

## Sentry II 9.0 Revision List

### Sentry II 9.0.21 Revisions:

- New feature in 'Configure->Watches/Alerts' for Watch Import/Export; easily Export selected Watches to a text file that can then be shared with other MonitorIT Servers where the Watches can be Imported from the text file; Imported Watches initially have no servers/devices assigned;
- Watch Import provides an option to auto-create a Secondary Group and assign the Watches for each Imported Watch set, which then provides easy Watch application by assigning servers/devices to the Secondary Group;
- Now ships currently with over 125 pre-configured Watches including pre-configured Watches for Backup Exec, Black Berry, Citrix, Dell, HP, Hyper V, IIS, MS Exchange, MS SQL, MySql, and Symantec EPS, and ready for Import in logical Sets of Watches;
- First time Sentry II startup has been enhanced to auto-create the Server service and auto-deploy the local Agent and create the Agent service; and now currently includes 30 pre-loaded, pre-configured basic Watches, assigned to an auto-created 'Default' Secondary Group, ready to automatically apply to any new added servers/devices; Sentry II now comes 'out-of-the-box', after Install, up and running & monitoring the local Agent with these 30 basic Watches, which will also be auto-applied to any new deployed Agents;
- Enhance 'Configure->Watches/Alerts' so that it now supports and allows saving New or Edited Watches that have no servers/devices assigned for all Watch types except CounterWatch, WinServicesWatch and ServerWatch;
- New ServerWatch SIP type for Session Initiated Protocol checking; this is a UDP, send request & receive response protocol check suitable for Telephone/PBX systems that support SIP, and other UDP port checking;
- Enhance the 'ServerWatch-AGENT Check' type Watch with a new '%CPU' parameter to monitor total percent CPU Utilization at a default 90% threshold;
- Enhance the latest 9.0.21 Agent to monitor total percent CPU utilization automatically; sampled once every 5 minutes with the value averaged over the 5 minute interval; the value is used for the 'Monitor->System Monitor' display of running Averaged and Last %CPU; and used for the 'ServerWatch-AGENT Check' monitoring;
- Enhance the 'Watch Report' feature in 'Configure->Watches/Alerts' with a new option to report by one or more Watches with all the Watch details and a list of all the servers/devices assigned; this compliments the previous option that reports by Server/Device;
- Miscellaneous:
  - Change User Logon/Logoff monitoring in the Agent to not treat status query errors as a Logoff;
  - Fix issue with Agent, introduced in previous 9.0.17 version in a new WMI call, that causes high-CPU utilization on Win2000 servers with a faulty

WMI install;

- Complete 'roll-up' of all the User Logon/Logoff monitoring feature fixes and enhancements introduced in 9.0.17;
- Fix the Memory utilization calls, used by the MonitorIT Server in its 1 minute uptime log messages and in the Agent 'ProcessWatch' thread, so that the PSAPL.DLL in the System32 folder is used to insure compatibility; also load the DLL only 1 time on the first call;
- Change the 'Network Status Display' on a database change message due to a Watch change to only query for the updated Watch info and eliminate the call to get OID info and the refresh of the display so as to minimize overhead especially when there are multiple open NSDs;
- Enhance FileWatch monitoring with the 'NOT' option for a specific file using the 'Duration' so that it will alert if a file is not created within the 'Duration' time frame;
- Fix 'Schedule Periodic Reports->Queued->Edit' issue with the EventLog 'Query' pop-up; it was not clearing the settings from a previous Edit so they looked wrong for the current Edit.
- Enhance the PING Checking thread to catch any faults and prevent the thread from getting terminated;
- Increase the default stack size for the main MonitorIT Server thread from 512KB to 655KB;
- Add prompt in 'Manage Agents' so the user can opt out of a Discovery, at the start and after each domain, if the 'Discovery' checkbox is checked;
- Filter negative CPU monitoring values that are occasionally seen, usually the result of a server reboot, and which result in a false alert;
- Prohibit the user viewing the 'Configure->Domains' screen if the user rights are not Full Administration;
- Fix problem with an Agent MUTEX that would occasionally be left set and prevent Agents from logging on again if previously disconnected;
- Streamline the 'System Monitor' lookup and handling;
- Accept the tilde character as valid in the Logon->Password in 'Manage Agents';
- Filter out negative SNMP values in SNMP Query Monitoring;
- No longer include MDAC in the download release; all Windows version today include it already;

### **Sentry II 9.0.17 Revisions:**

- New Agent and Agentless Logon/Logoff monitoring and reporting;
  - Monitor and report on interactive User Logon/Logoff activity for Windows;
  - Monitor servers & workstations with a deployed Windows Agent, or optional Agentless monitoring of remote servers & workstations using one or more deployed Windows Agents to monitor these remote, Agentless servers & workstations;
  - Each Agent can handle monitoring up to 500 remote, Agentless servers & workstations;
  - New 'User Logon/Logoff Data' Report in 'Run/Analyze & View' and 'Schedule Periodic' Reports';
  - New User Logon information in the pop-up tool-tips in 'System Monitor' and 'Network Status' displays;
- New 'Logoff' button for the 'console' so that you can exit and login with different user credentials without having to exit any other open IE windows;
- Enhance Agent to track and log its own CPU and Memory use for diagnostic purposes;
- Enhance MonitorIT Server and Agent to free its "send" buffer after any operation that uses a buffer larger than 512 bytes for more efficient memory use;
- Enhance the 'Watch/Alert Dependency' option on the 'Schedule' tab in 'Configure->Watches/Alerts' for ServerWatch type watches with a new option to specify a Watch name that can include the &N and &G macros to resolve the name down to a dependent Watch based on the name of the Server or the Group it belongs that is causing the alert condition;
- Enhance 'Configure->Watches/Alerts' so that on an Edit in the 'Selections' primary Group tree view, it auto expands those Groups that have servers/devices assigned to the Watch;
- Speed up the displaying of information to the 'Memory Monitor', 'HDD Monitor', 'System Monitor' and 'Network Status' displays; also speed up the 'Manage Agents' display;
- Enhance memory use so that after a decompression of a Receive message, call "realloc" to free memory used;
- Enhance Server logging with the addition of CPU and Memory used by the primary MonitorIT Server process 'RPMCCS.EXE' added to the one minute uptime log message;
- Additional Agent logging information on received events to the various Event Logs;

- Miscellaneous fixes:
  - Fix Agent to suppress any Windows error pop-up prompts if it ever tries to access a drive with removable storage such as a floppy drive;
  - Fix a 'memory fault' in updating Agents via 'Manage Agents';
  - Fix 'Configure->Group' edit to inhibit changing the Group type ('Primary' & 'Secondary'); and fix a problem in 'Assign Servers' where you could not uncheck a server once it was checked;
  - Fix problem with truncating the SNMP Trap VB data at a max of 256 characters when writing to the database; the new max is 1024;
  - Fix problem where an 'Agent' alert for Disk, Memory or Page File threshold did not log the 'Notified' state, and thus the report was not correct regarding 'Notified';
  - Fix problem with the 'Alert Notifications->ServerWatch' report if a large Email Subject was specified as part of the alert information; it caused a data truncation error when reading this from the database and aborted the 'ServerWatch' aspect of the report;
  - Change Disk threshold alerts so that the Severity on the 'Network Status' display is Critical-Red if the free space is less than one-half the threshold and Severe-Maroon if less than the threshold;
  - Self-monitoring of the MonitorIT Server's working set memory use and auto-restart if use exceeds 225000 KB for more than 10 minutes;
  - Fix a couple of problems with the #IF TIME... conditional email address feature; previously it was not resolving the &G and &N macros; add an OR option to the syntax and fix issue looking for the #END in a nested statement;
  - Fix problem with 'Email Group expansion' and 'AGENT Check conditional email address syntax processing' when either of these features are included in the '#IF TIME...' conditional email syntax feature;
  - Fix problem with CounterWatch reports where one counter would be skipped in the report for each server; this problem was introduced in 9.0.14;
  - Fix problem that occurs in rare instances when the MonitorIT Report Analysis thread hangs on startup causing high CPU utilization;
  - Fix the 'Delete' Group function so that when deleting all servers in the Group, those servers that have a connected Agent are sent a message so that the Agent uninstalls itself;
  - Fix the 'Logon->User Name' field in 'Manage Agents' so that only the tilde ('~') character is excluded; previously the exclamation and other special characters were excluded;

- Miscellaneous minor bug fixes found during the memory use review; include logging some 'Catch Fault' errors if any occur during 'DestroySocket' and 'NotifyDisconnect' connection processing;
- Fix memory leak in the Object Cache Lookup;
- Includes the roll-up of the miscellaneous robustness fixes by tightening up the mutex processing for some Agent and List operations.

### Sentry II 9.0.14 Revisions:

- Enhance the custom 'Counter Watch Reports' based on user custom collection sets with a new checkbox option on the 'Collection Set->Parameters' tab that filters the counters in the report and only displays those counters which exceed their specified, user defined 'Suggested Average' or 'Suggested Maximum' values; essentially this is a 'report by exception' and significantly improves report generation time, minimizes the report output length, and displays only those counters exceeding suggested average and maximum values over the report interval;
- Enhance 'Email Address' handling in 'Configure->Watches/Alerts' with a new Conditional Time/DayOfWeek option for determining who gets emailed when; Syntax is:

```
#IF TIME GT hh:mm AND LT hh:mm AND DOW n-m #THEN address1,address2 #ELSE  
address3 #END
```

- a) Where DOW = 1 for Sun thru 7 for Sat; range is optional;
- b) And GT, LT, EQ, DOW, AND, #ELSE are optional but at least one of GT, LT or EQ required;
- c) May be nested after #ELSE, e.g. #IF TIME ... #THEN addresses #ELSE #IF TIME ... #THEN addresses... #END #END
- d) Or nested with unconditional addresses, e.g. address1,address2, #IF TIME ... #THEN address3 #END

- Enhance ProcessWatch with a new checkbox option called 'Inc All'; when the 'Process Name' spec is a wild-card and the 'Incl All' checkbox is checked, then the cumulative CPU utilization of all the processes matching the spec is checked against the 'CPU (%)' threshold and alerts only if the cumulative CPU utilization exceeds it;
- Support the Conditional ServerWatch AGENT type syntax used for Email Address in the 'Action->Program->Program Name' field as well so that a program can be executed based on the AGENT check alert type.
- Enhance the look of the select new Watch pop-up display in 'Watches/Alerts'; better formatted text and uses 'radio' buttons;
- Enhance the Email Address pop-up edit box in 'Watches/Alerts' so the help is in a separate pop-up tool-tip;
- Enhance the performance of the 'Server/Workstation General' CounterWatch report;
- Enhance the screen loading performance of 'Configure->Watches/Alerts', and to a lesser extent other screens such as the report screens 'Create CounterWatch Reports' and 'Schedule Periodic Reports';
- Enhance the Console Introduction screen to include the current Access database size, if using Access, and pop-up an alert message when the database size exceeds 1.8 GB to alert the user to do a Repair operation to compact and repair the database before it hits the 2GB maximum; the steps to do the Repair operation are included with the pop-up;
- Enhance MonitorIT console logon authentication so that it now supports users anywhere in the Active Directory 'Forest' not just the local domain; now uses the AD 'Global Catalog' to authenticate; and now also uses 'FAST\_BIND' for better

performance in determining valid user credentials;

- Add a new Global option in 'Configure->Security' called 'Active Directory (or LDAP) Path for Verification' to allow the user to override the default path to the Global Catalog;
- Enhance SYSLOG from Linux/Unix to handle Syslog messages originating from Linux/Unix behind a WAN Router that will have a different IP address as the source of the SYSLOG; this involves editing the Linux server entry in "Servers/Agents & Devices" and appending the local IP address to the WAN address (picked up by MonitorIT) separated by the characters "<+>", for example:  
10.22.45.35<+>192.168.1.101 In this case, for Syslog monitoring via a proxy Windows Agent, it will use the Local IP Address (in this example, 192.168.1.101) as the valid originating IP address for the Syslog messages;
- Miscellaneous fixes:
  - Fix problem that was causing RPMCCS.EXE faults and MonitorIT auto-restarts; problem was related to the new Audit log feature introduced in 9.0.08;
  - Fix problem with deleting an 'orphaned' (that is no assigned servers or services) WinServicesWatch; if a WinServicesWatch was displayed prior to the delete, then the previous Watch that was displayed had its servers & services deleted and therefore 'orphaning' that Watch;
  - Fix problem in EventLogWatch and SyslogWatch displays 'Configure Filter'; occasionally when selecting the watch from the list box it would hang and not display any server/device entries;
  - Fix problem in 'Schedule Periodic Report' edit of EventLog and Syslog Data reports and Alert Notifications report; if selecting 'Choose Servers/Devices' it would not expand the tree view to show the currently selected items in the report;
  - Fix 'Session Log' in 'InvAnalysis.ocx' in 'Reports->Run/Analyze & View' where the 'Description' field in the record is greater than 256 bytes due to Group, Server or Watch restrictions; previously the report would show the user as 'Unknown' for a session;
  - Fix 'Average Disk secs per operation' type counters and eliminate a scaling of 100,000; now the Counter displays the actual unscaled value which can be quite small;
  - Add an Import & Export option to the 'Archive->EventLog View/Archive & Report' function for 'Load Filter'; now you can Export View filters from one MonitorIT Server and Import to another;
  - Fix an issue with FileWatch where in rare scenarios, alerts would not be generated due to a database write error; the scenario may occur when monitoring folders or wild-cards and many files are added or deleted resulting in a long string of information included with the alert; when the scenario occurs, FileWatch will not subsequently alert;
  - Fix the vulnerability in an EventLogWatch 'Edit' in 'Configure->Watches/Alerts' that would lead to the servers assigned to the Watch being

deleted; this could happen if you navigated away after clicking 'Save' before the Watch edit was complete; the vulnerability window is now closed and the Save is faster in completing;

- Fix the 'Configure->Security' option when specifying an Active Directory Group so that members are allowed; this validation against the Group error resulting in the validation failing was introduced in the previous 9.0.09 version;
- Fix the Alert Notifications report for FileWatch; previously there were a couple of fields that were not displayed with the correct information;
- Fix the 'Available Physical Memory' check so that it now handles very large numbers in computing the percentage available;
- Fix issue with 'Create CounterWatch Reports' where no 'Save' or 'Cancel' buttons displayed if the entry started with no servers assigned so you could not Edit to fix it and then Save;
- Fix 'Utilities->Database Maintenance->Purge'; with 9.0 the manual purge did not start due to a page script error;
- Fix problem with Agent where it would not enumerate the running processes correctly to ProcessWatch when selecting a server to see its running processes;
- Fix bug in the logical drive list management and processing which would lead to a truncated 'HDD Monitor' display as a symptom;
- Fix FileWatch send email alert problem due to File List and Date/Time text with a single 'OA' carriage-return character in the text; likely only occurs with some non-Exchange email servers;
- Fix problem with adding a new device with PING service in 'Servers/Agents & Devices' and then going to 'Watches/Alerts' to define the PING watch and the device is not visible;
- Fix the 'Audit.log' so that passwords from an 'Install Agent' operation are asterisked out;
- Fix 'ProcessWatch' by reverting back to previous 'OpenProcess' call arguments; should now work for all Windows versions including Win 2008 and VISTA;

### **Sentry II 9.0.08 Revisions:**

- New Win2008 Server & VISTA 'evtx' Event Log handling fixes:
  - Fix problem with resolving event Descriptions for all the Win2008 & VISTA 'evtx' event logs including the new logs;
  - Support for monitoring and archiving all the new Win2008 & VISTA event logs, including the new 'Microsoft-Windows-.../ Operational' event logs, using the Custom Event Log feature;
- Add New Audit Log feature to log all configuration changes made including who made the change and what the details are; the audit log file is called 'Sentry IIAudit.log' and is found in the '...\Sentry II\Bin' folder;
- Enhance 'Configure->Security' with a new Administration right called 'View Only'; this has the rights of 'Limited' Administration but further restricted to 'View Only' on the allowed 'Configuration' displays;
- Enhance the 'Action->Program' alert option for automated alert remediation and recovery with new options to specify the Username/Password credentials and have the specified executable run under this user security context; and also new options to specify the 'Working Start Directory' for the executable, and an option to 'Show Window' for the executable's Window GUI; this executable can be any Windows Batch, Script such as VBS & WMI, COM, EXE;
- Enhance 'CustomWatch' to also provide options to specify the Username/Password credentials and have the specified 'custom' executable run under this user security context; and also new options to specify the 'Working Start Directory' for the executable, and an option to 'Show Window' for the executable's Window GUI; this executable can be any Windows Batch, Script such as VBS & WMI, COM, EXE to extend and enhance Sentry II's monitoring capabilities; 'CustomWatch' will monitor for the termination of the executable and query for its exit code which can then be used to indicate success or failure and integrate this into Sentry II's standard alert processing including the enhanced 'Action->Program' alert option for automated alert remediation and recovery;
- Enhance the RPMCOMM.OCX and MONITORITLIVE.OCX to support a scripting interface for VBS, Powershell and other Windows scripting tools; include some initial sample scripts in the new '...\Sentry II\Scripts' folder; we will be expanding the scripting support with more samples and a documented interface;
- Miscellaneous fixes:
  - Fix problem with EventLog Archiving feature where it archived logs without appending the required originating machine name and thus the Archive Viewer would not process these logs;
  - Fix previous problem with Custom Event Log monitoring when in some cases after an Agent reconnect, monitoring of Custom Event Logs would stop;
  - Extend time-out on Agent updates via 'Manage Agents' to 4 minutes to accommodate updates over low-speed link Agent connection;
  - Prohibit EmailGroup 'Deletes' if logged on with less than 'Full' Sentry II Admin rights;

- Fix 'Monitor->System Monitor' so clicking the 'Refresh button will update any Agent version number changes;
- Fix 'Archives->EventLog View/Archive & Report' so that the Viewer feature sorts properly when an event description contains a string of '?' characters; previously this would prevent the sort from working correctly;
- Fix an Event Log archiving issue with determining a log file name if the associated Registry entry did not contain the 'File' value; now if the Registry entry value 'File' does not exist for a particular event log, it defaults to using the log name for the file name and uses the default folder depending on whether it is a Win Server 2008/VISTA 'evtx' log or an earlier 'evt' log;
- Fix problem with 'Utilities->Database Maintenance->Object Filtering' so that a change will activate filtering immediately;
- Update the 'Services' table and change the 'SendString' field to 'ntext' in the SQL database file 'MonitorIT.mdf'; this is done programmatically when using the database file but creates an 'Import' issue when trying to import to it from the Access database;
- Fix Edit and Delete of Email Groups so any name change or deletion is reflected in all the 'Email Address' fields of all Watches, and all 'Scheduled Periodic Reports' where the affected Email Group is referenced;
- Fix sorting problem on the Network Status Display where previously the 'Low' severity 'Olive' color option was treated as lower than active Maintenance 'Black' status;

### Initial Sentry II 9.0 Release as version 9.0.03:

- Update and freshen the user interface color scheme;
- Update the Reports with the new lighter color scheme;
- Win2008 Server/VISTA Workstation Issues:
  - Fix WinServicesWatch issue where checking service status and restarting non-running services on some services would fail;
  - Fix issue with CounterWatch on some Win2008 servers for the default 'System' Object Counters displayed in the display 'Monitor->System Monitor'; this should resolve the CounterWatch issue seen with this on some Win2008 servers;
  - Enhance 'EventLog View/Archive & Report' so that the Archive Viewer can view both EVT and EVT X (from Win2008 Server and VISTA) Archives when the Sentry II Server is itself running on a Win2008 Server or VISTA Workstation; previously in this configuration, only the EVT X Archives could be viewed; there is still an issue when trying to view EVT X Archives when the Sentry II Server runs on a server or workstation earlier than Win2008 or VISTA;
  - Fix Agent faulting issue on Win2008 and VISTA which caused Agent to auto-restart;
- Enhance 'Configure->Security' with:
  - New option to restrict a user to selected Watches; in 'Configure->Watches/Alerts' and other screens that display Watches, the user is only able to view and change the selected Watches to which he is restricted;
  - Change the security setting for 'Allow Administration->Limited Rights' so that the 'Configure->Security' and 'Utilities->Database Maintenance' screens are prohibited; previously 'Configure->Servers/Agents & Devices' was prohibited, but now that is allowed; also the option to set the global SMTP parameters for email are also restricted unless Full Admin rights;
  - New option to restrict a User to selected Servers/Devices across one or more Groups; this new option compliments the previously existing option to restrict a User to selected Groups, and affords more granularity by allowing access to select Servers/Devices within a Group; this new option can be used in conjunction with the Group restriction or independent of the Group restriction;
- Enhance FileWatch:
  - With new checkbox option 'Include Subfolders' to extend the specified FileWatch rule parameters to the 1<sup>st</sup> level subfolders of the specified folder; also, in this scenario, the 'Include All' checkbox option has also been extended to mean that if checked, the 'Max Size' and 'File Count' parameters apply to the COMBINED 'Max Size' and/or 'File Count' of the specified folder and the 1<sup>st</sup> level subfolders;

- So that if there is a match on a 'Search String' then the alert detail information shows the line of text that contained the matched search substring; previously it would show the preceding 128 characters and trailing 128 characters;
- 'Search String' parameter so that it supports a test of a numeric value as part of the search substring; The syntax for checking a numeric value as part of a search substring is as follows: <#GT nnnn>, <#LT nnnn> or <#EQ nnnn> where GT is 'greater than', LT is 'less than', and EQ is equal; for example, a 'Search String' of 'Value: <#LT 2000>' would be a match only if the file text contains a substring such as 'Value: 1999' because 1999 is less than 2000; whereas, a substring such as 'Value: 2001' would not match;
- 'Search String' with new support for Boolean AND search with multiple substrings using the plus sign, and Boolean OR using the comma, for example, s1+s2,s3+s4, meaning if substrings s1 AND s2 are found OR s3 AND s4 are found then there is a match. Any combination of substrings using the plus and comma are accepted such as s1+s2+s3 or s1+s2,s3,s4, etc. The comma has the highest precedence meaning combinations separated by comma are parsed 1st, and then within that, combinations with plus are parsed;
- Expand the Exclude Logical Drive parameter 'Excl Drv' in the 'ServerWatch-AGENT Check' Watch to a maximum length of 900 characters to hold exclusions for multiple, long Mount Point drive names, and also add a tool-tip to view the contents of the parameter when hovering with the mouse over the field;
- Enhance the Exclude Logical Drive parameter 'Excl Drv' parameter in the 'ServerWatch-AGENT Check' to support the asterisk wild-card as the last character in an exclude drive specification; for example, 'Syslog\*' would match and exclude any drive, such as mapped drives, that are defined as Syslog\A, Syslog\B, etc;
- Add a new ODBC IP Service for 'ServerWatch' checking and to compliment the existing SQL and ORACLE for pro-active database checking;
- Enhance ProcessWatch by adding the 'User Name' info that is reported along with the other process information on a ProcessWatch alert;
- Fix problem with EventLog and Syslog Archive Viewers when searching for records whose start and ending time was in a previous year;
- Change confirm in 'Configure->Groups' when assigning Watches to request confirm without listing all the Watches; previously, if many Watches, the OK button was not visible;
- Fix issue with Page File monitoring calculations with very large Page File space, for example, 32GB or larger;
- Fix Agent so that in an EventLogWatch 'Description' parameter, you can specify &T to represent a Tab character in the 'Description' match substring, or you can specify the match substring with no character where the Tab character would be; the Agent matching will strip Tab characters before the comparison search;

- Change the AgentService.exe so that on an Agent uninstall, via 'UninstallAgent.asp' or 'AgentService.exe -u', it does not flag to have itself deleted on the next system reboot; this was causing a problem when the user would uninstall and Agent and then re-install the Agent; since the 'AgentService.exe' was flagged to be deleted on the next reboot, if the user reinstalled the Agent, the next system reboot would still delete the 'AgentService.exe';
- Enhancement to Agent 'Keep-alive' processing to treat CounterWatch data and EventLog data as a 'Keep-alive' and evidence of a connected and functioning Agent;
- Filter out 'Maintenance Mode Active' status items from the 'Alert Notifications' Report for 'ServerWatch' type alerts;
- Fix problem with the DST switch handling; Enhancement to handle the Standard Time - Daylight/Summer Time switch so that Scheduled Reports and Maintenance Plans are adjusted correctly;
- Fix the support for Boolean AND using the plus character in the SyslogWatch 'Content' parameter, and the EventLogWatch 'Description' parameter; previously it did not work correctly;
- Fix issue in the 'Network Status Display' handling that would occasionally cause a lock-up and an auto-restart under situations where a 'Server/Device Maintenance' update was in process, particularly with servers monitoring 500+ Agents and a NSD 'Status Interval' of 3+ days;