And according to the value set for **ValidWhen**, the node **<Input id="keyword"/>** will be valid. According to the logic of the

ListLoc section, the location of the node **<Input id="keyword"/>** will be TEMPORARILY recorded (the location of the node **<Input id=" keyword"/> is** TEMPORARILY recorded, but is Not really recorded in the Compliance Guardian database, only there are something temporarily recorded in the **MatchElement** check section, can the **SecondaryMatch** section check start. If there are nothing recorded in the **MatchElement** check, the **SecondaryMatch** section check will not start, and the result of the check will be True).

- In the **SecondaryMatch** section, see the following nodes in file A:

  <Input id="keyword"/>
  <Input id=".docx">
  <label For=".docx">
  <label For="search-keyword"/>

  - According to the logic set in the **MatchElement** section, the node **<Input id=" keyword"/>** meets the condition and is taken to participate to the secondary check.
  - See the **Attributes** section under **SecondaryMatch** section, see the node: **<label For="search-keyword"/>**, the value of the attribute **For** (search-keyword) contains the value of the attribute **id**, so the check result of the **SecondaryMatch** section is True.
  - See the **ValidWhen** attribute under **SecondaryMatch**, **False** has been selected in the drop-down list under **ValidWhen**, but the check result of this check is True, so the result for **ValidWhen** attribute is Invalid.
  - See the **ListLoc** field, the result for **ValidWhen** is Invalid, so the check status (Note) and the location of the node **<Input id="keyword"/>** (the location of the attribute specified in the **SecondaryMatch** section will not be recorded, the location of the attribute that is specified in the **MatchElement** and meets the condition will be recorded in the database) will be recorded in Compliance Guardian database, users cannot see the status in the Compliance Guardian GUI.

- In the **SecondaryMatch** section, if you select the **MatchElementValue** radio button under the **TextCompare** section, the result of this check is not determined by the check result of the **MatchElement** section, and not determined by the check result of the **SecondaryMatch** section either. In the **MatchElement** section, if there are nothing temporarily recorded, the **SecondaryMatch** section check will not start, and the result of this check will be True; while in the **MatchElement** section, if there are something temporarily recorded, the **SecondaryMatch** section check will start. According to the logic in the **SecondaryMatch** section, if there are something recorded in the **SecondaryMatch** check, the result of this check will be False. While if there are nothing recorded in the **SecondaryMatch** check, the result of this check will be True.

  In this use case, according to the **SecondaryMatch** section, the node **<Input id="keyword"/>** will be recorded in Compliance Guardian database. So the result of this check will be False.

- In the **SecondaryMatch** section, if you select **TextCompare** radio button under the **TextCompare** section, if the element specified in the **MatchElement** section is not found, the result of this check will be the value set for the **ResultNA** attribute; if the element specified in the **MatchElement** section is found, the check result will be determined by the logic in the **SecondaryMatch** section, the attributes configured in the **MatchElement** section will not affect the result of this check.

FindText Type Check

The FindText type check is used to find specified text in a document. The following section provides a general introduction about configuring attributes for this type of check, as well as a test example for you to understand the test logic.

Configuring Attributes for FindText Type Check

Configure the attributes for the FindText type check according to the instructions in the following sections.

FindText

This element has the following attributes:

- **TrueIf** – Specify the condition when the check result is True. If **Found** is selected in the drop-down list under the **TrueIf** attribute, when finding an instance, the check result of this check will be True. If **NotFound** is selected in the drop-down list under the **TrueIf** attribute, when finding an instance, the check result of this check will be False.
- **SearchAll** – Specify whether or not to check the comments and scripts.
- **ListLocation** – Specify whether or not to record the instance's location in the Compliance Guardian database. If **Yes** is selected in the drop-down list under the **ListLocation** attribute, then every location of the instance found will be recorded in the Compliance Guardian database. If **No** is selected in the drop-down list under the **ListLocation** attribute, the check continues, but the locations of the instances found will not be recorded in the database.
- **ListLocStatus** – Specify the status for the instance that is found. The status will be recorded in the Compliance Guardian database. Note that if the status set for **True** Result or False Result is **Failed** in the **Report Text** step, the value for the **ListLocStatus** attribute will be **Fail**, and the value cannot be changed.
- **CaseSensitive** – Specify if the text being tested for must match the case exactly.
- **MustRepeat** – Specify the amount of times a word or phrase must be found before considering the condition to be True. When configuring the check, if you do not enter a value for this attribute, the value for this attribute will be considered 1 in the test.
- **CompareType** – Select **MustContain** or **MustEqual** for this attribute.
- **Value** – Specify a scanned value.

FindText Check Test Logic Example

Refer to the following example to better understand the test logic of the FindText type check.

The content of the file A that will be tested contains the following two values: 508, 508. Create and configure the FindText check test logic:

1. Create a **FindText** Type check. In the **Report Text** step, in the **False Result and Message** field, select **User Review Required** in the False Result drop-down list.
2. Configure the elements in the check:
    - Select **NotFound** in the drop-down list under the **TrueIf** attribute.
    - Select **Yes** in the drop-down list under the **SearchAll** attribute.
    - Select **Yes** in the drop-down list under the **ListLocation** attribute.
    - Select **Note** in the drop-down list under the **ListLocStatus** attribute.
    - Select **No** in the drop-down list under the **CaseSensitive** attribute.
    - Enter **2** as the value for the **MustRepeat** attribute.
    - Select **MustEqual** for the **CompareType** attribute.
    - Enter **508** in the **Value** field.
3. Save the check.
4. Run a Compliance Scanner job. The test suite used in this job contains the check configured above.

Review the Check test logic:

- If **MustEqual** is selected for the **CompareType** attribute, then the content must exactly equal the value we specified in order to be found. If **MustContain** is selected for this attribute, then the content only needs to contain the value in order to be found. For example, if the tested file contains the word **Front-end**, and we select **MustEqual** for the **CompareType** attribute with the value specified as **end**, then the word **Front-end** will not be found, but if we select **MustContain** for the **CompareType** attribute, the word **Front-end** will be found.
- We have set 2 for the **MustRepeat** attribute, and the value **508** has repeated 2 times in the file A, so the check is Found. We have set **NotFound** for the **TrueIf** value, so the check result of this check is False. According to the setting in **False Result and Message** in the **Report Text** step, the returning status is **User Review Required**, which will be displayed in the Compliance Guardian report.
- We have set **Yes** for the **ListLocation** attribute, and have set **Note** as the status, so the location of 508 in the file A will be recorded in the Compliance Guardian database, the status is **Note**.

ComplexFindText Type Check

The ComplexFindText type check offers a more complex way to detect if two text strings are coexisting in one document. The functionality of the ComplexFindText type check is similar to the FindText type check. The following section provides a general introduction about configuring attributes for this type of check, as well as a test example for you to better understand the test logic.

Configuring Attributes for ComplexFindText Type Check

Configure the attributes for the ComplexFindText type check according to the instructions in the following sections.

Primary

Configure the following attributes in this section:

- **TrueIf** – Specify the condition when the check result is True. If **Found** is selected in the drop-down list under the **TrueIf** attribute: when finding an instance, the check result of this check will be True. If **NotFound** is selected in the drop-down list under the **TrueIf** attribute: when finding an instance, the check result of this check will be False.
- **SearchAll** – Specify whether or not to check the comments and scripts.
- **ListLocation** – Specify whether or not to record the instance's location in the Compliance Guardian database. If **Yes** is selected in the drop-down list under the **ListLocation** attribute, then every location of the instance found will be recorded in the Compliance Guardian database. If **No** is selected in the drop-down list under the **ListLocation** attribute, the check continues, but the locations of the instances found will not be recorded in the database.
- **ListLocStatus** – Specify the status for the instance that is found. The status will be recorded in the Compliance Guardian database. Note that if the status set for **True** Result or False Result is **Failed** in the **Report Text** step, the value for the **ListLocStatus** attribute will be **Fail**, and the value cannot be changed.
- **CaseSensitive** – Specify if the text being tested for must match the case exactly.
- **MustRepeat** – Specify the amount of times a word or phrase must be found before considering the condition to be True. When configuring the check, if you do not enter a value for this attribute, the value for this attribute will be considered 1 in the test.
- **CompareType** – Select **MustContain** or **MustEqual** for this attribute.
- **ResultNA** – If the primary check in this check is not fulfilled, the scan status will be the value you selected for the **ResultNA** attribute.
- **Value** – Specify a scanned value for the primary check section.

Secondary

Configure the following attributes in this section:

- **TrueIf** – Specify the condition when the check result is True. If **Found** is selected in the drop-down list under the **TrueIf** attribute: when finding an instance, the check result of this check will be True. If **NotFound** is selected in the drop-down list under the **TrueIf** attribute: when finding an instance, the check result of this check will be False.
- **SearchAll** – Specify whether or not to check the comments and scripts.
- **ListLocation** – Specify whether or not to record the instance's location in the Compliance Guardian database. If **Yes** is selected in the drop-down list under the **ListLocation** attribute, then every location of the instance found will be recorded in the Compliance Guardian database. If **No** is selected in the drop-down list under the ListLocation attribute, the check continues, but the locations of the instances found will not be recorded in the database.
- **ListLocStatus** – Specify the status for the instance that is found. The status will be recorded in the Compliance Guardian database. Note that if the status set for **True** Result or False Result is **Failed** in the Report Text step, the value for the **ListLocStatus** attribute will be **Fail**, and the value cannot be changed.
- **CaseSensitive** – Specify if the text being tested for must match the case exactly.
- **MustRepea**t – Specify the amount of times a word or phrase must be found before considering the condition to be True. When configuring the check, if you do not enter a value for this attribute, the value for this attribute will be considered 1 in the test.
- **CompareType** – Select **MustContain** or **MustEqual** for this attribute.
- **Value** – Specify a scanned value for the secondary check section.

ComplexFindText Check Test Logic Example

Refer to the following example for better understanding the test logic of the ComplexFindText type check.

The content of the selected file A that will be tested contains the following two values: 508, Justice.

Create and configure the ComplexFindText check test logic:

1. Create a **FindText** Type check. In the **Report Text** step, in the **False Result and Message** field, select **User Review Required** in the False Result drop-down list.
2. Configure the Primary section:
    - Select **Found** in the drop-down list under the **TrueIf** attribute.
    - Select **Yes** in the drop-down list under the **SearchAll** attribute.
    - Select **Yes** in the drop-down list under the **ListLocation** attribute.
    - Select **Note** in the drop-down list under the **ListLocStatus** attribute.

- Select **No** in the drop-down list under the **CaseSensitive** attribute.
- Select **MustContain** in the drop-down list under the **CompareType** attribute.
- Select **FalseResult** in the drop-down list under the **ResultNA** attribute.
- Enter **508** in the **Value** field.

3. Configure the Secondary section:
    - Select **NotFound** in the drop-down list under the **TrueIf** attribute.
    - Select **Yes** in the drop-down list under the **SearchAll** attribute.
    - Select **Yes** in the drop-down list under the **ListLocation** attribute.
    - Select **Note** in the drop-down list under the **ListLocStatus** attribute.
    - Select **No** in the drop-down list under the **CaseSensitive** attribute.
    - Select **MustContain** in the drop-down list under the **CompareType** attribute.
    - Enter **JUSTICE** in the **Value** field.
4. Save the check.
5. Run a Compliance Scanner job, the test suite used in this job contains the check configured above.

Review the check test logic:

- If **MustEqual** is selected for the **CompareType** attribute, then the content must exactly equal the value we specified in order to be found. If **MustContain** is selected for this attribute, then the content only needs to contain the value in order to be found. For example, if the tested file contains the word **Front-end**, and we select **MustEqual** for the **CompareType** attribute with the value specified as **end**, then the word **Front-end** will not be found, but if we select **MustContain** for the **CompareType** attribute, the word **Front-end** will be found.
- In this type of check, if the result of the primary check is True, the secondary check can start for this check. If the result of the primary check is False, the secondary check will not start for this check and the result of this check will be determined by the primary check. For the **ResultNA** attribute, if **TrueResult** is set as the value of this attribute, the result of this check will be True. If **FalseResult** is set as the value of this attribute, the result of this check will be False. If **NAResult** is set as the value of this attribute, the status of the tested file will be Not Applicable, and Not Applicable will be displayed in the Compliance Guardian report.
- In this use case:
    - In the primary check, the value that will be searched for in the file is **508**, which can be found in the file A, so the result is Found. According to the logic of the **TrueIf** attribute, the result of the primary check is True. So the secondary check will start.

- In the secondary check, the value that will be searched for in the file is **JUSTICE**, which can be found in the file A, so the result is Found. According to the logic of the **TrueIf** attribute, the result of the secondary check is False. So the result of this check is False. According to the setting in **False Result and Message** in the **Report Text** step, the returning status is **User Review Required**, which will be displayed in the Compliance Guardian report.

RegularExpression Type Check

The RegularExpression type check is used to find a string of text that fits the format of the defined regular expression. The following section provides a general introduction about configuring attributes for this type of check, as well as a test example for you to understand the test logic.

Configuring Attributes for RegularExpression Type Check

Configure the attributes for the RegularExpression type check according to the instructions in the following sections.

RegularExpression

Configure the following attributes in this section:

- **IsFindText** – Specify whether or not to extract the text as the scanning content. If **Yes** is selected in the drop-down list under this attribute, the scan engine will extract the text as the scanning content. if **No** is selected in the drop-down list under this attribute, the scan engine will use the source code as the scanning content.
- **SearchAll** – Specify whether or not to check the comments and scripts.
- **CaseSensitive** – Specify if the text being tested for must match the case exactly.
- **TrueIf** – Specify the condition when the check result is True. If **Found** is selected in the drop-down list under the **TrueIf** attribute: when finding an instance, the check result of this check will be True. If **NotFound** is selected in the drop-down list under the **TrueIf** attribute: when finding an instance, the check result of this check will be False.
- **ListLocation** – Specify whether or not to record the instance's location in the Compliance Guardian database. If **Yes** is selected in the drop-down list under the **ListLocation** attribute, then every location of the instance found will be recorded in the Compliance Guardian database. If **No** is selected in the drop-down list under the **ListLocation** attribute, the check continues, but the locations of the instances found will not be recorded in the database.
- **ListLocStatus** – Specify the status for the instance that is found. The status will be recorded in the Compliance Guardian database. Note that if the status set for **True** Result or False Result is **Failed** in the **Report Text** step, the value for the **ListLocStatus** attribute will be **Fail**, and the value cannot be changed.
- **MustRepeat** – Specify the amount of times the value that matches the regular expression must be found before considering the condition to be True. When

configuring the check, if you do not enter a value for this attribute, the value for this attribute will be considered 1 in the test.

- **CustomCheck** – Enter a CustomCheck name for this attribute. The CustomCheck is used to calculate check digit on the result of the regular expressions, in order to validate the result. Refer to Appendix H: Using CustomCheck in Compliance Guardian for details on CustomCheck. This is optional.

Filter

If you want to configure the **Filter** section, select the checkbox before the element (this section is optional). Select the checkbox before **Text** if you want to configure the **Text** section:

- **CaseSensitive** – Specify if the element being tested must match the case exactly.
- **Separator** – Specify a separator if multiple values are specified.
- **Value** – Define one or more values for the test, and use the separator specified before to separate the values. If the scanned result that matches the specified regular expression exactly matches the value specified here, this result will be filtered out.

Select **Add Another Text** to add another Text filter check rule. Select the delete button ( ) to delete a Text filter check rule.

Select the checkbox before **Regex** if you want to configure the **Regex** section:

- **CaseSensitive** – Specify if the element being tested must match the case exactly.
- **Value** – Define a regular expression. If the scanned result that matches the specified regular expression also matches the regular expression specified here, this result will be filtered out.

Select **Add Another Regex** to add another Regex filter check rule. Select the delete button ( ) to delete a Regex filter check rule.

Value Field

Specify a regular expression. The value that matches the regular expression will be scanned.

RegularExpression Check Test Logic Example

Refer to the following example to better understand the test logic of the RegularExpression type check.

The file A that will be tested contains two words: Server-Side and front-end

Create and configure the RegularExpression type check:

1. Create a **RegularExpression** Type check. In the **Report Text** step, in the **True Result and Message** field, select **Passed** in the False Result drop-down list.
2. Configure the elements in the **RegularExpression** section:
    - Select **Yes** in the drop-down list under the **IsFindText** attribute.

- Select **Yes** in the drop-down list under the **SearchAll** attribute.
- Select **No** in the drop-down list under the **CaseSensitive** attribute.
- Select **Found** in the drop-down list under the **TrueIf** attribute.
- Select **Yes** in the drop-down list under the **ListLocation** attribute.
- Select **Warn** in the drop-down list under the **ListLocStatus** attribute.

3. Select the checkbox before **Filter**, and select the checkbox before **Text**. Configure the following attributes in the **Text** section:
    - Select **No** in the drop-down list under the **CaseSensitive** attribute.
    - Enter **;** as the separator.
    - Enter front-end;Server-Side in the Value field.
4. Enter the regular expression **\b[a-zA-Z]+-[a-zA-Z]+\b** in the **Value** field. A word that contains a hyphen can match the regular expression.
5. Save the check.
6. Run a Compliance Scanner job. The test suite used in this job contains the check configured above.

Review the check test logic:

- In this case, in the file A, the words **Server-Side** and **front-end** match the specified regular expression, but according to the logic we configured in the **Filter** section, the two words will be filtered out, so the result is Not Found. And we have set **NotFound** for the **TrueIf** value, so the check result of this check is True. According to the setting in **True Result and Message** in the **Report Text** step, the returning status is **Passed**, which will be displayed in the Compliance Guardian report.
- We set **Yes** for the **ListLocation** attribute, but no result that meets the condition in the check was found. No location will be recorded in the Compliance Guardian database.

ComplexRegEx Type Check

The ComplexRegEx type check offers a more complex way to detect if two strings of text are coexisting in one document. The functionality of the ComplexRegEx type check is similar to the RegularExpression type check. The following section provides a general introduction about configuring attributes for this type of check, as well as a test example to better understand the test logic.

Configuring Attributes for ComplexRegEx Type Check

Configure the attributes for the ComplexRegEx type check according to the instructions in the following sections.

ComplexRegex

Configure the following attribute in this section:

- **IsFindText** – Specify whether or not to extract the text as the scanning content. If **Yes** is selected in the drop-down list under this attribute, the scan engine will extract the text as the scanning content; if **No** is selected in the drop-down list under this attribute, the scan engine will use the source code as the scanning content.

Primary Check

Configure the following attributes in this section:

- **SearchAll** – Specify whether or not to check the comments and scripts.
- **CaseSensitive** – Specify if the text being tested for must match the case exactly.
- **TrueIf** – Specify the condition when the check result is True. If **Found** is selected in the drop-down list under the **TrueIf** attribute: when finding an instance, the check result of this check will be True. If **NotFound** is selected in the drop-down list under the **TrueIf** attribute: when finding an instance, the check result of this check will be False.
- **ListLocation** – Specify whether or not to record the instance's location in the Compliance Guardian database. If **Yes** is selected in the drop-down list under the **ListLocation** attribute, then every location of the instance found will be recorded in the Compliance Guardian database. If **No** is selected in the drop-down list under the **ListLocation** attribute, the check continues, but the locations of the instances found will not be recorded in the database.
- **ListLocStatus** – Specify the status for the instance that is found. The status will be recorded in the Compliance Guardian database. Note that if the status set for **True** Result or False Result is **Failed** in the **Report Text** step, the value for the **ListLocStatus** attribute will be **Fail**, and the value cannot be changed.
- **MustRepeat** – Specify the amount of times the value that matches the regular expression must be found before considering the condition to be True. When configuring the check, if you do not enter a value for this attribute, the value for this attribute will be considered 1 in the test.
- **CustomCheck** – Enter a **CustomCheck** name for this attribute. The **CustomCheck** is used to calculate the check digit on the result of the regular expressions, in order to validate the result. Refer to Appendix H: Using CustomCheck in Compliance Guardian for the details on **CustomCheck**. This is optional.
- **ResultNA** – If the primary check in this check is not fulfilled, the scan status will be the value you selected for the **ResultNA** attribute.
- **Filter** – This field is optional. Select the checkbox before **Filter**, the **Text** section and the **Regex** section appear:
    - **Text** – Select the checkbox before Text, and configure the following attributes:

        - **CaseSensitive** – Specify if the element being tested for must match the case exactly.
        - **Separator** – Specify a separator if multiple values are specified.
        - **Value** – Define one or more values for the test, and use the separator specified before to separate the values. If the scanned result that matches the specified regular expression exactly matches the value specified here, this result will be filtered out.

      Select **Add Another Text** to add another Text filter check rule. Select the delete button ( ) to delete this check rule.

    - **Regex** – Select the checkbox before Text, and configure the following attributes:
        - **CaseSensitive** – Specify if the element being tested for must match the case exactly.
        - **Separator** – Specify a separator if multiple values are specified.
        - **Value** – Define a regular expression. If the scanned result that matches the specified regular expression also matches the regular expression specified here, this result will be filtered out.

      Select **Add Another Regex** to add another Text filter check rule. Select the delete button ( ) to delete this Regex filter check rule.

- **Value** – Specify a regular expression for the secondary check section. The value that matches the regular expression will be scanned.

Secondary Check

Configure the following attributes in this section:

- **SearchAll** – Specify whether or not to check the comments and scripts.
- **CaseSensitive** – Specify if the text being tested for must match the case exactly.
- **TrueIf** – Specify the condition when the check result is True. If **Found** is selected in the drop-down list under the **TrueIf** attribute, when finding an instance, the check result of this check will be True. If **NotFound** is selected in the drop-down list under the **TrueIf** attribute, when finding an instance, the check result of this check will be False.
- **ListLocation** – Specify whether or not to record the instance's location in the Compliance Guardian database. If **Yes** is selected in the drop-down list under the **ListLocation** attribute, then every location of the instance found will be recorded in the Compliance Guardian database. If **No** is selected in the drop-down list under the **ListLocation** attribute, the check continues, but the locations of the instances found will not be recorded in the database.
- **ListLocStatus** – Specify the status for the instance that is found. The status will be recorded in the Compliance Guardian database. Note that if the status set for **True**

Result or False Result is **Failed** in the **Report Text** step, the value for the **ListLocStatus** attribute will be **Fail**, and the value cannot be changed.

- **MustRepeat** – Specify the amount of times the value that matches the regular expression must be found before considering the condition to be True. When configuring the check, if you do not enter a value for this attribute, the value for this attribute will be considered 1 in the test.
- **CustomCheck** – Enter a CustomCheck name for this attribute. The CustomCheck is used to calculate check digit on the result of the regular expressions, in order to validate the result. Refer to Appendix H: Using CustomCheck in Compliance Guardian for details on CustomCheck. This is optional.
- **Filter** – This is optional. Select the checkbox before **Filter**, the **Text** section and the **Regex** section appear:
    - **Text** – Select the checkbox before Text, and configure the following attributes:
        - **CaseSensitive** – Specify if the element being tested for must match the case exactly.
        - **Separator** – Specify a separator if multiple values are specified.
        - **Value** – Define one or more values for the test, and use the separator specified before to separate the values. If the scanned result that matches the specified regular expression exactly matches the value specified here, this result will be filtered out.

      Select **Add Another Text** to add another Text filter check rule. Select the delete button ( ) to delete this filter check rule.
    - **Regex** – Select the checkbox before Text, and configure the following attributes:
        - **CaseSensitive** – Specify if the element being tested for must match the case exactly.
        - **Separator** – Specify a separator if multiple values are specified.
        - **Value** – Define a regular expression. If the scanned result that matches the specified regular expression also matches the regular expression specified here, this result will be filtered out.

      Select **Add Another Regex** to add another Text filter check rule. Select the delete button ( ) to delete this Regex filter check rule.
- **Value** – Specify a regular expression for the secondary check section. The value that matches the regular expression will be scanned.

ComplexRegEx Check Test Logic Example

Refer to the following example to better understand the test logic of the ComplexRegEx type check.

The file A that will be tested contains a word **Server-Side**, and contains the Canadian Social Insurance Number: **046-454-286**.

Create and configure the ComplexRegEx check test logic:

1. Create a **ComplexRegEx** Type check. In the **Report Text** step, in the **False Result and Message** field, select **User Review Required** in the False Result drop-down list.
2. Configure the elements in the check:
    - Select **Yes** for the **IsFindText** attribute.
    - In the Primary section:
        - Select **No** in the drop-down list under the **SearchAll** attribute.
        - Select **No** in the drop-down list under the **CaseSensitive** attribute.
        - Select **Found** in the drop-down list under the **TrueIf** attribute.
        - Select **No** in the drop-down list under the **ListLocation** attribute.
        - Select **FalseResult** in the drop-down list under the **ResultNA** attribute.
        - Enter **1** for the **MustRepeat** attribute.
        - Enter the regular expression **\b[a-zA-Z]+-[a-zA-Z]+\b** in the **Value** field. A word that contains a hyphen can match the regular expression.
    - In the Secondary section:
        - Select **No** in the drop-down list under the **SearchAll** attribute.
        - Select **No** in the drop-down list under the **CaseSensitive** attribute.
        - Select **Found** in the drop-down list under the **TrueIf** attribute.
        - Select **No** in the drop-down list under the **ListLocation** attribute.
        - Enter **1** for the **MustRepeat** attribute.
        - Enter the regular expression **(?<=^|\b)\d{3}([-])\d{3}(\1)\d{3}(?=$|\b)** in the **Value** field. The Social Insurance Number can match the regular expression.
3. Save the check.
4. Run a Compliance Scanner job. The test suite used in this job contains the check configured above.

Review the check test logic:

- In this type of check, if the result of the primary check is True, the secondary check can start for this check. If the result of the primary check is False, the secondary check will not start for this check and the result of this check will be determined by the primary

check. For the **ResultNA** attribute, if **TrueResult** is set as the value of this attribute, the result of this check will be True. If **FalseResult** is set as the value of this attribute, the result of this check will be False. If **NAResult** is set as the value of this attribute, the status of the tested file will be Not Applicable, and Not Applicable will be displayed in the Compliance Guardian report.

- In the primary and secondary check section, we have set **No** for the ListLocation attribute. The location of the instance will not be recorded in the Compliance Guardian database, so the value for **LisLocStatus** is not required to be set.
- In this use case:
    - In the primary check, the value that matches the regular expression in the file is **Server-Side**, so the result is Found. According to the logic set of the **TrueIf** attribute, the result of the primary check is True. So the secondary check will be used.
    - In the secondary check, the value that matches the regular expression in the file is **046-454-286**, so the result is Found. According to the logic set of the **TrueIf** attribute, the result of the secondary check is False. So the result of this check is False. According to the setting in **False Result and Message** in the **Report Text** step, the returning status is **User Review Required**, which will be displayed in the Compliance Guardian report.

Dictionary Type Check

The Dictionary type check groups **FindText** check and **RegularExpression** check in one check, and take the **AND** operation on the search result. The dictionary settings enable end users to define multiple checking in each **FindText** or **RegularExpression** section. The following section provides a general introduction about configuring attributes for this type of check, as well as a test example for you to understand the test logic.

Configuring Attributes for Dictionary Type Check

Configure the attributes for the Dictionary type check according to the instructions in the following sections.

Dictionary

Configure the following attribute:

- **BreakIfFound** – Select **Yes** or **No** for this attribute. If **Yes** is selected, the scan will stop when one instance is found (to save scan time). If **No** is selected, the scan will only stop when all instances are found.

FindText

This section is optional. Configure the following attributes:

- Select the checkbox before **FindText**, the following attributes appear:
  - **TrueIf** – Specify the condition when the check result is True. If **Found** is selected in the drop-down list under the **TrueIf** attribute, when finding an instance, the check result of this check will be True. If **NotFound** is selected in the drop-down list under the **TrueIf** attribute, when finding an instance, the check result of this check will be False.
  - **SearchAll** – Specify whether or not to check the comments and scripts.
  - **ListLocation** – Specify whether or not to record the instance's location in the Compliance Guardian database. If **Yes** is selected in the drop-down list under the **ListLocation** attribute, then every location of the instance found will be recorded in the Compliance Guardian database. If **No** is selected in the drop-down list under the **ListLocation** attribute, the check continues, but the locations of the instances found will not be recorded in the database.
  - **ListLocStatus** – Specify the status for the instance that is found. The status will be recorded in the Compliance Guardian database. Note that if the status set for True Result or False Result is **Failed** in the **Report Text** step, the value for the **ListLocStatus** will be **Fail**, and the value cannot be changed.
  - **CaseSensitive** – Specify if the text being tested for must match the case exactly.
  - **CompareType** – Select **MustContain** or **MustEqual** for this attribute.
- **Dictionary** – Configure the following attributes:
  - **Separator** – Specify a separator if multiple values are specified.
  - **Value** – Define one or more values for the test, use the separator specified before to separate the values.

  Select the delete button ( ) to delete this **Dictionary** check rule. Select **Add Another Dictionary** to add another rule.

Regex

This section is optional. Configure the following attributes:

- Select the checkbox before **Regex**, the following attributes appear:
  - **TrueIf** – Specify the condition when the check result is True. If **Found** is selected in the drop-down list under the **TrueIf** attribute, when finding an instance, the check result of this check will be True. If **NotFoun**d is selected in the drop-down list under the **TrueIf** attribute, when finding an instance, the check result of this check will be False.
  - **SearchAll** – Specify whether or not to check the comments and scripts.

- **ListLocation** – Specify whether or not to record the instance's location in the Compliance Guardian database. If **Yes** is selected in the drop-down list under the **ListLocation** attribute, then every location of the instance found will be recorded in the Compliance Guardian database. If **No** is selected in the drop-down list under the **ListLocation** attribute, the check continues, but the locations of the instances found will not be recorded in the database.
- **ListLocStatus** – Specify the status for the instance that is found. The status will be recorded in the Compliance Guardian database. Note that if the status set for True Result or False Result is **Failed** in the **Report Text** step, the value for the **ListLocStatus** attribute will be **Fail**, and the value cannot be changed.
- **CaseSensitive** – Specify if the text being tested for must match the case exactly.
- **CustomCheck** – Enter a CustomCheck name for this attribute. The CustomCheck is used to calculate the check digit on the result of the regular expressions, in order to validate the result. Refer to Appendix H – Using CustomCheck in Compliance Guardian for the details on CustomCheck. This is optional.

- **Dictionary** – Configure the following attributes:
  - **Separator** – Specify a separator if multiple values are specified.
  - **Value** – Define one or more values for the test, use the separator specified before to separate the values.

  Select the delete button ( ) to delete this **Dictionary** check rule. Select **Add Another Dictionary** to add another rule.

- **Filter** – This is optional. Select the checkbox before **Filter**, the **Text** section and the **Regex** section appear:
  - **Text** – Select the checkbox before Text, and configure the following attributes:
    - **CaseSensitive** – Specify if the element being tested for must match the case exactly.
    - **Separator** – Specify a separator if multiple values are specified.
    - **Value** – Define one or more values for the test, and use the separator specified before to separate the values. If the scanned result that matches the specified regular expression exactly matches the value specified here, this result will be filtered out.

    Select **Add Another Text** to add another Text filter check rule. Select the delete button ( ) to delete this filter check rule.

  - **Regex** – Select the checkbox before Text, and configure the following attributes:
    - **CaseSensitive** – Specify if the element being tested for must match the case exactly.
    - **Separator** – Specify a separator if multiple values are specified.

- **Value** – Define a regular expression. If the scanned result that matches the specified regular expression also matches the regular expression specified here, this result will be filtered out.

Select **Add Another Regex** to add another Text check rule. Select the delete button ( ) to delete this Regex filter check rule.

Dictionary Check Test Logic Example

Refer to the following example for better understanding the test logic of the Dictionary type check.

The file A that will be tested contains a word **Server**, and contains the Canadian Social Insurance Number: **046-454-286**.

Create and configure the Dictionary check test logic:

1. Create a **Dictionary** Type check. In the **Report Text** step, in the **True Result and Message** field, select **Passed** in the True Result drop-down list.
2. Configure the elements in the check:
    - Select **Yes** in the drop-down list under the **BreakIfFound** attribute.
    - In the **FindText** section:
        - Select **Found** in the drop-down list under the **TrueIf** attribute.
        - Select **Yes** in the drop-down list under the **SearchAll** attribute.
        - Select **No** in the drop-down list under the **ListLocation** attribute.
        - Select **MustContain** in the drop-down list under the **CompareType** attribute.
        - Select **No** in the drop-down list under the **CaseSensitive** attribute.
        - Enter **server** in the **Value** field.
    - In the **Regex** section:
        - Select **Found** in the drop-down list under the **TrueIf** attribute.
        - Select **Yes** in the drop-down list under the **SearchAll** attribute.
        - Select **Yes** in the drop-down list under the **ListLocation** attribute.
        - Select **Note** in the drop-down list under the **ListLocStatus** attribute.
        - Select **No** in the drop-down list under the **CaseSensitive** attribute.
        - Enter the regular expression **(?<=^|\b)\d{3}([-])\d{3}(\1)\d{3}(?=$|\b)** in the **Value** field. The Social Insurance Number can match the regular expression.
3. Save the check.
4. Run a Compliance Scanner job. The test suite used in this job contains the check configured above.

Review the check test logic:

- For the **CompareType** attribute in **FindText** section, if **MustEqual** is selected for this attribute, then the content must be exactly equal to the value we specified in order to be found. If **MustContain** is selected for this attribute, the content will be found if the content contains the value we specified. For example, if the tested file contains the word **Front-end**, and we select **MustEqual** for the **CompareType** attribute with the value specified as **end**, then the word **Front-end** will not be found, but if we select **MustContain** for the **CompareType** attribute, the word **Front-end** will be found.
- See the logic set in the **FindText** section, the value that will be searched for in the file is **server**, so the result is Found. According to the logic of the **TrueIf** attribute, the result of the **FindText** section is True.
- According to the logic of the **BreakIfFound** attribute, if one instance is found, the scan will stop, so the test of the Regex section will not be continued.
- So the result of this check is True. According to the setting in **True Result and Message** in the **Report Text** step, the returning status is **Passed**, which will be displayed in the Compliance Guardian report.

Cookie Type Check

The Cookie type check is used to validate cookie domain and expiration dates. The following section provides a general introduction about configuring attributes for this type of check.

Configuring Attributes for Cookie Type Check

Configure the attributes for the Cookie type check according to the instructions in the following sections.

Cookie

Configure the following attributes under this element:

- **ThirdParty** – Instruct the scan engine to check if the cookie is from a third party.
- **PrivacyLinReq** – Instruct the scan engine (based on the cookie condition) to check for a privacy link.
- **ResultNA** – Specify a result when the specified element is not found. If **TrueResult** is selected, then if the specified element is not found, the True result will be returned; if **FalseResult** is selected, then if the specified element is not found, the False result will be returned. If **NAResult** is selected, then if the specified element is not found, the status of the tested file will be **Not Applicable**, which will be displayed in the Compliance Guardian report. This is basically stating that you have the option to set the result to **Not Applicable** if none of the elements are found.
- **Expires** – Instruct the testing core to check when the cookie expires in N seconds.

- **cPIITDF** – Instruct the testing core to use the specified check to identify PII in the webpage.
- **CType** – Identify the cookie type to test for (allowed values 1, 2, 3):
    - **1** – Single session. This tier encompasses any use of single session Web measurement and customization technologies.
    - **2** – Multi-session without PII. This tier encompasses any use of multi-session Web measurement and customization technologies when no PII is collected (including when the agency is unable to identify an individual as a result of its use of those technologies).
    - **3** – Multi-session with PII. This tier encompasses any use of multi-session Web measurement and customization technologies when PII is collected (including when the agency is able to identify an individual as a result of its use of those technologies).
- **PrivacyLink** – Enter a value in this field, if the privacy link in the file contains the value, this check will be True.

Cookie Check Test Logic Example

Refer to the following example for better understanding the test logic of the Cookie type check. A user's session cookie will be tested. Create and configure the Cookie check test logic:

1. Create a Cookie type check. In the **Report Text** step, in the **True Result and Message** field, select **Passed** in the True Result drop-down list.
2. Configure the elements in the check:
    - Select **True** in the drop-down list under the **ThirdParty** attribute.
    - Select **True** in the drop-down list under the **PrivacyLinkReq** attribute.
    - Select **TrueResult** in the drop-down list under the **ResultNA** attribute.
    - Select **1** in the drop-down list under the **CType** attribute.
    - Enter **privacy.htm** in the **PrivacyLink** field.
3. Save the check.
4. Run a Compliance Scanner job. The test suite used in this job contains the check configured above.

Review the check test logic:

- If the cookie is from a third party, the check result for this attribute will be True.
- Since we have selected **True** in the drop-down list under the **PrivacyLinkReq** attribute, and specified **privacy.htm** in the **PrivacyLink** field, so if the privacy link of the cookie contains **privacy.htm**, the check result for this attribute will be True.

- In this use case, if the check result for the **ThirdParty** attribute is True, and the check result for the **PrivacyLinkReq** attribute is True, the check result of this check will be True.

SSL Type Check

The SSL type check is used to validate HTTPS protocol encryption levels. The following section provides a general introduction about configuring attributes for this type of check, as well as a test example for you to understand the test logic.

Configuring Attributes for SSL Type Check

Configure the attributes for the SSL type check according to the instructions in the following sections.

SSL

Configure the following attributes under this element:

- **ElementName** – This is the element that will be tested.
- **CaseSensitive** – Instruct the testing core if the element name being tested for must match the case exactly.
- **ResultNA** – Specify a result when the specified element is not found. If **TrueResult** is selected, then if the specified element is not found, the True result will be returned. If **FalseResult** is selected, then if the specified element is not found, the False result will be returned; if **NAResult** is selected, then if the specified element is not found, the status of the tested file will be **Not Applicable**, which will be displayed in the Compliance Guardian report. In other words, you have the option to set the result to **Not Applicable** if none of the elements are found.
- **AttrName** – This is the attribute that will be tested.
- **AttrCaseSensitive** – Instruct the testing core if the attribute name being tested for must match the case exactly.
- **MinLevel** – Represent the minimum HTTPS protocol encryption level required by the check.

TextCompare

This section is optional. Select the checkbox before this element, and the following attributes appear:

- **CompareType** – Specify a compare type. The attributes for CompareType are **MustContain**, **MustNotContain**, **MustEqual** ,and **MustNotEqual**.
- **Separator** – Specify a separator if multiple values are specified.
- **CaseSensitive** – Specify if the attribute being tested for must match the case exactly.
- **Value** – Define one or more values for the test, use the separator specified before to separate the values.

Select the delete button ( ) to delete this check rule. Select **Add Another TextCompare** to add another rule.

TextCompare Check Test Logic Example

Refer to the following example for better understanding the test logic of the SSL type check. The webpage that will be scanned contains a node: *<input type="password" name="Passwd" id="Passwd">*. Create and configure the SSL check test logic:

1. Create a **SSL** Type check. In the **Report Text** step, in the **True Result and Message** field, select **Passed** in the True Result drop-down list
2. Configure the elements in the check:
    - Specify the element name **input** for the **ElementName** attribute.
    - Select **No** in the drop-down list under the **CaseSensitive** attribute.
    - Select **ResultNA** in the drop-down list under the **ResultNA** attribute.
    - Specify the attribute name **id** for the **AttrName** attribute.
    - Select **No** in the drop-down list under the **AttrCaseSensitive** attribute.
    - Enter **128** for the **MinLevel** attribute.
    - Select the checkbox before **TextCompare**, and configure the following attributes:
        - Select **MustContain** in the drop-down list under the **CompareType** attribute.
        - Enter **;** as the separator.
        - Select **No** in the drop-down list under the **CaseSensitive** attribute.
        - Enter **Pass** in the Value field.
3. Save the check.
4. Run a Compliance Scanner job. The test suite used in this job contains the check configured above.

Review the check test logic:

- The webpage contains the node <input type="password" name="Passwd" id="Passwd">, the value of the attribute **id** contains the value **Pass**, so the webpage meets the condition.
- If the minimum HTTPS protocol encryption level of the webpage is higher than 128, the result of this check will be True, or the result will be False.

WebBeacons Type Check

The WebBeacons type check is used to detect if Web Beacons are present on a webpage. The following section provides a general introduction about configuring attributes for this type of check, as well as a test example for you to understand the test logic.

Configuring Attributes for WebBeacons Type Check

Configure the attributes for the WebBeacons type check according to the instructions in the following sections.

WebBeacons

Configure the following attributes under this element:

- **ElementName** – Specify the element name that will be tested.
- **CaseSensitive** – Specify if the element name being tested for must match the case exactly.
- **ResultNA** – Specify a result when the specified element is not found. If **TrueResult** is selected, then if the specified element is not found, the True result will be returned; if **FalseResult** is selected, then if the specified element is not found, the False result will be returned; if **NAResult** is selected, then if the specified element is not found, the status of the tested file will be **Not Applicable**, which will be displayed in the Compliance Guardian report. This is basically stating that you have the option to set the result to **Not Applicable** if none of the elements are found.
- **AttrName** – Specify the attribute name that will be tested.
- **AttrCaseSensitive** – Specify if the attribute name being tested for must match the case exactly.
- **ValidWhen** – This is used to indicate if the result is valid when the condition is one of two values: True or False.

Elements

Configure the following attribute under this element:

- **Scope** – There are two values for this attribute: **All** and **One**. If **One** is selected, the scan will stop when one instance is found (to save scan time). If **All** is selected, the scan will only stop when all instances are found.

ListLoc

Configure the following attributes under this element:

- **Type** – There are two values for this attribute, **Valid** and **Invalid**. All elements that are considered valid or invalid are stored to the database (the Location).
- **Status** – This is used to indicate the disposition of the element and the severity selected by the user. Note that in the **Report Text** step, if the status set for True Result or False Result is **Failed**, the value for the **Status** attribute will be **Fail**, and the value cannot be changed.

DomainExclude

Configure the following attributes under this element:

- **Separator** – Specify a separator if multiple values are specified.
- **Value** – Enter one or more domains here, the links that are located in these domains will not be checked. Use the separator specified before to separate the values.

WebBeacons Check Test Logic Example

Refer to the following example to better understand the test logic of the WebBeacons type check. The webpage that will be tested contains the following nodes:

```
<html>
<body>
<div><img src="http://www.hello.com/img/img01.jpeg"/></div>
</body>
</html>
```

The domain of this webpage is **simer.com**.

Create and configure the WebBeacons check test logic:

1. Create a **WebBeacons** Type check. In the **Report Text** step, in the **True Result and Message** field, select **Passed** in the True Result drop-down list.
2. Configure the elements in the check:
    - In the **WebBeacons** section:
        - Specify **img** for the **ElementName** attribute.
        - Select **No** in the drop-down list under the **CaseSensitive** attribute.
        - Select **TrueResult** in the drop-down list under the **ResultNA** attribute.
        - Specify **src** for the **AttrName** attribute.
        - Select **No** in the drop-down list under the **AttrCaseSensitive** attribute.
        - Select **Yes** in the drop-down list under the **ValidWhen** attribute.
    - In the **Elements** section:
        - Select **One** in the drop-down list under the **Scope** attribute.
    - In the **ListLoc** section:
        - Select **Invalid** in the drop-down list under the **Type** attribute.
        - Select **Warn** in the drop-down list under the **Status** attribute.

- In the **DomainExclude** section:
    - Enter **http://www.hello.com** in the **Value** field under the **DomainExclude** attribute.

3. Save the check.
4. Run a Compliance Scanner job. The test suite used in this job contains the check configured above.

Review the check test logic:

- According to the logic set in the **WebBeacons** section, the node meets the condition.
- The domain of this webpage is **simer.com**, while the domain of the link in the node is **hello.com**. But according to the value we specified for the **DomainExclude** attribute, the domain **hello.com** will not be checked. So the result of this check is True.
- According to the logic set for the **ValidWhen** attribute as well as the logic set in the **ListLoc** section, the location of this node will not be recorded in the Compliance Guardian database.
- According to the setting in **True Result and Message** in the **Report Text** step, the returning status is **Passed**, which will be displayed in the Compliance Guardian report.

FindFile Type Check

The FindFile type check is used to find a specified file. The following section provides a general introduction about configuring attributes for this type of check, as well as a test example for you to understand the test logic.

Configuring Attributes for FindFile Type Check

Configure the following attributes:

- **TrueIf** – Specify the condition when the check result is **True**. If **Yes** is selected in the drop-down list under the **TrueIf** attribute, when finding an instance, the check result of this check will be True; If **No** is selected in the drop-down list under the **TrueIf** attribute: when finding an instance, the check result of this check will be False.
- **Path** – Enter the file's relative path or full path.

FindFile Check Test Logic Example

Refer to the following example to better understand the test logic of the FindFile type check. Create and configure the FindFile check test logic:

1. Create a **FindFile** type check. In the **Report Text** step, in the **True Result and Message** field, select **Passed** in the True Result drop-down list.

2. Configure the elements in the check:
    - Select **Yes** in the drop-down list under the **TrueIf** attribute.
    - Enter *http://sharepoint.avepoint.net/file/findthis.txt* for the Path attribute.
3. Save the check.
4. Run a Compliance Scanner job. The test suite used in this job contains the check configured above.

Review the check test logic:

- If the file **findthis.txt** exists, the result will be Found. Note that if you enter a relative URL **file/findthis.txt** for the Path attribute, by default, the full path of this file that Compliance Guardian will scan is **http://host name (IP address) + relative URL**. For example: if the URL of the selected site that will be performed a Compliance Guardian job is *http://avepoint2010a:10086/sites/1229url/0112site*, and the relative URL specified for the **Path** attribute in this check is **file/findthis.txt**, then CCE will scan the URL *http://avepoint2010a/file/findthis.txt* to check if the file exists.
- According to the logic set in the **TrueIf** attribute, the result of this check will be True.
- According to the setting in **True Result and Message** in the **Report Text** step, the returning status is **Passed**, which will be displayed in the Compliance Guardian report.

LinkValidation Type Check

The LinkValidation check is a check type that tests for the validity of links or bookmarks within any content that can contain links or bookmark references. The following section provides a general introduction about configuring attributes for this type of check, as well as a test example for you to understand the test logic.

Configuring Attributes for LinkValidation Type Check

Configure the attributes for the LinkValidation type check according to the instructions in the following sections.

LinkValidation

Configure the following attributes under this element:

- **ValidWhen** – This is used to indicate if the result is valid when the condition is one of two values: **True** or **False**.
- **TrueIf** – There are two values for this attribute: **All** and **One**. If **One** is selected, the scan will stop when one instance is found (to save scan time). If **All** is selected, the scan will only stop when all instances are found.
- **ResultNA** – Specify a result when no link is found. If **TrueResult** is selected, then if no link is found, the True result will be returned. If **FalseResult** is selected, then if no link is found, the False result will be returned. If **NAResult** is selected, then if no link is found,

the status of the tested file will be **Not Applicable**, which will be displayed in the Compliance Guardian report. In other words, you have the option to set the result to **Not Applicable** if none of the links are found.

- **ValidateBookmarks** – Select **True** or **False** for this attribute. If **True** is selected, the check will check whether the bookmarks work. If **False** is selected, the check will not check the bookmarks.
- **GetAllowCallHead** – Select **True** or **False** for this attribute. If **True** is selected, the link will be checked using the HEAD method, if the corresponding server does not support the HEAD method, the GET method will be used. If **False** is selected, the link will be checked using the HEAD method, if the corresponding server does not support the HEAD method, the GET method will not be used.

ListLoc

Configure the following attributes under this element:

- **Type** – There are two values for this attribute, **Valid** and **Invalid**. All elements that are considered valid or invalid are stored to the database (the Location).
- **Status** – This is used to indicate the disposition of the element and the severity selected by the user. In the **Report Text** step, if the status set for True Result or False Result is **Failed**, the value for the Status attribute will be **Fail**, and the value cannot be changed.

TextCompare

Configure the following attributes under this element:

- **CompareType** – Specify a compare type. The attributes for CompareType are **MustContain**, **MustNotContain**, **MustEqual**, and **MustNotEqual**.
- **Separator** – Specify a separator if multiple values are specified.
- **CaseSensitive** – Specify if the attribute name being tested for must match the case exactly.
- **Value** – Define one or more values for the test, use the separator specified before to separate the values.

Select the delete button (✕) to delete this check rule. Select **Add Another TextCompare** to add another rule.

LinkValidation Check Test Logic Example

Refer to the following example to better understand the test logic of the LinkValidation type check. The selected file 1 will be tested. It contains two links, one of the two links contain a character A, while the other one does not.

Create and configure the LinkValidation check test logic:

1. Create a LinkValidation type check. In the **Report Text** step, in the **True Result and Message** field, select **Passed** in the **True Result** drop-down list.
2. Configure the **LinkValidation** section:
    - Select **True** in the drop-down list under the **ValidWhen** attribute.
    - Select **All** in the drop-down list under the **TrueIf** attribute.
    - Select **ResultNA** in the drop-down list under the **ResultNA** attribute.
    - Select **True** in the drop-down list under the **ValidateBookmarks** attribute.
3. Configure the **ListLoc** section:
    - Select **Invalid** in the drop-down list under the **Type** attribute.
    - Select **Warn** in the drop-down list under the **Status** attribute.
4. Configure the **TextCompare** section:
    - Select **MustContain** in the drop-down list under the **CompareType** attribute.
    - Enter **,** as the separator.
    - Select **No** in the drop-down list under the **CaseSensitive** attribute.
    - Enter **A,B** in the **Value** field.
5. Save the check.
6. Run a Compliance Scanner job. The test suite used in this job contains the check configured above.

Review the check test logic:

- See the **TextCompare** section: since we have entered **A,B** in the **Value** field in this check, it means that the link that contains A or B will be tested. So the link that contains A in the selected file 1 will be tested by this check.
- See the **LinkValidation** section and **ListLoc** section: we have selected **Valid** for the **ValidWhen** attribute in the **LinkValidation** section, and have selected Invalid for the **Type** attribute in **ListLoc** section, so the location of the link will not be recorded in the Compliance Guardian database.
- See the **ValidateBookmarks** attribute in the **LinkValidation** section: since we have selected **True** for the **ValidateBookmarks** attribute, the check will check whether the bookmarks in the file 1 work. If one of the bookmarks in the file does not work, this check is False.

  Although the check result in other field is True, if the check result of **ValidateBookmarks** attribute field is False, the check result of this check is False.

FileProperty Type Check

The FileProperty check is a check type that test for the file properties, it is specifically designed for use with the MobileOK standard. The following section provides a general introduction about configuring attributes for this type of check, as well as a test example for you to understand the test logic.

Configuring Attributes for FileProperty Type Check

Configure the attributes for the FileProperty type check according to the instructions in the following sections.

FileProperty

Configure the following attributes under this element:

- **TrueIf** – There are two values for this attribute: **All** and **One**. If **One** is selected, the scan will stop when one instance is found (to save scan time). If **All** is selected, the scan will only stop when all instances are found.
- **ValidWhen** – This is used to indicate if the result is valid when the condition is one of two values: **True** or **False**

ListLoc

Configure the following attributes under this element:

- **Type** – There are two values for this attribute, **Valid** and **Invalid**. All elements that are considered valid or invalid are stored to the database (the Location).
- **Status** – This is used to indicate the disposition of the element and the severity selected by the user. Note that in the **Report Text** step, if the status set for True Result or False Result is **Failed**, the value for the Status attribute will be **Fail**, and the value cannot be changed.

Size

Configure the following attributes under this element:

- **MaxValue** – Specify a value as the maximum size, select a unit in the drop-down list.

Type

Configure the following attributes under this element:

- **CompareType** – Specify a compare type. The attributes for **CompareType** are **MustContain**, **MustNotContain**, **MustEqual**, and **MustNotEqual**.
- **Separator** – Specify a separator if multiple values are specified.
- **CaseSensitive** – Specify if the element being tested for must match the case exactly.

- **Value** – Define one or more Content-types for the test, use the separator specified before to separate the values.

Filter

This element is optional. Select the checkbox before **Filter**, and configure the following attributes under this element:

- **CompareType** – Specify a compare type. The attributes for **CompareType** are **MustContain**, **MustNotContain**, **MustEqual**, and **MustNotEqual**.
- **Separator** – Specify a separator if multiple values are specified.
- **CaseSensitive** – Specify if the element being tested for must match the case exactly.
- **Value** – Define one or more values for the test, use the separator specified before to separate the values.

Select the delete button (✕) to delete this check rule. Select **Add Another Filter** to add another rule.

FileProperty Check Test Logic Example

Refer to the following example to better understand the test logic of the FileProperty type check. In this example, we are testing file 1.

Create and configure the FileProperty check test logic:

1. Create a FileProperty type check. In the **Report Text** step, in the **False Result and Message** field, select **User Review Required** in the False Result drop-down list.
2. Configure the **FileProperty** section:
   - Select **All** in the drop-down list under the **TrueIf** attribute.
   - Select **True** in the drop-down list under the **ValidWhen** attribute.
3. Configure the **ListLoc** section:
   - Select **Invalid** in the drop-down list under the **Type** attribute.
   - Select **Warn** in the drop-down list under the **Status** attribute.
4. Configure the **Size** section:
   - Enter **10** in the **MinValue** field, select **KB** as the unit.
   - Enter **20** in the **MaxValue** field, select **KB** as the unit.
5. Configure the **Type** section:
   - Select **MustContain** in the drop-down list under the **CompareType** attribute.
   - Enter **;** as the separator.
   - Select **No** in the drop-down list under the **CaseSensitive** attribute.

- Enter **text/html;text/xml;mage/gif;image/jpeg** in the **Value** field.

6. Select the checkbox before **Filter**, configure the **Filter** section:
   - Select **MustNotContain** in the drop-down list under the **CompareType** attribute.
   - Enter **;** as the separator.
   - Select **No** in the drop-down list under the **CaseSensitive** attribute.
   - Enter **A;B** in the **Value** field.
7. Save the check. Run a Compliance Scanner job, the test suite used in this job contains the check configured above.

Review the check test logic:

- In the **Filter** section, we only compare the values specified with the **src** attribute's value in the **img** element, the **href** attribute's value in the **link** element, and the **data** attribute's value in the **object** element in the selected file.

  In this case, we specified **A;B** in the Value field, and selected **MustNotContain** for the **CompareType** value. The **img** elements whose values of the **src** attributes do not contain the characters **A** and **B** will be tested; the **link** elements whose values of the **href** attributes do not contain the characters **A** and **B** will be tested. The **object** elements whose values of the **data** attributes do not contain the characters A and B will tested.

- In the **Type** section, after the check in the **Filter** section, the **img** elements, **link** elements, and the **object** elements that meet the **Filter** check section (in this case, the **img** elements whose values of the **src** attributes do not contain the characters **A** and **B**, the **link** elements whose values of the **href** attributes do not contain the characters **A** and **B**, and the **object** elements whose values of the **data** attributes do not contain the characters **A** and **B** meet the **Filter** check section) will be taken to the check in the **Type** section.

  In this case, if one of the Content-types of the file or the three kinds of attributes'(**src**, **href** and **data**) values is not **text/html**, **text/xml**, **mage/gif** or **image/jpeg**, the check in the **Type** section will be False.

- In the **Size** section, the size = the file size + the size of the **src** attribute's value in the **img** element in the file (the corresponding image's size) + the size of the **href** attribute's value in the **link** element in the file (the corresponding linked file's size) + the size of the **data** attribute's value in the **object** element in the file (the corresponding image's size). If the size is not in the range we specified in the **Size** section of this check, this check result of this section will be False.
- If the result of the **Filter** check or **Size** check is False, the check result of this check is False.
- If the check result of this check is False, see the **ValidWhen** attribute in the **FileProperty** section. We have selected **Valid**, so the result of this attribute is Invalid. In the **ListLoc**

section, the result for **ValidWhen** is Invalid, so the check status will be **Warn**, and this check status will be recorded in the Compliance Guardian database. Users cannot see the status in the Compliance Guardian GUI.

According to the settings in **False Result and Message** in the **Report Text** step, the returning status is **User Review Required**, which will be displayed in the Compliance Guardian report.

Configuring CCC or MCC File Attributes

Refer to the following sections for configuring Content Compliance Collection (CCC) and Metadata Compliance Collection (MCC) files.

Content Compliance Collection (CCC) File Body Configuration

Configure the following attributes for the Content Compliance Collection (CCC) file.

RiskFormula

Select a Raw Risk Formula, Stepped Risk Formula, and a Weighted Risk Formula in the corresponding drop-down list. You can create a new Risk Formula by selecting **New Formula** in the drop-down list. A pop-up window will appear if you select **New Formula**. In the pop-up window, enter the name and the optional description for the Risk formula, define your own formula, and select **OK**. The new Risk Formula then will be created.

RunAsTestGroup

Group the specified checks. The checks can test files according to one checkpoint.

- Select the checkbox before the **RunAsTestGroup** element, and then configure the following attributes:
  - **Name** – Enter a name for the test group.
  - **DatabaseField** – This is the location in the Compliance Guardian database where the scan result data is stored. Compliance Guardian will automatically specify the location for storing data.
  - **ContentType** – Select the content types that will be scanned. If you do not select the content types, all the file content types that are supported to be scanned in Compliance Guardian will be scanned. Refer to the following steps for selecting the content types:
    - Select the text field under the **ContentType** attribute, a pop-up window appears.
    - In the pop-up window, select the checkbox before the desired content types. And then select **OK**.

Select the delete button ( ) to delete the **RunAsTestGroup** check rule.

- **Policy URL** – Specify a URL that will link to a website defining rules for how checks in this check group will test files.
- **Description** – Enter the description for the test group. In Scan Result of Compliance Guardian report, the description will display in the file's corresponding detailed report.

- **SubCheck** – Configure the following attributes for this element:
  - **CheckName** – Select a check. Refer to the following steps for selecting the check:
    - Select the text field under the **CheckName** attribute, a pop-up window appears.
    - In the pop-up window, select the radio button before the desired check, and then select **OK**.
  - **RunCheck** – If **True** is selected for this attribute, when running a Compliance Guardian job using the test suite, the files will be scanned according to the rule set in this check. If **False** is selected for this attribute, the corresponding check will not be used to scan the files.
  - **RiskLevel(r1)** – The Item Initial Risk value assigned on the initial occurrence of the compliance failure (related to the check being tested for) in the document or stream. Allowed values for **RiskLevel(r1)** are 1-10.
  - **RiskLevel(r2)** – The Item Additional Risk Level factor that the risk level grows at for every additional failure at the check level (for the same type) found in the document or stream. This number is optional where the integer "-1" means ignore the value (allowing to use the third value). If the value is -1 then the factor will be 1. Allowed values are -1 to 10. This is optional.
  - **RiskLevel(r3)** – The Item risk in relation to other checks. This Item is optional. If this number is missing then it is assumed that its value is "1". Allowed values are 1-10. This is optional.

    According to the formulas selected in the **RiskFormula** section, the check will have three risk levels after the scan job.
  - **ContentType** – Select the content types that will be scanned. If you do not select the content types, all the file content types that are supported to be scanned in Compliance Guardian will be scanned. Refer to the following steps for selecting the content types:
    - Select the text field under the **ContentType** attribute, a pop-up window appears.
    - In the pop-up window, select the checkbox before the desired content types. And then select **OK**.

Select the delete button ( ) to delete the **SubCheck** check rule. Select **Add Another Check** to add another rule.

DoRunCheck

The specified checks will not run as a group, they scan files separately. Select the checkbox before the **RunAsTestGroup** element, and then configure the following attributes:

- **CheckName** – Select a check. Select the text field under the **CheckName** attribute. A pop-up window appears. In the pop-up window, select the radio button before the desired check. And then select **OK**.
- **DatabaseField** – This is the location in the Compliance Guardian database where the scan result data is stored. Compliance Guardian will automatically specify the location for storing data.
- **RunCheck** – If **True** is selected for this attribute, when running a Compliance Guardian job using the test suite, the files will be scanned according to the rule set in this check. If **False** is selected for this attribute, the check will not be used to scan the files.
- **RiskLevel** – Specify the risk level for this check.
- **ContentType** – Select the content types that will be scanned. If you do not select the content types, all the file content types that are supported to be scanned in Compliance Guardian will be scanned. Select the text field under the **ContentType** attribute, a pop-up window appears. In the pop-up window, select the radio button before the desired check. And then select **OK**.
- **Role** – Assign a role to the corresponding check.
    - **MaxRow** – After scanned by the check that is assigned to the MaxRow role, the failed files will be reported in the Compliance Guardian File Errors Report, the error type of the failed file is Maximum Row Exception.
    - **DataTable** – After scanned by the check that is assigned to the DataTable role, the locations of the instances that are recorded will be reported in the Compliance Guardian Data Table Report.
    - **Cookie** – The check that is assigned this role can be used for the Cookie check.

Select the delete button (✕) to delete the **DoRunCheck** check rule. Select **Add Another DoRunCheck** to add another rule.

Metadata Compliance Collection File Body Configuration

Configure the following attributes for the Metadata Compliance Collection (MCC) file:

- **Tag** – Specify the name of the metadata element that will be created.
- **PlaceTags** – Define where the tag will be placed. There are four values for this attribute:
    - **0** – Do not add tag to the file and SharePoint
    - **1** – Add the tag to the file only
    - **2** – Add the tag to the file and SharePoint

    - **3** – Add the tag to SharePoint only

- **OverrideUser** – If the specified metadata already exists, select whether or not to override the original metadata.

Select the delete button ( ) to delete the **MCC** check rule.

AllowedTagValues

Configure the following attributes for this element:

- **Priority** – Specify the priority of the tag value. When scanning a file, different checks will return different scan results. This is used to determine which tag value will be added to the file.
- **Value** – Specify the tag value.

Select the delete button ( ) to delete the rule. Select **Add Tag Value** to add another tag value.

CheckIdGroup

Configure the following attributes for this element:

- **CheckName** – Select a check. Select the text field under the **CheckName** attribute, a pop-up window appears. In the pop-up window, select the radio button before the desired check, and then select **OK**.
- **True** – Select a value. If the test of this check evaluates to True, then the tag value will be this one.
- **False** – Select a value. If the test of this check evaluates to False, then the tag value will be this one.
- **N/A** – Select a value. If the test of this check evaluates to N/A, then the tag value will be this one.

Select the delete button ( ) to delete a rule. Select **Add Another Check** to another rule.

Select **Add Another Tag** to add another **MCC** rule.

Appendix C: Supported File Types in Compliance Guardian

Condition	File Type
Supported for Scanning	DOC
	DOCX
	XLS
	XLSX
	PPT
	PPTX
	PDF
	ASP
	ASPX
	HTM
	HTML
	TXT
	XML
	ZIP
	JSP
	PHP
Supported for Adding Tag	DOCX
	XLSX
	PDF
	HTM
	HTML
	ASPX
	PPTX

***Note:** Compliance Guardian currently does not support to add tags to Microsoft Office 2003 files even though they can be scanned and classified after installing a compatibility pack. In the XLS file and the XLSX file, the hidden sheet whose **Visible** property is set to **2 – xlSheetVeryHidden** is also supported to be scanned.

Appendix D: Using the Scan Engine API

Refer to the information below to use the Scan Engine API.

***IMPORTANT**: In this appendix, all references to TDFs refer to checks, and all references to TDF collections refer to test suite.

Initialize the ScanEngine Class

The use of Scan Engine API requires the support of the Compliance Guardian license. The third-party project must be compiled in the operating system where the Compliance Guardian agent is installed, and the third-party project must reference the CCE.Engine.dll in the bin folder of the Compliance Guardian agent installation path.

Currently, the Scan Engine supports to perform the single thread scan. When initializing the ScanEngine class, the constructor requires taking one argument with *ScanSetting* Class. The following coding sample indicates the construction:

```
ScanSetting setting = new ScanSetting();
ScanEngine engine = new ScanEngine(setting);
```

Figure 23: Coding sample 1.

Parameters of the ScanEngine.Scan Method

The following parameters are used for this method for completing the scan progress.

```
public object Scan(string xml, string url, string filePath, IDictionary<string, object> metadata)
```

Figure 27: Parameters used for the ScanEngine.Scan method.

- **string xml** – A string in the XML format, it combines the CCC/MCC XML string with the TDF XML string.
- **string url** – The original URL of the file that will be scanned.
- **string filePath** – The physical storage path of the file that will be scanned.
- **IDictionary<string, object> metadata** – A dictionary which holds the scanned file's related metadata information.

Usage Example

Refer to the following examples to understand how to scan files using CCC (the configuration file of TDF collection used for the Compliance Scanner) and MCC (the configuration file of TDF collection used for the Classification Scanner).

Scan Files Using CCC

To combine files using CCC, complete the following steps:

1. Combine TDFs according to the CCC XML file.


```
<?xml version="1.0" encoding="UTF-8"?>
<!-- Copyright 2001-2012 AvePoint All Rights Reserved. -->
- <CCC IsAccessibility="true">
    <Name>Accessibility Validation for Office Documents (508 and WCAG)</Name>
    <Description>Accessibility Validation for Office Documents</Description>
  - <TDFs>
      <DoRunTDF RiskLevel="3" RunCheck="True" DatabaseField="TDFResult2" tdfID="508_office_1"/>
      <DoRunTDF RiskLevel="3" RunCheck="True" DatabaseField="TDFResult3" tdfID="508_office_17"/>
    </TDFs>
</CCC>
```


Figure 24: The CCC XML file.


```
<?xml version="1.0" encoding="UTF-8"?>
<!-- Copyright 2001-2012 AvePoint All Rights Reserved. -->
- <Tdf TdfID="508_office_1">
  - <ReportText>
      <Name>A.1 All image objects require alternate text.</Name>
      <PolicyURL>http://www.avepoint.com/support/ComplianceGuardian/TestSuites/officeaccessibility.html</PolicyURL>
      <Description>All image objects use alternate text. Alternate text doesn't contain an image or file extension.</Description>
      <True result="Pass">All objects use alternate text.</True>
      <False result="Fail">Failed, one or more object failed the alternative text quality validation</False>
    </ReportText>
  - <Element ValidWhen="True" TrueIf="All" ResultNA="NAResult" CaseSensitive="No" Name="img">
      <ListLoc Status="Fail" Type="Invalid"/>
    - <Attributes>
      - <Attribute CaseSensitive="No" Name="alt" MustExist="Yes" AllowNull="No">
          <TextCompare CaseSensitive="No" Separator="," CompareType="MustNotContain">.emf</TextCompare>
          <TextCompare CaseSensitive="No" Separator="," CompareType="MustNotContain">.jpg</TextCompare>
          <TextCompare CaseSensitive="No" Separator="," CompareType="MustNotContain">.jpeg</TextCompare>
          <TextCompare CaseSensitive="No" Separator="," CompareType="MustNotContain">.wmf</TextCompare>
          <TextCompare CaseSensitive="No" Separator="," CompareType="MustNotContain">.jfif</TextCompare>
          <TextCompare CaseSensitive="No" Separator="," CompareType="MustNotContain">.jpe</TextCompare>
          <TextCompare CaseSensitive="No" Separator="," CompareType="MustNotContain">.png</TextCompare>
          <TextCompare CaseSensitive="No" Separator="," CompareType="MustNotContain">.bmp</TextCompare>
          <TextCompare CaseSensitive="No" Separator="," CompareType="MustNotContain">.dib</TextCompare>
          <TextCompare CaseSensitive="No" Separator="," CompareType="MustNotContain">.rle</TextCompare>
          <TextCompare CaseSensitive="No" Separator="," CompareType="MustNotContain">.gif</TextCompare>
          <TextCompare CaseSensitive="No" Separator="," CompareType="MustNotContain">.emz</TextCompare>
          <TextCompare CaseSensitive="No" Separator="," CompareType="MustNotContain">.wmz</TextCompare>
          <TextCompare CaseSensitive="No" Separator="," CompareType="MustNotContain">.pcz</TextCompare>
          <TextCompare CaseSensitive="No" Separator="," CompareType="MustNotContain">.tif</TextCompare>
          <TextCompare CaseSensitive="No" Separator="," CompareType="MustNotContain">.tiff</TextCompare>
          <TextCompare CaseSensitive="No" Separator="," CompareType="MustNotContain">.cgm</TextCompare>
          <TextCompare CaseSensitive="No" Separator="," CompareType="MustNotContain">.eps</TextCompare>
          <TextCompare CaseSensitive="No" Separator="," CompareType="MustNotContain">.pct</TextCompare>
          <TextCompare CaseSensitive="No" Separator="," CompareType="MustNotContain">.pict</TextCompare>
          <TextCompare CaseSensitive="No" Separator="," CompareType="MustNotContain">.wpg</TextCompare>
        </Attribute>
      </Attributes>
    </Element>
</Tdf>
```


Figure 25: Related TDF - 508.office.a.1.xml.

```
  <?xml version="1.0" encoding="UTF-8"?>
  <!-- Copyright 2001-2012 AvePoint All Rights Reserved. -->
- <Tdf TdfID="508_office_17">
  - <ReportText>
      <Name>J. Page numbering codes must be used for multiple pages.</Name>
      <PolicyURL>http://www.avepoint.com/support/ComplianceGuardian/TestSuites/officeaccessibility.html</PolicyURL>
      <Description>Page numbering codes must be used as opposed to manually typed page numbers.</Description>
      <True result="Pass">Automated Page numbering codes used.</True>
      <False result="HR">Did not find page numbers</False>
    </ReportText>
  - <Element ValidWhen="True" TrueIf="All" ResultNA="NAResult" CaseSensitive="No" Name="word">
      <ListLoc Status="Warn" Type="Invalid"/>
    - <Attributes>
      - <Attribute CaseSensitive="No" Name="ContainsPageNumber" MustExist="Yes" AllowNull="No">
          <TextCompare CaseSensitive="No" Separator="," CompareType="MustContain">true</TextCompare>
        </Attribute>
      </Attributes>
    </Element>
  </Tdf>
```

Figure 26: Related TDF - 508.office.j.xml.

With all CCC XML files and TDFs available, by using the **GetC3sDefinition** method in **ContentComplianceCollectionDefinitionUtility** class, the required argument **string xml** required by **ScanEngine.Scan** can be returned. Refer to Figure 27 for a coding sample.

```
string cccContent = File.ReadAllText(@"C:\ScanEgine Test\508 Office.xml");
List<string> list = new List<string>();
list.Add(File.ReadAllText(@"C:\ScanEgine Test\508.office.a.1.xml"));
list.Add(File.ReadAllText(@"C:\ScanEgine Test\508.office.j.xml"));
ContentComplianceCollectionDefinitionUtility utility = new ContentComplianceCollectionDefinitionUtility();
string xml = utility.GetC3sDefinition(cccContent, list);
```

Figure 27: Coding sample 2.

2. Set the original URL of the file that will be scanned.

```
string url = "http://www.avepoint.com/CG Document/Example.docx";
```

Figure 28: Set the original URL.

3. Set the physical storage path of the file that will be scanned.

```
string testingFile = @"C:\ScanEgine Test\Example.docx";
```

Figure 29: Set the physical storage path.

4. Set the scanned file's related metadata information.

```
Dictionary<string, object> metadata = new Dictionary<string, object>();
metadata["Cookie"] = "no cookie information";
metadata["Key"] = "key value";
```

Figure 30: Set the scanned file's related metadata information.

For detail information of constructing Metadata Dictionary, refer to Scan Metadata.

5. Call the **ScanEngine.Scan** method.

```
object result = engine.Scan(xml, url, testingFile, metadata);
```

Figure 31: Call the ScanEngine.Scan method.

Result Explanation

Figure 32 shows the sample word document containing a picture without Alt Text, which violates the scan language defined in the TDF **508.office.a.1.xml**.

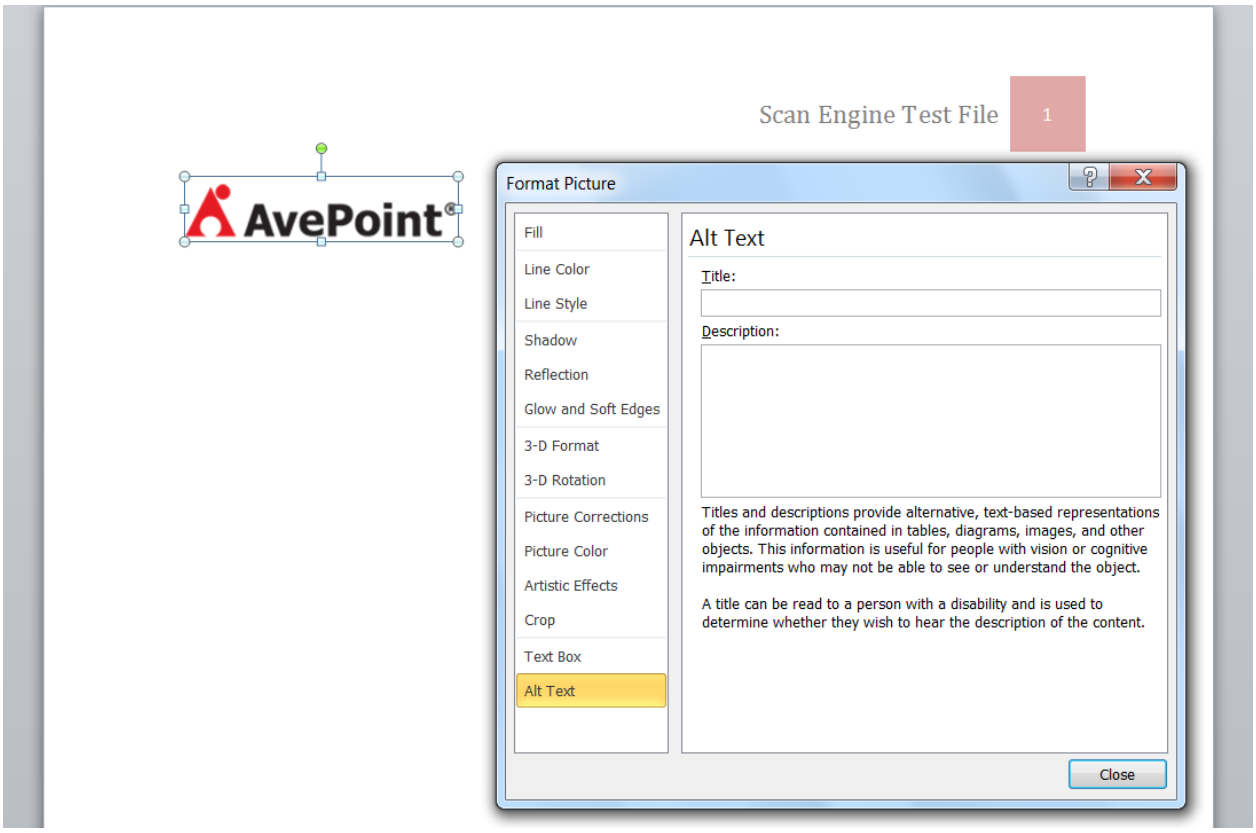

Figure 32: Screenshot of the sample Microsoft Word document 1.

Figure 33 shows the pages in a sample word document with a page number set up. This fulfills the TDF **508.office.j.xml**.

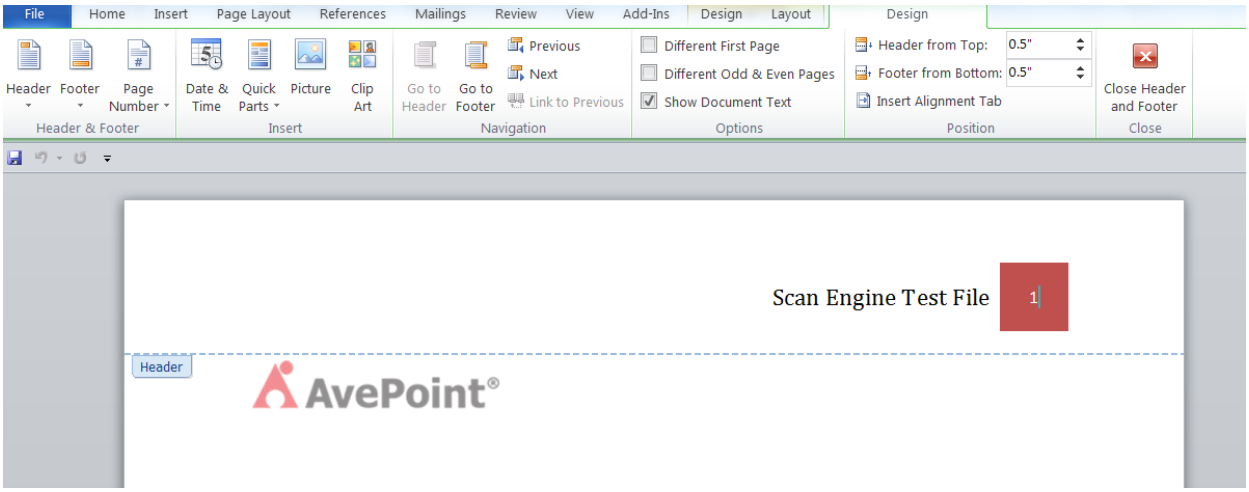

Figure 33: Screenshot of the sample Microsoft Word document 2.

Basing this sample document settings, the scan result status for this word document should be **Fail** (the **GetStatus** value in Figure 34. Furthermore, when drilling down to the details, the status (in the **TestResultList**) for the TDF **508.office.a.1.xml** is **Fail**, and the status for TDF **508.office.j.xml** is **Pass**. Refer to Figure 34, Figure 35, and Figure 36.

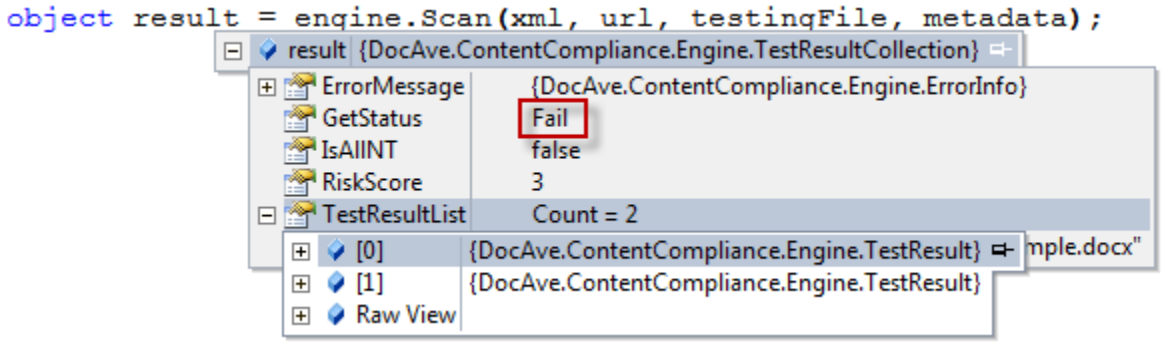

Figure 34: Scanned result 1.

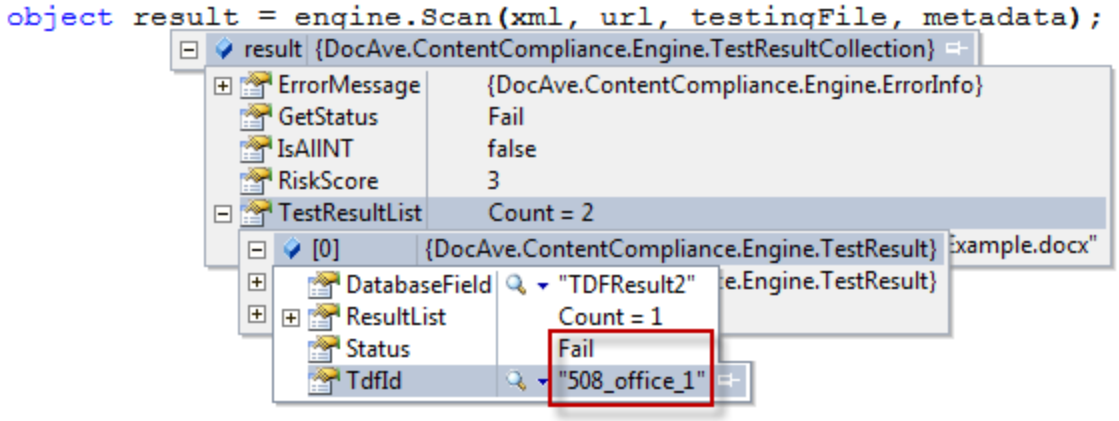

Figure 35: Scanned result 2.

```
object result = engine.Scan(xml, url, testingFile, metadata);
```

result	{DocAve.ContentCompliance.Engine.TestResultCollection}
ErrorMessage	{DocAve.ContentCompliance.Engine.ErrorInfo}
GetStatus	Fail
IsAllNT	false
RiskScore	3
TestResultList	Count = 2
[0]	{DocAve.ContentCompliance.Engine.TestResult}
[1]	{DocAve.ContentCompliance.Engine.TestResult}
DatabaseField	"TDFResult3"
ResultList	Count = 0
Status	Pass
TdfId	"508_office_17"

Figure 36: Scanned result 3.

Scan Files Using MCC

To scan files using MCC, complete the following steps:

1. Combine TDFs according to the MCC XML file.

```xml
<?xml version="1.0" encoding="UTF-8"?>
<!-- Copyright 2001-2013 AvePoint All Rights Reserved. -->
<!-- metadata definition file Created By User via USES positive test to define tag value -->
- <Classification>
    <Name>Classification</Name>
    <Description>Classification Control</Description>
  - <TagName overrideuser="True" placetags="2" tag="Sensitivity">
    - <AllowedTagValues>
        <TagValue priority="0">Low</TagValue>
        <TagValue priority="1">Medium</TagValue>
        <TagValue priority="2">High</TagValue>
      </AllowedTagValues>
    - <automated>
      - <tdfidgroup>
          <tdfid refine="true" na="Low" false="Low" true="Medium" id="Eric_7"/>
          <tdfid refine="false" na="Low" false="Low" true="High" id="Eric_8"/>
        </tdfidgroup>
      </automated>
    </TagName>
  </Classification>
```

Figure 37: The MCC XML file.

The related TDFs:

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- Copyright 2001-2012 AvePoint All Rights Reserved. -->
- <Tdf TdfID="Eric_7">
  - <ReportText>
      <Name>PHI Check</Name>
      <PolicyURL>http://www.avepoint.com/</PolicyURL>
      <Description>No Personal Health Information should be visible.</Description>
      <True result="HR">PHI found</True>
      <False result="Pass">PHI not found</False>
    </ReportText>
    <FindText SearchAll="True" CaseSensitive="No" ListLocStatus="Warn" ListLoc="No"
      TrueIf="Found">HAV</FindText>
</Tdf>
```

Figure 38: HAV.xml.

```
<?xml version="1.0" encoding="UTF-8"?>
<!-- Copyright 2001-2012 AvePoint All Rights Reserved. -->
- <Tdf TdfID="Eric_8">
  - <ReportText>
      <Name>PHI Check</Name>
      <PolicyURL>http://www.avepoint.com/</PolicyURL>
      <Description>No Personal Health Information should be visible.</Description>
      <True result="HR">PHI found</True>
      <False result="Pass">PHI not found</False>
    </ReportText>
    <FindText SearchAll="True" CaseSensitive="No" ListLocStatus="Warn" ListLoc="No"
      TrueIf="Found">HIV</FindText>
</Tdf>
```

Figure 39: HIV.xml.

With all MCC and TDF XMLs available, by using the **GetMCCDefinition** method in **ContentComplianceCollectionDefinitionUtility** class, the required argument **string xml** required by **ScanEngine.Scan** can be returned. Refer to Figure 40 for an example.

```
string mccContent = File.ReadAllText(@"C:\ScanEngine Test\MetadataDefinition.xml");
List<string> list = new List<string>();
list.Add(File.ReadAllText(@"C:\ScanEgine Test\HAV.xml"));
list.Add(File.ReadAllText(@"C:\ScanEgine Test\HIV.xml"));
ContentComplianceCollectionDefinitionUtility utility = new ContentComplianceCollectionDefinitionUtility();
string xml = utility.GetMCCDefinition(mccContent, list);
```

Figure 40: Coding sample 3.

2. Set the original URL of the file that will be scanned.

```
string url = "http://www.avepoint.com/CG Document/MCCExample.docx";
```

Figure 41: Set the original URL.

3. Set the physical storage path of the file that will be scanned.

```
string testingFile = @"C:\ScanEgine Test\MCCExample.docx";
```

Figure 42: Set the physical storage path.

4. Set the scanned file's related metadata information.

```
Dictionary<string, object> metadata = new Dictionary<string, object>();
metadata["Cookie"] = "no cookie information";
metadata["Key"] = "key value";
```

Figure 43: Set the scanned file's related metadata information.

5. Call the **ScanEngine.Scan** method.

```
object result = engine.Scan(xml, url, testingFile, metadata);
```

Figure 44: Call the ScanEngine.Scan method.

Result Explanation

Refer to Figure 45 for a sample of the Microsoft Word document.

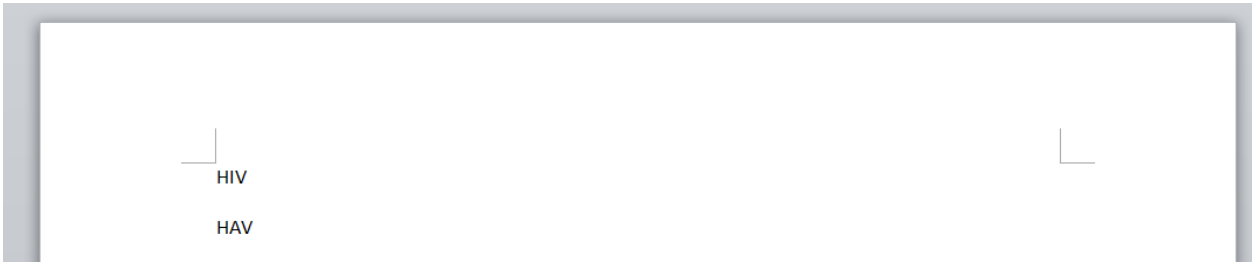

Figure 45: Screenshot of the sample Microsoft Word document 3.

Figure 45 shows the sample word document containing sensitive information **HIV** and **HAV**. According to the Language defined in the MCC's TDF **HAV.xml**, the **true** result for **HAV.xml** was set with the value **Medium**, when the scan engine found **HAV**, **TagValue** will be set as **Medium**. However, as what was defined in the MCC, since the value **High** for **HIV** has a higher priority, when the scan engine found **HIV** in the document, the final value for **TagValue** was overwritten by **High**. In this case, the scan result will be shown as the screenshot below.

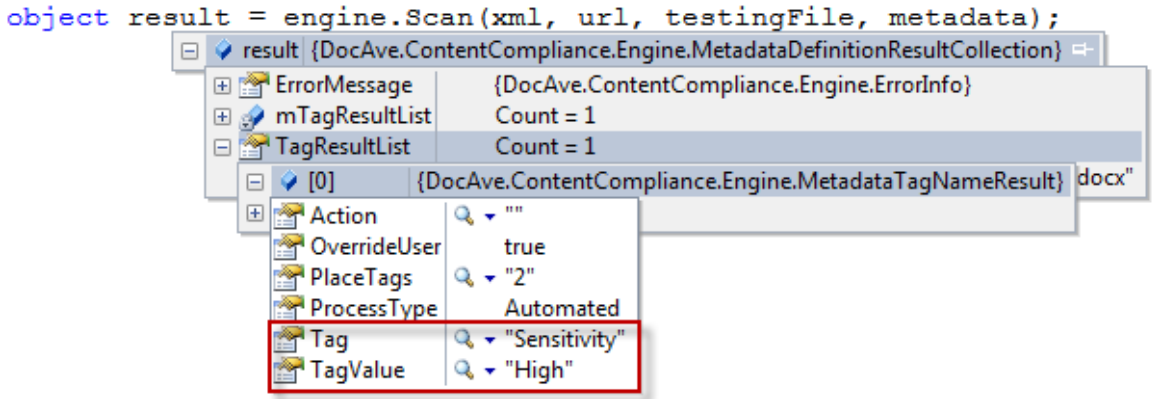

Figure 46: Scanned result 4.

Scan Metadata

Regarding the TDF language, the user is able to define a customized TDF to perform a customized scan according to their requirements. Among all kinds of supported TDF types, the SSL and Cookie Validation type TDFs will require the scan engine to test the SSL level or Cookie domain and expiration. The Compliance Guardian SharePoint metadata test is supported in the installation package.

Therefore, for Scan Engine API, the scan method requires the SSL level, Cookie information, or SharePoint Metadata for the source document, to be passed via an argument **metadata** if the corresponding SSL/Cookie /Metadata checking is defined and used in MCC/CCC.

```
Dictionary<string, object> metadata = new Dictionary<string, object>();
```

For SSL Level information, if the source site is under the HTTPS protocol and SSL level checking TDF is used, the SSL level for the source site should be set in metadata. The key for the scan engine to recognize SSL information is **PublicKeySize**, and the security level value should be an **Integer**.

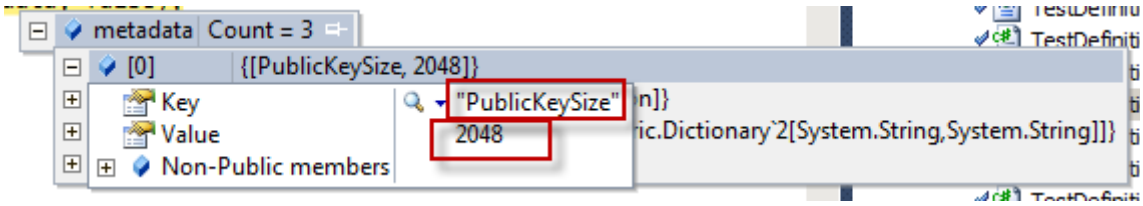

Figure 47: The key and value for SSL Level information.

For cookie information, if the cookie validation TDF is used in the CCC, the cookie collection should be passed via the **metadata** Dictionary. The Key should be **Cookie** and the value should be a **System.Net.CookieCollection** object, which contains all the cookie objects retrieved from the source environment.

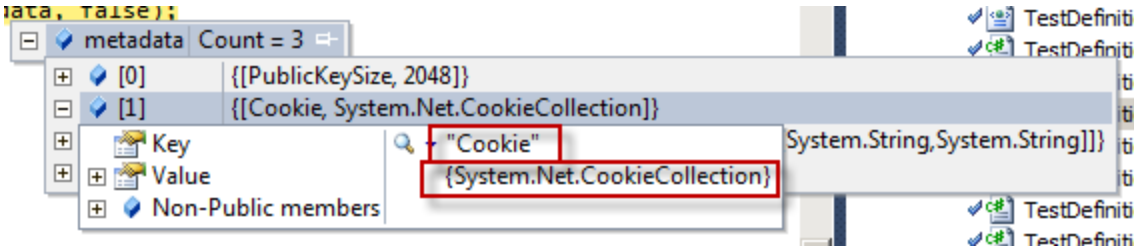

Figure 48: The key and value for cookie information.

For SharePoint Metadata information, the **Key** should be **Metadata**, however the **Value** object should be another **Dictionary<string, string>** instance, which uses the SharePoint column name as the key, and uses the SharePoint column value as the value.

***Notes**: For SharePoint build-in columns, the key should end with **\0\0**. The indicator **\0\0** tells the scan engine that the column is a SharePoint build-in column, which will be ignored by the scan engine during the scanning progress.

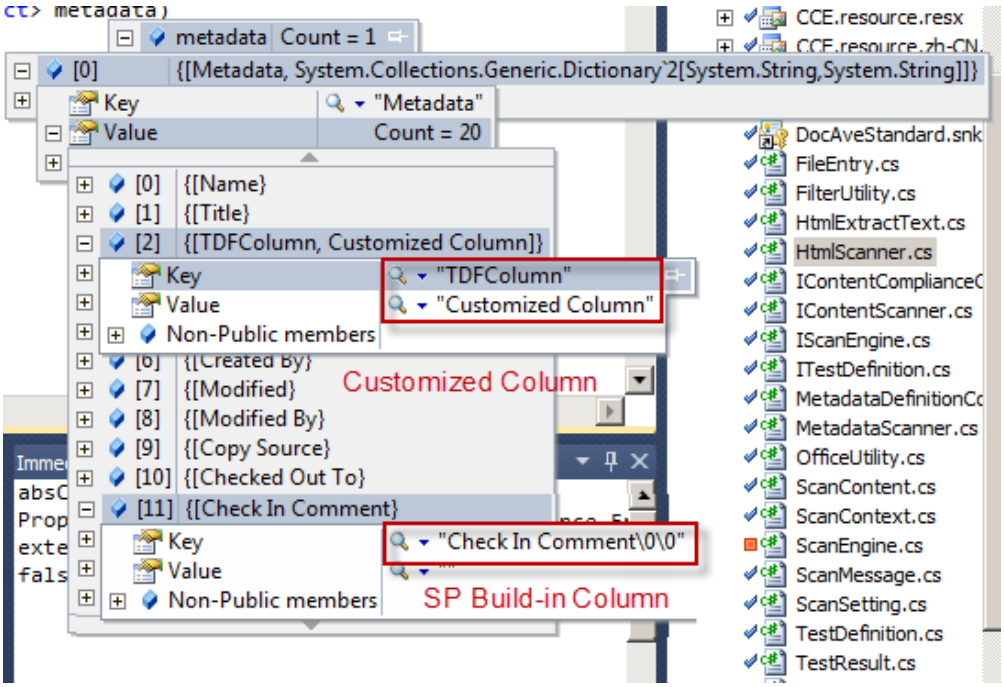

Figure 49: The key and value for SharePoint metadata.

CCE.EngineWorker.exe Mode

Use the parameter of the ScanSetting's object to modify the method of starting **CCE.EngineWorker.exe**. After the ScanSetting's object **setting** is created, the attribute **CommunicationSetting** of the ScanSetting's object is used to configure the method of starting **CCE.EngineWorker.exe**:

```
setting.CommunicationSetting.IsSingleProcess = true;
ScanEngine engine
object rel = engine.                                   es/pages/default.aspx", file, null);

return;
//var events = new L
//for (int i = 0; i
//{
```

setting.CommunicationSetting	{DocAve.ContentCompliance.Engine.Common.Commun
CheckInterval	60
IsRemote	false
IsSingleProcess	false
RemoteIP	"BJ00127-990"
RemotePort	14104
RetryTimes	3
ScanTimeout	180

Figure 50: The condition after the ScanSetting's object setting is created.

- **IsSingleProcess** – This attribute is used to configure if the **CCE.EngineWorker.exe** is started using the singe process. The default value is **false**.
  - If the value of this attribute is set to **false**: After creating the **engine** object, the **ScanEngine.Scan** method will be called and the CCE.EngineWorker.exe will start to scan files.

Image Name	PID	User Name	CPU	Working Se
acrotray.exe *32	4064	Administrator	00	4,256
AdobeARM.exe *32	1480	Administrator	00	10,252
[illegible]	[illegible]	LOCAL SERVICE	00	15,640
CCE.EngineWorker.exe	9680	Administrator	26	150,368
CCS.browser.exe	5908	Administrator	00	71,716
CCS.exe	11828	Administrator	00	78,744
CISVC.EXE	1640	SYSTEM	00	172
communicator.exe *32	8944	Administrator	00	179,960

Figure 51: The CCE.EngineWorker.exe starts.

  - If the value of this attribute is set to **true**: The CCE.EngineWorker.exe will not be started for scanning files.

- **IsRemote** – The attribute will take affect when the value of **IsSingleProcess** is set to **false**. It is used to configure whether the **CCE.EngineWorker.exe** process and the user process that is creating the **engine** object are running in a same machine where the corresponding agent is installed.
  - If the value of this attribute is set to **true**, the **CCE.EngineWorker.exe** process can run on another machine where another agent (this agent and the agent that is used to create **engine** object must connect to a same server) is installed. The values of the **RemoteIp** node and the **RemotePort** node must be specified. The default values are the IP and port of the machine where the agent that creates the **engine** object is installed. The **CCE.EngineWorker.exe** process will run on

the specified machine (according to the values you specified for the **RemoteIp** node and the **RemotePort** node).

  - If the value of this attribute is set to **false**, the **CCE.EngineWorker.exe** process will run on the machine where the agent that creates the **engine** object. The values of the **RemoteIp** node and the **RemotePort** node are invalid, and do not need to be specified.

- **ScanTimeOut** – The attribute will be taken affect when the value of the **IsSingleProcess** attribute is **false**. It is used to configure the timeout period. The default value is 180. The unit is **seconds**.
- **RetryTimes** – The attribute will be taken affect when the value of the **IsSingleProcess** attribute is **false**. It is used to define the times of retrying when an error occurred during scanning a file. The default value is **3**.
- **CheckInterval** – The attribute will be taken affect when the value of the **IsSingleProcess** attribute is **false**. It is used to define the interval of checking the **Keepalive** thread. The default value is 60. The unit is **seconds**.

Appendix E: Using Check Validator Tool

The Check Validator tool is used to verify if the custom check that is created using Compliance Guardian is correct, and also used to verify if you can get the type of scan results you want.

To use the Check Validator, complete the following steps:

1. Go to the machine with Compliance Guardian Agent installed and open the *…\AvePoint\Compliance Guardian\Agent\bin* directory to find the **CCE.TDFValidator.exe** file.
2. Open the **CCE.TDFValidator.exe** to start this tool.

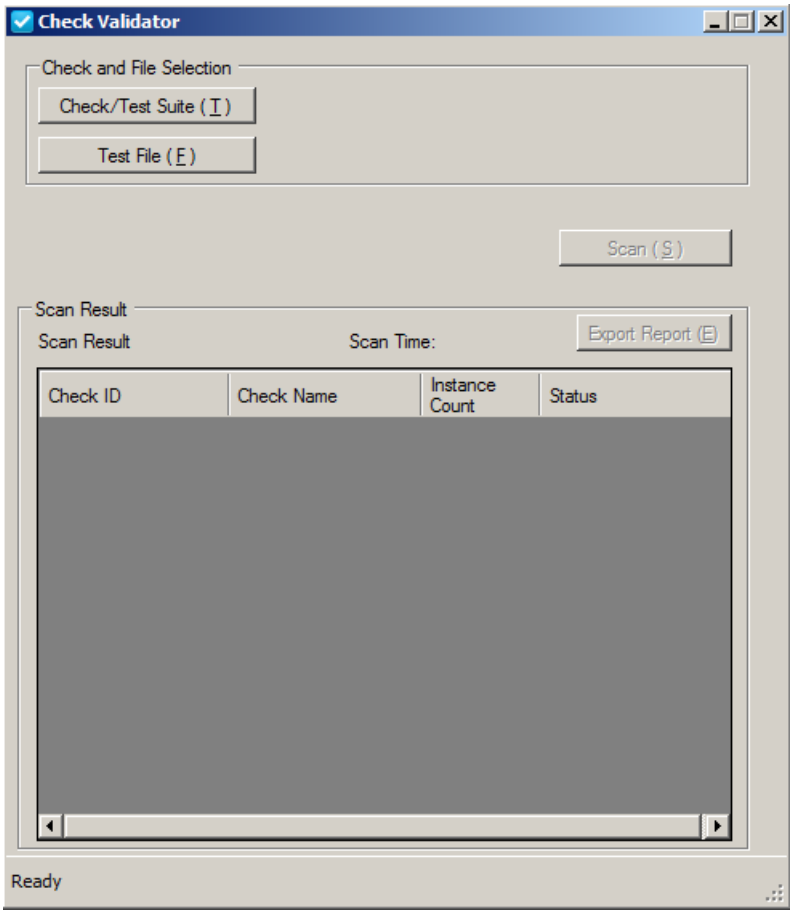

Figure 52: Check Validator interface.

3. Select the **Check/Test Suite (T)** button (or you can press **T** on your keyboard), a pop-up window appears, select the check, test suite or a CCC/MCC file that you want to validate, and then select **Open** in the pop-up window. The full path of the selected check/test suite will be displayed on the tool interface.
4. Select the **Test File (F)** button (or you can press **F** on your keyboard), a pop-up window appears, select the file you want to test, and then select **Open** in the pop-up window. The full path of the selected file will be displayed on the tool interface.

5. Select the **Scan** button, the file then will be tested according to the rules defined in the selected check or test suite.

6. The scan results will be displayed in the **Scan Result** field of this tool. In the **Scan Result** field, the Check ID, Check Name, the count of the instances that are found and the status of each check will be displayed. If one of the statuses of the checks is Failed, the Scan Result will be Failed. The time that the scan takes will also be displayed.

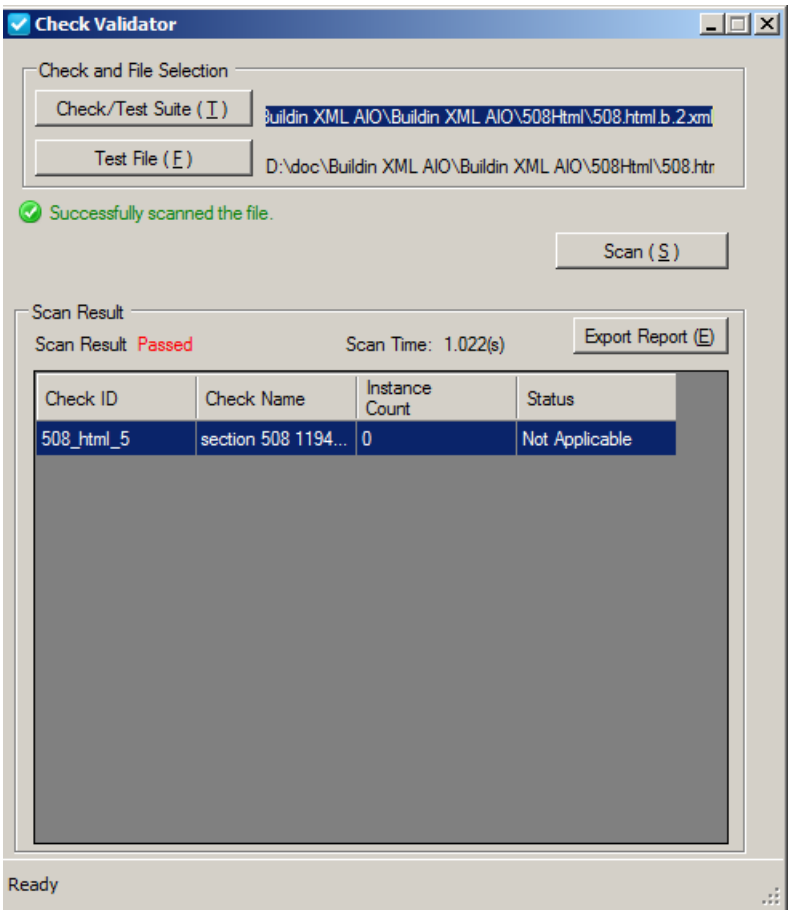

Figure 53: Scan results of Check Validator.

7. Select **Export Report** to generate the scan result. After you select the **Export Report** button, a pop-up window appears, select the location where you want to save the report, and select **OK** on the window. The detailed scan report will be saved in the specified location. You can check the report to verify if the scan results are what you wanted.

8. Before scanning the selected file, the tool will first validate if the check, test suite or CCC/MCC file is correct, if the selected check, test suite or CCC/MCC file is not correct, after you select the **Scan** button, the error message will be displayed on the tool interface, you can then review the logs for the detailed information.

9. After the scan job, a report is also generated in *…\AvePoint\Compliance Guardian\Agent\bin\TDFValidatorReport.* The report contains three kinds of files:

    - The file that is scanned by Check Validator.

- The HTML format of the scanned file.
- The report that contains all of the scanned file's violations as well as the violation's locations.


```
  <?xml version="1.0"?>
- <TestResultCollection>
  - <Result status="Fail" tdfID="508_office_A">
    - <Groups>
        <Result status="NA" tdfID="508_office_1"/>
        <Result status="NA" tdfID="508_office_2"/>
        <Result status="NA" tdfID="508_office_3"/>
      - <Result status="Fail" tdfID="508_office_4">
        - <Units>
            <Unit status="Fail" tdfID="508_office_4" length="33" column="1" line="311" startIndex="10371"><table name="Table1"
                head="true"></Unit>
          </Units>
        </Result>
      </Groups>
```


Figure 54: Check Validation report.

Related Configuration File

The tool has a related configuration file named **CCE.TDFValidator.exe.config**, the file is located under the directory *…\AvePoint\Compliance Guardian\Agent\bin* directory.

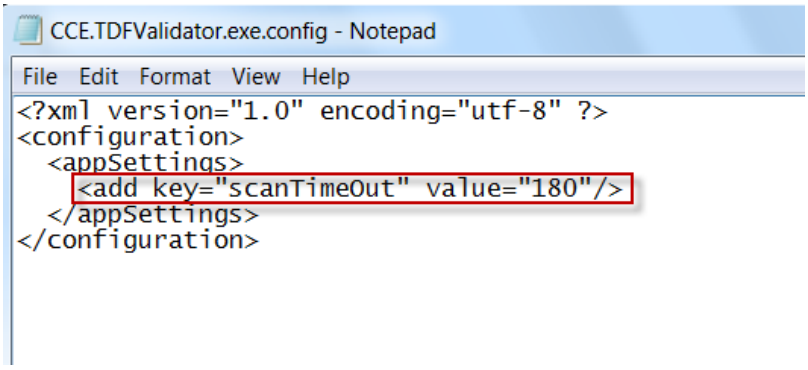

Figure 55: CCE.TDFValidator.exe.config file overview.

You can configure the **Value** attribute to specify the maximum scan time. If the time that the scan takes exceeds the specified scan time, an error message will be displayed on the tool interface, and the scan will stop. By default, the value for the **Value** attribute is 180 seconds.

Appendix F: Generate Detailed Risk Report of a File

Compliance Guardian supports to export the detailed risk report information of a file through the **ccr.sp2010riskananlyzer.exe** or **CCR.SP2007RiskAnalyzer.exe** files. Compared with the Risk Report that is displayed in the Compliance Guardian Report, or generated from Compliance Guardian Report, the detailed risk report combines all of the risk report information of a file to one CSV file, thus for user conveniently checking and viewing.

Before You Begin

In order to generate the detailed risk report, the **ccr.sp2010riskananlyzer.exe** or **CCR.SP2007RiskAnalyzer.exe** file must be run in the Command Line. The DocAve Auditor database must be connected so as to get the related auditing information.

To get the risk report, complete the following steps:

1. Go to the machine with Compliance Guardian Agent installed and open the *…\AvePoint\Compliance Guardian\Agent\bin* directory to find the **ccr.sp2010riskananlyzer.exe** file (**CCR.SP2007RiskAnalyzer.exe** is for the files in SharePoint 2007, here we take the **ccr.sp2010riskananlyzer.exe** as an example).

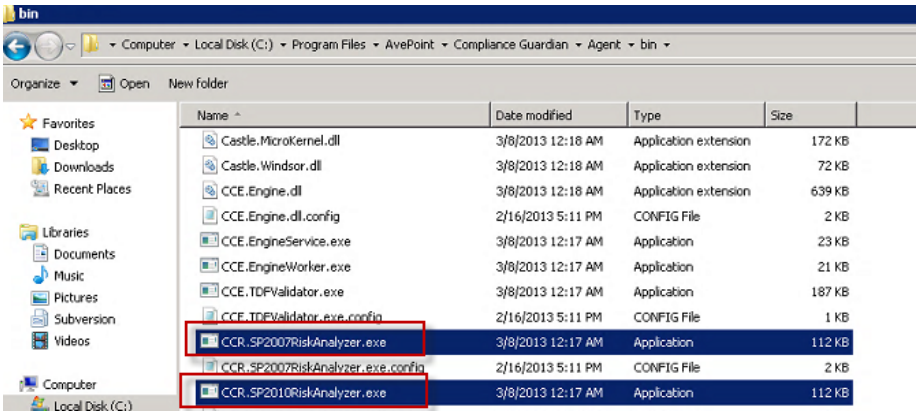

Figure 56: The EXE file location.

2. On the machine, navigate to **Start** > **All Programs** > **Accessories** > **Command Prompt**.
3. In the command-line interface, enter the directory. For example, *C:\Program Files\AvePoint\Compliance Guardian\Agent\bin*, and press **Enter**.

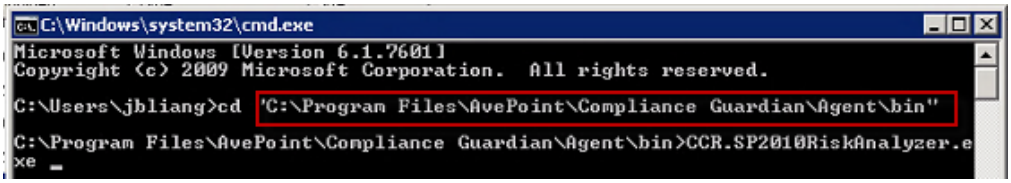

Figure 57: The command line overview 1.

4. Enter the **–fullpath** command, and then enter the full path of the file whose detailed risk report will be generated.

5. Enter the **–dbname** command, and then enter the database file name of the plan whose detailed risk report information will be exported.

   To get the database file name, go to the report location, and find the request's corresponding TXT file (the name of the TXF file is the Request ID + _ + the Request Name). Open the TXT file, you will find all the plans contained in this request, the database file name is following the corresponding plan. Then go back to the report location, basing on the database file name in the TXF file, you will find the database file's full name (the database name +.db) of the desired plan whose detailed risk information is going to be exported.

6. Enter the **-exportlocation** command, and then enter the export location where the detailed risk report will be generated.

   The **–exportlocation** command is optional, if you do not enter the command and do not specify an export location, by default, the report will be generated under the directory …\AvePoint\Compliance Guardian\Agent\bin\Risk Analyzer.

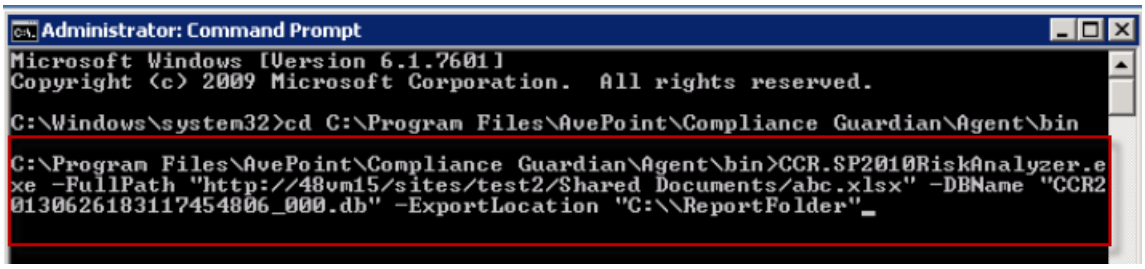

Figure 58: The command line overview 2.

7. Press **Enter** to execute the job. After the job completes, a prompt is shown as below.

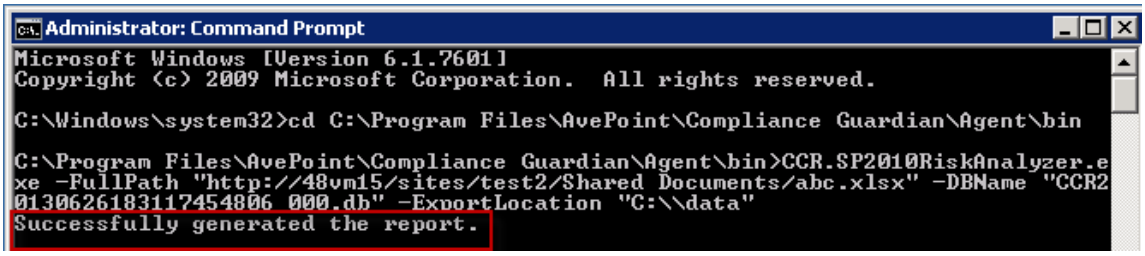

Figure 59: The command line overview 3.

8. You can then navigate to the specified export location to view the risk report.

Appendix G: Compliance Guardian Configuration File

When a user uploads checks or test suites to Compliance Guardian, the ZIP file of the checks or test suites will be temporarily unzipped to a default directory. The default directory is *…\Compliance Guardian\Manager\Work*. The full path of the checks or test suites that will be uploaded is *…\Compliance Guardian\Manager\Work\Test Suite Name\Check Name or …\Compliance Guardian\Manager\Work\Test Suite Name*. Due to the limitation of Microsoft Windows, the length of the check or test suite's full path cannot exceed 260 characters, or the check or test suite will not be uploaded to Compliance Guardian.

Compliance Guardian has a configuration file named **ComplianceSetting.config** that allows you to customize the directory where the checks or test suites will be temporarily unzipped through the customized directory to reduce the length of the check or test suite's full path.

To change the default directory where the checks or test suites will be temporarily unzipped, complete the following steps:

1. Go to the machines with Compliance Guardian Manager installed and open *the …\Compliance Guardian\Manager\Control\Config* directory to find the **ComplianceSetting.config** file.
2. Open the **ComplianceSetting.config** file and find the **ConfigureFilePath** node.
3. Change the value of the **IsConfigured** attribute to **True**. Then specify a path for the **path** attribute. Restart the Compliance Guardian Timer Service. The checks or test suites will be temporarily unzipped under the specified path.

   ***Note:** The path that you specified for the **path** attribute must exist.

Appendix H: Using CustomCheck in Compliance Guardian

CustomCheck is used to calculate the check digit on the result of the regular expressions, in order to validate the result.

Using CustomCheck

Refer to the following section for using the CutomCheck function.

Method

Define an Interface IValidation, all the implementation classes need to implement the interface and expose a public method "Validate" for CCE to use them. This Interface is initially defined as:

```
   public interface IValidation
   {
      string Parameters { get; set; }
      bool Validate(string id);
}
```

Configuration

Define the DLL and the class configuration file "ContentComplianceConfig.xml". The value of "Class" should be the full name of the class and the full name of the DLL, separated by a comma(**,**). Name refers to the name of the checksum algorithm. Regex will call the algorithm from this value. Node <Parameters> is for the parameters needed for specific algorithms, all content will be passed internally as a string.

```
<!-- CustomCheck Node -->
<CustomCheck Name="Credit Card Number" Class="DocAve.ContentCompliance.Engine.Checksum,
CommonChecksum">
     <Parameters>
     <![CDATA[ Parameter as string ]]>
     </Parameters>
</CustomCheck>
```

***Note**: In order to load the external DLLs, they must be put either in the agent\bin folder or in GAC.

Example

```
<!-- Canadian SIN & Credit Card Number-->
<RegEx CaseSensitive="No" ListLocStatus="Fail" ListLoc="Yes" SearchAll="True" TrueIf="NotFound"
CustomCheck="Credit Card Number">
<![CDATA[(?<=^|\b)\d{3}([- ])\d{3}(\1)\d{3}(?=$|\b)]]>
```

</RegEx>This is an example that how a checksum is defined in check. Note the checksum algorithm to the RegEx is defined by CustomCheck="Credit Card Number". A Class example which implements the interface:

```
public class LuhnAlgorithm : IValidation
{
   public string Parameters { get; set; }
   public LuhnAlgorithm(string parameters)
  {
      this.Parameters = parameters;
   }
   public bool Validate(string number)
   {
      if (string.IsNullOrEmpty(this.Parameters))
      {
         return ValidateInternal(number);
      }
      else
      {
         return ValidateInternal(number, this.Parameters);
      }
   }
   public bool ValidateInternal(string number)
   {
      //  Method without parameter
   }
   public bool ValidateInternal(string number, string parameters)
   {
      //  Method with parameter
   }
}
```

Related Configuration File

The configuration file ContentComplianceConfig.xml provides several built-in CustomCheck methods. The configuration file resides in *…\Compliance Guardian\Agent\Bin.* You can add your customized CustomCheck methods in the configuration file.

Appendix I: Using Compliance Guardian Transaction Capture

Compliance Guardian Transaction Capture is used to record the webpages that you access, and then you can save the recorded results as a transaction file, which is used by Compliance Guardian Website Scanner. The recorded URLs in the transaction file will be the start URLs used in Compliance Guardian scans.

Installing Compliance Guardian Transaction Capture

To install Compliance Guardian Transaction Capture, complete the following steps:

1. Find the **setup.exe** file in *...\Compliance Guaridan\Agent\bin\WebSiteRecorderInstallFiles.*
2. Open the **setup.exe** file, and select **Install** in the appeared drop-down menu. The **Compliance Guardian Transaction Script Recorder Setup** wizard appears, which helps you to install the Compliance Guardian Transaction Capture tool.
3. Select **Next** on the wizard welcome page.
4. Select a folder where the related files of this tool will reside. The default location is: *C:\Program Files (x86)\AvePoint\CG Transaction Script Recorder*. You can select **Browse** to select another location.

   Select the **Disk Cost…** button under the **Browse** button to view the drives you can install the tool, and each drive's available and required disk space of the tool.

   Under this wizard interface, there are two radio buttons:

   - **Everyone** – Anyone who use the computer can use the tool.
   - **Just me** – Only the current user can use the tool in the computer.

   Select **Next** on this page.

5. Confirm the installation on the **Confirm Installation** page, and select **Next**.
6. The tool will begin installing.
7. After the installation completes, select **Close** to exit the installation wizard. After exit the installation wizard, a pop-up message appears to confirm whether to restart the system right now for the tool to take effect. Select **Yes** to restart immediately, or select **No** if you plan to manually restart the system later.

   ***Note**: The **AgentToolWebSiteRecorder.msi** file is also used to install the Compliance Guardian Transaction Capture, but since the **setup.exe** file can check the environment for installing the tool, we recommend you to use the **setup.exe** file to install the Compliance Guardian Transaction Capture.

Using the Tool

To use Compliance Guardian Transaction Capture, open Windows Internet Explorer (x86) from the path …*Program Files (x86)**Internet Explorer*, select **View** on the **Menu Bar**, and select **Explorer Bars**. You will find Compliance Guardian Transaction Capture in the drop-down menu that appears. Select **Compliance Guardian Transaction Capture** to open this tool. The tool interface appears on the bottom of the current webpage. Refer to the following screenshot:

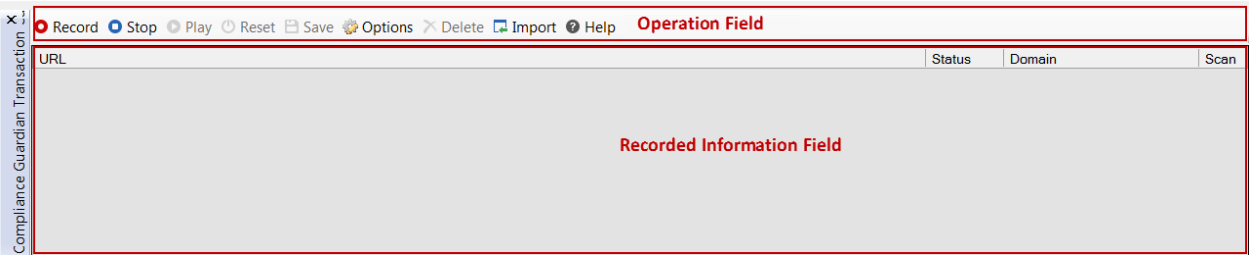

Figure 60: The Compliance Guardian Transaction Capture interface.

- **Operation Field** – You can perform the following actions in this field:
  - **Record** – On the webpage you want to record, select the **Record** button. Compliance Guardian Transaction Capture will then start to record the webpages you access from this current webpage. The URLs that are recorded will be displayed on the **Recorded Information Field**.
  - **Stop** – Select the **Stop** button to stop recording the webpages.
  - **Play** – Select the **Play** button. The series of webpages that you have recorded will automatically play as they are accessed.
  - **Reset** – Select the **Reset** button, all the recorded results will be cleared up.
  - **Save** – Select the **Save** button to save the series of operation results as a transaction file. After select the **Save** button, the **Save As** window pops up. Select a location, and then select **Save** on the **Save As** window to save the transaction file, which will be used for Compliance Guardian Website Scanner.
  - **Options** – Select the Options button, a pop-up window appears. Select the checkbox before **Capture the Ajax Request (XMLHttpRequest)**. Then Compliance Guardian Transaction Capture can record the webpages that use the Ajax Request.
  - **Delete** – Select a record in the **Recorded Information Field**, and select **Delete**, the record then will be deleted.
  - **Import** – Import a previously saved transaction file. You can view the results that the transaction file records by selecting **Play**.
  - **Help** – Select the **Help** button to view the Help information.
- **Recorded Information Field** – The recorded results will be displayed in this field.
  - **URL** – The webpage URLs that have been recorded.

- **Status** – The status code of a webpage.
- **Domain** – The domain of the URL.
- **Scan** – Select the checkboxes under this column. The corresponding URL will be signed. After you save the related transaction file for Compliance Guardian Website Scanner, only the URLs that are signed here can be used as the Start URLs to be scanned. Only the checkbox of the URL whose corresponding status code is 200 can be selected and scanned.

Select the close button (✕) on the top-right corner to close the Compliance Guardian Transaction Capture tool.

Appendix J: Using Detailed Risk Report Analysis Tool

Compliance Guardian supports exports of detailed risk report information of all the files in a site collection level Compliance Guardian Scanner for SharePoint job.

***Note**: The DocAve Auditor database must be connected so as to get the related auditing information.

Generating the Report

To generate the report, complete the following steps:

1. Go to the machine with Compliance Guardian Agent installed and open the *…\AvePoint\Compliance Guardian\Agent\bin* directory to find the **CCR.RiskReportTool.exe.config** file.
2. Open the **CCR.RiskReportTool.exe.config** and configure the following attributes:

```
<appSettings>
  <add key="DBName" value="CCR20130626134715019767_000_.db"/>
  <add key="ExcelLocation" value="C:\"/>
  <add key="FileShowCount" value="10"/>
  <add key="FileAuditDetailCount" value="25"/>
</appSettings>
```

Figure 65: Attributes for generating the report.

- **Database Name** – Specify the database file name as the value of the **DBName** attribute. To get the database file name, go to the report location, and find the request's corresponding TXT file (the name of the TXT file is the Request ID + _ + the Request Name). Open the TXT file. You will find all the plans contained in this request. The database file name follows the corresponding plan. Then go back to the report location, basing on the database file name in the TXT file, you will find the database file's full name (the database name +.db) of the desired plan whose detailed risk information is going to be exported. .
- **Export Location** – Specify the location as the value of the **excelLocation** attribute. The report will be generated into this location.
- **File Show Count** – Specify the number of the files as the value of the **fileShowCount** attribute. The files are displayed according to their risk scores calculated by the Raw type risk formula. For example, if you specify 10 as the value, then the risk information of 10 files that have the top 10 risk scores (calculated by the Raw type risk formula) will be displayed in the report. Each file's risk information is displayed in one sheet in the report excel.
- **Auditing Item Count** – Specify the number of the Auditing items that will be displayed in the report. The information of the most recent activities to the file will be displayed in the report.

After configuring the attributes, save the configuration file.

3. Under the same directory *(…\AvePoint\Compliance Guardian\Agent\bin*), find the **CCR.RiskReportTool.exe** file and select to **Run As Administrator**. After the **CCR.RiskReportTool.exe** file has been opened, wait until the following message appears, indicating the report has been generated into the specified location: **The report has been generated. Press any key to exit.**

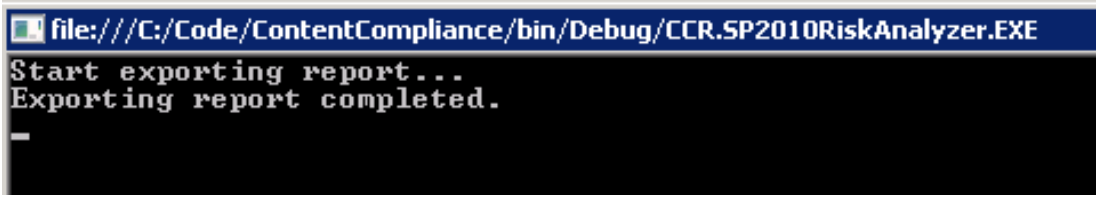

Figure 61: The CCR.RiskReportTool.exe file interface.

Information Included in the Exported Excel File

The generated risk report excel contains the **BasicInformation** sheet that displays the basic information of the risk files. Each risk file has its own sheet for displaying the file's risk information. The number of the files whose risk information will be displayed in the report is based on the value of **fileShowCount** attribute that you specify in the **CCR.RiskReportTool.exe.config** file.

You can view the following information in the exported report:

- **BasicInformation** sheet:
  - The risk scores (the risk scores calculated by the Raw type risk formula, the risk scores calculated by the Stepped type risk formula and the risk scores calculated by the Weighted type risk formula) of each site collection in the job. A bar chart is displayed to help you view the information intuitively.
  - The information of risk files that violated the regulations (check) in the job. A pie chart is displayed to help you view the information intuitively.
  - The detailed information of the risk files in each site collection, including the risk scores, the number of the Passed files, Failed files, User Review Required files, Not Applicable files, Not Tested files and Error files, and the percentage of the failed files. A bar chart is displayed for each site collection to help you view the information intuitively.
- Risk information of each file:
  - The file information, the risk scores, and the regulations (checks) that the file violated.
  - The related auditing information, including the access time to the file, the user who accessed the file, the action type and some related details.
  - The security information related information.

Appendix K: Using Compliance Guardian Report Database Upgrade Tool

Compliance Guardian Report Database Upgrade tool is used to upgrade the Compliance Guardian report database (created in the Compliance Guardian version before 3 SP1) if you want use it in Compliance Guardian 3 SP1.

Using the Tool

To upgrade the he Compliance Guardian report database, complete the following steps:

1. Go to the machines with Compliance Guardian Manager installed and open the *…\Compliance Guardian\Manager\Shared\Tools\CGReportDBUpgrade* directory to find the **CGReportDBUpgrade.exe** file.
2. Open the **CGReportDBUpgrade.exe** file, enter the Compliance Guardian Server IP address and press **Enter**; Enter the Compliance Guardian Server port, press **Enter**; enter the Compliance Guardian login username, and press **Enter**; enter the login password, press **Enter**. Wait until the **Press any key to exit** message appears after the database is finished upgrading.

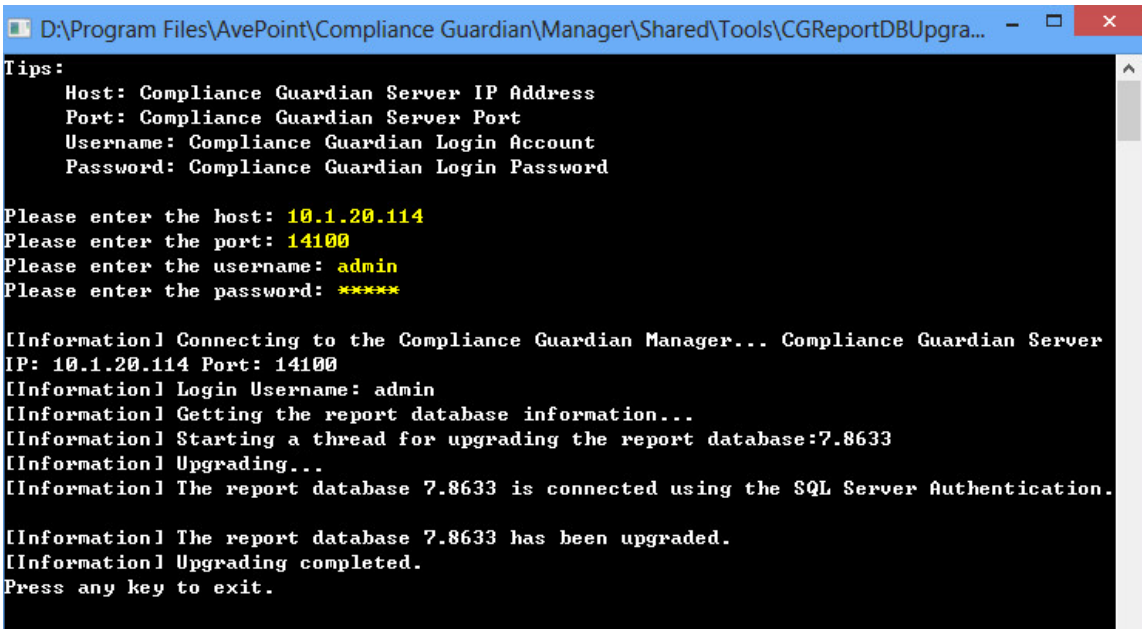

Figure 62: The CGReportDBUpgrade.exe file interface.

Appendix L: Displaying Only Violations in the Error Highlight Report

This function is used for **Compliance Guardian Scan Result > Failed Files > Error Highlight Report**. If a file size is quite large, it may affect the performance to display the whole file in the Error Highlight Report. Compliance Guardian provides you with a way to control whether the whole file with the violations (non-compliant content) is displayed in the Error Highlight Report, or just the file's violations (non-compliant content) are displayed in the report.

The configuration file **ContentComplianceConfig.xml** provides you with a node to provide this function. The configuration file resides in …*Compliance Guardian**Agent**Bin*.

Open the file, and find the node **<ViolationSummaryThreshold aCount="20" bCount="40">600</ViolationSummaryThreshold>**:

- **aCount** – The value of this attribute means the number of the characters after the non-compliant content that can be displayed in the error highlight report. The default value is 20. You can customize the value.
- **bCount** – The value of this attribute means the number of the characters before the non-compliant content that can be displayed in error highlight report. The default value is 40. You can customize the value.
- **Node Value** – If a file size is greater than the node value, the whole file will not be displayed in the Error Highlight Report for the performance consideration, only the violations (non-compliant content) along with the characters next to the violations (the characters before the violations and the characters after the violations) are displayed in the report. The default node value is 600 KB. You can customize the value.

Index

Account is inactive, 40, 52, 54
Account Manager, 46
Action Policy, 125, 126, 128
Action Policy Name, 125
Activate, 37, 54
Active Directory User/Group, 52
AD Integration, 42
AD User/Group Name, 52
Add, 43, 50, 52, 53, 66, 72
Add a Filter Level Group, 128, 130
Add Federation Trust, 46
Add Group, 49
Add Schedule, 71, 108, 109, 113
Add User, 51
Add user to a DocAve group, 52, 53
Add User to Group, 50
ADFS Claim, 53
ADFS Integration, 44, 46
ADFS Issuer, 44
Advanced, 71, 109, 114
After __ day(s), 54
Agent, 63, 64
Agent Groups, 65
Agent Monitor, 35
Agent(s) in Group, 66
Apply, 58
Authentication Manager, 42
Authentication Type, 42
Auto, 45
Automatically, 44
Back, 22, 25, 36, 42, 43, 44, 45, 49, 50, 58, 64, 66, 74, 76, 94
Back Up, 41
Browse, 20, 23, 38, 58, 63
By day, 71
By hour, 71
By month, 71
By week, 71
Calendar View, 109, 114, 166
Cancel, 22, 25, 43, 45, 48, 50, 52, 53, 54, 66, 69, 72, 93, 95, 97, 99, 105, 123, 126, 128, 148, 167
Change permissions, 128
Change to the end user browser used language, 38
Check for Updates, 62
Classification Result, 130
Clear Selection, 124
Close, 35, 37, 39, 42, 46, 56, 73, 74, 92

Compliance Guardian, 34
Compliance Guardian Quarantine Manager, 127
Compliance Guardian Timer Service, 12
Compliance Reporting Officer Group, 107, 112
Compliance Reports, 121
Condition, 130
Configure, 36, 70
Configure the schedule myself, 71
Confirm password, 52
Confirm Password, 54
Contains, 44, 45
Control Panel, 32, 34
Create, 65, 77, 79, 91, 93, 95, 97, 99, 102, 123, 125, 126, 141, 144
Create a new IIS web site, 21
Create Action Policy, 126, 141
Create Scan Policy, 124
Creator, 108, 129
Customized, 52
Date format, 38
Date Range, 167, 170
Day, 58, 109, 114, 167
Day __ of every __ month(s), 72
Day(s), 41, 70, 89, 109, 110, 113, 115, 149
Deactivate, 37, 54
Deactivate the account when the inactive period reaches:, 39
Debug, 73
Default, 52, 167
Delete, 43, 47, 64, 66, 77, 79, 91, 93, 95, 97, 99, 105, 123, 126, 148
Delete files/items, 127
Delete User, 54
Deploy, 75, 76
Description, 47, 49, 52, 68, 69, 91, 93, 107, 112, 122, 124, 125
Details, 20, 23, 76, 168
Disable, 43, 170
Display … for all users, 38
Display Name in DocAve, 39
Document, 130
Domain, 43
Download, 63, 168
Edit, 43, 45, 47, 66, 69, 77, 79, 91, 95, 97, 99, 102, 105, 123, 124, 126, 141, 144, 148
Edit Action Policy, 126, 141
Edit Group, 49
Edit Scan Policy, 124
Edit User, 54
E-mail, 52
E-mail notification, 41, 59
E-mail template, 108
Enable, 43, 170

Enable Actions Configuration, 127, 128
Enable network security, 40
Enable Outgoing E-mail Server Settings, 67
End after __ occurrence(s), 72
End after 1 occurrence, 106, 109, 110, 114, 115, 149
End after specified occurrence(s), 111, 115
End by, 111, 115
End by __, 72
Enter, 99
Equals, 40
Error, 73
Export, 45
Export Location, 77, 78, 88, 89, 91
Failed Logon Limitation, 39
Farm, 66, 74
Federation Metadata Trust, 44
Filter Policy, 92
Filter policy name, 93
Filter the column, 105, 148
Find, 53
Find Certificate, 44, 45
Find in:, 45
Find Now, 44, 45
Finish, 25, 28, 31, 45, 110, 114
Finish and Run Now, 110, 114
Form Mode, 107, 111, 115
FsDomSrv.ini, 11
Full Scan, 109, 110, 113, 114
General Settings, 38
Global permission, 49
Group Name, 49
Group Permissions, 129
Groups, 48
Hide Preview, 39
Hide the column, 105, 123, 125, 148
Hour(s), 39, 58, 106, 109, 110, 113, 115, 149
HTTP Proxy, 61
I accept the terms in the license agreement, 20, 23
If the action failed to execute, 129
If the action successfully executed, 129
If the files fail to move, it/they will be quarantined, 127
If the files(s) failed to move, it/they will be quarantined, 126
If the language does not change successfully, please select to use a default language, 38
Import, 58
Inactive Period, 39
Inbound Rules, 12
Incremental Scan, 106, 109, 110, 113, 114, 149
Information, 73

Install, 22, 25, 63, 75
Install the update for all the managers below, 63
Integration Settings, 67
Interval, 58, 59
Item, 130
Job Details, 168
Job Monitor, 70, 73, 164
Job Monitor tab, 166
Keep the last__ Job(s), 70, 88
Last Modified Time, 122, 125
License Manager, 56
List View, 166
Local, 167
Local User, 51
Locale(Location), 38
Log Manager, 73
Log Settings, 73
Login, 29
Logon will expire in, 39
Look in field:, 44, 45
Manage columns, 105, 123, 125, 148, 167
Manage Passphrase, 41
Manage Updates, 62
Manager, 63, 64
Manager Monitor, 35
Manu, 45
Manually, 44
Maximum, 40
Maximum User Session, 39
Minimum number of alpha, 40
Minimum number of numeric, 40
Minimum Password Length, 40
Minute(s), 39, 106, 109, 110, 113, 115, 149
Modifier, 108, 129
Modify, 41
Module, 167, 170
Month, 58, 109, 114, 167
Month(s), 41, 70, 89, 106, 109, 110, 113, 115, 149
Move to the specified allowed location, 126, 127, 128
MS SQL, 21
Name, 46, 47, 91, 126, 141
Negotiate(Kerberos), 42
Never, 54
New Database Policy, 107, 112
New E-mail template, 108
New Filter Policy, 108, 113
New Notification Profile, 108, 109, 114
New password, 54

Next, 20, 21, 22, 23, 25, 28, 30, 31, 44, 45, 107, 108, 109, 110, 112, 114, 151
Next., 23
No end date, 72, 111, 115
No Proxy, 61
No Pruning, 70, 88
No Schedule, 71
NTLM, 42
OK, 28, 36, 41, 42, 43, 44, 45, 47, 49, 50, 52, 53, 54, 59, 66, 71, 72, 74, 77, 79, 89, 91, 92, 93, 95, 97, 99, 105, 123, 124, 126, 128, 148, 167, 168, 169
On __, 54, 72
On day __ of __, 72
Open, 38, 58, 63
Option 1, 45
Option 2, 45
Options, 109, 113
Outgoing E-mail server (SMTP), 67
Overview, 66, 110, 114
Password, 36, 43, 52, 60, 61, 62, 92, 169
Password cannot contain space, 40
Password cannot contain user ID, 40
Password never expires, 52
Password on SMTP, 67
Permission for different farms, 49
Permission Level, 46
Plan Builder, 106
Plan Manager tab, 169
Plan Name, 107, 112
Popup message, 41
Popup message box when you login, 59
Port, 67
Preview, 38
Proxy host, 61, 62
Proxy port, 61, 62
Prune Now, 70
Quarantine files, 127
Quarantine files/items, 130
Range of Recurrence, 106, 109, 110, 114, 115, 149
Real-Time Classification Scanner, 135, 145
Reference Time, 106, 109, 110, 113, 115, 149
Relying Party Identifier, 44
Remove, 30, 31, 37, 66
Remove all users associated with the selected domain(s), 43
Remove configuration file, 30, 31
Repair, 76
Report Format, 168
Report Location, 169
Report Settings, 107, 112
Rescan, 20, 23

Restart, 37
Restore to Default, 39
Restricted network, 40
Retract, 76
Retrieve Version, 76
Rule, 130
Rules, 70
Run every __ week(s), 72
Run Now, 106, 149, 169
Save, 39, 66, 67, 70, 105, 148
Save As, 66
Scan Policy, 122, 123
Scan Policy Name, 122
Scan Settings, 107, 112
Schedule, 108
Scheduled Job Monitor tab, 166
Search all pages, 35, 42, 47, 48, 50, 51, 62, 64, 65, 67, 92, 95, 96, 100, 105, 123, 124, 125, 137, 148, 167
Search current page, 35, 42, 47, 48, 50, 51, 62, 64, 65, 67, 92, 95, 96, 98, 100, 105, 123, 124, 125, 137, 148, 167
Secure password authentication, 67
Security Information, 41
Security Settings, 39
Select, 44
Select a profile with address only, 109, 114
Select All, 107, 112
Select time below, 72
Send e-mail to, 108, 129
Sender, 67
Server, 46
Settings, 58, 70, 71
Setup.exe, 20
SharePoint Group Name, 129, 131
Show rows, 122, 125
Show Users(s), 49
Size of Each Log, 74
SOCKS5 Proxy, 61
Solution Manager, 74
Solution Properties, 76
Specify production time: **From __ to __**, 72
SQL Authentication, 21
SSL authentication, 67
Start time, 72, 111, 115
Stop, 44, 63, 169
Summary, 109, 114, 168
Test Run, 149
Test Suite, 124
Test Suite Manager, 79, 99, 124
The __ __ of __, 72

The __ __ of every __ month(s), 72
Time format, 38
Total Log Count, 74
Trusted network, 40
Turn off automatic updates, 61
UNC path, 60
UNC Path, 91, 169
Update Manager, 60
Update Port, 61
Update Settings, 60
Upgrade, 76
URL, 46
Use an existing IIS web site, 21
Use the Net Share path as the report location, 169
Use the Net Share path as the update storage location, 60
User cannot change password, 52
User must change password at next logon, 52
User Notification Settings, 67
User Type, 51
User who is specified in the following notification file, 108, 129
Username, 36, 43, 52, 60, 61, 62, 92, 169
Username on SMTP, 67
Users, 51
Validation Test, 43, 60, 67, 92
Value, 130
View, 69, 109, 114, 123, 126
View Details, 35, 37, 63, 64, 77, 79, 91, 105, 148, 168
View History, 62, 64
Virtual Buffer Pass-through, 11
Warning, 73
Week, 58, 109, 114, 167
Week(s), 70, 89, 110, 115
Windows Authentication, 21, 42
Windows Firewall, 12
Windows User/Group, 53
Windows User/Group Name, 53
Wizard Mode, 107

Notices and Copyright Information

Notice
The materials contained in this publication are owned or provided by AvePoint, Inc. and are the property of AvePoint or its licensors, and are protected by copyright, trademark and other intellectual property laws. No trademark or copyright notice in this publication may be removed or altered in any way.

Copyright
Copyright © 2013 AvePoint, Inc. All rights reserved. All materials contained in this publication are protected by United States and international copyright laws and no part of this publication may be reproduced, modified, displayed, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written consent of AvePoint, 3 Second Street, Jersey City, NJ 07311, USA or, in the case of materials in this publication owned by third parties, without such third party's consent. Notwithstanding the foregoing, to the extent any AvePoint material in this publication is reproduced or modified in any way (including derivative works and transformative works), by you or on your behalf, then such reproduced or modified materials shall be automatically assigned to AvePoint without any further act and you agree on behalf of yourself and your successors, assigns, heirs, beneficiaries, and executors, to promptly do all things and sign all documents to confirm the transfer of such reproduced or modified materials to AvePoint.

Trademarks
AvePoint®, DocAve®, the AvePoint logo, and the AvePoint Pyramid logo are registered trademarks of AvePoint, Inc. with the United States Patent and Trademark Office. These registered trademarks, along with all other trademarks of AvePoint used in this publication are the exclusive property of AvePoint and may not be used without prior written consent.

Microsoft, MS-DOS, Internet Explorer, Microsoft Office SharePoint Servers 2007/2010, SharePoint Portal Server 2003, Windows SharePoint Services, Windows SQL server, and Windows are either registered trademarks or trademarks of Microsoft Corporation.

Adobe Acrobat and Acrobat Reader are trademarks of Adobe Systems, Inc.

All other trademarks contained in this publication are the property of their respective owners and may not be used without such party's consent.

Changes
The material in this publication is for information purposes only and is subject to change without notice. While reasonable efforts have been made in the preparation of this publication to ensure its accuracy, AvePoint makes no representation or warranty, expressed or implied, as to its completeness, accuracy, or suitability, and assumes no liability resulting from errors or omissions in this publication or from the use of the information contained herein. AvePoint reserves the right to make changes in the Graphical User Interface of the AvePoint software without reservation and without notification to its users.

AvePoint, Inc.
3 Second Street
Jersey City, NJ 07311
USA