DiskBoss

DATA MANAGEMENT

File Integrity Monitor

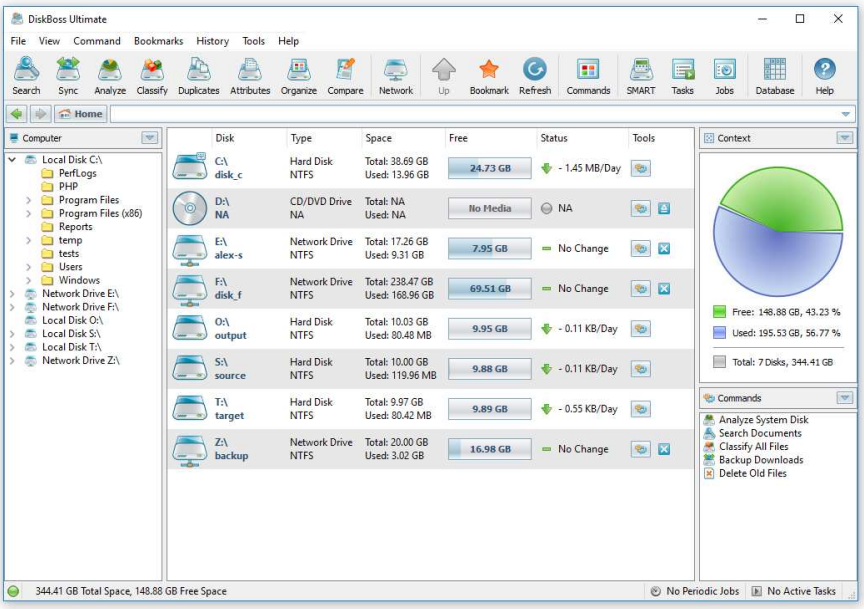
Version 9.3

May 2018

www.diskboss.com
info@flexense.com
Flexense Ltd.

1 Product Overview

DiskBoss is an automated, policy-based data management solution allowing one to analyze disks, directories and network shares, classify and categorize files, search and cleanup duplicate files, perform automated file management operations according to user-defined rules and policies, synchronize disks, directories and network shares, compare directories and files, perform bulk file delete and secure data wiping operations, detect unauthorized changes in files and directories, etc.



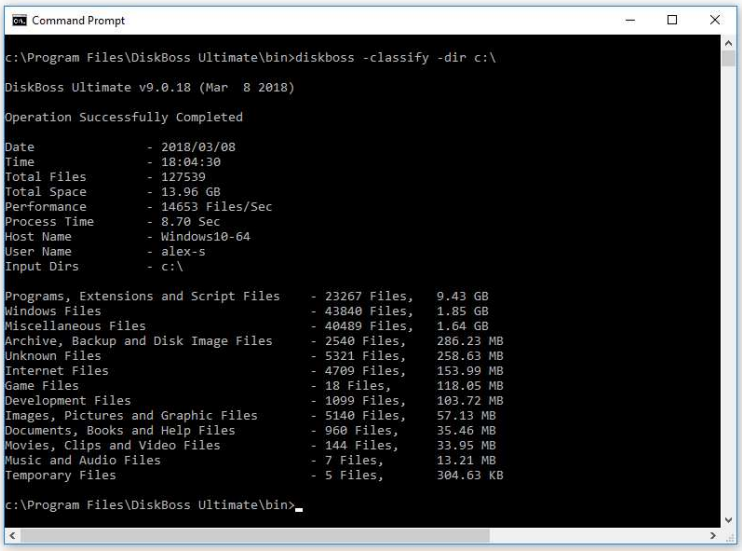
All disk space analysis and file management operations are integrated into a centralized and easy-to-use GUI application allowing one pre-configure analysis and file management operations as user-defined commands and execute any required command in a single mouse click using the DiskBoss GUI application or direct desktop shortcuts.

- Disk Space Analysis
- File Classification and Organizing
- Duplicate Files Search and Cleanup
- Bulk File Delete and Secure Data Wiping
- Automated, Policy-Based File Management
- Real-Time Disk Change Monitoring
- High-Speed File Synchronization
- Secure File Transfer Operations
- File Integrity Monitoring

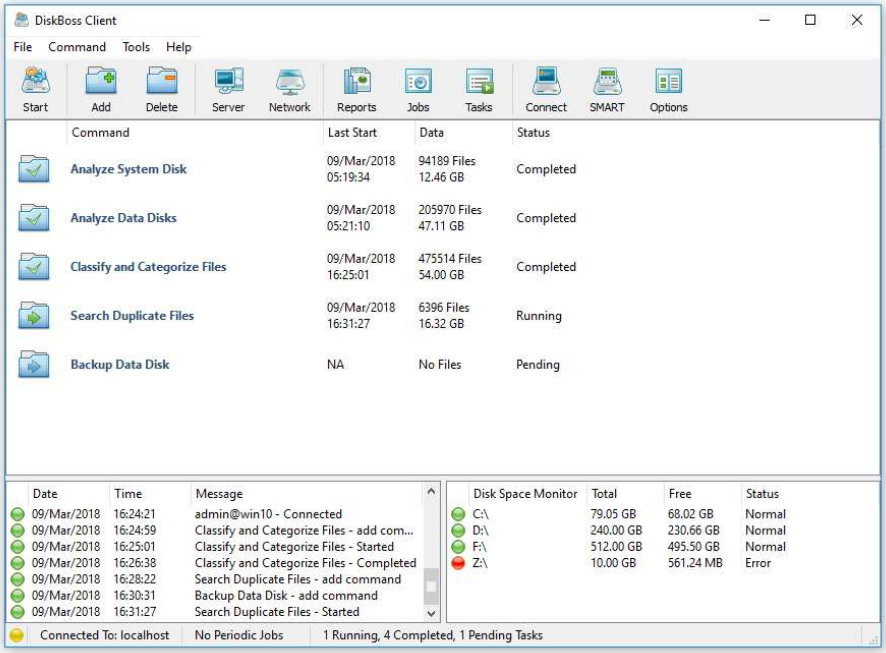
DiskBoss allows one to generate various types of pie charts and save HTML, PDF, Excel, text, CSV and XML reports for all types of disk space analysis, file classification and file search operations. The user is provided with the ability to categorize and filter analysis and file classification results and perform file management operations on categories of files.

IT administrators are provided with extensive SQL database integration capabilities allowing one to submit disk space analysis, file classification, duplicate files search and disk change monitoring reports into an SQL database. Reports from multiple servers and NAS storage devices may be submitted to a centralized SQL database allowing one to display charts showing the used disk space, file categories and duplicate files per user or per server and providing an in-depth visibility into how the disk space is used, what types of files are stored and how much space is wasted on duplicate files across the entire enterprise.

In addition to the DiskBoss GUI application, IT and storage administrators are provided with the DiskBoss command line utility, which can be used to execute all types of analysis and file management operations from batch files and shell scripts. The command line utility provides an extensive set of command line options allowing one to execute various types of disk space analysis, file synchronization, data migration and bulk file delete operations pre-configured for user-custom needs and hardware configurations.



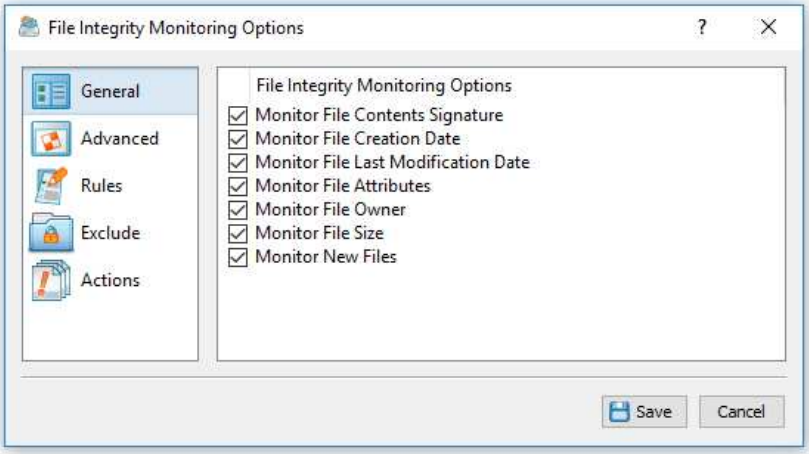
Finally, IT professionals and enterprise customers are provided with DiskBoss Server – a server-based product version, which runs in the background as a service and is capable of performing all type of disk space analysis and file management operations in a fully automatic and unattended mode according to a user-specified schedule.



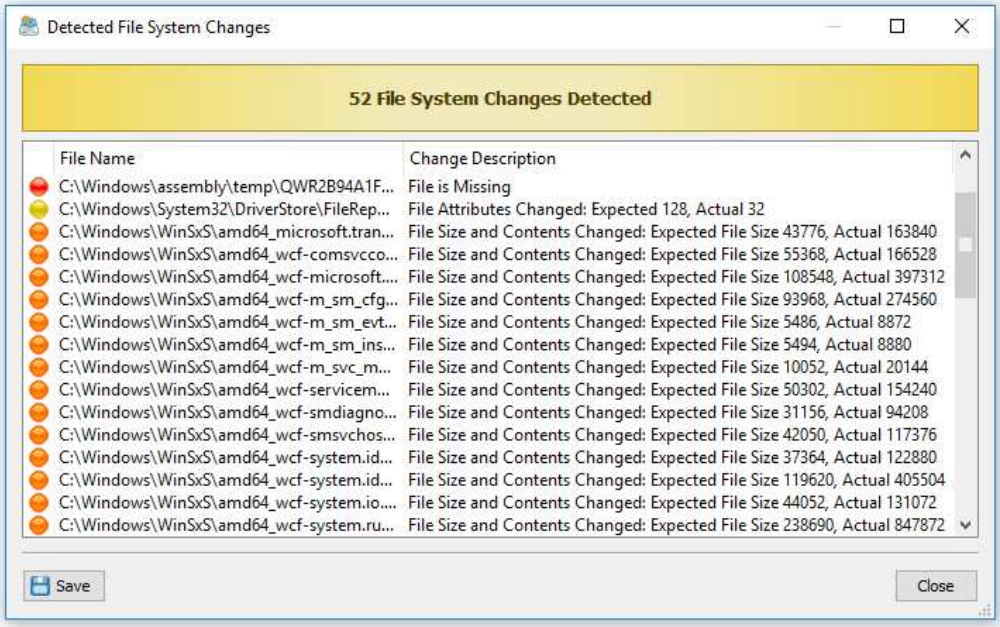
DiskBoss Server can be controlled locally or through the network using the DiskBoss client GUI application or the command line utility. DiskBoss Server provides the ability to pre-configure various types of disk space analysis and/or policy-based file management operations, schedule periodic jobs, save analysis reports into a number of different formats, export analysis results to an SQL database, periodically synchronize disks, directories and network shares and monitor critical disks and directories for unauthorized changes.

2 File Integrity Monitor

DiskBoss Ultimate and DiskBoss Server provide a built-in file integrity monitor allowing one to save digital signatures of critical system files and then periodically monitor the integrity of critical system files, detect unauthorized changes, export HTML, text, Excel CSV or XML reports and send E-Mail notifications.



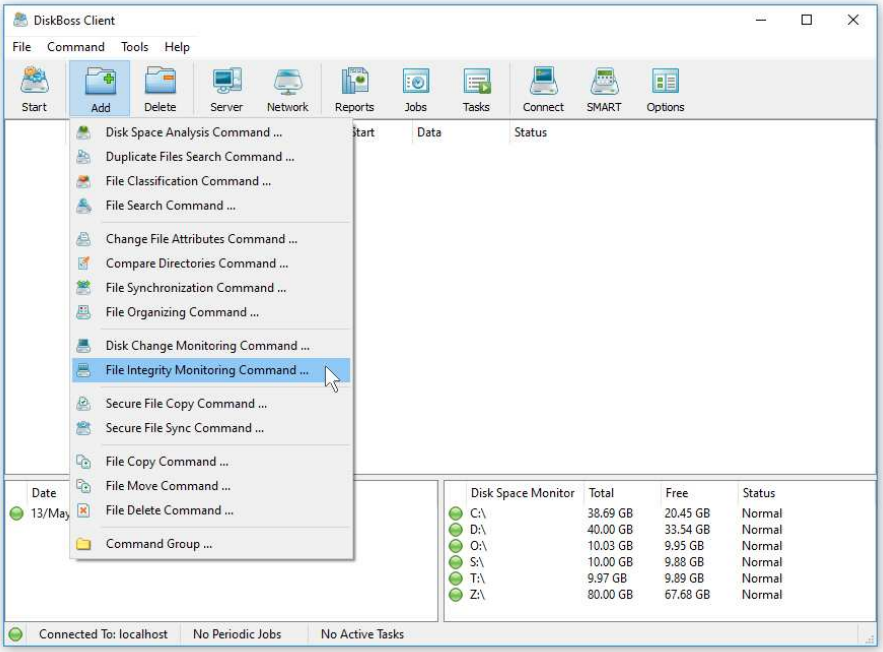
The user is provided with the ability to specify one or more disks or directories to be monitored, select which types of files should be monitored, types of changes that should be detected and optionally save reports, send E-Mail notifications or execute custom commands when a user-specified number of changes is detected.



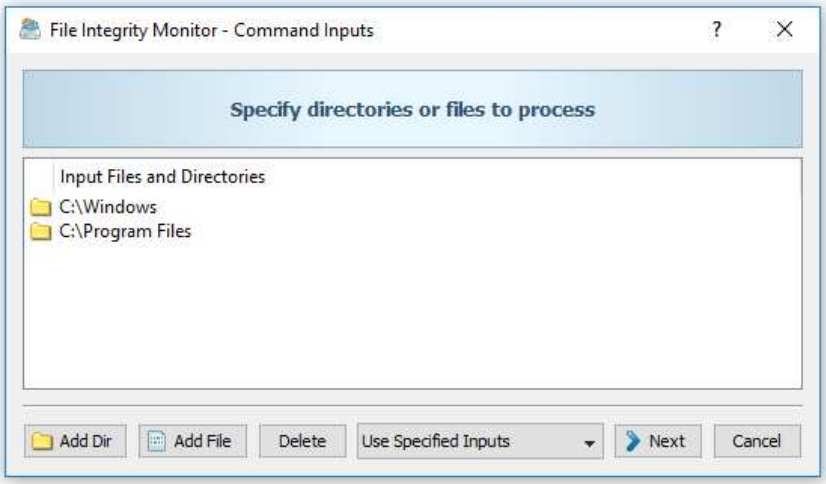
In addition to the file integrity monitoring capabilities available in the DiskBoss GUI application, DiskBoss provides a command line utility allowing one to verify the integrity of critical system files, save reports and send E-Mail notifications from shell scripts and batch files. Finally, DiskBoss Server, which runs in the background as a service, allows one to continuously monitor the integrity of system files in critical servers and NAS storage system.

3 Saving Signatures of Critical System Files

The DiskBoss file integrity monitor verifies the integrity of critical file system files by comparing a reference file system state with the current file system state including verification of digital signatures of critical system files, creation and last modification dates, attributes, file ownership information, etc. In order to be able to perform the verification process, the user needs to create a file integrity monitoring command, specify disks or directories that should be monitored, types of files that should be monitored and types of changes that should be detected.

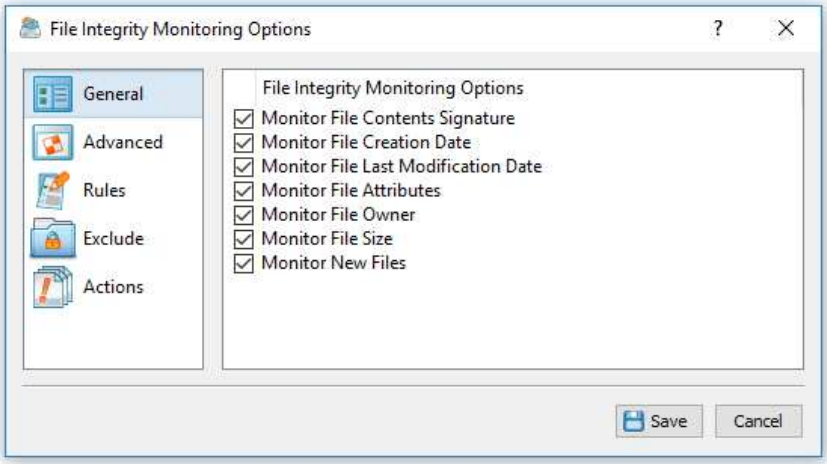


First of all, let's create a new file integrity monitoring command. On the user-defined commands dialog or the commands tool pane, select the 'Add New' menu item and select the 'File Integrity Monitoring Command' menu item. On the command name dialog, enter a unique command name and press the 'Ok' button.

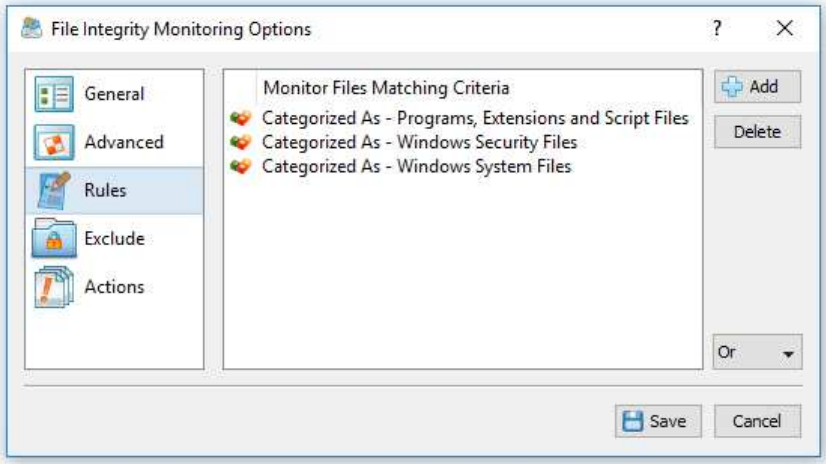


If you need to monitor the system disk on a critical server, add the 'Windows' directory and the 'Program Files' directory. In addition, on a 64-Bit server, add the 'Program Files (x86)' directory. Once finished adding input directories, press the 'Next' button.

On the file integrity monitoring options dialog, select the 'General' tab and select/unselect types of changes that should be detected. By default, the DiskBoss file integrity monitor detects all types of changes and usually there is no need to change the default configuration.



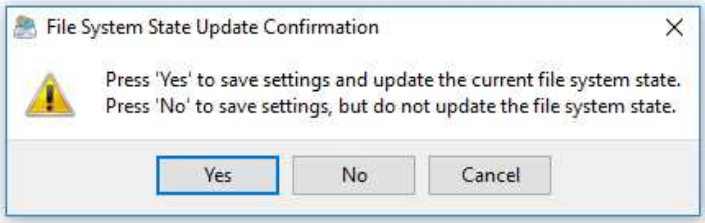
Now, select the 'Rules' tab and add one or more file matching rules specifying types of files that should be monitored. If no rules are added on this tab, the DiskBoss file integrity monitor will verify all types of files. If one or more file matching rules are specified, the DiskBoss file integrity monitor, will verify files matching the specified rules and skip all other types of files.



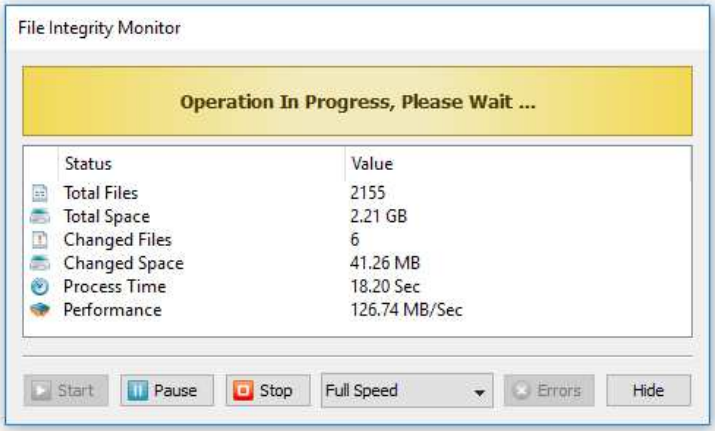
In the simplest case, just add a single file matching rule named 'Programs, Extensions and Script Files', which will match all types of programs, executable files, DLL libraries, batch files, various types of scripts, etc. For a more advanced configuration, consider adding Windows configuration files and security files.

In order to simplify the configuration process, DiskBoss provides a logically organized hierarchy of file types allowing one to easily select required file categories. In total, DiskBoss is capable of automatically recognizing more than 2,500 file types and categories making it very easy to select the types of files which should be monitored. During runtime, DiskBoss will categorize and classify file detected in the input disks and directories, verify files matching the specified rules and report all the detected file system changes.

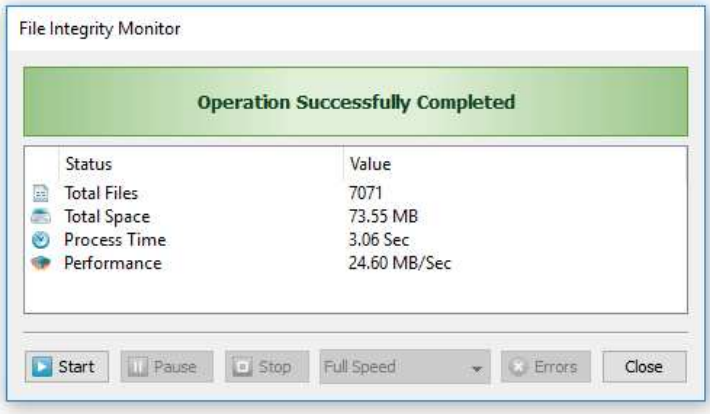
Once finished adding file matching rules, press the 'Save' button to save the file integrity monitoring command. Each time a file integrity monitoring command is saved, DiskBoss will show a confirmation message asking the user to confirm whether the command's settings and the file system state should be updated or the user wish to save just the command's configuration settings without updating the file system state file.



In general, if the user has changed input disks or directories, file matching rules or exclude directories, the file system state should be updated and the user needs to press the 'Yes' button. On the other hand, if the user has modified types of changes that should be detected and/or actions that should be executed when one or more changes are detected, there is no need to update the file system state file and the user can press the 'No' button.

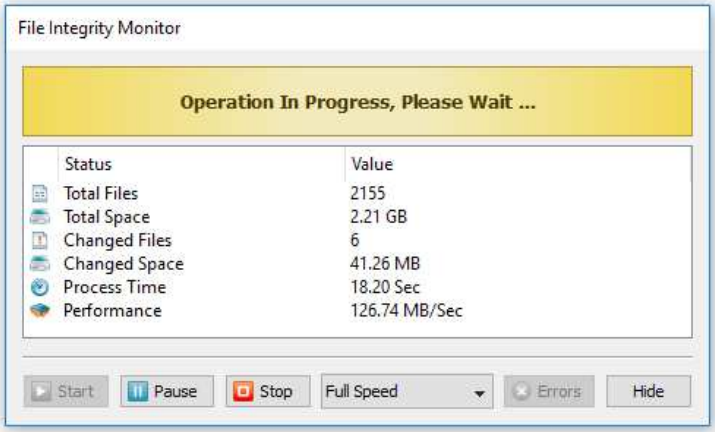


During the file system state update process, DiskBoss will display the process dialog showing the amount of processed disk space, the number of processed files and the current status. If you need to temporary pause the operation, press the 'Pause' button. Press the 'Continue' button, to resume the update operation. Wait for the file system state update process to complete and once the operation is finished, press the 'Close' button.

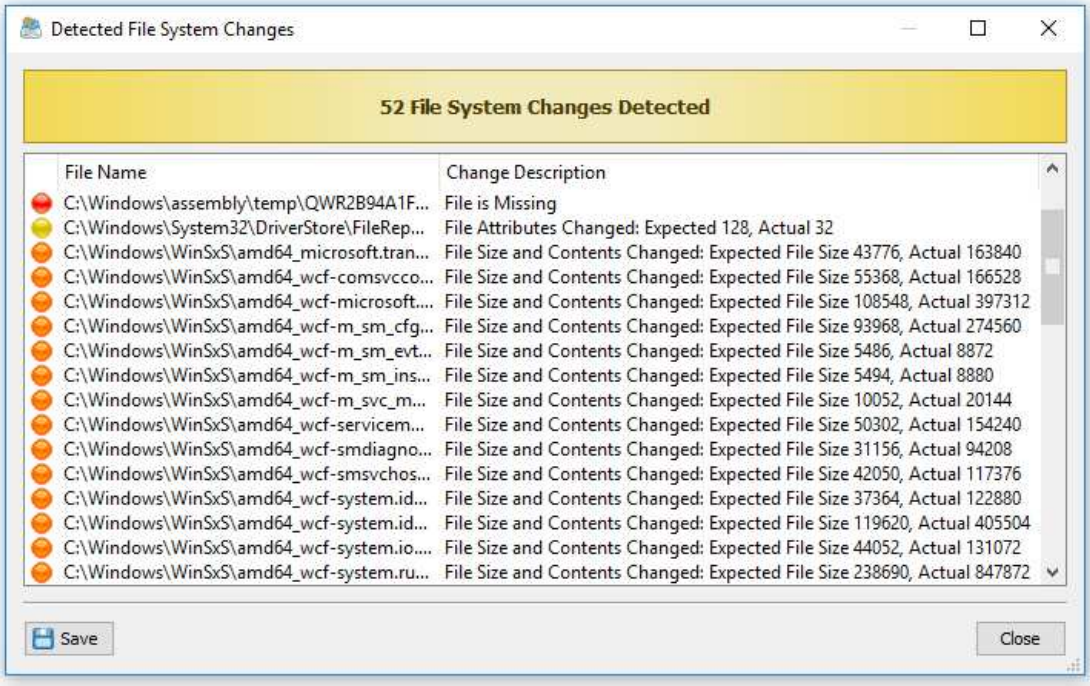


4 Verifying Critical System Files

In order to manually verify critical system files, just click on the required file integrity monitoring command in the user-defined commands tool pane. Another option is to create a desktop shortcut for the file integrity monitoring command and to execute the command directly from the Windows desktop.



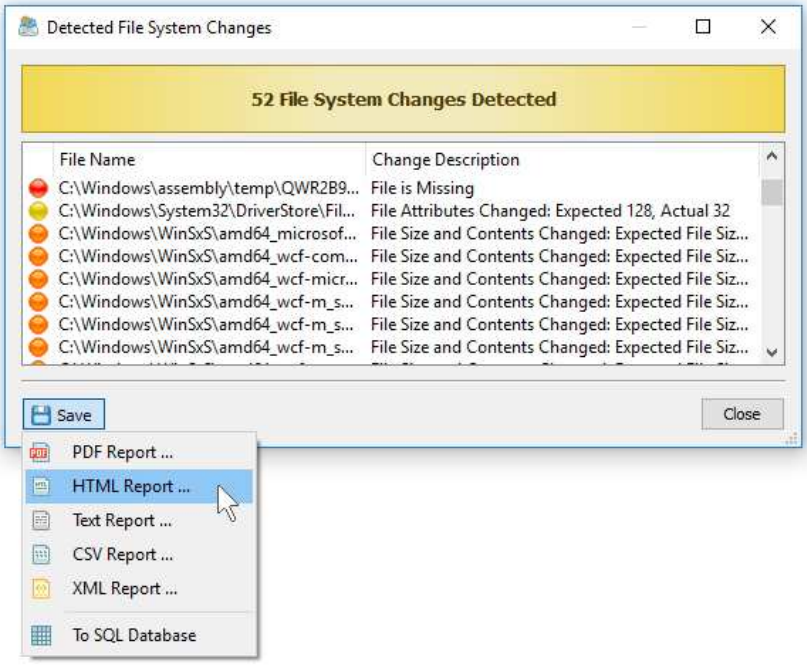
During the verification process the process dialog shows the verification status, the number of verified files, the number of detected changes, the verification performance and the process time. In order to temporary pause the verification process, press the 'Pause' button. Press the 'Continue' button to resume a previously paused verification operation.



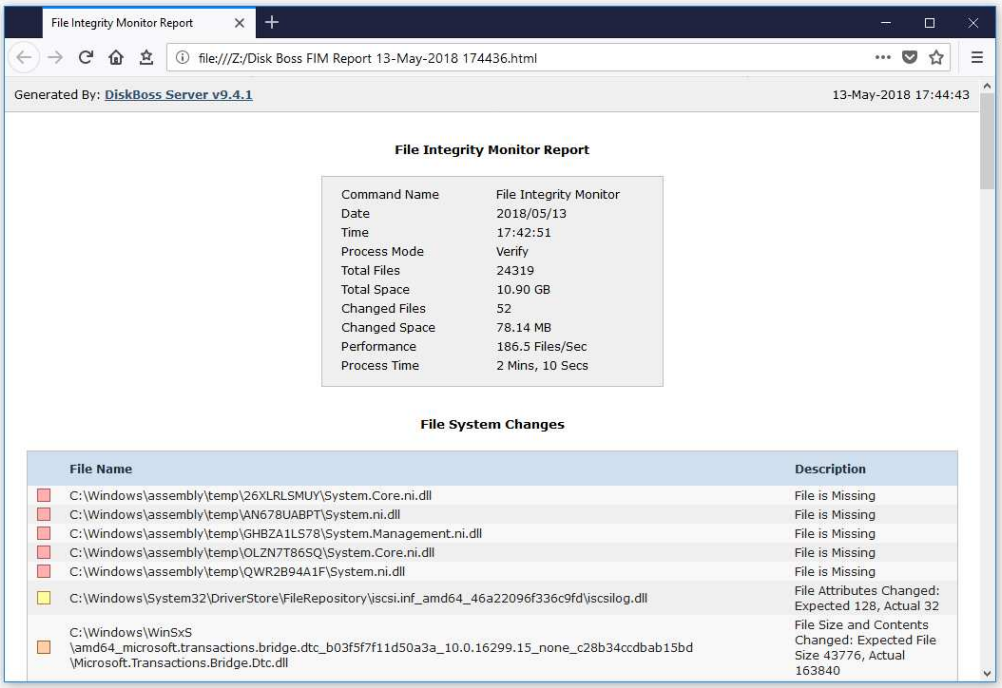
If one or more file system changes will be detected, the file integrity monitor will display the change list dialog showing all the detected file system changes and allowing one to review detected file system changes and export reports. For each detected file system change, the file integrity monitor displays the full name of the changed file and a change description explaining what exactly has been changed in each specific file.

5 Exporting Report Files

The DiskBoss file integrity monitor allows one to export HTML, PDF, Excel, text, CSV and XML report files. In order to export a report file, open the change list dialog, press the 'Save' button and select an appropriate report format.

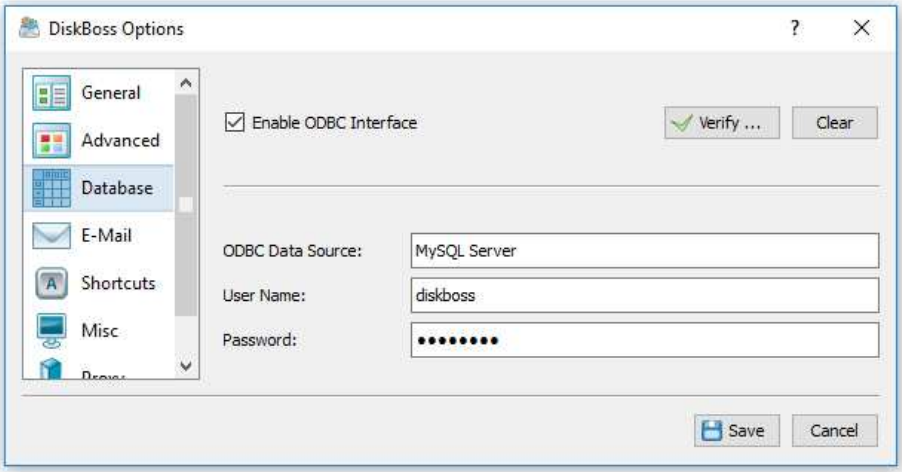


DiskBoss will open the save report dialog allowing one to select a destination directory and enter the report file name. A typical file integrity monitoring report includes a report title, a summary section showing general information and a list of detected file system changes. For each detected file system change, DiskBoss shows the full name of the changed file and a description explaining what exactly has been changed in each specific file.



6 Saving Detected Changes in SQL Database

The DiskBoss file integrity monitor allows one to save detected file system changes in an SQL database through the ODBC database interface. In order to enable database export capabilities, open the options dialog, select the 'Database' tab, enable the 'ODBC' interface and specify an ODBC data source name, user name and password that should be used to connect to the database.



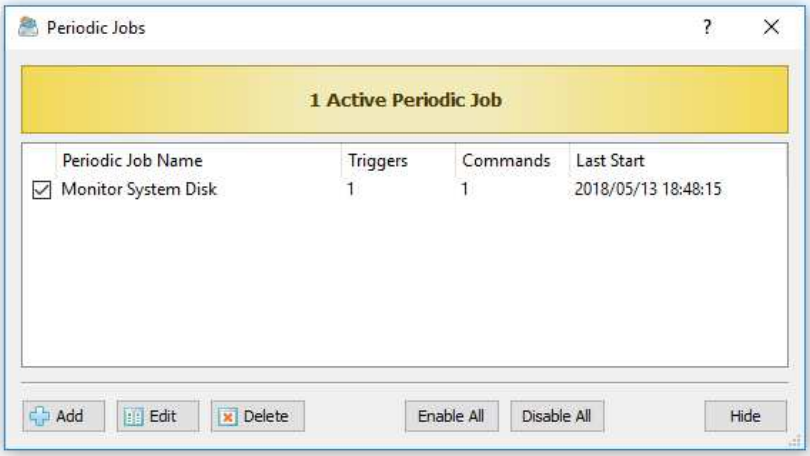
Once finished configuring the ODBC interface, press the 'Verify' button to make sure the DiskBoss file integrity monitor is capable of connecting to the database using the specified ODBC database interface. In order to manually save detected file system changes to the database, open the change list dialog, press the 'Save' button and select the 'SQL Database' menu item.

In order to see reports saved in the database, just press the 'Database' button located on the main toolbar. The top part of the database dialog provides a number of report filters allowing one to filter reports by the report type, title, host name, etc. In order to open a report, just click on a report item in the reports view.

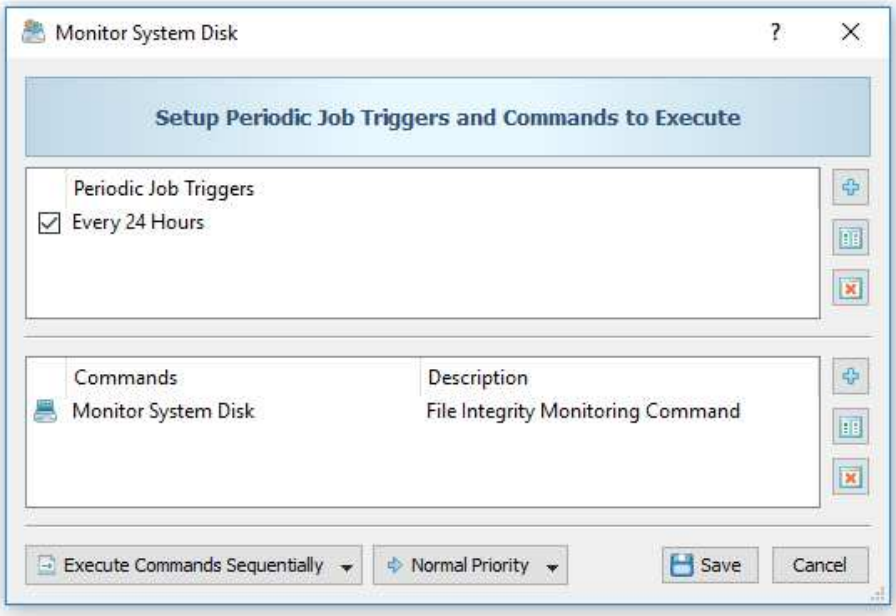
The database dialog allows one to export/import reports from/to the database. Select one or more reports, press the right mouse button and select the 'Export Reports' menu item to export the selected reports. Press the right mouse button over the reports view and select the 'Import Reports' menu item to import reports to the database.

7 Periodic Verification of Critical System Files

The DiskBoss file integrity monitor allows one to periodically verify critical system files, automatically detect unauthorized changes, generate reports, send E-Mail notifications and/or execute custom actions. In order to execute a file integrity monitoring command periodically, open the periodic jobs dialog and press the 'Add' button to add a new periodic job.



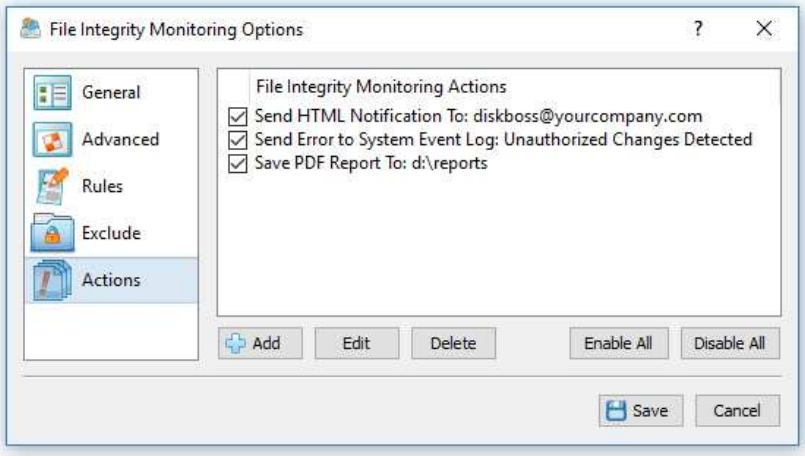
On the job dialog, select the file integrity monitoring command that should be executed and specify the required time interval. According to the selected time interval, the DiskBoss file integrity monitor will execute the specified command, verify critical system files, detect changes and optionally generate reports, send E-Mail notifications and/or execute custom commands, scripts or batch files.



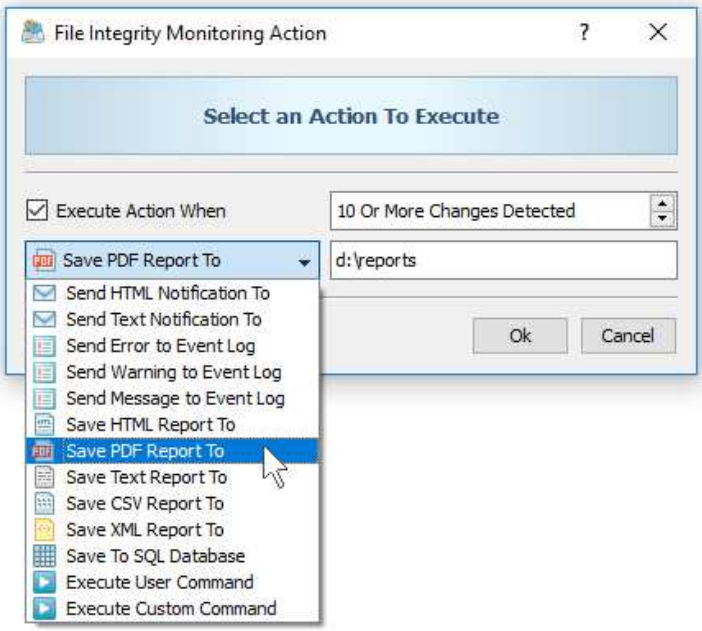
Important: Keep in mind that when using periodic file integrity monitoring commands in DiskBoss Ultimate, the DiskBoss main GUI application should be running. For continuously running mission critical servers, it is more appropriate to use **DiskBoss Server**, which runs in the background as a service and is capable of automatically verifying critical system files, generate reports and send E-Mail notifications even when no one is logged in.

8 File Integrity Monitoring Actions

The DiskBoss file integrity monitor provides the ability to automatically save reports, submit reports to an SQL database, send error messages to the system event log and/or send E-Mail notifications when a user-specified number of file system changes are detected. In order to add one or more file integrity monitoring actions, open the file integrity monitoring options dialog, select the 'Actions' tab and press the 'Add' button.



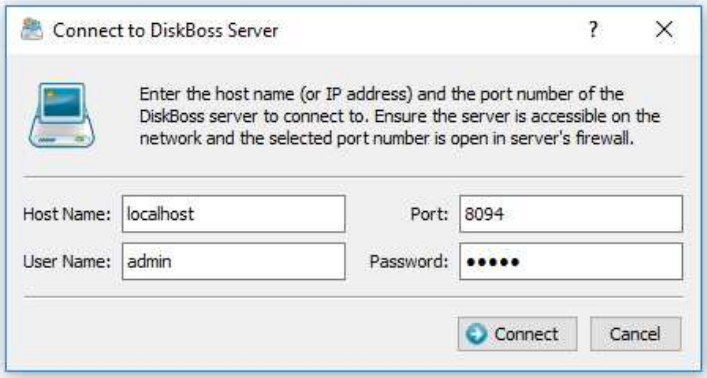
On the action dialog, enter the number of file system changes that should trigger the action, select an appropriate action type and enter an action value. For all types of report files, the action value should be set to an existing directory where to save report files or a full file name if all reports should be saved to the same file.



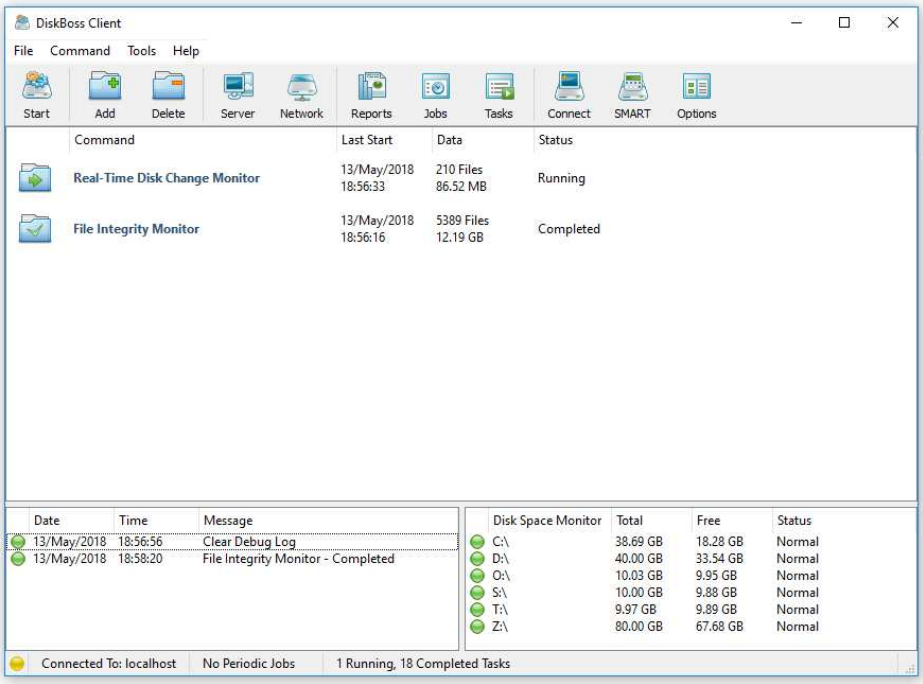
For E-Mail notifications, the action value should be set to the destination e-mail address. In addition, in order to be able to send E-Mail notifications, the user needs to open the options dialog, enable E-Mail notifications and specify an SMTP server to use to send E-Mail notifications. For system event log actions, the action value should specify a textual message that should be send to the system event log. For user-defined commands and custom commands, the action value should specify the name of the command to be executed.

9 Using DiskBoss Server to Monitor Critical Servers

DiskBoss Server, which runs in the background as a service, is capable of operating in a fully automatic mode, periodically verifying critical system files, generating reports, sending E-Mail notifications and/or executing user custom commands, scripts or batch files. DiskBoss Server may be controlled locally or through the network using the DiskBoss client GUI application or the DiskBoss command line utility.



In order to configure file integrity monitoring operations, connect to DiskBoss Server using the client GUI application, add a file integrity monitoring command and configure a periodic job to execute the file integrity monitoring operation at specific time intervals.



In addition to the ability to periodically verify critical system files, the user is provided with an option to setup a real-time disk change monitoring operation, which may automatically trigger verification of critical system files in real-time when a user-specified number of changes is detected in the system disk or the Windows system directory.

DiskBoss Server is capable of operating in a fully automated mode, without any user intervention, continuously monitoring the system disk, detecting file system changes, saving reports and sending E-Mail notifications even when no one is logged in allowing one to use it on mission critical servers requiring a high level of protection and security.

10 Using DiskBoss Command Line Utility

In addition to the GUI application, the DiskBoss file integrity monitor may be controlled using the DiskBoss command line utility, which is located in the **'<ProductDir>/bin'** directory. The DiskBoss command line utility allows one to execute file integrity monitoring commands, save reports, export detected changes to an SQL database, send E-Mail notifications, etc.

Command Line Syntax:

diskboss -fim_update <User-Defined File Integrity Monitoring Command>

This command scans the file system and updates the file system state file.

diskboss -fim_verify <User-Defined File Integrity Monitoring Command>

This command verifies critical system files, displays detected file system changes and optionally saves reports, exports detected changes to an SQL database, sends E-Mail notifications and/or executes custom actions, batch files or scripts.

Options:

-save_html_report [Report File Name or Directory]

This optional parameter saves detected file system changes to an HTML report file. If no file name is specified, DiskBoss will automatically generate a file name and save the report to the user's home directory.

-save_csv_report [Report File Name or Directory]

This optional parameter saves detected file system changes to an Excel CSV report file. If no file name is specified, DiskBoss will automatically generate a file name and save the report to the user's home directory.

-save_text_report [Report File Name or Directory]

This optional parameter saves detected file system changes to a text report file. If no file name is specified, DiskBoss will automatically generate a file name and save the report to the user's home directory.

-save_xml_report [Report File Name or Directory]

This optional parameter saves detected file system changes to an XML report file. If no file name is specified, DiskBoss will automatically generate a file name and save the report to the user's home directory.

-save_ report [Report File Name or Directory]

This optional parameter saves detected file system changes to a report file in the DiskBoss native report format. If no file name is specified, DiskBoss will automatically generate a file name and save the report to the user's home directory.

-save_to_database

This optional parameter saves detected file system changes to an SQL database according to the ODBC interface configured in the options dialog.

-v - This option shows the major version, minor version, revision and build date.

-help

This parameter shows the command line usage information.